QCMC2012

TU WIEN

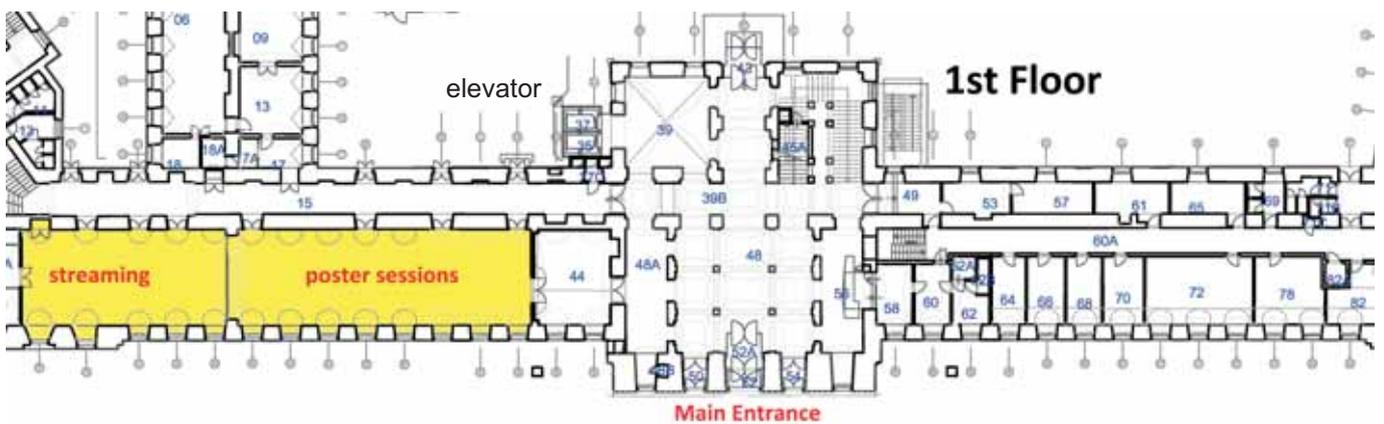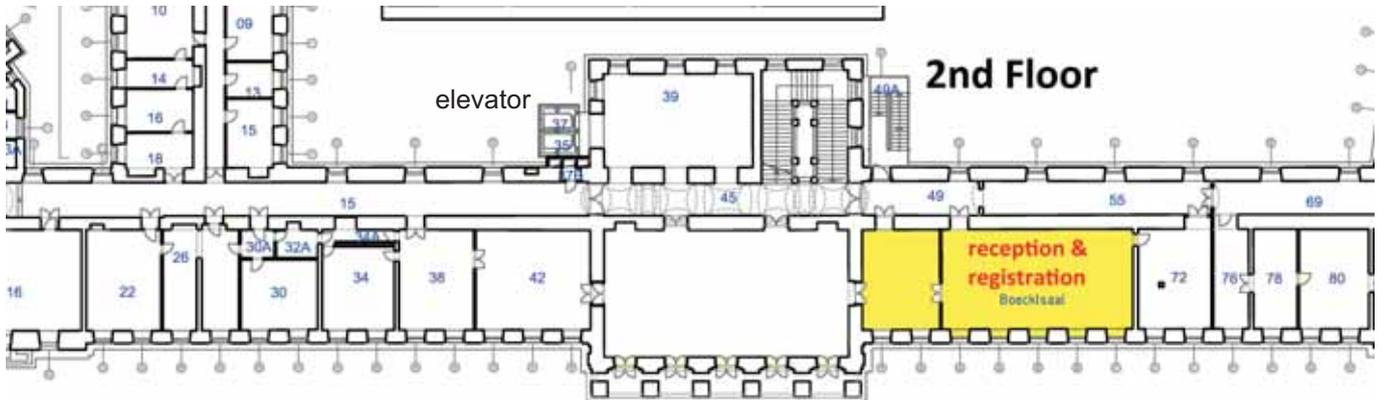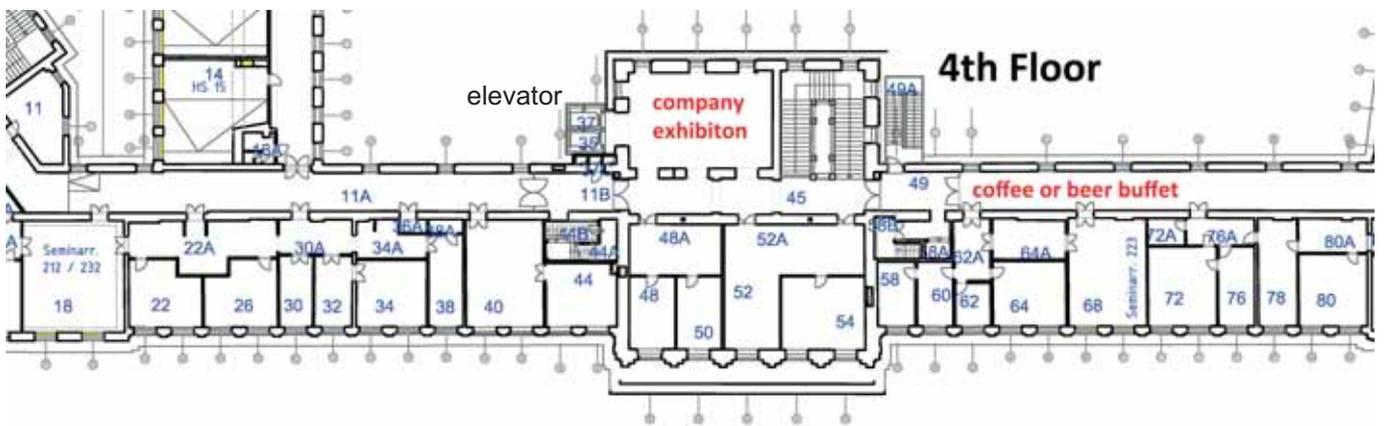**11th Intl. Conference on Quantum Communication, Measurement and Computing**
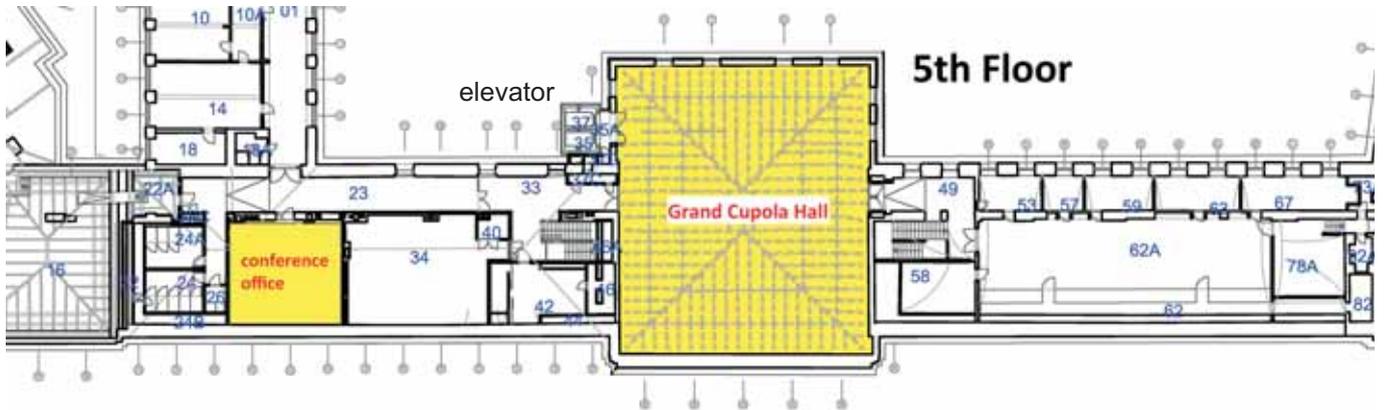
30th July – 3rd August 2012
Grand Cupola Hall
Karlsplatz, Main Building,
Vienna University of Technology
Vienna, Austria

Program
and
Book of Abstracts

www.qcmc2012.org

ATOMINSTITUT VCQ Vienna Center for Quantum Science and Technology OAW CoQuS ComplexQuantumSystems SEVENTH FRAMEWORK PROGRAMME universität wien TU WIEN TECHNISCHE UNIVERSITÄT WIEN Vienna University of Technolo

Conference Venue: TU Vienna Main Building

5th Floor

elevator

Grand Cupola Hall

conference office

4th Floor

elevator

company exhibiton

coffee or beer buffet

Seminarr. 212 / 232

2nd Floor

elevator

reception & registration
Boecklsaal

1st Floor

elevator

streaming

poster sessions

Main Entrance

Dear Colleagues,

"Servus" and welcome to Vienna !

We are pleased and honored to host the 11th International Conference on Quantum Communication, Measurement and Computing (QCMC) and hope that you will have an exciting and inspiring week. The goal of the QCMC is to encourage and bring together scientists and engineers working in the interdisciplinary field of quantum information science and technology. Browsing through this book of abstracts, you will find an impressive body of work in the talks and poster sessions.

Just as important, we encourage you to enjoy the beautiful city of Vienna and grasp the wonderful mixture of arts, culture, science, and savoir-vivre that it offers.

Science in general and a conference in particular is all about communicating and exchanging ideas. In this spirit of scientific exchange, we would like to thank you in advance for your active contribution to making QCMC 2012 a success.

With best wishes from the organizers,

Jörg Schmiedmayer   Arno Rauschenbeutel   Stephan Schneider
Principal Chair   Co-Chair   Organisation

About QCMC 2012

The International Conference on Quantum Communication, Measurement and Computing (QCMC) was established 1990 to encourage and bring together scientists and engineers working in the interdisciplinary field of quantum information science and technology. To date, ten such meetings have been held and the eleventh is taking place summer 2012 in Vienna/Austria.

Topics of the conference:

1   Foundation of Quantum Physics
2   Quantum Measurements and Metrology
3   Quantum Control
4   Quantum Communication and Cryptography
5   Quantum Information and Communication Theory
6   Quantum Information and Communication Implementations

In connection with the conference, proceedings will be published jointly with the American Institute of Physics (AIP), which will appear approximately one year after the conference.

Previous QCMC Conferences

- Quantum Aspects of Optical Communication, Paris, France, 1990
- Quantum Communication and Measurement, Nottingham, United Kingdom, 1994
- Quantum Communication and Measurement, Fuji-Hakone, Japan, 1996
- Quantum Communication, Measurement and Computing, Evanston, IL, USA, 1998
- Quantum Communication, Measurement and Computing, Capri, Italy, 2000
- Quantum Communication, Measurement and Computing, Cambridge, MA, USA 2002
- Quantum Communication, Measurement and Computing, Glasgow, UK, 2004
- Quantum Communication, Measurement and Computing, Tsukuba, Japan, 2006
- Quantum Communication, Measurement and Computing, Calgary, Canada, 2008
- Quantum Communication, Measurement and Computing, Brisbane, Australia, 2010

QCMC Steering Committee

- Founding Chair (Honorary) – Osamu Hirota
- Chair – Prem Kumar
- Past-Chair – Jeffrey Shapiro
- Vice-Chair – Mauro D'Ariano
- Australia – Ping Koy Lam
- Australia – Tim Ralph
- Canada – Christopher Fuchs
- Canada – Alexander Lvovsky
- Europe – Philippe Grangier
- Europe – Jörg Schmiedmayer
- China – Jian-Wei Pan
- Japan – Masahide Sasaki

Programm Commitee

- Rainer Blatt (University of Innsbruck, Austria)
- Tommaso Calarco (University of Ulm, Germany)
- Daniel Esteve (CEA Saclay, France)
- Christopher A. Fuchs (Perimeter Institute, Waterloo, Canada)
- Philippe Grangier (Laboratoire Charles Fabry, Palaiseau, France)
- Mikhail Lukin (Harvard University, USA)
- Hideo Mabuchi (Stanford University, USA)
- Gerard J. Milburn (University of Queensland, Brisbane, Australia)
- Kae Nemoto (NII, Tokyo, Japan)
- Jian-Wei Pan (University of Science and Technology of China, Hefei, China)
- Eugene S. Polzik (Nils Bohr Institute, Kopenhagen, Denmark)
- Trey Porto (NIST / JQI, Gaithersburg, USA)
- Masahide Sasaki (NICT, Koganei, Japan)
- Jeffrey H. Shapiro (MIT, Cambridge, USA)
- Barbara Terhal (RWTH Aachen, Germany)
- Anton Zeilinger (IQOQI, Vienna, Austria)
- Peter Zoller (University of Innsbruck, Austria)

Organizing Committee

- Jörg Schmiedmayer, Principal Chair (Vienna University of Technology, Austria)
- Arno Rauschenbeutel, Co-Chair, (Vienna University of Technology, Austria)
- Prem Kumar (ex-officio), (Northwestern University, Evanston, USA)
- Stephan Schneider, Organisation (Vienna University of Technology, Austria)
- Markus Aspelmeyer (University of Vienna, Austria)
- Rainer Blatt (University of Innsbruck / IQOQI, Austria)
- Thorsten Schumm (Vienna University of Technology, Austria)
- Rupert Ursin (University of Vienna / IQOQI, Austria)
- Frank Verstraete (University of Vienna, Austria)
- Philip Walther (University of Vienna, Austria)

QCMC Award Committee

- Prem Kumar (Steering Committee Chair)
- Giacomo Mauro D'Ariano (Steering Committee Vice-Chair)
- Jeffrey H. Shapiro (past Steering Committee Chair)
- Tim Ralph (past chair QCMC)
- Jörg Schmiedmayer (current chair QCMC)

QCMC Best Poster Award Committee

- Markus Aspelmeyer
- Tobias Nöbauer
- Sven Ramelow

QCMC Book of Abstracts

- Angelika Hable

General Information

PUBLIC TRANSPORT
The City of Vienna is proud of its well-developed and dense network of public transport. Options for tickets: Single ticket: 2 €, Weekly Ticket: 15 €, multi-trip tickets: 8€/4 journeys, 16€/8 journeys; Vienna tickets: 6.70 € /24h, or 11.70 € /48h or 14.50 € /72h (You get them from the red ticket machines at every subway or train station or from tobacco shops.)
Note: There will be no service on line U1 between Schwedenplatz and Reumanplatz

FROM THE AIRPORT TO THE CITY
Standard (24 min): railway 4 € (2 single tickets), leaves airport at xx:18 and xx:48; More expensive (16 min): City Airport Train (CAT): 10 €, leaves airport at xx:05 and xx:35; Even more expensive (approx. 30 min): Taxi ca. 40 €

TAXI SERVICE: Call 0160160 or 0131300 or 0140100 or 0136100

NAME BADGES: All participants are requested to wear their name badges at all times during the conference. Organizing committee members may be identified by the yellow name badges and student helpers by the green name badges.

TELEPHONE NUMBER: Conference office +43-1-58801-141 202

LUNCH TIME BREAK: There are several possibilities for lunch: from the basic and inexpensive student cafeteria (Mensa, 2nd floor, yellow area) to the famous Naschmarkt. You find several restaurants and cafes on the venue map at the back cover of this book.

SPEAKERS POWERPOINT PRESENTATIONS: For all technical issues, students are always available in the Grand Cupola Hall and will be happy to assist the speakers. Laser pointers will be provided.

POSTER SESSIONS: The poster boards will be 2x1m. Posters in size A0 will only fit in portrait format. Material for attaching the posters will be provided.

QCMC CONFERENCE OFFICE:
If you have any needs or special requirements, please ask our conference secretary:

Ms. Evgeniya Ryshkova   Ms. Evgeniya Ryshkova
Vienna University of Technology   Atominstitut
Main Building, 5th floor   Institute of Atomic and Subatomic Physics
Room AA-04-28   Vienna University of Technology
Karlsplatz 13   Stadionallee 2
1040 Vienna   1020 Vienna
Austria   Austria

Visit to Wine Tavern on Friday:
Address: "Heuriger Fuhrgassl-Huber", 1190 Wien, Neustift am Walde 68 (quite some distance away from city centre). Buses will pick us up on Fr. 6:30 pm from the Novomatic Forum and also bring us back at night to the town centre

Visit of Abbey Melk – Conference Dinner - boat trip to Vienna

The social event of the conference will take place on Wednesday afternoon, 1st of August. The participants will leave Vienna by bus and go in about one hour to the world famous Melk Abbey, a baroque Benedictine abbey, overlooking impressively the river Danube in the Wachau valley. After a guided tour of the abbey, we will embark on the recently renovated "MS Admiral Tegetthoff". The ship is booked exclusively for the participants of the conference. While travelling down the Danube, the conference dinner will be available as a buffet.

The time plan for Wednesday, 1st of August afternoon:

14:00   Buses leave intermittently from **Novomatic Forum** (Way from the TU Vienna main building to Novomatic Forum, where the bus leaves: walking 5 min)

15:00   Arrival at Abbey Melk and guided tour of the Abbey (Afterwards buses will bring you to the ship, but you may also take a pleasant walk in 30 min down to the landing stage)

16:00   Start boarding the "MS Admiral Tegetthoff"

17:15   "MS Admiral Tegetthoff" leaves towards Vienna

19:00   Conference Dinner

23:15   Arrival in **Vienna**, close to subway station **"Vorgartenstrasse"** (Subway U1 goes only to **Schwedenplatz**)

Very Important:
PLEASE BE AT 17:15 LATEST AT THE LANDING STAGE.
The ship imperatively needs to leave on time.

Walking time from arrival point in Vienna subway station: 10min

Quantum Communication, Measurement and Computing – Program at a Glance

Time	Sunday 29 July	Monday 30 July	Tuesday 31 July	Wednesday 1 August	Thursday 2 August	Friday 3 August
9:00		Milburn	Zeilinger	Cirac	Gisin	Oberthaler
9:50		Kielpinski	Kwiat	Kraus	Rau	Langen
10:10		Treutlein	Fickler	Gu	Ng	Hasegawa
10:30		coffee break	coffee break	coffee break	coffee break	coffee break
11:00		Bertet	Leibfried	Pan	Sasaki	Gavinsky
11:30		Painter	Roos		Giovannetti	Makarov
12:00		Munro	Rosenfeld	Lloyd	Dorenbos	Lim
12:20		Brukner	Nagaj		Gerrits	Tame
12:45		Lunch	Lunch	Lunch	Lunch	Lunch
14:00	Registration and Reception (TU Main building 2nd floor)	Silberhorn	Rabitz	Excursion: visit of Abbey Melk and boat trip to Vienna	Tittel	Grangier
14:30		White	Montangero		Walmsley	Brune
15:00		Laing	Bowen		Timoney	Ritter
15:30		Wiseman	Deutsch		Nemoto	Donner
15:45		break	break		break	break
16:15		Mitchell	Renner		Furusawa	Wrachtrup
16:45		Vuletič	Yao		Caves	Cappellaro
17:00		Chen	García-Patrón		Ferrie	Bernien
17:30		Volz	Yoshida		Rakher	Bar-Gill
17:50	beer, wine, and pretzels sponsored by	poster session and company exhibition (TU Main building Prechtl hall, 1st floor) beer, wine, and pretzels sponsored by	poster session and company exhibition (TU Main building Prechtl hall, 1st floor) beer, wine, and pretzels		poster session and company exhibition (TU Main building Prechtl hall, 1st floor) beer, wine, and pretzels	closing event: Heurigen (traditional wine tavern) sponsored by CITY of Vienna
19:00						

QCMC 2012
Vienna, Austria

Session and Abstracts

Contents

Monday

8:45   **Opening Remarks**

9:00   **Gerard J. Milburn**
Hybrid quantum systems (MON–1)

9:50   **David Kielpinski**
Quantum interface between an electrical circuit and a single atom (MON–2)

10:10   **Philipp Treutlein**
Hybrid atom-membrane optomechanics (MON–3)

10:30   **Coffee Break**

11:00   **Patrice Bertet**
Hybrid quantum circuit with a superconducting qubit coupled to a spin ensemble (MON–4)

11:30   **Oskar Painter**
Chip-Scale Optomechanics: towards quantum light and sound (MON–5)

12:00   **William Munro**
Coupling a superconducting flux qubit to an NV ensemble: A hybrid system's approach for quantum media conversion (MON–6)

12:20   **Caslav Brukner**
Quantum correlations with indefinite causal order (MON–7)

12:40   **Lunch Break**

14:00   **Christine Silberhorn**
Integrated, time multiplexed photonic networks (MON–8)

14:30   **Andrew White**
Engineering photonic quantum emulators and simulators (MON–9)

15:00   **Anthony Laing**
Observation of quantum interference as a function of Berry's phase in a complex Hadamard optical network (MON–10)

15:20   **Howard Wiseman**
Are dynamical quantum jumps detector-dependent? (MON–11)

15:40   **Coffee Break**

16:10   **Morgan W. Mitchell**
Quantum-enhanced magnetometry with photons and atoms (MON–12)

16:40   **Vladan Vuletić**
Slow photons interacting strongly via Rydberg atoms (MON–13)

17:10   **Zilong Chen**
Superradiant Raman Laser with <1 Intracavity Photon (MON–14)

17:30   **Jürgen Volz**
Observation of strong coupling of single atoms to a whispering-gallery-mode bottle microresonator (MON–15)

18:00   **Poster session 1**
TU Main building Prechtl hall, 1st floor

Tuesday

9:00 **Anton Zeilinger**
Schrödinger's Steering, Mutually Unbiased Bases, and Applications in Photonic Quantum Quantum Information (TUE–1)

9:50 **Paul Kwiat**
Efficiently heralded sources for loophole-free tests of nonlocality and single-photon vision research (TUE–2)

10:10 **Robert Fickler**
Entanglement of Very High Orbital Angular Momentum of Photons (TUE–3)

10:30 **Coffee Break**

11:00 **Dietrich Leibfried**
Towards scalable quantum information processing with trapped ions (TUE–4)

11:30 **Christian Roos**
Schrödinger cat state spectroscopy with trapped ions (TUE–5)

12:00 **Wenjamin Rosenfeld**
Heralded entanglement between widely separated atoms (TUE–6)

12:20 **Daniel Nagaj**
Quantum Speedup by Quantum Annealing (TUE–7)

12:40 **Lunch Break**

14:00 **Herschel A. Rabitz**
Control in the Sciences over Vast Length and Time Scales (TUE–8)

14:30 **Simone Montanegro**
Control of correlated many-body quantum dynamics (TUE–9)

15:00 **Warwick Bowen**
Quantum microrheology (TUE–10)

15:20 **Ivan H. Deutsch**
Fast quantum tomography via continuous measurement and control (TUE–11)

15:40 **Coffee break**

16:10 **Renato Renner**
Reliable Quantum State Tomography (TUE–12)

16:40 **Norm Yao**
Room Temperature Quantum Bit Memory Exceeding One Second (TUE–13)

17:10 **Raúl García-Patrón**
The Holy Grail of Quantum Optical Communication (TUE–14)

17:30 **Beni Yoshida**
Information storage capacity of discrete spin systems (TUE–15)

18:00 **Poster session 2**
TU Main building Prechtl hall, 1st floor

Wednesday

9:00 **Ignacio Cirac**
Quantum memories for few qubits: design and applications (WED–1)

9:50 **Barbara Kraus**
Compressed quantum simulation of the Ising model (WED–2)

10:10 **Mile Gu**
Occam's Quantum Razor: How Quantum Mechanics can reduce the Complexity of Classical Models (WED–3)

10:30 **Coffee Break**

QCMC AWARD SESSION

11:00 **Jian-Wei Pan**
Recent Experiments on Quantum Manipulation with Photons and Atoms (WED–4)

11:45 **Seth Lloyd**
Quantum Heat (WED–5)

12:40 **Lunch Break**

14:00 **Bus is going to Melk Abbey (see map on the back cover)**

Thursday

9:00   **Nicolas Gisin**
Quantum Cryptography and Quantum Repeaters (THU–1)

9:50   **Markus Rau**
Quantum key distribution using electrically driven quantum-dot single photon sources on a free space link (THU–2)

10:10   **Nelly Ng Huei Ying**
First implementation of bit commitment in the Noisy-Storage Model (THU–3)

10:30   **Coffee Break**

11:00   **Masahide Sasaki**
Novel quantum key distribution technologies in the Tokyo QKD Network (THU–4)

11:30   **Vittorio Giovannetti**
Quantifying the noise of a quantum channel by noise addition (THU–5)

12:00   **Sander N. Dorenbos**
Superconducting Nanowire Single Photon Detectors for quantum optics and quantum plasmonics (THU–6)

12:20   **Thomas Gerrits**
On-chip, photon-number-resolving, telecom-band detectors for scalable photonic information processing (THU–7)

12:40   **Lunch Break**

14:00   **Wolfgang Tittel**
Quantum repeaters using frequency-multiplexed quantum memories (THU–8)

14:30   **Ian Walmsley**
Entangbling - Quantum correlations in room-temperature diamond (THU–9)

15:00   **Nuala Timoney**
A long lived AFC quantum memory in a rare earth doped crystal (THU–10)

15:20   **Kae Nemoto**
Quantum Information Network based on NV Diamond Centers (THU–11)

15:40   **Coffee Break**

16:10   **Akira Furusawa**
Hybrid quantum information processing (THU–12)

16:40   **Carlton M. Caves**
Back to the future: QND, BAE, QNC, QMFS, and linear amplifier (THU–13)

17:10   **Christopher Ferrie**
Minimax quantum tomography: the ultimate bounds on accuracy (THU–14)

17:30   **Matthew T. Rakher**
Simultaneous Wavelength Translation and Amplitude Modulation of Single Photons from a Quantum Dot (THU–15)

18:00   **Poster session 3**
TU Main building Prechtl hall, 1st floor

Friday

9:00 **Markus Oberthaler**
Quantum Atom Optics - single and two mode squeezing with Bose Einstein condensates
(FRI–1)

9:50 **Tim Langen**
Relaxation and Pre-thermalization in an Isolated Quantum System (FRI–2)

10:10 **Yuji Hasegawa**
Error-disturbance uncertainty relation studied in successive spin-measurements (FRI–3)

10:30 **Coffee Break**

11:00 **Dmitry Gavinsky**
Quantum Money with Classical Verification (FRI–4)

11:30 **Vadim Makarov**
Laser damage of photodiodes helps the eavesdropper (FRI–5)

12:00 **Charles Ci Wen Lim**
Self-testing quantum cryptography (FRI–6)

12:20 **Mark S. Tame**
Experimental Characterization of the Quantum Statistics of Surface Plasmons in Metallic Stripe Waveguides (FRI–7)

12:40 **Lunch Break**

14:00 **Philippe Grangier**
Manipulating single atoms and single photons using cold Rydberg atoms (FRI–8)

14:30 **Michel Brune**
Stabilization of Fock states in a high Q cavity by quantum feedback (FRI–9)

15:00 **Stephan Ritter**
An Elementary Quantum Network of Single Atoms in Optical Cavities (FRI–10)

15:20 **Tobias Donner**
Exploring cavity-mediated long-range interactions in a quantum gas (FRI–11)

15:40 **Coffee Break**

16:10 **Jörg Wrachtrup**
Entangling distant electron spins (FRI–12)

16:40 **Paola Cappellaro**
Quantum information Transport in Mixed-State Networks (FRI–13)

17:00 **Hannes Bernien**
Quantum Networks with Spins in Diamond (FRI–14)

17:20 **Nir Bar-Gill**
Suppression of spin bath dynamics for improved coherence in solid-state systems (FRI–15)

18:30 **Bus is going to the Heurigen (wine travern)**

Poster session 1–Monday

Foundation of Quantum Physics

P1–0   Pawel Kurzynski, **Ravishankar Ramanathan** and Dagomir Kaszlikowski
Entropic Test of Quantum Contextuality and Monogamy

P1–1   **Jean-Daniel Bancal**, Stefano Pironio, Antonio Acín, Yeong-Cherng Liang, Valerio Scarani and Nicolas Gisin
Quantum nonlocality basedon finite-speedcausal influencesleads tosuperluminal signalling

P1–2   **Adam Bednorz**, Kurt Franke and Wolfgang Belzig
Time reversal symmetry violation in quantum weak measurements

P1–3   Adán Cabello **Costantino Budroni**, Otfried Gühne, Matthias Kleinmann and Jan-Åke Larsson
Tight inequality for qutrit state-independent contextuality

P1–4   Ognyan Oreshkov, **Fabio Costa** and Časlav Brukner
Quantum correlations with no causal order

P1–5   Devin H. Smith, Geoff Gillett, **Marcelo P. de Almeida**, Cyril Branciard, Alessandro Fedrizzi, Till J. Weinhold, Adriana Lita, Brice Calkins, Thomas Gerrits, Howard M. Wiseman, Sae Woo Nam, Andrew G. White
Conclusive quantum steering with superconducting transition edge sensors

P1–6   **Chirag Dhara**, Giuseppe Prettico and Antonio Acín
Symmetry arguments to certify and quantify randomness

P1–7   Yuji Hasegawa and **Daniel Erdösi**
Violation of a Bell-like inequality

P1–8   **David Evans** and Howard M. Wiseman
Optimal Strategies for Tests of EPR-Steering with No Detection Loophole

P1–9   **Masanori Hiroishi**, Holger F. Hofmann
Weak measurement statistics of correlations between input and output in quantum teleportation

P1–10   **Holger F. Hofmann**
Optimal cloning as a universal quantum measurement: resolution, back-action, and joint probabilities

P1–11   **Holger F. Hofmann**
What the complex joint probabilities observed in weak measurements can tell us about quantum physics

P1–12   **Issam Ibnouhsein** and Alexei Grinbaum
Twin Cheshire Photons

P1–13   **Jan Jeske** and Jared H. Cole
Decoherence due to spatially correlated fluctuations in the environment

Quantum measurements and metrology

P1–14 **Thomas Antoni**, Kevin Makles, Rémy Braive, Aurélien Kuhn, Tristan Briant, Pierre-François Cohadon, Alexios Beveratos, Izo Abram, Luc Le Gratiet, Isabelle Sagnes, Isabelle Robert-Philip, Antoine Heidmann
Cavity optomechanics with a nonlinear photonic crystal nanomembrane

P1–15 Stefan L. Christensen, **Jürgen Appel**, Jean-Baptiste Béguin, Heidi L. Sørensen, and Eugene S. Polzik
Towards realization and detection of a non-Gaussian quantum state of an atomic ensemble

P1–16 **Thomas B. Bahder**
Quantum and Classical Measurements: Information as a Metric of Quality

P1–17 **Hugo Benichi** and Akira Furusawa
Optical homodyne tomography with polynomial series expansion

P1–18 **Robin Blume-Kohout**
Robust error bars for quantum tomography

P1–19 **Agata M. Brańczyk**, Dylan H. Mahler, Lee A. Rozema, Ardavan Darabi, Aephraim M. Steinberg and Daniel F. V. James
Self-calibrating Quantum State Tomography

P1–20 **Gabriel A. Durkin**, Vadim N. Smelyanskiy and Sergey I. Knysh
Quantum Shape Sensor

P1–21 **T. Gerrits**, F. Marsili, V. B . Verma, A. E. Lita, Antia Lamas Linares, J. A. Stern, M. Shaw, W. Farr, R. P. Mirin, and S. W. Nam
Joint Spectral Measurements at the Hong-Ou-Mandel Interference Dip

P1–22 **Shuro Izumi**, Masahiro Takeoka, Mikio Fujiwara, Nicola Dalla Pozza, Antonio Assalini, Kazuhiro Ema and Masahide Sasaki
Quantum displacement receiver with feedforward operation for MPSK signals

P1–23 **Marcin Jarzyna** and Rafał Demkowicz-Dobrzański
Quantum interferometry with and without an external phase reference

P1–24 **B. Bell**, S. Kannan, A. McMillan, A. Clark, W. Wadsworth and J. Rarity
Quantum metrology with fibre sources

P1–25 Minaru Kawamura, **Tatsuya Mizukawa**, Ryouhei Kunitomi and Kosuke Araki
Observation of single spin by transferring the coherence to a high energy macroscopic pure state

P1–26 Tobias Moroder, **Matthias Kleinmann**, Philipp Schindler, Thomas Monz, Otfried Gühne and Rainer Blatt
Detection of systematic errors in quantum tomography

Quantum control

P1–27 **Sarah Adlong**, Stuart Szigeti, Michael Hush and Joe Hope
Quantum control of a Bose-Einstein condensate in a harmonic trap

P1–28 **Philipp Ambichl**, Florian Libisch, and Stefan Rotter
Generating Particlelike Scattering States in Wave Transport

P1–29   **Zilong Chen**, Justin G. Bohnet, Joshua M. Weiner and James K. Thompson
General Formalism for Evaluating the Impact of Phase Noise on Bloch Vector Rotations

P1–30   Li Li,   **Andy Chia** and Howard M. Wiseman
The Pointer Basis and Feedback Stabilization of Quantum Systems

Quantum Communication and Cryptography

P1–31   **Fabian Furrer**, Torsten Franz, Mario Berta, Volkher B. Scholz, Marco Tomamichel and Reinhard F. Werner
Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks

P1–32   **Rémi Blandino**, Anthony Leverrier, Marco Barbieri, Philippe Grangier and Rosa Tualle-Brouri
Heralded noiseless linear amplifier in continuous variables QKD

P1–33   **Brendon Higgins**, Jean-Philippe Bourgoin, Nikolay Gigov, Evan Meyer-Scott, Zhizhong Yan and Thomas Jennewein
Performance Analysis of the Proposed QEYSSAT Quantum Receiver Satellite

P1–34   **N. Bruno**, T. Guerreiro, P. Sekatski, A. Martin, C.I. Osorio, E. Pomarico, B. Sanguinetti, N. Sangouard, H. Zbinden and R.T. Thew
Characterization of pure narrow band photon sources for quantum communication

P2–35   Helen M. Chrzanowski, Mile Gu, Syed M. Assad, Thomas Symul, Kavan Modi, Timothy C. Ralph, Vlatko Vedral and **Ping Koy Lam**
Discord as a Quantum Resource for Bi-Partite Communication

P1–36   **Vedran Dunjko**, Elham Kashefi, Anthony Leverrier
Blind Quantum Computing with Weak Coherent Pulses

P1–37   **Mikio Fujiwara**, Tomoyasu Domeki, Ryo Nojima, and Masahide Sasaki
Secure network switch with Quantum key distribution system

P1–38   **Fumio Futami** and Osamu Hirota
Field transmission test of 2.5 Gb/s Y-00 cipher in 160-km (40 km × 4 spans) installed optical fiber for secure optical fiber communications

P1–39   **Thiago Guerreiro**, Enrico Pomarico, Bruno Sanguinetti, Nicolas Sangouard, Robert Thew, Hugo Zbinden, Nicolas Gisin, J. S. Pelc, C. Langrock and M. M. Fejer
Faithful Entanglement Swapping Based on Sum Frequency Generation

P1–40   **V. Händchen**, T. Eberle, J. Duhme, T. Franz, R.Werner and R. Schnabel
Quantum Key Distribution on Hannover Campus - Establishing Security against Coherent Attacks

P1–41   **B. Heim**, C. Peuntinger, C. Wittmann, C. Marquardt and G. Leuchs
Atmospheric Quantum Communication using Continuous Polarization Variables

P1–42   **Thomas Herbst**, Rupert Ursin and Anton Zeilinger
A high quality quantum link for space experiments

P1–43   Evan Meyer-Scott, Zhizhong Yan, Allison MacDonald, Jean-Philippe Bourgoin, Chris Erven, Alessandro Fedrizzi, Gregor Weihs, **Hannes Hübel** and Thomas Jennewein
Revival of short-wavelengths for quantum communication applications

Quantum Information and Communication theory

P1–44 **Seiseki Akibue** and Mio Murao
Implementability of two-qubit unitary operations over the butterfly network with free classical communication

P1–45 **Juan Miguel Arrazola**, Oleg Gittsovich and Norbert Lütkenhaus
Accessible nonlinear entanglement witnesses

P1–46 **Jeongho Bang**, Seung-Woo Lee, Hyunseok Jeong and Jinhyoung Lee
A characterization scheme of universal operation: the universal-NOT gate

P1-47 **Cai Yu**, Jean-Daniel Bancal and Valerio Scarani
CGLMP4 Inequality as a Dimension Witness

P1–48 **S. Campbell**, T. J. G. Apollaro, C. Di Franco, L. Banchi, A. Cuccoli, R. Vaia, F. Plastina and M. Paternostro
Propagation of non-classical correlations across a quantum spin chain

P1–49 **Tatjana Carle**, Julio De Vicente, Wolfgang Dür, Barbara Kraus
Purification to Locally Maximally Entangleable States

P1–50 M.F. Santos, M. Terra Cunha, R. Chaves and **A.R.R. Carvalho**
Quantum computing with incoherent resources and quantum jumps

P1–51 **Michele Dall'Arno**, Giacomo Mauro D'Ariano and Massimiliano F. Sacchi
Informational power of quantum measurements

P1–52 **Julio I. de Vicente**, Tatjana Carle, Clemens Streitberger and Barbara Kraus
Complete set of operational measures for the characterization of three–qubit entanglement

P1–53 **Simon. J. Devitt**, Alexandru. Paler, Ilia. Polian, and Kae Nemoto
Universality in Topological quantum computing without the Dual space

P1–54 Alexandru Paler, Simon J. Devitt, Kae Nemoto and Ilia Polian
Classical compilers for gate optimisation in fault-tolerant quantum computing

P1–55 **Kieuske Fujii**, Takashi Yamamoto, Masato Koashi and Nobuyuki Imoto
Fault-tolerant quantum computation and communication on a distributed 2D array of small local systems

P1–56 **Omar Gamel** and Daniel F. V. James
Explorations in the efficiency of quantum factoring

P1–57 **Miroslav Gavenda**, Lucie Čelechovská, Jan Soubusta, Miloslav Dušek and Radim Filip
Visibility bound caused by a distinguishable noise particle

P1–58 **Oleg Gittsovich** and Tobias Moroder
Calibration-robust entanglement detection beyond Bell inequalities

P1–59 **Saikat Guha**, Ranjith Nair, Brent J. Yen, Zachary Dutton and Jeffrey H. Shapiro
Quantum limit to capacity and structured receivers for optical reading

P1–60 **Otfried Gühne**, Sönke Niekamp and Tobias Galla
Characterizing multiparticle quantum correlations via exponential families

Quantum Information and Communication Implementations
Atoms/Ions

P1–61 **So-Young Baek**, Emily Mount, Rachel Noek, Stephen Crain, Daniel Gaultney, Andre van Rynbach, Peter Maunz and Jungsang Kim
Long-lived ion qubits in a microfabricated trap for scalable quantum computation

P1–62 **Erwan Bimbard** Jovica Stanojevic, Valentina Parigi, Rosa Tualle-Brouri, Alexei Ourjoumtsev and Philippe Grangier
Deterministic generation of non-classical states of light via Rydberg interactions

P1–63 **Tim Byrnes**
Two component Bose-Einstein condensates and their applications towards quantum information processing

P1–64 **Geoff Campbell**, Mahdi Hosseini, Ben Sparkes, Olivier Pinel, Tim Ralph, Ben Buchler and Ping Koy Lam
Gradient echo memory as a platform for manipulating quantum information

P1–65 **Cassettari D.**, Bruce G., Harte T., Richards D., Bromely S., Torralbo-Campo L. and Smirne G.
Novel Optical Traps For Ultracold Atoms

P1–66 **A. Goban**, K. S. Choi, D. J. Alton, D. Ding, C. Lacroûte, M. Pototschnig, J. A. M. Silva, C. L. Hung, T. Thiele, N. P. Stern and H. J. Kimble
Demonstration of a state-insensitive, compensated nanofiber trap

Quantum Information and Communication Implementations
Solid State: Superconductors, Quantum Dots, Nano mechanics etc...

P1–67 **Sabine Andergassen**, Dirk Schuricht, Mikhail Pletyukhov and H. Schoeller
Dynamical transport in correlated quantum dots: a renormalization-group analysis

P1–68 **Wolfgang Belzig**, Christoph Bruder, Abraham Nitzan and Adam Bednorz
Concepts and applications of weak quantum measurements

P1–69 **Timothy C. DuBois**, Manolo C. Per, Salvy P. Russo and Jared H. Cole
Delocalised Oxygen models of two-level system defects in superconducting phase qubits

P1–70 Márcio M. Santos, Fabiano O. Prado, Halyne S. Borges, Augusto M. Alcalde, José M. Villas-Bôas and **Eduardo I. Duzzioni**
Using quantum state protection via dissipation in a quantum-dot molecule to solve the Deutsch problem

Quantum Information and Communication Implementations
Defects and Ions in Crystals, Spins

P1–71 **Kathrin Buczak**, Achim Bittner, Christian Koller, Tobias Nöbauer, Johannes Schalko, Ulrich Schmied, Michael Schneider, Jörg Schmiedmayer and **Michael Trupke**
Diamond emitters in microcavities

Quantum Information and Communication Implementations
Photons and Linear Optics QIP

P1–72 **Stefanie Barz**, Elham Kashefi, Anne Broadbent, Joseph F. Fitzsimons, Anton Zeilinger and Philip Walther
Experimental Demonstration of Blind Quantum Computing

P1–73 **Federica A. Beduini**, Yannick A. de Icaza Astiz, Vito G. Lucivero, Joanna A. Zielińska and Morgan W. Mitchell
Multipartite photonic entanglement from polarization squeezing at 795 nm.

P1–74 **Hugo Benichi**, Shuntaro Takeda, Ladislav Mišta Jr., Radim Filip and Akira Furusawa
Conditional quantum teleportation of non-Gaussian non-classical states of light

P1–75 **Stefan Berg-Johansen**, Ioannes Rigas, Christian Gabriel, Andrea Aiello, Peter van Loock, Ulrik L. Andersen, Christoph Marquardt and Gerd Leuchs
Cluster state generation with cylindrically polarized modes

P1–76 **Bänz Bessire**, Christof Bernhard, André Stefanov and Thomas Feurer
Biphoton Interference and Phase Reconstruction of Time-Energy Entangled Photons through Spectral Amplitude and Phase Modulation

P1–77 **Jonatan Bohr Brask** and Rafael Chaves
Robust nonlocality tests with displacement-based measurements

P1–78 T. Kitagawa, **M. A. Broome**, A. Fedrizzi, M. S. Rudner1, E. Berg, I. Kassal, A. Aspuru-Guzik, E. Demler and A. G. White
Observation of topologically protected bound states in photonic quantum walks

P1–79 **Christopher Chudzicki**, Isaac Chuang and Jeffrey H. Shapiro
Deterministic and Cascadable Conditional Phase Gate for Photonic Qubits

P1–80 **Michele Dall'Arno**, Alessandro Bisio and Giacomo Mauro D'Ariano
Ideal quantum reading of optical memories

P1–81 Patrick J. Clarke, Robert J. Collins, **Vedran Dunjko**, Erika Andersson, John Jeffers and Gerald S. Buller
Experimental Demonstration of Quantum Digital Signatures

P1–82 E. Megidish, A. Halevy, T. Shacham, T. Dvir, L. Dovrat and **H. S. Eisenberg**
Quantum tomography of inductively created multi-photon states

P1–83 Devon N. Biggerstaff, Thomas Meaney, Ivan Kassal, **Alessandro Fedrizzi**, Martin Ams, Graham D. Marshall, Michael J.Withford and Andrew G. White
Experimental emulation of coherent quantum effects in biology

P1–84 **Franck Ferreyrol**, Nicolò Spagnolo, Rémi Blandino, Marco Barbieri, Rosa Tualle-Brouri and Philippe Grangier
Heralded processes on continuous-variable spaces as quantum maps

P1–85 **Jian Chen**, Jonathan L. Habif, Zachary Dutton and Saikat Guha
Photon-detection-induced Kennedy receiver for binary-phase coded PPM

P1–86 Bharath Srivathsan, **Gurpreet Kaur Gulati**, Chng Mei Yuen Brenda, Gleb Maslennikov, Dzmitry Matsukevich, Christian Kurtsiefer
Narrowband Source of Correlated Photon Pairs via Four-Wave Mixing in Atomic Vapour

Quantum Information and Communication Implementations
Hybrid quantum systems

P1–87 **S. Filipp**, T. Thiele, S. D. Hogan, J. A. Agner, F. Merkt and A. Wallraff
Interfacing Microwave Photons with Rydberg Atoms on a Superconducting Chip

P1–88 Katherine Louise Brown, Suvabrata De, **Viv Kendon** and Bill Munro
Qubus ancilla-driven quantum computation

P1–89 **Hideo Kosaka**, Takahiro Inagaki, Ryuta Hitomi, Fumishige Izawa, Yoshiaki Rikitake, Hiroshi Imamura, Yasuyoshi Mitsumori and Keiichi Edamatsu
Time-bin photonic state transfer to electron spin state in solids

P1–90 **Guillaume Lepert**, Michael Trupke, Ed Hinds, Jaesuk Hwang, Michael Hartmann and Martin Plenio
Atoms and molecules in arrays of coupled cavities

Quantum Information and Communication Implementations
Components: Detectors, Quantum memory etc...

P1–91 **H. M. Chrzanowski**, J. Bernu, B. Sparkes, B. Hage, A. Lund, T. C. Ralph, P. K. Lam and T. Symul
Photon number discrimination using only Gaussian resources and measurements

P1–92 **Eden Figueroa**, Tobias Latka, Andreas Nezner, Christian Nölleke, Andreas Reiserer, Stephan Ritter and Gerhard Rempe
Arbitrary shaping of light pulses at the single-photon level

P1–93 **Michael Förtsch**, Josef Fürst, Christoffer Wittmann, Dmitry Strekalov, Andrea Aiello, Maria V. Chekhova, Christine Silberhorn, Gerd Leuchs and Christoph Marquardt
A Versatile Single Photon Source for Quantum Information Processing

P1–94 **Antia Lamas-Linares**, Nathan Tomlin, Brice Calkins, Adriana E. Lita, Thomas Gerrits, Joern Beyer, Richard Mirin and Sae Woo Nam
Transition edge sensors with low jitter and fast recovery times

P1–95 **Lambert Giner**, Lucile Veissier, Ben Sparkes, Alexandra Sheremet, Adrien Nicolas, Oxana Mishina, Michael Scherman, Sidney Burks, Itay Shomroni, Ping Koy Lam, Elisabeth Giacobino and Julien Laurat
Discerning EIT from ATS: an experiment with cold Cs atoms

P1–96 **Ryan T. Glasser**, Ulrich Vogl and Paul D. Lett
Fast light images and the arrival time of spatial information in optical pulses with negative group velocity

P1–97 Ana Predojević, **Stephanie Grabher** and Gregor Weihs
Phase property measurements with an ultrafast pulsed Sagnac source of polarization -entangled photon pairs

P1–98 Christian Gabriel, Christoffer Wittmann, Bastian Hacker, Wolfgang Mauerer, Elanor Huntington, Metin Sabuncu, Christoph Marquardt and Gerd Leuchs
A High-Speed Quantum Random Number Generator Based on the Vacuum State

Poster session 2–Tuesday

Foundation of Quantum Physics

P2–0 Jiří Tomkovič, Michael Schreiber, Joachim Welte, Martin Kiffner, Jörg Schmiedmayer and **Markus K. Oberthaler**
Single spontaneous photon as a coherent beamsplitter for an atomic matter-wave

P2–1 **Minsu Kang**, M. S. Kim and Hyunseok Jeong
Generation of entanglement with highly-mixed systems

P2–2 **Michael Keller**, **Max Ebner**, **Mateusz Kotyrba**, Mandip Singh, Johannes Kofler and Anton Zeilinger
Creating and Detecting Momentum Entangled States of Metastable Helium Atoms

P2–3 **Johannes Kofler** and Ćaslav Brukner
Violation of macroscopic realism without Leggett-Garg inequalities

P2–4 **Radek Lapkiewicz**, Peizhe Li, Christoph Schaeff, Nathan K. Langford, Sven Ramelow, Marcin Wiesniak and Anton Zeilinger
Experimental non-classicality of an indivisible quantum system

P2–5 **Fatima Masot-Conde**,
Time reversibility in the quantum frame

P2–6 **E. Megidish**, A. Halevy, T. Shacham, T. Dvir, L. Dovrat and H. S. Eisenberg
Entanglement between photons that never co-existed

P2–7 S.M. Giampaolo, G. Gualdi, **Alex Monras** and F. Illuminati
Characterizing and Quantifying Frustration in Quantum Many-Body systems

P2–8 **Yoshifumi Nakata**, Peter S. Turner and Mio Murao
Entanglement of phase-random states

P2–9 **T.G. Philbin**
Quantum dynamics of damped oscillators

P2–10 L. I. Plimak and S.T. Stenholm
Quantum optics meets real-time quantum field theory: generalised Keldysh rotations, propagation, response and tutti quanti

P2–11 **Robert Prevedel**, Deny R Hamel, Roger Colbeck, Kent Fisher and Kevin J Resch
Experimental investigation of the uncertainty principle in the presence of quantum memory

P2–12 Pawel Kurzynski, **Ravishankar Ramanathan**, Akihito Soeda, Tan Kok Chuan, Marcelo F. Santos, and Dagomir Kaszlikowski
Entanglement and Quality of Composite Bosons

Quantum measurements and metrology

P2–13 Rafal Demkowicz-Dobrzanski, **Jan Kolodynski** and Madalin Guta
The elusive Heisenberg limit in quantum enhanced metrology

P2–14 **Aurélien G. Kuhn**, Emmanuel Van Brackel, Leonhard Neuhaus, Jean Teissier, Claude Chartier, Olivier Ducloux, Olivier Le Traon, Christophe Michel, Laurent Pinard, Raffaele Flaminio, Samuel Deleglise, Tristan Briant, Pierre-François Cohadon and Antoine Heidmann
A micropillar for cavity optomechanics

P2–15 **Nathan K. Langford**
Calculating errors in quantum tomography: diagnosing systematic vs statistical errors

P2–16 Vittorio Giovannetti, Seth Lloyd, **Lorenzo Maccone**,
Quantum measurement bounds beyond the uncertainty relations

P2–17 **Alberto M. Marino**, Neil Corzo, Kevin M. Jones, and Paul D. Lett
Noiseless Image Amplification

P2–18 Felippe A. S. Barbosa, Antônio S. Coelho, Alessandro Villar, Katiúscia N.Casemiro, Paulo Nussenzveig, Claude Fabre and **Marcelo Martinelli**
A complete characterization of the OPO, leading to hexapartite entanglement

P2–19 **O.V. Minaeva**, A.M. Fraine, R. Egorov, D. S. Simon and and A. V. Sergienko
High Resolution Measurement of Polarization Mode Dispersion (PMD) in Telecom Switch using Quantum Interferometry

P2–20 **C. R. Müller**, M. A. Usuga, C.Wittmann, M. Takeoka, Ch. Marquardt, U. L. Andersen and G. Leuchs
Four-State Discrimination via a Hybrid Receiver

P2–21 **Ranjith Nair**
Fundamental limits on the accuracy of optical phase estimation from rate-distortion theory

P2–22 **Kenji Nakahira** and Tsuyoshi Sasaki Usuda
A generalized Dolinar receiver with inconclusive results

P2–23 **Daniel K. L. Oi**, Václav Potoćek and John Jeffers
Measuring Nothing

P2–24 **Jan Peřina Jr.**, Ondřej Haderka, Václav Michálek and Martin Hamar
Photon-numberstatisticsoftwinbeams: self-consistentmeasurement, reconstruction, and properties

P2–25 **Changliang Ren** and Holger F. Hofmann
How to make optimal use of maximal multipartite entanglement in clock synchronization

P2–26 **Dylan J. Saunders**, Pete J. Shadbolt, Jeremy L. O'Brien and Geoff J. Pryde
Local non-realistic states observed via weak tomography - resolving the two-slit paradox

P2–27 **Tarik Berrada**, Sandrine van Frank, Robert Bücker, Thorsten Schumm, **Jean-François Schaff** and Jörg Schmiedmayer
Matter wave Mach-Zehnder interferometry on an atom chip

Quantum control

P2–28 **Alessandro Farace** and Vittorio Giovannetti
Enhancing Quantum Effects via Periodic Modulations in Optomechanical Systems

P2–29 Bin Hwang and **Hsi-Sheng Goan**
Optimal control of a qubit in a non-Markovian environment

P2–30 **Qudsia Quraishi**, Vladimir Malinovsky and Patricia Lee
Modeling spin entanglement with an optical frequency comb of atoms confined on atom -chip traps

Quantum Communication and Cryptography

P2–31 **Nitin Jain**, Elena Anisimova, Christoffer Wittmann, ChristophMarquardt, Vadim Makarov and Gerd Leuchs
Investigating the feasibility of a practical Trojan-horse attack on a commercial quantum key distribution system

P2–32 **J. Janousek**, S. Armstrong, B. Hage, J-F. Morizur, P. K. Lam and H-A. Bachor
Programmable Multi-mode Quantum Networks

P2–33 **Florian Kaiser**, Lutfi Arif Ngah, Amandine Issautier, Olivier Alibart, Anthony Martin and Sébastien Tanzilli
Ultra narrowband telecom polarisation entanglement source for future long distance quantum networking

P2–34 **Imran Khan**, Christoffer Wittmann, Nitin Jain, Nathan Killoran, Norbert Lütkenhaus, Christoph Marquardt and Gerd Leuchs
Long distance continuous-variable quantum communication

P2–35 **Mario Krenn**, Robert Fickler, William Plick, Radek Lapkiewicz, Sven Ramelow and Anton Zeilinger
Entanglement of Ince-Gauss Modes of Photons

P2–36 **Mikolaj Lasota**, Rafal Demkowicz-Dobrzanski and Konrad Banaszek
Security of practical quantum cryptography with heralded single photon sources

P2–37 Peter Shadbolt, Tamás Vértesi, **Yeong-Cherng Liang**, Cyril Branciard, Nicolas Brunner and Jeremy L. O'Brien
Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices

P2–38 **Nicoló Lo Piparo** and Mohsen Razavi
Long-distance quantum key distribution with imperfect devices

P2–39 **Vladyslav C. Usenko**, Lars S. Madsen, Mikael Lassen, Radim Filip and Ulrik L. Andersen
Continuous variable quantum key distribution with optimally modulated entangled states

P2–40 **Oliver Maurhart**, Christoph Pacher, Andreas Happe, Thomas Lorünser, Gottfried Lechner, Cristina Tamas, Andreas Poppe and Momtchil Peev
Quantum Key Distribution Software maintained by AIT

P2–41 **Michal Mičuda**, Ivo Straka, Martina Miková, Miloslav Dušek, Nicolas J. Cerf, Jaromír Fiurášek and Miroslav Ježek
Noiseless loss suppression in quantum optical communication

P2–42 **William Plick**, Mario Krenn, Sven Ramelow, Robert Fickler, and Anton Zeilinger
Do the Ince-Gauss Modes of Light Give Keys New Places to Hide?

Quantum Information and Communication theory

P2–43 L. Gyongyosi and S. Imre
Polaractivation of Quantum Channels

P2–44 **L. Gyongyosi** and S. Imre
Quasi-Superactivation of Zero-Capacity Quantum Channels

Quantum Information and Communication Implementations
Atoms/Ions

P2–60　Philipp Schindler, Julio T. Barreiro, Daniel Nigg, Matthias Brandl, Michael Chwalla, Thomas Monz, **Markus Hennrich** and Rainer Blatt
Experimental quantum measurement reversal using quantum error correction

P2–61　**I. Herrera**, P. Lombardi, J. Petrovic, F. Schaefer and F. S. Cataliotti
Light pulse analysis with a multi-state atom interferometer

P2–62　**K. Inaba**, Y. Tokunaga, K. Tamaki, K. Igeta and M. Yamashita
Control of Wannier orbitals for generating tunable Ising interactions of ultracold atoms in an optical lattice

P2–63　Syed Abdullah Aljunid, Dao Hoang Lan, Yimin Wang, **Gleb Maslennikov**, Valerio Scarani and Christian Kurtsiefer
Excitation of a single atom with a temporally shaped light pulses

P2–64　**Nicolas C. Menicucci**, S. Jay Olson and Gerard J. Milburn
Simulating quantum effects of cosmological expansion using a static ion trap

P2–65　**Sylvi Händel**, Andreas Jechow, Benjamin G. Norton, Erik W. Streed and David Kielpinski
Single atom lensing

Quantum Information and Communication Implementations
Solid State: Superconductors, Quantum Dots, Nano mechanics etc...

P2–66　L.-H. Sun, G.-X. Li and **Z. Ficek**
Coherence and entanglement in a nano-mechanical cavity

P2–67　**Andrew L. C. Hayward**, Andrew M. Martin and Andrew D. Greentree
Fractional Quantum Hall Physics in Jaynes-Cummings-Hubbard Lattices

P2–68　Harishankar Jayakumar, **Tobias Huber**, Thomas Kauten, Ana Predojević, Glenn Solomon and Gregor Weihs
Effect of excitation jitter on the indistinguishability of photons emitted from an InAs quantum dot

P2–69　**Harishankar Jayakumar**, Ana Predojević, Tobias Huber, Thomas Kauten, Glenn S. Solomon and Gregor Weihs
Coherent creation of a single photon cascade in a quantum dot to gernerate time-bin entangled photon pairs

Quantum Information and Communication Implementations
Defects and Ions in Crystals, Spins

P2–70　Daniel L. Creedon, Karim Benmessai, Warwick P. Bowen and **Michael E. Tobar**
Paramagnetic Kerr-type $\chi(3)$ Nonlinearity in a Highly Pure Ultra-Low Loss Cryogenic Sapphire Microwave Whispering Gallery Mode Resonator

Quantum Information and Communication Implementations
Photons and Linear Optics QIP

P2–71 L. K. Shalm, **D. R. Hamel**, Z. Yan, C. Simon, K. J. Resch and T. Jennewein
Showing the genuine tripartite energy-time entanglement of photon triplets produced by cascaded down-conversion

P2–72 Seung-Woo Lee and **Hyunseok Jeong**
Deterministic linear-optics quantum computing based on a hybrid approach

P2–73 **Fumihiro Kaneda**, Ryosuke Shimizu, Satoshi Ishizaka, Yasuyoshi Mitsumori, Hideo Kosaka and Keiichi Edamatsu
Activation of Bound Entanglement in a Four-Qubit Smolin State

P2–74 **Sacha Kocsis**, Guoyong Xiang, Tim C. Ralph and Geoff J. Pryde
Heralded noiseless amplification of a polarization-encoded qubit

P2–75 Monika Patel, Joseph B. Altepeter, **Yu-Ping Huang**, Neal N. Oza, and Prem Kumar
Quantum Interference of Independently Generated Telecom-band Single Photons

P2–76 **Sang Min Lee**, Sang-Kyung Choi and Hee Su Park
Direct fidelity estimation by post-selected C-SWAPs for three photons

P2–77 **Enrique Martin-Lopez**, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou and Jeremy O'Brien
Experimental realisation of Shor's quantum factoring algorithm using qubit recycling

P2–78 **Genta Masada**, Kazunori Miyata, Alberto Politi, Jeremy L. O'Brien and Akira Furusawa
Generation and characterization of EPR beams by using waveguide-interferometers integrated in a chip

P2–79 **Darran Milne**, Natalia Korolkova and Peter van Loock
Quantum computation with non-Abelian continuous-variable anyons

P2–80 **Olivier Morin**, Claude Fabre and Julien Laurat
A source of high-purity heralded single-photons and a novel witness for single-photon entanglement

P2–81 **Jonas S. Neergaard-Nielsen**, Yujiro Eto, Chang-Woo Lee, Hyunseok Jeong and Masahide Sasaki
Quantum tele-amplification with a continuous variable superposition state

P2–82 **Hee Su Park**, Kevin T. McCusker and Paul G. Kwiat
A pseudo-deterministic single-photon source based on temporally multiplexed spontaneous parametric down-conversion

P2–83 **K. Poulios**, D. Fry, J. D. A. Meinecke, M. Lobino, J. C. F. Matthews, A. Peruzzo, X. Zhou, A. Politi, N. Matsuda, N. Ismail, K. Wörhoff, R. Keil, A. Szameit, M. G. Thompson and J. L. O'Brien
Multi-particle Quantum Walks on Integrated Waveguide Arrays

P2–84   A. J. Bennet, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman and **G. J. Pryde**,
Loss-tolerant EPR-steering over 1 km of optical fibre

P2–85   **Sven Ramelow**, Nathan K. Langford, Robert Prevedel, William J. Munro, Gerard J. Milburn and Anton Zeilinger
Towards implementing coherent photon conversion (CPC) for scalable optical quantum information processing

Quantum Information and Communication Implementations
Hybrid quantum systems

P2–86   **S. Minniberger**, F. R. Diorico, S. Schneider and J. Schmiedmayer
Towards a Hybrid Quantum System: Ultracolold atoms meet a superconducting surface

P2–87   **Rudolf Mitsch**, Daniel Reitz, Philipp Schneeweiss and Arno Rauschenbeutel
State preparation of cold cesium atoms in a nanofiber-based two-color dipole trap

P2–88   **K. P. Nayak**, Y. Kawai, Fam Le Kien, K. Nakajima, H. T. Miyazaki, Y. Sugimoto and K. Hakuta
Nano-Structured Optical Nanofiber: A Novel Workbench For Cavity-QED

Quantum Information and Communication Implementations
Components: Detectors, Quantum memory etc...

P2–89   **Rikizo Ikuta**, Hiroshi Kato, Yoshiaki Kusaka, Shigehito Miki, Taro Yamashita, Hirotaka Terai, Mikio Fujiwara, Takashi Yamamoto, Masato Koashi, Masahide Sasaki, Zhen Wang and Nobuyuki Imoto
High-fidelity frequency down-conversion of visible entangled photon pairs with superconducting single-photon detectors

P2–90   Mustafa Gündoğan, **Patrick M. Ledingham**, Attaallah Almasi, Matteo Cristiani and Hugues de Riedmatten
Quantum Storage of Polarization Qubits in a Doped Solid

P2–91   **Alberto M. Marino**, Quentin Glorieux, Jeremy B. Clark and Paul D. Lett
Storage of Multiple Images using a Gradient Echo Memory in a Vapor Cell

P2–92   **A. R. McMillan**, A. S. Clark, L. Labonté, B. Bell, O. Alibart, A. Martin, S. Tanzilli, W. J. Wadsworth and J. G. Rarity
Demonstration of non-classical interference between heralded single photons from PCF and PPLN-based sources

P2–93   **Mattia Minozzi**, Stefano Bonora, Alexander V. Sergienko, Giuseppe Vallone and Paolo Villoresi
Bi-photon generation with optimized wavefront by means of Adaptive Optics

P2–94   **Adrien Nicolas**, Lambert Giner, Lucile Veissier, Alexandra Sheremet, Michael Scherman, Jose W.R. Tabosa, Elisabeth Giacobino and Julien Laurat
Quantum storage of orbital angular momentum at the single photon level in cold Cs atoms

P2–95   R. Wiegner, **J. von Zanthier** and G. S. Agarwal
Superradiance from entangled atoms

P2–96   Gerhard Humer, Andreas Poppe, Momtchil Peev, Martin Stierle,   Sven Ramelow, Christoph Schäff, Anton Zeilinger and Rupert Ursin
New free-running, low noise 1550nm single photon detector for commercial applications

P2–97   **F. Sciarrino**, L. Sansoni, P. Mataloni, A. Crespi, R. Ramponi and R. Osellame
Integrated quantum photonics for polarization encoded qubits

Poster session 3–Thursday

Foundation of Quantum Physics

P3–0 **So-Young Baek**, Fumihiro Kaneda, Masanao Ozawa and Keiichi Edamatsu
Experimental test of measurement-disturbance relations in generalized photon-polarization measurements

P3–1 **Junghee Ryu**, Changhyoup Lee and Jinhyoung Lee
Multi-settings Greenberger-Horne-Zeilinger nonlocality for N-partite quDits

P3–2 **Juha Salmilehto**, Paolo Solinas, Mikko Möttönen and Jukka P. Pekola
Conservation of operator current in open quantum systems and application to Cooper pair pumping

P3–3 Jukka Kiukas, Pekka Lahti, **Jussi Schultz** and Reinhard F. Werner
Informationally complete phase space observables

P3–4 **L. Krister Shalm**, Sacha Kocsis, Boris Braverman, Sylvain Ravets, Martin J. Stevens, Richard P. Mirin and Aephraim M. Steinberg
Observing the Average Trajectories of Single Photons in a Two-Slit Interferometer

P3–5 **S. Shelly Sharma** and N.K. Sharma
Three qubit correlations in Four qubit States

P3–6 **Piotr Kolenderski**, Urbasi Sinha, Li Youning, Tong Zhao, Matthew Volpini, Adán Cabello, Raymond Laflamme and Thomas Jennewein
Implementing the Aharon-Vaidman quantum game with a Young type photonic qutrit

P3–7 **Christoph Spengler**, Marcus Huber, Stephen Brierley, Theodor Adaktylos and Beatrix C. Hiesmayr
Entanglement detection via mutually unbiased bases

P3–8 **S. Sponar**, J. Klepp, R. Loidl, C. Schmitzer, H. Bartosik, K. Durstberger-Rennhofer, H. Rauch and Y. Hasegawa
Tests of alternative Quantum Theories with Neutrons

P3–9 **Yutaro Suzuki**, Masataka Iinuma and Holger F. Hofmann
Experimental demonstration of Legett-Garg inequality violations by measurements with high resolution and back-action

P3–10 **Eyuri Wakakuwa** and Mio Murao
Chain Rule Implies Tsirelson's Bound

P3–11 **Zizhu Wang** and Damian Markham
Nonlocality of Symmetric States

P3–12 **Bernhard Wittmann**, Sven Ramelow, Fabian Steinlechner, Nathan K. Langford, Nicolas Brunner, Howard M. Wiseman, Rupert Ursin and Anton Zeilinger
Loophole-free Einstein-Podolsky-Rosen Experiment via quantum steering

P3–13 **Magdalena Zych**, Fabio Costa, Igor Pikovski, and Časlav Brukner
Quantum interferometric visibility as a witness of general relativistic proper time

Quantum measurements and metrology

P3–14   Caspar F. Ockeloen, Max F. Riedel, **Roman Schmied** and Philipp Treutlein
Quantum metrology with a scanning probe atom interferometer

P3–15   **Matthias Schreitl**, Georg Winkler, Georgy Kazakov, Georg Steinhauser and Thorsten Schumm
Towards a nuclear clock with Thorium-229

P3–16   **A. V. Sergienko**, A.M. Fraine, O.V. Minaeva, R. Egorov and D. S. Simon
High-resolution Quantum Interferometry Meets Telecom Industry Needs

P3–17   **Yutaka Shikano**
On Signal Amplification via Weak Measurement

P3–18   **Piotr Kolenderski**, Artur Czerwinski, Carmelo Scarcella, Simone Bellisai, Alberto Tosi and Thomas Jennewein
Reconstruction of single photon's transverse spatial wave function

P3–19   **Nicolò Spagnolo** Chiara Vitelli, Vittorio Giovannetti, Lorenzo Maccone and Fabio Sciarrino
Phase estimation for noisy detectors via parametric amplification

P3–20   **Takanori Sugiyama**, Peter S. Turner and Mio Murao
Understanding boundary effects in quantum state tomography-one qubit case

P3–21   Dmitry A. Kalashnikov, **Si-Hui Tan**, Timur Sh. Iskhakov, Maria V. Chekhova and Leonid A. Krivitsky
Measurement of two-mode squeezing with photon number resolving multi- pixel detectors

P3–22   Douglas Vitoreti, Thiago Ferreira da Silva, **Guilherme P. Temporão** and Jean Pierre von der Weid
Tailoring two-photon interference from independent sources

P3–23   Maxim Goryachev, Daniel L. Creedon, Eugene N. Ivanov, Serge Galliou, Roger Bourquin and **Michael E. Tobar**
Extremely high Q-factor mechanical modes in quartz Bulk Acoustic Wave Resonators at millikelvin temperature

P3–24   S. Oppel, Th. Büttner, P. Kok and J. von Zanthier
Beating the classical resolution limit via multi-photon interferences of independent light sources

P3–25   Maria Tengner, Sara L. Mouradian, Tian Zhong, P. Ben Dixon, Zheshen Zhang, **Franco N. C. Wong** and Jeffrey H. Shapiro
Experimental Implementations of Quantum Illumination

P3–26   Ranjith Nair, **Brent J. Yen**, Saikat Guha, Jeffrey H. Shapiro and Stefano Pirandola
Quantum M-ary Phase Discrimination

P3–27   **Tian Zhong** and Franco N. C. Wong
Franson interferometry with 99.6% visibility via fiberoptic dispersion engineering

Quantum control

P3–28   **Burkhard Scharfenberger**, William J. Munro and Kae Nemoto
Coherent manipulation of an NV center and an carbon nuclear spin

P3–29   **Mankei Tsang** and Carlton M. Caves
Evading quantum mechanics

P3–30 **Thomas Vanderbruggen**, Ralf Kohlhaas, Andrea Bertoldi, Simon Bernon, Alain Aspect, Arnaud Landragin, and Philippe Bouyer
Quantum feedback control of atomic coherent states

Quantum Communication and Cryptography

P3–31 Thomas Lorünser, Andreas Happe, Momtchil Peev, Florian Hipp, Damian Melniczuk, Pattama Cummon, Pituk Panthong, Paramin Sangwongngam and **Andreas Poppe**
Timing synchronization with photon pairs for quantum communications

P3–32 Xiongfeng Ma and **Mohsen Razavi**
Practical schemes for measurement-device-independent quantum key distribution

P3–33 **K. Shimizu**, T. Honjo, M. Fujiwara, S. Miki, T. Yamashita, H. Terai, Z. Wang and M. Sasaki
Middle-term operation performance of long-distance quantum key distribution over a field-installed 90-km fiber-optic loop

P3–34 Kaoru Shimizu, Kiyoshi Tamaki and Nobuyuki Imoto
Cheat-sensitive commitment of a classical bit coded in a block of mxn round-trip qubits

P3–35 **Devin H. Smith**, Geoff Gillett, Cyril Branciard, Marcelo de Almeida, Alessandro Fedrizzi, Brice Calkins, Thomas Gerrits, Adriana Lita, Antia Lamas-Linares, SaeWoo Nam and Andrew G. White
Implmentation of Semi-device-independent Quantum Key Distribution

P3–36 **Masaki Sohma** and Osamu Hirota
Coherent pulse position modulation quantum cipher

P3–37 Alessio Avella, Giorgio Brida, Dino Carpentras, Andrea Cavanna, Ivo Pietro Degiovanni, Marco Genovese, Marco Gramegna and **Paolo Traina**
Novel QKD experiments performed at INRIM

P3–38 Ivan Capraro, Andrea Tomaello, Thomas Herbst, Rupert Ursin, Giuseppe Vallone and Paolo Villoresi
Turbulent single-photon propagation in the Canary optical link

P3–39 **Nathan Walk**, Thomas Symul, Ping Koy Lam and Timothy C. Ralph
Security of Continuous Variable Quantum Cryptography with Post-selection

P3–40 **Shuang Wang**, Zhen-Qiang Yin, Wei Chen, Jun-Fu Guo, Hong-Wei Li, Guang-Can Guo and Zheng-Fu Han
Gigahertz quantum key distribution over 260 km of standard telecom fiber

P3–41 **K. Yoshino**, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki and A. Tajima
WDM quantum key distribution system using dual-mode single photon detectors

P3–42 **Michael Zwerger**, Wolfgang Dür and Hans J. Briegel
Measurement-based quantum repeaters

Quantum Information and Communication theory

P3–43 Akihito Soeda, Yoshiyuki Kinjo, Peter S. Turner and **Mio Murao**
Implementing controlled-unitary operations over the butterfly network

Quantum Information and Communication Implementations
Atoms/Ions

P3–61 **Philipp Schindler**, Markus Müller, Daniel Nigg, Julio Barreiro, Thomas Monz, Michael Chwalla, Markus Hennrich, Sebastian Diehl, Peter Zoller and Rainer Blatt
Simulation of driven open quantum systems with trapped ions

P3–62 L. Slodička, N. Röck, P. Schindler, M. Hennrich, G. Hétet, R. Blatt
Entanglement of two ions by single-photon detection

P3–63 **Matthias Steiner**, Hendrik-Marten Meyer and Michael Köhl
Towards an ion-cavity system with single Yb+ions

P3–64 **Stuart Szigeti**, Russell Anderson, Lincoln Turner and Joseph Hope
Precise manipulation of a Bose-Einstein condensate's wavefunction

Quantum Information and Communication Implementations
Solid State: Superconductors, Quantum Dots, Nano mechanics etc...

P3–65 **A. Jöckel**, M. T. Rakher, M. Korppi, S. Camerer, D. Hunger, M. Mader, and P. Treutlein
Spectroscopy of mechanical dissipation in micro-mechanical membranes

P3–66 **Thomas Kauten**, Harishankar Jayakumar, Ana Predojević and Gregor Weihs
Time-bin interferometry of short coherence down-conversion photon pairs

P3–67 **Casey R. Myers**, Thomas. M. Stace and Gerard J. Milburn
The Synchronisation of Nano-Mechanical Resonators Coupled via a Common Cavity Field in the Presence of Quantum Noise

P3–68 Harishankar Jayakumar **Ana Predojević**, Thomas Kauten, Tobias Huber, Glenn S. Solomon and Gregor Weihs
All Optical Resonant Excitation and Coherent Manipulation of a Single InAs Quantum Dot for Quantum Information Experiments

P3–69 **Ramachandrarao Yalla**, K. P. Nayak, and K. Hakuta
Fluorescence photon measurements from single quantum dots on an optical nanofiber

Quantum Information and Communication Implementations
Defects and Ions in Crystals, Spins

P3–70 **Imam Usmani**, Christoph Clausen, Félix Bussières, Nicolas Sangouard, Mikael Afzelius and Nicolas Gisin
Heralded quantum entanglement between two crystals

Quantum Information and Communication Implementations
Photons and Linear Optics QIP

P3–71 Borivoje Dakic, Yannick Ole Lipp, Xiaosong Ma, **Martin Ringbauer**, Sebastian Kropatschek, Stefanie Barz, Tomasz Paterek, Vlatko Vedral, Anton Zeilinger, Časlav Brukner and Philip Walther
Quantum Discord as Resource for Remote State Preparation

P3–72 **Christoph Schaeff**, Robert Polster, Radek Lapkiewicz, Robert Fickler, Sven Ramelow and Anton Zeilinger
Photonic platform for experiments in higher dimensional quantum systems

P3–73 **A. Schreiber**, A. Gábris, P. P. Rohde, K. Laiho, M. Štefaňák, V. Potoček, C. Hamilton, I. Jex and C. Silberhorn
A 2D Quantum Walk Simulation of Two-Particle Dynamics

P3–74 **Christian Schwemmer**, Géza Tóth, Alexander Niggebaum, Tobias Moroder, Philipp Hyllus, Otfried Gühne and Harald Weinfurter
Permutationally invariant tomography of symmetric Dicke states

P3–75 **L. Sansoni**, I. Bongioanni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi and R. Osellame
Integrated photonic quantum gates for polarization qubits

P3–76 Damien Bonneau, Erman Engin, Josh Silverstone, Chandra M. Natarajan, M. G. Tanner, R. H. Hadfield, Sanders N. Dorenbos, Val Zwiller, Kazuya Ohira, Nobuo Suzuki, Haruhiko Yoshida, Norio Iizuka, Mizunori Ezaki and Jeremy L. O'Brien, Mark G. Thompson
Silicon Quantum Photonic Technology Platform: Sources and Circuits

P3–77 **Nicolò Spagnolo**, Lorenzo Aparo, Chiara Vitelli, Andrea Crespi, Roberta Ramponi, Roberto Osellame, Paolo Mataloni and Fabio Sciarrino Mataloni and Fabio Sciarrino
3D integrated photonic quantum interferometry

P3–78 **Jovica Stanojevic**, Valentina Parigi, Erwan Bimbard, Alexei Ourjoumtsev, Pierre Pillet and Philippe Grangier
Generating non-Gaussian states using collisions between Rydberg polaritons

P3–79 **André Stefanov**, Christof Bernhard, Bänz Bessire and Thomas Feurer
Qudits implementation with broadband entangled photons

P3–80 Shuntaro Takeda, Takahiro Mizuta, Maria Fuwa, Jun-ichi Yoshikawa, Hidehiro Yonezawa and Akira Furusawa
Generation of time-bin qubits for continuous-variable quantum information processing

P3–81 **T. Tashima**, M. S. Tame, Ş. K. Özdemir, M. Koashi and H.Weinfurter
Photonic multipartite entanglement conversion using nonlocal operations

P3–82 Muthiah Annamalai, Nikolai Stelmakh, **Michael Vasilyev** and Prem Kumar
Spatial eigenmodes of traveling-wave phase-sensitive parametric amplifiers

P3–83 **Jian Yang** and Paul Kwiat
Photon-Photon Interaction in Strong-Coupling Cavity-Quantum Dot System

P3–84 **Kevin Zielnicki** and Paul Kwiat
Engineering a Factorable Photon Pair Source

Quantum Information and Communication Implementations
Hybrid quantum systems

P3–85 **András Pályi**, Philipp R. Struck, Mark Rudner, Karsten Flensberg and Guido Burkard
Spin-orbit-induced strong coupling of a single spin to a nanomechanical resonator

P3–86 **S. Putz**, R. Amsüss, Ch. Koller, T. Nöbauer, R. Voglauer, A. Maier, S. Rotter, K. Sandner, S. Schneider, H. Ritsch, J. Schmiedmayer and J. Majer
Hybrid Quantum System: Coupling Atoms and Diamond Color Centers to Superconducting Cavities

P3–87 **K. Stannigel**, P. Komar, S. J. M. Habraken, S. D. Bennett, M. D. Lukin, P. Zoller and P. Rabl
Optomechanical quantum information processing with photons and phonons

Quantum Information and Communication Implementations
Components: Detectors, Quantum memory etc...

P3–88 **C. I. Osorio**, N. Bruno, N. Sangouard, A. Martin, H. Zbinden, N. Gisin and R. T. Thew
Heralded photon amplification for quantum communication

P3–89 **Lorenzo Procopio**, Max Tillmann and Philip Walther
Ultrafast superconducting nanowire single-photon detectors for femtosecondpulsed multi-photon experiments

P3–90 **B. M. Sparkes**, C. Cairns, M. Hosseini, D. Higginbottom, G. T. Campbell, P. K. Lam and B. C. Buchler
Precision Spectral Manipulation Using a Coherent Optical Memory

P3–91 **Fabian Steinlechner**, Pavel Trojek, Marc Jofre, Henning Weier, Josep Perdigues, Eric Wille, Thomas Jennewein, Rupert Ursin, John Rarity and Morgan W. Mitchell, Juan P. Torres, Harald Weinfurter and Valerio Pruneri
A high brightness source of polarization entangled photons for applications in space

P3–92 **Jiří Svozilík**, Adam V. Marí, Michal Mičuda, Martin Hendrych and Juan P. Torres
Towards efficient photon pairs production in Bragg reflection waveguides

P3–93 Daqing Wang, Thomas Herbst, Sebastian Kropatschek, Xiaosong Ma, Anton Zeilinger and Rupert Ursin
Characterization of single-photon detectors for free-space quantum communica- tion

P3–94 **Christian Wuttke** and Arno Rauschenbeutel
Nanofiber-Based Fabry-Pérot Microresonators: Characteristics and Applications

P3–95 **Lars S. Madsen**, Adriano Berni, Mikael Lassen and Ulrik L. Andersen
Experimental Investigation of the Evolution of Gaussian Quantum Discord in an Open System

P3–96 **R.J. Sewell**, M. Koschorreck, M. Napolitano, B. Dubost, N. Behbood, G. Colangelo, F. Martin and M.W. Mitchell
Spin squeezing via QND measurement in an Optical Magnetometer

P3–97 A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez and **W. Tittel**
A quantum key distribution system immune to detector attacks

Monday talks abstracts

Hybrid quantum systems.

G. J. Milburn [1]

[1] *Centre for Engineered Quantum Systems, The University of Queensland, QLD 4072, Australia.*

The last decade has seen a considerable increase in the variety and size of physical systems which can be subjected to coherent quantum control[1]. A feature of these systems is that quantisation is carried out by identifying particular macroscopic degrees of freedom that can be described quantum mechanically. For example, in many optomechanical and nanomechanical systems the vibrational modes of a bulk mechanical resonator are described as a quantised simple harmonic oscillator. In the case of superconducting circuits one moves to an effective LC circuit and quantisation is preformed via the canonical variables of charge on an effective capacitor and the flux through an equivalent inductor.

The key lesson is that, given sufficiently sophisticated fabrication, certain collective degrees of freedom can be engineered so as to enable coherent quantum control. Of course microscopic degrees of freedom remain as a source of dissipation and noise. Indeed, the degree of engineering required is precisely directed at carefully controlling decoherence through coupling to residual microscopic degrees of freedom or directly engineering new kids of dissipative channels[2]. We are justified in referring to these new kinds of collective quantum systems as engineered quantum systems and to distinguish their behaviour from that observed in naturally occurring quantum systems found in atomic, molecular and condensed matter physics.

One other important features of these systems is worth noting: they are often anything but microscopic. LIGO, for example, is a quantum machine covering many square kilometres operating up against the Heisenberg uncertainty principle. The old equivalence of quantum/classical with microscopic/macroscopic begins to look a little dated in the light of recent advances in engineered quantum systems. Of course the old puzzles of quantum theory remain just as evident as ever, but are now in the context of a single rather large quantum system that can exhibit both classical and quantum degrees of freedom in one and the same device.

Engineered quantum systems are now moving beyond single technology platforms towards hybrid systems. Examples include;

- combining optical and microwave control of electron and nuclear spins in solids such as NV diamond[3]

- controlling semiconductor quantum dots with superconducting quantum circuits[4]

- combining superconducting electronic circuits with trapped ions and molecules[5, 6]

- interfacing microwave and optical cavities via nanomechanical and micromechanical quantum resonators[7]

- interfacing cold atoms and micromechanics[8]

- quantum optoelectronics[9]

to name but a few of this rapidly growing list. Hybrid quantum systems has become the leitmotif for a new generation of quantum science research.

The continued development of this field will require a more systems-level engineering perspective to address such issues as noise and decoherence in complex, multi platform systems, quantum and classical control of diverse physical components with diverse timescales, in-line quantum information processing and quantum memories, coexistence of discrete and continuous dynamics etc. In this talk I will give some examples of how these issues arise in the context of particular hybrid quantum systems and give some (admittedly speculative) examples of possible quantum enabled technologies based on hybrid quantum systems.

References

[1] M. J. Woolley and G. J. Milburn , Acta Physica Slovaca **61**, 483 601 (2011).

[2] A. Tomadin, S. Diehl, P. Zoller, Phys. Rev. A **83**, 013611 (2011).

[3] X. Zhu, S. Saito, A. Kemp, K. Kakuyanagi, S. Karimoto, H. Nakano, W. J. Munro, Y. Tokura, M. S. Everitt, K. Nemoto, M. Kasu, N. Mizuochi, K. Semba, Nature **478**, 221-224 (2011); Y. Kubo, C. Grezes, A. Dewes, T. Umeda, J. Isoya, H. Sumiya, N. Morishita, H. Abe, S. Onoda, T. Ohshima, V. Jacques, A. Dreau, J. -F Roch, I. Diniz, A. Auffeves, D. Vion, D. Esteve, P. Bertet, Phys. Rev. Lett. **107**, 220501 (2011)

[4] T Frey, P. J. Leek, M. Beck, A. Blais, T. Ihn, K. Ensslin, A. Wallraff, Phys. Rev. Lett. **108**, 046807 (2012).

[5] D. Kielpinski, D. Kafri, M. J. Woolley, G. J. Milburn, and J. M. Taylor, Phys. Rev. Lett. **108**, 130504 (2012).

[6] P. Rabl, D. Demille, J. Doyle, M. Lukin, R. Schoelkopf, P. Zoller, Phys. Rev. Lett, **7** 033003 (2006).

[7] Sh. Barzanjeh, D. Vitali, P. Tombesi, and G. J. Milburn, Phys. Rev. A 84, 042342 (2011).

[8] S. Camerer, M. Korppi, A. Jöckel, D. Hunger, T. W. HŁnsch, and P. Treutlein, Phys. Rev. Lett. **107**, 223001 (2011).

[9] M. Tsang, Phys. Rev. A **84**, 043845 (2011).

Quantum interface between an electrical circuit and a single atom

D. Kielpinski[1], **D. Kafri**[2], **M. J. Woolley**[3], **G. J. Milburn**[3], and **J. M. Taylor**[2]

[1]*Centre for Quantum Dynamics, Griffith University, Nathan, QLD 4111, Australia*
[2]*Joint Quantum Institute/NIST, College Park, MD, USA*
[3]*Centre for Engineered Quantum Systems, School of Mathematics and Physics, The University of Queensland, St Lucia, QLD 4072, Australia*

Atomic systems are remarkably well suited to storage and processing of quantum information. However, their properties are tightly constrained by nature, causing difficulties in interfacing to other optical or electronic devices. On the other hand, quantum electronic circuits, such as superconducting interference devices, may be easily engineered to the designer's specifications and are readily integrated with existing microelectronics. The naturally existing couplings between a single atom and a single microwave photon in a superconducting circuit are too weak for practical coherent interfaces [1].

We propose a method to couple single trapped ions with microwave circuits, bridging the gap between the very different frequencies of ion motion and microwave photon by parametric modulation of the microwave frequency [2]. The resulting coupling strength of $\sim 2\pi \times 60$ kHz is sufficient for high-fidelity coherent operations and similar to the strength of currently obtained ion-ion couplings. A simple model system illustrating the key concepts is shown in Fig. 1(a). Microwave photons reside in a superconducting LC circuit with natural frequency $\omega_{\mathrm{LC}} = 1/\sqrt{LC} \approx 1$ GHz. A single ion is confined within the capacitor C_s and can oscillate at the motional frequency $\omega_i \approx 10$ MHz. The circuit voltage across C_s generates an electric field that couples to the ion's motional electric dipole. Modulating the circuit capacitance by C_{mod} at a frequency ν causes the superconducting voltage to acquire sidebands at frequencies $\omega_{\mathrm{LC}} \pm \nu$. The coupling between the superconducting circuit and the ion motion becomes resonant when $\omega_i \approx \omega_{\mathrm{LC}} - \nu$. The interaction Hamiltonian is then

$$H_{\mathrm{int}} = \hbar g\, ab^\dagger + \text{h.c.} \tag{1}$$

where a and b are the annihilation operators of the microwave photon mode and the ion motional mode, respectively.

In the proposed device (Fig. 1(b)), ions are confined above a set of island electrodes, which couple the electric dipole arising from ion motion to a superconducting inductor and a bulk-acoustic-wave capacitance modulator. The ion trap uses a planar electrode structure of a type now widely used for microfabricated trap arrays (Fig. 1(c)). Applying appropriate voltages to the electrodes generates RF electric fields, which provide a ponderomotive confining potential transverse to the trap axis, and DC fields that give rise to a harmonic potential along the axis. To activate the ion-circuit coupling, one excites acoustic waves in the BAW at frequency $\nu_B \approx \omega_{\mathrm{LC}} - \omega_i$ by voltage driving of metallic electrodes on the BAW surface (Fig. 1(d)). The modulation of the BAW-substrate gap distance provides the desired capacitance modulation.

The coupling between the LC circuit and the ion motion allows us to generalize all the well-known protocols operating on ion spin and motion to protocols operating on ion spin
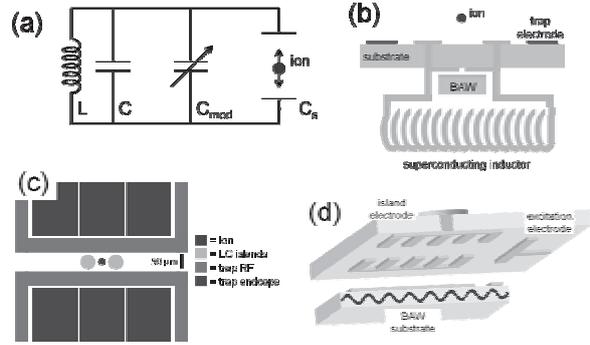

Figure 1: a) Equivalent-circuit model of our scheme for ion-circuit coupling. b) Top view of surface ion trap showing RF and DC trapping electrodes. The "LC island" electrodes couple the ion motion to the LC circuit excitation. c) Side view of device, showing ion trap, superconducting inductor, and BAW device. d) Exploded side view of BAW device. Purple line: transverse displacement of BAW substrate due to classical driving.

and LC state. Ion spin-motion protocols now allow for generation of nearly arbitrary spin/motion entangled states [3]. By this means, one can establish a quantum communications channel between LC circuits in separate dewars, couple ion spins through a common LC circuit for large-scale quantum computing on a single chip, and perform Heisenberg-limited voltage metrology in the microwave domain by generating large Schrödinger cat states of the LC mode.

References

[1] J. Verdú et al., Strong magnetic coupling of an ultracold gas to a superconducting waveguide cavity, Phys. Rev. Lett. **103**, 043603 (2009).

[2] D. Kielpinski, D. Kafri, M. J. Woolley, G. J. Milburn, and J. M. Taylor, Quantum interface between an electrical circuit and a single atom, to appear in Phys. Rev. Lett. (2012).

[3] D. Leibfried, R. Blatt, C. Monroe, and D. Wineland, Quantum dynamics of single trapped ions, Rev. Mod. Phys. **75**, 281 (2003).

Hybrid atom-membrane optomechanics

M. Korppi[1], **A. Jöckel**[1], **S. Camerer**[2], **D. Hunger**[2], **M. Rakher**[1], **T. W. Hänsch**[2], and **P. Treutlein**[1]

[1]*Department of Physics, University of Basel, Switzerland*
[2]*Max-Planck-Institute of Quantum Optics and Ludwig-Maximilians-University, Munich, Germany*

Laser light can exert a force on dielectric objects through radiation pressure and through the optical dipole force. In the active field of optomechanics, such light forces are exploited for cooling and control of the vibrations of mechanical oscillators, with possible applications in precision force sensing and studies of quantum physics at macroscopic scales. This has many similarities with the field of ultracold atoms, where radiation pressure forces are routinely used for laser cooling and optical dipole forces are used for trapping and quantum manipulation of atomic motion. It has been proposed that light forces could also be used to couple the motion of atoms in a trap to the vibrations of a single mode of a mechanical oscillator (see [1] for a review). In the resulting hybrid optomechanical system the atoms could be used to read out the motion of the oscillator, to engineer its dissipation, and ultimately to perform quantum information tasks such as coherently exchanging the quantum state of the two systems. Here we discuss the experimental realization of a hybrid optomechanical system in which an optical lattice mediates a long-distance coupling between ultracold atoms and a micromechanical membrane [2].

The coupling scheme is illustrated in Fig. 1a. A laser beam is partially reflected at a SiN membrane and forms a 1D optical lattice for an ultracold atomic ensemble. Motion of the membrane displaces the lattice and thus couples to atomic motion. Conversely, atomic motion is imprinted as a power modulation onto the laser, thus modulating the radiation pressure force on the membrane. In this way, the lattice laser light mediates an optomechanical coupling between membrane vibrations and atomic center-of-mass motion [3]. If the trap frequency ω_{at} of the atoms in the lattice is matched to the eigenfrequency ω_m of the membrane, the coupling leads to resonant energy transfer between the two systems.

In our experiment, we observe for the first time the backaction of the atomic motion onto the membrane vibrations, which is required for cooling and manipulating the membrane with the atoms. The backaction is observed in membrane ringdown measurements, which directly probe the mechanical decay rate. We choose the lattice laser power so that $\omega_{at} = \omega_m$ and perform alternating experiments with and without atoms in the lattice. Figure 1b shows the observed change $\Delta\gamma$ in the membrane decay rate due to the presence of the atoms as a function of the atom number N. We find a linear dependence of $\Delta\gamma$ on N that quantitatively agrees with the full quantum theory of our system described in [3]. This mechanism can be used to sympathetically cool the membrane vibrations with laser-cooled atoms.

The coupling strength can be enhanced by placing the membrane and/or the atoms into an optical cavity. Theoretical investigations show that such a system gives access to the strong coupling regime, where the atom-membrane coupling is stronger than all dissipation rates of the system [4].
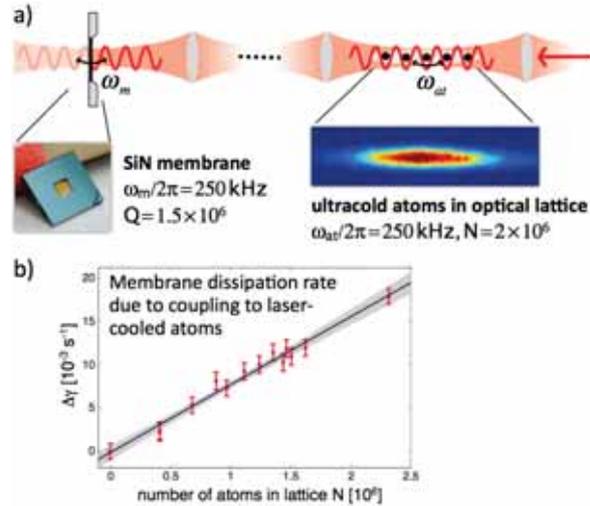

Figure 1: Optomechanical coupling of atoms and membrane. (a) Schematic of the experiment. Laser light mediates an optomechanical coupling between the vibrations of a SiN membrane oscillator at frequency ω_m and the center-of-mass motion of N ultracold atoms in an optical lattice with trap frequency ω_{at}. (b) Backaction of atoms onto membrane vibrations. The graph shows the measured change $\Delta\gamma$ in the membrane dissipation rate due to the coupling to N laser-cooled atoms.

References

[1] D. Hunger, S. Camerer, M. Korppi, A. Jöckel, T. W. Hänsch, and P. Treutlein, C. R. Physique **12**, 871 (2011).

[2] S. Camerer, M. Korppi, A. Jöckel, D. Hunger, T. W. Hänsch, and P. Treutlein, Phys. Rev. Lett. **107**, 223001 (2011).

[3] K. Hammerer, K. Stannigel, C. Genes, P. Zoller, P. Treutlein, S. Camerer, D. Hunger, and T. W. Hänsch, Phys. Rev. A **82**, 021803 (2010).

[4] K. Hammerer, M. Wallquist, C. Genes, M. Ludwig, F. Marquardt, P. Treutlein, P. Zoller, J. Ye, and H. J. Kimble, Phys. Rev. Lett. **103**, 063005 (2009).

Hybrid quantum circuit with a superconducting qubit coupled to a spin ensemble

Y. Kubo[1], **C. Grezes**[1], **T. Umeda**[2], **J. Isoya**[2], **H. Sumiya**[3], **N. Morishita**[4], **H. Abe**[4], **S. Onoda**[4], **T. Ohshima**[4], **V. Jacques**[5], **A. Drau**[5], **J.-F. Roch**[5], **I. Diniz**[6], **A. Auffeves**[6], **D. Vion**[1], **D. Esteve**[1], and **P. Bertet**[1]

[1]*Quantronics group, SPEC (CNRS URA 2464), IRAMIS, DSM, CEA-Saclay, 91191 Gif-sur-Yvette, France*
[2]*Research Center for Knowledge Communities, University of Tsukuba, Tsukuba 305-8550, Japan*
[3]*Sumitomo Electric Industries Ltd., Itami 664-001, Japan*
[4]*Japan Atomic Energy Agency, Takasaki 370-1292, Japan*
[5]*LPQM (CNRS UMR 8537), ENS de Cachan, 94235 Cachan, France*
[6]*Institut Neel, CNRS, BP 166, 38042 Grenoble, France*

Making a hybrid quantum machine that would store quantum information in microscopic quantum objects with good coherence properties and that would process this information in a fast and efficient way with superconducting qubits is appealing. We report here an experiment along this idea, in which a macroscopic number of electronic spins is used as a single qubit memory, strongly coupled to a Josephson qubit by a quantum bus. The spins are nitrogen-vacancy centers in a diamond crystal, the qubit is a Cooper pair box of the Transmon type, and the bus a superconducting resonator with tunable frequency. We demonstrate strong coupling between the spins and the bus [1], vacuum Rabi oscillations between the qubit and the bus, as well as storage of a single photon from the qubit to the spins [2], and partial retrieval of it with fidelity of about 10%. We also use this hybrid circuit to demonstrate a new type of high-sensitivity electron spin resonance spectroscopy at the level of a few excitations in the spin ensemble [3].

References

[1] Y. Kubo, *et al.*, Phys. Rev. Lett. **105**, 140502 (2010).

[2] Y. Kubo, *et al.*, Phys. Rev. Lett. **107**, 220501 (2011).

[3] Y. Kubo, *et al.*, subm. to Phys. Rev. X (2012).

Chip-Scale Optomechanics: towards quantum light and sound

Oskar Painter[1]

[1]*California Institute of Technology, Pasadena, United States*

In the last several years, rapid advances have been made in the field of cavity optomechanics, in which the usually feeble radiation pressure force of light is used to manipulate, and precisely monitor, mechanical motion. Amongst the many new geometries studied, coupled phononic and photonic crystal structures (dubbed optomechanical crystals) provide a means for creating integrated, chip-scale, optomechanical systems. Applications of these new nano-opto-mechanical systems include all-optically tunable photonics, optically powered RF and microwave oscillators, and precision force, acceleration and mass sensing. Additionally there is the potential for these systems to be used in hybrid quantum networks, enabling storage or transfer of quantum information between disparate quantum systems. A prerequisite for such quantum applications is the removal of thermal excitations from the low-frequency mechanical oscillator. In this talk I will describe our recent efforts to optically cool and measure the quantum mechanical ground-state of a GHz mechanical resonator formed in a quasi-1D nanobeam optomechanical crystal, and the use of this structure to demonstrate efficient translation between light and sound quanta.

QCMC 2012
Vienna, Austria

Coupling a superconducting flux qubit to an NV ensemble: A hybrid system's approach for quantum media conversion

<u>W. J. Munro</u>[1,2], S. Saito[1], X. Zhu[1], Y. Matsuzaki[1], Kae Nemoto[2], T. Shimooka[3], N. Mizuochi[3] & K. Semba[1]

[1] *NTT Basic Research Laboratories, NTT Corporation,3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, 243-0198, Japan*
[2]*National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo-to 101-8430, Japan*
[3]*University of Osaka, Graduate school of Engineering Science,1-3, Machikane-yama, Toyonaka, Osaka, 560-8531, Japan*

Quantum information has reached a very interesting stage in its development, where we have seen many fundamental experiments laying the foundation for practical systems. One particularly promising candidate are superconducting quantum bits based on Josephson junctions. These systems have demonstrated many of the fundamental operations needed for quantum computation, however, the experimentally reported coherence times are likely to be insufficient for future large-scale distributed quantum computation. Additionally it is also not clear how quantum information can be moved between the distributed parts of the quantum computer. A potential solution is to design and use a dedicated engineered quantum memory based on atomic/molecular systems that also had an optical transition. In this context a superconductor-spin ensemble hybrid system has attracted increasing interest[1, 2]. Such schemes have the potential to couple superconducting solid-state qubits to optical fields via atomic systems, thus allowing quantum media conversion.

Nitrogen vacancy color centers in diamond have suitable properties to act as such a memory and an interface between the optical and microwave regimes. The ground state of a NV- centre is a triplet (S=1) with the $|m_s = 0\rangle$ state separated by 2.878GHz from the near-degenerate excited states $|m_s = \pm 1\rangle$ (under zero magnetic field). This energy separation is ideal for a superconducting qubit to be brought into and out of resonance with it (this is especially true for a gap tunable flux qubit[3]). Next the NV- centre possesses an 637nm transition which allows the state of NV center (or centers) to be transferred to an optical field. The first step in this process is hence going to be coherently couple the superconducting qubit to the NV- ensemble[4, 5].
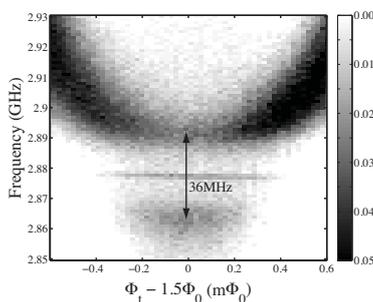

Figure 1: Energy spectrum of the flux qubit coupled to an NV ensemble.

We have fabricated a gap tunable superconducting flux qubit on a sapphire substrate and positioned a diamond chip containing NV- centers (4.7×10^{17} cm^{-3}). The qubit spectrum illustrated in Figure 1 shows an energy anti crossing at 2.878 GHz due to the NV- centers. The large splitting of 36 MHz means that the qubits is coupling to millions of NV-centers collectively. This collective coupling can be used to transfer a single microwave quantum of energy from the flux qubit to the NV- ensemble (shown in Figure 2 as vacuum Rabi oscillations). Furthermore we can show definite entanglement between this two systems as well as the ensemble acting as a memory for the flux qubit.
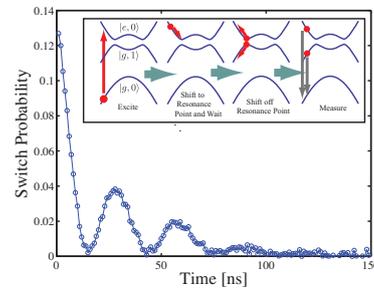

Figure 2: Vacuum Rabi oscillations of the flux qubit/NV- ensemble resonantly coupled system of an initially excited flux qubit. Inset, measurement sequence.

This is a significant step towards the realization of a long-lived quantum memory for condensed-matter systems, with an additional potential future application as an interface between the microwave and optical domains

References

[1] Y. Kubo et. al, *Strong coupling of a spin ensemble to a superconducting resonator*, Phys. Rev. Lett. 105, 140502 (2010).

[2] R. Amsuss et. al, *Cavity QED with magnetically coupled collective spin states*, Phys. Rev. Lett. 107, 060502 (2011).

[3] D. Marcos et. al, *Coupling nitrogen-vacancy centers in diamond to superconducting flux qubits*. Phys. Rev. Lett. 105, 210501 (2010).

[4] X. Zhu et. al, *Coherent coupling of a superconducting flux-qubit to an electron spin ensemble in diamond*, Nature **478**, 221-224 (2011).

[5] Y. Kubo et. al, *Hybrid Quantum Circuit with a Superconducting Qubit Coupled to a Spin Ensemble*, Phys. Rev. Lett. 107, 220501 (2011)

Quantum correlations with indefinite causal order

Caslav Brukner

Faculty of Physics, University of Vienna, Austria

In quantum physics it is standardly assumed that the background time or definite causal structure exists such that every transformation is either in the future, in the past or space-like separated from any other transformation. Consequently, the correlations between transformations respect definite causal order: they are either signalling correlations for the time-like or no-signalling correlations for the space-like separated transformations. We develop a framework that assumes only that transformations in local laboratories are described by quantum mechanics (i.e. are completely-positive maps), but relax the assumption that they are causally connected. Remarkably, we find situations where two transformations are neither causally ordered nor in a probabilistic mixture of definite causal orders, i.e. one cannot say that one transformation is before or after the other. The correlations between the transformations are shown to enable performing a communication task that is impossible if the operations are ordered according to a fixed background time.

INTEGRATED, TIME MULTIPLEXED PHOTONIC NETWORKS

Silberhorn, Ch.[1,2]**, Schreiber, A**[1,2]**, Cassemiro, K.N.**[1,2]**, Laiho K.**[1,2]**, Rohde P.P.**[1,4]**, Jex I.**[3]**, Gabris A.**[3]**, Stefanak M.**[3]**, Potocek V.**[3] **and Hamilton C.**[3]

[1] *University of Paderborn, Integrated Quantum Optics, Paderborn, Germany*
[2] *Max Planck Institute for Science of Light, Erlangen, Germany*
[3] *Department of Physics, Faculty of Nuclear Sciences and Physical Engineering, Praha,, Czech Republic*
[4] *Centre for Engineered Quantum Systems, Department of Physics and Astronomy, Macquarie University, Australia*

The experimental realization of optical quantum networks with a large number of modes poses stringent conditions on the stability and synchronization of events, the control of all system pa-rameters and the preparation pure photonic quantum state. Based on pulsed light, integrated op-tics and time-multiplexing geometries we explore the possibilities for the implementation of large photonic quantum systems. We present our progress in this field by presenting our results on dif-ferent aspects of an overall system.

Most recently photonic quantum walks have attracted attention, because they can be considered as a standard model to describe the dynamics of quantum particles in a discretized environment. They can serve as a test bed for the simulation of various quantum systems. We employ time multiplexing with pulsed light in specific fiber loop geometries to demonstrate different types photonic quantum walks. By using the polarisation as internal degree of freedom we can imple-ment arbitrary coin states, while the realization of the step operator in the temporal domain pro-vides superior coherence properties for the scalability of the walk [1]. We demonstrate a fully coherent photonic quantum walk over 28 steps on a line, cor-responding to a network of over four hundred beam splitters. By introducing an optical modulator we can precisely control the dy-namics of the photonic walk. We have studied the propagation of a quantum particle in the pres-ence of different types of engineered noise resulting in a classical quantum walk or Anderson localization [2]. We further extended our 1D quantum walk experiment to a 2D graph structure, and show a fully coherent quantum walk on a lattice over 12 steps and 196 position. The higher dimensional topological structure and the flexibility of our setup with dynamic control allows us to simulate the creation of entanglement in bipartite systems, non-linear interactions, and two-particle scattering [3].

For the generation pulsed quantum states of light we use parametric down conversion (PDC) waveguide sources in combination with spectral source engineering. Thus we can accomplish complete control over the spatio-spectral mode properties enabling us to tune our state character-istics from genuine single mode to multi-mode. The reduction of the PDC to the low number of excited modes features exceptional source brightness, and the definition of the spatial modes by the guide provides a good compatibility with fiber networks [4].

References

[1] A. Schreiber, et al., Science, **336**, 55 (2012).

[2] A. Schreiber, et al., Phys. Rev. Lett., **106**, 180403 (2011).

[3] A. Schreiber, et al., Phys. Rev. Lett., 104, 050502 (2010).

[4] A. Schreiber, et al., Phys. Rev. Lett., **106**, 013603 (2011).

Engineering photonic quantum emulators and simulators

Andrew White[1−3]

[1] *Centre for Engineered Quantum Systems, and* [2] *Centre for Quantum Computing and Communication Technology,*
[3] *School of Mathematics and Physics, University of Queensland, Brisbane, Australia*

In principle, it is possible to model any physical system exactly using quantum mechanics; in practice, it quickly becomes infeasible. Recognising this, Feynman suggested that quantum systems be used to model quantum problems[1].

There are two approaches: *simulation*, where digital outcomes yield the desired physical quanties—e.g. via a universal quantum computer—and *emulation*, where physical measurements yield the physical quantities, e.g. spatial probabilities of a quantum walk. In recent years both approaches have been explored, for example the first quantum simulation was of the smallest quantum chemistry problem: obtaining the energies of H_2, the hydrogen molecule, in a minimal basis[2].

Here we report on our efforts using quantum emulation to explore systems in condensed matter physics[3], biology, and complexity theory. Engineered photonic systems, with their precise controllability, provide a versatile platform for creating and probing a wide variety of quantum phenomena.

One of the most striking features of quantum mechanics is the appearance of phases of matter with topological origins. First recognised in the integer and fractional quantum Hall effects in the 1980s, topological phases have been identified in physical systems ranging from condensed-matter[4] and high-energy physics[5] to quantum optics[6] and atomic physics[7]. Topological phases are parametrised by integer topological invariants: as integers cannot change continuously, a consequence is exotic phenomena at the interface between systems with different values of topological invariants. For example, a topological insulator supports conducting states at the surface, precisely because its bulk topology is different to that of its surroundings[4]. Creating and studying new topological phases remains a difficult task in a solid-state setting because the properties of electronic systems are often hard to control.

We use photonic quantum walks to investigate topological phenomena: the photon evolution simulates the dynamics of topological phases which have been predicted to arise in, for example, polyacetylene. We experimentally confirm the long-standing prediction of topologically protected localised states associated with these phases by directly imaging their wavefunctions[3]. Moreover, we reveal an entirely new topological phenomenon: the existence of a topologically protected pair of bound states which is unique to periodically driven systems—demonstrating a powerful new approach for controlling topological properties of quantum systems through periodic driving[3].

In light-harvesting molecules in photosynthesis the energy is localised much faster than can be explained by a naïve tunnelling model: it has instead been suggested that it is in fact due to a partially-decohered quantum walk. Subsequently, coherence in light-harvesting complexes has been measured so many times[8,9] that its existence is now unquestioned in the field. The initial surprise that long-lived quantum coherences occur in biology was in large part a consequence of using old theoretical models from other fields outside of their range of validity—with an appropriate treatment, long-lived coherences are quite natural[10]. But many questions remain open: how robust is the coherence? Does it assist transport? Is it optimised by natural selection? These are difficult to address experimentally because it is very difficult to modify the structure of a biological complex. Here we report our efforts to understand quantum transport by engineering a photonic emulator for biological systems[11], with the goal of being able to easily turn handles to vary the structure, the degree of coherence, or even the environment.

A landmark recent paper shows that even simple quantum computers—built entirely from linear photonic elements with nonadaptive measurements—cannot be efficiently simulated by classical computers[12]. Such devices are able to solve sampling problems and search problems that are classically intractable under plausible assumptions; alternatively if such devices can be efficiently simulated there are far-reaching consequences for the field of complexity theory. Given recent advances in photon sources[13] and detectors[14], we discuss the requirements for experimentally realising such devices.

References

[1] R. P. Feynman, *International Journal of Theoretical Physics* **21**, 467 (1982).

[2] B. P. Lanyon, J. D. Whitfield, G. G. Gillet, et al., *Nature Chemistry* **2**, 106 (2010).

[3] T. Kitagawa, M. A. Broome, et al., *Nature Communications* **3**, 882 (2012).

[4] X. L. Qi and S. C. Zhang, *Reviews of Modern Physics* **83**, 1057–1110 (2011).

[5] R. Jackiw and C. Rebbi, *Physical Review D* **13**, 3398 (1976).

[6] Z. Wang, Y. Chong, J. D. Joannopoulos, and M. Soljačić, *Nature* **461**, 772 (2009).

[7] A. S. Sørensen, E. Demler, and M. D. Lukin, *Physical Revew Letters* **94**, 086803 (2005).

[8] E. Collini, C. Y. Wong, K. E. Wilk, P. M. G. Curmi, P. Brumer and G. D. Scholes, *Nature* **463**, 644, (2010).

[9] E. Harel and G. S. Engel, *Proceedings of the National Academy of Sciences* **109**, 706 (2012).

[10] L. A. Pachón and P. Brumer, *Journal of Physical Chemistry Letters* **2**, 2728 (2011).

[11] J. O. Owens, M. A. Broome, D. N. Biggerstaff, et al., *New Journal of Physics* **13**, 075003 (2011).

[12] S. Aaronson and A. Arkhipov, *STOC'11 Proceedings of the 43rd annual ACM symposium on Theory of computing*, 333–342 (2011). doi:10.1145/1993636.1993682

[13] A. Dousse, et al., *Nature* **466**, 217 (2010).

[14] D. H. Smith, G. G. Gillett, et al. *Nature Communications* **3**, 625 (2012).

Observation of quantum interference as a function of Berry's phase in a complex Hadamard optical network

Anthony Laing, Thomas Lawson, Enrique Martín López, Jeremy L. O'Brien

Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, BS8 1UB, United Kingdom

Emerging models of quantum computation driven by multi-photon quantum interference, while not universal, may offer an exponential advantage over classical computers for certain problems. Implementing these circuits via geometric phase gates could mitigate requirements for error correction to achieve fault tolerance while retaining their relative physical simplicity. We report an experiment in which a geometric phase is embedded in an optical network with no closed-loops, enabling quantum interference between two photons as a function of the phase.

When a quantum mechanical system evolves under some Hamiltonian, the probability amplitudes associated with indistinguishable events can accumulate dynamical and geometric phases [1] and interfere constructively or destructively. In Hong Ou Mandel (HOM) interference [2], when two photons meet at the input ports of a beamsplitter, the event that both photons are transmitted is indistinguishable from the event that both photons are reflected, but the associated probability amplitudes have opposite phases so interfere destructively: the probability to detect one photon at each output port is zero. This quintessentially *quantum* photonic interference generates the non-classical correlations in multi-photon quantum walks [3] and the computational complexity of many-photon interference in large optical networks [4, 5, 6]. These emerging models of quantum computation are unlikely to be universal, but may be exponentially more powerful than classical computers for certain problems. Crucially, since the basic models do not require initial entanglement, conditional gates, or feed-forward operations, large scale examples will be substantially less challenging to physically construct than a universal quantum computer. Achieving fault tolerance in these schemes without sacrificing their relative physical simplicity to unwieldy error correction is a key goal.

Geometric phases and, more generally, non abelian holonomies have been proposed as a method to implement fault-tolerant gates for *universal* quantum computation [7, 8, 9, 10], since they are robust against perturbations to which the important global geometric properties are invariant [11, 12, 13, 14, 15, 16]. In light of the quantum computational attributes of interference between photons and the desire to achieve fault tolerance in physically feasible computational models driven by this effect, demonstrating exquisite control over photonic quantum interference via an intrinsically robust geometric phase gate is a key step. Furthermore, to directly observe the influence of the geometric phase on interference between photons, any measurement statistics should not be obfuscated by other phase dependent phenomena. In particular, single-photon interference, which has been demonstrated to be predictably receptive to the geometric phase, should ideally be independent from the geometric phase.

We establish an experimental functional relationship connecting a variable geometric phase (vGP) to sinusoidal quantum interference between individual photons of a pair. The vGP is imparted inside a four mode optical network that contains no closed loops, such that no single-photon interference can take place. Applied to only one photon of the pair in one of the modes, the vGP arises through a traversal of the polarisation-sphere comprising a closed cycle and an open path. The other three modes traverse lengths on polarisation-sphere equal to that of the vGP mode, but these include a path retracing such that no GP is finally imparted. We observe high visibility quantum interference fringes, and find an approximate flat line response for one-photon inputs, confirming the absence of single-photon interference.

References

[1] M. V. Berry, Proc. R. Soc. Lond. A, **392**, 45, (1983).

[2] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett., **59**, 2044, (1987).

[3] A. Peruzzo, et al., Science, **329**, 1500, (2010).

[4] L. G. Valiant, Theor. Comp. Sci., **8**, 189, (1979).

[5] ,S. Scheel, arXiv:quant-ph/0406127v1(2004).

[6] S. Aaronson and A. Arkhipov, QIP 2010 (2010).

[7] P. Zanardi and M. Rasetti, Phys. Lett. A, **94**, 94, (1999).

[8] J. Pachos, P. Zanardi, and M. Rasetti, Phys. Rev. A, **61**, 010305, (1999).

[9] J. A. Jones, V. Vedral, A. Ekert, and G. Castagnoli, Nature, **403**, 869, (2000).

[10] L.-M. Duan, J. I. Cirac, and P. Zoller, Science, **292**,1695, (2001).

[11] A. Carollo, I. Fuentes-Guridi, M. França Santos, and V. Vedral, Phys. Rev. Lett., **90**, 160402 (2003).

[12] G. De Chiara and G. M. Palma, Phys. Rev. Lett., **91**, 090404 (2003).

[13] A. Carollo, I. Fuentes-Guridi, M. França Santos, and V. Vedral, Phys. Rev. Lett., **92**, 020402, (2004).

[14] P. Solinas, P. Zanardi, and N. Zanghì, Phys. Rev. A, **70**, 042316 (2004).

[15] I. Fuentes-Guridi, F. Girelli, and E. Livine, Phys. Rev. Lett., **94**, 020503, (2005).

[16] S. Filipp, J. Klepp, Y. Hasegawa, C. Plonka-Spehr, U. Schmidt, P. Geltenbort, and H. Rauch, Phys. Rev. Lett., **102**, 030404 (2009).

Are dynamical quantum jumps detector-dependent?

Howard M. Wiseman[1,2] and Jay M. Gambetta[3]

[1]*Centre for Quantum Dynamics, Griffith University, Brisbane QLD 4111, Australia*
[2]*ARC Centre for Quantum Computation and Communication Technology, Griffith University, Brisbane QLD 4111, Australia*
[3]*IBM T. J. Watson Research Center, Yorktown Heights, New York 10598, USA*

Quantum jumps—the discontinuous change in the state of a microscopic system (such as an atom) at random times—were the first form of quantum *dynamics* to be introduced [1]. This was in the 1910s, long before the notion of entanglement, and its puzzles such as the Einstein-Podolsky-Rosen (EPR) paradox [2].Thus they were conceived of as objective dynamical events, linked to objective photon emission events.

The modern concept of quantum jumps in atomic systems is based on "quantum trajectory" theory [3], introduced independently in Refs. [4]. This theory comprises stochastic evolution equations for the microscopic system state conditioned on the results of monitoring the bath to which it is weakly coupled. These are also known as "unravellings" [3] of the system's master equation, as the ensemble average of the quantum trajectories of the (ideally pure) state of an individual system replicates the mixture-inducing evolution of the master equation. In the atomic case, a photodetection event causes the state of the distant atom to jump because of entanglement between the bath (the electromagnetic field) and the atom. That is, the quantum jumps are *detector-dependent*; in the absence of a measurement there would be no jumps.

One could well be tempted to ask what difference does it make if we say a jump is caused by the emission of a photon rather than saying it is caused by the detection of a photon? If photon detection were the only way to measure the emitted quantum field then the answer would indeed be: no real difference at all. But there are many (in fact infinitely many) other ways to measure the emitted field. For instance one can interfere it with a local oscillator (LO)—that is, another optical field in a coherent state—prior to detection [3, 5]. In quantum optical detection theory radically different stochastic dynamics for the atomic state occur depending on the detection scheme used by a distant observer [3, 5]. This is why neither quantum jumps, nor quantum diffusion [6] can be regarded as *objective* (detector independent).

In Ref. [7] we drop the assumption that quantum optical measurement theory is correct in order to ask whether, and how, one could perform *experiments* to try to rule out *all* objective pure-state dynamic models. We propose experimental tests on a strongly driven two-level atom that do not require perfect efficiency, nor any special preparation of the atom or field. The key to these tests is the ability to implement two different ways of monitoring the radiated field, giving rise to two different sorts of stochastic evolution. This is an instance of the EPR phenomenon, called "steering" by Schrödinger [2], when understood sufficiently generally [8]. Specifically, under the assumption that an objective pure state exists (obeying some dynamical model), we derive an *EPR-steering inequality* [9]. We consider two particular unravellings: an adaptive spectrally resolved jump unravelling 'S', and a Y-homodyne unravelling. We then show that an EPR-

steering inequality suitable for these continuous-in-time measurements can be violated for an efficiency $\eta > 0.58$. We also consider the option of using two different homodyne schemes (X and Y). Although the minimum sufficient efficiency is somewhat higher in this case ($\eta > 0.73$), this test would probably be more practical. Finally we derive a *necessary* efficiency condition $\eta > 1/2$ which pertains even if one could implement the whole class of diffusive unravellings.
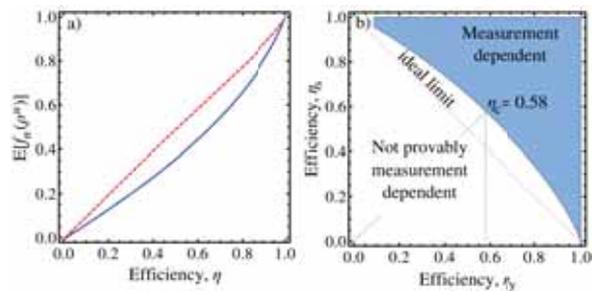

Figure 1: As a function of efficiency η, we plot: (red dashed) $E[(\langle \hat{\sigma}_x \rangle^S)^2]$ for the 'S' unravelling; (solid blue) $E[(\langle \hat{\sigma}_y \rangle^Y)^2 + (\langle \hat{\sigma}_z \rangle^Y)^2]$ for the Y-homodyne unravelling. b) The region (blue) when the experiment is predicted to rule out all theories of objective pure-state dynamical models.

References

[1] N. Bohr, Phil. Mag. **26**, 1 (1913); A. Einstein, Physikalische Zeitschrift **18**, 121 (1917).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935); E. Schrödinger, Proc. Camb. Phil. Soc. **31**, 553 (1935).

[3] H. J. Carmichael, *An Open Systems Approach to Quantum Optics* (Springer, Berlin, 1993).

[4] J. Dalibard, Y. Castin, and K. Mølmer, Phys. Rev. Lett. **68**, 580 (1992); C. W. Gardiner, A. S. Parkins, and P. Zoller, Phys. Rev. A **46**, 4363 (1992); A. Barchielli, Int. J. Theor. Phys. **32**, 2221 (1993).

[5] H. M. Wiseman and G. J. Milburn, *Quantum Measurement and Control* (Cambridge University Press, 2010).

[6] N. Gisin and I. C. Percival, J. Phys. A **25**, 5677 (1992).

[7] H. M. Wiseman and J. M. Gambetta, arXiv:1110.0069

[8] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

[9] E. G. Cavalcanti *et al.*, Phys. Rev. A **80**, 032112 (2009).

Quantum-enhanced magnetometry with photons and atoms.

Federica A. Beduini[1], Naeimeh Behbood[1], Brice Dubost[1], Yannick de Icaza[1], Mario Napolitano[1] Robert J. Sewell[1], Florian Wolfgramm[1], Joanna Zielińska[1] and Morgan W. Mitchell[1,2]

[1]ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain
[2]ICREA-Institució Catalana de Recerca i Estudis Avançats, 08015 Barcelona, Spain

We describe experiments to enhance the sensitivity of magnetic field measurements using optically-detected atomic spin precession (optical magnetometry). This technique is of practical interest because it offers the highest reported sensitivities for measurements of low-frequency fields, and also low-power, small footprint operation with chip-scale devices. State-of-the-art magnetometers are approaching their quantum noise limits, suggesting an important role for quantum enhancement in the near future. The quantum physics of optical magnetometers offers several new features relative to optical interferometers: a hybrid atom-photon system, spin (not canonical) variables, and a significant role for atom-atom or photon-photon interactions during measurement [1].

Squeezed-light magnetometry. We recently demonstrated the first use of photonic entanglement in magnetometry, by using polarization-squeezed light to probe a rubidium vapor cell optical magnetometer [2]. This first demonstration achieved 3.2 dB of sensitivity enhancement in a measurement based on alignment-to-orientation conversion.

Squeezed-atom magnetometry. Squeezing by quantum non-demolition (QND) measurement, a proven technique for "clock" transitions, has not been successful with magnetically-sensitive ensembles due to the more complex spin structure, which couples spin alignment degrees of freedom to the spin orientation. We overcome this limitation in a cold, optically-trapped ^{87}Rb atomic ensemble [3], probed with a projection-noise-limited Faraday rotation measurement [4]. A two-pulse probing method allows us to dynamically decouple the spin orientation from the alignment degrees of freedom [5], finally allowing spin squeezing by quantum non-demolition measurement [6]. As shown in Fig. 1, this succeeds in generating spin squeezing in the ensemble. Also shown, we have recently demonstrated magnetic field measurement beyond the standard quantum limit using these spin-squeezed states.

Exotic entangled states for magnetometry. We are studying macroscopic singlet states, collective spin states with zero net spin, as detectors of inhomogeneity, e.g. in gradient magnetometry. These exotic states can be produced by quantum feedback control [7], and in principle achieve the Heisenberg limit of sensitivity while operating in a decoherence-free subspace intrinsically immune to uniform background fields [8]. We have also shown quantum-enhanced magnetometry with "NooN" states prepared by ultra-bright cavity-enhanced down-conversion [9] and atom-based filtering [10, 11, 12]. This demonstrates quantum enhancement in an interferometer subject to a variety of real-world imperfections, including state-dependent and parameter-dependent losses.
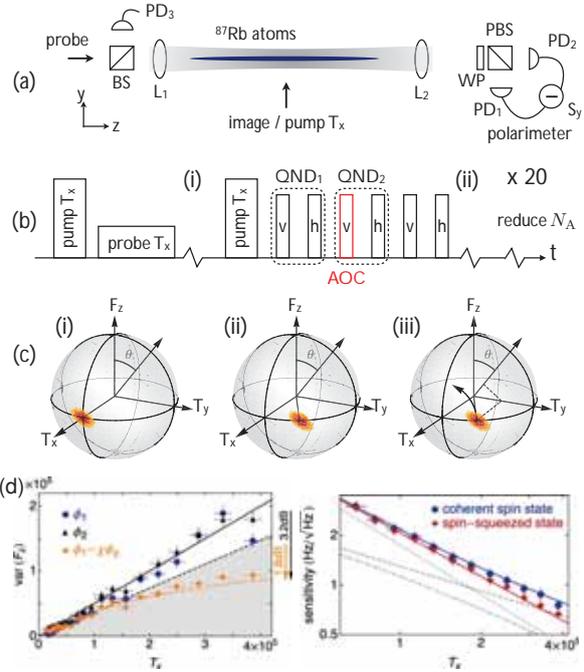

Figure 1: Spin squeezing and quantum-enhanced magnetometry by alignment-to-orientation conversion (AOC). (a) experimental geometry (b) experimental sequence (c) Alignment (T_x, T_y) and orientation (F_z) phase-space picture. (i) measurement-induced squeezing (ii) magnetic precession (iii) AOC readout. (d) spin squeezing results quantified by conditional variance (left) and Zeeman shift measurement (right), showing noise (orange|red) reduced below the standard quantum limit (blue, black). Curves show theoretical predictions.

References

[1] Napolitano, *et al. Nature*, **471** 486 (2011).

[2] Wolfgramm, *et al. Phys. Rev. Lett.*, **105** 053601 (2010).

[3] Kubasik, *et al. Phys. Rev. A*, **79** 043815, (2009).

[4] Koschorreck, *et al. Phys. Rev. Lett.*, **104**, (2010).

[5] Koschorreck, *et al. Phys. Rev. Lett.*, **105** (2010).

[6] Sewell, *et al.* arXiv:1111.6969 (2011).

[7] Tóth and Mitchell, *New J. Phys.*, **12** 053007 (2010).

[8] Urizar-Lanz, *et al.* arXiv:1203.3797 (2012).

[9] Wolfgramm, *et al. Opt. Express*, **16** 18145 (2008).

[10] Cerè, *et al. Opt. Lett.*, **34** 1012 (2009).

[11] Wolfgramm, *et al. Phys. Rev. Lett.*, **106** 053602 (2011).

[12] Zielińska, *et al. Opt. Lett.*, **37** 524 (2012).

Slow photons interacting strongly via Rydberg atoms

Thibault Peyronel[1], Qi-Yu Liang[1], Ofer Firstenberg[1,2], Alexey Gorshkov[3], Thomas Pohl[4], Mikhail D. Lukin[2], and <u>Vladan Vuletić</u>[1]

[1]*Department of Physics and Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, US*
[2]*Department of Physics, Harvard University, Cambridge, MA 02138, USA*
[3]*Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA 91125, USA*
[4]*Max Planck Institute for the Physics of Complex Systems, Nöthnitzer Str. 38, D-01187 Dresden, Germany*

The realization of strong nonlinear interactions between individual light quanta (photons) is a long-standing goal in optical science and engineering. In conventional optical materials, the nonlinearity at light powers corresponding to single photons is negligibly weak. Here we report a medium that is nonlinear at the level of individual quanta, exhibiting strong absorption of photon pairs while remaining transparent to single photons. The quantum nonlinearity is obtained by coherently coupling slowly propagating photons [1] to strongly interacting atomic Rydberg states [2, 3, 4, 5, 6, 7, 8] in a cold, dense atomic gas, as pioneered by Pritchard *et al.* [9]. Our approach opens the door for quantum-by-quantum control of light fields, including single-photon switching [8], and the realization of strongly correlated many-body states of light [10].

The quantum nonlinearity can be viewed as a photon-photon blockade mechanism that prevents the transmission of any state with a photon number larger than one. The nonlinearity arises from the Rydberg excitation blockade [11] which precludes the simultaneous excitation of two Rydberg atoms that are separated by less than a blockade radius. During the optical excitation under EIT conditions, an incident single photon is converted into a Rydberg polariton inside the medium. However, due to the Rydberg blockade, a second polariton cannot travel within a blockade radius from the first one, and EIT is destroyed. Accordingly, if the second photon approaches the single Rydberg polariton, it will be significantly attenuated, provided that the Rydberg-Rydberg interaction is sufficiently strong on the length scale set by the resonant attenuation length in the medium [8]. Using Rydberg states with principal quantum numbers $46 \leq n \leq 100$, we can realize blockade radii between 3 μm and 13 μm, while for our highest atomic densities, the attenuation length is below 2μm. The optical medium then acts as a quantum nonlinear absorption filter, converting incident laser light into a non-classical train of single-photon pulses.

References

[1] M. Fleischhauer, A. Imamoglu, and J. P. Marangos, "Electromagnetically induced transparency: Optics in coherent media," Rev. Mod. Phys. **77**, 633–673 (2005).

[2] D. Tong, S. M. Farooqi, J. Stanojevic, S. Krishnan, Y. P. Zhang, R. Côté, E. E. Eyler, and P. L. Gould, "Local Blockade of Rydberg Excitation in an Ultracold Gas," Phys. Rev. Lett. **93**, 063 001 (2004).

[3] K. Singer, M. Reetz-Lamour, T. Amthor, L. G. Marcassa, and M. Weidemüller, "Suppression of Excitation and Spectral Broadening Induced by Interactions in a Cold Gas of Rydberg Atoms," Phys. Rev. Lett. **93**, 163 001 (2004).

[4] R. Heidemann, U. Raitzsch, V. Bendkowsky, B. Butscher, R. Löw, and T. Pfau, "Rydberg Excitation of Bose-Einstein Condensates," Phys. Rev. Lett. **100**, 033 601 (2008).

[5] T. A. Johnson, E. Urban, T. Henage, L. Isenhower, D. D. Yavuz, T. G. Walker, and M. Saffman, "Rabi Oscillations between Ground and Rydberg States with Dipole-Dipole Atomic Interactions," Phys. Rev. Lett. **100**, 113 003 (2008).

[6] E. Urban, T. A. Johnson, T. Henage, L. Isenhower, D. D. Yavuz, T. G. Walker, and M. Saffman, "Observation of Rydberg blockade between two atoms," Nat. Phys. **5**, 110–114 (2009).

[7] A. Gaetan, Y. Miroshnychenko, T. Wilk, A. Chotia, M. Viteau, D. Comparat, P. Pillet, A. Browaeys, and P. Grangier, "Observation of collective excitation of two individual atoms in the Rydberg blockade regime," Nat. Phys. **5**, 115–118 (2009).

[8] A. V. Gorshkov, J. Otterbach, M. Fleischhauer, T. Pohl, and M. D. Lukin, "Photon-Photon Interactions via Rydberg Blockade," Phys. Rev. Lett. **107**, 133 602 (2011).

[9] J. D. Pritchard, D. Maxwell, A. Gauguet, K. J. Weatherill, M. P. A. Jones, and C. S. Adams, "Cooperative Atom-Light Interaction in a Blockaded Rydberg Ensemble," Phys. Rev. Lett. **105**, 193 603 (2010).

[10] D. E. Chang, V. Gritsev, G. Morigi, M. D. Vuletic, V.and Lukin, and E. A. Demler, "Crystallization of strongly interacting photons in a nonlinear optical fibre," Nat. Phys. **4**, 884–889 (2008).

[11] M. D. Lukin, M. Fleischhauer, R. Coté, L. M. Duan, D. Jaksch, J. I. Cirac, and P. Zoller, "Dipole blockade and quantum information processing in mesoscopic atomic ensembles," Phys. Rev. Lett. **87**, 037 901 (2001).

Superradiant Raman Laser with < 1 Intracavity Photon

Justin G. Bohnet[1], **Zilong Chen**[1], **Joshua M. Weiner**[1], **Dominic Meiser**[1,2], **Murray J. Holland**[1] and **James K. Thompson**[1]

[1]*JILA, University of Colorado and NIST, Boulder, Colorado 80309, USA*
[2]*Present address: Tech-X Corp., 5621 Arapahoe Ave. Ste. A, Boulder, Colorado 80303, USA*

We present a realization of a cold-atom Raman laser operating deep in the bad-cavity, or superradiant regime, where the effective excited state decay linewidth is much narrower than the cavity linewidth [1]. Lasers in the optical regime typically operate in the good-cavity limit, storing coherence mainly in the light field (Fig 1a). In contrast, a superradiant laser stores its coherence primarily in the collective atomic dipole while the photon field provides a means to couple useful phase information out of the system (Fig. 1b).
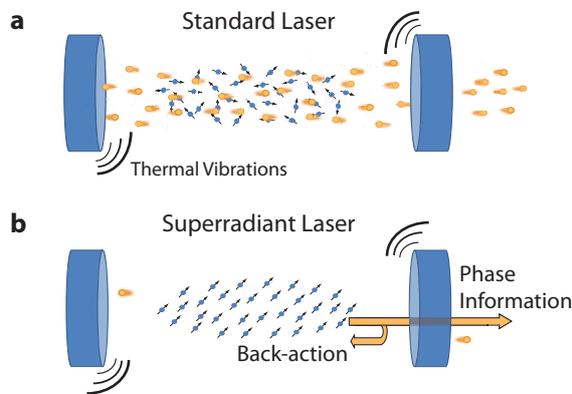
Figure 1: **a:** A good-cavity laser operating far above threshold. Many photons (yellow) circulate inside the cavity, extracting energy from the largely incoherent atomic gain medium (blue). Thermal vibrations of the cavity mirrors modulate the cavity resonance frequency, limiting the stability of the laser. **b:** In a superradiant laser, the collective atomic dipole stores the coherence, and continuous stimulated emission can be achieved even with less than one photon in the cavity. The stimulation enables phase information to be extracted at a useful rate, while the small intracavity photon number leads to only weak cavity-induced backaction on the collective atomic dipole.

We demonstrate quasi-steady state lasing sustained with as low as 0.2 intracavity photons on average. Operating at low intracavity photon number isolates the collective atomic dipole from the environment, resulting in a measured suppression of cavity-pulling by $> 10^4$. Such a high degree of isolation may help overcome thermal fluctuations of the cavity mirrors that currently limit the stability of state-of-the-art lasers. The emitted light has a measured linewidth relative to the Raman dressing laser $> 10^4$ below the Schawlow-Townes linewidth usually applied to good-cavity lasers. The measured linewidth is also below single particle linewidths associated with the decay of the excited state, repumping induced broadening of the ground state, and dephasing between the excited and ground states. Our system confirms key predictions [2] that may enable the creation of superradiant lasers operating on highly forbidden atomic transitions that would have coherence lengths on the order of the earth-sun distance. Such a highly phase coherent light source might improve optical atomic clocks by orders of magnitudes, and would enable more stringent tests of fundamental physics.

References

[1] J. G. Bohnet, Z. Chen, J. M. Weiner, D. Meiser, M. J. Holland, and J. K. Thompson, Nature, **484**, 78 (2012).

[2] D. Meiser, J. Ye, D. R. Carlson, and M. J. Holland, Phys. Rev. Lett., **102**, 163601 (2009).

Observation of strong coupling of single atoms to a whispering-gallery-mode bottle microresonator

Jürgen Volz[1], **Christian Junge**[1], **Danny O'Shea**[1] and **Arno Rauschenbeutel**[1]

[1]*Vienna Center for Quantum Science and Technology, Atominstitut - TU Wien, Stadionallee 2, 1020 Vienna, Austria*

Whispering-gallery-mode (WGM) microresonators provide a powerful system for the investigation of cavity quantum electrodynamics and future quantum information and communication applications [1]. They allow one to combine strong coupling between atoms and the resonator field as well as low optical losses in the same system.

We describe our recent results demonstrating strong coupling between single rubidium atoms and a novel high-Q WGM resonator [2] – a so-called bottle microresonator (Q = 50 million). Light is coupled evanescently into the resonator using two tapered optical fibers with an actively stabilized fiber-resonator gap [3]. Cold rubidium atoms with an average temperature of 5 μK are delivered to the resonator by means of an atomic fountain [4]. We observe clear signals of individual atoms passing through the resonator mode with interaction times on the order of several microseconds. Given this brief interaction time, we have implemented a real-time atom detection/probing scheme based on fast digital FPGA logic. This allows us to react to the arrival of atoms with a response time of less than 150 ns.

With this setup, we investigate the light transmission and reflection characteristics of the coupled atom-resonator system. Our experimental results show a strong interaction between the atom and the resonator mode, which is observed by the large change in light transmission through the coupling fibers.

In addition, the resonator can be operated in a four-port configuration with two coupling fibers, where the atom – depending on its internal state – routes the incoming light between different output ports of the two ultra-thin coupling fibers. We experimentally characterize the routing properties of our system. In a first experiment, we observe classical switching of the light between the two coupling fibers and we investigate the possible pathways towards the realization of an efficient quantum mechanical switch – a four-port device capable of coherently routing photons between two optical nanofibers.
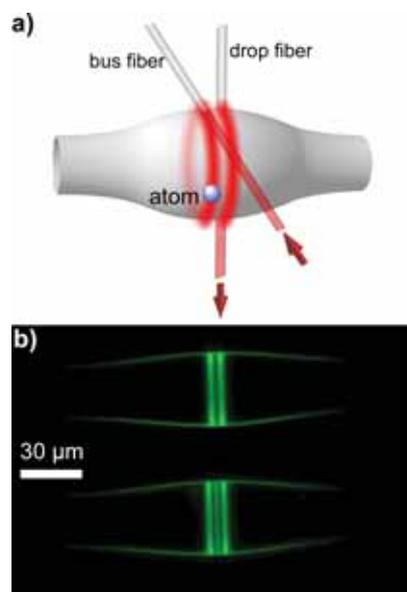
Figure 1: a) Schematic of a bottle microresonator operated in the so-called add-drop configuration. The resonator light field can be efficiently accessed with two tapered coupling fibers. Depending on the atomic state, light propagating on the bus fiber either continues to propagate along the bus fiber or is coupled into the resonator mode and exits the resonator through a second ultrathin fiber, referred to as the drop fiber. b) Experimental micrograph of a bottle mode, visualized via the upconverted green fluorescence of dopant erbium ions in a 36-m diameter bottle microresonator.

References

[1] T. Aoki, B. Dayan, E. Wilcut, W. P. Bowen, A. S. Parkins, T. J. Kippenberg, K. J. Vahala, and H. J. Kimble, Observation of strong coupling between one atom and a monolithic microresonator, Nature **443**, 671 (2006).

[2] Y. Louyer, D. Meschede, and A. Rauschenbeutel, Tunable whispering-gallery-mode resonators for cavity quantum electrodynamics, Phys. Rev. A **72**, 031801(R) (2005).

[3] M. Pöllinger and A. Rauschenbeutel, All-optical signal processing at ultra-low powers in bottle microresonators using the Kerr effect, Opt. Express **18**, 17764 (2010).

[4] D. O'Shea, C. Junge, M. Pöllinger, A. Vogler, and A. Rauschenbeutel, All-optical switching and strong coupling using tunable whispering-gallery-mode microresonators, Appl. Phys. B, **105**, 1, 129 (2011).

Tuesday talks abstracts

Schrdinger's Steering, Mutually Unbiased Bases, and Applications in Photonic Quantum Quantum Information

Anton Zeilinger

University of Vienna and Austrian Academy of Sciences

At least as early as 1931, it was realized by Erwin Schrdinger that entanglement permits nonlocal influences, which he later called "steering". Steering is also central to the Einstein-Podolsky-Rosen Paradox and we suggest that it is at least as fundamental as Bell's Inequalities. It will be argued that for most practical purposes, loophole-free steering, as demonstrated in a recent experiment, is sufficient. The essential point is that steering is a phenomenon within quantum mechanics that, while a local realistic interpretation as required for the Bell argument, would be outside quantum mechanics - a rather unlikely position. The reasoning of steering is also relevant for the question of the number of mutually unbiased bases in a Hilbert space of dimension d where entanglement comes in in a way which increases with dimension such that entanglement becomes the rule rather than exception for high dimension. Other applications include quantum teleportation, entanglement witnesses and a nonlocal quantum eraser experiment. Finally I will comment on blind quantum computation as realized with measurement-based linear optics.

Efficiently heralded sources for loophole-free tests of nonlocality and single-photon vision research

Paul G. Kwiat, Kevin T. McCusker, Rebecca M. Holmes and Bradley Christensen

University of Illinois at Urbana-Champaign, Urbana, Illinois, USA

Spontaneous parametric downconversion (SPDC) is readily used as a source of heralded single photons, and many applications of such a source rely on high heralding efficiency. We report on our progress towards a loophole-free test of nonlocality using efficiently heralded SPDC, and an application of a single-photon source to determine the lower limit of human vision.

SPDC can be used to generate pairs of photons entangled in polarization, suitable for Bell-type tests of nonlocality. All tests of nonlocality to date, including those based on SPDC, have been subject to the timing and/or detection loopholes. While the timing loophole can easily be closed in such a system by moving the detectors sufficiently far apart, closing the detection loophole is more difficult. In the standard experiment using maximally entangled states with the maximal violation of the CHSH inequality [1], an overall efficiency of 83% is required. This limit can be lowered to 67% by using non-maximally entangled states (although sensitivity to noise is greatly increased) [2].

We are engineering our source to achieve maximal heralding efficiency, by carefully optimizing the spatial and spectral filtering. The spatial filtering is done by imaging a portion of the pumped crystal onto single-mode fibers, and the spectral filtering is done by combining multiple tunable interference filters to create a custom, high-efficiency spectral filter. Polarization cross-talk is limited by using high-extinction-ratio polarizing beamsplitters. When these methods are combined with high-efficiency transition-edge sensors [3], closure of the detection loophole is within reach.

We are also developing a single-photon source with high heralding efficiency to investigate the possibility of single-photon vision in humans. Rod cells in the human retina are known to respond to single photons [7, 8], but the minimum number of photons necessary to trigger the entire visual pathway is not known. Previous studies have used attenuated lights, and have estimated the detection threshold to be 1-7 photons with model-fitting methods [9, 10]. Using an efficiently heralded source of single photons (see Figure 1), we can directly determine the threshold for vision.

In our experiment, a human observer seated in a dark room will be presented with one (or N) photons on either the left or right side of his or her retina. For each trial, the observer will make a forced-choice response indicating where he or she thinks the stimulus appeared. We estimate that 6,000 trials presented to about 20 observers will be sufficient to distinguish between single-photon vision and random guessing. Demonstrating single-photon vision would make it possible to test the predictions of quantum mechanics applied to human perception. Eventually we hope to demonstrate quantum nonlocality directly through the visual system by replacing one detector with a human observer in a test of Bell's inequality.
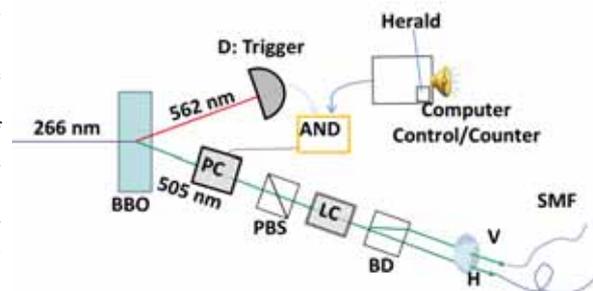

Figure 1: Schematic of a single-photon source for human vision research. Ultraviolet laser photons enter a nonlinear (BBO) crystal, where some split into pairs of lower-energy daughter photons. Detecting one daughter photon heralds the presence of its partner [4, 5, 6]. The trigger detector activates a Pockels cell (PC), allowing N signal photons to pass through. A liquid crystal (LC) sends photons to the left or right side of an observer's retina via single-mode fibers.

References

[1] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, Phys. Rev. Lett. **23,** 880 (1969).

[2] P.H. Eberhard, Phys. Rev. A **47**, R747–R750 (1993).

[3] A. E. Lita, A. J. Miller, and S. Nam, Opt. Exp. **16**, 3032–3040 (2008).

[4] C. K. Hong and L. Mandel, Phys. Rev. Lett. **56**, 58 (1986).

[5] P. G. Kwiat and R. Y. Chiao, Phys. Rev. Lett. **66**, 588 (1991).

[6] E. Jeffrey, N. Peters, and P. G. Kwiat, New J. Phys. **6,** 100 (2004).

[7] F. Rieke and D. A. Baylor, Rev. Mod. Phys. **70**, 1027 (1998).

[8] T. Doan, A. Mendez, P. B. Detwiler, J. Chen, and F. Rieke, Science **313**, 530 (2006).

[9] S. Hecht, S. Shlaer, and M. H. Pirenne, J. Gen. Physiol. **25**, 819 (1942).

[10] B. Sakitt, J. Physiol. 223, 131 (1972).

Entanglement of Very High Orbital Angular Momentum of Photons

Robert Fickler[1,2], **Mario Krenn**[1,2], **Radek Lapkiewicz**[1,2], **Christoph Schaeff**[1,2], **Bill Plick**[1,2], **Sven Ramelow**[1,2] and **Anton Zeilinger**[1,2]

[1]*Institut of Physics, University of Vienna, Vienna, Austria*
[2]*Institute for Quantum Optics and Quantum Information, ÖAW, Vienna, Austria*

Orbital angular momentum (OAM) of single photons represents a relatively novel optical degree of freedom for the entanglement of photons [1],[2]. A physical realization of OAM carrying light beams are the so called Laguerre-Gaussian modes which have the required helical phase structure. One big advantage over the well known polarization degree of freedom is the possibility of realizing entanglement between two photons with very high quantum numbers and momenta respectively. However, the creation of photonic OAM entanglement by the widely used spontaneous parametric down conversion (SPDC) process is limited by the strongly reduced efficiency for higher momenta [3]. We have realized a novel, very flexible method to create entanglement between two photons which is not constrained by the SPDC efficiency nor the conservation law for the OAM degree of freedom. By transferring the polarization entanglement to the orbital angular momentum degree of freedom within an interferometric scheme (Fig. 1), we created and measured the entanglement of asymmetric states where one photon carries $\pm 10\hbar$ and the other $\pm 100\hbar$ of OAM. Furthermore, we realized entanglement of two photons with up to $600\hbar$ difference in their angular momentum (see Fig. 2), which is, to our knowledge, the highest entangled quantum number that has been measured so far. Additionally, we used hybrid entangled biphoton states between polarization and OAM to show the angular resolution enhancement in possible remote sensing applications.

(A) $|-10, +100\rangle + |+10, -100\rangle$

(B) $|-300, 300\rangle + |300, -300\rangle$

Figure 2: Measured coincidence count rates where the signal photon is transferred from polarization to $l = \pm 10$ and the idler photon to $l = \pm 100$ (A) or both to $l = \pm 300$ (B)
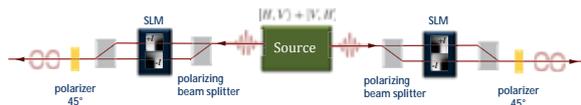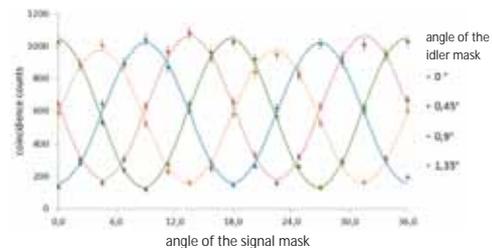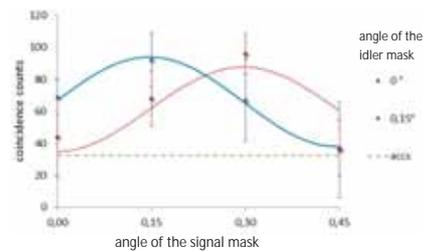

Figure 1: Schematic sketch of the setup to transfer polarization entanglement to orbital angular momentum entanglement. The polarization entanglement is created in a parametric downconversion process (box in the center). Afterwards the two photons are sent to two transfer setups where they are split and transferred by an liquid crystal Spatial Light Modulator (SLM) to higher order Laguerre-Gaussian modes depending on their polarization. After recombining the paths, a polarizer at $45°$ projects the photon to diagonal polarization and therefore completes the transfer.

References

[1] G. Molina-Terriza, J. P. Torres, L Torner, Nature Physics 3, 305 (2007).

[2] A. Mair, A. Vaziri, G. Weihs, A. Zeilinger, Nature 412, 313 (2001).

[3] B. Jack, J. Leach, H. Ritsch, S. M. Barnett, M. J. Padgett, S. Franke-Arnold, NJP 11, 103024 (2009).

Towards scalable quantum information processing with trapped ions

Dietrich Leibfried[1]

[1]*National Institute of Standards and Technology, Boulder, CO, USA*

We discuss experiments towards scalable quantum information processing in the Ion Storage Group at NIST Boulder. Our architecture is based on quantum information stored in internal (hyperfine) states of the ions. We investigate the use of laser beams and microwave fields to induce both single-qubit rotations and multi-qubit gates mediated by the Coulomb interaction between ions. Moving ions through a multi-zone trap architecture allows for keeping the number of ions per zone small, while sympathetic cooling with a second ion species can remove energy and entropy from the system. We will provide an update on experiments towards benchmarking operation fidelities and improved ion transport.

Work is under way to leverage miniaturized surface-electrode trap arrays towards a higher level of integration. We have implemented a universal gate set based on microwave near-field control directly integrated on the trap chip on a magnetic field insensitive qubit [1] and are working on improving the operation fidelities in this approach. The close proximity of the ions to the trap electrodes also warrants a better understanding of "anomalous" heating observed by many groups. Some evidence ties this heating to surface effects, so besides cooling the trap to cryogenic temperatures, cleaning of the electrode surfaces might be beneficial. We will report on the status of our efforts towards better understanding of anomalous heating.

References

[1] C. Ospelkaus, U. Warring, Y. Colombe, K. R. Brown, J. M. Amini, D. Leibfried, and D. J. Wineland, "Microwave quantum logic gates for trapped ions", Nature 476, 181 (2011).

Schrödinger cat state spectroscopy with trapped ions

Cornelius Hempel[1,2], **Petar Jurcevic**[1,2], **Ben Lanyon**[1,2], **Rene Gerritsma**[1,3], **Rainer Blatt**[1,2] **and Christian Roos**[1,2]

[1]*Institute for Quantum Optics and Quantum Information, Innsbruck, Austria*
[2]*Institute for Experimental Physics, University of Innsbruck, Innsbruck, Austria*
[3]*now at: Institute of Physics, University of Mainz, Germany*

Trapped and laser-cooled ions have excellent properties for high-precision spectroscopy. By quantum logic spectroscopy, ions whose internal state cannot be detected easily can be read out via a second ion species trapped together with the spectroscopy ion. In my talk, I will discuss the use of geometric phases for a particular type of quantum logic spectroscopy that can be used to detect the absorption or emission of single photons with high detection efficiency. By preparing a Schrödinger cat state of a two-ion crystal where the ions's motion is entangled with the internal states of the logic ion, a photon scattered by the spectroscopy ion manifests itself by a geometric phase that can be subsequently read out via the logic ion. This measurement scheme is applied to a mixed ion crystal of two calcium isotopes.

Heralded entanglement between widely separated atoms

J. Hofmann[1], **M. Krug**[1], **N. Ortegel**[1], **M. Weber**[1], **Wenjamin Rosenfeld**[1,2], **H. Weinfurter**[1,2]

[1] *Faculty of Physics, Ludwig-Maximilians-Universitaet, D-80799 Munich, Germany*
[2] *Max-Planck-Institute of Quantum Optics, D-85748 Garching, Germany*

Entanglement between remote atomic quantum memories will be a key resource for future applications in quantum communication. However, generation of entanglement over large distances is an experimentally challenging task. One approach is based on entanglement swapping. It starts by entangling each quantum memory with a photon, which can be conveniently transported via optical fibers. A Bell-state measurement on the photons then projects the atomic system onto an entangled state.

Figure 1: Experimental setting: two single atom traps (distance: 20 meters) are connected via optical fibers. Single photons, which are entangled with an atom on each side interfere on a 50-50 beamsplitter and are detected by single photon counting avalanche photodetectors (APDs). Coincident detection of the two photons heralds entanglement between the atoms. The inset shows the scheme for generation of single photons whose polarization is entangled with the atomic spin.

Here we show entanglement between two single Rb-87 atoms separated by a distance of 20 meters. In our experiment two independently operating atomic traps are situated in neighboring laboratories. On each side we capture a single neutral Rb-87 atom in an optical dipole trap. Next, both atoms are prepared in an excited state (see Fig. 1, inset) by short optical pulses. In the following spontaneous decay process each atom emits a single photon whose polarization is entangled with the atomic spin [1]. The emitted photons are collected with high-NA objectives into single-mode optical fibers and guided to a non-polarizing 50-50 fiber beam-splitter where they interfere. To ensure good temporal overlap of the photon wave-functions, the excitation pulses in the two experiments are synchronized with sub-nanosecond precision [2].

After interference the photons are detected by avalanche photodetectors. Certain coincident detection events project the photons onto maximally entangled states thereby entangling the two remote atoms. This scheme is probabilistic but heralded, i.e., one obtains a signal every time the two atoms were successfully entangled.

Conditioned on the heralding signal the spin state of both atoms is read out. By performing correlation measurements in two complementary bases we have proven entanglement of the two atoms which was also high enough to violate Bell's inequality. By increasing the distance to 300 meter and implementing fast atomic state detection [3] this system may enable a future loophole-free test of Bell's inequality.

References

[1] J. Volz et al., Phys. Rev. Lett. **96**, 030404 (2006).

[2] W. Rosenfeld et al., Optics and Spectroscopy **111**, 535 (2011).

[3] F. Henkel et al., Phys. Rev. Lett. **105**, 253001 (2010).

Quantum Speedup by Quantum Annealing

Daniel Nagaj[1], **Rolando Somma**[2] **and Mária Kieferová**[1]

[1]*Research Center for Quantum Information, Slovak Academy of Sciences, Bratislava, Slovakia*
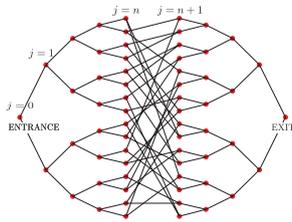[2]*Los Alamos National Laboratory, Los Alamos, NM 87545, USA*

Figure 1: Two binary trees of depth $n = 4$ glued by a random cycle. The number of vertices is $N = 2^{n+2} - 2$. Each vertex is labeled with a randomly chosen $2n$-bit string.
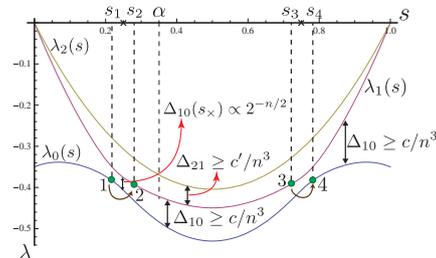

Figure 2: The three lowest eigenvalues of our parametrized Hamiltonian $H(s)$ in the column subspace. We divide the evolution in 5 stages according to $s_1, \ldots, s_4$. Inside $[s_1, s_2]$ and $[s_3, s_4]$, the gap $\Delta_{10}(s)$ becomes exponentially small in n. Brown arrows depict level transitions for an annealing rate in which $\dot{s}(t) \propto 1/\text{poly}(n)$. Other scalings are also shown.

We study the glued-trees problem of Childs, et. al. [1] (see Fig.1) in the adiabatic model of quantum computing and provide an annealing schedule to solve an oracular problem exponentially faster than classically possible. The Hamiltonians involved in the quantum annealing do not suffer from the so-called sign problem. Unlike the typical scenario, our schedule is efficient even though the minimum energy gap of the Hamiltonians is exponentially small in the problem size.

Quantum annealing (QA) is a powerful heuristic to solve problems in optimization [2]. It consists of preparing a low-energy or ground state $|\psi\rangle$ such that, after a simple measurement, the optimal solution is obtained with large probability. $|\psi\rangle$ is prepared by following a particular annealing schedule, with a parametrized Hamiltonian path subject to initial and final conditions. A ground state of the initial Hamiltonian is then transformed to $|\psi\rangle$ by varying the parameter adiabatically. In contrast to more general quantum adiabatic state transformations, the Hamiltonians along the path in quantum annealing are termed *stoquastic* and do not suffer from the so-called *numerical sign problem*: for a specified basis, the off-diagonal Hamiltonian-matrix entries are nonpositive [3]. This property is useful for classical simulations.

A sufficient condition for convergence of the quantum method is given by the quantum adiabatic approximation. It asserts that, if the rate of change of the Hamiltonian scales with the energy gap Δ between their two lowest-energy states, $|\psi\rangle$ can be prepared with controlled accuracy [**?**]. It turns out that the *relevant* energy gap for the adiabatic approximation in these cases is not Δ and can be much bigger.

Because of the properties of the Hamiltonians, the annealing can also be simulated using probabilistic classical methods such as quantum Monte-Carlo (QMC). We know that if the Hamiltonians satisfy an additional frustration-free property, efficient QMC simulations for QA exist [4]. This places a doubt on whether a quantum-computer simulation of general QA processes can ever be done using substantially less resources than QMC or any other classical simulation. Towards answering this question, we provide an oracular prob-

lem and give a QA schedule that, on a quantum computer, prepares a quantum state $|\psi\rangle$ encoding the solution. The time required to prepare $|\psi\rangle$ is polynomial in the problem size. The oracular problem was first introduced in Ref. [1] in the context of quantum walks, where it was also shown that no classical method can give the solution using $\text{poly}(n)$ number of oracle calls. Our result thus places limits on the power of classical methods that simulate quantum annealing, even when the sign-problem is not present.

The annealing schedule we provide is not intended to follow the ground state in the path; transitions to the closest (first-excited) eigenstate are allowed. Nevertheless, the system (almost) remains in the subspace spanned by these two states at all times. There are regions in the path where $\Delta \propto \exp(-n)$. We induce transitions in that subspace by choosing an annealing rate that is much larger than Δ, i.e. at $1/\text{poly}(n)$ rates. However, such transitions are useful here. They guarantee that $|\psi\rangle$ is prepared after the annealing due to a symmetry argument: The same type of transition that transforms the ground to the first-excited state, later transforms the first-excited state back to the final ground state $|\psi\rangle$.

References

[1] A.M. Childs et al., *Proc. 35th STOC*, 59–68 (2003).

[2] E. Farhi et al., Science **292**, 472–476 (2001). A. Das et al., *Quantum Annealing and Related Optimization Methods*, Springer (2005).

[3] S. Bravyi, D.P. DiVicenzo, R. Oliveira, B.M. Terhal, Quantum Inf. Comp. **8**, 0361 (2008).

[4] R.D. Somma, C.D. Batista, and G. Ortiz, Phys. Rev. Lett. **99**, 030603 (2007), S. Bravyi and B. Terhal, SIAM J. Comp. **39**, 1462 (2009).

Control in the Sciences over Vast Length and Time Scales

Rabitz, H.

Princeton University, Princeton, New Jersey, USA

The control of physical, chemical, and biological phenomena are pervasive in the sciences. The dynamics involved span vast length and time scales with the associated controls ranging from shaped laser pulses out to the application of special chemical reagents and processing conditions. Despite all of these differences, there is clear common behavior found upon seeking optimal control in these various domains. Evidence of this common behavior will be presented from the control of quantum, chemical, and biological processes. The most evident finding is that control efforts can easily beat the so-called "curse of dimensionality" upon satisfaction of assumptions that are expected to widely hold. Quantum phenomena provide a setting to quantitatively test the control principles. The potential consequences of the observations will be discussed.

Control of correlated many-body quantum dynamics

Simone Montangero[1]

[1] *University of Ulm, Ulm, Germany*

Quantum optimal control has been used for decades to perform desired transformations in few-body quantum systems, as for example in Nuclear Magnetic Resonance experiments. However, the exponential increase of the Hilbert space size with the number of the system components and the correspondent complexity of the optimization task prevents the application of standard optimal control techniques to the complex dynamics of many-body quantum systems. We present the CRAB optimal control technique recently introduced to merge state-of-the-art many-body quantum system simulations tools with optimal control: we show that it is possible to perform open- and closed-loop optimal control of complex quantum dynamics in open and closed systems. We introduce the concept of complexity of the optimization task and we present different theoretical and experimental applications of optimal control to correlated quantum systems dynamics as the optimal crossing of a quantum phase transition and the production of stable and robust-against-noise entangled states.

Quantum microrheology

M. A. Taylor[1], **J. Janousek**[2], **V. Daria**[2], **J. Knittel**[1], **B. Hage**[2], **H.-A. Bachor**[2], and <u>**W. P. Bowen**</u>[1]

[1]*Centre for Engineered Quantum Systems, University of Queensland, Queensland, Australia*
[2]*Department of Quantum Sciences, Australian National University, A.C.T., Australia*

The quantum nature of light places a fundamental limit on the sensitivity of optical measurements. In circumstances with constrained optical power, this limit may only be surpassed using non-classical resources. Despite the promise of non-classical resources, to date the sole example of a real application is in interferometric gravity wave detection where the optical power is constrained due to absorptive heating[1]. A much broader and widely discussed application area is biological sensing[2], where low light levels are often required to avoid damaging the specimen. Here we report, to our knowledge, the first experimental demonstration of quantum enhanced sensitivity in this context. By injecting appropriately spatially engineered squeezed light into an optical tweezer, the motion of naturally occurring lipid granules in a live yeast cell were tracked in real time with sensitivity surpassing the quantum noise limit by 42%. The granules reside within the polymer network of the cells cytoplasm, allowing dynamical quantum microrheology experiments to be performed. These experiments reveal subdiffusive motion, providing characteristic information about the cytoplasms viscoelastic properties in agreement with recent observations using classical light[3]. The approach demonstrated here provides a pathway towards microrheology of cell mechanics and the cytoskeleton at high frequencies, where motion amplitudes are beneath the sensitivity of current technology.

To our knowledge only one biological imaging experiment has previously been performed using non-classical light[4]. In that work, onion-skin tissue was imaged using optical coherence tomography with non-classically correlated photon pairs reflected from embedded gold nanoparticles. However, quantum enhanced sensitivity was not demonstrated, and, due to the low photon flux, measurements of biological dynamics were precluded.

Our experimental apparatus is shown in Fig. 1. The specimen was suspended in water within a sample chamber formed by two microscope coverslips, and trapped with a dual beam optical trap at 1064 nm. An orthogonally polarized "probe" field was spatially engineered using a phase plate for maximum sensitivity to motion of the specimen (see panels on the right of Fig. 1) and injected into the optical tweezers. A further "signal" laser field, coherent with the squeezed probe field, was injected transversely to the optical axis of the tweezers. Scattering of this field interfered with the squeezed field, encoding position information about the specimen which could be retrieved via direct detection. Apart from the deleterious effects of optical losses and spatial distortion in the objectives and specimen, a major technical challenge was to minimize exposure to noise sources at the sub kHz frequencies relevant to biological motion. This was achieved by stroboscopically pulsing the signal field at 3.522 MHz, which had the effect of mixing up the motion into the region of strongest squeezing. This technique should
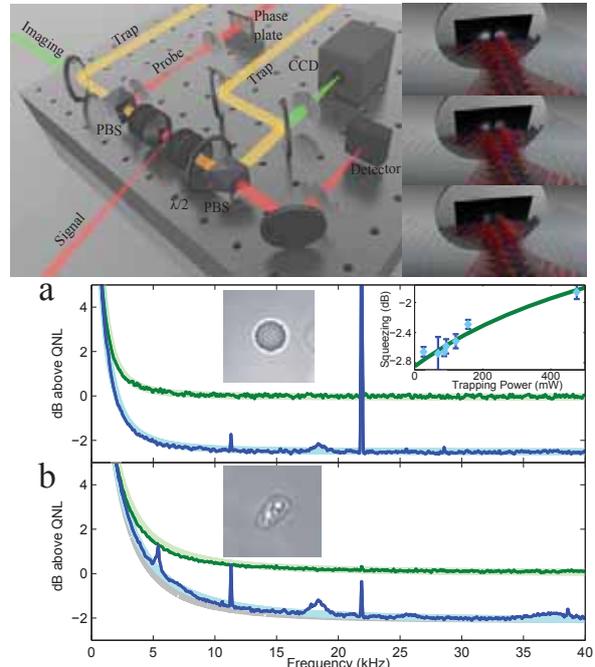

Figure 1: *Top Left*: experimental schematic. *Top Right*: Probe (red) and scattered (blue) fields, showing dependence of detected intensity on particle position. *Bottom*: Motional noise spectra relative to quantum noise limit for shot noise limited (green) and squeezed (blue) probe. In a) and b) the specimen are, respectively, a silica bead and a yeast cell.

be broadly applicable to squeezed light enhanced sensors.

Motion sensitivity surpassing the quantum limit by up to 2.7 dB and 2.4 dB was achieved, respectively, for trapped silica beads and lipid granules within a yeast cell; with typical experimental results shown in Fig. 2. At low frequencies the motion of the specimen can be observed. The bead motion is consistent with diffusive Brownian motion. As can be seen, the lipid granule motion drops away with frequency more slowly, with a frequency dependence of $\omega^{-1.73\pm0.04}$ consistent with recent classical measurements[3].

References

[1] H. Vahlbruch *et al.* Class. Quantum Grav. **27** 084027 (2010)

[2] N. Treps *et al.* Phys. Rev. Lett. **88**, 203601 (2002)

[3] I. M. Tolić-Nørrelykke *et al.* Phys. Rev. Lett. **93**, 078102 (2004)

[4] M. B. Nasr *et al.* Opt. Commun. **282** 1154 – 1159 (2009)

Fast quantum tomography via continuous measurement and control

Carlos A. Riofrío[1,3] , Robert Cook[1,3] , Aaron C. Smith[2,3], Brian E. Anderson[2,3], Poul S. Jessen[2,3], and <u>Ivan H. Deutsch</u>[1,3]

[1]*University of New Mexico, United States*
[2]*University of Arizona, United States*
[3]*Center for Quantum Information and Control (CQuIC), United States*

Quantum tomography is traditionally a time consuming and demanding process requiring a large number of measurements on many identically prepared copies, N, of the state. In situations where one has simultaneous access to the entire ensemble and the ability to perform a collective measurement, one can extract the required information much more efficiently. Moreover, if the measurement is performed weakly and continuously, one can obtain an informationally complete signal if the system is controlled in a well chosen way. The combination of control and continuous measurement provides a protocol to perform fast quantum tomography.

We study the implementation of this protocol in a spin-ensemble of cesium atoms prepared in an arbitrary superposition of hyperfine ground state magnetic sublevels, a 16 dimensional Hilbert space [1]. Continuous measurement is performed by polarimetry, whereby an off-resonant laser beam probes the collective magnetization through the Faraday effect. An informationally complete measurement record is obtained when the system is driven with appropriately modulated rf and microwave fields while probed by the laser field. The Faraday rotation signal registers the expectation values of the entire Lie algebra su(16), required to estimate an arbitrary state.

We model the dynamics through a detailed Linblad CP-map that evolves the measured observables, including the effects of decoherence and inhomogeneities in the Hamiltonian parameters across the ensemble. When the shot-noise of the probe is very large compared to the projection noise in the collective spin, quantum backaction is negligible, and the noisy measurement record occurs according to the probability distribution

$$P\left(\{M_i\}|\rho_0\right) \propto \prod_i e^{-\frac{\{M_i - N\mathrm{Tr}(\hat{f}_z(t_i)\rho_0)\}^2}{2\sigma^2}}, \qquad (1)$$

where M_i is the measurement at time t_i, $\hat{f}_z(t_i)$ is the Heisenberg-picture observable at time t_i, σ^2 is the shot-noise variance, and ρ_0 is the initial state to be estimated. An example of the experimentally measured and simulated signals for a known prepared pure state is shown in Fig 1.

We employ two compressed sensing algorithms to estimate the quantum states. In the first we use a maximum likelihood estimate, constrained by the fact that $\rho_0 \geq 0$. In the second we use the tools of matrix completion to search for a low rank (highly pure) state consistent with the measurement record [2]. Both methods perform well for pure states, yielding high fidelity estimates well before the signal is informationally complete for an arbitrary state. The matrix completion estimator is more robust to technical noise and imperfections in the measurement record. The constrained maximum likelihood performs better for more mixed states.

The fundamental limits of our protocol are set by the finite number of copies in the ensemble. In the absence of decoherence, measurement-induced backaction ultimately becomes important in the continuous-time measurement record. We study this limit for the simplest problem – estimating the state of a qubit given N identical copies. Using the same Faraday polarimetry probe discussed above, we generate an informationally complete measurement record through time-dependent Larmor precession of the spins. We estimate the state using a "projection filter" that seeks the initial condition the matches the measurement record under the assumption that the system remains always in a product state of identical copies. This is an excellent approximation due to the dynamical decoupling induced by the rapid control. In the absence of the Larmor control, the backaction of the QND measurement induces strong correlations between the spins, as associated with collective spin squeezing. The rapid rotations wash out the squeezing, on average. We find that this protocol does not reach the bound of $(N+1)/(N+2)$ associated with the optimal POVM on the collective state [3], with the deficit arises from the control policy and the approximation of the project filter.
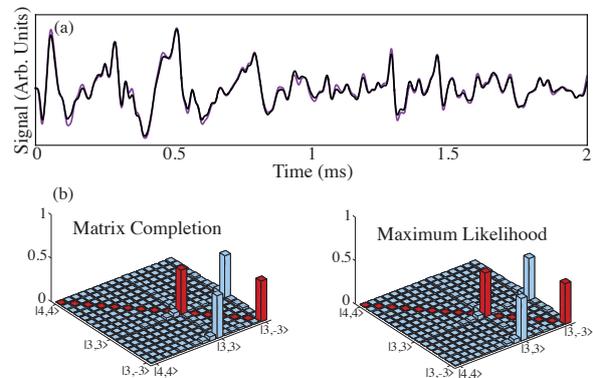
Figure 1: Example tomography of the state $|3,3\rangle + |3,-3\rangle$. (a) measurement record: experimental (red) model (black). (b,c) reconstructed states from estimation algorithms

References

[1] C. A. Riofrío, P. S. Jessen and I. H. Deutsch, J. Opt. B, **44**, 154007 (2011).

[2] D. Gross *et al.*, Phys. Rev. Lett. **105**, 150401 (2010).

[3] S. Massar, S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).

Reliable Quantum State Tomography

Matthias Christandl[1] **and** <u>**Renato Renner**</u>[1]

[1] *Institute for Theoretical Physics, ETH Zurich, Switzerland*

Quantum state tomography is the task of estimating the state of a quantum system using measurements. Typically, one is interested in the (unknown) state, in the following denoted σ, generated during an experiment which can be repeated arbitrarily often in principle. However, the number, n, of actual runs of the experiment, from which data is collected, is always finite (and often small). As pointed out recently (see, e.g., [1, 2, 5]), this may lead to unjustified (or even wrong) claims when employing standard statistical tools without care. Here we propose a method for obtaining *reliable* estimates from finite tomographic data. Specifically, the method allows the derivation of *confidence regions*, i.e., subsets of the state space in which the unknown state σ is contained with probability almost one.

In this abstract, we briefly describe our approach, making some simplifying assumptions for convenience. We refer to the full paper [5] for the general case as well as for a further more detailed discussion. The proof of the main theorem is based on techniques introduced in [6, 3].
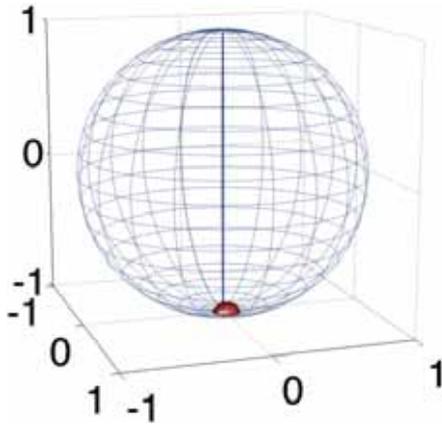
Figure 1: Example of a confidence region $\Gamma_{\mathbf{x}}^{\delta}$ (red set) obtained by tomography on a two-dimensional quantum system (shown in the Bloch sphere representation). The shape and size of the confidence region depends on the type and number of measurements applied to the system.

Scenario and notation: Consider an experiment that is repeated n times. Assume that, in each run, the system evolves to the same unknown state, specified by an element σ of the set $\mathcal{S}(\mathcal{H})$ of density operators on a Hilbert space $\mathcal{H}$. Subsequently, a measurement specified by a POVM $\{B_x\}_x$ (on $\mathcal{H}$) is applied. The measurement outcomes of the n runs are denoted by $x_1, \ldots, x_n$, respectively.

In the next paragraph, we describe a general criterion for constructing confidence regions, $\Gamma_{\mathbf{x}}^{\delta} \subseteq \mathcal{S}(\mathcal{H})$, depending on the experimental data $\mathbf{x} = (x_1, \ldots, x_n)$ (c.f. Fig. 1). We then state a theorem, which asserts that $\sigma \in \Gamma_{\mathbf{x}}^{\delta}$ holds with probability almost one, therefore justifying the construction.

Deducing confidence regions: For any possible sequence of measurement outcomes $\mathbf{x}$, let $\mu_{\mathbf{x}}$ be the probability distribution on the state space $\mathcal{S}(\mathcal{H})$ defined by

$$\mu_{\mathbf{x}}(\bar{\sigma})d\bar{\sigma} = \mathcal{N} \prod_{i=1}^{n} \text{tr}[\bar{\sigma} B_{x_i}]d\bar{\sigma} , \qquad (1)$$

where $\mathcal{N}$ is a normalization constant and $d\bar{\sigma}$ denotes the Hilbert Schmidt measure. Furthermore, for some fixed $\varepsilon > 0$ and for any $\mathbf{x}$, let $\Gamma_{\mathbf{x}}$ be a subset of $\mathcal{S}(\mathcal{H})$ with weight

$$\int_{\Gamma_{\mathbf{x}}} \mu_{\mathbf{x}}(\bar{\sigma})d\bar{\sigma} \geq 1 - \frac{\varepsilon}{2c_n} , \qquad (2)$$

where $c_n = \binom{2n+d^2-1}{d^2-1}$, with d the dimension of $\mathcal{H}$. Finally, we define $\Gamma_{\mathbf{x}}^{\delta}$ as the set of all $\bar{\sigma} \in \mathcal{S}(\mathcal{H})$ whose distance (measured in terms of the *purified distance* [7]) to a density operator in $\Gamma_{\mathbf{x}}$ is at most $\delta = (\frac{2}{n} \ln \frac{2}{\varepsilon} + \frac{4}{n} \ln c_n)^{\frac{1}{2}}$.

Theorem [5]. *For any $\sigma \in \mathcal{S}(\mathcal{H})$*

$$\text{Prob}_{\mathbf{x}}[\sigma \in \Gamma_{\mathbf{x}}^{\delta}] \geq 1 - \varepsilon \qquad (3)$$

where the probability is taken over all possible measurement outcomes $\mathbf{x}$, distributed according to $p_{\mathbf{x}} = \prod_{i=1}^{n} \text{tr}[\sigma B_{x_i}]$.

The theorem guarantees that, whatever the "true" state σ is, the confidence region $\Gamma_{\mathbf{x}}^{\delta}$ will contain this state almost certainly. Note that, crucially, the criteria for specifying the confidence region (c.f. Eq. 2) only depends on the measurement data $\mathbf{x}$, but not on the (initially unknown) state σ.

Generalizations: The above claim can be shown to hold within a more general setup than the one described here (see [5]). In particular, using the quantum de Finetti's theorem [4], the assumption that an identical state σ is generated in each run of the experiment can be relaxed to the assumption that the actual runs of the experiment are chosen at random from an (in principle) infinitely long sequence of runs. Furthermore, nothing needs to be assumed about the nature of the measurements. In particular, they may depend on each other and can have an unbounded number of possible outcomes.

References

[1] R. Blume-Kohout, New J. Phys., **12**, 043034 (2010).

[2] R. Blume-Kohout, arXiv:1202.5270 (2012).

[3] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett., **102**, 020504 (2009).

[4] M. Christandl, R. König, G. Mitchison, and R. Renner, Comm. Math. Phys., **273**, 473 (2007).

[5] M. Christandl and R. Renner, arXiv:1108.5329 (2011).

[6] M. Hayashi, Comm. Math. Phys., **293**, 171 (2010).

[7] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theor., **56**, 4674 (2010).

Room Temperature Quantum Bit Memory Exceeding One Second

Peter Maurer[1], **Georg Kucsko**[1], **Christian Latta**[1], **Liang Jiang**[2], **Norm Yao**[1], **Steven Bennett**[1], **Fernando Pastawski**[3], **David Hunger**[3], **Nick Chisholm**[1], **Matthew Markham**[4], **Daniel Twitchen**[4], **Ignacio Cirac**[3], **Mikhail Lukin**[1]

[1]*Harvard University, Cambridge, United States*
[2]*Yale University, New Haven, United States*
[3]*Max-Planck-Institut für Quantenoptik, Garching, Germany*
[4]*Element Six Ltd, Ascot SL5 8BP, United Kingdom*

Many applications in quantum communication and quantum computation rely upon the ability to maintain qubit coherence for extended periods of time. Furthermore, integrating such quantum mechanical systems in compact, mobile devices remains an outstanding experimental task. While trapped ions and atoms can exhibit coherence times as long as minutes, they typically require a complex infrastructure involving laser-cooling and ultra-high vacuum. Other systems, most notably ensembles of electronic and nuclear spins, have also achieved long coherence times in bulk ESR and NMR experiments; however, owing to their exceptional isolation, individual preparation, addressing and high fidelity measurement remains challenging.

We demonstrate high-fidelity control of a solid-state qubit, which preserves its polarization for several minutes and features coherence lifetimes exceeding 1 second at room temperature. Our approach is based upon an individual nuclear spin in a room-temperature solid. We work with an isotopically pure diamond sample consisting of 99.99% spinless ^{12}C isotope. The qubit consists of a single ^{13}C ($I = 1/2$) nuclear spin in the vicinity of a nitrogen-vacancy color center, which is used to initialize the nuclear spin [1] in a well defined state and to read it out in a single shot using quantum non-demolition measurement [2, 3]. The long qubit memory time was achieved via a technique involving dissipative decoupling of the single nuclear spin from its local environment. A combination of laser illumination and RF decoupling pulse sequences [4, 5] enables the extension of our qubit memory lifetime by nearly three orders of magnitude. This approach decouples the nuclear qubit from both the nearby electronic spin and other nuclear spins, demonstrating that dissipative decoupling can be a robust and effective tool for protecting coherence.

As a future application of our techniques the realization of fraud resistant quantum tokens can be considered. Here, secure bits of information are encoded into long-lived quantum memories. Along with a classical serial number, an array of such memories, may possible constitutes a unique unforgeable token [6, 7]. With a further enhancement of storage times, such tokens may potentially be used as quantum-protected credit cards or as quantum identification cards [7] with absolute security. Furthermore, NV-based quantum registers can take advantage of the nuclear spin for storage, while utilizing the electronic spin for quantum gates and readout. In particular, recent progress in the deterministic creation of arrays of NV centers enables the exploration of robust quantum state transfer [8] and scalable architectures for room temperature quantum computers [9].

References

[1] M. V. G. Dutt, L. Childress, L. Jiang, E. Togan, J. Maze, F. Jelezko, A. S. Zibrov, P. R. Hemmer and M. D. Lukin, Science **316**, 1312-1316 (2007).

[2] L. Jiang, J. S. Hodges, J. R. Maze, P. Maurer, J. M. Taylor, D. G. Cory, P. R. Hemmer, R. L. Walsworth, A. Yacoby, A. S. Zibrov and M. D. Lukin, Science **326**, 267-272 (2009).

[3] P. Neumann, J. Beck, M. Steiner, F. Rempp, H. Fedder, P. R. Hemmer, J. Wrachtrup and F. Jelezko, Science **329**, 542-544 (2010).

[4] T. D. Ladd, D. Maryenko, Y. Yamamoto, E. Abe and K. M. Itoh, Phys. Rev. B **71**, 014401 (2005).

[5] G. de Lange, Z. H. Wang, D. Riste, V. V. Dobrovitski and R. Hanson, Science **330**, 60-63 (2010).

[6] S. Wiesner, Sigact News **15**, 78 (1983).

[7] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin and J. I. Cirac, arXiv: 1112.5456.

[8] N. Y. Yao, L. Jiang, A. V. Gorshkov, Z. X. Gong, A. Zhai, L. M. Duan and M. D. Lukin, Phys. Rev. Lett. **106**, 040505 (2011).

[9] N. Y. Yao, L. Jiang, A. V. Gorshkov, P. C. Maurer, G. Giedke, J. I. Cirac and M. D. Lukin, Nature Communications **3**, 800 (2012).

The Holy Grail of Quantum Optical Communication

__Raúl García-Patrón__[1], Carlos Navarrete-Benlloch[1], Seth Lloyd[2], Jeffrey H. Shapiro[2], and Nicolas J. Cerf[3]

[1]*Max-Planck Institut für Quantenoptik, Hans-Kopfermann-Str. 1, D-85748 Garching, Germany*
[2]*Research Laboratory of Electronics, MIT, Cambridge, Massachusetts 02139, USA*
[3]*QuIC, Ecole Polytechnique de Bruxelles, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*

Optical parametric amplifiers together with phase-shifters and beam-splitters have certainly been the most studied objects in the field of quantum optics. Interestingly, despite such an intensive study, optical parametric amplifiers still keep secrets from us. We will show how they seem to hold the answer to one of the oldest problems in quantum communication theory, the calculation of the optimal communication rate of optical channels.

Optical communication channels, such as optical fibers and amplifiers, are ubiquitous in todays telecommunication networks. Therefore knowing the ultimate communication capacity is of crucial importance. Since information is necessarily encoded in a physical system and since quantum mechanics is currently our best theory of the physical world, it is natural to seek the ultimate limits on communication set by quantum mechanics. Contrary to what happens in classical Shannon theory [1], a simple and universal formula for the capacity $C(\mathcal{M})$ of sending classical bits over a quantum channel $\mathcal{M}$ has not yet been found (neither disproved to exist) despite huge amounts of work by the quantum information community. Nevertheless, for some highly symmetric channels, such as depolarizing channels or unital qubit channels, people were able to obtain their capacity by showing it to be equal to the Holevo capacity

$$C_H(\mathcal{M}) = \max_{\mathcal{S}} \left(S\left(\mathcal{M}(\rho)\right) - \sum_a p_a S\left(\mathcal{M}(\rho_a)\right) \right) \quad (1)$$

where $\mathcal{S} = \{p_a, \rho_a\}$ is the coding source and where $\rho = \sum_a p_a \rho_a$ and $S(\sigma)$ is the von Neumann entropy of the quantum state σ. For a long time it was strongly believed by the quantum information community that the Holevo capacity $C_H(\mathcal{M})$ was additive and therefore gave the exact channel capacity for all quantum channels. This believe was proven to be wrong in 2009 by Hastings [2], therefore showing that entanglement could be a useful resource for transmitting classical information over quantum channels.

An important step towards the elucidation of the classical capacity of an optical quantum channel was made in [3], where the authors showed that $C(\mathcal{L})$ of a pure-loss channel $\mathcal{L}$—a good (but idealized) approximation of an optical fiber—is achieved by random coding of coherent states using an isotropic Gaussian distribution. It had long been conjectured that such an encoding achieves $C(\mathcal{M})$ for the whole class of optical channels called single-mode *phase-insensitive* Gaussian bosonic channels, including noisy optical fibers and amplifiers [4, 5]. Despite multiple attempts, this conjecture has since then escaped a proof. Actually, proving a slightly stronger result known as the *minimum output entropy* conjecture, namely that a vacuum input state minimizes the output entropy of phase-insensitive channels, would be sufficient. Unfortunately, even the simpler case of proving vacuum to minimize the output entropy for a single use of the channel has turned out to be an extremely challenging task. On top of that, it was not known whether the Holevo capacity is additive for phase-insensitive Gaussian bosonic channels. If that would not be the case, as in Hasting's counterexample, obtaining the capacity would become a real daunting task.

In a recent work the authors showed that the minimum output entropy conjecture for a single-use of a phase-insensitive Gaussian bosonic channels could be reduced to prove that among all input states $|\phi\rangle_{AE} \equiv |\varphi\rangle \otimes |0\rangle$ of a two-mode squeezer

$$U(r) = \exp\left[r(a_A a_E - a_A^\dagger a_E^\dagger)/2 \right], \quad (2)$$

the vacuum state $|0\rangle_{AE} \equiv |0\rangle \otimes |0\rangle$ minimizes the output entanglement [6]. The authors also provided a partial proof of this conjecture for a special class of input states, namely photon number states. Therefore, we are left with the (possibly simpler) task of showing that the input states which minimizes the output-entropy is isotropic in phase space.

Later some of the authors discovered that the result of [6] can be extended by showing that the Holevo capacity is additive if the minimum output entropy conjecture holds [7]. Interestingly, for some important quantum-limited channels one can even prove the additivity of the Holevo capacity independently of the minimum output entropy conjecture being true or not. The combination of those two recent results ([6, 7]) brings a new perspective on one of the oldest open problems in quantum communication theory, which could potentially lead to its final solution by reducing it to a detail study of the entangling properties of optical parametric amplifiers.

References

[1] C. E. Shannon, Bell Syst. Tech. J. **27,** 379 (1948).

[2] M. B. Hastings, Nature Physics **5,** 255 (2009).

[3] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. **92,** 027902 (2004).

[4] C. Weedbrook, S. Pirandola, R. García-Patrón, T. Ralph, N. J. Cerf, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys., to appear (2012).

[5] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, and J. H. Shapiro, Phys. Rev. A **70,** 032315 (2004).

[6] R. García-Patrón, C. Navarrete-Benlloch, S. Lloyd, J. H. Shapiro, and N. J. Cerf, Phys. Rev. Lett. **108,** 110505 (2012).

[7] R. García-Patrón and N. J. Cerf, unpublished work (2012).

Information storage capacity of discrete spin systems

Beni Yoshida[1]

[1]*Center for Theoretical Physics, Massachusetts Institute of Technology, United States*

Introduction: What is the limit of information storage capacity of physical systems? For continuum systems, this problem has been answered by Bekenstein where he showed there is an upper bound for the amount of information that can be stored inside a finite volume. The most surprising outcome is the fact that black holes saturate this theoretical limit.

Here we ask a similar question for discrete spin systems on a lattice, inspired a pioneering work [1]. In particular, we study classical error-correcting codes which can be physically realized as the energy ground space of gapped local Hamiltonians.

For spin systems on a D-dimensional lattice governed by local frustration-free Hamiltonians, the following bound is known to hold; $kd^{1/D} \leq O(n)$ where k is the number of encodable logical bits, d is the code distance, and n is the total number of spins in the system [1]. Yet, previously found codes were far below this bound and it remained open whether there exists an error-correcting code which saturates the bound or not (see Fig. 1b).
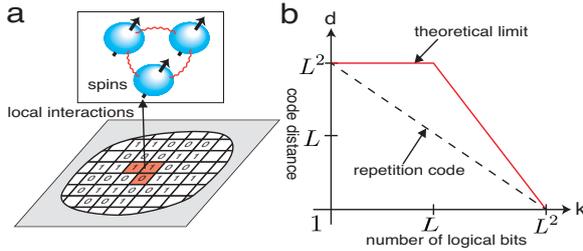
Figure 1: a. Encoding of information into discrete spin systems via local interactions. b. Theoretical limit on information storage capacity of discrete spin systems for $D = 2$. L is the linear length of the lattice. Coding properties of repetition codes, supported by ferromagnetic interactions, are shown with a dotted line

Here, we give a construction of local spin systems which saturate the bound asymptotically with $k \sim O(L^{D-1})$ and $d \sim O(L^{D-\epsilon})$ for an arbitrary small $\epsilon > 0$ where L is the linear length of the system. Therefore, our construction gives the best error-correcting code that is physically realizable as the gapped ground space.

Model: Our model borrows an idea from a fractal geometry arising in Sierpinski triangle. The Sierpinski triangle can be physically realized as a ground state on a square lattice via three-body interactions with degenerate ground states. Recently, its coding properties have been predicted as [1]:

$$k \sim O(L), \qquad d \sim O(L^{\frac{\log 3}{\log 2}}) \qquad (1)$$

where $\frac{\log 3}{\log 2} \sim 1.585$.

Despite a remarkable idea of constructing a local code based on the Sierpinski triangle, this system is still below the theoretical limit. Also a complete mathematical proof for the prediction was missing.
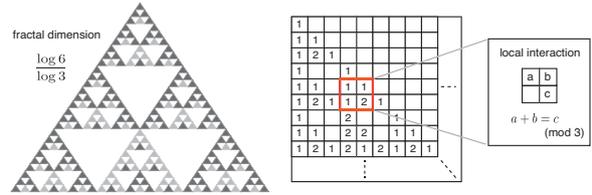

Figure 2: Physical realizations of the generalized Sierpinski triangle.

Our construction utilizes a generalization of the Sierpinski triangle to higher-dimensional spins. Fractal properties of the Sierpinski triangle with three-dimensional spins with possible spin values $0, 1, 2$ are shown in Fig. 2. The number of non-zero spins in this generalized Sierpinski triangle is $L^{\frac{\log 6}{\log 3}}$, and thus, its fractal dimension is $\frac{\log 6}{\log 3} \sim 1.631$. This generalization gives a fractal code with $k \sim O(L)$ and $d \sim O(L^{\frac{\log 6}{\log 3}})$ where k is the number of encodable three-dimensional spins.

The key observation is that the fractal dimension of the Sierpinski triangle grows as the inner dimension of spins, denoted by p, increases. Assuming p is a prime number, at the limit where p goes to infinity, we notice

$$\mathcal{D}_p^{(2)} = \frac{\log(\frac{p(p+1)}{2})}{\log p} \to 2 \qquad \text{for} \quad p \to \infty \qquad (2)$$

where $\mathcal{D}_p^{(2)}$ is the fractal dimension of the Sierpinski triangle with p-dimensional spins. Therefore, by taking sufficiently large p, one can construct a fractal code with $k \sim O(L)$ and $d \geq O(L^{2-\epsilon})$ for an arbitrary small $\epsilon > 0$ where k is the number of encodable p-dimensional spins. This family of fractal codes will saturate the theoretical limit asymptotically. A similar construction works for $D > 2$ too. All the mathematical details and proofs leading to these claims are presented in [2].

To conclude, we point out that an area law naturally arises on coding properties of fractal codes: the number of encoded bits k is area-like with $k \sim O(L^{D-1})$, while the code distance d is asymptotically volume-like with $d \sim O(L^{D-\epsilon})$. However, a connection between fractal codes and black holes has not been established, with further work needed.

References

[1] S. Bravyi, D. Poulin, and B. Terhal, Phys. Rev. Lett. **104**, 050503 (2010).

[2] Beni Yoshida, arXiv:1111.3275.

Wednesday talks abstracts

Quantum memories for few qubits: design and applications

J. Ignacio Cirac

[1]*Max-Planck Institute for Quantum Optics, Hans-Kopfermannstr. 1, D-85748 Garching, Germany*

The realization of devices which harness the laws of quantum mechanics represents an exciting challenge at the interface of modern technology and fundamental science. An exemplary paragon of the power of such quantum primitives is the concept of "quantum money" as introduced by Wisner more than thirty years ago. A dishonest holder of a quantum bank-note will invariably fail in any forging attempts; indeed, under assumptions of ideal measurements and decoherence-free memories such unconditional security is guaranteed by the no-cloning theorem. In any practical situation, however, noise, decoherence and operational imperfections abound. Thus, the development of secure "quantum money"-type primitives capable of tolerating realistic infidelities is of both practical and fundamental importance. Here, we propose a novel class of such protocols and demonstrate their tolerance to noise; moreover, we prove their rigorous security by determining tight fidelity thresholds. Our proposed protocols require only the ability to prepare, store and measure single qubit quantum memories, making their experimental realization accessible with current technologies. Such memories are devices where one can store quantum information in the presence of noise. There have been several proposals on how to achieve this goal, as well as proof of principle demonstrations. In this talk we also revise some of those proposals and explain under which conditions they can work; that is, what kind of noise they can withstand. Joint work with F. Pastawski, L. Mazza, M. Rizzi, N. Yao, L. Jiang, and M. Lukin.

Compressed quantum simulation of the Ising model

Barbara Kraus [1]

[1] *University of Innsbruck, Innsbruck, Austria*

In [R. Jozsa, B. Kraus, A. Miyake, J. Watrous, Proc. R. Soc. A **466**, 809-830 (2010)] it has been shown that a match gate circuit running on n qubits can be compressed to a universal quantum computation on $\log(n) + 3$ qubits. Here, we show how this compression can be employed to simulate the Ising interaction of a 1D–chain consisting of n qubits using a universal quantum computer running on $\log(n)$ qubits. We demonstrate how the adiabatic evolution can be realized on this exponentially smaller system and how the magnetization, which displays a quantum phase transition, can be measured. This shows that the quantum phase transition of very large systems can be observed experimentally with current technology [1].

Due to the exponential growth of the required resources, like space and time, as a function of the number of considered quantum systems, the simulation of certain quantum systems on a classical computer seems to be an unfeasible task. As conjectured by Feynman and proven by LLoyd, however, a quantum system can be used to simulate the behavior of another. The former one being such that the interactions between the systems are well–controllable and that the measurements can be performed sufficiently well. The suitability for the realization of such a quantum simulator has been shown for experimental schemes based on optical lattices or ion–traps [2]. Recently, several experiments using for instance trapped ions, neutral atoms or NMR have realized quantum simulations [3].

An important application of the quantum simulator is the study of the ground state properties of certain condensed matter systems. Quantum spin models are well suited for the investigations of quantum phase transitions, which occur at zero temperature due to the change of some parameter, like the strength of the magnetic field, or pressure. The 1D quantum Ising model, for instance, exhibits such a phase transition. It can be detected by measuring the magnetization as a function of the ratio between the interaction strength and the strength of the external magnetic field, which will be denoted by J here. Since the Ising interaction is relatively simple, this is a good model for the experimental demonstration of quantum simulation, even though it can be simulated classically efficiently. Experimentally, the ground state properties, like the magnetization, $M(J)$, of the Ising model for a small number of qubits have been recently observed.

Here we use a different approach, which makes use of the fact that certain quantum circuits, the so–called matchgate (MG) circuits (MGC), can be simulated by an exponentially smaller quantum system [4]. We extend here this result and introduce new techniques to show that the evolution of the 1D Ising model (including the measurement of the magnetization) of a spin chain consisting of n qubits can be simulated by a compressed algorithm running only on $\hat{m} \equiv \log(n)$ qubits. More precisely, it is shown that the magnetization, $M(J)$, can be measured using the following algorithm: 1)

First prepare the initial $\hat{m}$–qubit state $\rho_{in} = \mathbf{1} \otimes |+_y\rangle \langle +_y|_{\hat{m}}$, with $|+_y\rangle = 1/\sqrt{2}(|0\rangle - i\,|1\rangle)$; 2) evolve the system up to a certain value of J according to a specific unitary operator $W(J)$; 3) measure the $\hat{m}$–th qubit in y–direction, i.e. $Y_{\hat{m}}$. The expectation value of $Y_{\hat{m}}$ coincides with the magnetization, $M(J)$ (for n qubits) up to a factor -1. The size of this circuit, i.e. the total number of single and two–qubit gates required to implement $W(J)$, is at most as large as the one required to implement $U(J)$ for the original circuit. Moreover, the error due to the Trotter approximation is the same as the one of the original system, since we are simulating the gates exactly. Due to the fact that this compressed quantum computation corresponds to the simulation of the Ising model not only the magnetization, but also other quantities, like correlations can be measured.

This result allows for the experimental measurement of the quantum phase transition of very large systems with current technology. Consider for instance, experiments with ion-traps or NMR quantum computing where say 8 qubits can be well–controlled. According to the results presented here such a system can be employed to simulate the interaction of $2^8 = 256$ qubits. Of course, for such a large system the phase transition can be well observed. Note, that in contrast to [4], where arbitrary MGC are considered, we use here the properties of the Ising model to show that only $\log(n)$ (instead of $\log(n) + 3$) qubits are required for the simulation. That is, in the experiment suggested above the phase transition of 256 instead of $2^5 = 32$ qubits can be observed.

References

[1] B. Kraus, Phys. Rev. Lett. **107**, , 250503 (2011) .

[2] E. Jané, G. Vidal, W. Dür, P. Zoller, J.I. Cirac, Quant. Inf. Comp., **3**, 1, 15 (2003); D. Porras, J. I. Cirac, Phys. Lett. **92**, 207901 (2004); D. Jaksch and P. Zoller, Annals of Physics **315**, 52 (2005).

[3] see for instance A. Friedenauer, H. Schmitz, J. Glueckert, D. Porras and T. Schaetz. Nature Physics **4**, 757 (2008);K. Kim, M.-S. Chang, S. Korenblit, R. Islam, E. E. Edwards, J. K. Freericks, G.-D. Lin, L.-M. Duan3, C. Monroe, Nature, **465**, 590 (2010); R. Islam et. *al*, Nature Communications, **2**, 377 (2011); B. P. Lanyon et. *al.*, Science, 1208001 (2011); I. Bloch, J. Dalibard, W. Zwerger, Rev. Mod. Phys. **80**, 885 (2008); J. Zhang, T.-Ch. Wei, R. Laflamme, Phys. Rev. Lett. **107**, 010501 (2011).

[4] R. Jozsa, B. Kraus, A. Miyake, J. Watrous, Proc. Roy. Soc. A **466**, 809 (2010).

Occam's Quantum Razor: How Quantum Mechanics can reduce the Complexity of Classical Models

Mile Gu[1], **Karoline Wiesner**[2], **Elisabeth Rieper**[1] **and Vlatko Vedral**[1,3,4]

[1] *Center for Quantum Technology, National University of Singapore, Republic of Singapore*
[2] *School of Mathematics, Centre for Complexity Sciences, University of Bristol, Bristol BS8 1TW, United Kingdom*
[3] *Atomic and Laser Physics, Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX13PU, United Kingdom*
[4] *Department of Physics, National University of Singapore, Republic of Singapore*

Occam's razor is an important principle that guides the development of theoretical models in quantitative science. In the words of Isaac Newton,"We are to admit no more causes of natural things than such as are both true and sufficient to explain their appearances." Take for example application of Newton's laws on an apple in free fall. The future trajectory of the apple is entirely determined by a second order differential equation, that requires only its current location and velocity as input. We can certainly construct alternative models that predict identical behavior, that demand the apple's entire past trajectory as input. Such theories, however, are dismissed by Occam's razor, since they demand input information that is either unnecessary or redundant.

Generally, a mathematical model of a system of interest is an algorithmic abstraction of its observable output. Envision that the given system is encased within a black box, such that we observe only its output. Within a second box resides a computer that executes a model of this system with appropriate input. For the model to be accurate, we expect these boxes to be operationally indistinguishable; their output is statistically equivalent, such that no external observer can differentiate which box contains the original system.

There are numerous distinct models for any given system. Consider a system of interest consisting of two binary switches. At each time-step, the system emits a 0 or 1 depending on whether the state of the two switches coincides, and one of the two switches is chosen at random and flipped. The obvious model that simulates this system keeps track of both switches, and thus requires an input of entropy 2. Yet, the output is simply a sequence of alternating 0s and 1s, and can thus be modeled knowing only the value of the previous emission. Occam's razor stipulates that this alternative is more efficient and thus superior; it demands only an input of entropy 1 (i.e., a single bit), when the original model required two.

Efficient mathematical models carry operational consequence. The practical application of a model necessitates its physical realization within a corresponding simulator (Fig. 1). Therefore, should a model demand an input of entropy C, its physical realization must contain the capacity to store that information. The construction of simpler mathematical models for a given process allows potential construction of simulators with reduced information storage requirements. Thus we can directly infer the minimal complexity of an observed process once we know its simplest model. If a process exhibits observed statistics that require an input of entropy C to model, then whatever the underlying mechanics of the observed process, we require a system of entropy C to simulate its future statistics.

These observations motivate maximally efficient models; models that generate desired statistical behavior, while requiring minimal input information. In this presentation, we discuss recent results that even when such behavior aligns with simple stochastic processes, such models are almost always quantum [1]. For any given stochastic process, we outline its provably simplest classical model, We show that unless improvement over this optimal classical model violates the second law of thermodynamics, our construction and a superior quantum model and its corresponding simulator can *always* be constructed.

We discuss the implications of this result to complexity theory, where the minimum amount of memory to simulate a process is employed as a measure of how much structure a given process exhibits [2]. The rationale being that the optimal simulator of such a process requires at least this much memory. Many organisms and devices operate based on the ability to predict and thus react to the environment around them, and thus the possibility of exploiting quantum dynamics to make identical predictions with less memory implies that such systems need not be as complex as one originally thought.
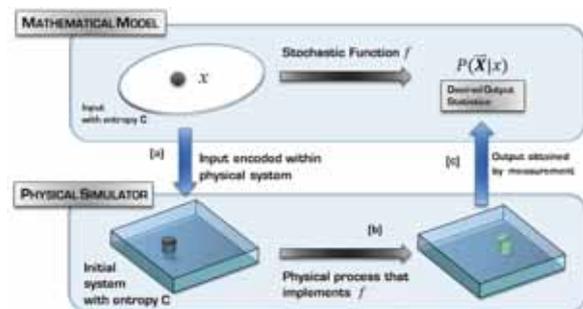

Figure 1: To implement a mathematical model, we must realize it within some physical simulator. To do this, we (a) encode 'x' within a suitable physical system, (b) evolve the system according to a physical implementation of f and (c) retrieve the predictions of model by appropriate measurement.

References

[1] Mile Gu, Karoline Wiesner, Elisabeth Rieper, Vlatko Vedral, Quantum Mechanics can reduce the Complexity of Classical Models, *Nat. Commun.* **3**, 762, 2002

[2] Crutchfield, J. P., Inferring statistical complexity, *Phys. Rev. Lett.* **63**, 105–108, 1989

Recent Experiments on Quantum Manipulation with Photons and Atoms

Jian-Wei Pan

National Laboratory for Physical Sciences at Micro-scale, University of Science and Technology of China, PR China

Quantum information technology has been developing rapidly in last two decades. Very recently, quite a few optical quantum key distribution networks have been reported, enabling preliminary practical applications in secure information transfer. Meanwhile, a number of significant progresses have also been made in the research of linear optical quantum computing, simulation and metrology. However, on the way towards large-scale optical quantum information processing serious problems occur. On the one hand, the distance of fiber?based quantum communication is limited, due to intrinsic fiber loss and decreasing of entanglement quality caused by the noisy environment. On the other hand, the probabilistic feature of single and entangled photon sources would also cause an exponentially increasing overhead for large-scale optical quantum information processing.

To solve the above problems, quantum repeaters and/or transmission of optical quantum bits over free space channel can be efficiently exploited for future wide?area realization of quantum communication. In addition, memory built-in quantum repeaters would also enable scalable linear optical quantum computing, simulation and high precision measurement. In this talk I will present some recent experiments from our group, including eight-photon entanglement, topological quantum error-correction, quantum repeater and efficient and long-lived quantum memory, and entanglement distribution and quantum teleportation over 100km-scale free-space quantum channels. These experiments show the promising future possibility towards scalable quantum information processing with photons and atoms.

Quantum Communication Award 2012

Quantum Heat

Seth Lloyd

Department of Mechanical Engineering, MIT, United States

In quantum communication, information moves from one place to another, while in quantum heat transport, entropy and energy do the moving. Because entropy is a form of information, the same physics governs both processes. Near-field heat transport can occur at rates substantially greater than the black-body limit. I derive a quantum-communication based limiting rate for near-field heat transport.

Quantum
Communication
Award
2012

Thursday talks abstracts

Quantum Cryptography and Quantum Repeaters

Nicolas Gisin

Group of Applied Physics, University of Geneva, Switzerland

Quantum cryptography is the most advanced application of quantum communication. It has found niche markets, with several commercial systems running continuously on several continents.

Today's, there are at least two Grand Challenges for academic research in quantum communication. The first one aims at futuristic continental scale quantum networks. The second one concerns "device independent QKD", that is an implementation of Quantum Key Distribution that exploits the nonlocal correlation observed in violations of Bell's inequality to realize "self testing QKD apparatuses".

We first present our recent results on solid state multimode **quantum memories** [1, 2], including quantum memories for photonic polarization qubits [3]. In addition of being a key component for quantum repeaters, entangled quantum memories can be seen as "mesoscipic entanglement" in a sense to be discussed.

Next, we present ideas [4]and preliminary results [5] on a **qubit amplifier**. This should be a central component for Device Independent QKD, hence, possibly also for a loophole free Bell test.

References

[1] Christoph Clausen, Imam Usmani, Félix Bussières, Nicolas Sangouard, Mikael Afzelius, Hugues de Riedmatten and Nicolas Gisin, *Quantum storage of photonic entanglement in a crystal*, Nature **469**, 508-511 (2011).

[2] Imam Usmani, Christoph Clausen, Félix Bussières, Nicolas Sangouard, Mikael Afzelius and Nicolas Gisin, *Heralded quantum entanglement between two crystals*, Nature Photonics **6**, 234-7 (2012), quant-ph/1109.0440

[3] Christoph Clausen, Félix Bussièress, Mikael Afzelius and Nicolas Gisin, *Quantum storage of polarization qubits in birefringent and anisotropically absorbing materials*, Phys. Rev. Lett. **108**, 190503 (2012), quant-ph/1201.409

[4] Nicolas Gisin, Stefano Pironio and Nicolas Sangouard, *Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier*, Physical Review Letters **105**, 070501 (2010), quant-ph/1003.0635

[5] Clara I. Osorio, Natalia Bruno, Nicolas Sangouard, Hugo Zbinden, Nicolas Gisin and Robert T. Thew, *Heralded photon amplification for quantum communication*, quant-ph/1203.3396

Quantum key distribution using electrically driven quantum-dot single photon sources on a free space link

Markus Rau[1], **Tobias Heindel**[2], **Christian A. Kessler**[3], **Christian Schneider**[4], **Martin Fürst**[5], **F. Hargart**[3], **Wolfgang-Michael Schulz**[3], **Marcus Eichfelder**[3], **Robert Roßbach**[3], **Sebastian Nauerth**[1,5], **Matthias Lermer**[4], **Henning Weier**[5], **Michael Jetter**[3], **Martin Kamp**[4], **Stephan Reitzenstein**[2], **Sven Höfling**[4], **Peter Michler**[3], **Alfred Forchel**[4] and **Harald Weinfurter**[1,6]

[1] *Fakultät für Physik, Munich, Germany*
[2] *Institut für Festkörperphysik, Berlin, Germany*
[3] *Institut für Halbleiteroptik und Funktionelle Grenzflächen, Stuttgart, Germany*
[4] *Technische Physik, Würzburg, Germany*
[5] *qutools GmbH, Munich, Germany*
[6] *Max-Planck-Institut für Quantenoptik, Garching, Germany*

Increasing the key generation rate is one the the most important goals in the development of quantum key distribution. Systems which rely on sensitive single photon detectors are limited by the maximal countrate of these detectors. Yet this countrate directly determines the achievable key generation rate. If this countrate limit is reached, the keyrate can only be increased if the ammount of key that is lost during the privacy amplification step in the QKD-protocol is reduced.

The original BB84 QKD-protocol[1] uses single photons as qubits for the key distribution. The privacy amplification in BB84 depends only on the error rate of the transmission. If a system uses faint laser pulses instead of single photons an extension to the BB84 protocol is necessary to guarantee security: the Decoy protocol[2]. The Decoy protocol introduces additional losses during the privacy amplification compared to BB84, in order to compensate the advantage an eavesdropper gains from faint pulses which occasionally contain multiple photons. Therefore, changing from faint pulses to single photons enables to increase the possible key rate. However, this would requires a very efficient and convenient single photon source. Electrically driven quantum dots are a promising type of single photon sources which might offer the required efficiency to overcome this threshold in a practical manner.

Compared to attenuated pulse systems, the main problem problem using single photon sources is the coding of the photons, as it requires extremely fast optical modulators or switches. If the extinction ratio of the modulator is too low the error rate will increase and the secure key rate will go down. Such an effect could easily foil the possible gain of single photon sources over faint laser pulses.

We performed several experiments in a lab environment using InAs quantum dots emitting in the near infrared spectral range, which were fabricated at the university of Würzburg[3]. A very high photon extraction efficiency was achieved using an optimized micropillar cavity design resulting in efficiencies up to 30%. We could successfully demonstrate QKD and achieved a sifted key rate of 35 kBit/s and an error rate of 3.8 % with a $g^{(2)}$-value of 0.40. In a second run of experiments we used InP quantum dots emitting in the red spectral range, which were manufactured at the university of Stuttgart[4]. Their emission wavelength perfectly matches the peak detection effeciency of SI APDs. We could achieve a sifted key rate of 95 kBit/s and an error rate of 4.2 % with a $g^{(2)}$-value of 0.48.

Using the experience gathered, we integrated the InAs single photon source into the 500 meter free space QKD link in downtown munich. The main challenge was to transfer a typical lab setup to verly limited space replace the liquid He cooling system.

Finally, we could fully characterize the source also in the new setup and successfully demonstrate QKD over a 500 meter free space link. The achieved sifted rates of over 10 kHz with error rates of 6 % demonstrate the feasibility and pave the way towards increased QKD rates.

References

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), pp. 175.

[2] X.-B. Wang, Appl. Phys. Lett. **94**, 230503 (2005).

[3] T. Heindel, C. Schneider, M. Lermer, S. H. Kwon, T. Braun, S. Reitzenstein, S. Höfling, M. Kamp, and A. Forchel Appl. Phys. Lett. **96**, 011107 (2010).

[4] M Reischle, C Kessler, W-M Schulz, M Eichfelder, R Robach, M Jetter and P Michler, Appl. Phys. Lett. **97**, 143513 (2010).

First implementation of bit commitment in the Noisy-Storage Model

Nelly Ng Huei Ying,[1,2,*] Siddarth K. Joshi,[2] Chia Chen Ming,[2]

Mario Berta,[3] Christian Kurtsiefer,[2] and Stephanie Wehner[2]

[1]*School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371*

[2]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543 Singapore*

[3]*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*

(Dated: March 31, 2012)

Traditionally, the main objective of cryptography is to protect communication from the prying eyes of an eavesdropper. Yet, with the advent of electronic communications, new cryptographic challenges arose as we would like to enable two-parties Alice and Bob, to solve joint problems even if they do not trust each other. Examples of such tasks include secure auctions, or the problem of secure identification, e.g. of a customer to an ATM machine. Whereas protocols for general two-party cryptographic problems may be involved, it is known that they can in principle be built from basic building blocks known as oblivious transfer and bit commitment.

Unfortunately, it has been shown that even with quantum communication none of these tasks can be implemented securely. Only weak variants can be obtained, where the attacker can cheat with large probability, rendering them uninteresting for practical applications. Yet, since two-party protocols form a central part of modern cryptography, one is willing to make assumptions on how powerful an attacker can be in order to implement them securely. In particular, the bounded [1] and noisy-storage model [4] make the physical assumption that the attacker's quantum memory device is limited and/or imperfect to enable security. This is indeed realistic today, as constructing large scale quantum memories that can store arbitrary information successfully has proved rather challenging.

Results

Protocol and analysis In this work, we first adapt the bit commitment protocol of [2] and provide a full analysis of its security in an experimental context. We prove its security for a wide range of experimental parameters. In essence, our slight adaptation of the protocol from [2] makes it robust against experimental losses and errors.

Experimental implementation Second, we perform the first ever experimental implementation of bit commitment in the noisy-storage model. This is the first ever implementation of a protocol in the bounded/noisy-storage model, and demonstrates the feasibility of implementing two-party protocols in such models.

New uncertainty relation Enabling the experiment, is our development of a new uncertainty relation for BB84 measurements. Previously, the security of two party protocols was based on the uncertainty relation developed in [1], which yields an exponentially decreasing error in the limit of large block length. While this is sufficient for a proof of principle, an implementation based on this relation is extremely time-consuming due to the size of block length required for a small error parameter. We have proven entropic uncertainty relations that pave the way for a practical implementation of many other BB84 and six-state protocols [1, 3, 4] at small block length. As
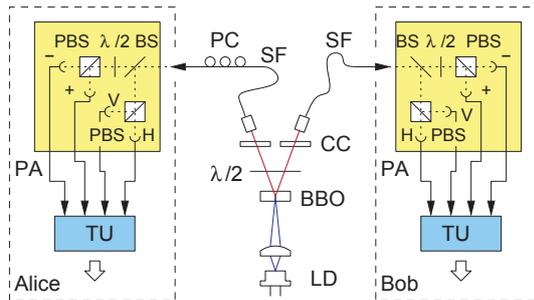

FIG. 1: Experimental setup. Polarization-entangled photon pairs are generated via non-collinear type-II spontaneous parametric down conversion of blue light from a laser diode (LD) in a Barium-betaborate crystal (BBO), and distributed to polarization analysers (PA) at Alice and Bob via single mode optical fibers (SF). The PA are based on a nonpolarizing beam splitter (BS) for a random measurement base choice, a half wave plate ($\lambda/2$) at one of the of the outputs, and polarizing beam splitters (PBS) in front of single-photon counting silicon avalanche photodiodes. Detection events on both sides are timestamped (TU) and recorded for further processing according to the bit commitment protocol. A polarization controller (PC) ensures that polarization anti-correlations are observed in all measurement bases.

part of our proof we show tight uncertainty relations for a family of Rényi entropies that may be of independent interest. In the practically feasible regime, our relation provides a decisive advantage enabling an experimental implementation of all protocols proposed in such models to date. We employ this for our experimental implementation of bit commitment, significantly reducing the amount of classical information post-processing required in the protocol.

———————

* nell0002@e.ntu.edu.sg

[1] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Proceedings of CRYPTO 2007*, Springer Lecture Notes in Computer Science, pages 360–378, 2007.

[2] R. König, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory - To appear*, 2009. arXiv:0906.1030v3.

[3] C. Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Physical Review A*, 82:032308, 2010. arXiv:1002.1495v2.

[4] S. Wehner, C. Schaffner, and B. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, 2008.

Novel quantum key distribution technologies in the Tokyo QKD Network

__M. Sasaki__[1], M. Fujiwara[1], K. Yoshino[2], A. Tanaka[2*], S. Takahashi[2], Y. Nambu[3], A. Tajima[2],T. Domeki[4], J. F. Dynes[5], A. R. Dixon[5], A. W. Sharpe[5], Z. L. Yuan[5], A. J. Shields[5], and S. Uchikoga[5], T. Hasegawa[6], Y. Sakai[6], H. Kobayashi[6], T. Asai[6], K. Shimizu[6], T. Tokura[6], T. Tsurumaru[6], M. Matsui[6], T. Hirano[7], A. Tomita[8], T. Honjo[9], K. Tamaki[10,1], K. Shimizu[10], S. Miki[11],T. Yamashita[11], H. Terai[11], Z. Wang[11], Y. Takayama[12], and M. Toyoshima[12]

[1] *Quantum ICT Laboratory, National Institute of Information and Communication Technology (NICT), 4-2-1 Nukui-kitamachi, Koganei, Tokyo 184-8795, Japan*

[2] *Green Platform Research Laboratories, NEC Corporation, 1753 Shimonumabe, Nakahara, Kawasaki, Kanagawa 211-8666, Japan*

[3] *Smart Energy Research Laboratories, NEC Corporation, 34 Miyukigaoka, Tsukuba, Ibaraki 305-8501, Japan*

[4] *Network Platform Business Division, NEC Communication Systems, 3-4-7 Chuo, Aoba, Sendai, Miyagi 980-0021, Japan*

[5] *Toshiba Research Europe Ltd, 208 Cambridge Science Park, Cambridge CB4 0GZ, United Kingdom*

[6] *Information Technology R& D Center, Mitsubishi Electric Corporation, 5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan*

[7] *Department of Physics, Gakushuin University, 1-5-1 Mejiro, Toshima-ku, Tokyo 171-1588, Japan*

[8] *Graduate School of Information Science and Technology, Hokkaido University, Kita-ku, Sapporo, Hokkaido 060-0814, Japan*

[9] *NTT Secure Platform Laboratories, NTT Corporation, 3-9-11 Midori-cho, Musashino, Tokyo 180-8585, Japan*

[10] *NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato, Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[11] *Nano ICT Laboratory, NICT, 588-2, Iwaoka, Iwaoka-cho, Nishi-ku, Kobe, Hyogo 651-2492, Japan*

[12] *Space Communication System Laboratory, NICT, 4-2-1 Nukui-kitamachi, Koganei, Tokyo 184-8795, Japan*

Quantum key distribution (QKD) offers a function to generate secure random numbers on demand over a point-to-point optical link. Although its performance is still restrictive, this important function should be appreciated in many scenes, not only for protecting data confidentiality but also for providing keys for authentication and signature. These QKD-based services will be useful in intra-server networks and campus-scale networks of mission-critical organizations. If QKD devices can be compact and cheap, they will be used for key exchange for those purposes. A typical structure of QKD-secured network, referred to as secure photonic network, is depicted in Fig. 1a. Secure keys are generated in the quantum layer, and provided to the key management (KM) layer, where the secure keys are stored and managed by the KM agents for security sevices in the application layer.

In this talk, we present and discuss our recent results and future issues on QKD and related technologies in each layer. In quantum layer there are three main issues; QKD link, quantum node, and quantum side-channels. We have developed GHz-clocked QKD link technologies, and deployed them in a testbed "Tokyo QKD Network" [1]. Its current topology is shown in Fig. 1b. NEC-NICT system (BB84) demonstrated three-wavelength-division-multiplexing QKD at 1.24GHz rate at each wavelength in an 45km installed fiber, using semiconductor avalanche photodiodes (APD) and superconducting single photon detectors [2]. Toshiba system (BB84) realized high bit rate QKD over a 45km field link with a record bit-rate distance product of 13.2×10^6 (bits/s)-km, using novel self-differencing APDs and an active stabilization technique. NTT-NICT system (DPS-QKD) has been put to long term operation test over a 90km distance. A countermeasure against the so-called bright illumination attack is proposed and experimentally demonstrated for this system.

New applications based on QKD have also been developed. Mitsubishi system (BB84) has an interface to upload secure keys to smartphones. NICT fabricated an QKD-assisted authentication of network swiches to prevent spoofing and falsification in the key management layer.

The network topology will be revised in a couple years as shown in the middle of Fig. 1b, including continuous variable QKD link (Gakushuin system). The current status of this technology will be reported in the talk. The revised topology allow us to perform multiparty tasks. In 2015, a free space QKD link and some further fiber links will be added. Some nodes will perform wavelength and format conversion for fiber-space link in the quantum domain (quantum node). It is still an open question what kind of topology would be the best. It will be designed according to the best knowledge obtained until then.

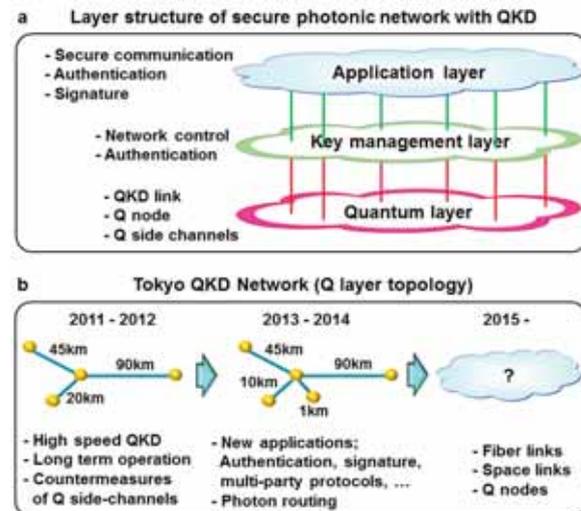* A. Tanaka is currently with NEC Laboratories America.

Figure 1: Conceptual view of secure photonic network and quantum layer topology of Tokyo QKD Network

References

[1] M. Sasaki, et al., Opt. Express.__19__, 10387 (2011).

[2] K. Yoshino, et al., Opt. Lett. __37__, 223 (2012).; A. Tanaka, et al., IEEE J. Quantum Electron. __48__, 542 (2012).

Quantifying the noise of a quantum channel by noise addition

Antonella De Pasquale and <u>Vittorio Giovannetti</u>

*NEST, Scuola Normale Superiore and Istituto Nanoscienze-CNR,
piazza dei Cavalieri 7, I-56126 Pisa, Italy*

A new method for quantifying the noise level associated to a given quantum transformation is introduced. The key mechanism lying at the heart of the proposal is *noise addition*: in other words we compute the amount of extra noise we need to add to the system, through convex combination with a reference noisy map or by reiterative applications of the original map, before the resulting transformation becomes entanglement-breaking. We also introduce the notion of entanglement-breaking channels of order n (i.e. maps which become entanglement-breaking after n iterations), and the associated notion of amendable channels (i.e. maps which can be prevented from becoming entanglement-breaking after iterations by interposing proper quantum transformations). Explicit examples are analyzed in the context of qubit and one-mode Guassian channels.

In quantum information several entropic functionals (the so called quantum capacities) have been introduced that provide a sort of "inverse measures" of the noise level associated with a given process, see e.g. Refs. [1, 2, 3]. Quantum capacities have a clear operational meaning as they gauge the optimal communication transmission rates achievable when operating in parallel on multiple copies of the system: consequently the noisier the channel is, the lower are its associated quantum capacities. Unfortunately however, even for small systems, these quantities are also extremely difficult to evaluate since require optimization over large coding spaces, e.g. see Ref. [4, 5].

In [6] we introduce an alternative way to determine how disruptive a channel might be which, while still having a simple operational interpretation, it is easier to compute than the quantum capacities. The starting point of our analysis is to use Entanglement-Breaking (EB) channels [7, 8] as the fundamental benchmarks for evaluating the noise level of a transformation. A reasonable way to quantify the noise level of a generic map Φ can then be introduced by computing how much extra noise we need to "add" to it before the resulting transformation becomes entanglement-breaking. The intuitive idea behind this approach is that channels which are less disruptive should require larger amount of extra noise to behave like an entanglement-breaking map.

In particular we analyze two different mechanisms of noise addition. The first one assumes to form convex combinations of the input channel Φ with generalized depolarizing channel Φ_{DEP}, i.e.

$$(1 - \mu)\Phi + \mu\Phi_{DEP} \ . \tag{1}$$

In this approach the level of noise associated with the original map Φ is gauged by the minimum value μ_c of the mixing parameter μ which transforms the above mixture into an entanglement-breaking map (of course a proper characterization of this measure requires an optimization upon Φ_{DEP} too).

The second mechanisms assumes instead the reiterative ap-

plication of Φ on the system, i.e.

$$\Phi^n := \underbrace{\Phi \circ \Phi \circ \cdots \circ \Phi}_{n \text{ times}} \ . \tag{2}$$

In this case the noise level is determined by the minimum value n_c of iterations needed to transform Φ in an entanglement-breaking map (*if* such minimum exists). The definition of n_c gives us also the opportunity of introducing the set of the entanglement-breaking channels of order n, and the notion of *amendable* channels. The former is composed by all CPT maps Φ which, when applied n times, are entanglement-breaking. Vice-versa a channel Φ is amendable if it can be prevented from becoming entanglement-breaking after n_c iterations via a proper application of intermediate quantum channels.

References

[1] A. S. Holevo and V. Giovannetti, Rep. Prog. Phys. **75**, 046001 (2012).

[2] M. Keyl, Phys. Rep. **369**, 431 (2002).

[3] C. Bennett and P. W. Shor, IEEE Trans. Inf. Th. **44**, 2724 (1998).

[4] P. W. Shor, Math. Program. Ser. B 97 311 (2003).

[5] M. B. Hastings, Nature Phys. **5** 255 (2009).

[6] A. De Pasquale and V. Giovannetti, arXiv:1204.5589v1 [quant-ph].

[7] A. S. Holevo, Russian. Math. Surveys **53**, 1295 (1999).

[8] M. Horodecki, P. W. Shor, M. B. Ruskai, Rev. Math. Phys **15**, 629 (2003).

Superconducting Nanowire Single Photon Detectors for quantum optics and quantum plasmonics

Sander N. Dorenbos[1], **Iman Esmaeil Zadeh**[1], **Reinier W. Heeres**[1], **Hirotaka Sasakura**[2], **Ikuo Suemune**[2], **Gesine Steudle**[3], **Oliver Benson**[3], **Leo P. Kouwenhoven**[1] **and Val Zwiller**[1]

[1]*Kavli Institute of Nanoscience, Delft University of Technology, Delft, The Netherlands*
[2]*Research Institute for Electronic Science, Hokkaido University, Sapporo, Japan*
[3]*Humboldt-Universität zu Berlin, Berlin, Germany*

In the past few years superconducting nanowire single photon detectors have become a prominent choice for the detection of single photons at telecommunication wavelengths. They combine a short dead time (<10 ns) with a low dark count rate (<10 cps) and a low timing jitter (60 ps). Its quantum efficiency is however moderate ($\tilde{5}\%$ at 1550 nm). In this talk I will show which steps we have taken to improve the efficiency and the implementation in experiments of this higher efficiency detectors.

The most limiting factor for the efficiency is the absorption in the thin superconducting film. To increase the absorption we have fabricated SNSPDs on an oxidized silicon substrate. In addition we have developed a fiber coupling technique, by etching the chip in the shape of an FC connectorized fiber (see Fig. 1a), which makes it straightforward to implement the detectors in experiments. In this way we achieve a system detection efficiency of 34% at 1300 nm.

is observed and we show a biexciton-exciton cascade, which can be used to create entangled photon pairs .

The short dead time of the SNSPD allows us to perform an elementary experiment to unambiguously demonstrate the quantum nature of light. This experiment uses only one light source and one detector (Fig. 1c), in contrast to a Hanbury-Brown and Twiss configuration, where a beam splitter directs light to two photodetectors, creating the false impression that the beam splitter is a fundamentally required element. As additional benefit, our results provide a major simplification of the widely used photon-correlation techniques.

I will also demonstrate that SSPDs can be used to directly detect surface plasmon polaritons (plasmons). Plasmons are electromagnetic waves propagating on the surface of a metal with appealing characteristics of shortened wavelengths, enhanced field strengths and easy on-chip waveguiding. We detect plasmons by positioning an SSPD in the near field of the propagating plasmon (see Fig. 1d). We will prove the quantum nature of plasmons by performing an antibunching experiment. This opens the door for (quantum-) optics-on-a-chip experiments.
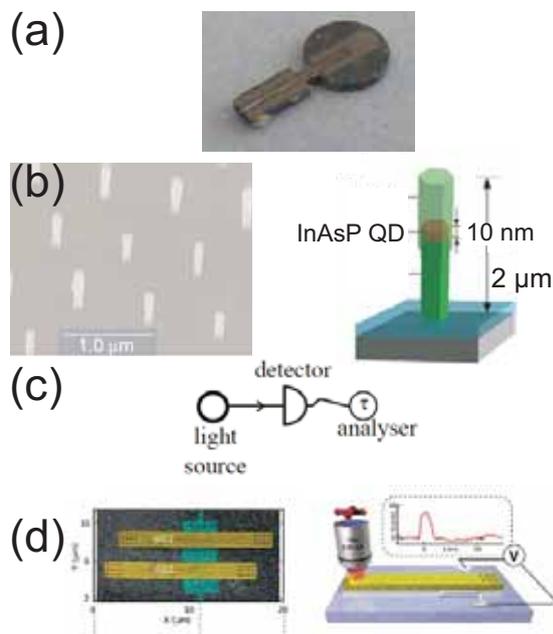
Figure 1: (a) SNSPD device (b)InAsP quantum dots in InP nanowires (c)Setup to measure antibunching with a single detector (d) Gold plasmon waveguide on an SNSPD.

This high system detection efficiency allows us to demonstrate single-photon and cascaded photon pair emission in the infrared, originating from a single InAsP quantum dot embedded in a standing InP nanowire (Fig. 1b). Clear antibunching

On-chip, photon-number-resolving, telecom-band detectors for scalable photonic information processing

T. Gerrits[1], N. Thomas-Peter[2], J. C. Gates[3], A. E. Lita[1], B. J. Metcalf[2], B. Calkins[1], N. A. Tomlin[1], A. E. Fox[1], A. Lamas Linares[1], J. B. Spring[2], N. K. Langford[2], R. P. Mirin[1], P. G. R. Smith[3], I. A. Walmsley[2], S. W. Nam[3]

[1] *National Institute of Standards and Technology, Boulder, CO, 80305, USA*
[2] *Clarendon Laboratory, University of Oxford, Parks Road, Oxford, UK, OX1 3PU, United Kingdom*
[3] *Optoelectronics Research Centre, University of Southampton, Highfield SO17 1BJ, United Kingdom*

We demonstrate the operation of an integrated photon-number resolving transition edge sensor (TES), operating in the telecom band at 1550 nm, employing an evanescently coupled design that allows the detector to be placed at arbitrary locations within a planar optical circuit. This concept eliminates the scalability problems associated with probing optical modes from the end facets of integrated circuits when using fiber-coupled single photon detectors. The device consists of a UV-written silica waveguide and a tungsten TES deposited onto the waveguide structure. The waveguide structure used was written by use of a UV laser writing technique designed to alter the index of a Ge-doped silica core layer, the underclad being a 17 μm layer of thermally grown silicon oxide. No top cladding was fabricated, to maximize the evanescent coupling to the TES. The planar core/cladding layer refractive index contrast was 0.6 % with a core layer thickness of 5.5 μm. The UV-written channel had a Gaussian index-profile with a contrast of 0.3 % and a width of about 5 μm. The TES dimensions were 25 μm x 25 μm x 40 nm with wiring to the tungsten achieved using niobium. The TES is photon-number-resolving, meaning the detector can distinguish the energy correlated to the absorption of not only a single photon (click detector), but energy correlated to the absorption of several photons. Figures 1 and 2 show the experimental results when detecting a pulsed coherent state with mean photon number of about 1 and wavelength of 1550 nm. Figure 1 shows the histogram of detected pulse heights for the pulsed coherent input state. Clear separation of individual photon peaks is achieved and up to 5 photons are resolved in the guided optical mode via absorption from the evanescent field into the TES. Figue 2 shows raw output traces of the evanescently coupled TES. The detection efficiency of a photon that is in the waveguide is 7.2 ± 0.5 %. The coupling efficiency from our laser source into the waveguide structure is 47.9 ± 5.2 %. The detection efficiency of these devices can be improved by elongating the detector along the waveguide structure to increase the absorption length. In addition, multiplexing several TESs along the waveguide will further increase the systems performance. Also, the waveguide core thickness can be reduced to increase the mode overlap of the guided mode with the detector. We are currently pursuing all of these approaches and will present our progress in developing these detectors with higher system detection efficiency.
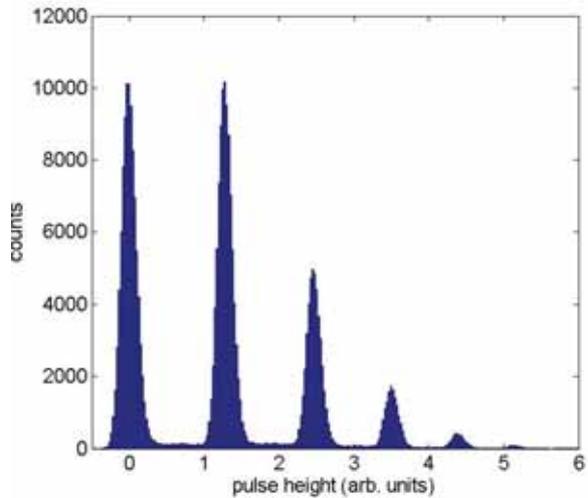
Figure 1: Photon pulse height distribution for a measured coherent state with a mean photon number of about 1.
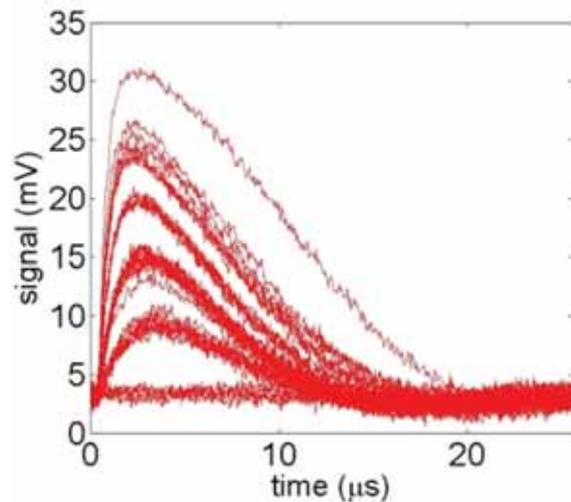
Figure 2: Electrical TES output traces for different numbers of photons in the weak laser pulse; the photon number resolving capability is clearly visible here

Quantum repeaters using frequency-multiplexed quantum memories

N. Sinclair[1], **E. Saglamyurek**[1], **H. Mallahzadeh**[1], **J. A. Slater**[1], **J. Jin**[1], **C. Simon**[1], **D. Oblak**[1], **M. George**[2], **R. Ricken**[2], **W. Sohler**[2], and **W. Tittel**[1]

[1]*Institute for Quantum Information Science and Department of Physics & Astronomy, University of Calgary, Canada.*
[2]*Department of Physics - Applied Physics, University of Paderborn, Germany*

The ability to send quantum information encoded into photons over large distances is hampered by unavoidable loss in the communication channel. In classical communication, this is alleviated by amplifying the information. However, as described by the no-cloning theorem, this approach is not viable for quantum information. Instead, long-distance quantum communication relies on quantum-repeaters [1, 2], which allow distributing entanglement over the entire channel by means of entanglement swapping across subsections. To synchronize this procedure in adjacent subsections, quantum repeaters must incorporate quantum memories [3] – devices that allow storing (entangled) quantum states until needed. Many different approaches to quantum state storage have been proposed, and experimental progress during the past few years has been fast. An interesting approach, which has recently been shown to allow storage of entangled states of light [4, 5], is based on atomic frequency combs (AFCs) and a photon-echo-type light-atom interaction [6]. However, despite a first proof-of-principle demonstration [7], recall on demand remains a challenge for such AFC quantum memories.

In this talk we will show that storage and synchronized re-emission of photons that arrive at different times can be replaced by storage of simultaneously arriving, frequency multiplexed photons and recall on demand in the frequency domain. Furthermore, employing a Tm-doped $LiNbO_3$ waveguide cooled to 4 K [5, 8], we will demonstrate such storage with attenuated laser pulses at the few-photon level. This removes one further obstacle to building quantum repeaters using rare-earth-ion doped crystals as quantum memory devices.

References

[1] H.-J. Briegel, et al., Phys. Rev. Lett. **81**, 5932 (1998).

[2] N. Sangouard, et al., Rev. Mod. Phys. **83**(1), 33 (2011).

[3] A. I. Lvovsky, B. C. Sanders, and W. Tittel, Nat. Photon. **3**(12), 706 (2009).

[4] C. Clausen, et al., Nature **469**, 508 (2011).

[5] E. Saglamyurek, et al., Nature **469**, 512 (2011).

[6] M. Afzelius, et al., Phys. Rev. A **79**, 052329 (2009).

[7] M. Afzelius, et al., Phys. Rev. Lett. **104**, 040503 (2010).

[8] N. Sinclair, et al., J. Lumin. **130**(9), 1586 (2010).

Entangbling - Quantum correlations in room-temperature diamond

Ian A Walmsley[1], **J. Nunn**[1], **K. C. Lee**[1], **M. Sprague**[1], **B. J. Sussman**[2]

[1] *University of Oxford, Department of Physics, Clarendon Laboratory, parks Rd, Oxford, OX1 3PU, United Kingdom*
[2] *National Research Council, Ottawa, Canada*

We demonstrate entanglement between the vibrations of two macroscopic, spatially-separated diamonds at room temperature by means of off-resonant Raman scattering of ultrashort optical pulses and quantum erasure.

The familiar world of everyday objects has at its heart a fitful, counter-intuitive microworld in which things may be in two places at once and may be tied more closely than identical twins. Yet, as Schrodinger noted in his famous cat gedanken experiment, this is not something that seems to translate into common experience in the normal world. Perhaps the most enigmatic quantum phenomena are correlations, such as entanglement, between separate entities underpin phenomena that run counter to our classical intuition of usual macroscopic objects. Such correlations also provide an important resource for quantum communication and quantum computing. Quantum correlations are not easy to produce under ambient laboratory conditions, especially in matter, since decoherence rapidly degrades the quantum states in which they may be present. This is especially true for solid-state materials, where the coupling between elementary excitations and other degrees of freedom is especially strong [1, 2] . Thus it remains a challenge to harness quantum phenomena for applications using room-temperature solids.

In order to generate and observe quantum correlations in solids, it is necessary to work rapidly and access material excitations that have little chance of being excited by the environment. At room temperature, quantum effects degrade rapidly in solids. Therefore working at very short timescales, using very energetic material excitations, is key. Using such an approach we have been able to show entanglement between the motion of two macroscopic, solid-state objects at room temperature [3]. In particular, we entangles the optical phonon modes of two pure, bulk samples of chemical-vapour-deposition-grown diamond. This is achieved by means of Raman scattering of ultrashort optical pulses, by which a phonon is generated and detected [4], and quantum erasure of the origin of the corresponding scattered Stokes photon [5]. Detection of an anti-Stokes photon verifies the entanglement [6] by reading-out the single phonon from the pair of diamonds. Because the optical pulses are so brief (approx 100 fs duration), both write and read steps take place before the phonon decoheres (which takes about 10 ps). This approach draws quantum phenomena closer to the human scale and offering a novel platform for studying macroscopic quantum phenomena at ambient conditions. For applications in quantum information processing, for instance optical phonons in diamond may be useful in a chip-scale integrated diamond architecture [7].

Figure 1: Main: Set up for generating entanglement between two separate bulk diamonds. Orthogonally polarized write and read pulses generate and probe a single phonon distributed across two diamonds by means of Raman scattering. Inset: One of the diamonds compared to a 5p coin.

References

[1] F. C. Waldermann, B. J. Sussman, J. Nunn *et al.*, Phys. Rev. B, 78, 155201 (2008).

[2] K. C. Lee, B. J. Sussman, J. Nunn et al., Diam. Relat. Mat., 19, 1289 (2010).

[3] K. C. Lee, M. R. Sprague, B. J. Sussman, et al., Science , 334 1253 (2011).

[4] K. C. Lee, B. J. Sussman, M. R. Sprague et al., Nat. Phot., 6, 41 (2012).

[5] L. M. Duan, M. Lukin,, J. Cirac, and P. Zoller, Nature 414, 413418 (2001).

[6] S. van Enk, N. Lutkenhaus and H. J. Kimble, Physical Review A 75(5), 052318 (2007).

[7] e.g. A. Faraon, P. E. Barclay, C. Santori, K.-M. Fu and R. G. Beausoleil, Nat Phot. 5, 301 (2011).

A long lived AFC quantum memory in a rare earth doped crystal.

Nuala Timoney, Imam Usmani, Mikael Afzelius and Nicolas Gisin

Group of applied physics, Univiersity of Geneva, CH-1211 Geneva 4, Switzerland

Quantum communication provides a platform for provably secure communications. The fact that a quantum state cannot be copied is the reason why quantum communication is secure but also limits the distance over which quantum communication can be performed. This obstacle is overcome by a quantum repeater scheme. An essential part of this scheme is a quantum memory - where a photonic quantum state can be stored and retrieved at a time determined after the storage - a so called on demand memory [1].

A potential scheme for implementing such a memory is the atomic frequency comb (AFC) [2]. The spectral separation (Δ) of the teeth of a comb of atoms determine the storage time of $1/\Delta$. A sample comb is shown in the state $|g\rangle$ in figure 1. Recent results using this scheme include heralded entanglement of two crystals. However this experiment and its precursors did not involve an on demand read out or particularly long storage times (33 ns) [3].

A complete AFC scheme involves transferring the optical coherence to a spin coherence before the time $1/\Delta$ has elapsed. The time evolution of this scheme is shown in the lower part of figure 1. To date such experiments have been hampered by the inhomogeneous spin broadening of the material, the longest times reported are of the order of 10 μs [4].

Here we report storage times almost an order of magnitude larger, using a $^{151}Eu^{3+}Y_2Si_2O_5$ crystal. This is due to the smaller inhomogeneous spin linewidth (γ_{IS}) of the material. The decay of the echo which has been stored in the spin state is shown in figure 2. The inhomogeneous spin broadening does not cause a hard limit for the storage time in rare earth doped crystals. It is known that RF refocussing pulses will increase the storage time to the T_2 of the spin transition [5]. The T_2 of a $^{151}Eu^{3+}Y_2Si_2O_5$ crystal has been mesured to be 15.5 ms [6]. The smaller inhomogeneous spin linewidth means that less bandwidth is required of future refocussing pulses, reducing the technical challenges of future experiments. Also in future experiments, we aim to perform this experiment at a single photon level.

References

[1] N. Sangouard et al., *Rev. Mod. Phys.*, 83(1):33–34, March 2011.

[2] M. Afzelius et al, *Phys. Rev. A*, 79:052329,2009.

[3] I. Usmani et al., *Nat. Photon.* 6:234, 2012

[4] M. Afzelius et al., *Phys. Rev. Lett.*, 104:040503, 2010. *and* Timoney et al., *J Phys. B*, *T*o appear

[5] K. Heshami et al.,*Phys. Rev. A* 83:032315, 2011

[6] A. L. Alexander et al., *J. Opt. Soc. Am. B*, 24(9):2479, 2007.
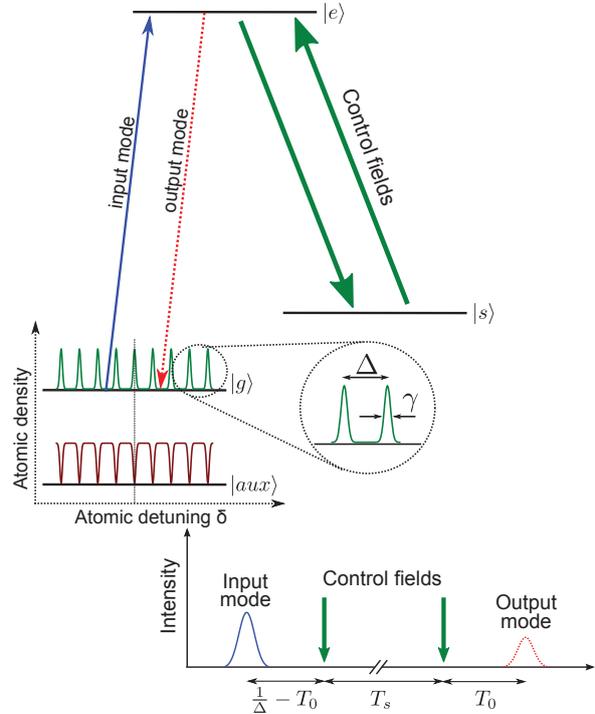
Figure 1: This figure shows a sample atomic system on which a complete AFC scheme can be performed. The lower figure shows the time evolution of an AFC scheme, as discussed in the text.
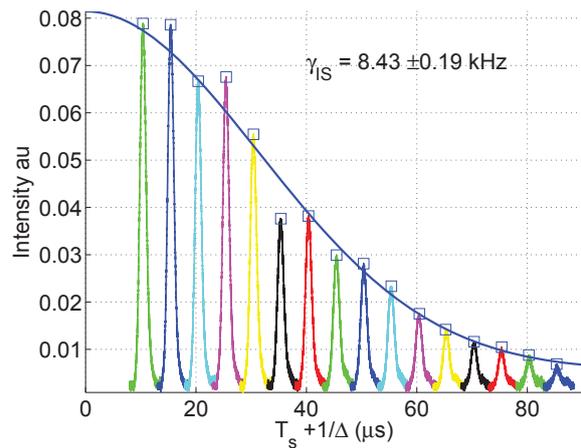
Figure 2: In this figure the decay of the spin stored echo is shown for an AFC where $1/\Delta = 5$ μs. The x axis shows the total storage time. The decay is due to the inhomogeneous spin linewidth, which is measured to be 8.43 ± 0.19 kHz.

Quantum Information Network based on NV Diamond Centers

Kae Nemoto[1], Mark S. Everitt[1], Simon J. Devitt[1], A. M. Stephens[1], Michael Trupke[2], Jörg Schmiedmayer[2], and W.J. Munro[3]

[1]*National Institute for Informatics, 2-1-2, Hitotsubashi, Chiyoda-ku, Tokyo, Japan*
[2]*Vienna Center for Quantum Science and Technology, Atominstitut, TU Wien, 1020 Vienna, Austria*
[3]*NTT Basic Research Laboratories, NTT Corporation,3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, 243-0198, Japan*

In recent years, NV centers in diamond has attracted significant attention as a candidate for quantum information devices showing promising quantum features such as easy manipulation and a long coherent time. The negatively charged NV center (NV-), in particular, has been intensely investigated [1]. NV- centers host an electron spin qubit with several nuclear spins around the vacancies. The ground state of the electron spin qubit has a long coherence time and an optical transition at 637nm, which can facilitate an interface between matter and optical qubits. The nuclear spins around the vacancies may be considered as a long-lived quantum memory. The natural hyperfine coupling between the nuclear and electron spins is an interface for the nuclear spin memory. With these excellent quantum properties, NV centers have been used to theoretically propose designs for quantum information processing [2], while single photon emission and nuclear quantum memory [3] have been experimentally demonstrated. However, the properties of NV- centers are not always ideal, for instance the electron spins are not naturally qubits as they are in fact a $spin-1$ system and also the optical transition is not in the telecom band. Despite such disadvantages pure diamond has a simple structure, a vast transparency band ranging from the ultraviolet (220 nm) to the microwave regime and has a large number of different impurities. Hence we could expect that there properties can be improved with other impurities, while the well-characterized nature of NV-centers can be exploited to demonstrate to a scalable device for quantum information processing.

In this talk, we propose a hybrid quantum information device (depicted in Fig 1) based on a NV- center embedded in an optical cavity and illustrate its use for quantum communication. Our model has experimental advantages, and encapsulates the important physics intrinsic to these types of devices. Here the electron spin qubit is an interface between light and matter qubits, and the nuclear spin coupled with the electron spin at the NV center can be used as a long-lived quantum memory. A single photon comes from the left of the cavity in the figure and is conditionally reflected or transmitted dependent on the state of the electron spin qubit. After this interaction, the single photon and electron spin qubit are entangled, giving a valuable resource for quantum information processing. The optical part is responsible for creating entanglement between remote devices. With this distributed nature, the hybrid device alone allows us to construct an efficient quantum information network. The generated entanglement will be transferred to the electron spin qubit in different cavities by linear-optical gate processing. The entanglement can be stored on the nuclear spin via the electron-nuclear spin coupling. The last two processes can be swapped depending on the applications. For instance, if optical quantum signal needs to travel a long distance, the storage process needs to be done first. The nuclear-spin memory enable us to store

entangled states, of which properties can be tailored by the system protocols run on each NV center. For long distance communication, the entangled pairs will be used to run quantum repeater protocols. Furthermore, the entanglement can be stored in order to create a 3D-cluster state, which is the resource for measurement based topological computation.
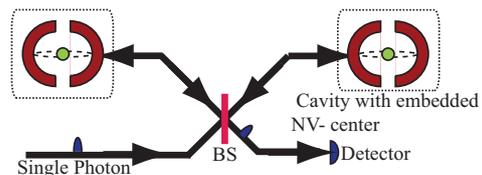

Figure 1: Schematic representation of an NV center based cavity device. The input light will be either transmitted or reflected dependent on the state of the electron spin qubit.

This model has a clear advantage by being a hybrid system of both light and matter. The single photons can travel long distance with low decoherence, and so a system made of many of this devices can distribute quantum information over long distances. The hybrid and distributed nature of this model also gives us the flexibility to merge quantum communication and computation, which is an ideal fundamental building block for quantum information networks. Photon loss can however be a concern, but by utilizing the nature of both cluster states and coupling between nuclear and electron spins, we can develop a protocol to maintain quantum coherence of the states stored in nuclear spin. Even when the natural coupling is always on, we can tolerant photon loss at high rate by compensating for photon loss at the expense of the clock speed of the quantum information system. The second advantage of this model is in its implementation. Several of the physical processes in the device have been already been experimentally demonstrated. Although more experimental efforts are necessary, the calculated physical requirements are feasible. One of the advantages of this scheme in comparison to existing schemes is that unlike emitter based schemes, our model avoids excitation of the electron spin qubit. This in turn reduces catastrophic errors and significantly simplifies any error behavior. Finally, the most important aspect of this device is its scalability. The device structure is closed and has a module nature. We will sketch out in this talk a scalable architecture for this device, and demonstrate its scalability.

References

[1] Michael Trupke et.al, Progress in informatics, No.8, pp. 33-37,(2011), and also see the references in this article.

[2] N. Y. Yao et.al, Phys. Rev. Lett. 106, 040505, (2010).

[3] E. Togan et.al, Nature (London) 466, 730 (2010).

Hybrid quantum information processing

Akira Furusawa[1]

[1] *The University of Tokyo, Tokyo, Japan*

There are two types of schemes for quantum information processing (QIP). One is based on qubits, and the other is based on continuous variables (CVs). When we make an optical QIP, both of them have advantages and disadvantages. In the case of qubits, although the fidelity of operations is very high, the experiments presented so far are mostly based on postselection because of low quantum efficiencies of creation and detection of single-photon-based qubits. On the other hand, CV QIP is deterministic with high-quantum-efficiency homodyne measurements, however, the fidelity of operations is not so high because perfect fidelity needs infinite energy.

In order to combine advantages of both schemes, "hybrid" approach is proposed [1] . One example is qubit teleportation with a CV teleporter [2, 3]. The big advantage of the hybrid scheme is determinism coming from CV teleportation [4], which enables us full Bell measurements at sender Alice. However, the experimental realization was too demanding when the proposal was made in early 2000's.

There were a couple of difficulties for the realization. First, we need very high level of squeezing for resource entanglement to teleport photonic qubits, which are highly nonclassical states. The world record of squeezing at that time was 6dB [5] and it was not enough for such teleportation. We tried to find a new nonlinear crystal to make highly squeezing and finally got 9dB of squeezing with periodically poled $KTiOPO_4$ [6], which is enough for the CV teleportation. Note that now the world record is 11.7dB with the same nonlinear crystal, realized by Hannover's group [7].

Second, since we have to use a photon-counting device like an avalanche photo diode to create single-photon-based qubits, the state inevitably becomes a wave packet, i.e., a pulse, which has a broad bandwidth in frequency domain. Conventional CV teleporters work upon the single mode picture that means they only work upon a narrow band [4]. Therefore we could not teleport a wave packet by using a conventional setup of CV teleporters. In order to break through such difficulty, we tried to broaden the bandwidth of CV teleporters. We first broadened the bandwidth of entanglement [8] and then teleported highly nonclassical wave packets of light with the broadband and high level of entanglement [9]. So it is ready for the hybrid teleportation.

Although the proposals of qubit teleportation with a CV teleporter handle polarized single photons, i.e., polarization qubits [2, 3], we are now trying to use time-bin qubits, which is superposition of a single photon in two temporal bins; $c_0|1,0\rangle + c_1|0,1\rangle$. The reason why we use the time-bin qubits is that we can teleport them with a single CV teleporter, while we need two CV teleporters for polarization qubits. Figs. 1 and 2 show our experimental setup for creation of time-bin qubits and an example of density matrix of the qubit, respectively [10]. Here, the time-bin qubits are characterized with dual-homodyne measurements and it follows that the qubits are compatible with a CV teleporter, which relies on homodyne measurements. We are now trying to teleport them with the same teleporter for highly nonclassical wave packets of light [9].

On top of the experiment, we are pursuing the possibility of hybrid QIP, especially of teleportation-based one. As an example, we have succeeded in squeezing a single photon by using a teleportation-based squeezer, which is a typical CV QIP.
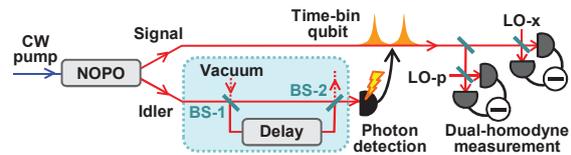
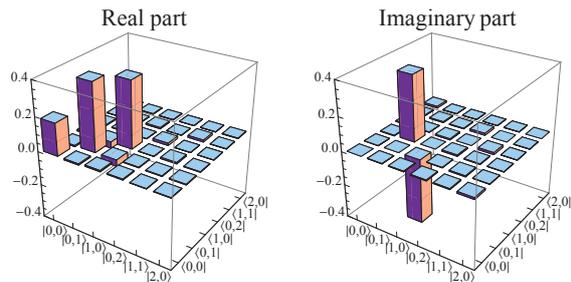Figure 1: Experimental setup for creation of time-bin qubits.

Figure 2: Density matrix of the created time-bin qubit $(|1,0\rangle - i|0,1\rangle)/\sqrt{2}$ [10].

References

[1] A. Furusawa and P. van Loock, *Quantum Teleportation and Entanglement: A Hybrid Approach to Optical Quantum Information Processing* (Wiley-VCH, Weinheim, 2011)

[2] T. Ide, *et. al.*, Phys. Rev. A, **65**, 012313 (2001).

[3] A. Dolińska, *et. al.*, Phys. Rev. A, **68**, 052308 (2003).

[4] A. Furusawa, *et. al.*, Science **282** 706 (1998).

[5] E. S. Polzik, J. Carri, and H. J. Kimble, Appl. Phys. B **55**, 279 (1992).

[6] Y. Takeno, *et. al.*, Opt. Exp. **15**, 4321 (2007).

[7] T. Eberle, *et. al.*, Phys. Rev. Lett. **104**, 251102 (2010).

[8] N. Takei, *et. al.*, Phys. Rev. A **74**, 060101(R) (2006).

[9] N. Lee, *et. al.*, Science **332**, 330 (2011).

[10] S. Takeda, *et. al.*, arXiv:1205.4862 [quant-ph]

Back to the future: QND, BAE, QNC, QMFS, and linear amplifiers

Carlton M. Caves

Center for Quantum Information and Control, University of New Mexico, MSC07-4220, Albuquerque, New Mexico 87131-0001, USA
Center for Engineered Quantum Systems, University of Queensland, Brisbane, QLD 4072, Australia

Various strategies have been devised for circumventing naïve quantum limits on the detection of a classical force acting on a linear system. These strategies are variously described as measuring a quantum nondemolition (QND) observable [1, 2, 3], employing back-action evasion (BAE) [1, 2, 3], or using quantum noise cancellation (QNC) [4, 5]. Recently these various strategies have been unified underneath a new umbrella, called a *quantum-mechanics-free subspace* (QMFS) [6]. In a QMFS, a set of positions and momenta, all of which commute, can undergo arbitrary dynamics, without any quantum noise; if observables in the QMFS are measured, all of the quantum back action is diverted onto conjugate positions and momenta, whose dynamics does not feed back onto the observables of the QMFS.

The simplest example of a QMFS is that of a quadrature component corresponding to the blue and red sidebands of a carrier frequency. This simplest QMFS is exploited in the broadband squeezed light that has been developed for and recently used in interferometric gravitational-wave detectors [7] and is the basis of a magnetometry experiment that evades back action by using two entangled atomic ensembles [8].

I will give a very brief introduction to QMFSs. Depending on what other talks are being given at QCMC, I will either proceed to a more detailed discussion of QMFSs, reporting on work carried out with M. Tsang, or I will segue to a discussion of quantum limits on noise in linear amplifiers.

Phase-sensitive linear amplifiers, which need not add noise to a signal [9], can be thought of as amplifying a signal encoded in the simple QMFS discussed above. Phase-preserving linear amplifiers, by contrast, amplify a signal encoded in a bosonic mode and thus are constrained by unitarity to add noise [9]. The standard, by now highly developed, discussion of quantum limits on phase-preserving linear amplifiers [9, 10] characterizes amplifier noise performance in terms of second moments of the added noise, i.e., in terms of noise temperature or noise power. The approach of Josephson-effect linear amplifiers to the fundamental quantum limit on noise temperature [11, 12] and the need to characterize quantum-limited experiments at microwave frequencies [13] has sparked renewed interest in low-noise linear amplifiers.

J. Combes, Z. Jiang, S. Pandey, and I have generalized the standard discussion to provide a complete characterization of the quantum-mechanical restrictions on the entire probability distribution of added noise. For a single-mode amplifier, one can show that, no matter how the amplifier is actually constructed, the added noise is characterized by the Wigner function of an ancillary mode that undergoes a two-mode squeezing interaction with the amplified mode. I will discuss this result, the methods used to prove it, bounds it places on moments of the added noise, and generalizations to more complicated scenarios.

References

[1] C. M. Caves *et al.*, "On the measurement of a weak classical force coupled to a quantum-mechanical oscillator. I. Issues of principle," Rev. Mod. Phys. **52**, 341 (1980).

[2] V. B. Braginsky, Y. I. Vorontsov, and K. S. Thorne, "Quantum nondemolition measurements," Science **209**, 547–557 (1980).

[3] V. B. Braginsky and F. Ya. Khalili, *Quantum Measurement* (Cambridge University Press, Cambridge, 1992).

[4] M. Tsang and C. M. Caves, "Coherent quantum-noise cancellation for optomechanical sensors," Phys. Rev. Lett. **105**, 123601 (2010).

[5] M. Tsang, H. M. Wiseman, and C. M. Caves, "Fundamental quantum limit to waveform estimation," Phys. Rev. Lett. **106**, 090401 (2011).

[6] M. Tsang and C. M. Caves, "Evading quantum mechanics," e-print arXiv:1203.2317.

[7] The LIGO Scientific Collaboration, "A gravitational-wave observatory operating beyond the quantum shot-noise limit," Nature Phys. **7**, 962-965 (2011).

[8] W. Wasilewski *et al.*, "Quantum noise limited and entanglement-assisted magnetometry," Phys. Rev. Lett. **104**, 133601 (2010).

[9] C. M. Caves, "Quantum limits on noise in linear amplifiers," Phys. Rev. D **26**, 1817–1839 (1982).

[10] A. A. Clerk *et al.*, "Introduction to quantum noise, measurement, and amplification," Rev. Mod. Phys. **82**, 1155–1208 (2010).

[11] N. Bergeal *et al.*, "Phase-preserving amplification near the quantum limit with a Josephson ring modulator," Nature **465**, 64–68 (2010).

[12] D. Kinion and J. Clarke, "Superconducting quantum interference device as a near-quantum-limited amplifier for the axion dark-matter experiment," Appl. Phys. Lett. **98**, 202503 (2011).

[13] C. M. Wilson *et al.*, "Observation of the dynamical Casimir effect in a superconducting circuit," Nature **479**, 376–379 (2011).

Minimax quantum tomography: the ultimate bounds on accuracy

Christopher Ferrie[1] **and Robin Blume-Kohout**[2]

[1]*Institute for Quantum Computing, University of Waterloo, Canada*
[2]*Sandia National Laboratories, Albuquerque NM*

There are many methods for *quantum state tomography* (e.g., linear inversion, maximum likelihood, Bayesian mean...). But none of them is clearly "the most accurate" for data of finite size N. Even the upper limits on accuracy are as yet unknown, which makes it difficult to say that a given method is "accurate enough". We address this problem here by (i) calculating the minimum achievable error for single-qubit tomography with N Pauli measurements, (ii) finding *minimax* estimators that achieve this bound, and (iii) comparing the performance of known estimators.

Quantum tomography (used to characterize the state or process produced in an experiment) proceeds in two steps: (1) measuring identically prepared systems in different bases to collect data D; and (2) approximating the state ρ by plugging the data into an **estimator** $\hat\rho(D)$. The estimator should (must) be accurate – i.e., have low expected error (or *risk*) for all true states. Some popular estimators (e.g. linear inversion, or maximum likelihood) have no provable accuracy properties for finite N. Others (Bayesian mean estimation) are provably optimal only on *average* over a particular ensemble of input states – which isn't particularly helpful, since device states in the laboratory are not selected at random.

Instead, estimators can be ranked by their *worst-case* risk – the maximum, over all ρ, of the expected error. The best-performing estimator by this metric is called the **minimax** estimator. Different error metrics (e.g., fidelity, trace-norm, etc.) yield different minimax estimators; here we focus on *relative entropy* error (the canonical choice in classical predictive estimation and machine learning). The minimax estimators for quantum tomography are strange, unwieldy, and impractical (see below), but they serve as a critical **benchmark**: a tomography algorithm is "good enough" inasmuch as its risk is close to that of the minimax estimator.

RESULTS: Our research produced four main results. **(1)** We constructed minimax estimators for reconstructing single-qubit states from $N = 2\ldots128$ measurements of the Pauli operators (σ_x, σ_y, σ_z), used them to get absolute lower bounds on achievable risk (Fig. 1a), and found that risk scales as $N^{-1/2}$ (for classical probabilities, risk scales as N^{-1}). **(2)** We compared the performance of minimax estimators to Bayesian mean estimation with a "flat" Hilbert-Schmidt prior, and hedged maximum likelihood (Fig. 1a). **(3)** We studied minimax estimators' state-dependent performance ("risk profile"; Fig. 1b) and the their associated *least favorable priors* (Fig. 1b, and see below). **(4)** We reproduced most features of quantum tomography, including $N^{-1/2}$ risk scaling, within a simple model called the "noisy coin".

DISCUSSION: The minimax estimator (optimal worst-case risk) is also the *Bayes* estimator (optimal *average* risk) for some distribution known as the *least favorable prior* (LFP). We constructed minimax estimators by numerical optimization over priors, and found that LFPs are always *discrete*

(Fig. 1b). This seems peculiar (if not insane), but using Monte Carlo sampling to find priors that are *almost* least favorable (Fig. 1b, small grey dots), showed that risk is relatively insensitive to fine details of the prior. So there are smooth priors that are almost least favorable. We also studied Bayes estimation with the simple and popular *Hilbert-Schmidt* prior, and found it significantly less accurate than minimax (Fig. 1a). A simple heuristic called *hedged maximum likelihood*[1] comes much closer to optimal accuracy for large N (Fig. 1a).
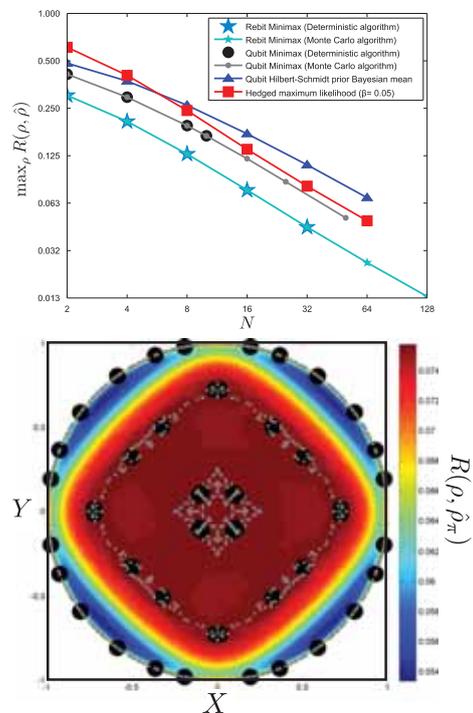

Figure 1: **TOP:** Minimax risk (worst-case expected error of the best possible estimator) for Pauli-measurement tomography on rebits and qubits, vs. the number of times each Pauli was measured (N). A deterministic algorithm (large black dots) provides tight error bounds, but Monte Carlo sampling (smaller grey dots) is far more efficient and nearly as accurate. Standard methods are also shown; Bayesian mean estimation with a Hilbert-Schmidt prior is outperformed by hedged maximum likelihood. **BOTTOM:** The minimax estimator's risk profile $R(\rho)$ for $N = 16$ Pauli measurements on a rebit. Dots indicate support points of the least favorable prior (LFP) as found by near-exact (black) and Monte Carlo (grey) algorithms. Although the two priors appear quite different, they have near-identical risk profiles ($\pm 1\%$ at most).

---

[1]*Un*-hedged MLE has infinite risk because it reports rank-deficient states.

Simultaneous Wavelength Translation and Amplitude Modulation of Single Photons from a Quantum Dot

Matthew T. Rakher[1,2], Lijun Ma[2], Marcelo Davanço[2], Oliver Slattery[2], Xiao Tang[2], and Kartik Srinivasan[2]

[1]*Universität Basel, Basel, Switzerland*

[2]*National Institute of Standards and Technology, Gaithersburg, United States*

The integration and coupling of disparate quantum systems is an ongoing effort towards the development of distributed quantum networks [1]. Impediments to hybrid schemes which use photons for coupling are the differences in transition frequencies and linewidths among different systems. Here, we use pulsed frequency upconversion to simultaneously change both the frequency and temporal amplitude profile of single photons produced by a semiconductor quantum dot (QD). Triggered single photons that have an exponentially decaying temporal profile with a time constant of 1.5 ns and a wavelength of 1300 nm are converted to photons that have a Gaussian temporal profile with a full-width at half-maximum (FWHM) as narrow as 350 ps and a wavelength of 710 nm. Photon antibunching measurements explicitly confirm that the quantum nature of the single photon stream is preserved. We anticipate that this combination of wavepacket manipulation and quantum frequency conversion will be valuable in integrating quantum dots with quantum memories [2].

We generate single photons at 1.3 μm from a single InAs QD embedded in a GaAs mesa. Pulsed excitation at 780 nm is introduced via single mode optical fiber into a liquid He flow cryostat at $\approx$7 K. There, the fiber's diameter is adiabatically reduced to $\approx$1 μm to form a fiber taper waveguide, which efficiently excites and collects photoluminescence (PL) from the QD. The PL from an excitonic transition is directed into the upconversion setup where it is combined with a strong 1550 nm pulse in a periodically-poled LiNbO$_3$ (PPLN) waveguide (Fig. 1(a)). The pulse is created by a tunable laser with an electro-optic modulator (EOM) that seeds an erbium-doped fiber amplifier. An electrical pulse generator drives the EOM synchronously with the 780 nm QD excitation laser, but at half the repetition rate. It generates pulses with controllable FWHM (τ_{mod}) and delay (ΔT_{mod}). The strong 1550 nm pulse ($\approx$ 100 μW average power) interacts with the QD single photon via quasi-phase-matched sum frequency generation in the PPLN waveguide. Light exiting the PPLN is spectrally filtered to remove background from the excitation and the pump laser. The 710 nm photons are detected by a Si single photon counting avalanche detector (SPAD) for time-resolved measurements, or are split at a 50:50 beamsplitter and detected by two Si SPADs for second-order correlation measurement ($g^{(2)}(\tau)$).

We measure $g^{(2)}(\tau)$ for photons that are upconverted using 500 ps pump pulses (Fig. 1(b)). The result is clearly antibunched with $g^{(2)}(0) < 0.5$, showing that the signal is dominantly composed of single photons. The non-zero value is mostly due to unwanted photons resulting from upconversion of anti-Stokes Raman photons from the strong 1550 nm beam [3]. Next, we perform time-resolved measurements of the 710 nm photons. Here, the pulsed 1550 nm pump not only upconverts the QD photon to 710 nm, but also modulates its
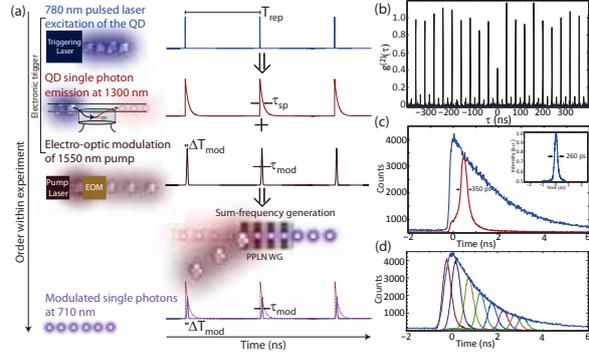
Figure 1: a) Schematic of experiment. b) $g^{(2)}(\tau)$ measurement. c) Temporal amplitude profile after upconversion. d) Amplitude profiles as ΔT_{mod} is varied.

temporal amplitude profile. Figure 1(c) displays the temporal amplitude profile of 710 nm single photons generated using a 1550 nm pulse with $\tau_{mod} = 260$ ps, along with that of single photons generated with a CW pump for comparison.

We also step the delay ΔT_{mod} between the 1550 nm pulse and 1300 nm QD single photon from 0.0 ns to 3.5 ns in steps of 500 ps with $\tau_{mod} = 260$ ps as shown in Fig. 1(d). The heights of the pulsed profiles nicely follow the exponential decay of the CW profile. This clearly indicates that, while the quantum nature of the photon has been inherited from the QD emission near 1300 nm, its temporal profile has been inherited from the strong pump pulse near 1550 nm. This is a direct consequence of the nonlinear nature of the upconversion process.

In summary, we have demonstrated quantum frequency upconversion of QD-generated single photons with a pulsed pump [4]. We showed that, while the upconverted photons have the same photon statistics as the original photons, the temporal amplitude profile is changed to match that of the classical pump. We measure Gaussian-shaped single photon profiles with FWHMs as narrow as 350 ps, limited by the electrical pulse generator. Such methods may prove valuable for integrating disparate quantum systems and for achieving high resolution in time-resolved experiments.

References

[1] H. J. Kimble, Nature **453**, 1023 (2008).

[2] K. F. Reim *et al*, Nature Photonics **4**, 218 (2010).

[3] M. T. Rakher *et al*, Nature Photonics **4**, 786 (2010).

[4] M. T. Rakher *et al*, Phys. Rev. Lett. **107**, 083602 (2011).

Friday talks abstracts

Quantum Atom Optics - single and two mode squeezing with Bose Einstein condensates

Markus Oberthaler[1]

[1] *Kirchhoff-Institute for Physics, Heidelberg, Germany*

In recent years a significant step forward in the direction of quantum atom optics has been undertaken. Especially Bose Einstein condensed atomic gases prove as a versatile experimental system which allows to probe and explore new regimes of quantum optics. This is mainly due to the high level of control of particle number as well as interaction. In this presentation we will report on the first implementation of atomic homodyning which allows for the detection of two mode entanglement generated in the process of spin changing collision - the physics is directly connected to the parametric down conversion known in the field of optics. Furthermore we will report on a novel way of dynamically generating spin squeezing atomic states by preparing an atomic sample at a classical unstable fixed point.

Relaxation and Pre-thermalization in an Isolated Quantum System

Tim Langen[1], **Michael Gring**[1], **Maximilian Kuhnert**[1], **Bernhard Rauer**[1], **Remi Geiger**[1], **Igor Mazets**[1], **David A. Smith**[1], **Takuya Kitagawa**[2], **Eugene Demler**[2], **Jörg Schmiedmayer**[1]

[1]*Vienna Center for Quantum Science and Technology, Atominstitut, TU Wien, Stadionallee 2, 1020 Vienna, Austria*
[2]*Harvard-MIT Center for Ultracold Atoms, Department of Physics, Harvard University, Cambridge, Massachusetts 02138, USA*

Understanding relaxation processes is an important unsolved problem in many areas of physics, ranging from cosmology to high-energy physics to condensed matter. These problems remain a challenge despite considerable theoretical and experimental efforts, and their difficulty is exacerbated by the scarcity of experimental tools for characterizing complex transient states. One scenario is that the relaxation process is governed by a single timescale during which all degrees of freedom approach equilibrium. An intriguing alternative phenomenon that has has been first suggested in the context of high-energy heavy ion collisions is pre-thermalization [1]. It predicts the rapid establishment of a quasi-stationary state that differs from the real thermal equilibrium of the system. In this context, systems of ultracold atoms provide unique opportunities for studying non-equilibrium phenomena in isolated quantum systems due to their perfect isolation from the environment and relaxation timescales that are easily accessible in experiments.

We employ measurements [2] of full quantum mechanical probability distributions of matter-wave interference contrast to study the relaxation dynamics of a coherently split 1d Bose gas and obtain unprecedented information about the dynamical states of the system. The evolution of the distributions clearly reveals the multi-mode nature inherent to 1d Bose gases and is in very good agreement with a theoretical description based on the Tomonaga-Luttinger liquid formalism [3, 4]. Following an initial rapid evolution, we observe the approach towards a thermal-like steady state characterized by an effective temperature that is independent from the initial equilibrium temperature of the system before the splitting process. Furthermore, this steady state retains a strong memory of the initial non-equilibrium state. We conjecture that it can be described through a generalized Gibbs ensemble and associate it with pre-thermalization.

References

[1] J. Berges, S. Borsanyi, and C. Wetterich, Phys. Rev. Lett. **93**, 142002 (2004)

[2] M. Gring, M. Kuhnert, T. Langen, T. Kitagawa, B. Rauer, M. Schreitl, I. Mazets, D. A. Smith, E. Demler, and J. Schmiedmayer, arXiv:1112.0013

[3] T. Kitagawa, S. Pielawa, A. Imambekov, J. Schmiedmayer, V. Gritsev, E. Demler, Phys. Rev. Lett. **104**, 255302 (2010)

[4] T. Kitagawa, A. Imambekov, J. Schmiedmayer, and E. Demler, New J. Phys. **13**, 073018 (2011)
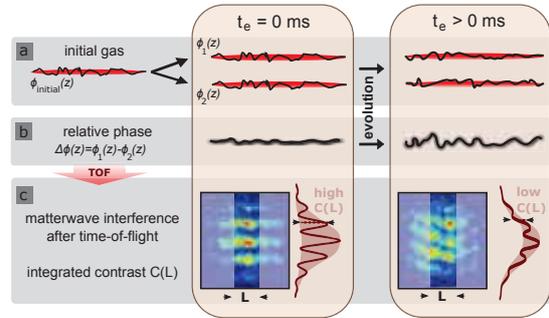
Figure 1: **Experimental scheme.** (a) An initial phase fluctuating 1d Bose gas is split into two uncoupled gases with almost identical phase distributions $\phi_1(z)$ and $\phi_2(z)$ (represented by the black solid lines) and allowed to evolve for a time t_e. (b) At $t_e = 0$ ms, fluctuations in the local phase difference $\Delta\phi(z)$ between the two gases are very small, but start to randomize during the evolution. It is an open question if and how this randomization leads to the thermal equilibrium situation of completely uncorrelated gases. (c) shows typical experimental matter-wave interference patterns obtained by overlapping the two gases in time-of-flight after different evolution times. Differences in the local relative phase lead to a locally displaced interference pattern. Integrated over a length L, the contrast $C(L)$ in these interference patterns is a direct measure of the strength of the relative phase fluctuations and therefore allows to directly probe the dynamics .
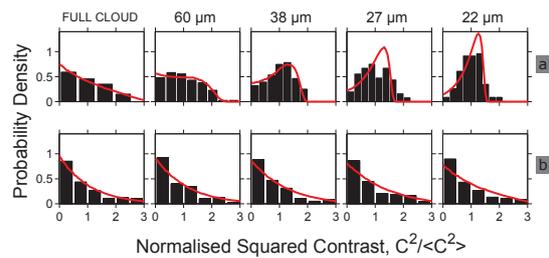
Figure 2: **Revealing the presence of a pre-thermalized state.** (a) Experimental *non-equilibrium distributions* (histograms) of the matterwave interference contrast after an evolution time of $t_e = 27$ ms. The solid red lines show theoretical *equilibrium* distributions with an effective temperature of 14 nK, which is significantly lower than the true initial temperature of the gas (120 nK). The pre-thermalized nature of the state is clearly revealed by comparing to the vastly different true thermal equilibrium situation shown in (b), which can be prepared by creating two completely independent 1d Bose gases.

Error-disturbance uncertainty relation studied in successive spin-measurements

Jacqueline Erhart[1], Stephan Sponar[1], Georg Sulyok[1], Gerald Badurek[1], Masanao Ozawa[2] and Yuji Hasegawa[1]

[1]*Atominstitut, Vienna University of Technology, Austria;* [2]*Graduate School of Information Science, Nagoya University, Japan*

The uncertainty relation was first proposed by Heisenberg in 1927 as a limitation of simultaneous measurements of canonically conjugate variables owing to the back-action of the measurement[1]: the measurement of the position Q of the electron with the error $\epsilon(Q)$, or 'the mean error', inevitably induces the disturbance $\eta(P)$, or 'the discontinuous change', of the momentum P so that Heisenberg insisted that they always satisfy the relation

$$\epsilon(Q)\eta(P) \sim \frac{\hbar}{2}. \quad (1)$$

Afterwards, Robertson derived another form of uncertainty relation for standard deviations $\sigma(A)$ and $\sigma(B)$ for arbitrary pairs of observables A and B as

$$\sigma(A)\sigma(B) \geq \frac{1}{2}|\langle\psi|[A, B]|\psi\rangle|. \quad (2)$$

This relation has a mathematical basis, but has no immediate implications for limitations on measurements. The proof of the reciprocal relation for the error $\epsilon(A)$ of an A measurement and the disturbance $\eta(B)$ on observable B caused by the measurement is not straightforward. Recently, rigorous and general theoretical treatments of quantum measurements have revealed the failure of Heisenberg's relation (eq.1), and derived a new universally valid relation [2, 3] given by

$$\epsilon(A)\eta(B)+\epsilon(A)\sigma(B)+\sigma(A)\eta(B) \geq \frac{1}{2}|\langle\psi|[A, B]|\psi\rangle|. \quad (3)$$

Here, the error $\epsilon(A)$ is defined as the root mean squared (r.m.s.) of the difference between the output operator O_A actually measured and the observable A to be measured, whereas the disturbance $\eta(B)$ is defined as the r.m.s. of the change in observable B during the measurement.
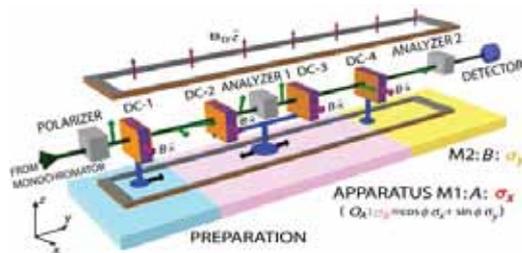
Figure 1: Neutron optical test of error-disturbance uncertainty relation.

We have experimentally tested the universally valid error-disturbance relation (eq.3) for neutron spin measurements [4]. Experimental setup is depicted in Fig.1. We determined experimentally the values of error $\epsilon(A)$ and the disturbance $\eta(B)$. A trade-off relation between error and disturbance was clearly observed, which is plotted in Fig.2.
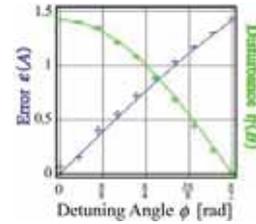
Figure 2: Trade-off relation between error and disturbance.

From the experimentally determined values of error $\epsilon(A)$, disturbance $\eta(B)$, and the standard deviations, $\sigma(A)$ and $\sigma(B)$, the Heisenberg error-disturbance product $\epsilon(A)\eta(B)$ and the universally valid expression, that is, the left-hand side of eq.3, are plotted in Fig.3. This figure clearly illustrates the fact that the Heisenberg product is always below the (expected) limit and that the universally valid expression is always larger than the limit in our experiment. This demonstration is the first evidence for the validity of the new relation (eq.3) and the failure of the old naive relation is illustrated. This experiment confirms the solution of a long-standing problem of describing the relation between measurement accuracy and disturbance and sheds light on fundamental limitations of quantum measurements.
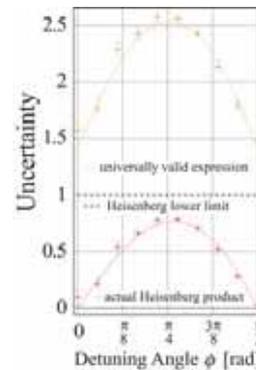
Figure 3: Experimentally determined values of the Heisenberg product and the three-term sum (eq.3).

References

[1] J.A. Wheeler and W.H. Zurek (eds) *Quantum Theory and Measurement* (Princeton Univ. Press, 1983).

[2] M. Ozawa, Phys. Rev. A **67**, 042105 (2003).

[3] M. Ozawa, Ann. Phys. **311**, 350–416 (2004).

[4] J. Erhart, S. Sponar, G. Sulyok, G. Badurek, M. Ozawa and Y. Hasegawa, Nature Physics **8**, 185-189 (2012).

Quantum Money with Classical Verification

Dmitry Gavinsky
NEC Laboratories America, Princeton, U.S.A.

*We propose and construct a quantum money scheme that allows verification through **classical** communication with a bank, this gives the first demonstration that a secure quantum money scheme exists that does not require quantum communication for coin verification.*
*Our scheme is secure against **adaptive** adversaries – this property is not directly related to the possibility of classical verification, nevertheless none of the earlier quantum money constructions is known to possess it.*

In 1983 Wiesner [Wie83] proposed a new quantum cryptographic scheme, that later became known as *quantum money*. Informally, a *quantum coin* is a unique object that can be created by a trusted *bank*, then circulated among untrusted *holders*. A holder of a coin should be able to verify it, and the verification must confirm that the coin is authentic if it has been circulated according to the prescribed rules. On the other hand, if a holder attempts to counterfeit a coin, that is, to create several objects such that each of them would pass verification, he must fail in doing so with overwhelmingly high probability.

Wiesner demonstrated that quantum mechanics (as opposed to classical physics) allowed money schemes. The basic principle that made such constructions possible was that of *quantum uncertainty*, stating that there were properties of a quantum object known to its "manufacturer" that couldn't be learnt by an observer who measured the object. It turned out that some of such properties could be later "verified" by the manufacturer; accordingly, a bank could prepare objects with this type of "secret properties", letting the holders use them as quantum coins. Not knowing the secrets, untrusted holders were not able to forge counterfeits.

In Wiesner's original construction [Wie83, BBBW83], a coin had to be sent back to the bank in order to get verified. This could be viewed as a possible drawback: a coin might get "stolen", or intentionally "ruined" by an adversary who had access to the communication channel between a coin holder and the bank. This problem has been addressed in a number of works (cf. [TOI03, Aar09, LAF+10, FGH+10, MS10, AC12]), but no satisfactory solution has been found yet.

Relatively recently another limitation of all previously known quantum money schemes has been noticed [Aar09, Lut10]: An adversary can gain more power from interacting with the bank *adaptively*. Prior to our work, no quantum money scheme was know to be resistant to adaptive attacks.

Our results

In [Gav12] we are proposing to use *classical communication with a bank* in order to verify a quantum coin. We construct such a scheme. This demonstrates, for the first time, that *a secure quantum money scheme exists that does not require quantum communication for coin verification.*

Some advantages of our construction over the previously known ones are:

- Unlike the original scheme of Wiesner and the constructions in [MS10], *our construction does not require quantum communication with a bank* in order to verify a coin.

- We *prove* that our scheme is (unconditionally) secure. Security arguments for schemes with local verification (as proposed in [Aar09, LAF+10, FGH+10, AC12]) require either unproved hardness assumptions or a major mathematical breakthrough (complexity lower bounds). Moreover, to the best of our knowledge, no such scheme has been shown to be secure under so-called "widely believed" unproved assumptions.

- Unlike the schemes with local verification, our construction remains *secure against computationally unlimited adversary* who obeys the laws of quantum mechanics.

Besides offering possible practical advantages, the concept of quantum money with classical verification gives rise to natural and attractive theoretical questions.

Another advantage of our construction is not directly related to the possibility of quantum verification:

- Our scheme remains secure against an adversary who uses *adaptive multi-round attacks*; no such scheme was known before.

This work was published as

Laser damage of photodiodes helps the eavesdropper

Audun Nystad Bugge[1], **Sebastien Sauge**[2], **Aina Mardhiyah M. Ghazali**[3], **Johannes Skaar**[1,4], **Lars Lydersen**[1,4] and **Vadim Makarov**[5]

[1]*Department of Electronics and Telecommunications, Norwegian University of Science and Technology, Trondheim, Norway*
[2]*School of Information and Communication Technology, Royal Institute of Technology (KTH), Kista, Sweden*
[3]*Department of Science in Engineering, Faculty of Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia*
[4]*University Graduate Center, Kjeller, Norway*
[5]*Institute for Quantum Computing, University of Waterloo, Waterloo, Canada*

Quantum key distribution, although secure in principle, suffers from discrepancies between the simplified model of apparatus used in its security proof, and the actual hardware being used. Often, such discrepancies can be exploited by an eavesdropper to steal the secret key.

One of the assumptions about the apparatus made in the security proof is that the eavesdropper, in general, *cannot* arbitrarily and permanently change the characteristics of the legitimate parties' apparatus. Here we disprove this assumption experimentally, by permanently damaging and thus changing the photonic and electrical characteristics of silicon avalanche photodiodes using high-power illumination. Such one-time change can open the quantum key distribution system to eavesdropping.

We exposed PerkinElmer C30902SH silicon avalanche photodiodes to a focused 807 nm continuous-wave laser radiation at a range of powers up to 3 W [1]. The photodiodes were characterized between exposures. After about 1 W power, the photodiodes permanently developed a large dark current, which made them blind to single photons in a passively-quenched detector scheme, yet deterministically controllable by bright light pulses, allowing eavesdropping [2]. Above 1.7 W power exposure, the photodiodes lost photosensitivity and became electrically either a resistor or an open circuit, accompanied by visible structural changes (Fig. 1).

This attack immediately applies to quantum key distibution schemes operating over a free-space channel. Future studies should investigate laser damage to actively-quenched avalanche photodetectors, optical scheme components other than photodiodes, various fibre-optic components, as well as contermeasures to this new class of attacks.

References

[1] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen and V. Makarov, *unpublished*.

[2] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer and V. Makarov, Nat. Commun. **2**, 349 (2011).
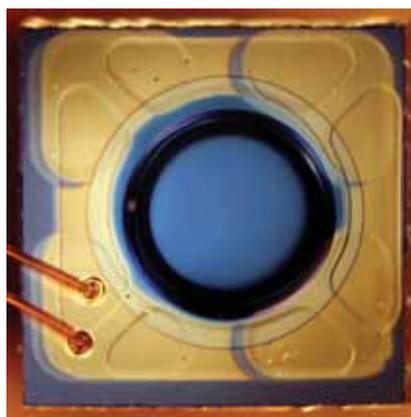
(a)
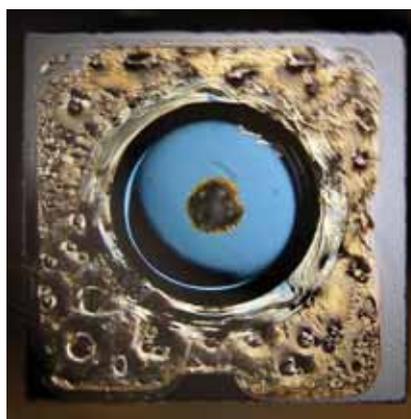
(b)

Figure 1: Microscope images of PerkinElmer C30902SH avalanche photodiode. **(a)** undamaged photodiode (bright field illumination). **(b)** photodiode after exposure to 3 W focused light for 60 s. A hole melted through the chip in the center, and the gold electrode melted (photodiode sample different from image (a); dark field illumination).

Self-testing quantum cryptography

Charles Ci Wen Lim[1], Christopher Portmann[1,2], Marco Tomamichel[2], Renato Renner[2] and Nicolas Gisin[1]

[1]*Group of Applied Physics, University of Geneva, Switzerland*
[2]*Institute for Theoretical Physics, ETH Zurich, Switzerland*

Device-independent quantum key distribution (QKD) allows the users (traditionally called Alice and Bob) to generate provably secure cryptographic keys as long as the observed statistics violate a Bell's inequality. In other words, full knowledge of the devices is not required for the security. However, if one considers a lossy channel, then the problem of detection loophole problem arises. More specifically, the global detection efficiency (the probability that Bob receives a valid output given that Alice sends something) must be sufficiently high, otherwise provably secure device-independent QKD is not possible. Note that the feasibility of device-independent QKD is still limited by the channel loss (at most $\sim$ 4km), even if one trusts the classical devices, e.g., efficiencies of the detectors are characterized. The main reason for this impasse lies in the configuration of device-independent QKD: Alice and Bob have to perform a Bell test across communication distances. Clearly, we have reached a situation whereby trusting the efficiencies of the detectors is still not enough.

In this work, we propose and provide the security proof (including the finite key analysis [1]) for a self-testing QKD protocol that allows Alice and Bob to perform Bell tests locally. The protocol consists of two parts: (1) certification of prepared states [2] and (2) key generation engine [3, 4]. In the following, we briefly explain the operations.

Certification of prepared states.— Alice and Bob each hold a self-testing source, a device that is supposed to produce BB84 states: it internally outputs an entangled bipartite state and the user can choose to perform either the CHSH test on it or to measure one half in either the Z or X basis, and send the other half on the quantum channel. By randomly sampling some bipartite states for the CHSH test, the user can estimate the quality of the preparation process. For instance, if the user observes a CHSH violation of $2\sqrt{2}$, then the preparation process necessarily correspond to the correct BB84 preparation. We note that the devices in the self-testing source setup are arbitrary and only the knowledge of the CHSH violation is required for the assessment of the prepared states.

Key generation engine.—The prepared states from Alice and Bob are sent to an untrusted central station (ideally, performs a Bell state measurement) which outputs a flag (pass or fail). Conditioned on the passing events, Alice and Bob publicly announce their basis choice and identify two sets of data $\mathcal{Z}$ and $\mathcal{X}$ which correspond to the sifted data in the bases Z and X, respectively. For the unsuccessful events, they discard

the data. Let basis Z be the key generation basis, then with the generalized entropic uncertainty relation [5] and the connection to the observed CHSH value, one can show that the secret key rate (in the asymptotic limit) is

$$R = 1 - \log \Omega(\max\{S_A, S_B\}) - 2\mathrm{h}(\delta) \qquad (1)$$

where $\Omega : x \to 1 + x\sqrt{8-x^2}/4$ and h is the binary entropy function. The parameters S_A and S_B are the observed CHSH violations for Alice and Bob, respectively. For simplicity, we let the error rate in (1) be identical, i.e., $\delta_\mathsf{Z} = \delta_\mathsf{X} = \delta$.

Comparison to device-independent QKD.— We also compare the asymptotic performances of self-testing QKD and device-independent QKD [6]. The quantum channel is assumed to be a depolarizing channel parameterized by the error rate δ and the local CHSH violations are assumed to be identical. From Figure 2, we note that for high local CHSH
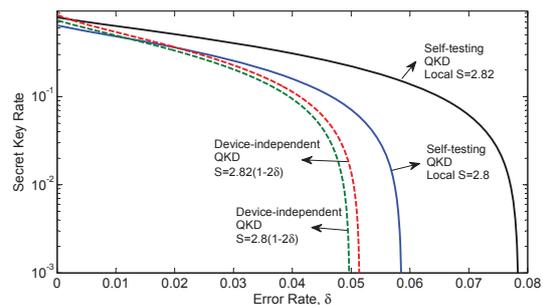

Figure 2: Comparison against [6], assuming that the quantum channel is a depolarizing channel with an error rate δ.

violations, the key rates of self-testing QKD are better. Most importantly, self-testing QKD is not limited by the channel loss and can be used for large communication distances.

Figure 1: Self-testing QKD configuration.

References

[1] M. Tomamichel, C. C. W. Lim, N. Gisin and R. Renner, Nat. Commun. **3**, 634 (2012)

[2] E. Hanggi and M. Tomamichel, e-print, arXiv:1108.5349 (2011).

[3] H-K. Lo, M. Curty and B. Qi, e-print, arXiv:1109.1473 (2011)

[4] S. L. Braunstein and S. Pirandola, e-print, arXiv:1109.2330 (2011)

[5] M. Tomamichel, PhD thesis Diss. ETH No. 20213, arXiv:1203.2142 (2012)

[6] L. Masanes, S. Pironio and A. Acin, Nat. Commun. **2**, 238 (2011)

Experimental Characterization of the Quantum Statistics of Surface Plasmons in Metallic Stripe Waveguides

M. S. Tame[1], **G. Di Martino**[2], **Y. Sonnefraud**[2], **S. Kéna-Cohen**[2], **Ş. K. Özdemir**[3], **M. S. Kim**[1] and **S. A. Maier**[2]

[1]*Imperial College London, Blackett Laboratory, Quantum Optics and Laser Science Group, SW7 2AZ London UK*
[2]*Imperial College London, Blackett Laboratory, Experimental Solid State Group, SW7 2AZ London UK*
[3]*Department of Electrical and Systems Engineering, Washington University, St. Louis, MO 63130, USA*

Surface plasmon polaritons (SPPs) are highly confined electromagnetic excitations coupled to electron charge density waves propagating along a metal-dielectric interface. Significant effort is currently being devoted to the study of their unique light-matter properties and to their use in optoelectronic devices exhibiting sub-wavelength field confinement [1]. Most recently there has been a growing excitement among researchers about the prospects for building plasmonic devices that operate faithfully at the quantum level. The main hindrance to the use of SPPs in practical devices is, however, their lossy character. Still, recent work has shown that SPPs can maintain certain quantum properties of their exciting photon field. Despite the progress made in using quantum optical techniques to study plasmonic systems, adapting them to realistic structures will require a much more detailed understanding of the quantum properties of SPPs when loss is present. This is an important area so far lacking an in-depth study. Understanding how loss affects the quantum behavior of SPPs may open up a route toward the realistic design and fabrication of nanophotonic plasmon circuits for quantum information processing.

I will review the emerging field of quantum plasmonics, looking at what it offers beyond conventional quantum photonic systems and highlight a recent experimental characterization of the effects of loss on the quantum statistics of waveguided SPPs [2]. Here, using single photons produced
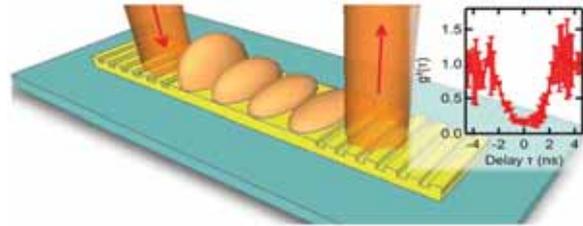
Figure 2: Metallic stripe waveguide injected with single photons for characterizing the effects of loss on the quantum statistics of surface plasmon polaritons. Inset: $g^{(2)}(\tau)$.

by type-I parametric down conversion [3], quanta of SPPs are excited in thin metallic stripe waveguides, one of the fundamental building blocks for plasmonic circuits [4, 5, 6], as shown in Figure 1. The second-order quantum coherence, $g^{(2)}(\tau)$, is measured (see Figure 2), and Fock state populations and mean excitation count rates for a range of different waveguide lengths are also investigated. The mean excitation rate is found to follow the classical intensity rate as the waveguide length increases, but the second-order quantum coherence remains markedly different from that expected in the classical regime. The dependence is found to be consistent with a linear uncorrelated Markovian environment [6]. This study complements well and goes beyond previous studies looking into the preservation of entanglement via localised plasmons [7] and nonclassicality via long-range surface plasmons [8], where elements of plasmon loss were considered.

These results provide important information about the effect of loss for assessing the realistic potential of building plasmonic waveguides for nanophotonic circuitry that operates faithfully in the quantum regime.

References

[1] J. Takahara *et al.*, Opt. Lett. **22**, 475 (1997).

[2] G. Di Martino *et al.*, Nano Letters (2012).

[3] C. K. Hong and L. Mandel, Phys. Rev. Lett. **56**, 58 (1986).

[4] B. Lamprecht *et al.*, App. Phys. Lett. **79**, 51 (2001).

[5] R. Zia *et al.*, Phys. Rev. B **71**, 165431 (2005).

[6] M. S. Tame *et al.*, Phys. Rev. Lett. **101**, 190504 (2008).

[7] E. Altewischer *et al.*, Nature **418**, 304 (2002).

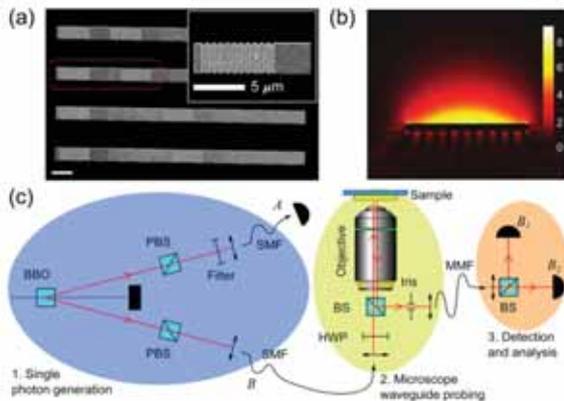[8] A. Huck *et al.*, Phys. Rev. Lett. **102**, 246802 (2009).

Figure 1: Experimental configuration. (a) Scanning electron microscope image of a selection of waveguides. (b) Fundamental SPP mode in our stripe waveguide – electric field profile along the cross section of the waveguide calculated using the FEM. (c) Schematic of the experimental setup including single-photon source, waveguide probing and final analysis.

Manipulating single atoms and single photons using cold Rydberg atoms

Philippe Grangier

Laboratoire Charles Fabry, Institut d'Optique, 91127 Palaiseau, France

We will present experimental and theoretical results about the use of trapped cold Rydberg atoms for applications in quantum information : either performing quantum gates with individually trapped atoms, or designing "giant" optical nonlinear effects by using ensemble of cold atoms in an optical cavity.

Stabilization of Fock states in a high Q cavity by quantum feedback

X. Zhou[1], I. Dotsenko[1], B. Peaudecerf[1], T. Rybarczyk[1], C. Sayrin[1], S. Gleyzes[1], J.M. Raimond[1], M. Brune[1] and S. Haroche[1,2]

[1] *Laboratoire Kastler-Brossel, ENS, UPMC-Paris 6, CNRS, 24 rue Lhomond, 75005 Paris, France*
[2] *Collège de France, 11 place Marcellin Berthelot, 75005 Paris, France*

We apply quantum non-demolition (QND) photon counting to a field stored in a high Q cavity, which acts as a photons trap. It is made of superconducting mirrors and stores microwave photons for durations as long as one tenth of a second. Non-resonant Rydberg atoms send one by one trough the cavity are used as sensitive probes of the stored microwave field (Fig. 1) They act as tiny atomic clocks whose oscillation rate is slightly affected by the intensity of the cavity field. Detecting one atom provides partial information about the photon number. Accumulating information by detecting many atoms within the photon lifetime amounts to a progressive projection of the field state on a photon number state [1]. This process realizes an ideal projective QND measurement whose result is fundamentally random.
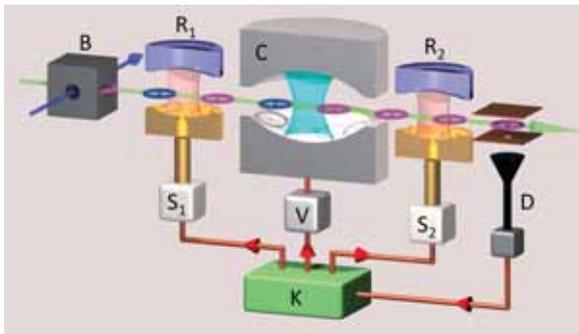
Figure 1: Experimental setup. Rydberg atoms prepared in box B cross the high Q cavity C and are finally detected in the sate selective detector D. The low Q cavities R_1 and R_2 are used to apply resonant microwave pulses with the classical sources S_1 and S_2. The voltage source V is used to set the atoms in or out of resonance with C by Stark effect. For QND sensor atoms pulses in R_1 and R_2 are set for detecting cavity induced light shifts by Ramsey interferometry.

By feeding the quantum information provided by individual atomic detections into a controller K one reacts in real time on the cavity field state. Depending on the detection results, the controller performs precise state estimation and applies a feedback action by deciding to use the next atom crossing C as emitter, absorber or QND probe. For that purpose, it uses the voltage source V to switch the interaction from dispersive for QND sensor to resonant for emitters or absorbers. The initial state of resonant atom is controlled by applying in R_1 a resonant π pulse on the atoms initially prepared in the lower state of the atomic transition.

We show that under steady state operation of the feedback loop, the QND measurement process is turned into an efficient method of deterministic preparation and stabilization of number states of light. It additionally allows to protect them from decoherence by reversing the destructive effect of quantum jumps [2, 3]. Fig. 2 shows the photon number distribution as estimated in real time by the controller in a single realization of the experiment. Under closed loop operation, the system follows closely the varying target number state. Independent state reconstruction performed just after opening the feedback loop demonstrates high fidelity preparation of Fock states up to 7 photons.
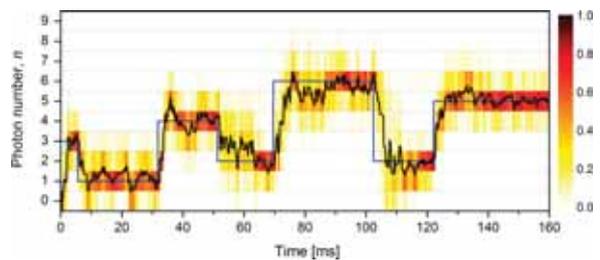
Figure 2: Programmed sequence of Fock states. The target number state varies stepwise as indicated by the thin line. The photon number distribution inferred by K is shown in color and gray scale, together with its average value (thick line).

References

[1] C. Guerlin *et al.*, Nature (London) **448**, 889 (2007).

[2] C. Sayrin *et al.*, Nature (London) **477**, 73 (2011).

[3] X. Xhou *et al.*, Phys. Rev. Lett. **108**, 243602 (2012).

An Elementary Quantum Network of Single Atoms in Optical Cavities

Stephan Ritter[1], **Christian Nölleke**[1], **Carolin Hahn**[1], **Andreas Reiserer**[1], **Andreas Neuzner**[1], **Manuel Uphoff**[1], **Martin Mücke**[1], **Eden Figueroa**[1], **Joerg Bochmann**[1,†], **and Gerhard Rempe**[1]

[1]*Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Strasse 1, 85748 Garching, Germany*

The distribution of quantum information as well as the utilization of non-locality are at the heart of quantum networks, which show great promise for future applications like quantum communication, distributed quantum computing and quantum metrology. Their practical realization however is a formidable challenge. On the one hand, the state of the respective quantum system has to be under perfect control, ideally in all degrees of freedom. This requires low decoherence, i.e. minimal interaction with the environment. But at the same time, strong, tailored interactions are required to enable all envisioned processing tasks. In this respect single atoms and photons are the ideal building blocks of a quantum network [1]. Atoms can act as stationary nodes as they are long-lived and their interaction with the environment is weak, while their external and internal degree of freedom can precisely be controlled and manipulated. Photons can be transmitted over larger distances using existing fiber technology and do not mutually interact.

We realize the necessary enhanced coupling between single atoms and photons using an optical cavity. The toolbox provided by cavity QED has allowed us to demonstrate the controlled generation of single photons based on dynamic control of coherent atomic dark states. We can thus map the qubit state of the atom onto the polarization of a single photon [2]. In this way, quantum information can be distributed by storing the photon at another network node. Using process tomography we have proven that our single-atom–cavity system is the most fundamental implementation of a quantum memory with higher fidelity than any classical device [3].

Consequently, single atoms in optical cavities are ideally suited as universal quantum network nodes capable of sending, storing and retrieving quantum information. We demonstrate this by presenting an elementary version of a quantum network based on two identical nodes in remote, independent laboratories [4]. The reversible exchange of quantum information and the creation of remote entanglement are both achieved by exchange of a single photon. Arbitrary qubit states are coherently transferred between the two network nodes. We show how to create maximally entangled Bell states of the two atoms at distant nodes and characterize their fidelity and lifetime. The resulting nonlocal state is manipulated via unitary operations applied locally at one of the nodes. This cavity-based approach to quantum networking offers a clear perspective for scalability, thus paving the way towards large-scale quantum networks and their plethora of applications.
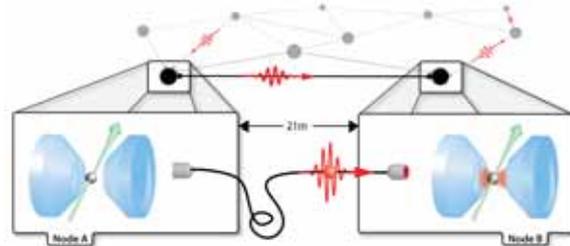
Figure 1: A quantum network based on single atoms in optical cavities. Two remote network nodes are connected by an optical fibre link. Quantum information is exchanged by the controlled emission and absorption of single photons.

[2] T. Wilk, S.C. Webster, A. Kuhn, and G. Rempe, Science **317**, 488 (2007).

[3] H.P. Specht, C. Nölleke, A. Reiserer, M. Uphoff, E. Figueroa, S. Ritter, and G. Rempe, Nature **473**, 190 (2011).

[4] S. Ritter, C. Nölleke, C. Hahn, A. Reiserer, A. Neuzner, M. Uphoff, M. Mücke, E. Figueroa, J. Bochmann, and G. Rempe, accepted for publication in Nature, arXiv:1202.5955 (2012).

† Present address: Department of Physics, and California NanoSystems Institute, University of California, Santa Barbara, California 93106, USA.

References

[1] J.I. Cirac, P. Zoller, H.J. Kimble, and H. Mabuchi, Phys. Rev. Lett. **78**, 3221 (1997).

Exploring cavity-mediated long-range interactions in a quantum gas

Tobias Donner, Ferdinand Brennecke, Rafael Mottl, Renate Landig, Kristian Baumann and Tilman Esslinger

ETH Zurich, Switzerland

Creating quantum gases with long-range atom-atom interactions is a vibrant area of current research, possibly leading to the observation of novel quantum phases and phase transitions. In our approach, we couple a Bose-Einstein condensate to the vacuum mode of a high-finesse optical cavity using a non-resonant transverse pump beam. This gives rise to cavity-mediated atom-atom interactions of global range, which are tunable in magnitude and sign.

Increasing the strength of the interaction leads to a softening of an excitation mode at finite momentum, preceding a superfluid-to-supersolid phase transition. We probe the excitation spectrum with a cavity-based variant of Bragg spectroscopy and study the mode softening across the phase transition. The observed data agrees well with an ab initio model [1].

This mode softening, which is reminiscent of the roton-minimum in liquid Helium, is accompanied by diverging fluctuations of the atomic and photonic fields. The openness of the cavity allows us to observe density quantum fluctuations in real-time. At the same time the unavoidable measurement backaction renders the phase transition to be non-equilibrium, which significantly changes the thermodynamics. Our system can be seen as a basic building block for quantum simulations of key models in quantum-many body physics.
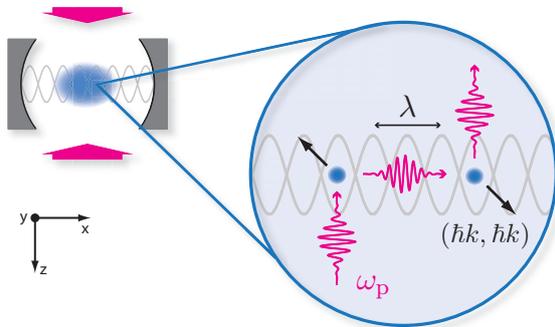
Figure 1: Cavity-mediated long range-interaction. A BEC (blue) located in the mode of an optical high-finesse cavity is transversally illuminated by a standing wave pump laser at frequency ω_p, which is far red-detuned from the atomic resonance, but closely detuned from the cavity resonance. Atoms coherently scatter photons from the pump into the cavity mode and back, which leads to an infinite-range interaction between the atoms, mediated by the cavity mode. The zoom displays one of four possible scattering processes, in which both atoms gain momentum.

References

[1] R. Mottl, F. Brennecke, K. Baumann, R. Landig, T. Donner, and T. Esslinger, Science, **336**, 1570 (2012).

Entangling distant electron spins

Jörg Wrachtrup

3rd Institute of Physics, University of Stuttgart, Germany

Generation of entanglement between spins in solids is a core challenge in quantum technology. Early examples on bulk ensembles of nuclear and electron spins have paved the way towards current approaches using nano positioned systems and single site readout. The talk will describe deterministic entanglement between engineered electron spins of diamond defects. Rapid dephasing of entangled electron spin states is mitigated by high fidelity entanglement storage on nuclear spins yielding ms entanglement lifetimes under ambient conditions. The impact of spin correlations on photon emission of defect pairs is analyzed. Roads towards large scale entanglement generation will be discussed.

Quantum Information Transport in Mixed-State Networks

Gurneet Kaur[1], **Ashok Ajoy**[1] **and** **Paola Cappellaro**[1]

[1]*Nuclear Science and Engineering Department and Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA – USA*

A promising approach toward a scalable quantum information processor is a distributed architecture, where small computational nodes are connected by quantum spin wires. Coherent transmission of quantum information over short distances is enabled by internal couplings among spins, ideally aligned in a one-dimensional (1D) chain. Given the practical challenge of engineering 1D chains with exact spin spacing and of preparing the spins in a pure state, we propose to use more general spin networks with the spins initially in the maximally mixed state.

Similarities between the transport properties of pure and mixed-state chains enable protocols for the perfect transfer of quantum information and entanglement in mixed-state chains [1]. Remarkably, mixed-state chains allow the use of a broader class of Hamiltonians, which are more readily obtainable from the naturally occurring magnetic dipolar interaction, thus enabling an experimental implementation of quantum state transport.

Owing to their unique geometry, nuclear spins in apatite crystals provide an ideal test-bed for the experimental study of quantum information transport, as they closely emulate an ensemble of 1D spin chains. Nuclear Magnetic Resonance techniques can be used to drive the spin chain dynamics and probe the accompanying transport mechanisms. We demonstrated initialization and read-out capabilities in these spin chains, even in the absence of single-spin addressability [2].

These control schemes enable preparing desired states for quantum information transport and probing their evolution under the transport Hamiltonian (see Fig. 1). It thus becomes possible to explore experimentally the effects of discrepancy from the ideal 1D nearest-neighbor coupling model and the perturbation due to the interaction of the chains with the environment.

To extend these results to systems where the spin position is not precisely set by nature, we considered arbitrary networks of spins, where the random position of the spins and the spatial dependence of their interaction sets the coupling topology and strength [3]. We show that perfect state transfer is possible for any coupling topology, provided we have control on the coupling strength and energy of the end-spins between which the state transfer is operated. These results open the possibility of experimental implementations of quantum information transfer in natural and engineered solid-state systems. For example nitrogen defect centers in diamond could be implanted and used as spin wires to connect the optically addressable Nitrogen-Vacancy defect centers, acting as quantum computational nodes.

References

[1] P. Cappellaro, L. Viola, and C. Ramanathan, Phys. Rev. A **83**, 032304 (2011)

[2] G. Kaur and P. Cappellaro, ArXiv:1112.0459 [quant-ph] (2011)

[3] A. Ajoy and P. Cappellaro, "Mixed-state quantum transport in correlated spin networks", to appear in Phys. Rev. A (2012)

Figure 1: Quantum information transport in an ensemble of ^{19}F nuclear spin chains in a synthetic crystal of fluorapatite. Red full circles: Experimental results of polarization transport with initialization and readout of the chain-end spins. Dash-dotted line: fitting of the experimental to the analytical solution of the transport dynamics. Because of the transport times explored and of the distribution in chain lengths we could only observe information leaking out of one end of the chain, but could not observe the information packet arriving at the other end of the chain. For comparison, the blue circles show the experimental evolution of the thermal state, when measuring the collective spin magnetization (the blue dashed line is the fitting to the analytical expression for the spin-chain dynamics).

Quantum Networks with Spins in Diamond

Hannes Bernien[1], **Lucio Robledo**[1], **Lilian Childress** [2], **Bas Hensen**[1], **Wolfgang Pfaff**[1], **Tim Taminiau**[1], **Matthew Markham**[3], **Daniel Twitchen**[3], **Paul Alkemade**[1] **and Ronald Hanson**[1]

[1] *Kavli Institute of Nanoscience, Delft, The Netherlands*
[2] *Bates College, Lewiston, United States*
[3] *Element Six, Ltd., Berkshire, United Kingdom*

A key challenge in quantum science is to robustly control and to couple long-lived quantum states in solids. The electronic and nuclear spins associated with the nitrogen-vacancy (NV) center in diamond constitute an exceptional solid state system for applications in quantum information science. Combining long spin coherence times [1] and fast manipulation [2] with a robust optical interface [3, 4], NV-based quantum registers have been envisioned as building blocks for quantum repeaters, cluster state computation, and distributed quantum computing.

Figure 1: Two-photon quantum interference. A pulsed laser excites two seperate NV centers with a repetition rate of 10 MHz. The emitted photons are overlapped on a beam splitter and the coincedences of the two detectors in the output ports recorded. For orthogonal polarization of the photons (a) the coincidence distribution corresponds to the temporal overlap of two independent wavepackets. For parrallel polarization (b) two-photon quantum interference is observed: around zero detection time difference the two photons mainly leave the beam splitter into the same output port. Simulations with no free parameters (red lines) show excellent agreement with the experimental data.

In this talk, we report on our latest advances towards realizing long-distance quantum networks with spins in diamond. First, we demonstrate preparation and single-shot measurement of a quantum register containing up to four quantum bits [5]. Projective readout of the electron spin of a single NV center in diamond is achieved by resonant optical excitation. In combination with hyperfine-mediated quantum gates, this readout enables us to prepare and measure the state of multiple nuclear spin qubits with high fidelity. We show compatibility with qubit control by demonstrating initialization, coherent manipulation, and single-shot readout in a single experiment on a two-qubit register, using techniques suitable for extension to larger registers. Second, we observe quantum interference of photons emitted by two spatially separated NV centers [6], Figure 1. Combined with recently shown spin-photon entanglement [3], this effect enables measurement-based entanglement of two distant NV centers. By using electrical tuning of the optical transition frequencies, we are able to observe two-photon interference even for initially dissimilar centers, indicating a viable path for scaling towards a multi-node diamond-based quantum network. We will present these results, along with our most recent data, and discuss the prospects of realizing quantum networks with NV centers in diamond in the near future.

References

[1] G. Balasubramanian et al., Nature Materials, **8**, 383 (2009)

[2] G. D. Fuchs, V. V. Dobrovitski, D. M. Toyli, F. J. Heremans, D. D. Awschalom, Science, **326**, 1520 (2009)

[3] E. Togan*, Y. Chu* et al., Nature, **466**, 730 (2010)

[4] L. Robledo, H. Bernien, I. v. Weperen, R. Hanson, PRL, **105**, 177403 (2010)

[5] L. Robledo*, L. Childress*, H. Bernien*, B. Hensen, P. Alkemade, R. Hanson, Nature, **477**, 547 (2011)

[6] H. Bernien, L. Childress, L. Robledo, M. Markham, D. Twitchen, R. Hanson , PRL, **108**, 043604 (2012)

Suppression of spin bath dynamics for improved coherence in solid-state systems

Nir Bar-Gill[1,2], Linh M. Pham[3], Chinmay Belthangady[2], David Le Sage[3] and Ronald Walsworth[1,2]

[1] *Department of Physics, Harvard University, Cambridge MA, USA*
[2] *Harvard-Smithsonian Center for Astrophysics, Cambridge, MA, USA*
[3] *School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, USA*

Understanding and controlling the coherence of multi-spin-qubit solid-state systems is crucial for quantum information science, basic research on quantum many-body dynamics and quantum sensing and metrology. Examples of such systems include Nitrogen-Vacancy (NV) color centers in diamond, phosphorous donors in silicon and quantum dots. In particular, for solid-state spin qubits the coherence time T_2 is typically limited by interaction with an environment (i.e., bath) of paramagnetic spin impurities.

Here we study experimentally the spin environment of NV color centers in room temperature diamond (Fig. 1(a,b)). We apply a spectral decomposition technique [1, 2] to characterize the dynamics of the composite solid-state spin bath, consisting of both electronic spin (N) and nuclear spin (^{13}C) impurities [3].

This spectral decomposition technique determines the spectral function of the bath fluctuations from decoherence measurements of the NV spin. By applying a modulation to the NV spins, e.g. through dynamical decoupling Carr-Purcell-Meiboom-Gill (CPMG) pulse sequences, the spectral component of the bath at the modulation frequency can be extracted.

Experimentally, we manipulate the $|0\rangle$-$|1\rangle$ spin manifold of the NV triplet electronic ground-state (Fig. 1(c)) using a static magnetic field and resonant microwave pulses, and employ a 532 nm laser to initialize and provide optical readout of the NV spin states. More specifically, we optically initialize the NV spins to $m_s = 0$, apply CPMG pulse sequences (see Fig. 1(d)) with varying numbers of π pulses n and varying free precession times τ, and then measure the NV spin state using optical readout to determine the remaining NV multi-spin coherence. The measured coherence is then used to extract the corresponding spin bath spectral component as described above.

We study three different diamond samples with a wide range of NV densities and impurity spin concentrations (measuring both NV ensembles and single NV centers), and find unexpectedly long correlation times for the electronic spin baths in two diamond samples with natural abundance (1.1%) of ^{13}C nuclear spin impurities. We identify a possible new mechanism in diamond involving an interplay between the electronic and nuclear spin baths that can explain the observed suppression of electronic spin bath dynamics. This spin-bath suppression enhances the efficacy of dynamical decoupling for samples with high N impurity concentration, enabling increased NV spin coherence times

We explain this suppression of spin-bath dynamics as a result of random, relative detuning of electronic spin energy levels due to interactions between proximal electronic (N) and nuclear (^{13}C) spin impurities. The ensemble average effect of such random electronic-nuclear spin interactions is to induce an inhomogeneous broadening of the resonant electronic spin transitions in the bath, which reduces the electronic spin flip-flop rate, thereby increasing the bath correlation time.
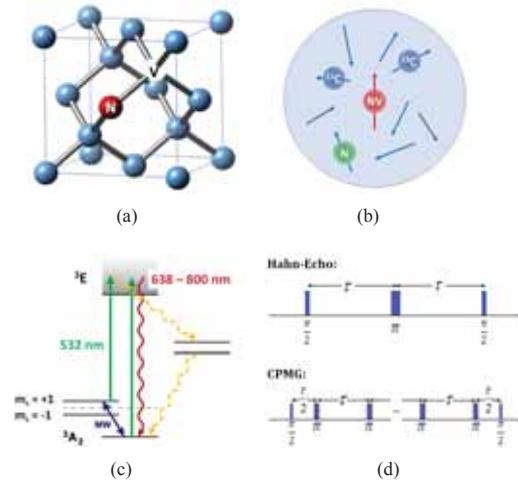

Figure 1: NV-center in diamond, and applied spin-control pulse-sequences. (a) Lattice structure of diamond with an NV color center. (b) Magnetic environment of NV center electronic spin: ^{13}C nuclear spin impurities and N electronic spin impurities. (c) Energy-level schematic of negatively-charged NV center. (d) Hahn-echo and multi-pulse (CPMG) spin-control sequences.

The present results pave the way for quantum information, sensing and metrology applications in a robust, multi-qubit solid-state architecture. We demonstrate this through the improvement in magnetic field sensitivity of a variety of different samples, using the dynamical decoupling sequences described above [4].

References

[1] Bylander, J. *et al.*, Nature Physics, **7**, 565–570 (2011)

[2] Álvarez, G. A. & Suter, D., Phys. Rev. Lett., **107**, 230501 (2011)

[3] Bar-Gill, N. *et al.*, arXiv:1112.0667v2 (2011)

[4] Pham L. M. *et al.*, arXiv:1201.5686 (2012)

Poster session 1 Monday abstracts

Entropic Test of Quantum Contextuality and Monogamy

Pawel Kurzynski[1,2], **Ravishankar Ramanathan**[1] and Dagomir Kaszlikowski[1,3]

[1]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2]*Faculty of Physics, Adam Mickiewicz University, Umultowska 85, 61-614 Poznań, Poland*
[3]*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*

The essence of the classical description of Nature is *realism*, the assumption that the physical world exists independently of any observers and that the act of observation does not disturb it. A mathematical consequence of realism is that there exists a joint probability distribution for the outcomes of measurements for all physical properties of the system, however quantum theory does not incorporate realism [1]. The lack of realism in certain entangled systems has information-theoretic consequences; the conditional Shannon entropies of the outcomes of certain measurements do not obey fundamental classical properties such as the chain rule [2], this is used here to formulate entropic inequalities to test contextuality.

The notion of contextuality, as introduced by Kochen and Specker (KS) can be explained as follows. Suppose a measurement A on a given system can be jointly performed with one of two other measurements, either with B or with C, but that B and C cannot be jointly performed. Measurements B and C are said to provide two different contexts for A. The measurement A is contextual if its outcome depends on whether it was performed together with B or with C; the essence of contextuality is thus the inability to assign an outcome to A prior to its measurement, independently of the context in which it was performed. Quantum theory can be proven to be contextual for any system whose dimension is greater than two. The Bell theorem is a special instance of the KS theorem, where contexts naturally arise from the spatial separation of measurements.

A convenient language to study the measurements that reveal contextuality is graph theory. Measurements are denoted by the vertices of a graph and edges connect any two vertices when the corresponding measurements can be jointly performed. We study the minimal set of measurements necessary to reveal contextuality for the simplest contextual system, the qutrit, and analytically show that the five-cycle is the minimal graph to reveal its contextuality confirming earlier numerical observations [3]. To prove this, we explicitly construct joint probability distributions for some smaller graphs than the pentagon and demonstrate that measurements corresponding to other smaller graphs, such as the four-cycle, cannot be realized on the qutrit.

An entropic inequality for contextuality is formulated using two fundamental properties of the Shannon entropy, $H(A) = -\sum_a p(A = a) \log_2 p(A = a)$ of measurement outcomes. The first is the chain rule $H(A, B) = H(A|B) + H(B)$ and the second is the inequality $H(A|B) \leq H(A) \leq H(A, B)$. The latter inequality has the interpretation that conditioning cannot increase information content of a random variable A and that two random variables A, B cannot contain less information than one of them. We use these properties on the classical (non-contextual) hypothetical joint probability distribution for the measurements that form the five-cycle, $H(A_1, A_2, A_3, A_4, A_5)$, and derive the entropic contextual inequality [4]

$$H(A_1|A_5) \leq \sum_{i=1}^{4} H(A_i|A_{i+1}) \qquad (1)$$

Similar entropic inequalities can be constructed for larger number of measurements and any system dimension as well. We proceed to demonstrate a method to construct joint probability distributions for certain measurement configurations [5]. In particular, we establish

Proposition 1: A commutation graph G representing a set of n measurements (for any n) admits a joint probability distribution for these measurements if it is a chordal graph.

A chordal graph is a graph that does not contain an induced cycle of length greater than 3. This comprises a large class among all graphs of n vertices and the above Proposition thus excludes the construction of contextual inequalities (or Kochen-Specker proofs) from all such graphs.

Finally, we study an intriguing aspect of contextuality, its monogamy. A set of measurements is said to have 'monogamous contextuality' if it can be partitioned into disjoint subsets, each of which can by themselves reveal contextuality, but which cannot all simultaneously be contextual. We show how one can construct monogamies for contextual inequalities using the Gleason principle of no-disturbance. To do this, we employ the graph-theoretic technique of vertex decomposition of a graph representing a set of measurements into subgraphs of suitable independence numbers that themselves admit a joint probability distribution. We end by establishing

Proposition 2: Consider a commutation graph representing a set of n KCBS-type contextual inequalities [3] each of which has non-contextual bound R. Then this graph gives rise to a monogamy relation if and only if its vertex clique cover number is $n * R$.

References

[1] A. Fine, Phys. Rev. Lett., **48**, 291 (1982), S. Kochen and E. P. Specker, J. Math. Mech., **17**, 59 (1967), J. S. Bell, Physics **1**, 195 (1964).

[2] S. L. Braunstein and C. M. Caves, Phys. Rev. Lett., **61**, 662 (1988).

[3] A. A. Klyachko *et al.*, Phys. Rev. Lett., **101**, 020403 (2008).

[4] P. Kurzynski, *et al.*, arXiv/quant-ph: 1201.2865, accepted in PRL (2012).

[5] R. Ramanathan *et al.*, arXiv/quant-ph: 1201.5836, accepted in PRL (2012).

Quantum nonlocality based on finite-speed causal influences leads to superluminal signalling

Jean-Daniel Bancal[1], Stefano Pironio[2], Antonio Acín[3,4], Yeong-Cherng Liang[1], Valerio Scarani[5,6], Nicolas Gisin[1]

[1]*Group of Applied Physics, University of Geneva, Switzerland*
[2]*Laboratoire d'Informatique Quantique, Université Libre de Bruxelles, Belgium*
[3]*Institut de Ciències Fotòniques, Castelldefels (Barcelona), Spain*
[4]*Institució Catalana de Recerca i Estudis Avançts, Barcelona, Spain*
[5]*Center for Quantum Technologies, National University of Singapore, Singapore 117543*
[6]*Department of Physics, National University of Singapore, Singapore 117542*

When measurements are performed on two entangled quantum particles separated far apart from one another, such as in the experiment envisioned by Einstein, Podolsky, and Rosen (EPR) [1], the measurement results of one particle are found to be correlated to the measurement results of the other particle. Bell showed that if these correlated values were due to past causes common to both measurements, then they would satisfy a series of inequalities [2]. But theory predicts and experiments confirm that these inequalities are violated [3], thus excluding any past common cause type of explanations for quantum nonlocal correlations.

Still, quantum nonlocal correlations could arise from common causes supplemented by the exchange of some influences between distant measurements. Since the measurement events can be space-like separated [4, 5, 6], any type of explanation based on causal influences must involve influences propagating faster than light [7]. Here, the speed of supraluminal influences is defined with respect to a universal priviledged reference frame (as for example the one in which the cosmic microwave backround radiation is isotropic).

Despite propagating faster than light, these influences might remain hidden, in the sense of not allowing observable correlations to be used to communicate faster than light. This is what led Abner Shimony to name the situation as "peaceful coexistence" between hidden influences behind the quantum and no signalling at the level of accessible correlations [8].

Here we show that there is a fundamental reason why influences propagating at a finite speed v may not account for the nonlocality of quantum theory: all such models for quantum correlations give, for any $v > c$, predictions that can be used for faster-than-light communication. This answers a long-standing question on the plausibility of these models first raised in [9, 10]. An inspiring progress on this problem was recently made in [11], where a conclusion with a similar flavor was obtained, but not for correlations predicted by the quantum theory.

In contrast with previous experimental approaches to hidden influence models, which relied on testing the violation of Bell inequalities with systems that are further apart and better synchronized to put a lower-bound on the speed v needed to reproduce the observed correlations [12, 13], our result opens the possibility for experiments to test hidden influences of arbitrary finite speed $v < \infty$.

Quantum communication and a significant part of the advantage offered by quantum information processing are based on the assumption that quantum correlations cannot be explained merely by shared randomness and finite speed communication. This work sets our belief in entanglement and quantum nonlocality on a firmer ground.

References

[1] A. Einstein, B. Podolsky, and N. Rosen, Physical Review **47**, 777 (1935).

[2] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics: Collected papers on quantum philosophy* (Cambridge University Press, Cambridge, 2004).

[3] A. Aspect, Nature **398**, 189 (1999).

[4] A. Aspect, J. Dalibard, G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).

[5] W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, Phys. Rev. Lett. **81**, 3563-3566 (1998).

[6] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).

[7] J. S. Bell, *La nouvelle cuisine*, in reference [2].

[8] A. Shimony. In J. T. Cushing and E. McMullin, editors, *Philosophical Consequences of Quantum Theory*, pages 25-37 (University of Notre Dame Press, Notre Dame, 1989).

[9] V. Scarani and N. Gisin, Phys. Lett. A **295**, 167 (2002)

[10] V. Scarani and N. Gisin, Braz. J. Phys. **35**, 2A (2005).

[11] S. Coretti, E. Hänggi, and S. Wolf, Phys. Rev. Lett. **107**, 100402 (2011).

[12] D. Salart, A. Baas, C. Branciard, N. Gisin, and H. Zbinden, Nature **454**, 861 (2008).

[13] B. Cocciaro, S. Faetti and L. Fronzoni, Phys. Lett. A **375**, 379 (2011).

Time reversal symmetry violation in quantum weak measurements

Adam Bednorz[1], **Kurt Franke**[2] **and Wolfgang Belzig**[2]

[1] *Faculty of Physics, University of Warsaw, Hoża 69, PL-00681 Warsaw, Poland*
[2] *Fachbereich Physik, Universität Konstanz, D-78457 Konstanz, Germany*

The concept of quantum weak measurement [1] is a way to circumvent the invasive nature of projective measurements. It relies on a simple model of a pointer detector that is weakly coupled to the measured system, with the pointer values rescaled by the coupling in order to interpret them as the values of the system quantities. The detector-system coupling represents the measurement strength and can be made arbitrarily small to reduce the invasiveness at the price of introducing large detector noise. In the limit of zero strength one can describe the results of the measurement by the quasiprobability [2]. The quasiprobability explains known paradoxes of weak measurement such as unusually large conditional averages [1] or violation of the Leggett-Garg inequality [3].

We present a new paradox regarding the time reversal symmetry of sequential weak measurements, [4]. Sequential projective quantum measurements of incompatible observables break the time-reversal symmetry, due to their invasive nature. However, one could try to circumvent the induced asymmetry by performing a weak quantum measurement, expected to leave the state of the system intact. We show that, paradoxically, time-reversal symmetry is still violated for this type of measurement. The violation calls the noninvasiveness of weak measurement into question and, as we show below, is detectable in third-order correlation functions. It is important to stress the difference to the macroscopic arrow of time, which appears solely due to loss of information and is the essence of the second law of thermodynamics. We can exclude this by taking equilibrium systems as examples or, alternatively, one could consider just the coherent microscopic evolution. We also propose an experiment with quantum dots to measure this apparent violation of time reversal symmetry in a third-order current correlation function.

The time reversal symmetry condition of time-dependent observables $a(t)$ is written as

$$\langle a_1(t_1) \cdots a_n(t_n) \rangle = \langle a_n^T(-t_n) \cdots a_1^T(-t_1) \rangle^T . \quad (1)$$

Here ^{T} denotes time reversal operation ($x \to x$, $p \to -p$). The symmetry is valid always in classical physics and for quantum compatible measurements.

The correlation function obtained from quantum weak measurements is given by [2]

$$\left\langle \prod_k a_k(t_k) \right\rangle = \mathrm{Tr}\{A_n(t_n), ..\{A_2(t_2), \{A_1(t_1), \rho\}\}..\}/2^n$$

$$(2)$$

for $t_n > \ldots > t_2 > t_1$. We denoted by a the result of measurement of quantity A, the initial state ρ and $\{A, B\} = AB + BA$. For $n = 2$ the time symmetry holds generally, but for $n \geq 3$ it can be violated.

Let us demonstrate the paradox in a simple system consisting of a particle in a double-well potential as in Fig. 1. For simplicity, we take an equilibrium state, but the asymmetry
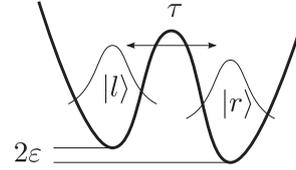
Figure 1: The double well example

appears also in a completely general case. The particle is effectively described by the ground states of the left and right wells, $|l\rangle$ and $|r\rangle$ respectively. We assume that higher excited states can be ignored for low temperatures, leaving an effective two state system. Using these basis states, the operator for the location is $Z = |l\rangle\langle l| - |r\rangle\langle r|$, and the effective Hamiltonian reads

$$H = \varepsilon(|l\rangle\langle l| - |r\rangle\langle r|) + \tau(|l\rangle\langle r| + |r\rangle\langle l|), \quad (3)$$

where 2ε is the energy difference between the wells and τ is the tunneling amplitude. Since no magnetic fields are present, H and Z are even under time reversal. We are now in a position to test equation (1) with z measured at three separate times and with the initial thermal state $\rho \propto \exp(-H/k_B T)$. The correlation for three weak measurements can be calculated using (2) and $Z(t) = e^{iHt/\hbar} Z e^{-iHt/\hbar}$:

$$\langle z(t_1)z(t_2)z(t_3) \rangle = \alpha(\varepsilon^2 + \tau^2 \cos(2(t_3 - t_2)\Delta/\hbar)), \quad (4)$$

where $\Delta = \sqrt{\varepsilon^2 + \tau^2}$, $\alpha = -(\varepsilon/\Delta^3)\tanh(\Delta/k_B T)$. For this system and measurements, the expression corresponding to the right hand side of (1) differs from (4) by the exchange of $t_3 - t_2$ with $t_2 - t_1$. However, (4) clearly changes under this replacement, demonstrating that time reversal symmetry is broken for correlations of quantum weak measurements.

The implications of our observation will be discussed. One possibility would be that weak measurements cannot exist, which, however, looks unreasonable since numerous experiments are performed in the weak regime. Alternatively, it reveals an up-to-now undiscovered arrow of time in quantum mechanics, of which consequences remain to be explored.

References

[1] Y. Aharonov, D.Z. Albert, and L. Vaidman, Phys. Rev. Lett. **60**, 1351 (1988).

[2] A. Bednorz and W. Belzig, Phys. Rev. Lett. **105**, 106803 (2010)

[3] A.J. Leggett and A. Garg, Phys. Rev. Lett. **54**, 857 (1985).

[4] A. Bednorz, K. Franke, and W. Belzig, arXiv:1108.1305

Tight inequality for qutrit state-independent contextuality

Adán Cabello[1], Costantino Budroni[1], Otfried Gühne[2], Matthias Kleinmann[2], and Jan-Åke Larsson[3]

[1]*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*
[2]*Universität Siegen, Naturwissenschaftlich-Technische Fakultät, Walter-Flex-Straße 3, D-57068 Siegen, Germany*
[3]*Institutionen för Systemteknik, Linköpings Universitet, SE-58183 Linköping, Sweden*

The characterization of nonclassical features of quantum correlations is a fundamental problem both for the foundations of quantum physics and for the applications in quantum information theory.

For instance, a fundamental tool for such investigation is given by Bell inequalities: For every measurement scenario, there exists a finite set of inequalities, called "tight" Bell inequalities, which provides necessary and sufficient conditions for the existence of a local hidden variable (LHV) theory reproducing the corresponding set of quantum correlations. Such inequalities represent the boundaries of the convex set of classical correlations: Without a complete set of tight inequalities only a subset of nonlocal correlations can be identified.

Another nonclassical phenomenon, with analogous, but far less explored, applications in quantum information processing, is that of quantum contextuality. The latter can be investigated by means of noncontextuality inequalities: They are constraints on the correlations among the results of compatible or jointly measurable observables, which are satisfied by any noncontextual hidden variable (NCHV) theory. The notion of tightness also applies to noncontextuality inequalities.

As opposed to Bell inequalities, noncontextuality inequalities can be violated by general quantum systems and states, not only by composite system and entangled states, but the most surprising difference is that such violations can be independent of the quantum state of the system, a property known as state-independent contextuality (SIC) [1]. SIC has been observed recently in experiments [2].

Recently, Yu and Oh [3] have introduced an inequality for observing SIC on a single qutrit. What makes Yu and Oh's inequality of fundamental importance is that it identifies a specific 13-setting scenario (see Figure 1) which has proven to be the simplest one in which qutrit SIC can be observed. However, the inequality they provided is not tight.

In this contribution, we present the first tight SIC inequality for Yu and Oh's scenario, which has been found as a solution of the maximization problem for the state-independent quantum violation. The same method is shown to provide a tight SIC inequality also when additional restriction on measurements are imposed in the same scenario. We recall that, even if there exist algorithms for computing complete sets of tight inequalities, the time required to compute them grows enormously as the number of settings increases. In Yu and Oh's scenario, such a computation is not feasible.

To complete our analysis, we also derive a partial list of tight inequalities for Yu and Oh's scenario. Such inequalities correspond to structures, subsets of Yu and Oh's set of measurements, previously identified by Kochen and Specker [4], Klyachko *et al.* [5], and others. However, in the best case, they lead to state-dependent violations which do

$$v_1=(1,0,0) \quad v_4=(0,1,-1) \quad v_{10}=(-1,1,1)$$
$$v_2=(0,1,0) \quad v_5=(1,0,-1) \quad v_{11}=(1,-1,1)$$
$$v_3=(0,0,1) \quad v_6=(1,-1,0) \quad v_{12}=(1,1,-1)$$
$$v_7=(0,1,1) \quad v_{13}=(1,1,1)$$
$$v_8=(1,0,1)$$
$$v_9=(1,1,0)$$
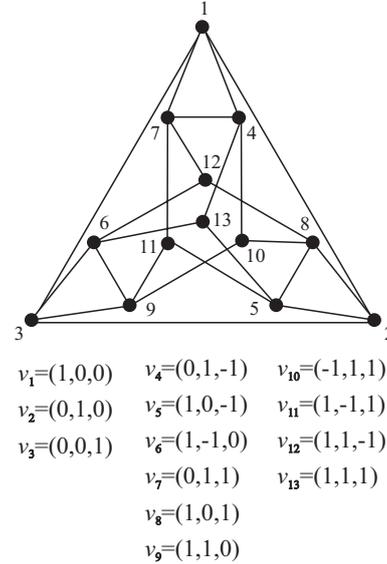
Figure 1: Graph of the compatibility relations between the observables in Yu and Oh's scenario. Dots represent vectors $|v_i\rangle$, or the observables $A_i = \mathbf{1} - 2|v_i\rangle\langle v_i|$, and edges represent orthogonality, or compatibility, relations.

not even reach the maximum quantum value for such structures. Again, this emphasizes the importance of our SIC inequality which provides, at the same time, tightness, state-independence and maximal quantum violation.

References

[1] A. Cabello, Phys. Rev. Lett. **101**, 210401 (2008).

[2] G. Kirchmair *et al.*, Nature (London) **460**, 494 (2009).

[3] S. Yu and C. H. Oh, Phys. Rev. Lett. **108**, 030402 (2012).

[4] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967).

[5] A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumovsky, Phys. Rev. Lett. **101** 020403 (2008).

Quantum correlations with no causal order [1]

Ognyan Oreshkov[1,2], **Fabio Costa**[1] and Časlav Brukner[1,3]

[1] *Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria.*
[2] *QuIC, Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium.*
[3] *Institute of Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria.*

Much of the recent progress in understanding quantum theory has been achieved within an operational approach. Within this context quantum mechanics is viewed as a theory for making probabilistic predictions for measurement outcomes following specified preparations. However, thus far essential elements of the theory — space, time and causal structure — elude this operational formulation and are assumed to constitute a pre-existing "stage" on which events take place. Even the most abstract constructions, in which no explicit reference to space-time is made, do assume a definite order of events: if a signal is sent from an event A to an event B in the run of an experiment, no signal can be sent in the opposite direction in that same run. But are space, time, and causal order truly fundamental ingredients of nature? Is it possible that, in some circumstances, even causal relations would be "uncertain", similarly to the way other physical properties of quantum systems are [2]? What new phenomenology would such a possibility entail?

We ask whether quantum mechanics allows for such a possibility. We develop a framework that describes all correlations that can be observed by two experimenters under the assumption that in their local laboratories physics is described by the standard quantum formalism. All correlations observed in situations that respect definite causal order can be expressed in this framework; these include non-signalling correlations arising from measurements on a bipartite state, as well as signalling ones, which can arise when a system is sent from one laboratory to another through a quantum channel. We find that, surprisingly, more general correlations are possible, which are not included in the standard quantum formalism. These correlations are incompatible with any underlying causal structure: they allow performing a task—the violation of a "causal inequality"—which is impossible if events take place in a causal sequence. This is directly analogous to the famous violation of local realism: quantum systems allow performing a task–the violation of Bell's inequality—which is impossible if the measured quantities have pre-defined local values. The inequality considered here, unlike Bell's, concerns signalling correlations: it is based on a task that involves communication between two parties. Nevertheless, it cannot be violated if this communication takes place in a causal space-time.

We also find that, contrary to the quantum case, classical correlations are always causally ordered, which suggests a deep connection between definite causal structures and classicality. It also suggests that indefinite causal orders could provide a new kind of quantum resource, with possible advantages over classical computers [3].

References

[1] O. Oreshkov, F. Costa and Časlav Brukner, *Quantum Correlations with no Causal Order*. arXiv:1105.4464v1 [quant-ph] (2011).

[2] L. Hardy, *Probability Theories with Dynamic Causal Structure: A New Framework for Quantum Gravity*. arXiv:gr-qc/0509120v1 (2005).

[3] Chiribella, G., D'Ariano, G. M., Perinotti, P. & Valiron, B. *Beyond quantum computers*. arXiv:0912.0195v2 [quant-ph] (2009).

Conclusive quantum steering with superconducting transition edge sensors

Devin H. Smith[1], **Geoff Gillett**[1], **Marcelo P. de Almeida**[1], **Cyril Branciard**[2], **Alessandro Fedrizzi**[1], **Till J. Weinhold**[1], **Adriana Lita**[3], **Brice Calkins**[3], **Thomas Gerrits**[3], **Howard M. Wiseman**[4], **Sae Woo Nam**[3], **Andrew G. White**[1]

[1]*Centre for Engineered Quantum Systems and Centre for Quantum Computation and Communication Technology (Australian Research Council), School of Mathematics and Physics, University of Queensland, 4072 Brisbane, QLD, Australia*
[2]*School of Mathematics and Physics, University of Queensland, 4072 Brisbane, QLD, Australia*
[3]*National Institute of Standards and Technology, 325 Broadway, Boulder CO 80305, USA*
[4]*Centre for Quantum Computation and Communication Technology (Australian Research Council), Centre for Quantum Dynamics, Griffith University, 4111 Brisbane, QLD, Australia*

Quantum steering was originally introduced by Erwin Schrödinger [1], in reaction to the Einstein, Podolsky and Rosen (EPR) "paradox" [2]; it describes the ability to remotely prepare different ensembles of quantum states by performing measurements on one particle of an entangled pair [3].

We define steering as a task with two parties: Alice and Bob receive particles from a black box (the source, S) and want to establish whether these are entangled. From a prearranged set, they each choose measurements to be performed on their respective particles. Bob's measurement implementation is trusted, but this need not be the case for Alice's; her measurement device is also treated as a black box from which she gets either a "conclusive", $A_i = \pm 1$, or a "nonconclusive" outcome, $A_i = 0$. To demonstrate entanglement, Alice and Bob need to show that she can *steer* his state by her choice of measurement. They can do so through the violation of a steering inequality (Fig. 1).

Figure 1: Conceptual depiction of a steering experiment.

A conclusive demonstration of steering through the violation of a steering inequality is of considerable fundamental interest and opens up applications in quantum communication. Similarly to the case of Bell inequalities, a conclusive violation of a steering inequality requires that the experiment does not suffer from any relevant loopholes. When one has untrusted devices, the so-called *detection loophole* in particular is critical. To date all experimental tests with single photon states have relied on post-selection, allowing untrusted devices to cheat by hiding unfavourable events in losses.

Here we close this "detection loophole" by combining a highly efficient source of entangled photon pairs with superconducting transition edge sensors. We achieve an unprecedented ∼62% conditional detection efficiency of entangled photons and violate a steering inequality with the minimal number of measurement settings by 48 standard devia-

tions [4]. Our results provide a clear path to practical applications of steering and to a photonic loophole-free Bell test.

References

[1] E. Schrödinger, *Proc. Camb. Phil. Soc.* **31**, 553 (1935).

[2] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).

[3] H. M. Wiseman, S. J. Jones, A. C. Doherty, *Phys. Rev. Lett.* **98**, 140402 (2007)

[4] D. H. Smith, *et al. Nat. Comm.* **3**, 625 (2012).

Symmetry arguments to certify and quantify randomness.

Chirag Dhara[1], **Giuseppe Prettico**[1] **and Antonio Acín**[1,2]

[1]*ICFO-The Institute of Photonic Sciences, Castelldefels (Barcelona), Spain*
[2]*ICREA - Institució Catalana de Reserca i Estudis Avançats, Barcelona, Spain*

Among the remarkable features of quantum mechanics, its nonlocal character and its intrinsic randomness play a crucial role. Although the notion of randomness is naturally defined and intuitively familiar, its characterization is elusive. Generally, statistical tests are used to verify the absence of certain patterns in a strings of numbers. However these tests are far from complete. In principle, every classical system admits a deterministic description and thus the perceived randomness stems from the lack of knowledge of the full description of the system.

Violation of Bell's inequalities by quantum systems certifies the presence of intrinsic genuine randomness in these systems[1]. However, non-locality and randomness have been shown to be inequivalent physical quantities[2]. In particular, it is unclear when and why non-locality certifies maximal randomness. We provide here a simple argument to certify the presence of maximal local and global randomness based on symmetries of a Bell's inequality and the existence of a unique quantum probability distribution that maximally violates it. The advantage of this approach is also its device-independence which is particularly relevant in a adversarial or cryptographic approach where no assumptions are made on the devices or the states and their dimensions.

We use our arguments to reach significant conclusions in different cases. For the CHSH [3] and the chained inequalities[4], we show that one and two bits respectively can be certified while for the Mermin's inequalities [5] in $(N, 2, 2)$, we show the maximum possible N bits of global randomness. Our results are encapsulated in the table below.

| Bell's Inequalities | Quantum | | Uniqueness |
	Local	Global	
CHSH (2,2,2)	1-bit	–	anl
CGLMP (2,M,d)	1-dit	–	num
Chain (2,M,2)	1-bit	2-bits	num
Mermin (N_{odd},2,2)	1-bit	N-bits	anl
Mermin (N_{even},2,2)	1-bit	$(N-1)$bits	anl

We conclude that simple arguments of symmetry and uniqueness can be used to reach significant conclusions about the randomness inherent in quantum probability distributions. While our formulation does not explicitly refer to the quantum set, we have evidence that the it is the particular shape of the quantum set that enables these results to hold.

References

[1] S. Pironio *et. al.* "*Random numbers certified by Bells theorem*", Nature **464** (2010), 1021.

[2] A. Acín, S. Massar, and S. Pironio, "Randomness versus Nonlocality and Entanglement", Phys. Rev. Lett. **108** (2012), 100402.

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories", Phys. Rev. Lett. **23** (1969), 15, 880.

[4] S. L. Braunstein and C. M. Caves, "Wringing out better Bell inequalities", Annals of Physics **202**, 22 (1990).

[5] N.D. Mermin "Extreme quantum entanglement in a superposition of macroscopically distinct states", Phys. Rev. Lett. **65**, 18381840 (1990).

Violation of a Bell-like inequality

Yuji Hasegawa[1] and <u>**Daniel Erdősi**</u>[1]

[1]*Atominstitut, Vienna University of Technology, Stadionallee 2, A-1020 Wien, Austria*

While lots of experimental tests of the violation of Bell's inequalities have been made with correlated photon pairs, also a single-neutron system becomes a more and more interesting subject for such tests [1, 2, 3]. We demonstrate the violation of a Bell-like inequality on the basis of a single-neutron interferometer (IFM) experiment with polarized neutrons [4]. The entanglement is accomplished between the spin and the path degrees of freedom of the neutron, i.e., between the spinor part and the spatial part of the neutron's total wave function, which has the form

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|\leftarrow\rangle \otimes |\mathrm{I}\rangle + |\rightarrow\rangle \otimes |\mathrm{II}\rangle \right), \qquad (1)$$

where $|\leftarrow\rangle$ and $|\rightarrow\rangle$ denote the spin states and $|\mathrm{I}\rangle$ and $|\mathrm{II}\rangle$ denote the two beam paths in the IFM. Observables of the spinor part commute with those of the spatial part, which justifies the derivation of a Bell-like inequality, according to the noncontextual hidden-variable theories (NCHVTs) [5].

A Bell-like inequality for a single-neutron experiment is given in terms of expectation values $E(\alpha, \chi)$ by [5]:

$$-2 \leq S \leq 2, \qquad (2)$$

where $S := E(\alpha_1, \chi_1) + E(\alpha_1, \chi_2) - E(\alpha_2, \chi_1) + E(\alpha_2, \chi_2)$ and the theoretical maximum violation is given by $S = 2\sqrt{2} \approx 2.828 > 2$. The parameters α and χ are experimentally varied by polarization analysis of the generated Bell-like state and by phase shift, respectively.

In the present experiment [4] we have applied a new method for the generation of the Bell-like state (1). In our previous experiment [1], we used a spin-up polarized neutron beam with spinor $|\uparrow\rangle$, which enters the IFM and splits into two partial beams I and II at the first plate. In one beam path the spin was rotated by $\pi/2$ and in the other path by $-\pi/2$, so that the spinor in path I became to $|\leftarrow\rangle$ while in path II to $|\rightarrow\rangle$, thus yielding the Bell-like state (1). The neutrons in path I and II had to pass through a Mu-metal sheet, which, as an unwanted side-effect, reduced interference contrast by $\sim$19% due to dephasing. Our new method (see Fig. 1), used in [4], to generate state (1) is based on the fact that only the directions of the spin flips are different for the two paths, whereas the amounts of the flips are equal. Therefore, state generation can be separated into two steps: (a) in the first step the spin is manipulated by a $\pi/2$ flip that changes the spinor from $|\uparrow\rangle$ to $|\rightarrow\rangle$, and (b) in the second step the azimuthal angles of the spins in path I and II are turned by π relative to each other, so that in one path the spinor remains $|\rightarrow\rangle$ while in the other path it is changed to $|\leftarrow\rangle$. Since only step (b) requires a split-up beam, it is necessary to perform only this spin manipulation within the IFM, whereas step (a) can be done already before the IFM, so that the spinor of the neutron beam entering the IFM is given by $|\rightarrow\rangle$. Applying a spin rotator before the IFM is of course trivial, it is rather the combination of the two aforesaid manipulations (a) and (b) that is new. For the realization of the above new method, we developed a new spin turner for the IFM as required for step (b), which was realized by an appropriate magnetic shielding in one of the two beam paths in the IFM. For this purpose a cylindrical tube made of Mu-metal was used with both ends open, where the neutron beam passes in axial direction through the tube, without touching any material (see Fig. 1). With our new, two stepped generation method of the Bell-like state (1) no material needs to be placed into the beam, so that by far less interference contrast loss in average was caused, which is crucial for the significance of such an experiment. The achieved overall mean contrast significantly exceeded the one achieved in the previous experiment [1].

Our new maximum value for S is

$$S = 2.202 \pm 0.007 > 2. \qquad (3)$$

This violates the Bell-like inequality by $\sim$29 standard deviations and so clearly confirms quantum contextuality.

Presently we are concerned with the generation of W and GHZ neutron states and corresponding entanglement witnesses.
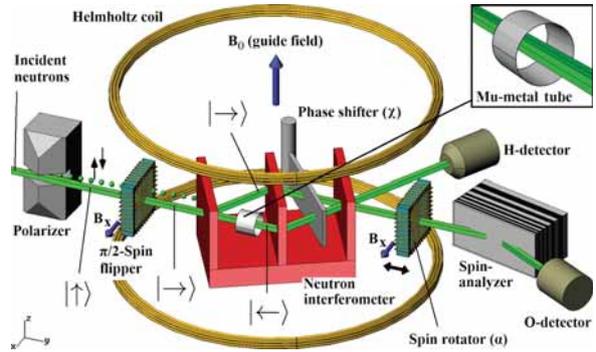
Figure 1: Sketch of the experimental setup

References

[1] Y. Hasegawa, R. Loidl, G. Badurek, M. Baron, and H. Rauch, *Nature (London)* **425**, 45 (2003).

[2] S. Sponar, J. Klepp, C. Zeiner, G. Badurek, and Y. Hasegawa, *Phys. Lett. A* **374**, 431 (2010).

[3] S. Sponar, J. Klepp, R. Loidl, S. Filipp, K. Durstberger-Rennhofer, R.A. Bertlmann, G. Badurek, Y. Hasegawa, and H. Rauch, *Phys. Rev. A* **81**, 042113 (2010).

[4] Y. Hasegawa and D. Erdősi, *AIP Conf. Proc.* **1384**, 214-217 (2011).

[5] S. Basu, S. Bandyopadhyay, G. Kar, and D. Home, *Phys. Lett. A* **279**, 281 (2001).

Optimal Strategies for Tests of EPR-Steering with No Detection Loophole

David Evans[1,2] and Howard M. Wiseman[1,2]

[1]*Centre for Quantum Dynamics, Griffith University, Brisbane QLD 4111, Australia*
[2]*ARC Centre for Quantum Computation and Communication Technology, Griffith University, Brisbane QLD 4111, Australia*

As demonstration of Bell nonlocality requires violation of a Bell inequality [1], so too does demonstration of EPR-Steering [2, 3] require the violation of EPR-Steering inequalities, which are less experimentally demanding than Bell inequalities.

Tests of EPR-Steering are such that one party's results are explicitly trusted, while the other is deemed untrustworthy. Therefore, in such tests, we need only account for the inefficiency in one of the two detectors necessary for experimental execution of the test (in contrast to a loophole-free Bell inequality, for which we would have to consider both detectors in this manner). When under a fair sampling assumption, a *detection loophole* is opened – the untrusted party (Alice) could take advantage of a claimed inefficiency in her detectors in order to falsely convince the other party (Bob) that she can steer his state. Closing such loopholes results in EPR-Steering inequalities becoming more difficult to violate experimentally. Therefore, it is worthwhile to know which EPR-Steering bounds are the easiest to violate while still being free of loopholes.

Derivations of EPR-Steering inequalities have been detailed in several publications [4], and recently, experimental EPR-Steering tests have been performed using these inequalities [5], even while closing the detection loophole [6, 7].

The EPR-Steering inequalities we will use are linear correlation functions between the measured spins of entangled qubit pairs (the same form as in [6]). They are of the form

$$S_n = -\frac{1}{n} \sum_k^n p_k \langle A_k \hat{\sigma}_k^\beta \rangle, \qquad (1)$$

where $\hat{\sigma}_k^\beta$ are Bob's observables, p_k are the weightings with which Bob uses each measurement, and A_k are Alice's reported results (we make no assumptions about whether they are actual measurement results or not). The number n is the number of different measurement settings used by Bob in the experiment.

EPR-Steering can be successfully demonstrated if (and only if) Alice and Bob genuinely share an entangled state with a correlation function, S_n, greater than or equal to $k_n(\epsilon)$, and Alice's detector efficiency is greater than or equal to ϵ.

We obtain EPR-Steering bounds by assuming Bob's measurements to be genuine and Alice's measurements to be fabricated using knowledge of Bob's local hidden state to imitate nonlocality as best possible. In this task, Alice is assumed to take advantage of her declared inefficiency, by declaring non-null results only when it is most favourable for her to do so.

In deriving EPR-Steering tests of this form, previous publications [5, 6] have employed the intuitive strategy of choosing qubit measurements that are equally spaced about the Bloch sphere. This equated to using the vertices of platonic solids to define Bob's measurement settings. However, this methodology was ultimately an educated best guess, and the results

of [6] actually show that this choice is not optimal. Specifically, for an efficiency of approximately $\epsilon = 0.5$, using $n = 3$ settings (octahedron vertices) was found to be more powerful than using $n = 4$ settings (cube vertices), showing that the latter cannot be optimal for $n = 4$ (see fig. 1). Optimisation of S_n for $n = 3$ and $n = 4$ yielded p_k and $\hat{\sigma}_k$ values from which we obtained the bounds shown in Figure 1 (for $n = 3$, the platonic bound was found to already be optimal).
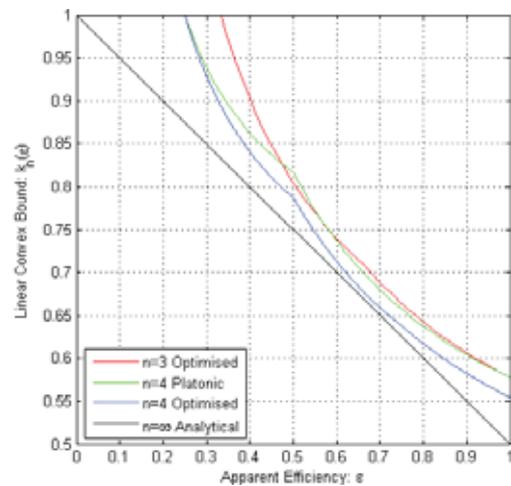
Figure 1: Optimal EPR-Steering bound when using at most 3 (red line) and 4 (blue line) measurements. The diagonal line is an analytical bound [3] for demonstrating EPR-Steering with infinitely many measurements.

References

[1] J.S. Bell, Physics **1**, 1950 (1964).

[2] E. Schrödinger, Naturwiss. **23**, 807 (1935).

[3] H. M. Wiseman, S. J. Jones, A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

[4] E. G. Cavalcanti, M. D. Reid, J. Mod Opt. **54**, 2373 (2007); E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, M. D. Reid, Phys. Rev. A **80**, 032112 (2009).

[5] D. J. Saunders, S. J. Jones, H. M.Wiseman, G. J. Pryde, Nat. Phys. **76**, 845-849 (2010).

[6] A. J. Bennet et al., arXiv:1111.0739 (2011).

[7] D. H. Smith et al., Nature Communications **3**, 625 (2012); B. Wittmann et al., arXiv:1111.0760 (2011).

Weak measurement statistics of correlations between input and output in quantum teleportation

Masanori Hiroishi[1] and **Holger F. Hofmann**[1,2]

[1]*Graduate School of Advanced Sciences of Matter, Hiroshima University*
[2]*JST, CREST, Tokyo, Japan*

In quantum teleportation, if an input state $\mid \psi \rangle_A$ and system R of the Bell state $\mid E \rangle_{RB}$ are projected onto a Bell state of the same type $\mid E \rangle_{AR}$, the remote system B of the first Bell state is projected onto the state $\mid \psi \rangle_B$, which is identical to the input state. Although the Bell measurement is necessary to define the output state $\mid \psi \rangle_B$, there is no evidence of any physical change in the system B at the time of the Bell measurement, and quantum theory is consistent with the assumption that any measurement performed on B will have the same result, whether it occurs before or after the Bell measurement. From a statistical viewpoint, this suggests that the state $\mid \psi \rangle_B$ might represent a subensemble that was already part of the statistics of system B even before the Bell measurement selected it.

The idea that the Bell measurement merely post-selects a subensemble corresponds to the statistical interpretation of weak measurements. Specifically, weak measurements can be used to investigate the statistical properties of post-selected ensembles in detail. Recently, the theory of weak measurements was used to show that the input state $\mid \psi \rangle$ of quantum teleportation seems to appear simultaneously in systems A and B before the Bell measurement [1]. However, weak measurement theory may provide even more details about the teleportation process. In particular, we can also analyze the joint state of A and B to find out about the kind of correlations between A and B that could be observed in post-selected weak measurements. In this presentation, we show that the two systems are in fact correlated, even though each local system is described by the pure state $\mid \psi \rangle$. We point out that these correlations can be interpreted as identical quantum fluctuations, indicating that the teleportation process transfers all physical properties equally, independent of the input state.

As shown in [2], weak measurement statistics can be summarized by a transient state $\hat{R}_m$ given by the normalized product of the initial density matrix $\hat{\rho}_I$ and the final measurement operator $\hat{\Pi}_m$,

$$\hat{R}_m = \frac{\hat{\rho}_I \hat{\Pi}_m}{\mathrm{Tr}(\hat{\rho}_I \hat{\Pi}_m)} \qquad (1)$$

In analogy to the derivation of expectation values from density operators, the weak value of any obserbable $\hat{O}$ can be determined from the product tace $\mathrm{Tr}(\hat{R}_m \hat{O})$. Therefore, $\hat{R}_m$ can be interpreted as a representation of the quantum state between preparation and post-selection. We can apply this theory to quantum teleportation to obtain a compact description of the complete quantum statistics between the preparation of the entangled state and the Bell measurement. The initial state $\hat{\rho}_I$ is $\mid \psi \rangle_A \langle \psi \mid \otimes \mid E \rangle_{RB} \langle E \mid$ and the measurement operator $\hat{\Pi}_m$ of the Bell measurement is $\hat{U}_A(m) \mid E \rangle_{AR} \langle E \mid \hat{U}_A^\dagger(m) \otimes \hat{I}_B$. Here, the identity $\hat{I}_B$ in the measurement operator indicates that we do not consider any final measurement

on system B. After tracing out system R, the transient state of systems A and B is given by

$$\hat{R}_m^{(AB)} = \sum_k \mid \psi \rangle_A \langle k \mid \hat{U}(m)^\dagger \otimes \mid k \rangle_B \langle \psi \mid \hat{U}(m). \qquad (2)$$

Clearly, this state is not a product of a state in A and a statistically independent state in B. Instead, the sum over the arbitrary orthogonal basis $\mid k \rangle$ indicates some kind of correlation between the systems. Still, the partial traces of the result both seem to describe the pure state $\mid \psi \rangle$ or its unitary transforms,

$$\hat{R}_m^{(A)} = \mid \psi \rangle_A \langle \psi \mid, \quad \hat{R}_m^{(B)} = \hat{U}(m)^\dagger \mid \psi \rangle_B \langle \psi \mid \hat{U}(m) \qquad (3)$$

In particular, post-selecting the case of $U(m) = \hat{I}$ result in the apparent co-existence of $\mid \psi \rangle$ in systems A and B before the measurement, which is the result that was identified with cloning in [1].

What kind of correlation does eq.(2) describe when both systems appear to be "clones" of the input state $\mid \psi \rangle$? To find this out, we can apply a projection onto the same orthogonal basis $\{\mid a \rangle\}$ to both systems in $R_{\hat{U}=\hat{I}}^{(AB)}$. The result are the weak values of conditional probabilities for a and a', given by

$$\mathrm{Tr}\{\hat{R}_{\hat{U}=\hat{I}}^{(AB)}(\mid a \rangle_A \langle a \mid \otimes \mid a' \rangle_B \langle a' \mid)\} = \delta_{a,a'} \mid \langle a \mid \psi \rangle \mid^2 \qquad (4)$$

Interestingly, this result is all positive and looks just like a classical probability distribution, where the values of a and a' must always be equal, but are otherwise distributed according to the standard probability of measuring a in $\mid \psi \rangle$. This means that the state $\hat{R}_{\hat{U}=\hat{I}}^{(AB)}$ describes perfect correlations between the quantum fluctuations in the input system A and the output system B, indicating that the teleportation process transfers all physical properties, not just the eigenvalues of the input state. It might also be worth noting that the same statistical structure can be observed in the correlation between optimally cloned systems [3], indicating that quantum processes act on physical properties even when they are not defined by the initial state.

References

[1] E. Sjöqvist, J. Åberg, Phys. Lett. A **354**, 396 (2006).

[2] H. F. Hofmann, Phys. Rev. A **81**, 012103 (2010).

[3] H. F. Hofmann, e-print arXiv:1111.5910v2 (2011).

Optimal cloning as a universal quantum measurement: resolution, back-action, and joint probabilities

Holger F. Hofmann[1,2]

[1]Hiroshima University, Higashi Hiroshima, Japan
[2]JST-CREST, Tokyo, Japan

It is a fundamental law of quantum mechanics that non-commuting observables cannot be measured jointly since there are no common eigenstates that could represent the outcomes of such joint measurements. In more intuitive terms, it is often said that the measurement of one property must disturb the system in such a way that the other property can change its value in an uncontrolled way. Following this intuitive logic about the values of observables, it is clear that quantum mechanics cannot allow perfect cloning, because a perfect copy of all physical properties would result in perfect simultaneous measurements of any two observables. It should therefore be possible to identify the no-cloning theorem with the uncertainty principle and the limits of optimal cloning with the uncertainty limits of measurement theory. However, cloning is usually evaluated and discussed in terms of quantum state fidelities, not in terms of measurement errors. It may therefore be necessary to re-examine the statistical properties of cloning in the light of measurement statistics to achieve a better understanding of the general physics involved [1].

In this presentation, I will approach the problem in terms of measurement theory. In general, cloning is similar to quantum measurement since the goal of the cloning interaction is to reproduce a target observable in a different system. The difference is that measurement usually targets a specific observable, while universal cloning must consider all observables equally because the input state may be an eigenstate of any property of the system. In this sense, the cloning process describes a universal measurement interaction, where information about all possible observables is transferred to the meter (that is, to the clone). It is then possible to perform any measurement on the system by reading out the meter in an appropriate measurement basis $\{\mid a\rangle\}$, where the cloning fidelity now represents the accuracy of the measurement. Since the accuracy should be the same for every possible measurement, the back-action must be completely isotropic in Hilbert space. The back-action can therefore be described by the addition of a white noise background to the density matrix, which defines the reduction of cloning fidelity in the original system. Thus, cloning fidelities can be identified with the measurement resolution and the measurement back-action of a universal quantum measurement.

Using the well-known formalism for optimal universal cloning, it is possible to derive the linear map $E_a(\hat{\rho})$ that describes the measurement process for the measurement basis $\{\mid a\rangle\}$,

$$E_a(\hat{\rho}) = \frac{1}{2d+2}\left(\hat{\rho} + \langle a\mid \hat{\rho}\mid a\rangle\hat{I} + \hat{\rho}\mid a\rangle\langle a\mid + \mid a\rangle\langle a\mid \hat{\rho}\right). \quad (1)$$

These operators describe the effects of a measurement of a performed by cloning the system and measuring the clone.

Specifically, the measurement probabilities are given by

$$p(a) = \mathrm{Tr}\left(E_a(\hat{\rho})\right) = \frac{d+2}{2d+2}\langle a\mid \hat{\rho}\mid a\rangle + \frac{1}{2d+2}, \quad (2)$$

and the back action is given by

$$\hat{\rho}_{\mathrm{out}} = \sum_a E_a(\hat{\rho}) = \frac{d+2}{2d+2}\hat{\rho} + \frac{1}{2d+2}\hat{I}. \quad (3)$$

It is therefore possible to re-formulate universal cloning as a measurement process acting on a single input system, where the clone is used as a meter for an arbitrary physical property of the system. Significantly, the measurement interaction is now independent of the physical property to be probed, and the measurement back-action affects all physical properties equally.

As pointed out in [1], the cloning process itself can be interpreted as a statistical mixture of swap, no swap, and perfect copying. In terms of measurements, this translates into perfect transmission without measurement ($E_a(\rho) = \rho$), perfect measurement and replacement of the input with white noise ($E_a(\rho) = \hat{I}/d$), and a perfect back-action free measurement represented by the non-positive operation

$$E_a^{\mathrm{ideal}}(\hat{\rho}) = \frac{1}{2}\left(\hat{\rho}\mid a\rangle\langle a\mid + \mid a\rangle\langle a\mid \hat{\rho}\right). \quad (4)$$

Interestingly, the output state for this back-action free measurement is identical to the post-selected transient state obtained by weak measurement tomography [2]. The analysis of the cloning measurement as mixture of measurement errors with a non-positive representation of uncertainty-free measurement is therefore consistent with the interpretation of weak measurement statistics as quantum statistics conditioned by the final measurement outcome of a. However, in the present measurement by quantum cloning, a is the measurement result obtained from the meter system and the conditional quantum state appears as a non-negligible component of the actual output density matrix, where positivity is ensured by additions of the original density matrix $\hat{\rho}$ and white noise $\hat{I}/d$ according to Eq. (1). Thus measurements by quantum cloning can provide a more direct access to conditional quantum statistics than post-selected weak measurements [1].

References

[1] H. F. Hofmann, e-print arXiv:1111.5910v2

[2] H. F. Hofmann, Phys. Rev. A 81, 012103 (2010).

at t e comple joint probabilities observed in eak measurements can tell us about quantum p sics

Holger F. Hofmann[1,2]

[1]Hiroshima University, Higashi Hiroshima, Japan
[2]JST-CREST, Tokyo, Japan

In physics, measurements should tell us all we need to know about the reality of physical objects. It is therefore extremely perplexing that quantum measurement fails to do so. At the very heart of this failure lies the uncertainty principle: although the outcomes of individual measurements appear real enough, measurements cannot provide us with a satisfactory characteri ation of the relation between non-commuting properties. Recently, weak measurements are attracting a lot of attention because they appear to offer a solution to the problem of measurement uncertainty: by reducing the measurement interaction to negligible levels, weak measurements can obtain statistical information about properties that do not commute with a precise final measurement of a different property. In principle, weak measurements can therefore measure correlations between non-commuting properties of a system and address questions that seemed to be fundamentally inaccessible in conventional quantum measurements.

Several experiments have already shown that quantum paradoxes can be explained as a consequence of negative conditional probabilities observed in weak measurements (see [1] and references therein). However, such resolutions of quantum paradoxes do not really explain why negative probabilities appear in the first place. For a more complete understanding of quatum physics, it would be desirable to understand why an extension of statistics to non-positive and even complex values could be helpful, and how these complex probabilities relate to the more familiar notions of quantum coherence known from coventional approaches to quantum physics. In this presentation, I address these questions by showing that the structure of complex joint probabilities provides a natural link between classical phase space and Hilbert space. The transformation laws that describe the relation between non-commuting properties can then provide new insights into the nature of dynamics and time dependence in quantum mechanics that might change the way we think about fundamental physics.

omplex joint probabilities arise naturally in the quantum formalism as a consequence of quantum coherence. In the case of pure states, the complex phases of weak conditional probabilities provide a direct description of the coherent wavefunction [2]. For a general density matrix $\hat{\rho}$, the joint probability $\rho(a, b)$ of two measurement outcomes represented by the non-orthogonal quantum states $| a \rangle$ and $| b \rangle$ is

$$\rho(a, b) = \langle b | a \rangle \langle a | \hat{\rho} | b \rangle. \tag{1}$$

This joint probability corresponds to a mixed representation of the density matrix, where the left side of the matrix is expressed in the a-basis, and the right side is expressed in the b-basis. The complex joint probabilities $\rho(a, b)$ obtained in weak measurements of a and final measurements of b therefore provide complete descriptions of arbitrary quantum states in any Hilbert space [3, 4].

Interestingly, the joint probabilities given by (1) were already considered in the early days of quantum mechanics, when irkwood introduced the complex joint probability $\rho(x, p)$ as a possible representation of phase space statistics [5]. It therefore seems only natural to interpret $\rho(a, b)$ as the quantum limit of phase space statistics. However, there is one fundamental difference between a classical phase space point and the quasi-reality described by (a, b). At a phase space point, all physical properties should be defined as functions of the parameters a and b. In particular, the transformation to a new parameteri ation (c, b) should be represented by a deterministic function $c = f_c(a, b)$ that assigns a well-defined value of c to every phase space point. ppositely, quantum mechanics defines the change from (a, b) to (c, b) as a unitary transformation in Hilbert space. Using this standard formalism, it is possible to show that the probablities are transformed by a complex valued scattering process, where the contribution of (a, b) to (c, b) is given by the complex conditional probabilities $p(c|a, b)$ of weak measurement statistics [4]. However, this process is merely a change of representation, and therefore cannot describe any random effects. This observation motivates a new definition of determinism that can also be applied in the quantum limit: a scattering process described by conditional probabilities is reversible and therefore deterministic, if (and only if) the following relation holds:

$$\sum_c p(a'|c, b) p(c|a, b) = \delta_{a, a'}. \tag{2}$$

This definition of quantum determinism shows why the relation between non-commuting observables con icts with realist interpretations. Since observables at different times can be represented by non-commuting operators in the same Hilbert space, this result has important implications for the dynamics of quantum systems. In particular, it can be shown how established notions of trajectories, such as the orbitals of bound states or Feynman paths, and possible alternatives such as the ohmian trajectories recently reconstructed from weak measurement results [ ] emerge from the more fundamental concept of quantum determinism.

References

[1] H. F. Hofmann, ew . Phys. , 103009 (2011).

[2] . S. undeen et al., ature (ondon) , 1 (2011).

[3] . S. undeen and . amber, Phys. Rev. ett. 8, 0 0402 (2012).

[4] H. F. Hofmann, e-print arXiv:1111.5910v2, to be published in ew . Phys.

[5] . . irkwood, Phys. Rev. , 31 (1933).

[ ] S. ocsis et al. Science , 11 0 (2011).

Twin Quantum Cheshire Photons

Issam Ibnouhsein[1,2]**, Alexei Grinbaum**[1]

[1]*CEA Saclay, Gif-sur-Yvette, France*
[2]*Universite Paris-Sud, Orsay, France*

Abstract: In experiments with pre- and post-selection, one can separate path and polarization degrees of freedom of a photon [2]. We generalize this result to four degrees of freedom.

Basic concepts: Post-selection is the power of discarding all runs of an experiment in which a given event does not occur [2]. Formally we define a pre-selected (or prepared) state $|\psi\rangle$ and a post-selected one $\langle\phi|$ and define the weak value of an operator $\mathcal{O}$ with pre- and post-selected states $|\psi\rangle$ and $\langle\phi|$ as [1]:

$$\langle\mathcal{O}\rangle_w = \frac{\langle\phi|\mathcal{O}|\psi\rangle}{\langle\phi|\psi\rangle}. \qquad (1)$$

Formalism: Our pre- and post-selected states for the first experiment are:

$$|\psi\rangle = \frac{|13\rangle + |14\rangle + |23\rangle + |24\rangle}{2} \otimes |A\rangle, \qquad (2)$$

$$\langle\phi_1| = \frac{(\langle13| + \langle24|) \otimes \langle A| + (\langle14| - \langle23|) \otimes \langle B|}{2}, \qquad (3)$$

where $|A\rangle = \frac{|H,V\rangle + |V,H\rangle}{\sqrt{2}}$, and $\langle B| = \frac{\langle H,V| - \langle V,H|}{\sqrt{2}}$. $|H\rangle$ and $|V\rangle$ denote horizontally and vertically polarized light respectively. Note that $\langle A|B\rangle = 0$.

The post-selected state for the second experiment is:

$$\langle\phi_2| = \frac{\langle13| \otimes \langle A| + (\langle14| - \langle23| - \langle24|) \otimes \langle B|}{2}. \qquad (4)$$

Define position measurement operators:

$$\Pi_{ij} = |ijHV\rangle\langle VHji| + |ijVH\rangle\langle HVji|, \qquad (5)$$

$$\Pi_{i\cdot} = \Pi_{i1} + \Pi_{i2}, \qquad (6)$$

$$\Pi_{\cdot j} = \Pi_{1j} + \Pi_{2j}, \qquad (7)$$

where i (resp. j) denotes the arm of the left (right) interferometer on which measurement is performed. The dot $\cdot$ represents a measurement carried on both arms of the corresponding interferometer, which is equivalent to tracing out one of the entangled particles.

A measurement of polarization along axis α for the first photon and β for the second photon in arms i and j ($i = 1, 2; j = 3, 4$) corresponds to the operator:

$$\sigma_{\alpha\beta}^{ij} = \Pi_{ij}\sigma_{\alpha\beta}. \qquad (8)$$

Trace out one of the particles:

$$\sigma_{\alpha\beta}^{i\cdot} = \Pi_{i\cdot}\sigma_{\alpha\beta}, \qquad (9)$$

$$\sigma_{\alpha\beta}^{\cdot j} = \Pi_{\cdot j}\sigma_{\alpha\beta}. \qquad (10)$$

Experimental Setup: The Mach-Zender interferometers are so tuned that both detectors in the pair (D11,D22) or in the pair (D12,D21) always click, whereas D13 and D23 never click. Post-selection is implemented in the first experiment by inserting half-wave plates (HWP) at some arms of the interferometer.
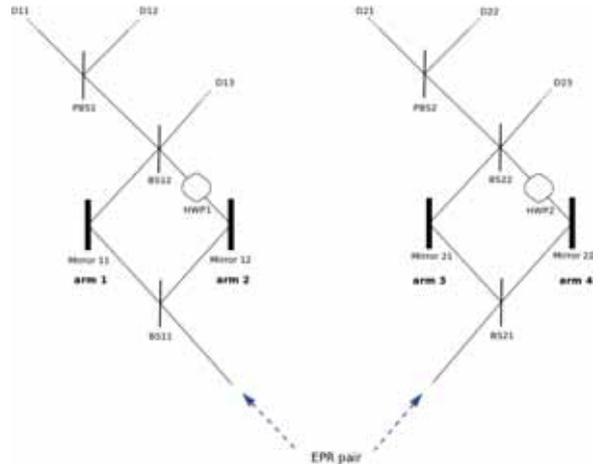
Figure 1: EPR pair entering two MZ interferometers.

Results: The results of the first experiment ($\langle\phi1||\psi\rangle$) are:

Pola. Meas.	σ_{zz}^{13}	σ_{zz}^{14}	σ_{zz}^{23}	σ_{zz}^{24}	$\sigma_{zz}^{1\cdot}$	$\sigma_{zz}^{2\cdot}$	$\sigma_{zz}^{3\cdot}$	$\sigma_{zz}^{4\cdot}$
Weak Values	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Pola. Meas.	σ_{zx}^{13}	σ_{zx}^{14}	σ_{zx}^{23}	σ_{zx}^{24}	$\sigma_{zx}^{1\cdot}$	$\sigma_{zx}^{2\cdot}$	$\sigma_{zx}^{3\cdot}$	$\sigma_{zx}^{4\cdot}$
Weak Values	0	$\frac{1}{2}$	$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$

The results of the second experiment ($\langle\phi2||\psi\rangle$) are:

Pola. Meas.	σ_{zz}^{13}	σ_{zz}^{14}	σ_{zz}^{23}	σ_{zz}^{24}	$\sigma_{zz}^{1\cdot}$	$\sigma_{zz}^{2\cdot}$	$\sigma_{zz}^{3\cdot}$	$\sigma_{zz}^{4\cdot}$
Weak Values	1	0	0	0	1	0	1	0
Pola. Meas.	σ_{zx}^{13}	σ_{zx}^{14}	σ_{zx}^{23}	σ_{zx}^{24}	$\sigma_{zx}^{1\cdot}$	$\sigma_{zx}^{2\cdot}$	$\sigma_{zx}^{3\cdot}$	$\sigma_{zx}^{4\cdot}$
Weak Values	0	-1	1	1	-1	2	1	0

Note that $\langle\sigma_{zx}^{2\cdot}\rangle_w = 2$ and $\langle\sigma_{zx}^{1\cdot}\rangle_w = -1$: interesting effects arise when a system weakly interacts with arms 1 or 2.

Conclusions: We have shown that the disembodiment of physical properties from objects to which they supposedly belong in pre- and post-selected experiments can be generalized to more than two degrees of freedom. It appears even stronger since the correspondence between objects and properties is completely lost in some situations. The results can be extended to more general situations: for example, a separation of the spin from the charge of an electron, or the mass of an atom from the atom itself [2].

References

[1] Y.Aharonov, A.Botero, S.Popescu, B.Reznik, and J.Tollaksen. *Phys. Lett. A*, 301(3-4):130–138, 2002.

[2] Y.Aharonov, S.Popescu, and P.Skrzypczyk. *arxiv:1202.0631v1*.

Decoherence due to spatially correlated fluctuations in the environment

Jan Jeske, Jared H. Cole

Chemical and Quantum Physics, School of Applied Sciences, RMIT University, Melbourne 3001, Australia

Motivation

Decoherence is the environmentally induced loss of phase coherence between states in quantum mechanical systems. This process destroys superposition effects and reduces the dynamics of the system to that of a classical ensemble. It is one of the major limiting factors for most applications of quantum systems, in particular the use of quantum two-level systems for computational purposes.

As both experimental and theoretical modelling capabilities increase to larger systems, individual subsystems are influenced by environmental fluctuations which cause decoherence effects and the spatial correlations of these fluctuations become relevant. Spatially correlated decoherence in qubit systems also relates to quantum error correction where correlated errors can require their own correction codes[1] but can also lead to a better performance of the correction process[2]. A theory of spatially correlated decoherence may even find application in such unusual fields as quantum biology, where the intricate interplay between delocalized excitations and decoherence mechanisms has been suggested to play a key role in photosynthetic systems[3, 4, 5].

Formalism

Two common master equations for decoherence modelling are the Lindblad equations and the Bloch-Redfield equations. The Lindblad equations guarantee physical behaviour (i.e. complete positivity) of the time evolution via their mathematical form. The free parameters in the Lindblad equations are essentially chosen phenomenologically although in some circumstances they can be derived from a physical model. The Bloch-Redfield equations are more sophisticated to set up and to work with, however they derive from a more physically motivated model with a system-environment coupling operator $H_{int} = \sum_j s_j B_j$, where s_j and B_j refer to system and environmental operators respectively.

In both master equations decoherence is usually modelled as either a collective effect with just one environmental "bath" which couples to all subsystems at once or as an individual effect with several uncorrelated "baths" each coupling to one subsystem. We present a formalism beyond the usual models of decoherence to incorporate spatial correlations in the environmental fluctuations and to derive the resulting decoherence rates for the system. In our formalism we extend the Bloch-Redfield equations and add a spatial contribution to the spectral noise function. In the eigenbasis of the system Hamiltonian H_s the equations then read:

$$\dot{\rho} = i[\rho, H_s] + \sum_{j,k} \left(-s_j q_{jk}\rho + q_{jk}\rho s_j - \rho \hat{q}_{jk} s_j + s_j \rho \hat{q}_{jk} \right)$$

where ρ is the system's density matrix, s_j are the system operators that couple to the environment and the elements of q_{jk} and $\hat{q}_{jk}$ are defined as:

$$\langle a|q_{jk}|b\rangle := \langle a|s_k|b\rangle C_{jk}(\omega_b - \omega_a, \vec{r}_j, \vec{r}_k)/2$$
$$\langle a|\hat{q}_{jk}|b\rangle := \langle a|s_k|b\rangle C_{kj}(\omega_a - \omega_b, \vec{r}_k, \vec{r}_j)/2$$

where ω_a is the a-th diagonal element of H_s, i.e. an eigenvalue. The spectral function $C_{j,k}(\omega, \vec{r}_j, \vec{r}_k)$ represents a Fourier transform of a temporal correlation function of the bath[1]:

$$C_{j,k}(\omega, \vec{r}_j, \vec{r}_k) := \int_{-\infty}^{\infty} d\tau \, e^{i\omega\tau} \langle \tilde{B}_j(\tau, \vec{r}_j)\tilde{B}_k(0, \vec{r}_k)\rangle$$

and determines the frequency spectrum of the environmental fluctuations, where we add a dependency on the spatial positions $\vec{r}_j$ and $\vec{r}_k$ of the respective bath operators B_j and B_k. This allows empirical models of spatial correlations by assuming any suitable function of spatial dependency. Typically this function will decay with increasing distance $|\vec{r}_j - \vec{r}_k|$ and the decay will have a characteristic correlation length ξ. In many cases the resulting master equations can be rewritten in Lindblad form, although this is not guaranteed for an arbitrary form of the spatial correlations.

Spatially correlated decoherence in spin chains

This formalism is then applied to a chain of two-level systems (TLS) with nearest neighbour coupling. Numerical solutions show that the decoherence is heavily influenced by the correlation length ξ of the environmental fluctuations. For uncoupled TLS a large correlation length leads to a relaxation-free subspace. For coupled TLS the system dynamics is preserved when the correlation length ξ is longer than the packet width of an excitation passing through the chain.

A deeper understanding of spatially correlated decoherence provides a method for modelling large-size quantum systems taking into account any appropriate model of spatial correlations in the environment. This may also lead to new ways of suppressing decoherence effects in spatially distributed systems.

References

[1] R. Alicki et al, Phys. Rev. A, **65**, 062101, 2002.

[2] A. Shabani, Phys. Rev. A, **77**, 022323, 2008.

[3] J. A. Davis et al, New J. Phys., **12**(8), 085015, 2010.

[4] G. S. Engel et al, Nature, **446**(7137), 782–786, 2007.

[5] M. B. Plenio et al, New J. Phys., **10**(11), 113019, 2008.

---

[1] The bath operators $\tilde{B}_j$ in this notation are taken in the interaction picture of the system-environment interaction.

Cavity optomechanics with a nonlinear photonic crystal nanomembrane

Thomas Antoni[1,2], **Kevin Makles**[1], **Rémy Braive**[2,3], **Aurélien Kuhn**[1], **Tristan Briant**[1], **Pierre-François Cohadon**[1], **Alexios Beveratos**[2], **Izo Abram**[2], **Luc Le Gratiet**[2], **Isabelle Sagnes**[2], **Isabelle Robert–Philip**[2], **Antoine Heidmann**[1]

[1]*Laboratoire Kastler Brossel, UPMC-ENS-CNRS,*
Case 74, 4 place Jussieu, F75252 Paris Cedex 05, France
[2]*Laboratoire de Photonique et Nanostructures LPN-CNRS, UPR-20,*
Route de Nozay, 91460 Marcoussis, France
[3]*Université Paris Diderot, 75205 Paris, Cedex 13, France*

Cavity optomechanics is a very efficient technique to cool down a mechanical resonator and observe its quantum ground state. Small displacement detection and optical cooling require a very high finesse cavity. This is usually obtained using dielectric Bragg mirrors but such optical coatings limit the mass of the resonators to a few tens of micrograms whereas downsizing the resonators would allow a better coupling to radiation pressure [1]. Multilayer coatings are furthermore responsible for mechanical losses that limit the mechanical quality factor of the resonators, hence the possibility to optically cool them.

To overcome these limitations, we developed $30 \times 30 \times 0.260 \ \mu$m indium phosphide photonic crystal slabs, that do not make use of optical coating anymore and have masses about a hundred of picograms. We took advantage of slow optical modes coupled to normal incidence radiation in square photonic crystal lattices to obtain a good reflectivity at normal incidence, about 95% for optical waists as small as 2.5 μm [2]. We also developed specific coupling mirrors with small radius of curvature to build a Fabry-Perot cavity with a small optical waist (3.5 μm) using such a fully-clamped suspended membrane as an end mirror. Optical finesse larger than 100 was measured, yielding to a shot-noise limited sensitivity about $\delta x_{\min} = 2 \times 10^{-17}$ m/$\sqrt{\text{Hz}}$.
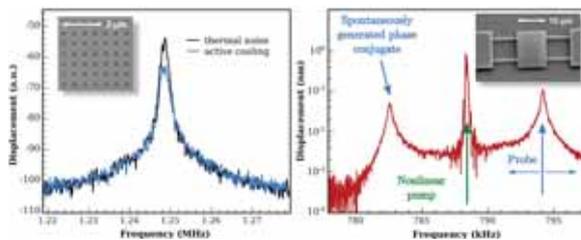
Figure 1: Left: thermal noise and active cooling of a fully clamped photonic crystal membrane (inset). Right: nonlinear behavior of geometrically optimized suspended nanomembranes (inset).

We observed the thermal noise of the membrane and characterized mechanical modes in the megahertz range with mechanical quality factors about 500 (see figure 1 left). We used a piezo actuation to drive the membrane into motion and reduce its temperature by a cold-damping feedback loop [3]. We were able to cool the modes by a factor of two from room temperature.

For mechanical resonators with frequencies in the megahertz range, the classical to quantum transition is expected at a few hundreds of micro-kelvins. As a consequence, mechan-ical quality factors greater than one thousand are required to allow optical cooling over two orders of magnitude from dilution cryostat temperatures. To this end, we worked on the design of the photonic crystal nanomembranes with a geometry optimized to limit clamping losses [2]. We were able to fabricate membranes with quality factors about 4 000. With these characteristics, the membrane has zero-point quantum fluctuations about $\delta x_Q = 5 \times 10^{-17}$ m/$\sqrt{\text{Hz}}$, larger than the sensitivity expected for our cavity.

Due to their geometry and very small scales, these resonators exhibit a very strong nonlinear behavior [4]. This feature turns out to have a dramatic impact on the dynamics of a mechanical mode, as well as an intermodal effect observed on the frequency shift of a second mode when a first mode is actuated in its nonlinear regime. We proceeded to study the underlying nonlinear dynamics, both by monitoring the phase-space trajectory of the free resonator and by characterizing the mechanical response in presence of a strong pump excitation. We observed in particular the frequency evolution during a ring-down oscillation decay, and the emergence of a phase conjugate mechanical response to a weaker probe actuation; the mechanical response exhibits both a resonance at a frequency above the pump frequency and a spontaneously generated mechanical motion at a lower frequency symmetrically located below the pump frequency (see figure 1 right)

Besides this new physics, the combination of optical and mechanical characteristics of the membranes would allow to perform cold-damping cooling in a dilution fridge down to a temperature low enough to observe their quantum ground state. In addition, due to the versatility of the photonic crystal design and compactness of the cavity, integrated optomechanics applications can be foreseen.

References

[1] P. Verlot et al., C. R. Physique **12**, 797 (2011).

[2] T. Antoni et al., Optics Letters **17**, 3436 (2011).

[3] P.-F. Cohadon et al., Phys. Rev. Lett. **83**, 3174 (1999).

[4] T. Antoni et al., arXiv:1202.3675/ .

Towards realization and detection of a non-Gaussian quantum state of an atomic ensemble.

Stefan L. Christensen[1], **Jürgen Appel**[1], **Jean-Baptiste Béguin**[1], **Heidi L. Sørensen**[1] **and Eugene S. Polzik**[1]

[1]*QUANTOP, Niels Bohr Institute, University of Copenhagen, Denmark*

Non-Gaussian states of atomic ensembles are an important prerequisite for continuous variable quantum information processing and can be a valuable resource for quantum metrology applications [1, 2, 3]. We are working towards engineering such a state in a dipole-trapped ensemble of Cs atoms. The experimental apparatus is described in [4, 5]. On a daily basis this setup is capable of resolving the atomic projection noise, which we verify by scaling analysis (see figure 1). By performing quantum non-demolition measurements of the atomic population difference in the clock-levels using a dispersive dual-color probing-scheme we can produce spin squeezed states in the ensemble, both in terms of Holstein-Primakoff-quadrature operators as well as with respect to the angular uncertainty of the macroscopic pseudo-spin.
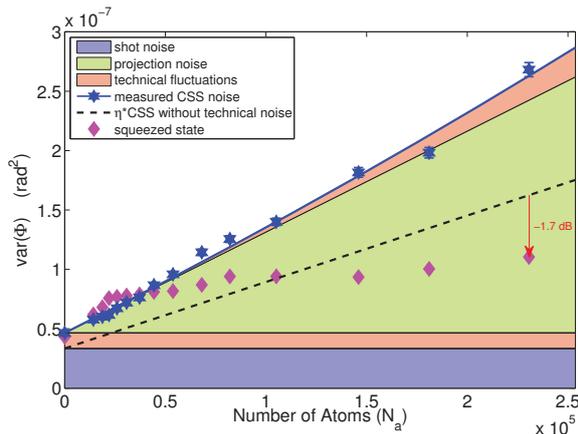
Figure 1: Blue points: Light phase fluctuations for different atom numbers for a coherent spin state(CSS). The scaling of the noise as a function of the number of atoms N_a allows us to identify noise contributions: blue area: light shot noise, green area: atomic projection noise, red areas: technical fluctuations. Black dashed line: predicted noise for a CSS. Magenta diamonds: Noise for a squeezed state.

We are now looking to produce more exotic quantum states in the ensemble, and currently focus on the generation of a single excitation state. This clearly non-Gaussian state is prepared as follows: We load $N \approx 10^5$ Cs atoms from a MOT into a far off resonant dipole trap formed by the $40 \mu m$ Waist of a 10W laser with a wavelength of $\lambda = 1064nm$. By combining optical pumping, microwave (MW) pulses, and optical purification pulses we prepare all atoms in the upper hyperfine ground state. The idea is now to generate a weak excitation, using a dim pulse, resonant with the $|F = 4, m_F = 0\rangle \rightarrow |F' = 4, m_F = +1\rangle$ D_2-transition. As this requires that we can resolve the different Zeeman lev-

els of the $F = 4$ excited states, we apply a magnetic bias field of $|B| \approx 20$ Gauss, splitting the $|F' = 4, m_F = -1\rangle$ and $|F' = 4, m_F = +1\rangle$ excited states by several linewidths. The excitation pulse excites some of the atoms, which can now decay through several different channels. Both polarization and frequency filtering allow us to discriminate against all but two decay channels. Conditioned on the detection of a single photon we know that with a probability of $\approx 2/3$ a single atom has been scattered into the lower $|F = 3, m_F = 0\rangle$ clock level and the collective quantum state of the example is now described by

$$|\Psi> = \sum_{i=1}^{N_a} |\uparrow\uparrow \cdots \uparrow\downarrow_i\uparrow \cdots \uparrow> . \qquad (1)$$

With the ensemble in this superposition state, we apply a MW $\pi/2$-pulse with varying phase, which will make the single atom interfere with the remaining ground state atoms.

We then perform a strong dispersive quantum non-demolition measurement of the population difference to analyze the atomic state. Repeating this several thousand times allows us to infer the marginal distribution of the non-Gaussian Wigner function of this single excitation state and to compare this to a coherent superposition state, which displays a Gaussian Wigner function.

References

[1] J.I. Cirac, P. Zoller, H.J. Kimble and H. Mabuchi, Phys. Rev. Lett. 78, 3221–3224 (1997)

[2] N. Brunner, E.S. Polzik and C. Simon, Phys. Rev. A. 84, 041804(R) (2011)

[3] M. Ohliger, K. Kieling and J. Eisert, Phys. Rev. A 82, 042336 (2010)

[4] J. Appel, P.J. Windpassinger, D. Oblak, U.B. Hoff, N. Kjærgaard and E.S. Polzik, PNAS vol. 106 no. 27 10960-10965 (2009)

[5] A. Louchet-Chauvet, J. Appel, J.J. Renema, D. Oblak, N. Kjærgaard and E.S. Polzik, New J. Phys. 12 065032 (2010)

Quantum and Classical Measurements: Information as a Metric of Quality

Thomas B. Bahder

Charles M. Bowden Research Facility
Aviation and Missile Research, Development, and Engineering Center
US Army RDECOM
Redstone Arsenal, AL 35898 U.S.A.

In recent years, much work has gone into exploring the advantages of quantum measurements over classical measurements. It is generally believed that quantum measurements, which often exploit entanglement, can provide greater accuracy than classical measurements, see for example Ref [1] and references contained therein. The metric used to compare the accuracy of a measurement is often the standard deviation of a measurement that is repeated a number of times. In both cases of quantum and classical measurements, there exists a conditional probability distribution, $P(\xi|\phi,\rho)$, which is the probability of measuring ξ given that there are one or more parameters ϕ in the experiment, and the state of the system is represented by ρ. The conditional probability distribution, $P(\xi|\phi,\rho)$, enters into the definition of information measures, such as Fisher information [2] and fidelity [3], which is the Shannon mutual information [4] between measurements and physical quantities.

Historically, the quality of measurements has been discussed in terms of parameter estimation [5], using the Fisher information to provide an upper bound on the variance of an unbiased estimator through the Cramér-Rao inequality [6, 7]. I argue that there are two objections against using the Fisher information as a measure of the quality of measurements. First, the Fisher information may depend on the unknown physical quantity (parameter ϕ to be determined), which may occur when dissipation is present [7]. Second, the Fisher information does not take into account prior information about the parameter, as does the fidelity. Therefore, depending on the question to be answered, the fidelity (defined as the Shannon mutual information between measurements and physical quantities) may be a better measure of the quality of a measurement [3, 7]. The fidelity does not suffer from the two objections raised against the Fisher information. Also, the fidelity is sufficiently general that it allows the comparison of classical and quantum measurement experiments, to determine which is a better measurement device (experiment) overall.

The goal of any experiment is to determine some physical quantity, ϕ. However, in most cases, the quantity that is directly measured is ξ, not the quantity ϕ that we intend to determine through the experiment. For example, we may want to determine a wavelength of an atomic optical transition, however, the quantity that we directly measure may be a voltage. The question arises: how good is our measurement of the wavelength? Another important question is: given two different experiments that attempt to determine the wavelength, which experiment is better? To answer this question, I propose the use of Shannon mutual information (fidelity) between the directly measured quantity, the voltage, and the quantity that we seek, the wavelength. The experiment with the highest Shannon mutual information (fidelity) provides, on average, the best measurement of the wavelength. Also, the fidelity also takes into account our prior information about the wavelength through a prior probability distribution.

The fidelity and Fisher information are two complimentary metrics for discussing measurements. The complementary measures of fidelity and Fisher information may be contrasted as follows. Assume that I want to shop to purchase the best measurement device to determine the unknown parameter ϕ. If I do not know the true value of the parameter ϕ, I would compare the overall performance specifications of several devices and I would purchase the device with the best overall specifications for measuring ϕ. The fidelity is the overall specification for the quality of the device, so I would purchase the device with the largest fidelity. After I have purchased the device, I want to use it to determine a specific value of the parameter ϕ based on several measurements (data). This involves parameter estimation, which requires the use of Fisher information, and depends on the true value of the parameter ϕ.

Using several examples, I will discuss the quality of a measurements in terms of Fisher information and fidelity. As a first example, I will show the role of Fisher information and fidelity in determining whether a coin is fair. As a second example, I compare the quality of measurements made by a classical and a quantum Mach-Zehnder interferometer. As a final example, I compute a fundamental upper bound on the fidelity of a classical Sagnac gyroscope. In order for a quantum gyroscope to be better than the classical Sagnac gyroscope, it must have a higher fidelity.

References

[1] V. Giovannetti, S. Lloyd, and L. Maccone. Advances in quantum metrology. *Nature Photonics*, 5:222, 2011.

[2] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. J. Wiley & Sons, Inc., Hoboken, New Jersey, second edition edition, 2006.

[3] T. B. Bahder and P. A. Lopata. Fidelity of quantum interferometers. *Phys. Rev. A*, 74:051801R, 2006.

[4] C. E. Shannon. *The Bell System Technical Journal*, 27:379, 1948.

[5] H. Cramér. *Mathematical Methods of Statistics*. Princeton University Press, Princeton, 1958. eighth printing.

[6] C. W. Helstrom. *Quantum Detection and Estimation Theory*. Academic Press, New York, 1976.

[7] T. B. Bahder. Phase estimation with non-unitary interferometers: Information as a metric. *Phys. Rev. A*, 83:053601, 2011.

QCMC 2012
Vienna, Austria

Optical homodyne tomography with polynomial series expansion

Hugo Benichi[1,2] **and Akira Furusawa**[1]

[1]*The University of Tokyo, Tokyo, Japan*
[2]*National Institute of Information and Communications Technology, Tokyo, Japan*

To obtain full knowledge about a quantum state $\hat{\rho}$ it is necessary to accumulate measurement statistics of observables, such as position $\hat{x}$ or momentum $\hat{p}$, on many different bases. In quantum optics, this statistical measurement can be achieved by angle resolved homodyne measurement of the operator $\hat{x}_\theta = \hat{x}\cos\theta + \hat{p}\sin\theta$ to acquire statistics of the squared modulus of the wave function, or $\langle x_\theta|\hat{\rho}|x_\theta\rangle$ in the general case. The reconstruction of $\hat{\rho}$, or equivalently $W(q, p)$, from the observation of $\langle x_\theta|\hat{\rho}|x_\theta\rangle$ is not immediate and requires the additional reconstruction of the complex phase of the quantum system from the many angle resolved measurements. These two operations together are referred to as quantum homodyne tomography or optical homodyne tomography [1].

Tomography algorithms can be roughly classified into two species: linear and variational methods. The former linear methods such as the filtered back-projection algorithm [1, 2] exploit and inverse the linear relationship between the experimentally measurable quantity $\langle x_\theta|\hat{\rho}|x_\theta\rangle$ and $\hat{\rho}$ or $W(q, p)$. Linear methods, however, suffer in general from technical difficulties associated with the numerical deconvolution necessary to perform the linear inversion of the Radon transform[3]. Fortunately, most of their associated problems are only technical in nature and can in principle be solved. In [4] it was shown that is it possible to design a linear reconstruction algorithm with better resilience to noise and better physical properties overall than the usual filtered back-projection method for the problem of optical homodyne tomography. Different from the usual filtered back-projection algorithm, this method uses an appropriate polynomial series to expand the Wigner function and the marginal distribution, and discretize Fourier space.

We show that this tomography technique solves most technical difficulties encountered with kernel deconvolution based methods and reconstructs overall better and smoother Wigner functions with fewer reconstruction artifacts(see Fig.1). More precisely, polynomial series tomography is superior with fewer experimental data points and when higher radial resolution is needed for higher photon number states. We also provide estimators of the reconstruction errors and use these estimators to shown that it performs better than filtered back-projection tomography with respect to statistical errors. The success of this approach lies in a systematic expansion of both the Wigner function $W(q, p)$ and the marginal distribution $p(x, \theta)$ in polar coordinates, with respectively the Zernike polynomials and the Chebysheff polynomials of the second kind. We show that the Radon transform preserves the orthogonality of these two families of polynomials and therefore can be diagonalized so that the inverse problem of optical homodyne tomography takes an especially simple form in this case.
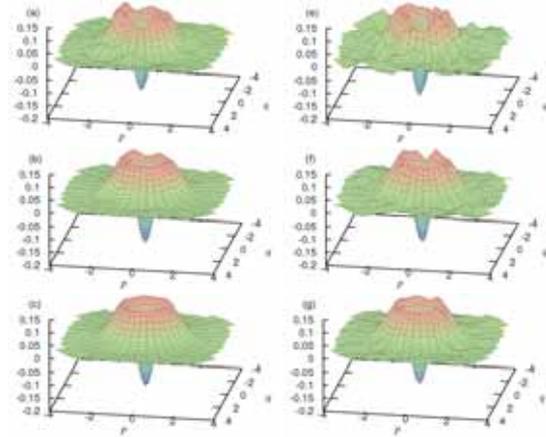
Figure 1: Comparison between polynomial series tomography (left panels, (a), (b) and (c)) and filtered back-projection tomography (right panels, (e), (f) and (g)) for the state $\rho = 0.8|1\rangle\langle1| + 0.2|0\rangle\langle0|$ for different sizes of synthetically generated data sets. Top row (a) and (e) panels, 50×10^3 data points. Middle row (b) and (f) panels, 20×10^3 data points. Bottom row (c) and (g) panels, 80×10^3 data points.

References

[1] D. T. Smithey *et al*, PRL **70**, 1244 (1993).

[2] K. Vogel and H. Risken, PRA **40**, 2847 (1989).

[3] J. Radon (by P. C. Parks), IEEE Transactions on medical imaging **MI-5**, 170 (1986).

[4] H. Benichi and A. Furusawa, PRA **84**, 032104 (2011).

Robust error bars for quantum tomography

Robin Blume-Kohout

Sandia National Laboratories, Albuquerque NM

In quantum tomography, a quantum state or process is estimated from the results of measurements on many identically prepared systems. Tomography can never identify the state (ρ) produced by a quantum device *exactly*, just as N flips of a coin cannot reveal its bias exactly. Any point estimate $\hat{\rho}$ has precisely zero probability of coinciding exactly with the true ρ, for infinitely many nearby states are equally consistent with the data. To make a tomographic assertion about the device that *is* true (at least with high probability) – we must report a *region* of states (Fig. 1).
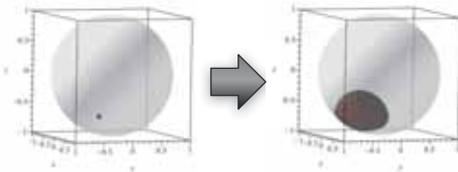
Figure 1: *Point estimators* (left) cannot provide meaningful, rigorous statements about the true (but unknown) state ρ, but a good *region estimator* (right) defines a rigorously valid assertion – "ρ lies within $\hat{\mathcal{R}}$ with 90% certainty."

I present here a procedure for assigning *likelihood ratio (LR) confidence regions*, an elegant and powerful generalization of error bars. LR regions contain the true ρ with guaranteed and controllable probability $\alpha \approx 1$. Within that [essential] constraint, they are almost optimally powerful – i.e., as small as possible. Finally, they are practical and convenient – for example, they are always connected and convex, and relatively easy to use and describe using convex programming (see examples in Fig. 2).

Definition 1. *Given observed data D, the **likelihood** is a function on states given by $\mathcal{L}(\rho) = Pr(D|\rho)$. The **log likelihood ratio** is a function on states given by $\lambda(\rho) = -2\log\left[\mathcal{L}(\rho)/\max_{\rho'}\mathcal{L}(\rho')\right]$. Given data D, the **likelihood ratio region** with confidence α is $\hat{\mathcal{R}}_\alpha(D) = \{$all ρ such that $\lambda(\rho) < \lambda_\alpha\}$, where λ_α is a constant that depends on the desired confidence α and the Hilbert space dimension d.*

The threshold value λ_α plays a critical role: increasing λ_α increases the size of the region (and thus its *coverage probability*), but reduces its *power* (large regions imply less about ρ). So λ_α should be set to the smallest value that ensures coverage probability at least α. This optimal value is hard to compute exactly, but upper bounds are provided in `arxiv/1202.5270` that guarantee coverage probability at least α (at the cost of slightly increasing the regions' size).

Discussion: Region estimators generalize the idea of "error bars", assigning a data-adapted region (within which the true state is asserted to lie) of arbitrary shape. To date, most attempts to assign regions (e.g., via bootstrapping or per-measurement error bars) have been based on *standard errors*,
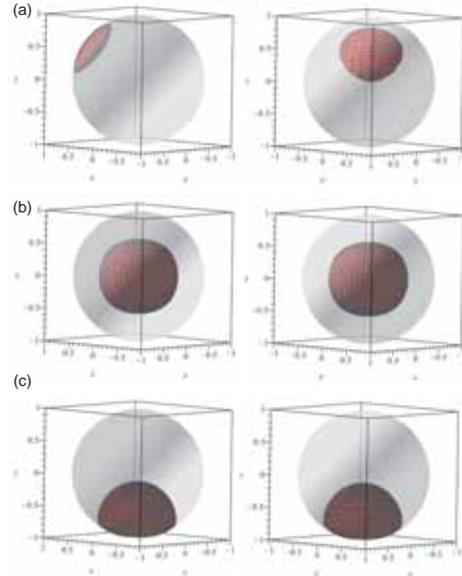
Figure 2: Examples of 90% confidence LR regions for $N = 3 \times 20$ measurements of $\{\sigma_x, \sigma_y, \sigma_z\}$. Rows are distinct datasets; columns show different views of the same region.

which quantify the variance of a given point estimator. Unfortunately, their connection with the experimentalist's uncertainty about ρ is tenuous at best, and nonexistent for quantum state estimation (because all tomographic point estimators are biased). *Confidence regions*, a statistically rigorous alternative, have the defining property that: **A confidence region estimator must assign a region $\hat{\mathcal{R}}$ containing the true (unknown) ρ with probability α no matter what ρ is.** This is not a Bayesian concept; the probability that $\hat{\mathcal{R}}$ contains ρ is defined *before* data are taken, not after. Nonetheless, confidence regions are the most reliable way known to objectively characterize uncertainty.

The LR prescription is unique among confidence region estimators because it assigns *small* regions. The proof (see `arxiv/1202.5270`) proceeds in two steps. First, it is shown rigorously that the smallest *average* region size (with respect to any specified distribution μ over states) is achieved by something called a *probability ratio* estimator. Then, LR regions are identified as a particularly even-handed example of probability ratio estimators.

Christandl and Renner recently (`arxiv/1108.5329`) introduced a confidence-region construction based on Bayesian reasoning. Their construction – and its relationship to LR regions – is quite interesting. The LR regions presented here appear to be (1) somewhat more powerful, and (2) substantially easier to construct and apply in real experiments. Ultimately, a hybrid of the two methods may well dominate them both.

Self-calibrating Quantum State Tomography

Agata M. Brańczyk[1], **Dylan H. Mahler**[1], **Lee A. Rozema**[1], **Ardavan Darabi**[1], **Aephraim M. Steinberg**[1] and **Daniel F. V. James**[1]

[1]*CQIQC and IOS, Department of Physics, University of Toronto, 60 Saint George St., Toronto, Ontario M5S 1A7, Canada*

Quantum state characterization is essential to the development of quantum technologies, such as quantum computing [1], quantum information [2] and quantum cryptography [3]. The successive measurement of multiple copies of the quantum state and subsequent reconstruction of the state's density matrix is known as *quantum state tomography* (QST) [4, 5].

We introduce and experimentally demonstrate a technique for performing *self-calibrating tomography* (SCT) on multiple-qubit states [6]. Our technique is effective despite lack of complete knowledge about the unitary operations used to change the measurement basis. We find that given local unitary operations with unknown rotation angles, and known and adjustable rotation axes, it is possible to reconstruct the density matrix of a state up to local $\hat{\sigma}_z$ rotations, as well as recover the magnitude of the unknown rotation angles.

We demonstrate SCT in a linear-optical system, using polarized photons as qubits. An inexpensive smartphone screen protector, i.e. an uncharacterized birefringent polymer sheet, is used to change the measurement basis. We go on to investigate the technique's robustness to measurement noise and retardance magnitude, and demonstrate SCT of a two-qubit state using liquid crystal wave plates (LCWPs) with tuneable retardances.

The state of a qubit, given by the density matrix $\hat{\rho}$, can be decomposed into a sum of orthogonal operators $\hat{\rho} = \frac{1}{2}\sum_{i=0}^{3}\lambda_i\hat{\sigma}_i$ where $\hat{\sigma}_0$ is the identity operator and $\hat{\sigma}_{1-3}$ are the Pauli matrices. The coefficients λ_j are given by the expectation values of the basis operators, $\lambda_i = \mathrm{Tr}[\hat{\rho}\hat{\sigma}_i]$.

Projective measurements of subsequent copies of the state lead to measurement statistics given by expectation values $n_j = \mathcal{N}_j\mathrm{Tr}[\hat{\rho}\hat{\mu}_j(\alpha)]$ where α characterizes the projector $\hat{\mu}_j(\alpha) = \hat{U}_j(\alpha)^\dagger\hat{\mu}_0\hat{U}_j(\alpha)$ with respect to a trusted, fixed projector $\hat{\mu}_0$. $\mathcal{N}_j$ is a constant that depends on the duration of data collection, detector efficiency, loss etc. The relationship between the measurement statistics and the parameters which characterize the density matrix is given by $n_j = \frac{\mathcal{N}_j}{2}\sum_{i=0}^{3}\mathrm{Tr}[\hat{\mu}_j(\alpha)\hat{\sigma}_i]\lambda_i$. In standard tomography, α is a known parameter and it is sufficient to measure only four different expectation values n_j to solve for λ_i. Given an *uncalibrated* unitary operation, i.e. an unknown α, an additional measurement is required to solve for both λ_i and α.

For a linear-optical demonstration of this method, we performed SCT on polarization-encoded one- and two-qubit states. Single-qubit states were prepared by pumping a $1mm$ long type-I down-conversion beta-barium borate (BBO) crystal with a $405nm$ diode laser. The detection of a horizontally polarized photon in one spatial mode of the down-converted photon-pair heralds the presence of a horizontally polarized photon in the other mode. Quarter- and half-wave plates then prepare arbitrary polarization states. For the trusted, fixed projector, we chose $\hat{\mu}_0 = |R\rangle\langle R|$, implemented with a quarter-wave plate and a polarizing beamsplitter, followed by coincidence-counting. We constructed additional projectors
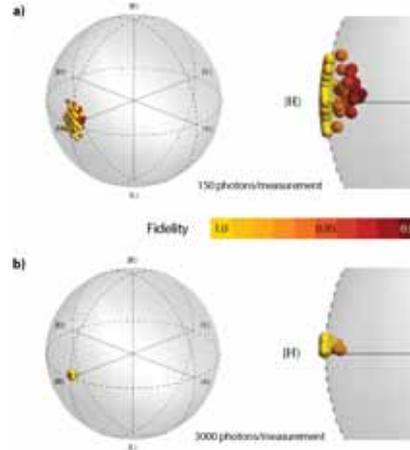
Figure 1: Distribution of states on the Bloch sphere as predicted by SCT using a smartphone screen protector to change the measurement basis for: a) high noise; and b) low noise. Notice the somewhat separate clump of lower-fidelity states in a). There are 100 states shown in each sphere.

using different orientations of a birefringent polymer sheet.

For multi-qubit tomography, entangled two-qubit states, $|\psi\rangle = a|HH\rangle + b|VV\rangle$, were prepared using two $1mm$ long type-I down-conversion BBO crystals with optical axes aligned in perpendicular planes [7] pumped by a $405nm$, diode laser. The parameters a and b were tuned by changing the polarization of the pump beam with a HWP. LCWPs in each arm, implemented the unknown unitary operations, followed by detection of $\hat{\mu}_0 = |R\rangle\langle R|$ in both modes.

References

[1] P. Kok *et al.*, Rev. Mod. Phys. **79**, 135 (2007).

[2] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).

[3] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179 (1984).

[4] D. F. V. James *et al.*, Phys. Rev. A **64**, 052312 (2001).

[5] J. B. Altepeter *et al.*, in *Qubit Quantum State Tomography* (Springer, 2004), Chap. 4.

[6] A. M. Brańczyk *et al.*, arXiv:1112.4492v1 [quant-ph] (2011).

[7] P. G. Kwiat *et al.*, Phys. Rev. A **60**, R773 (1999).

Quantum Shape Sensor

Gabriel A. Durkin, **Vadim N. Smelyanskiy and Sergey I. Knysh**

Quantum Laboratory, Applied Physics Center, NASA Ames Research Center, Moffett Field, California 94035, USA

This work promotes the use of quantum light in fiber optic 'shape sensors' for use in space environments where the current state of the art, detection of strains around 20nm amplitude for light at one micron wavelength, may not provide enough sensitivity. One application of high relevance is nextgen space telescopes such as the European Space Agency's LISA and GAIA, NASA's Space Interferometry Mission (SIM) and the international James Webb Space Telescope. These high performance instruments utilize multiple telescopes and mirrors [1, 2] or segmented mirror design (Air Force's deployable optical telescope [3]) to create large aperture optics or formation-flying of components [4] and all require sub-nanometer tolerances.

It is known that using quantum states of light may increase the sensitivity of interferometric measurements [5] of phase, and this translates easily into enhanced measurements of distance and time, magnetic fields, acceleration and rotation. This is not a notional concept, recently in GEO600 quantum light was utilized in a real-world experimental setting to produce a dramatic decrease in the noise threshold of a hyper-sensitive long baseline optical interferometer (arm length 600m) designed to detect gravity waves [6].

Optic fibers can be viewed as two-mode interferometers, the two fiber polarisation modes are analogous to the two spatial light modes in a Mach-Zehnder or Michelson interferometer. Due to the refractive indices being different for the two perpendicular polarisation modes, the fiber is said to be *birefringent* and this leads to a relative phase accumulating between the two modes of light as they propagate through the fiber.

$$|\phi\rangle = \sum_{n=0}^{N} e^{-in\zeta} \phi_n |n\rangle_h \otimes |N-n\rangle_v, \qquad (1)$$

The most general two-mode input state of N photons evolving in a noiseless environment is given in Eq.(1) a superposition of $N+1$ possible sharings of the N photons between the two polarizations (horizontal and vertical denoted h and v). Each photon number term with $n \in [0, N]$ photons in one polarisation and $N-n$ in the other accumulates a relative phase of $n\zeta$ over time ζ. Previously we explored the limitations imposed on phase estimation by quantum mechanics on optical interferometers subjected to dissipation, [7, 8].

We calculate the set of input probability amplitudes $\phi_n \in [0, 1]$, weightings that characterize an optimal input state to be injected into the fiber being utilized as a nano bending/twisting sensor, which we now explain. Besides the unitary ζ phase accumulation, another type of dynamics that is significant for light in optic fibers is the non-unitary process of depolarisation, where phase information is lost over time. This is often considered to be a type of non-dissipative noise, actually more significant in fibers than signal attenuation and scattering, which is by contrast quite well-characterised. The depolarising can occur due to random changes in the fiber's orientation as it connects one optical component to the next.

Until now, depolarization in fiber was seen as a nuisance, environmental noise that interfered with the process of phase estimation [9]. We choose instead to focus on the estimation of the two-mode optical depolarization channel itself under dissipative noisy conditions. The mathematical form of this non-unitary channel is given in Eq.(2), it represents a mixing of the input state $\rho_0 = |\phi\rangle\langle\phi|$ with the maximally mixed state. Now θ is the depolarizing parameter to be estimated, monotonic in time and in fiber length:

$$\rho_\theta = \Gamma_\theta[\rho_0] = \theta\rho_0 + \frac{(1-\theta)}{1+N} \sum_{n=0}^{N} |n\rangle_h |N-n\rangle_v \langle n|_h \langle N-n|_v, \qquad (2)$$

By establishing quantum states of light that offer much improved sensitivity to this parameter $\theta \in [0, 1]$ over standard laser light we can potentially *much* reduce the signal threshold $\Delta\theta$ corresponding to anomalous bending/twisting in the fiber. This would allow much earlier detection of such skew anomalies, e.g. across aircraft control surfaces in flight or during re-entry, wings/flaps/aerilons as they are subject to turbulent airflow. The quantum shape sensor is also deformable and can be applied to challenging geometries, e.g. inside space telescope components and mountings. Due to the small form factor of these tiny fibers, that may be only the width of a human hair so many of them in dense arrays can give hitherto unseen high resolution feedback.

References

[1] R. Gouillioud et. al, Aero. Conf. 2010 IEEE Big Sky, MT, ISBN: 978-1-4244-3887-7, DOI: 10.1109/AERO.2010.5446699

[2] Astro and Space Opt. Sys. Edited by P. G. Warren et al., Proceedings SPIE **7439**, 743915 (2009).

[3] S. A. Lane, S. L. Lacy, et. al. Jour. Spacecraft & Rockets **45**, 3, 568-586 (2008)

[4] T. Schuldt et. al., Class. Quantum Grav. **26** 085008 (2009).

[5] G. A. Durkin and J. Dowling, Phys. Rev. Lett. **99**, 070801 (2007).

[6] J. Abadie at al., Nature Physics **7**, 962965 (2011)

[7] H. Cable and G. A. Durkin, Phys. Rev. Lett. **105**, 013603 (2010)

[8] S. Knysh, V. Smelyanskiy, and G. A. Durkin, Phys. Rev. A **83**, 021804(R) (2011).

[9] M. Genoni, S. Olivares, and M Paris, Phys. Rev. Lett. **106**, 153603 (2011).

Joint Spectral Measurements at the Hong-Ou-Mandel Interference Dip

T. Gerrits[1]**, F. Marsili**[1]**, V. B . Verma**[1]**, A. E. Lita**[1]**, Antia Lamas Linares**[1]**, J. A. Stern**[2]**, M. Shaw**[2]**, W. Farr**[2]**, R. P. Mirin**[1]**, and S. W. Nam**[1]

[1]*National Institute of Standards and Technology, 325 Broadway, Boulder, Colorado, 80305, USA*
[2]*Jet Propulsion Laboratory, 4800 Oak Grove Dr., Pasadena, California 91109, USA*

We employed a 2 channel single-photon detection system with high detection efficiency and low jitter to characterize the joint spectral distribution (JSD) of the correlated photons emerging from a Hong-Ou-Mandel interference (HOMI) arrangement. We show the JSDs between the two output ports of the 50/50 beamsplitter while scanning the relative delay between the two photons impinging on the 50/50 beamsplitter. The photon pair source (a pp-KTP crystal, with down-conversion center wavelength of 1570 nm and about 250 fs temporal width) and fiber spectrometer to measure the JSDs is based on Ref 3. The fiber spectrometer employs two fiber spools of 1.3 km (2.3 km) length, which combined with the detector jitter results in a spectral FWHM resolution of 5.1 nm (4.8 nm). Our detector system employs two super-conducting nanowire single photon detectors (SNSPDs) [1] based on amorphous tungsten silicide (WSi) nanowires [2]. Both channels had a System Detection Efficiency SDE > 50 % at a wavelength (λ) of 1570 nm, negligible dark-count rate, background light count rate (BCR) of 300 cps (1000 cps) and 140 ps (200 ps) FWHM jitter. The low jitter and low background rate along with the high detection efficiency allows us to measure the JSD directly based on the timing information of the fiber spectrometer with very short measurement times [3]. We found an overall detection efficiency of 18 %, which is more than one order of magnitude larger than in previous studies. Therefore, our coincidence rate was improved by almost a factor of 1000. Figure 1a shows the JSD of the photon pairs generated by our source. A circular shape with some faint side lobes is observed. Note that this data was acquired in 5 minutes. When interfering both photons in a HOMI setup we observe the HOMI dip shown in Figure 2. Note that the asymmetry in the dip originates from the poor coupling of the photons into the fiber when the delay is far away from the optimized fiber coupling point at the HOMI dip. We observe a 69.6 % visibility of the HOMI for this conventional method. Figure 1b shows the relative HOMI dip intensity JSD observed for the two otput ports of the 50/50 beam splitter of the HOMI setup. The data was obtained by the ratio of the JSD at $\Delta t = 0$ (point B in Figure 2) and the JSD $\Delta t = 0.3ps$ (point A in Figure 2). The data shows a minimum coincidence probability at the center of the JSD and preliminary data analysis reveals a HOMI visibility of 92 % at the center, whereas the side lobe areas do not show any interference, i.e. zero HOMI visibility. In conclusion, the highly efficient SNSPDs enable us to study frequency-mode dependent phenomena of a photon pair source, such as the JSD dependence of the HOM interference.

Figure 1: (a) Normalized pair-source JSD. (b) Relative HOMI dip intensity JSD (same color scale as Figure 1a)
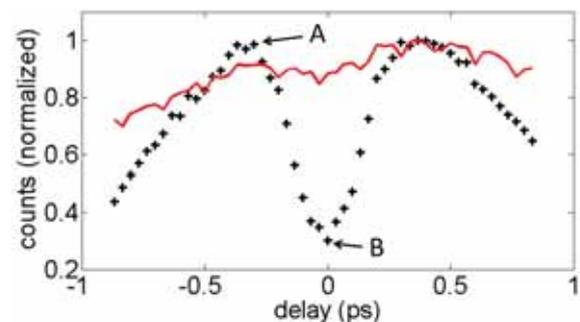
Figure 2: Black crosses: normalized, conventional HOMI. Note that the assymetry in the curve is due to the decreased fiber coupling efficiency into the fiber when far away from the dip position. Red line: normalized single photon fiber coupling, showing the effect of misalignemt when far away from the optimum coupling position.

[2] B. Baek, A. E. Lita, V. Verma, S. W. Nam, Appl. Phys. Lett, **98**, 251105 (2011).

[3] T. Gerrits *et al.*, Optics Express, **19**, 24434 (2011).

References

[1] G. N. Gol'tsman *et al.*, Appl. Phys. Lett., **79**, 705 (2001).

Quantum displacement receiver with feedforward operation for MPSK signals

Shuro Izumi[1,2], **Masahiro Takeoka**[1], **Mikio Fujiwara**[1], **Nicola Dalla Pozza**[3], **Antonio Assalini**[3], **Kazuhiro Ema**[2] and **Masahide Sasaki**[1]

[1]*National Institute of Information and Communications Technology(NICT), 4-2-1 Nukui-kitamachi, Koganei, Tokyo 184-8795, Japan*
[2]*Sophia University, 7-1 Kioicho, Chiyoda-ku, Tokyo 102-8554, Japan*
[3]*Department of Information Engineering, University of Padua, Via Gradenigo 6/B, 35131, Padova, Italy*

We propose and study quantum receivers for 3- and 4-ary phase-shift-keyed (PSK) coherent states to outperform the conventional limit, in the bit error rate (BER), achievable by heterodyne detection known as the standard quantum limit (SQL). The simplest implementation is known as the Kennedy receiver for binary PSK signals, which consists of a displacement operation and an on/off detection[1]. It can reach very close to the ultimate bound, i.e. the Helstrom bound. Its extension with feedforward operations is known as the Dolinar receiver which can theoretically attain the Helstrom bound[2]. The class of receivers with displacement operation, an on/off detection and feedforward operations is called the displacement receivers. Implementations of them in the laboratory, still suffered from imperfect efficiencies, have been reported in the literatures[3].

Figure1 shows our simplest structure of the displacement receiver for 3PSK signals $\{\left|\alpha e^{i\frac{2m}{3}\pi}\right\rangle (m = 0, 1, 2)\}$. The
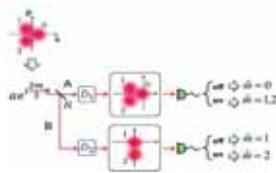
Figure 1: 3PSK detection scheme

optical signal is split into two paths A and B via a beam splitter of reflectance R. On path A the signal is first displaced with an amount $-\alpha$ such that the signal "0" to be the vacuum $|0\rangle$, and detected by the on/off detector, while on path B the signal is displaced with an amount $-\alpha e^{i\frac{2}{3}\pi}$ such that the signal "1" is displaced to the vacuum $|0\rangle$. Decision is made according to (off,off) or (off,on)→"0", (on,off)→"1", and (on,on)→"2".

This scheme can be extended to N-port detection circuit with feedforward operations. The basic structure is the same, i.e. the signal is split into N paths, displaced at each port and is discriminated by an on/off detector. The displacement operation at nth path is updated depending on the previous measurement results up to $(n-1)$th path. By increasing the number of paths N, the BER can be improved dramatically.

Figure2 shows the tree of possible events for the signal "1". Figure3 (a) and (b) presents the theoretical BERs for 3- and 4-PSK signals.

As N increases, the BERs of the displacement receiver decrease, approaching the Helstrom, but can never reach it with remaining a gap. The gap is bigger for 4-PSK signals. This is in contrast with the binary PSK case, where the displacement receiver can exactly realize the Helstrom bound in the limit of
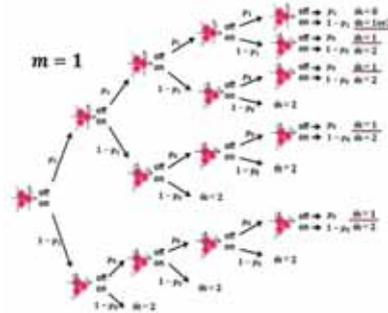
Figure 2: Decision tree of possible events for the signal "1" in the 3PSK receiver with feed-forward to calculate the channel matrix $P(j|1)$. $p_0 = e^{-\nu}$, $p_1 = e^{-\nu - \frac{3\eta|\alpha|^2}{N}}$
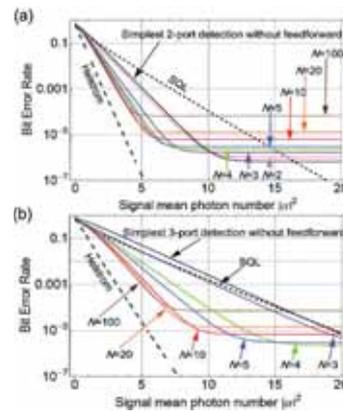
Figure 3: (a)3PSK BER(b)4PSK BER- detection efficiency η=90%, dark count ν=10^{-6}count/pulse.

$N \to \infty$. Thus as the number of signals M becomes larger, some new schemes have to be devised to improve the BER characteristics. It would offer an important insight into quantum information processing to clarify what they look like.

References

[1] R.S.Kennedy, Research Laboratory of Electronics, MIT, Quarterly Progress Report No. 108, p. 219, (1973).

[2] S. Dolinar, Research Laboratory of Electronics, MIT, Quarterly Progress Report No. 111, p. 115, (1973).

[3] Kenji Tsujino et al., Phys. Rev. Lett. **106**, 250503 (2008).; R. L. Cook, et al., Nature **446**, 774 (2007).; C. Wittmann, et al., Phys. Rev. Lett. **101**,210501 (2008).

Quantum interferometry with and without an external phase reference

Marcin Jarzyna[1], **Rafał Demkowicz-Dobrzański**[1]

[1]*University of Warsaw, Faculty of Physics, Warsaw, Poland*

Laws of quantum mechanics impose fundamental bounds on measurement precisions of basic physical quantities such as position, momentum, energy, time, phase etc. Theses bounds follow from the structure of the theory itself which contrasts the situation encountered in classical physics where measurement uncertainties are due to factors which in principle may be eliminated by improving the quality of measurement procedures. One of the most important measurement techniques where such bounds have been analyzed is optical interferometry, where the task is to measure phase delay between two arms of the interferometer.

In general, looking for the optimal phase estimation protocols is difficult since one needs to optimize over the input state that is fed into the interferometer, the measurement that is performed at the output and the estimator — a function that assigns a phase value to a given measurement outcome. One of the popular ways to obtain useful bounds in quantum metrology, without the need for cumbersome optimization, is to use the concept of the quantum Fisher information (QFI) [1, 2].

In [3] we have shown that in general, if one simply calculates QFI, one arrives at a physically counterintuitive result that the precision depends strongly on the way the phase shift between the beams is modeled inside the interferometer (Fig. 1). The explanation of this fact is that the information about phase is only available if one has the access to the additional reference beam with respect to which the phase delay φ is defined, in other words, there is no such thing as an absolute phase shift.
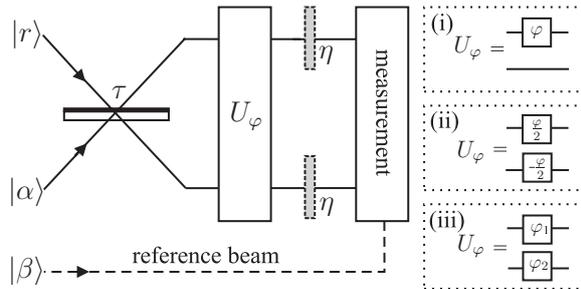
Figure 1: An interferometric scheme with coherent and squeezed vacuum states interfered at a beam-splitter, with arbitrary quantum measurement potentially involving an additional reference beam. The interferometer phase delay is modeled in three ways.

We managed to solve the problem in the absence of reference beam, which means that one should use not the simple tensor product of two states at the input of the interferometer but rather a phase averaged state given by a density matrix. In such case only the relative phase between the beams is taken into account, which makes the result independent on the model of phase shift.

Finally we analyzed the setup in which we have access to very strong reference beam which means that in the two input ports of the interferometer we have states with well defined phase. In such case we have to introduce instead of one parameter φ, two parameters φ_1, φ_2, which are phase shifts in the upper and lower arm of the interferometer (see Fig. 1). To solve this problem we have used Fisher information matrix and get a result, which indicates that in general, precisions in the presence of the reference beam and without it are different. On the other hand they are the same if the state after the beam splitter is path-symmetric, which in the lossless case can be done simply just by taking balanced beam splitter.
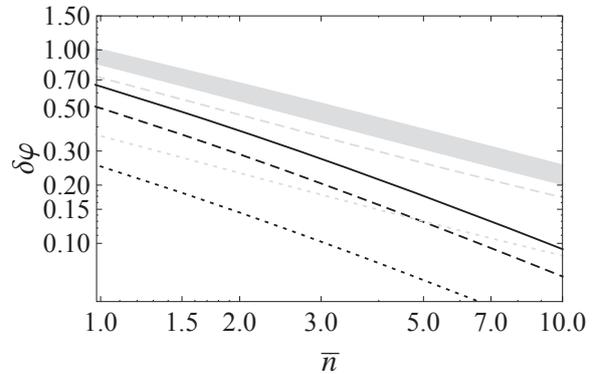
Figure 2: Bounds on the phase estimation precision optimized over α, r and τ with the constrained average photon number $\bar{n}$, in case of an ideal (black) and lossy (gray) interferometer. Different curves correspond to QFI calculated using different models (i) - dotted, (ii) - dashed, phase averaged state - solid. In case of a lossy interferometer the additional reference beam may improve the precision (gray region) while for the ideal interferometer these quantities coincide.

In summary we have pointed out some possible flaws in the interpretations of the results obtained using the QFI for states which are superpositions of different total photon number terms and showed that the full understanding of the problem is only possible if the role of an additional reference beam is properly taken into account.

References

[1] C. W. Helstrom, Quantum detection and estimation theory, (Academic press, 1976)

[2] Samuel L. Braunstein ,Carlton M.Caves, Phys.Rev.Lett. **72**, 3439 (1994)

[3] M.Jarzyna, R. Demkowicz-Dobrzański, Phys. Rev. A **85**, 011801(R) (2012)

Quantum metrology with fibre sources

B Bell[1], S Kannan[1], A McMillan[1], A Clark[1], W Wadsworth[2], J Rarity[1]

[1]*Centre for Quantum Photonics, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol BS8 1UB, UK*
[1]*Centre for Photonics and Photonic Materials, Department of Physics, University of Bath, Claverton Down, Bath BA2 7AY, UK*

The field of Quantum Metrology has attracted attention in recent years due to the possibility of improving the sensitivity of interferometric measurements, and fundamental interest in the limitations imposed on the accuracy of a measurement by quantum mechanics. In a measurement of a phase θ using n detections of uncorrelated photons, statistical uncertainty in n limits the accuracy with which θ is known to the standard quantum limit (SQL), $\Delta\theta \geq 1/\sqrt{n}$. However using entangled photons it is possible to beat the SQL and reach the Heisenberg limit, $\Delta\theta \geq 1/n$ [1].

Experiments in quantum metrology have used down-conversion sources of indistinguishable pairs of photons and Hong-Ou-Mandel (HOM) interference to generate entanglement and beat the SQL[2, 3]. Instead, we produce path entangled states by placing a pair photon source in each arm of the interferometer. This removes the requirement of indistinguishability between the signal and idler of the pairs, and the need to accurately overlap two modes at a beamsplitter for HOM interference, making this a relatively robust approach. Our source is based on four-wave mixing in photonic crystal fibre (PCF), pumped by $720nm$ picosecond pulses from a Ti:Sapphire laser, generating signal and idler photons widely spaced from the pump and entirely distinguishable by wavelength at $620nm$ and $860nm$ [4]. We used an automatically stable Sagnac interferometer with clockwise and counter-clockwise paths passing through a 15cm length of PCF, allowing the generation of pairs in either direction, then monitored both outputs of the interferometer for photons at the signal and idler wavelengths. A variable phase delay between the clockwise and counter-clockwise path was realised with a birefringent plate.

Assuming that a signal-idler pair is produced in either path with equal probability, and allowing that the wavelength dependence of the phase delay will result in different relative phases for signal and idler, θ_s and θ_i, we can write the state inside the interferometer in the photon number basis:

$$|\psi\rangle = \frac{|1\rangle_{1s}|0\rangle_{2s}|1\rangle_{1i}|0\rangle_{2i} + e^{i(\theta_s+\theta_i)}|0\rangle_{1s}|1\rangle_{2s}|0\rangle_{1i}|1\rangle_{2i}}{\sqrt{2}}$$

(1)

Here the two paths are labelled by the subscripts 1 and 2, and the subscripts s and i indicate signal and idler. The state evolves with a total phase $\theta_s + \theta_i$, oscillating sinusoidally between the two extreme cases where either the photons always emerge from the same interferometer output as each other, or separate ones. This behaviour is identical to a two photon NOON state. However, for 2-NOON experiments with downconverted light, the wavelength of a photon pair is double that of the pump laser. Ignoring the effects of dispersion, the phase accumulated is inversely proportional

to wavelength, $\theta = 2\pi n L/\lambda$, so that in measuring a length L with refractive index n, there is no advantage in using the two entangled photons compared to classical interference with the pump laser. For a four-wave mixing source we expect that $\theta_s + \theta_i \approx 2\theta_p$, so that the two photon fringe has about half the period of a classical one, and an advantage in sensitivity is seen when measuring the optical pathlength.
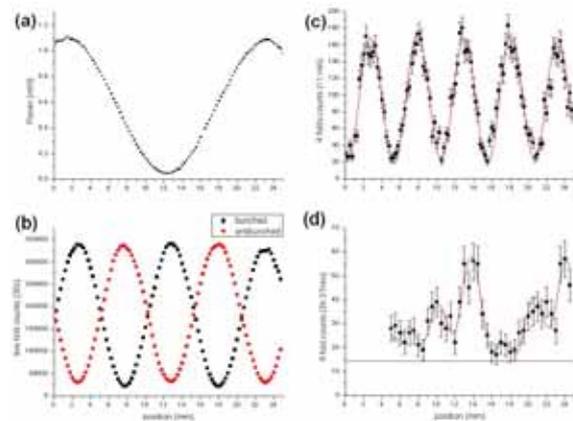
Figure 1: Interference with (a) Classical power measurement (b) Two photon coincidences (c) Four photon coincidences (d) Six photon coincidences at high pump power.

We confirm this experimentally by comparing classical interference of the pump laser (Fig. 1a) to two photon coincidences (Fig. 1b). The two photon fringe visibility is well above 70.7%, the usual threshold for beating the SQL. We will also discuss using entangled states of 4 and 6 photons in this setup, and present results for fringes with 1/4 and 1/6 of the pump wavelength (Fig. 1(c) and (d)).

References

[1] J. Dowling, "Quantum optical metrology - the lowdown on high-N00N states," Contemp. Phys. **49**, 125 (2008).

[2] T. Nagata, R. Okamoto, J. O'Brien, K. Sasaki and S. Takeuchi, "Beating the Standard Quantum Limit with Four-Entangled Photons," Science **316**, 726 (2007)

[3] G. Y. Xiang, B. L. Higgins, D. W. Berry, H. M. Wiseman and G. J. Pryde, "Entanglement-enhanced measurement of a completely unknown optical phase," Nature Photonics **5**, 43 (2011)

[4] J. Fulconis, O. Alibart, W. Wadsworth, P. Russell, and J. Rarity, "High brightness single mode source of correlated photon pairs using a photonic crystal fiber," Optics Express, **13**, 19, pp. 7572-7582 (2005)

Observation of single spin by transferring the coherence to a high energy macroscopic pure state

Minaru Kawamura[1], **Tatsuya Mizukawa**[2], **Ryouhei Kunitomi**[3] and **Kosuke Araki**[3]

[1]*Electrical and Electronic Engineering, Okayama University of Science, Okayama, Japan*
[2]*Graduate School of Engineering, Okayama University of Science, Okayama, Japan*
[3]*School of Engineering, Okayama University of Science, Okayama, Japan*

In this work we discuss the observation of a single spin under a strong magnetic field by transferring the coherence to a high energy level state of the harmonic oscillator which is composed of an inductor L connected to a capacitor C, all metallic parts being superconducting. The Hamiltonian of the circuit can be written as

$$H = \hbar\omega \left(b^\dagger b + \frac{1}{2} \right), \quad (1)$$

where $b^\dagger$ and b are the creation and the annihilation operators for photons in the resonator and $\omega = \frac{1}{\sqrt{LC}}$ is the resonance frequency of the circuit, which is tuned to the Larmor frequency. Taking the magnetic flux, Φ induced in the inductor to be along x-direction, the interaction between the nuclear spin and the flux can be written as

$$H_J = \hbar J_c B_x I_x, \quad (2)$$

where J_c is a coupling constant, $B_x = b^\dagger + b$, and I_x is x-component of the nuclear spin operator. However, for the sake of simplicity, the interaction Hamiltonian is assumed to be written as

$$H_J = \hbar J_c \left(B_x I_x + B_y I_y \right), \quad (3)$$

where $B_y = b^\dagger - b$, and I_y is y-component of the nuclear spin operator. Supposing the LC circuit is tuned the Larmor frequency, the total Hamiltonian is given as

$$H_a = -\hbar\omega I_z + \hbar\omega \left(b^\dagger b + \frac{1}{2} \right) + J_c \left(b^\dagger I^- + b I^+ \right), \quad (4)$$

where $I^+ = I_x + iI_y$, and $I^- = I_x - iI_y$. We can take as a convenient basis for the oscillator states of the eigenvectors of $\hat{n} = b^\dagger b$:

$$\hat{n}|n\rangle = n|n\rangle. \quad (5)$$

Supposing spin=1/2, we can take a basis as for the nuclear spin states of the two eigenvectors of I_z:

$$I_z|0\rangle = \frac{1}{2}|0\rangle, I_z|1\rangle = -\frac{1}{2}|1\rangle. \quad (6)$$

Using these bases, we can write arbitrary states of the system as

$$\Psi = \frac{1}{\sqrt{2(n_c+1)}} \sum_{m=0,n=0}^{m=1,n=n_c} |m\rangle \otimes |n\rangle, \quad (7)$$

where n_c is defined by the critical current of the superconducting inductor or the capacitor. Now consider the motion of the LC circuit when the initial state is given by

$$\Psi(0) = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |n\rangle + |1\rangle \otimes |n\rangle \right). \quad (8)$$

Then, the expectation value of $B_x = b^\dagger + b$, which correspond to the current induced the precessing nuclear spin in the inductor, is given as

$$\begin{aligned} B_x(t) &= \langle \Psi(0)|e^{\frac{i}{\hbar}H_a t} \left(b^\dagger + b \right) e^{-\frac{i}{\hbar}H_a t}|\Psi(0)\rangle \\ &= \left[\left(\sqrt{n+1} + \sqrt{n} \right) \sin\left\{ \left(\sqrt{n+1} - \sqrt{n} \right) J_c t \right\} \right. \\ &\quad \left. + \left(\sqrt{n+1} - \sqrt{n} \right) \sin\left\{ \left(\sqrt{n+1} + \sqrt{n} \right) J_c t \right\} \right]. \end{aligned} \quad (9)$$

From this result, the maximum amplitude of the induced current is approximately proportional to $\sqrt{n}$, though the time required to transfer the coherence to the LC circuit increases with $\sqrt{n}$. The numerical calculation results regarding the expectation values on the frame rotating with is shown in Figure 1. This fact indicates that we can amplify the magnetic resonance signal by increasing the initial energy level of the superconducting current in a macroscopic quantum pure state, and which must be measured with slight dissipation by using superconducting mixer and SQUID [1], and which means that if the initial state could be prepared, we can observe arbitrary quantum states of a single nuclear spin without the reduction. In principle, we cannot measure the expectation values of I_z and I_x simultaneously with high precision, however, it seems that this observation method would allow to measure the both I_z and I_x successively by applying a $\frac{\pi}{2}$ pulse after the observation. The details of this process will be described and discussed in this work.
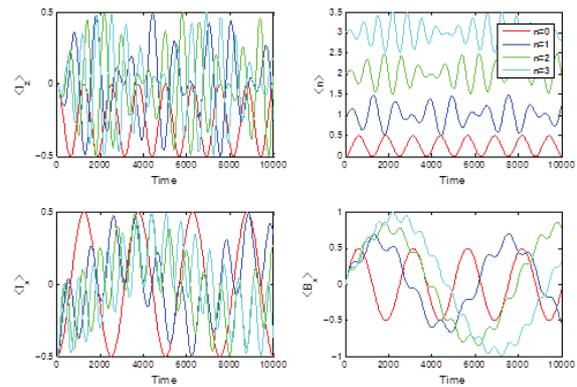
Figure 1: The calculation results of the expectation values of I_z and I_x, and the energy and the induced current of the harmonic oscillator are shown, where $J_c = 0.01$. The n's indicate the energy level number of the initial state.

References

[1] Vladimir B. Braginsky and Farid Ya. Khalili, Quantum measurement (Cambridge university press 1992)

Detection of systematic errors in quantum tomography

Tobias Moroder[1,2], **Matthias Kleinmann**[2], **Philipp Schindler**[3], **Thomas Monz**[3], **Otfried Gühne**[2], **and Rainer Blatt**[1,3]

[1]*Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, 6020 Innsbruck, Austria*
[2]*Naturwissenschaftlich-Technische Fakultät, Universität Siegen, 57068 Siegen, Germany*
[3]*Institut für Experimentalphysik, Universität Innsbruck, 6020 Innsbruck, Austria*

Quantum tomography has become a standard method in order to demonstrate the quality of a preparation of a quantum state or of an implementation of a quantum gate. Since the experimental progress meanwhile allows to manipulate very large quantum system, the number of events per measurement outcome in a tomographic scheme has outcome becomes very low—in particular due to time constraints and issues concerning the stability of the experiments. This leads to the problem that a naïve evaluation of the tomographic data yields manifestly unphysical results. As a countermeasure, the analysis of the experimental data has become subject to sophisticated statistical methods, the most prominent being the maximum likelihood method [1], but also Bayesian methods [2] or maximum entropy methods [3] have been suggested.

However, as the quantum systems under investigation become large and larger, the actual experimental implementation becomes increasingly difficult and the question, whether the experiments suffer from calibration errors and other sources of systematic errors becomes more and more urgent. The evaluation schemes in use today, unfortunately, do not take into account any kind of systematic errors—in fact even completely unphysical data could yield a perfectly valid quantum state. We here present a rigorous treatment in order to detect situations, where the systematic errors are significant compared to the uncertainty that arises due to the stochastic nature of the measured data.

A common tomography protocol is the Pauli measurement scheme, where for each of the 3^n possible combinations of Pauli operators on n qubits, one locally measures in the associated eigenbasis, yielding 2^n outcomes per setting. More generally, a tomography protocol consists of several measurement settings α with outcomes $i|\alpha$. If the system is in the state $\varrho_{\exp}$, then the probability for the outcomes $i|\alpha$ is given by $p_{i|\alpha} = \mathrm{tr}(E_{i|\alpha}\varrho_{\exp})$, where $E_{i|\alpha}$ denote appropriate operators describing the measurement apparatuses.

The general hope now is, that if each measurement is repeated sufficiently often, then the observed frequencies $f_{i|\alpha}$ will be rather close to the predicted probabilities $p_{i|\alpha}$. If this is the case, a least square approach will yield a reasonable estimate ϱ_{ls} for the true state $\varrho_{\exp}$. (This procedure is also called *linear inversion*.) However, in the case of low sampled data, ϱ_{ls} will have negative eigenvalues and this could not only be a sign of stochastic fluctuations, but could also very well be an indication of systematic errors. We can distinguish both situations, by virtue of the following result:

Assume, that two sets A and B of experimental data have been taken from the same state $\varrho_{\exp}$ and that $|\psi\rangle$ with $\langle\psi|\psi\rangle = 1$ minimizes $\langle\psi|\varrho_{\mathrm{ls}}^A|\psi\rangle$. If no systematic error is present, then for any $t > 0$, we have

$$\mathrm{Prob}[\langle\psi|\varrho_{\mathrm{ls}}^B|\psi\rangle < -t] \le \exp(-t^2 N_B/const_\psi), \quad (1)$$

where N_B is the number of samples per setting for the data set B. (This is a special case of a much more general result.)

This has a twofold interpretation. Firstly, if no systematic error is present, then the data set A cannot be used to guess a direction $|\psi\rangle$ for the data set B, such, that the naïve reconstructed state has a negative exception value in that direction, $\langle\psi|\varrho_{\mathrm{ls}}^B|\psi\rangle < -t$. Secondly, we may use this result in order to check, whether the description of the measurements by the operators $E_{i|\alpha}$ is in contradiction to the data. This is possible, since our result is of the form, that under the assumption that the data were sampled from $p_{i|\alpha} = \mathrm{tr}(E_{i|\alpha}\varrho_{\exp})$, we have

$$\mathrm{Prob}[T(\mathrm{data}) > t] = F_N(t), \quad (2)$$

where $T(\mathrm{data})$ is a function of the combined data A and B and we at least know an upper bound on the function $F_N(t)$. Hence, the *p-value* $F_N[T(\mathrm{data})]$ is a probability, under which—at most—the data are consistent with the employed description $E_{i|\alpha}$.

While Eq. (1) holds independent of the sample size, we go further and provide a (potentially stronger) test that does not require two independent data sets A and B, if the sample size is moderately high. This test is based on the likelihood ratio method and a result due to Wilks [4]. The test is of the form (2), where the function T can be computed by means of cone programming and the function $F_N(t)$ is approximated very well by an explicitly known function.

Finally, we demonstrate the practical use of our theoretical results by applying them to experimental data obtained on an ion trap quantum processor. In particular, if a typical systematic error is introduced on purpose (an increased "cross-talk" during the measurement process), we find that our methods very reliable detect such errors and lead to a refutation of the data. We also apply our results to measurements with a high number of samples (≈ 7000) per setting, to a situation where the experiment suffered from intensity fluctuations, and on low-sampled data of a 5 qubit tomography. In summary, our methods are well-suited to detect typical systematic errors and can be directly applied to experimental data—even if only a low number of samples was taken.

References

[1] Hradil, Z. *Phys. Rev. A* **55**, R1561 (1997).

[2] Blume-Kohout, R. *New J. Phys.* **12**, 043034 (2010).

[3] Teo, Y. S., Zhu, H., Englert, B.-G., Řeháček, J., and Hradil, Z. *Phys. Rev. Lett.* **107**, 020404 (2011).

[4] Wilks, S. S. *Mathematical statistics*. John Wiley & Sons, New York, London, (1962).

QCMC 2012
Vienna, Austria

Quantum control of a Bose-Einstein condensate in a harmonic trap

Sarah Adlong[1], Stuart Szigeti[1], Michael Hush[1] and Joe Hope[1]

[1]*Department of Quantum Science, Research School of Physics and Engineering, Australian National University, Canberra, Australia*

Over the last decade, the world has witnessed the birth of a generation of technologies that exploit the unique features of quantum mechanics [1, 2]. Investment in these technologies has reached the multi-million dollar scale. These technologies have applications in precision metrology [2, 3], quantum information processing and quantum cryptography [4, 5]. Future development of these technologies will require the precise control of non-trivial quantum systems.

Engineers and physicists alike have attempted to use quantum control to connect the physical realisation of quantum states to applications in technology. To this date there has been significant success controlling small quantum systems [6, 7, 8]. However, there has been limited application to large quantum systems. In order for quantum control to be viable technological application it needs to work on large systems. An interesting, large quantum system is a Bose-Einstein condensate (BEC) [11]. We will investigate the prospect of using active measurement feedback control to drive a BEC to a stable spatial mode.

The problem was approached from a quantum control perspective where we used quantum filtering theory to generate a best estimate of the BEC state conditioned on continuous weak measurement. Using this model we were able to address two important issues: the effect of the inclusion of technical noise on the control, and whether the semiclassical model was valid for a BEC under a continuous weak measurement.

One of the most important points of this investigation, vital for any possibility of experimental implementation, was the inclusion of technical noise in the model. In order to reduce computational time a semiclassical approximation was made - an assumption that the system had fixed number. Unlike previous approximations, where the measurement was solely corrupted by vacuum noise, we included noises caused by experimental imperfections. In this manner we demonstrated that our control was robust against changes in efficiency, noises in the modes of the trap and the addition of a time delay between the system and filter. Including these noises did not significantly impact on either the steady state the model reached or the time it took for the model to reach this steady state. It was conjectured that these results meant that our model could be assumed to be in a pure state, and thus our new approximation could be considered to be equivalent to the Hartree-Fock approximation.

Previously it had been shown that an optimum value for the measurement strength, α, existed [10]. In this investigation it was shown that changing this variable led to roughly linear scalings in the final energy. However, decreasing α led to an increase in the time taken it took the energy to reach a steady state. Our optimum value was chosen such that it cooled to the minimum energy possible within the lifetime of the BEC. It was found to be $\alpha = 0.1\omega$, where ω is the filter's trap frequency.

Although the Hartree-Fock approximation is a valid semi-classical approximation for many systems, it leaves out dynamics of the BEC which may be important. To gain some insight into this issue, we examined the filter in the case of a full field model and compared it to the Hartree-Fock approximation. The full field model was simulated using a new stochastic technique developed by Michael Hush *et al* [1]. It was shown that for fine spatial resolutions in the measurement the full field model heated indefinitely, in contrast to the Hartree-Fock model which cooled to a stable spatial mode. It was hypothesised the Hartree-Fock approximation suppressed some of the spontaneous emission, as only collective emission events can occur. In the full-field model, the atoms can be excited individually and the spontaneous emission is fully retained.

References

[1] M.R. Hush, A.R.R. Carvalho and J.J. Hope, Phys. Rev. A, **80**, 3 (2009).

[2] V.P. Belavkin and M. Guta, World Scientific (2006).

[3] V. Giovannetti, S. Lloyd and L. Maccone, Phys. Rev. A, **96** (2006).

[4] M. Neilsen and I. Chuang, Cambridge University Press (2000).

[5] N. Gisin, G. Ribordy, T. Wolfgang and H. Zbinden, Phys. Rev. Lett., **84** (2002).

[6] H. Wiseman and G. Milburn, Cambridge (2010).

[7] W.P. Smith, J.E. Reiner, L.A. Orozco, S. Kuhr and H.M. Wiseman, Phys. Rev. Lett., **89** (2002).

[8] D. Steck, K. Jacobs, H. Mabuchi, T. Battacharya and S. Habib, Phys. Rev. Lett., **92**, 22 (2004).

[9] S.S. Szigeti, M.R. Hush, A.R.R. Carvalho and J.J. Hope, Phys. Rev. A, **82**, 4 (2010).

[10] S.S. Szigeti, M.R. Hush and A.R.R. Carvalho, Phys. Rev. A, **80**, 1 (2009).

[11] M.R. Hush, A.R.R. Carvalho and J.J. Hope, Phys. Rev. A, **85**, 2 (2012).

Generating Particlelike Scattering States in Wave Transport

Philipp Ambichl[1]**, Florian Libisch**[1]**, and Stefan Rotter**[1]

[1]*Institute for Theoretical Physics, Vienna University of Technology, A-1040 Vienna, Austria*

Motivated by recent experiments that made the information stored in the scattering matrix of a complex system accessible to measurements [1, 2], we propose a procedure which employs this information for the generation of wave scattering states with particlelike properties [3]. Specifically, our procedure allows us to generate stationary waves which follow the bouncing pattern of a classical particle throughout the entire scattering process. This goal is achieved through the so-called Wigner-Smith time-delay matrix [4] which measures the time that a wave spends inside a scattering region.

We illustrate the operation of our procedure by way of the scattering setup shown in Fig. 1, consisting of a rectangular, two-dimensional scattering region to which two leads are attached to the left and right. When injecting through the left lead a superposition of waves into this cavity the resulting scattering state will typically fill the whole cavity area (see Fig. 1a). In our procedure we use the system's scattering matrix to evaluate the eigenstates of the Wigner-Smith time-delay operator. In this way we select from all the possible scattering states those which feature a well-defined time-delay between the moments when the wave enters and leaves the cavity. The states resulting from this condition are focused wave beams which follow the trajectory of a classical particle in the cavity and which, correspondingly, cover only a small fraction of the cavity area (see Fig. 1b). Quite differently from ordinary scattering states our particlelike beams also have the deterministic property of leaving the cavity only through one of the two leads rather than through both.

These "classical" properties are particularly useful for a number of applications. Consider, e.g., the situation shown in Fig. 1b where a signal is transmitted from the cavity entrance (A) to the exit (B) without an eavesdropper (E) being able to intercept the transmission. The highly collimated wave fronts resulting from our procedure might also prove useful for low-power communication where all the flux emanating from a sender/emitter is directed to the envisioned receiver/target.

We emphasize that our procedure is generally applicable to different types of waves (quantum, acoustic, electromagnetic, etc.). It can be applied to very general types of scattering systems of which the scattering matrix and not necessarily the geometric details are known. These results pave the way for the experimental realization of highly collimated wave fronts in transport through complex media.

References

[1] O. Dietz, U. Kuhl, H.-J. Stöckmann, N.M. Makarov, F.M. Izrailev, Phys. Rev. B **83**, 134203 (2011)

[2] S.M. Popoff, G. Lerosey, R. Carminati, M. Fink, A.C. Boccara, S. Gigan, Phys. Rev. Lett. **104**, 100601 (2010)

[3] S. Rotter, P. Ambichl, F. Libisch, Phys. Rev. Lett. **106**, 120602 (2011) (see also Phys. Rev. Focus **27**, 13 (2011)).

[4] E. P. Wigner, Phys. Rev. **98**, 145 (1955); F. T. Smith, Phys. Rev. **118**, 349 (1960)
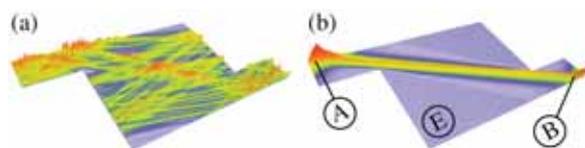
Figure 1: Scattering throuh a rectangular cavity confined by hard-wall boundaries. Two wave guides are attached to the scattering region, flux is injected from the left. The left panel (a) shows the intensity of a scattering state with typical wave-like properties like diffraction and interference. The right panel (b) shows a scattering state as resulting from our procedure: The wave displays particlelike features by following the trajectory of a classical particle throughout the scattering process. The insets illustrate the possibility to use such a state for transferring information between a sender (A) and a receiver (B) which bypasses a potential eavesdropper (E).

General Formalism for Evaluating the Impact of Phase Noise on Bloch Vector Rotations

Zilong Chen[1], **Justin G. Bohnet**[1], **Joshua M. Weiner**[1] **and James K. Thompson**[1]

[1]*JILA, University of Colorado and NIST, Boulder, Colorado 80309, USA*

Quantum manipulation protocols for quantum sensors and quantum computation often require many single qubit rotations. Most rotation protocols assume that the phase of the field that rotates the qubit is perfectly stable, and that imperfections arise only due to slowly varying amplitude errors or detuning errors. Composite rotation sequences can be used to reduce these errors to essentially arbitrary order. However, the phase of the qubit-field coupling is never perfectly stable, largely due to phase noise in the local oscillator used to generate the field. The impact of phase noise on qubit rotations is often neglected or treated only for special cases. We present a general framework for calculating the impact of phase noise on the state of a qubit, as described by its equivalent Bloch vector. The analysis is very general, applying to any Bloch vector orientation, and any rotation axis azimuthal angle for both a single pulse, and pulse sequences. Experimental examples are presented for several special cases. We apply the analysis to commonly used composite pulse sequences used to suppress static amplitude and detuning errors, and to spin echo sequences. We expect the formalism presented will guide the development and evaluation of future quantum manipulation protocols.

References

[1] Z. Chen, J. G. Bohnet, J. M. Weiner and J. K. Thompson, (submitted), http://arxiv.org/abs/1207.1688
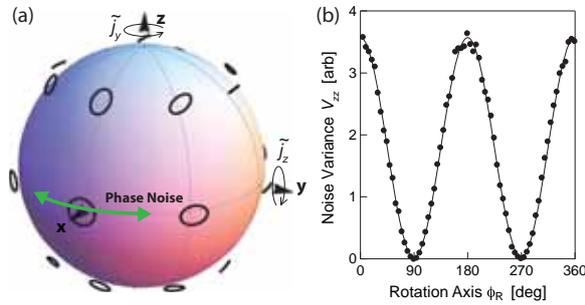
Figure 1: **a:** Phase modulation of the local oscillator causes modulation of the rotation axis (green arrow) about its mean orientation, here along $\hat{\mathbf{x}}$ or $\phi_R = 0$. The final Bloch sphere of points is deflected by an amount described by a small rigid rotation $R_y(-\widetilde{j}_z)R_z(\widetilde{j}_y)$ where $\widetilde{j}_z, \widetilde{j}_y$ are small angles depending on the modulation amplitude, frequency and phase. The deflection of a Bloch vector depends on the ideal final vector $\mathbf{J}_f^\circ$. If a set of possible deflections for an ideal final vector $\mathbf{J}_f^\circ$ along $\hat{\mathbf{x}}$ is described by a circle $\widetilde{j}_y^2 + \widetilde{j}_z^2 = \text{const}$ (shown outside sphere for clarity), the same set of deflections for other $\mathbf{J}_f^\circ$ are described by ellipses and lines centered at $\mathbf{J}_f^\circ$. **b:** The noise mapping shown in (a) for $\phi_R = 0$ and for $\mathbf{J}_f^\circ$ on the equator can be equivalently demonstrated by keeping the final vector oriented along $\mathbf{J}_f^\circ = \hat{\mathbf{x}}$ and varying the rotation axis ϕ_R. The observed noise variance V_{zz} (solid circles) of the vector projection along $\hat{\mathbf{z}}$ varies as the predicted $\cos^2 \phi_R$ (solid line).

The Pointer Basis and Feedback Stabilization of Quantum Systems

Li Li[1,2,3], Andy Chia[1,2,4] and Howard M. Wiseman[1,2]

[1]*ARC Centre for Quantum Computation and Communication Technology, Griffith University, Brisbane QLD 4111, Australia*
[2]*Centre for Quantum Dynamics, Griffith University, Brisbane QLD 4111, Australia*
[3]*Key Laboratroy of Quantum Information, University of Science and Techonology of China, CAS, Hefei 230026, PRC*
[4]*Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583*

The dynamics for an open quantum system can be 'unravelled' in infinitely many ways [1], depending on how the environment is monitored, yielding different sorts of conditioned states, evolving stochastically.

In the case of ideal monitoring these states are pure (assuming we monitor for sufficiently long), and the set of states for a given unravelling forms a basis (which is overcomplete in general) for the system. Let us denote the unravelling (i.e. monitoring scheme) by U and the pure states obtained under a given unravelling by $\{\pi_k^{\mathsf{U}}\}_k$, where each π_k^{U} is obtained with probability $\wp_k$, and the superscript on the state denotes its dependence on U. It has been argued [2] that the 'pointer basis' as introduced by Zurek and co-workers [3], should be identified with the unravelling-induced basis which decoheres most slowly, where the rate of decoherence may be characterized by the inverse of the mixing time τ_{mix}, defined as follows: We start by assuming that our system has evolved, under the master equation $\dot{\rho} = \mathcal{L}\rho$, to its steady state ρ_{ss}. We then monitor our quantum system with unit detection efficiency until a pure state π_k^{U} is obtained. The mixing time is defined as the time required on average for the purity to drop from its initial value (being 1) to a value of θ if the system were allowed to evolve under the master equation (or in the language of quantum measurement theory—under unconditional evolution). It thus satisfies

$$\mathrm{E}\Big\{\mathrm{Tr}\Big[\big\{\exp(\mathcal{L}\,\tau_{\mathrm{mix}})\,\pi_k^{\mathsf{U}}\big\}^2\Big]\Big\} = \theta \,, \qquad (1)$$

where $\mathrm{E}\{X\}$ denotes the ensemble average of X. Remember that π_k^{U} is random, realized with probability $\wp_k$. We will write $\theta \equiv 1 - \epsilon$ and take θ to be close to 1 (or equivalently ϵ close to zero).

Here we show the applicability of this concept of pointer basis to the problem of state stabilization for linear Gaussian (LG) quantum systems. An LG system is defined by linear stochastic differential equations driven by Gaussian noise for (i) the system configuration in phase space

$$\hat{\boldsymbol{x}} \equiv (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots, \hat{q}_N, \hat{p}_N)^\top \,, \qquad (2)$$

(with $[\hat{q}_j, \hat{p}_k] = i\delta_{jk}$) and (ii) the measurement output $\boldsymbol{y}$:

$$
\begin{aligned}
d\hat{\boldsymbol{x}} &= A\,\hat{\boldsymbol{x}}\,dt + B\boldsymbol{u}(t)dt + E\,d\hat{\boldsymbol{v}}_{\mathrm{p}}(t) \,, & (3)\\
\boldsymbol{y}(t)\,dt &= \mathsf{C}\,\langle\hat{\boldsymbol{x}}\rangle_{\mathrm{c}}\,dt + d\boldsymbol{v}_{\mathrm{m}}(t) \,, & (4)
\end{aligned}
$$

where A, B, E, and C are all constant matrices; $d\hat{\boldsymbol{v}}_{\mathrm{p}}(t)$ and $d\boldsymbol{v}_{\mathrm{m}}(t)$ are vector Wiener increments; and $\langle\hat{\boldsymbol{x}}\rangle_{\mathrm{c}} = \mathrm{Tr}[\hat{\boldsymbol{x}}\rho_{\mathrm{c}}]$ with ρ_{c} denoting the system state conditioned on the history of $\boldsymbol{y}(t)$. The vector $\boldsymbol{u}(t)$ is the control input, taken to be of the form $\boldsymbol{u}(t) = -k\langle\hat{\boldsymbol{x}}(t)\rangle_{\mathrm{c}}/\tau_{\mathrm{mix}}^\star$ where k is a dimensionless real number and $\tau_{\mathrm{mix}}^\star$ is the mixing time of the pointer basis with

Gaussian initial states (i.e. each π_k^{U} has a Gaussian Wigner function).

We prove that, for LG quantum systems, if the feedback control is assumed to be strong compared to the decoherence of the pointer basis (i.e. when $k > 1$), then the system can be stabilized in one of the pointer basis states with a fidelity in the long-time limit ($F_{\mathrm{fb}}^{\mathrm{ss}}$) close to one. It can be shown in general (i.e. θ not necessarily close to one) that

$$F_{\mathrm{fb}}^{\mathrm{ss}} = \big[\,1 - (1 - \theta^{-2})/4k\,\big]^{-1/2} \,, \qquad (5)$$

where the superscript ss means 'steady state' and the subscript fb means 'feedback.' When θ is close to one this simplifies to $F_{\mathrm{fb}}^{\mathrm{ss}} = 1 - \epsilon/(4k)$. When θ is close to one the purity ($P_{\mathrm{fb}}^{\mathrm{ss}}$) of the feedback-stabilized state can also be derived: $P_{\mathrm{fb}}^{\mathrm{ss}} = 1 - \epsilon/(2k)$. Moreover, the optimal unravelling for stabilizing the system (in any state) is that which induces the pointer basis. This is interesting since in general the optimal unravelling in the feedback loop is target-state dependent [4].

Classical systems undergoing continuous observation and control with dynamics satisfying Eqs. (3) and (4) are widely studied in optimal feedback with the criterion of optimality being a quadratic cost function (quadratic in $\hat{\boldsymbol{x}}$ and $\boldsymbol{u}$). Such a problem is termed LQG control [5] and we show that our results can also be obtained within the established framework of quantum LQG control when the cost of control tends to zero (as one might guess) [6].

We illustrate these results with a canonical decoherence model that is LG: quantum Brownian motion. We show that even if the feedback control strength is comparable to decoherence, the optimal unravelling still induces a basis very close to the pointer basis. However if the feedback control is weak compared to the decoherence, this is not the case.

References

[1] H. J. Carmichael, An Open Systems Approach to Quantum Optics (Springer, 1993).

[2] D. Atkins, Z. Brady, K. Jacobs and H. M.Wiseman, Europhys. Lett., **69**, 163 (2005).

[3] W. H. Zurek, S. Habib, and J. P. Paz, Phys. Rev. Lett., **70**, 1187 (1993).

[4] H. M. Wiseman and A. C. Doherty, Phys. Rev. Lett., **94**, 070405 (2005).

[5] E. Hendricks, O. Jannerup, and P. H. Sørensen, Linear Systems Control (Prentice-Hall, 1980).

[6] H. M. Wiseman and G. J. Milburn, Quantum Measurement and Control (Cambridge University Press, 2010).

Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks

Fabian Furrer[1], **Torsten Franz**[1], **Mario Berta**[2], **Volkher B. Scholz**[2], **Marco Tomamichel**[2] and **Reinhard F. Werner**[1]

[1]*Institut für Theoretische Physik, Leibniz Universität, Hannover, Germany*
[2]*Institut für Theoretische Physik, ETH, Zürich, Switzerland*

Quantum key distribution (QKD) is the art of generating a shared key between two distant parties (Alice and Bob), secret from any eavesdropper (Eve), using communication over a public quantum channel and an authenticated classical channel. We consider here a continuous variable (CV) protocol using two-mode squeezed vacuum states measured via homodyne detection. We present a security analysis against coherent (general) attacks, which provides a lower bound on the number of secret bits that can be extracted from a finite number of runs of the protocol. This is the first security analysis for a CV protocol resulting in a positive key rate while taking into account that only a finite number of measurements are performed (finite-key analysis) and being secure against coherent attacks.

Before, finite-key effects for CV schemes were only analyzed for the case of collective Gaussian attacks [2]. It is generally argued that the results of [3] based on a quantum de-Finetti theorem together with an energy bound imply security against coherent attacks (which is true in the case of infinitely many measurements). Unfortunately this argument leads to very pessimistic bounds for the key rate in the finite-key regime and is generally not robust in experimental parameters.

As opposed to most literature on CV QKD, the security definition we use in our analysis is composable, which means that the protocol can be securely combined with any other composable secure cryptographic primitives. The key ingredient in our security proof is an entropic uncertainty relation with quantum side information [4] generalized to continuous variable systems [5], which offers an elegant way to proof security for generic protocols.

In the protocol, Alice prepares $2N$ two-mode squeezed states from which she sends one part to Bob. Both apply homodyne detection to measure randomly one out of two conjugated quadratures. The measurement outcomes are discretized by dividing the real line into intervals of length δ and whenever a quadrature outcome higher than a certain threshold α is measured, the protocol is aborted. By means of classical communication, Alice and Bob discard all measurement results in which they have measured different quadratures and end up with roughly N data points X_A and X_B. After checking the correlation between X_A and X_B on a random sample, they either proceed with error correction and privacy amplification or abort the protocol (see [1, 5] for details).

The length of the secure key that can be extracted is lower bounded by [6, 5]

$$H^{\varepsilon}_{\min}(X_A|E)_{\omega} - \text{leak}_{\text{EC}} - \log \frac{1}{\epsilon} , \qquad (1)$$

where $H^{\varepsilon}_{\min}(X_A|E)_{\omega}$ is the smooth conditional min-entropy of X_A given E [6], leak_{EC} is the number of bits broadcasted in the error correction step, and ε, ϵ are functions of the se-

curity parameters. The state $\omega_{X_A E}$ between Alice's measurement outcomes and Eve is not known and the corresponding conditional min-entropy has to be estimated given the measured data. This is achieved by an entropic uncertainty relation for smooth entropies [4, 5] limiting Eve's information about X_A given Bob's knowledge X_B. But the latter information is accessible (it is with Alice and Bob) and can be estimated by a generalized Hamming distance between X_A and X_B (see [1] for details).
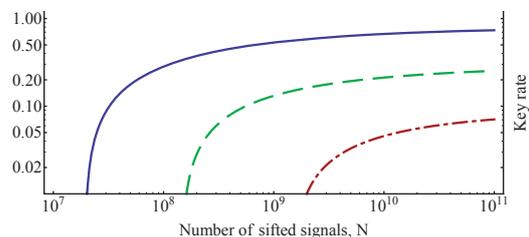
Figure 1: Key rate for an input squeezing/antisqueezing of 11dB/16dB and additional symmetric losses of 0% (solid line), 4% (dashed line) and 6% (dash-dotted line).

In Fig. 1, we plotted the optimized key rate for a two-mode squeezed state with squeezing/anti-squeezing of 11dB/16dB [7] depending on various symmetric losses and excess noise of 1%. This shows that a positive key rate secure against coherent attacks is possible using experimental parameters reachable today. Finally, we also compare this with a finite-key analysis only known to be secure against collective Gaussian attacks. We find that the resulting gap between the two rates basically emerges because the uncertainty relation we use is not tight for Gaussian states.

References

[1] F. Furrer, T. Franz, M. Berta, V. B. Scholz, M. Tomamichel and R. F. Werner, arXiv:1112.2179 (2011).

[2] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[3] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[4] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[5] M. Berta, F. Furrer, and V. B. Scholz, arXiv:1107.5460 (2011).

[6] R. Renner, Ph.D. thesis, ETH Zurich (2005).

[7] T. Eberle, V. Händchen, J. Duhme, T. Franz, R. F. Werner, R. Schnabel, arXiv:1110.3977

Heralded noiseless linear amplifier in continuous variables QKD

Rémi Blandino[1], Anthony Leverrier[2], Marco Barbieri[1], Philippe Grangier[1] and Rosa Tualle-Brouri[1,3]

[1]*Laboratoire Charles Fabry, Institut d'Optique, CNRS, Université Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau cedex, France*
[2]*ICFO-Institut de Ciencies Fotoniques, Av. Carl Friedrich Gauss 3, 08860 Castelldefels, Barcelona, Spain*
[3]*Institut Universitaire de France, 103 boulevard St. Michel, 75005, Paris, France*

We discuss the use of an heralded noiseless amplifier in continuous variables quantum key distribution. We specifically consider the GG02 protocol [1], using amplitude and phase modulated coherent states with reverse reconciliation, and show analytically that the key rate between Alice and Bob in presence of a noiseless lossy channel cannot be improved using this device, for a constant reconciliation efficiency. We also consider the case of a signal-to-noise-dependent reconciliation efficiency, and show numerically that in that case the amplifier could increase the distance of the transmission.

The performances of quantum key distribution (QKD) schemes are affected by non-ideal behaviors of the components, such as losses in the transmission channels, which contribute to decrease the mutual information shared between the partners involved. While amplifiers can effectively recover classical signals, they only offer limited advantages when working on quantum signals, as amplification is bound to preserve the original signal to noise ratio (SNR) [2].

Recently, it has been realised that, since the SNR has to be preserved only on average, one can harmlessly conceive a noiseless linear amplifier (NLA) which, by a probabilistic operation, can increase signals, while retaining the initial level of noise [4, 5]. The question arises if this more sophisticated device can deliver a compensation of losses with a success rate such that it may improve the key rate $\Delta I = \beta I_{AB} - I_{BE}$ (where β is the reconciliation efficiency).

We investigate this question when Bob uses a perfect NLA described by $g^{\hat{n}}$, where g is the gain and $\hat{n}$ the number operator. Prior to any classical communication with Alice, Bob receives a thermal state whose variance depends on Alice's modulation. We show that for this thermal state, the probability of success of the NLA is fundamentally limited to at most $1/g^2$.

In the Entanglement-Based representation of the protocol [3], the effect of the NLA can be described by introducing an effective modulation variance and an effective transmissivity, both increasing with the value of the gain [4]. Since the post-selected states remain gaussian, one can compute the corresponding key rate ΔI^g using their covariance matrix. Furthermore, since the relevant quantity is the maximal key rate achievable over a given channel, Alice is allowed to optimize her modulation variance in order to maximize ΔI and ΔI^g.

In the case of a constant reconciliation efficiency, we prove that the maximal average key rate $\frac{1}{g^2}\Delta I^g_{max}$ obtained with the NLA is always smaller than the maximal key rate ΔI_{max} which can be obtained without it.

The hypothesis of a constant β may not be satisfied by the
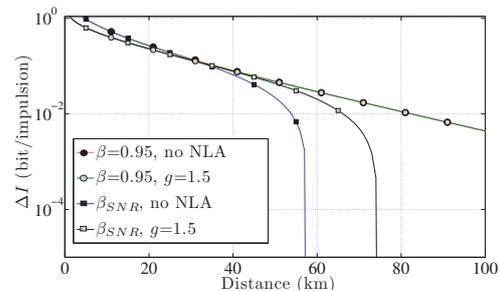
Figure 1: Maximized key rate as a function of the distance of transmission. β denotes a constant reconciliation efficiency. β_{SNR} denotes a SNR-dependent efficiency, decreasing for small SNR, with a limit value of 0.95 for high SNR.

commonest and simplest protocols for reconciliation: we proceed in our analysis by adopting a simple model to describe its variations with the SNR. We show that this dependence leads to a maximal distance of transmission which can be interestingly increased using the NLA, as shown in Fig. 1.

Finally, we also consider a lossy channel with thermal noise, and highlight some interesting behaviors.

References

[1] F. Grosshans and P. Grangier, Phys. Rev. Lett. 88, 057902 (2002).

[2] C. M. Caves, Phys. Rev. D 26, 18171839 (1982).

[3] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, arXiv:1110.3234 (2011).

[4] T. C. Ralph and A. P. Lund, arXiv:0809.0326 (2008).

[5] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. 104, 123603 (2010).

Performance Analysis of the Proposed QEYSSAT Quantum Receiver Satellite

Brendon Higgins[1]**, Jean-Philippe Bourgoin**[1]**, Nikolay Gigov**[1]**, Evan Meyer-Scott**[1]**, Zhizhong Yan**[1] **and Thomas Jennewein**[1]

[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada*

The long-distance implementation of a quantum key distribution (QKD) protocol is challenging because quantum signals cannot be copied accurately. This being the basis of the protocol's security, it also forbids the use of classical repeaters to boost the signal when transmission losses become significant. Without practical quantum repeaters yet available, current implementations of QKD are limited to distances of only a few hundred kilometres [1].

The successful demonstration of free-space transmission of quantum signals over such a distance [2] illustrates that a QKD link between the Earth and a satellite is feasible. Such links present a way to significantly extend the reach of QKD, potentially to the global scale [3]. Additionally, they also present the opportunity of testing quantum theory in previously unexplored regimes of distance, velocity, and gravitational gradient. The Canadian Space Agency is studying a proposal, entitled *Quantum Encryption and Science Satellite* (QEYSSAT), in which a microsatellite in low Earth orbit will act as a trusted node, establishing shared secure keys between two ground locations via night-time photonic quantum links as the satellite passes over each site.

As part of the feasibility study of the QEYSSAT proposal, we have conducted a thorough analysis of the optical link and its suitability in both the generation of a secure quantum key and to perform quantum entanglement tests. Our findings indicate that of two possible scenarios—uplink (quantum signals sent from ground to space) and downlink (quantum signals sent from space to ground)—an uplink, while experiencing greater losses, is certainly a feasible approach. In fact, the uplink scenario has many advantages owing to its reduced complexity and lower storage, processing, and communications requirements, and the additional flexibility of having (potentially various) sources located on the ground.

In our analysis we consider numerous phenomena which are likely to affect the optical link performance, including turbulent beam divergence effects, atmospheric transmittance, diffraction, source/receiver telescope sizes, and detector noise due to natural sources and artificial sources at different ground locations and inherent dark counts. Many of these parameters vary with the elevation angle of the satellite with the ground station. We perform exhaustive numerical calculations to determine the amount of secure key such a link would provide for several of these parameters as the satellite orbits. For the QEYSSAT uplink scenario, we calculate several hundreds of kilobits of secure key can be extracted per satellite pass, given typical passes under reasonable conditions, and a high-performing 300 MHz weak coherent pulsed source.

Following the link analysis, we expect to experience photon losses of 38 dB (mean useable) to the order of 50 dB. Experiments have demonstrated that QKD can in principle be performed with up to 55 dB of loss [4], but the cryogenic cooling required to operate low-noise superconducting detectors is generally considered too impractical for a satellite pay-
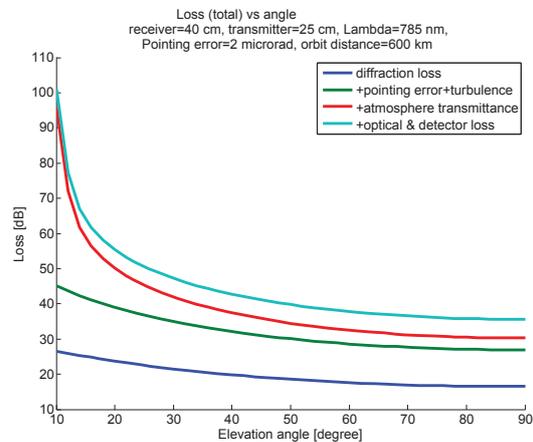
Figure 1: Calculated loss due to effects on the optical link.

load. Some of us recently showed that commercially available Si-APD photon detectors and advanced timing analysis can achieve the transmission of quantum signals sufficient for QKD at up to 57 dB of photon loss [5]. Based on this work, we are constructing a fully-operating QKD receiver system, developing the operational protocols necessary to facilitate QKD under a restricted resource environment, and employing a new receiver apparatus constructed from commercially available, largely off-the-shelf, optical components. Our goal is to develop the necessary technologies for a satellite-based quantum receiver by building a complete working quantum receiver system that in many ways reflects the requirements of a final satellite payload and operations platform.

Our optical link analysis and experimental demonstrations provide a crucial basis for the advancement of the QEYSSAT mission and the utility of quantum receivers on satellite platforms. They show that these concepts are feasible and achievable with current technologies, and thereby offer vital support to the development of platforms for global quantum-secured communications.

References

[1] N. Lütkenhaus and A. J. Shields, New J. Phys., **11**, 045005 (2009).

[2] R. Ursin et al., Nat. Phys., **3**, 481–486 (2007).

[3] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto and P. Villoresi, New J. Phys., **11**, 045017 (2009).

[4] R. J. Collins, R. H. Hadfield, V. Fernandez, S. W. Nam and G. S. Buller, Electron. Lett., **43**, 180–181 (2007).

[5] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel and T. Jennewein, Phys. Rev. A, **84**, 062326 (2011).

Characterization of pure narrow band photon sources for quantum communication.

N. Bruno[1], **T. Guerreiro**[1], **P. Sekatski**[1], **A. Martin**[1], **C.I. Osorio**[1], **E. Pomarico**[1], **B. Sanguinetti**[1], **N. Sangouard**[1], **H. Zbinden**[1] and **R.T. Thew**[1]

[1]*Group of Applied Physics, University of Geneva, Switzerland*

Many applications of quantum communication, such as device-independent Quantum Key Distribution (DIQKD) [1], quantum repeater protocols [2], rely on high fidelity multi-photon interference experiments. Pure states of narrow band photons are required for these purposes, and an interesting problem is how to engineer and characterize sources of such quantum states [3]. We are currently working on several approaches for generating photon pairs and heralded photons sources using both SPDC in PPLN (type II and 0) as well as four wave mixing in fibre. In a communication experiment, at least one of the photons of the pair should be in telecom regime and coupled into a single mode fibre. As such we define a single spatial mode, but in order to have pure photons we also need to efficiently select a single spectral mode.

In particular, we study how to characterize and eventually improve the spectral purity of these quantum states, comparing several approaches and exploring different regimes (such as high and low pump power, with both pulsed and continuous wave pump laser).

A well known method to have some information about the spectral properties of photon pairs generated via SPDC is to measure the joint spectral density function of the state $S(\omega_s, \omega_i)$ (see Fig. 1), scanning the wavelength of the two photons with two narrow band filters. However, in many of

Measuring a HOM dip between photons belonging to the same pair gives us some information about the indistinguishability of the photons but not their purity. To access the purity one normally needs to perform a much harder task and measure the HOM dip between two photons coming from two different sources. The visibility of this dip will depend on both the purity and indistinguishability of the two photons, and provides a more operational measure for how useful the photon pair sources can be for complex quantum communication and network applications.

A third way to access some information about the purity is to look at the photon probability distribution [4], which is related to the second order autocorrelation function: $g^{(2)}(0) = \frac{2P_2}{P_1^2} = 1 + \frac{1}{N}$, where P_i is the probability to have $i = 1, 2$ photons and N is the number of modes. For $N = 1$ we have $g^{(2)}(0) = 2$ (Bose-Einstein distribution), as N increases we will reach $g^{(2)}(0) = 1$ (Poisson distribution). The autocorrelation function can easily be measured with a beam splitter, two APD detectors and a TDC, and it no longer requires narrow band filters (as an example see fig 2).
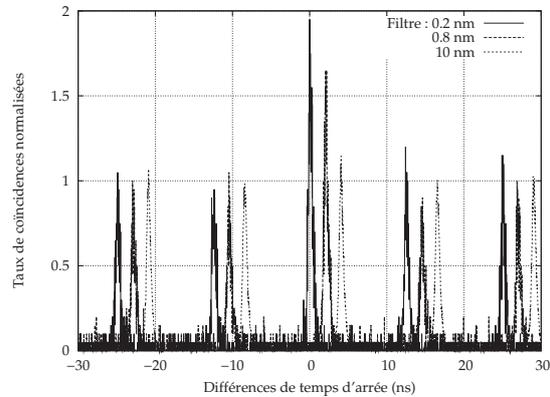
Figure 2: $g^{(2)}(0)$ for different statistical distributions [5].

We are investigating how well these different approaches perform as well as looking at quantifying how the purity varies with $g^{(2)}(0)$ in between the two limiting cases.

Figure 1: joint spectrum in case of not perfectly pure photons.

the cases that we are interested in, the tunable narrow band filters are already too broad for our photons. Therefore, we are looking for an experimentally feasible means of measuring the purity in this regime.

References

[1] A. Acín et al. *Phys. Rev. Lett.* **98** 230501(2007).

[2] N. Sangouard et al., *Rev. Mod. Phys.* **83**, 33 (2011)

[3] E. Pomarico et al., N. J. of Physics, **14**, 033008 (2012).

[4] P.R. Tapster and J.G. Rarity, *J. Mod. Opt.* **45**, 595 (1998).

[5] A. Martin et al., N. J. of Physics, **14**, 025002 (2012) .

Discord as a Quantum Resource for Bi-Partite Communication

Helen M. Chrzanowski[1], **Mile Gu**[2], **Syed M. Assad**[1], **Thomas Symul**[1], **Kavan Modi**[2], **Timothy C. Ralph**[3], **Vlatko Vedral**[2] and **Ping Koy Lam**[1]

[1]*Centre for Quantum Computation and Communication Technology, Department of Quantum Science, The Australian National University*
[2]*Centre for Quantum Technologies, National University of Singapore*
[3]*Centre for Quantum Computation and Communication Technology, Department of Physics, University of Queensland*

For many years, the notion of quantum advantage afforded by many quantum information protocols was equated with the notion of entanglement. Recently, the requirement of entanglement to preform efficient quantum computation has been questioned both theoretically and experimentally [1, 2]. It has been proposed that, for certain mixed state quantum computing protocols, a non-classical quantity called quantum discord is all that is required for speed-up. Discord arises from the discrepancy between the quantum analogues of the two classically equivalent expressions for the mutual information: $I(\rho) = S(\rho_A) + S(\rho_B) - S(\rho)$ and $J_A(\rho) = S(\rho_B) - S(\rho_B|\rho_A)$. The discord, $D(\rho) = I(\rho) - J_A(\rho)$, captures all the non-classical correlations in ρ [3, 4].

Whilst quantum discord is proving to be a promising candidate to complete the description of quantum correlations, explicit protocols that directly exploit discord as a quantum resource have remained elusive. Here we demonstrate that discord of a bipartite system is consumed to encode information that can only be accessed by coherent quantum interactions. The inability to access this information by any other means allows us to use discord to directly quantify this 'quantum advantage'.

We present a protocol where Alice prepares a non-entangled bi-partite resource ρ_{AB} that possesses some discord. Alice then encodes a signal $\mathbf{X}$ on one of her subsystems, and subsequently transmits her now encoded state $\tilde{\rho}_{AB}$ to Bob and asks how much information regarding the encoding Bob can access. We consider two possible scenarios: Bob can coherently interact the two subsystems locally and subsequently measure, and alternatively, when Bob is restricted to local measurements on each subsystem. We theoretically and experimentally demonstrate that when ρ_{AB} possesses discord, coherent interactions are advantageous to Bob's estimate of $\mathbf{X}$. Furthermore, we demonstrate that Bob's information advantage when he implements coherent interactions is directly linked with the discord consumed during encoding of $\mathbf{X}$. For a maximal encoding that results in an encoded state $\tilde{\rho}_{AB}$ with zero discord, the advantage is exactly the discord of the original state ρ_{AB}. Thus we introduce and demonstrate an operational method to use discord as a physical resource.

Figure 1: Alice prepares a separable bi-partite state ρ_{AB}. Alice then encodes independent signals $\mathbf{X}_s$ and $\mathbf{Y}_s$ on the phase and amplitude quadrature of her subsystem and subsequently transmits her state to Bob. We compare Bob's capacity to extract information in two different scenarios: when Bob is (a) limited to incoherent interactions, and (b) able to preform a joint measurement.
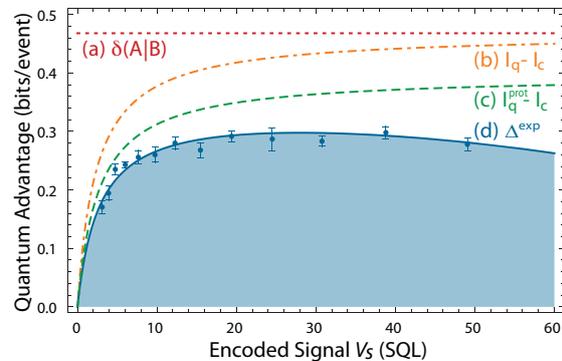
Figure 2: Plot of quantum advantage for varying signal strength with $V = 10.0 \pm 0.1$. (b) corresponds to the maximum possible quantum advantage, assuming Bob can perform an ideal decoding protocol. In the limit of large V_s, this tends to the discord of the original resource (a). The actual advantage that can be harnessed by our proposed protocol is represented by (c). In practice, experimental imperfections reduce the experimentally measured advantage to (d).

References

[1] Datta, A., Shaji, A. & Caves, C. M., Phys. Rev. Lett. **100**, 050502 (2008).

[2] Lanyon, B. P., Barbieri, M., Almeida, M. P. & White, A. G., Phys. Rev. Lett. **101**, 200501 (2008).

[3] Henderson, L. & Vedral, V., J. of Phys. A. **34**, 6899–6905 (2001).

[4] Ollivier, H. & Zurek, W. H., Phys. Rev. Lett. **88**, 017901 (2001).

Blind Quantum Computing with Weak Coherent Pulses

Vedran Dunjko[1], **Elham Kashefi**[2], **Anthony Leverrier**[3,4]

[1]*SUPA, School of Engineering and Physical Sciences, David Brewster Building, Heriot Watt University, Edinburgh, EH14 4AS, UK*
[2]*School of Informatics, The University of Edinburgh, Edinburgh EH8 9AB, U.K.*
[3]*ICFO-Institut de Ciencies Fotoniques, Av. Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona) - Spain*
[4]*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*

Building quantum computers is exceptionally hard. Optimistically, large quantum servers may soon take a role occupied by superclusters today, remotely accessed by many clients using relatively simple devices, to solve their quantum computational tasks. Then, the level of privacy guaranteed to the clients becomes crucial. For this reason, the Universal Blind Quantum Computation (UBQC) protocol [1] has been receiving considerable attention by the scientific community, and has already prompted experimental demonstrations [2]. UBQC allows a client to perform quantum computation on a remote server, and perfect privacy (called *blindness*) is guaranteed if the client is capable of producing specific, randomly chosen perfect single qubit states $|+_\theta\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)$ with $\theta \in \{0, \pi/4, \ldots, 7\pi/4\}$, and passing them to the server. From a theoretical point of view, this may constitute the lowest possible quantum requirement, but pragmatically, generation of such states to be sent along long distances can never be achieved perfectly. While certain levels of errors still allow the correct computation using fault-tolerant constructions, the crucial question of how such imperfections influence the protocol's security has so far not been addressed.

Here, we investigate the security of UBQC with realistic imperfections for the client, i.e. the ones which may jeopardize security. For this purpose, we introduce the framework of approximate blindness (ϵ-*blindness*) inspired by similar approaches in the context of Quantum Key Distribution [3]. While the UBQC protocol is adaptive, we show that blindness can be studied by inspecting a fixed post-selected state joint client-server state of the form:

$$\pi_{AB}^{\text{ideal}} = \frac{1}{2^{4S}} \sum_{\overrightarrow{\phi}, \overrightarrow{r}} \bigotimes_{i \in [S]} \underbrace{|\phi_i\rangle\langle\phi_i| \otimes |r_i\rangle\langle r_i|}_{\text{Client (A)}} \otimes \underbrace{|+_{\theta_i}\rangle\langle+_{\theta_i}| \otimes |\delta_i\rangle\langle\delta_i|}_{\text{Server (B)}}$$

which contains all the relevant information pertaining to the security of a run of a UBQC protocol as seen by the server. In this classical-quantum (cq) state, S denotes the overall *size* of the computation. The client's register contains the client's secret information - the computational angles ϕ_i characterizing the desired computation, and the r_i parameters chosen randomly and unknown to the server. The server's register contains the qubits in states $|+_{\theta_i}\rangle$ which are sent by the client, as well as the measurement angles δ_i. Note that ϕ_i, r_i and δ_i are all represented by orthogonal states.

Since the unconditional security holds for any action of the server [1] (represented by a CPTP map $\mathcal{E}$), we define the family $\mathcal{F}$ of *unconditionally blind* states:

$$\mathcal{F} = \left\{(\hat{\mathbf{1}}_A \otimes \mathcal{E})\pi_{AB}^{\text{ideal}} | \mathcal{E} \text{ is a CPTP map}\right\}.$$

From here ϵ-blindness is defined in operational terms:

A realistic UBQC protocol with imperfect client preparation is ϵ-blind if the probability of distinguishing between the unconditionally blind states and the client-server states realized in the realistic protocol is less than $\frac{1}{2} + \epsilon$.

Such a notion of security is particularly desirable as it is composable [3].

Under realistic assumptions, we show that the value of ϵ depends on the distinguishability between the individual imperfect states generated by the client and the desired qubit states only. High quality qubits imply high levels of security.

We present a *Remote Blind qubit State Preparation* (RBSP) protocol , where the client only needs to prepare and send sequences of weak coherent pulses (WCP) with given polarizations over a (noisy) quantum channel. Following this, through classical communication, the client distills an arbitrarily good approximation of a random qubit state in the possession of the server, which can then safely be used for UBQC. The 'quality' of the distilled qubit is shown to increase exponentially in terms of the number of coherent pulses used in one call to the RBSP protocol. Thus, RBSP serves as a viable substitute to the process of sending ideal qubits, where the requirements on the client are minimal.

We prove the following result concerning the security of the UBQC using RBSP generated qubits:
A UBQC protocol of computation size S, where the client's preparation phase is replaced with S calls to the RBSP protocol, where the coherent pulse mean photon number set to $\mu = T$, with a lossy channel between client and the server of transmittance no less than T, is correct and ϵ-blind for a chosen $\epsilon > 0$ if the number of coherent pulses N of each instance of the RBSP called is chosen as follows:

$$N \geq \frac{18\ln(S/\epsilon)}{T^4}.$$

This result shows that secure delegated blind quantum computation is in principle possible even when the client only has access to technologies available today.

References

[1] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* , 2009, pp. 517–526.

[2] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, *Science* **335**, 303 (2012).

[3] M. Ben-or, D. W. Leung, and D. Mayers, in *Theory of Cryptography: Second Theory of Cryptography Conference, volume 3378 of Lecture* (Springer-Verlag, 2005), pp. 386–406.

Secure network switch with Quantum key distribution system

Mikio Fujiwara[1]**, Tomoyasu Domeki**[2]**, Ryo Nojima**[1]**, and Masahide Sasaki**[1]

[1]*National Institute of Information and Communications Technology, Japan*
[2]*NEC Communication systems, Japan*

After the past two decades of development, the experimental quantum key distribution (QKD) has achieved significant improvement, and the transmission distance has extended to 250 km [1]. However, key relay via trusted nodes is still a practical solution to make QKD service in multi-user networks in a metropolitan scale [2, 3], and in a country scale in future. The problem is how to make a trusted node really trusted. One should seriously care about the security not only in the physical layer but also the upper layers in the node. Switches in layer 2 and 3 (in terms of OSI layer model) are of particular importance. We have developed an integrated network switch of layer 2 and layer 3 whose security is enhanced with secure keys from QKD systems.

Layer 3 switch

The scenario that QKD is used for key establishment between two local area networks has been demonstrated within the BBN DARPA network project[4] and other networks[2]. A point to point local area network (LAN) or virtual private network (VPN) encryptor provides secure key to the layer 3 switch. Payload are encrypted by IPSEC protocol with QKD-based key exchange. The security of the transmitted data over such a link is limited by the security of the encryption scheme. However, frequent key renewal of the symmetric-key encryption should enhance the security level[5]. Therefore, we are developing the QKD based layer 3 switch in that the symmetric-key is refreshed to each packet.

Layer 2 switch

The encryption scheme at exchanged data between VPNs has been drawing attention, however, serious security holes are also recognized at layer 2. Ethernet technology has been established on the assumption that users are fundamentally good. In other words, unauthorized access from the inside-network PC is very easy. De-concentration of access authority is adopted in the network in order to construct a secure network. However, such a protection scheme is destroyed by impersonation from the inside-network PC. Media access control (MAC) address is used to identify a host in the layer 2. MAC address spoofing tools are relayed via network. Even if a network authentication is employed, it is difficult to prevent unauthorized access completely due to sophistication of spoofing attack. In order to enhance the security of the inside-network, we develop the layer 2 switch that uses random number provided from QKD system for authentication of hosts. At first, the switch and each host share random number, and MAC address is encoded using that random number. One-time-pad encryption is adopted, and MAC address is encoded to each packet between the host and the layer 2 switch. In the layer 2 switch, consistency is checked by using decoded MAC address and IP address. If the host sends correct addresses, the layer 2 switch passes the packet. Our switch has strong protection against MAC spoofing, IP address spoofing, spoofing using ICMP Redirect, ARP poison-

ing attack and so on. Throughput performance of this switch decreases to 30%, however, it will be improved 90% in near future.

We have developed a QKD-based network switch that enables to prevent illegal access from external and internal network efficiently. This switch will contribute to construct the trusted node and play an indispensable role in imbedding a QKD network into current infrastructure of secure network. Poor convenience of secret communication tool should provoke human error that poses a serious threat to the network security . The QKD-based network switches would be also useful to reduce such risks enhancing the security with user-friendliness.
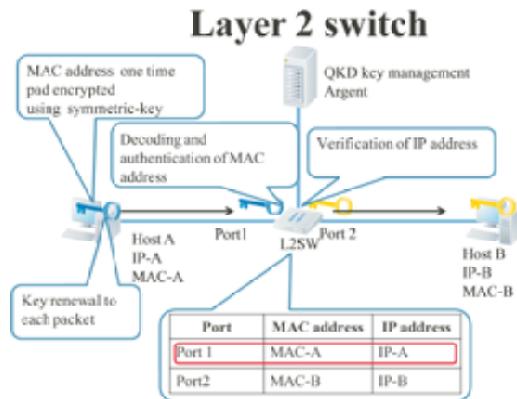
Figure 1: Conceptual view of secure L2 switch

References

[1] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).

[2] R. Alleaume et al., SECOQC White paper on quantum key distribution and cryptography, http://www.secoqc.net/

[3] M. Sasaki et al., Optics Express **19**, 10387 (2011).

[4] C. Elliott, A. Colvin. D. Person, O. Pikalo, J. S. Schlafer, H. Yeh, http://arxiv.org/ftp/quant-ph/papers/0503/0503058.pdf

[5] R. Nojima, in preparation.

Field transmission test of 2.5 Gb/s Y-00 cipher in 160-km (40 km × 4 spans) installed optical fiber for secure optical fiber communications

Fumio Futami[1] and Osamu Hirota[1]

[1]*Quantum ICT Research Institute, Tamagawa University, Tokyo, Japan*

Security in optical data link of local area networks and wide area networks is an issue especially for data centers providing services of the cloud computing where confidential information is transmitted. The use of the physical cryptography whose security relies on the physical effect is a promising way for enhancing the security of optical data link together with the mathematical encryption. The quantum stream cipher by Yuen 2000 protocol (Y-00) is noise-based physical layer encryption and has a possibility that realizes the unbreakable security level [1]. It also features high compatibility with the current optical fiber communication systems and is suitable for high-speed (> Gb/s) communication. It employs dense M-ary keying (multi-level modulation) for the binary information to realize security, which requires no excess bandwidth. A fundamental idea of Y-00 cipher to avoid eavesdropping is shown in Fig. 1. The noise masks the Y-00 cipher signal level and disables the correct level discrimination of an eavesdropper. Prototypes of Y-00 cipher transceiver using multi-level phase modulation (PSK Y-00) [2] and intensity modulation (ISK Y-00) [3] have already been developed. We have focused on the research of ISK Y-00 since it has an advantage of simple configuration. So far, we demonstrated ISK Y-00 at 2.5 Gb/s using signals with the intensity level number of upto 4096 [4,5], and at 10 Gb/s and 40 Gb/s using 64-intensity level signals [6,7]. In the reports, transmission performances were usually investigated in optical fibers in the laboratory, and investigation terms were several hours at longest. However, for practical use, a longer term investigation is desirable in optical fibers installed in the field.

In this work, we demonstrate a long term investigation of an ISK Y-00 transmitter and receiver in the field optical fiber transmission line, TAMA net #1. The transmitter has signal intensity levels of 4096 and bit rate of 2.5 Gb/s. The Y-00 signal is transmitted over 160 km of the optical fiber installed in the field. The transmission line consists of 4 spans of a 40-km standard single mode optical fiber (SMF) and an optical amplifier.

So far, we constructed the experimental setup shown in Fig. 2. The optical fibers are installed under the ground in Tamagawa University. The length of each optical fiber is 40 km. The net length is 160 km. The 2.5-Gb/s transmitter and receiver and optical repeaters are placed in our laboratory. The detail of the transmitter and receiver is described in [5]. Waveforms were observed by a sampling oscilloscope after Y-00 signals were converted to the electrical signal by the direct-detection with a PIN photo-diode followed by a transimpedance amplifier and a limiter amplifier. Waveforms of the Y-00 signal and deciphered binary signal measured with the persistence time of 12 hours are shown in Fig. 3. The Y-00 signal waveform (Fig.3 (a)) looked rather noisy since it had 4096 intensity levels. However, clear eye opening was observed after deciphered to the binary signals (Fig.3 (b)). The error free transmission over 160 km was confirmed for the short term (several hours). Presently, we are measuring the long term bit error rate (BER) characteristics, which will be presented in the conference.

In conclusion, we are conducting the long term investigation of an ISK Y-00 transmitter and receiver whose number of signal intensity levels is 4096 and bit rate is 2.5 Gb/s in the transmission line of the 160-km long optical fiber installed in the field. The detail of the results including the long term measurement of the BER characteristics will be presented in the conference.

Figure 1: Basic concept of Y-00 cipher to protect eavesdropping.
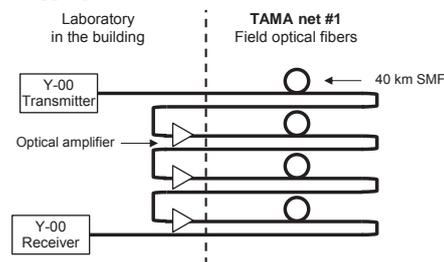
Figure 2: Schematic of the experimental setup.
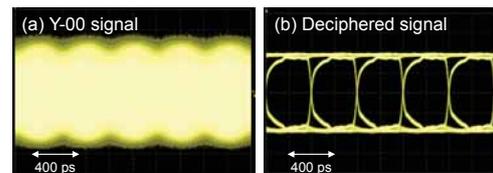
Figure 3: Waveforms of Y-00 and deciphered signals measured for 12 hours.

Acknowledgement

References

[1] O. Hirota, "Practical security analysis of quantum stream cipher by Yuen 2000 protocol," Phys Rev A, 032307, 2007.

[2] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states," Phys. Rev. Lett., vol.22, 227901, 2003.

[3] O. Hirota, M. Sohma, M. Fuse, and K. Kato, "Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme," Phys. Rev. A, 72, 022335, 2005.

[4] K. Harasawa, O. Hirota, K. Yamashita, M. Honda, K. Ohhata, S. Akutsu, T. Hosoi, and Y. Doi, "Quantum encryption communication over a 192-km 2.5-Gbit/s line with optical transceivers employing Yuen-2000 protocol based on intensity modulation," J. of Lightwave Technol. vol. 29, no. 3 , pp.361-323, 2011.

[5] F. Futami and O. Hirota, "Masking of 4096-level intensity modulation signals by noises for secure communication employing Y-00 cipher protocol," 37th European Conference on Optical Communication (ECOC), Tu.6.C.4, 2011.

[6] Y. Doi, S. Akutsu, M. Honda, K. Harasawa, O. Hirota, S. Kawanishi, K. Ohhata, and K. Yamashita, "360 km field transmission of 10 Gbit/s stream cipher by quantum noise for optical network," Optical Fiber Communication Conference (OFC), OWC4, 2010.

[7] F. Futami and O. Hirota, "40 Gbit/s (4 × 10 Gbit/s) Y-00 Protocol for Secure Optical Communication and its Transmission over 120 km," Optical Fiber Communication Conference (OFC), OTu1H.6, 2012.

Faithful Entanglement Swapping Based on Sum Frequency Generation

Thiago Guerreiro[1], **Enrico Pomarico**[1], **Bruno Sanguinetti**[1], **Nicolas Sangouard**[1] **Robert Thew**[1], **Hugo Zbinden**[1], **Nicolas Gisin**[1], **J. S. Pelc**[2], **C. Langrock**[2], **M. M. Fejer**[2]

[1]*Group of Applied Physics, University of Geneva, Switzerland*
[2]*E. L. Ginzton Laboratory, Stanford University, 348 Via Pueblo Mall, Stanford, California 94305, USA*

Device independent quantum key distribution (DIQKD) [1] is a difficult task that requires the distribution of entanglement to distant parties. Since such protocols are based on the violation of Bell-type inequalities, it is very important to close the detection loophole regardless of transmission losses. One solution to this would require heralded entanglement generation and faithful entanglement swapping.

Six-photon protocols for the generation of heralded entangled pairs based on linear optics have been proposed [2]. Such schemes, however, are very challenging [3]. In addition, entanglement swapping protocols based on linear optics and usual Spontaneous Parametric Down Conversion sources (SPDC) suffers from low fidelities [4] $F \leq 50\%$ and requires post selection.

Could we then exploit non-linear optical effects between single photons to generate and distribute entanglement in a heralded way? Experimental demonstrations on this direction have been made [5] using cascaded SPDC. Our work is motivated by a recent theoretical proposal by some of us [4], based on sum frequency generation (SFG) to prepare such heralded maximally entangled pairs. Since SFG can take place with telecom photons, our scheme can be used to herald entangled pairs at a distance.

In the context of DIQKD, figure 1 shows two Spontaneous Parametric Down Conversion sources used to generate time-bin entangled photon pairs. One photon from each source is then combined in a non-linear SFG waveguide, with suitable phase-matching conditions. Once a detection of an upconverted photon occurs, the remaining photons are projected onto a maximally entangled state without the need of post-selection.
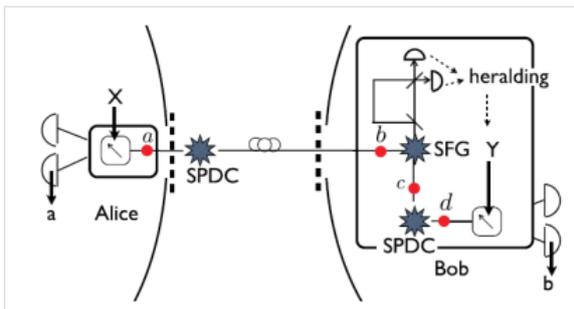
Figure 1: Scheme for faithful heralded time-bin entanglement swapping based on sum frequency generation.

Such faithful entanglement swapping can be experimentally realized using the appropriate sources and an optimized SFG setup. For this reason we have designed and characterized broadband SPDC sources at telecom wavelengths with MHz rates and high coupling efficiencies up to 80% into optical fibres with a set-up similar to the one shown in figure 2.
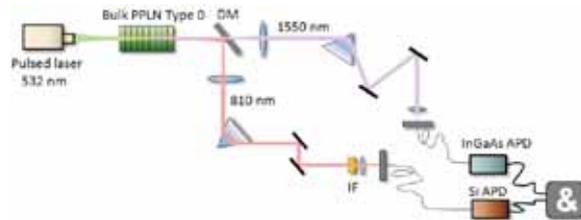
Figure 2: Schematic of an efficient, high rate, photon pair source that can be optimised for performing SFG with single photons. DM stands for dichroic mirror and IF for interference filter.

We have already shown the feasibility of this scenario with weak coherent light to below the single photon level and we now have access to PPLN waveguides with even better efficiency than the one reported in [4]. We are now looking to test this with single photons generated by SPDC.

References

[1] A. Acin et. al., Phys. Rev. Lett., **98**, 230501 (2007).

[2] C. Sliwa, K. Banaszek, Phys. Rev. A, **67**, 030101(R) (2003).

[3] S. Barz et. al., Nature Photonics, 4, 553 (2010).

[4] N.Sangouard et. al., Phys. Rev. Lett., **106**, 120403 (2011).

[5] H. Hubel et. al., Nature, **466**, 601-603 (29 July 2010).

Quantum Key Distribution on Hannover Campus - Establishing Security against Coherent Attacks

V. Händchen[1,3], **T. Eberle**[1,3], **J. Duhme**[2,3], **T. Franz**[2,3], **R. Werner**[2,3], **and R. Schnabel**[1,3]

[1]*Institut für Gravitationsphysik, Leibniz Universität Hannover und Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut)*
[2]*Institut für Theoretische Physik, Leibniz Universität Hannover*
[3]*QUEST Centre for Quantum Engineering and Space-Time Research, Leibniz Universität Hannover*

Regarding quantum key distribution (QKD) one has to distinguish between the discrete and the continuous variable (CV) approach. The latter has the advantage of utilizing homodyne detection schemes with a detection efficiency of almost 100%. The bandwidth, i.e. the speed of homodyne detectors, is not limited by any dead time and can reach more than 100 MHz together with low detector dark noise [1]. Furthermores squeezed light fields, which are a key resource for CV QKD, have been demonstrated with bandwidths above 100 MHz [2]. Altogether, this should in principle allow for secure key rates of similar bandwidth.

To establish CV QKD one can exploit the quantum correlations of quadrature measurements on two-mode squeezed states. Recent theoretical results have shown that two-mode squeezed states with high purity and initial squeezing beyond -10 dB enable QKD which is secure against general coherent attacks [3]. In this scenario an eavesdropper is no longer restricted to collective attacks, i.e. one does not assume that an eavesdropper attacks every signal in the same way. The security analysis of this protocol relies on entropic uncertainty realations and is valid for finite keys. This makes it applicable in experimental realizations.

In the course of the Cluster of Excellence QUEST at the Leibniz Universität Hannover an experiment for CV QKD is implemented. For that purpose an entanglement source at the telecommucation wavelength of 1550 nm was set up. It consists of two squeezed-light sources which, by now, achieved a nonclassical noise reduction of up to 11 dB compared to the vacuum. After superposition of the two squeezed modes on a balanced beam splitter the two entangled output modes are distributed to the participating parties. From the synchronized homodyne measurements with detection efficiencies of nearly 95% a secret key can be extracted using the protocol from [3].

The realization of security against coherent attacks is an important step for future applications of QKD. We will present a detailed analysis of the experimental results as well as a comparision to the theoretical description. Furthermore, an outlook will be given on a planned implementation of an optical fiber for transmission of one entangled output to another institute.

References

[1] Y.M. Chi, B. Qi, W Zhu, L. Qian, H.-K. Lo, S.-H Youn, A.I. Lvovsky, L. Tian, New J. Phys. **13** 013003 (2011).

[2] M. Mehmet, H. Vahlbruch, N. Lastzka, K. Danzmann, R. Schnabel, Phys. Rev. A **81**, 013814 (2010).

[3] F. Furrer, T. Franz, M. Berta, V.B. Scholz, M. Tomamichel, R.F. Werner, arXiv:1112.2179 (2011).

Atmospheric Quantum Communication using Continuous Polarization Variables

B. Heim[1,2,3], **C. Peuntinger**[1,2], **C. Wittmann**[1,2], **C. Marquardt**[1,2,3], **and G. Leuchs**[1,2,3]

[1]*Max Planck Institute for the Science of Light, Erlangen, Germany*
[2]*Institute of Optics, Information and Photonics, Friedrich-Alexander University of Erlangen-Nuremberg (FAU)*
[3]*Erlangen Graduate School in Advanced Optical Technologies (SAOT), FAU*

Atmospheric Quantum Key Distribution (QKD) was demonstrated in 1996 for the first time [1] and since then, a variety of schemes have been implemented (for a review see [2]). These previous systems use single-photon detectors, whereas in our system, we apply an alternative approach: with the help of a bright local oscillator (LO), we perform homodyne measurements on weak coherent states [3]. Polarization multiplexing of signal and LO and propagation of both through the atmospheric channel in the same spatial mode then guarantees an inherently excellent interference at Bob's detection, performed as a Stokes measurement [3, 4]. Channel-induced phase fluctuations are auto-compensated and the detection efficiency is intrinsically high without any need for interference stabilization. The LO acts as a lossless spectral and spatial filter, allowing for unrestrained daylight operation. Note that single-photon detection based schemes in contrast require additional and thus lossy spatial and spectral filters in order to reduce background light. A small portion of the LO is used as a feedback signal to effectively compensate for atmospheric beam wandering. Our experimental focus lies on the characterization of the quantum channel, an intra-city point-to-point link of distance 1.6 km, the principle of which is shown in figure 1.

Effects on continuous variable (CV) quantum states have only recently been studied in the context of propagation through turbulent atmosphere [4, 5, 6, 7]. Here, the main channel influences, i.e. excess noise and losses, can be detrimental to the quantum properties of the transmitted states and therefore must be kept as low as possible.

We successfully transmitted coherent polarization states through the 1.6 km channel, whereas no polarization excess noise was detected above 80 kHz. By improving the receiver's optics and implementation of a beam stabilization system based on an active feedback loop, a mean link transmission of $\approx 70\,\%$ over several hours is achieved. Moreover, the preservation of CV quantum properties by the channel was recently also verified by a successful distribution of polarization squeezed states with 1 dB of squeezing measured at the receiver.

These promising results paved the way towards high bandwidth free space quantum communication such as QKD and transmission of nonclassical states.

Figure 1: Alice produces a polarization state combining signal and local oscillator (LO) in the same spatial mode. Thus, Bob's quantum state detection, a Stokes measurement [3, 4], is immune to atmospheric fluctuations and stray light. Furthermore, we use a small portion of the bright LO as a feedback signal for atmospheric beam stabilization.
CW: continuous wave, (P)BS: (polarizing) beam splitter, HWP: half wave plate, QWP: quarter wave plate, PSD: position sensitive detector

References

[1] B. C. Jacobs, J. D. Franson, Opt. Lett. **21,** 1854 (1996).

[2] V. Scarani et al., Rev. Mod. Phys. **81,** 1301 (2009).

[3] S. Lorenz et al., Appl. Phys. B **79,** 273 (2004).

[4] D. Elser et al., New J. Phys. **11,** 045014 (2009);
B. Heim, et al., Appl. Phys. B **98,** 635 (2010); B. Heim et al., Applications of Lasers for Sensing and Free Space Communications, OSA Technical Digest (2011), paper LWD3

[5] J. Heersink et al., Phys. Rev. Lett. **96,** 253601 (2006);
R. Dong et al., Nat. Phys. **4,** 919 (2008);
B. Hage et al., Nat. Phys. **4,** 915 (2008).

[6] C. Wittmann et al. , Phys. Rev. A **78,** 032315 (2008).

[7] A. A. Semenov, W. Vogel, Phys. Rev. A **80,** 021802 (2009); A. A. Semenov et al., Phys. Rev. A **85,** 013826 (2012).

A high quality quantum link for space experiments

Thomas Herbst[1,2], Rupert Ursin[2], and Anton Zeilinger[1,2]

[1]Vienna Center for Quantum Science and Technology (VCQ), Quantum Optics, Quantum Nanophysics and Quantum Information, Faculty of Physics, University of Vienna, Vienna, Austria
[2]Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Vienna, Austria

Quantum entanglement is the fundamental feature of quantum physics. It describes the situation in which the information about the state of a composite system of two (or more) distinct particles is "stored" solely in joint properties. Bringing entangled photon pairs to a Space environment will not only provide unique opportunities for quantum communication applications over long distances but will also enable to perform a new range of experiments investigating very fundamental questions of physics. Even though the preservation of entanglement was tested already over distances of up to 144km on a horizontal Earth-based link between the Canary Islands La Palma and Tenerife [1, 2], the important question remains whether the distance between two entangled quantum systems is limited. Hence, satellite based experiments would allow expanding the scale for testing the validity of quantum physics by several orders of magnitude - clearly beyond the capabilities of Earth-based laboratories. Besides its importance for fundamental physics, the correlations between entangled quantum systems have become a basic building block in the novel field of quantum information processing and the Space infrastructure will eventually enable the development of a world-wide network for quantum communication. The success of future space experiments and quantum networks will rely on a stable and efficient quantum link between the satellite and the ground station. Losses due to the turbulent atmosphere have to be minimized in order to increase the signal over the quantum channel.

We present a high-speed adaptive-optics (AO) system based on the blind optimization scheme [3] which is capable of pre-compensating for the atmospheric turbulences in order to establish a high quality link for point-to-point quantum communication. First experiments between the Canary Islands La Palma and Tenerife (see Fig. 1) showed an increase of the link efficiency of 18% (see Fig. 2).
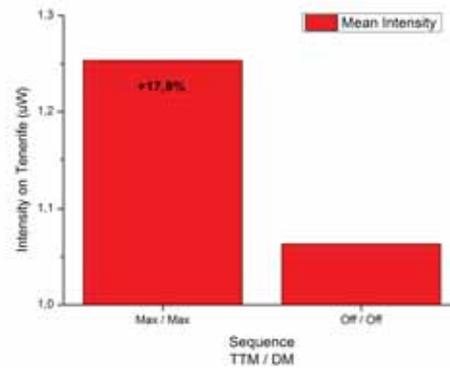
Figure 2: Mean intensity of the received 808nm signal, measured with a powermeter in the focal point of the 1m telescope on Tenerife. The column Max/Max corresponds to the TTM and DM in optimization mode. Off/Off means that both adaptive mirrors were switched off.

References

[1] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek et al., Nature Physics, vol. 3, pp. 481-486, 2007.

[2] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, Nature Physics, vol. 5, pp. 389-392, 2009.

[3] V. Polejaev, P. Barbier, G. Carhart, M. Plett, D. Rush, and M. Vorontsov, Proceedings of SPIE, vol. 3760, p. 88, 1999.
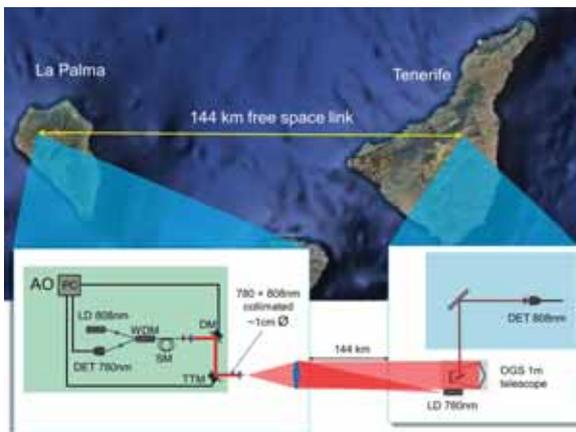
Figure 1: Experimental setup of the AO-system test between the Canary Islands La Palma and Tenerife.

Revival of short-wavelengths for quantum communication applications

Evan Meyer-Scott[1], Zhizhong Yan[1], Allison MacDonald[1], Jean-Philippe Bourgoin[1], Chris Erven[1], Alessandro Fedrizzi[2], Gregor Weihs[3], Hannes Hübel[4] and Thomas Jennewein[1]

[1]*Institute for Quantum Computing, University of Waterloo, 200 University Avenue W, Waterloo ON N2L 3G1, Canada*
[2]*ARC Centre for Engineered Quantum Systems, ARC Centre for Quantum Computer and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane, QLD 4072, Australia*
[3]*Institut für Experimentalphysik, Universität Innsbruck, Innrain 52, 6020 Innsbruck, Austria*
[4]*Fysikum, University of Stockholm, 106 91 Stockholm, Sweden*

Quantum communication protocols, like quantum key distribution (QKD), have been successfully demonstrated with photons of various wavelengths. The preferred wavelength for free-space transmission is around 800 nm, where single photon detectors have high efficiency and the atmosphere is transparent. In contrast, the transmission in optical fibres is performed with photons around 1550 nm, exploiting the low absorption in this region. However for certain scenarios it is preferable not to adhere to the above conventions and use shorter wavelengths. We present here two such cases: Firstly, we demonstrated the feasibility of ground to satellite QKD using single photons at 532 nm. Secondly, we demonstrated a QKD link in deployed telecom fibres using entangled photons at 800 nm.

In order to overcome the distance limitations faced by QKD in terrestrial transmissions, satellite QKD might be a way to enable worldwide secure communication. In the most immediately feasible scenario, the satellite acts as a trusted node to relay a key between Alice and Bob's ground stations. Work has mainly been concentrated on a downlink of photons from the satellite due to minimal losses from atmospheric turbulence [1]. The satellite uplink in contrast requires only a static receiver and single photon detectors, but it must be able to cope with the higher losses (40 - 50 dB). Such losses can be accommodated using fast detectors and timing methods. The creation of short-pulsed, phase randomized, polarization and amplitude modulated light at 532 nm is realised by polarization-preserving up-conversion of a modulated telecom beam with a pulsed infrared laser. As shown in Fig. 1, we performed experiments over a controllable-loss channel, finding the maximum permissible total loss of the system to be 57 dB [2], with a secure key generation rate at this maximal loss of 2 bits/s. We also performed satellite orbit simulations, and show that our system can generate 5.7×10^4 bits of secure key at our 76 MHz clock rate.

In our second investigation we demonstrate the distribution of entangled photons of wavelength 810 nm through standard telecom fibres. This allows quantum communication protocols to be performed over established fibre infrastructure, and makes use of the smaller and better performing setups available around 800 nm, as compared to those which use telecom wavelengths around 1550 nm. The combination of fibre loss and higher detection efficiencies of Si based single photon detectors results in better performance at 800 nm for up to 2.4 km of optical fibre. Launching polarisation entangled photons at 810 nm into telecom fibres results in the excitation of higher order modes which are also guided by the fibre [3]. However the higher order modes experience a different polarisation rotation lowering the visibility of the entangled state.
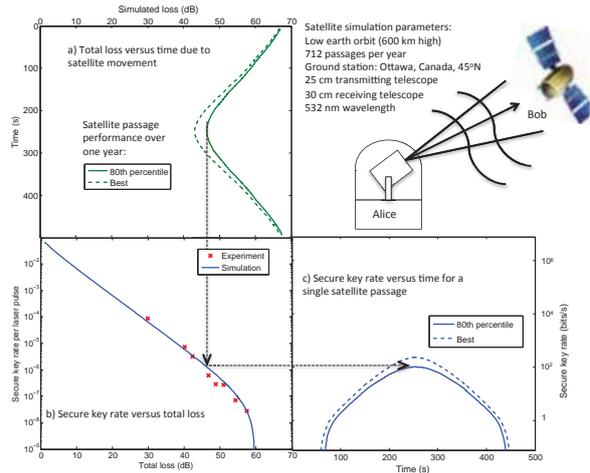
Figure 1: Secure key rate over high loss channel. a) Simulation of total loss versus visible passage time for a satellite uplink. b) Experimental results and simulation of secure key rate versus loss. c) Expected secure key rate versus time for a satellite passage.

We performed distributions up to 6 km in fibre spools [4], and by either spatial or temporal filtering the visibility could be brought to 96%, which is close to the value measured directly at the source. To illustrate the utility of using such a distribution channel, we performed a full QKD protocol over two symmetric 2.2 km channels of installed telecom fibres, leading to a total distribution distance of 4.4 km. The average quantum bit error ratio was 4.3% (i.e. 91.4% visibility) with both temporal and spatial filtering, leading to an average secure key rate of 350 bits/s. The increase in the error rate was attributed to disturbances from passing cars, trains, and thermal fluctuations in the deployed fibres.

References

[1] J.G. Rarity, P.R. Tapster, P.M. Gorman and P. Knight, New Journal of Physics, 4, 82 (2002).

[2] E. Meyer-Scott, Z. Yan, A. MacDonald, J.P. Bourgoin, H. Hübel and T. Jennewein, PRA, 84, 062326 (2011).

[3] P. D. Townsend, Photonics Technology Lett., IEEE, 10, 1048 (1998).

[4] E. Meyer-Scott, H. Hübel, A. Fedrizzi, C. Erven, G. Weihs and T. Jennewein, APL, 97, 031117 (2010).

Implementability of two-qubit unitary operations over the butterfly network with free classical communication

Seiseki Akibue[1] **and Mio Murao**[1]

[1]*The University of Tokyo, Tokyo, 113-0033, Japan*

We investigate what subset of $SU(4)$ operations is implementable over the butterfly network presented in Figure 1 in the setting *with free classical communication*. We extend a protocol which allows one to perform 2-pair quantum communication over the butterfly network with free classical communications proposed by Kobayashi *et al.* [1, 2], and present a protocol that implements two classes of $SU(4)$ operations, which contain all Clifford and controlled-unitary operations, over the butterfly network without additional resources.
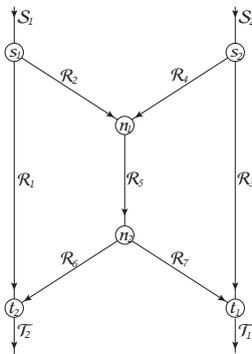
Figure 1: The butterfly network with the input nodes (s_1 and s_2), output nodes (t_1 and t_2) and the repeater nodes (n_1 and n_2). The directed edges $S_1, S_2, T_1, T_2, R_1, \cdots, R_7$ represent a single-qubit quantum channel. The indices of the Hilbert spaces of the transmitted qubits corresponding to the edges are also denoted by $S_1, S_2, T_1, T_2, R_1, \cdots, R_7$. Operations on the qubits at the same node are considered local operations.

Setting: Implementations of unitary operations over networks are generalizations of *k-pair quantum communication* tasks to *network computation* tasks [3]. k-pair quantum communication over a network is a unicast communication task that faithfully transmits a k-qubit state given at k distinct input nodes to k distinct output nodes through the network, where the pairings $\{m, n\}$ between the input node s_m and the output node t_n are described by a permutation π. The total output state $|output\rangle$ at the k output nodes can be regarded as a state obtained by performing a unitary operation U_π corresponding to a permutation π on the total input state $|input\rangle$ given at the k input nodes, namely, $|output\rangle = U_\pi |input\rangle$.

In quantum mechanics, not only U_π but more general quantum operations (quantum maps) are allowed. In this poster, we investigate implementations of two-qubit unitary ($SU(4)$) operations over the butterfly network where quantum communication is restricted by the network configuration but any classical communication is allowed freely.

The Kobayashi *et al.* **protocol:** The protocol of 2-pair

quantum communication presented in [2] for the butterfly network is composed of two stages. In the first stage, the encoding stage, a gate sequence consisting only of CNOT gates is performed corresponding to the classical network coding. In the second stage, the disentangling stage, two kinds of disentangling operations depending on the measurement outcomes s are performed. One of the disentangling operations is given by

$$\Gamma_{d2}^s = \sum_{z=0,1} Z^s |z\rangle (\langle s|H \otimes \langle z|). \quad (1)$$

In the last part of the Kobayashi *et al.* protocol, four qubits $\{R_1, R_3, T_1, T_2\}$ are entangled but the other qubits are measured and disentangled.

Our protocol: We modify the last disentangling operation of the Kobayashi *et al.* protocol. Instead of performing Γ_{d2}^s on the pairs of qubits $\{R_1, T_1\}$, and on $\{R_3, T_2\}$, we first perform a local unitary operation $U \in SU(4)$ on the pairs of qubits $\{R_1, T_2\}$ and on $\{R_3, T_1\}$ and then perform Γ_{d2}^s. By the requirement of determinism of the output state, we can prove the following theorem.

Theorem: Our modified protocol implements $SU(4)$ operations over the butterfly network if and only if U is an element of $U_\pi(\{\theta_i\}) \in SU(4)$ defined by

$$U_\pi(\{\theta_i\}) = \sum_{i=0}^{3} e^{i\theta_{\pi_i}} |\pi_i\rangle\langle i|, \quad (2)$$

where π_i denotes a permutation, $\{|i\rangle\}_{i=0,1,2,3}$ denotes the 2-qubit computational basis and $\theta_i \in [0, 2\pi)$. By taking $U = U_\pi(\{\frac{\theta_i}{2}\})$ in the modified protocol, $U_\pi(\{\theta_i\})$ is implementable over the butterfly network.

Two classes: We can classify $U_\pi(\{\theta_i\})$ into two classes. The elements of the first class are locally unitarily equivalent to a controlled-phase operation $|00\rangle\langle00| + |01\rangle\langle01| + |10\rangle\langle10| + e^{i\theta}|11\rangle\langle11|$, which is implementable even in the setting where classical communication is also restricted [3]. The second class is locally unitarily equivalent to a controlled-phase operation followed by a swap operation $|00\rangle\langle00| + |01\rangle\langle10| + |10\rangle\langle01| + e^{i\theta}|11\rangle\langle11|$.

References

[1] H. Kobayashi, F. Le Gall, H. Nishimura and M. Rötteler, arXiv preprint 0902.1299.

[2] H. Kobayashi, F. Le Gall, H. Nishimura and M. Rötteler, arXiv:1012.4583.

[3] A. Soeda, Y. Kinjo, P.S. Turner and M. Murao, Phys. Rev. A 84, 012333 (2011).

QCMC 2012
Vienna, Austria

Accessible nonlinear entanglement witnesses

Juan Miguel Arrazola, Oleg Gittsovich and Norbert Lütkenhaus[1,2]

[1]*Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, N2L 3G1 Waterloo, Ontario, Canada*
[2]*Department of Physics and Astronomy, University of Waterloo, 200 University Avenue West, N2L 3G1 Waterloo, Ontario, Canada*

Verification of entanglement is an important tool to characterize sources and devices for use in quantum computing and communication applications. Evaluation of entanglement witnesses (EW) are a particularly valuable technique to prove the presence of entanglement, especially for higher-dimensional systems as they do not require a reconstruction of the underlying quantum state (full tomography). In this work, we provide a method to construct *accessible nonlinear EWs*, which incorporate two important properties.

First, they improve on linear EWs in the sense that each nonlinear EW detects more entangled states than its linear counterpart and therefore allow the verification of entanglement without critical dependence on having found the "right" linear witness. Second, they can be evaluated using exactly the same data as for the evaluation of the original linear witness.

This allows a reanalysis of published experimental data to strengthen statements about entanglement verification without the requirement to perform additional measurements. These particular properties make the accessible nonlinear EWs attractive for the implementations in current experiments, as they also enhance the statistical significance of the entanglement verification.

Construction of accessible nonlinear EWs: Our starting point is a specific decomposition of a linear EW $W \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ in terms of local observables $\{A_i \otimes B_i\}_{i=1}^N$. In other words, W can be written as $W = \sum_i c_i A_i \otimes B_i$. This implies that its expectation value can be computed solely from the expectation values $\{\langle A_i \otimes B_i \rangle\}_{i=1}^N$ that are obtained from experimental data.

In our work we make use of the Choi-Jamiołkowski isomorphism to construct nonlinear improvements W_{NL} of *any* linear EW W. Most importantly, for a fixed decomposition of W in terms of local observables, we provide sufficient conditions for the expectation value of any W_{NL} to be computable from the same data as their linear ancestor. We call these *accessible* nonlinear entanglement witnesses.

Additionally, we show that for special choices, we can construct powerful nonlinear EWs whose expectation value can be expressed as a simple analytic formula. For this case, we even provide necessary and sufficient conditions for the nonlinear EWs to be accessible.

One of the main characteristics of accessible EWs is that they always detect more states than their linear counterparts. This is clearly illustrated in Figure 1 for the case of two qubits, but it must be noted that similar behaviour also occurs for higher-dimensional systems. This fact is a property that has important implications for significance statements in entanglement verification experiments.

The usual and widely used approach of placing error bars on measured data has led to counterintuitive statements (cf. [1]). In order to make reliable and meaningful statements
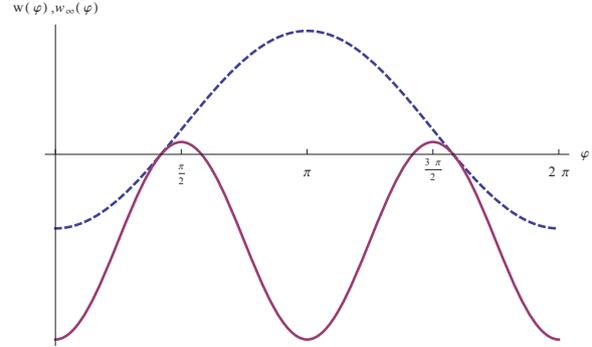
Figure 1: Value of the linear witness w (dashed blue curve) and its nonlinear improvement w_∞ (purple curve) for the state $\rho(\varphi) = (2/3)|\varphi\rangle\langle\varphi| + (\mathbb{1}/12)$ where $|\varphi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - e^{i\varphi}|10\rangle)$. The starting witness is $W = (\mathbb{1} + \sum_{\alpha=x,y,z} \sigma_\alpha \otimes \sigma_\alpha)$.

for detection significance in entanglement verification experiments, a more consistent framework has been recently presented by M. Christandl and R. Renner in [2]. There, the outcomes of n runs of an experiment leads to an estimate density $\mu_n(\rho)$ which can be seen as a measure on the space of all states.

This picture can be related to the detection significance provided by the entanglement witnesses in the following sense. Denote by Γ_W the set of all states that are detected by a witness W. The probability of a state to lie in Γ_W is then given by

$$P_{\mu_n}(\Gamma_W) = \int_{\Gamma_W} \mu_n(\rho) d\rho. \qquad (1)$$

Since the set of states $\Gamma_{W_{NL}}$ detected by a nonlinear witness W_{NL} is always larger than that of a linear witness, it always holds that $P_{\mu_n}(\Gamma_{W_{NL}}) > P_{\mu_n}(\Gamma_W)$. Hence, accessible EWs can only increase detection significance in entanglement detection experiments.

References

[1] B. Jungnitsch, S. Niekamp, M. Kleinmann, O. Gühne, H. Lu, W. Gao, Y. Chen, Z. Chen, and J. Pan, *Phys. Rev. Lett. 104, 210401 (2010)*.

[2] M. Christandl and R. Renner, *arXiv:1108.5329*.

[3] J.M. Arrazola, O. Gittsovich and N. Lütkenhaus, *arXiv:1203.1239v1*.

[4] T. Moroder, O. Gühne and N. Lütkenhaus, *Phys. Rev. A*, **78**, 032326, (2008).

A characterization scheme of universal operation: the universal-NOT gate

Jeongho Bang[1,2], **Seung-Woo Lee**[1], **Hyunseok Jeong**[1], and **Jinhyoung Lee**[1,2]

[1]*Center for Macroscopic Quantum Control & Department of Physics and Astronomy, Seoul National University, Seoul, 151-747, Korea*
[2]*Department of Physics, Hanyang University, Seoul 133-791, Korea*

We propose a scheme how to characterize a universal operation. By the term "universal", we mean an operation without any dependence on the set of input states. Cloning an arbitrary quantum state is a typical example of such an operation. Another universal operation is the universal-NOT (UNOT) operation, which transforms an arbitrary qubit state $|\Psi\rangle$ to its orthogonal one $|\Psi^{\perp}\rangle$. It is known that the perfect operation of such a task is forbidden by the quantum mechanical law [1], and it is thus natural to find an approximate but optimal one.

Average fidelity has been considered as an indicator of optimality for a given universal operation. When considering an operation $\hat{O}$ for an arbitrary input $|\Psi\rangle$ and its target $|\Psi_{\tau}\rangle$, the average fidelity F is given by

$$F = \int d\Psi f, \qquad (1)$$

where $f = |\langle \Psi_{\tau}| \hat{O} |\Psi\rangle|^2$ is the fidelity between the output and target state, the integral is over all possible inputs $|\Psi\rangle$.

The average fidelity F does not necessarily imply a universal approximation to a given task. For UNOT gate, the optimal average fidelity is $2/3 \simeq 0.666$ [1, 2]. Thus, an additional parameter is required to characterize if a found operation is universal. We call it "fidelity deviation". The fidelity deviation D is quantified by the standard deviation Δ of the fidelity f over possible input states, such that

$$D = 2\Delta = 2 \left(\int d\Psi f^2 - F^2 \right)^{1/2}, \qquad (2)$$

where $D = 0$ when the operation fidelity is independent of the input, *i.e.* universal so that $f = F$ for all input states, and it increases otherwise. The fidelity deviation D satisfies the condition

$$0 \leq D \leq 2\sqrt{F(1 - F)} \leq 1. \qquad (3)$$

We employ both of the average fidelity F and fidelity deviation D in characterizing the optimality and universality of an operation.

In this approach, we consider NOT gate operations implemented on one, two, and three qubit(s), respectively, and analyze them on the space of the average fidelity and the fidelity deviation. We show that all the three operations of NOT can be realized so as to reach $2/3$ of the average fidelity, for all possible Bloch states, the same as the original UNOT of using three qubits. To the contrary, a one-qubit operation of NOT depends strongly on its input state so that the fidelity deviation D is a linear function of the average fidelity F, and it never vanishes if $F \neq 0$. A two-qubit NOT shows a better universal behavior in the sense that it has a smaller fidelity deviation and a learger average fidelity than any one-qubit NOT. A NOT operation can be universal only if three qubits
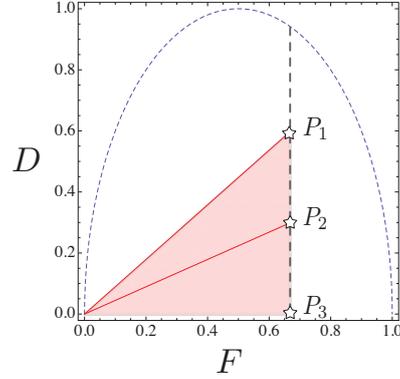
Figure 1: The possible regions of one-, two-, and three-qubit NOT gate are drawn in the space of (F, D). Every one-qubit NOT gate corresponds to a point on the line $\overline{OP_1}$. Two-qubit NOT gate does a point inside and on the triangle OP_1P_2, and it is optimal at $P_2(F = \frac{2}{3}, D = \frac{2}{3\sqrt{5}} \simeq 0.298)$ in the sense that F is the largest and D is the smallest. On the other hand, a three-qubit NOT gate is located in the regin of the triangle OP_1P_3, and it can be universal with the zero fidelity deviation. The dashed curve stands for the mathematical boundary of a universal operation, given in Eq. (3).

are employed to realize. It is remarkable that every average fidelity of the maximum $2/3$ does not imply a universal NOT, because the fidelity deviation does not necessarily vanish, as seen in the line $\overline{P_1P_3}$, Fig. 1.

We analyze the NOT gates in realistic experimental conditions. In particular we consider an operational error, originating from an imperfect device. In the presence of a small error of order, the average fidelity is 0.634 ± 0.018, close to $2/3$ in a theory and also to the value in an experiment [3], but the fidelity deviation is 0.214 ± 0.051, rather large value, in the sense that it is close to that of the randomly generated one, 0.298 ± 0.067. This feature is important, as the fidelity deviation is necessary to characterize a UNOT gate in terms of the universality as well as the optimality.

We expect that our approach will provide a better insight on universal quantum operations, and also may be useful in a practical experiment as well.

References

[1] V. Bužek, M. Hillery, and R. F. Werner, Phys. Rev. A **60**, 2626 (2009).

[2] V. Bužek, M. Hillery, and R. F. Werner, J. Mod. Opt. **47**, 211 (2000).

[3] F. D. Martini, V. Bužek, F. Sciarrino, and C. Sias, Nature **419**, 815 (2002).

CGLMP$_4$ Inequality as a Dimension Witness

Cai Yu[1], **Jean-Daniel Bancal**[2] and **Valerio Scarani**[1,3]

[1]*Centre for Quantum Technologies, National University of Singapore, Singapore*
[2]*Group of Applied Physics, University of Geneva, Switzerland*
[3]*Department of Physics, National University of Singapore, Singapore*

Introduction: The dimensionality of the quantum system can be seen as resource for quantum information processes. This work presents a dimension witness based on bipartite correlations.

Bell's inequalities were first introduced to test whether a distribution could be arisen from local hidden variables. It turns out that Bell inequality has other important applications in quantum information processing. Such as lower bounding the dimension of the Hilbert space the describes the system. Previous work done by Brunner *et al.* [1] first introduces the idea of dimension witness. The inequality relevant to this work is the Collins-Gisin-Linden-Massar-Popescu (CGLMP) inequality [2].

The CGLMP inequality, I_n, is a generalization of the CHSH inequality to a 2-party, 2-input and n-outcome case. In such an experiment, the joint probability distribution of the outcomes may be recorded as $P(a,b|x,y)$, where $a, b \in \{0, 1, \cdots, n-1\}$ denote the outcomes, and $x, y \in \{0, 1\}$ denote the choice of measurements. On top of non-negativity and normalization, we also impose the no-signalling condition.

The joint probabilities could be organised in an array:

$$P = \frac{\begin{array}{c|c} & \| \ P(b|y=0) \ | \ P(b|y=1) \end{array}}{\begin{array}{c|c|c} P(a|x=0) & \| \ P(a,b|0,0) & \ P(a,b|0,1) \\ \hline P(a|x=1) & \| \ P(a,b|1,0) & \ P(a,b|1,1) \end{array}}, \quad (1)$$

where $P(a,b|x,y)$ are n-by-n arrays denoting the joint distributions, $P(a|x)$ and $P(b|y)$ are the respective marginals.

The CGLMP inequality can similarly be expressed in an array form:

$$\langle I_n, P \rangle \leq 0. \quad (2)$$

I_n has the form of:

$$I_n = \frac{\begin{array}{c|c} & \| \ \mathbf{-1} \ | \ \mathbf{0} \end{array}}{\begin{array}{c|c|c} \mathbf{-1} & \| \ \mathbf{J} & \ \mathbf{J}^T \\ \hline \mathbf{0} & \| \ \mathbf{J}^T & \ \mathbf{-J}^T \end{array}}, \quad (3)$$

where $\mathbf{J}$ is an upper triangular matrix filled with 1's and $\langle \cdot, \cdot \rangle$ denotes term-by-term multiplication. While 0 is local bound for this inequality, PR$_{2,n}$-boxes violate I_n up to $\frac{n-1}{n}$.

From here onwards, we will be looking at a particular CGLMP inequality, the I_4 inequality, which deals with the scenario with $n = 4$ outcomes.

Maximum violation of the I_4 inequality by ququads: It has been shown in the Table 1 of [3], that the maximal violation of I_4 is bounded by $I_4^* \approx 0.364762$, by the positive semidefinite criteria. On the other hand, a class of ququad states were found to reach such a violation up to numeric precision. Thus the maximal violation of I_4 is found analytically

to be $I_4^* = -\frac{3}{4} + \frac{C + yS + \sqrt{\frac{1-y^2}{2}}(1+2S)}{2}$, where $C = \cos\frac{\pi}{8}$, $S = \sin\frac{\pi}{8}$, $x = \sqrt{1 - \frac{1}{\sqrt{2}}}$ and $y = \frac{x}{\sqrt{3x^2 + \sqrt{2}x + 1}}$.

Maximum violation of the I_4 inequality by qutrits: The idea of dimension witness is that there exists an upper bound of CGLMP violation if we restrict ourself to lower dimension systems. In this case, the maximum violation of the I_4 with qutrits on each party, $\max_{Q|3} I_4$, is strictly lesser than I_4^*.

As an first attempt, we analyse the maximal violation of the I_4 with quqtrits over a restricted class of POVM. On that class, the I_4 violation could be shown to identical to that of I_3. Similarly to how we found the maximum violation of I_4, the maximum violation of I_3 could found to be $I_3^* = \frac{\sqrt{33}-3}{9} \approx 0.304951$.

Numerical proof: For the general POVM's we turned to numerical optimization method. An iterative numerical optimization procedure, called the see-saw method was introduced in [4]. With the see-saw method, numerical evidence strongly suggests that I_3^* is indeed the maximum violation of the inequality I_4, even with general POVMs.

Conclusion: We show that CGLMP$_4$ inequality I_4, could be a dimension witness for four level systems (ququads). Maximum violation of the inequality with ququads is shown to be $I_4^* \approx 0.364762$. We obtain strong numerical evidence that, with qutrits, the bound becomes $I_3^* = \frac{\sqrt{33}-3}{9} \approx 0.304951$ and provide an analytical proof of this bound for a restricted class of POVMs. The violation of this bound indicates the presence of entangled ququads or higher dimensional systems.

References

[1] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. Méthot, and V. Scarani, "Testing the dimension of hilbert spaces," *Phys. Rev. Lett.*, vol. 100, no. 21, p. 210503, 2008.

[2] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, "Bell inequalities for arbitrarily high-dimensional systems," *Phys. Rev. Lett.*, vol. 88, p. 040404, Jan 2002.

[3] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," *New J. Phys.*, vol. 10, p. 073013, 2008.

[4] R. F. Werner and M. M. Wolf *Quant. Inf. Comp.*, vol. 1, p. 1, 2001.

Propagation of non-classical correlations across a quantum spin chain

S. Campbell[1,2,8], **T. J. G. Apollaro**[3], **C. Di Franco**[1], **L. Banchi**[3,4], **A. Cuccoli**[3,4], **R. Vaia**[5], **F. Plastina**[6,7], **and M. Paternostro**[8]

[1]*Department of Physics, University College Cork, Republic of Ireland*
[2]*Quantum Systems Unit, Okinawa Institute of Science and Technology, Okinawa, Japan*
[3]*Dipartimento di Fisica e Astronomia, Università di Firenze, Italy*
[4]*INFN Sezione di Firenze, via G.Sansone 1, I-50019 Sesto Fiorentino (FI), Italy*
[5]*Istituto dei Sistemi Complessi, Consiglio Nazionale delle Ricerche, Italy*
[6]*Dipartimento di Fisica, Università della Calabria, 87036 Arcavacata di Rende (CS), Italy*
[7]*INFN - Gruppo collegato di Cosenza, Università della Calabria, Italy*
[8]*Queen's University, Belfast BT7 1NN, United Kingdom*

The behavior of features such as quantum coherence and entanglement in a composite quantum system whose state is exposed to the effects of environmental actions has been the focus of an extensive research activity. Recently, much attention has been paid to the case of environments embodied by systems of interacting quantum particles. Such dynamical environments can induce interesting back actions on the evolution of a system, thus significantly affecting its properties. From the point of view of coherent information processing, on the other hand, the non-trivial dispersion properties of networks of such interacting particles represent an interesting opportunity for their use as short-haul communication channels for the inter-connections among on-chip nodes in the next generation of information processing devices.

While most of the work in these contexts has focused on the study of the properties of entanglement upon propagation in such media, it is now widely accepted that the space of non-classical correlations accommodates more than *just* quantum entanglement. Figures of merit such as quantum discord and measurement-induced disturbance, to cite only two of the most popular ones [1, 2], are able to capture the content of non-classical correlations of a state well beyond entanglement. Although the role played by such broader forms of non-classical correlations in the quantum mechanical manipulation of information has yet to be fully understood, enormous is the interest they bring about as the manifestation of the various facets of quantumness in a system. It is thus very important to work on the exploration of the behavior of such quantities upon exposure to dynamical and finite environments of the sort addressed above, so as to build a useful parallel with the much more extensively investigated case of entanglement.

We study the propagation of quantum correlations across a system of interacting spin-$1/2$ particles [3], Fig 1 (a). Our main goal is to compare the way important indicators of non-classicality, such as quantum discord (QD) [1, 2] and entanglement of formation (EoF) [4], are transferred through a medium offering non-trivial dispersion properties. In doing this, we aim at understanding whether or not the fundamentally conceptual difference between entanglement and discord leaves signatures in the way such non-classical quantities are transferred. We show that this is indeed the case by preparing a non-separable (in general mixed) state of an isolated spin and the one occupying the first site of a linear spin-chain. We then compare the quantum-correlation properties of such an initial state with those of the state achieved, at a given instant of time of the evolution, between the isolated spin and the one

occupying the last site of the chain itself. QD appears to be better transmitted than entanglement (as quantified by EoF) in a wide range of working conditions and regardless of the details of the initial state being considered as shown in Fig. 1 (b).
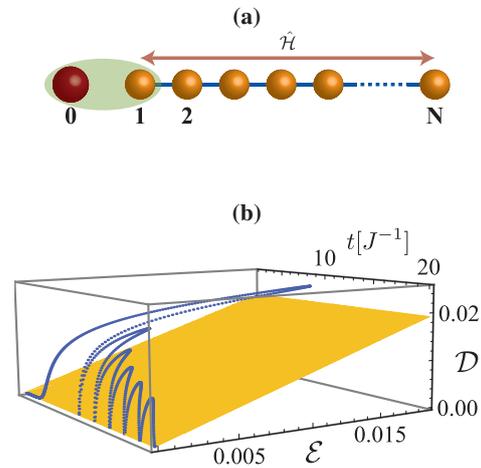
Figure 1: (a) We consider a chain of N interacting spin-$1/2$ particles coupled through a XX Hamiltonian model. We study how the general quantum correlations of such a state propagate across the chain. (b) Behavior of QD against EoF and propagation time for a chain of 15 spins, homogeneous intra-chain couplings. The yellow plane at $\mathcal{D}=\mathcal{E}$ is used as a guide to the eye for discerning whether or not $\mathcal{D} \geq \mathcal{E}$.

References

[1] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).

[2] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).

[3] S. Campbell, T. G. A. Apollaro, C. Di Franco, L. Banchi, A. Cuccoli, R. Vaia, F. Plastina, and M. Paternostro, Phys. Rev A, **84**, 052316, (2011).

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wooters, Phys. Rev. A **54**, 3824 (1996); W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

Purification to Locally Maximally Entangleable States

Tatjana Carle[1], **Julio De Vicente**[1], **Wolfgang Dür**[1], **Barbara Kraus**

[1]*Institute for Theoretical Physics, University of Innsbruck, Austria*

The motivation for purifying a quantum state is that for most applications in quantum information theory it is crucial to have a pure or almost pure quantum state at hand. In most setups the generated states are noisy and therefore it is desired to purify the state actively. Since the parties which share the quantum state, e.g. in a communication scenario, can be spatially separated the protocol should make only use of local operations and classical communication (LOCC). If the desired state is multipartite entangled one of the main challenges is to access and process the non-local information with such a LOCC protocol.

The multipartite entangled states we show one can purify to are called Locally Maximally Entangleable (LME) states [1]. They form a large class meaning 2^n real parameters are in general needed to describe an n-qubit quantum state. Physically those states arise from a multipartite Ising interaction and they can for example be used to encode optimally the maximal number of classical bits and contain prominent subclasses such as stabilizer states and graph states. We present a purification protocol for certain LME states and show how well the protocol performs if the quantum states are subjected to certain kind of noise channels. We also show that the multipartite purification scheme can outperform purification schemes which rely on bipartite strategies. For graph and stabilizer states there already existed purification protocols[2]. However, since the stabilizers of the LME states are in general non-local, in contrast to the stabilizers of graph and stabilizer states, we had to develop new methods which go beyond the commonly used CNOT-procedure.

References

[1] C. Kruszynska, B. Kraus, PRA **79**, 052304 (2009).

[2] C. Kruszynska, A. Miyake, H. J. Briegel, W. Dür, PRA **74**, 052316 (2006) and S. Glancy, E. Knill, H.M. Vasconcelos, PRA **74**, 032319 (2006).

Quantum computing with incoherent resources and quantum jumps

M.F. Santos[1], **M. Terra Cunha**[2], **R. Chaves**[3], **A.R.R. Carvalho**[4]

[1]*Departamento de Física, Universidade Federal de Minas Gerais, Belo Horizonte, CP 702, 30123-970, Brazil*
[2]*Departamento de Matemática, Universidade Federal de Minas Gerais, Belo Horizonte, CP 702, 30123-970, Brazil*
[3]*ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*
[4]*Centre for Quantum Computation and Communication Technology, Department of Quantum Sciences, Research School of Physics and Engineering, The Australian National University, Canberra, ACT 0200 Australia*

Quantum computation requires a set of basic operations: measurements on the computational basis, single qubit rotations, and specific two-qubit entangling gates. In the traditional circuit model of quantum computation, for example, a quantum algorithm is implemented by the sequential action of entangling gates and local unitaries followed by a final measurement stage that reveals the result of the computation.

A major obstacle to any practical implementation is decoherence: qubits are encoded in quantum systems that are unavoidably coupled to the environment, reducing the capacity to process quantum information. However, here we show that when the environment is suitably monitored one is able to build all the fundamental blocks needed to perform quantum computation. In particular we show how to implement two-qubit entangling gates and how they can be interconnected to efficiently build up the cluster states necessary for measurement-based quantum computation.

Our scheme involves the detection of spontaneously emitted (s.e.) and inelastic scattered (i.s.) photons, two notable examples of decoherence processes harmful to quantum computation. The emitted photons come naturally from the qubit decay while the scattered ones are produced through the incoherent pumping back to the excited state shown in Fig. 1-a. The pumping can be adjusted so that one builds a symmetric effective environment interaction where the probabilities of excitation and decay are the same (Fig. 1-b). The detection of such photons leads to the observation of quantum jumps in the system, usually associated with irreversible processes. Indeed, the detection of a "s.e." photon corresponds to the decay to the ground state while the complementary excitation process is connected with the detection of photons in the "i.s." channel. It seems unlikely then, that one could build the entangling unitary gates necessary for quantum computation purely from the detection of quantum jumps.

The solution is to design the measurement process shown in Fig. 1-c. If we assume that both "s.e." and "i.s." processes are tuned to output photons that are indistinguishable in frequency and linewidth but of orthogonal circular polarisations, then, by placing polarised beam splitters (PBS) before the photocounters, the which process information is erased. In this case, the detection of a photon that comes out of the PBS will implement quantum jumps that are linear combinations of σ_- and σ_+, in particular σ_x and σ_y [2]. Now, in order to create entanglement between two qubits, a second quantum erasing process is required, one that destroys the "which qubit" information. This is achieved by combining the output ports of the PBS of two different qubits in a standard Beam Splitter (BS). In this case, as a consequence of the erasing process, clicks in the detectors of the newly defined channels

will correspond to entangling jumps given by linear combinations of local unitary flips, such as $X_{AB}^{\pm} = (\sigma_{x_A} \pm i\sigma_{x_B})/\sqrt{2}$, where the sign is randomly determined by the channel where the photon is detected. These engineered jumps that correspond to unitary operations, allowed us to show that quantum jumps actually have full and efficient quantum computing power [1]. As an example, Fig. 1-c shows the time taken to build cluster states of N qubits from the concatenation of the jump entangling gates.
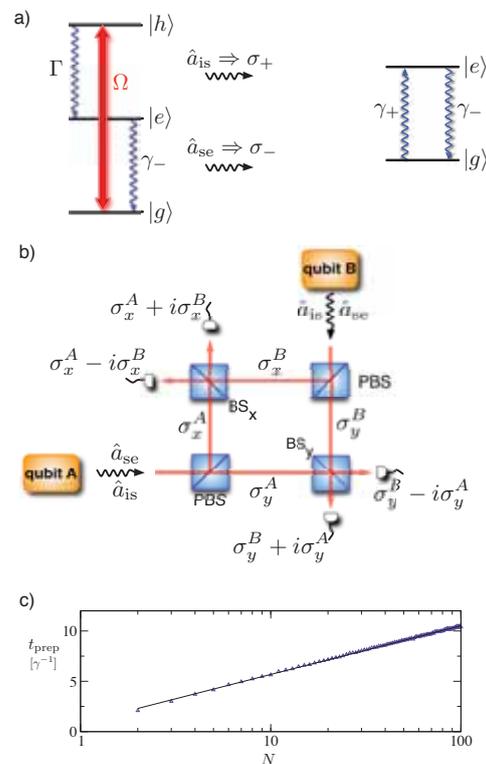
Figure 1: a) Level scheme for decay and excitation processes. b) Detection scheme for generating entangling jumps. c) Time taken to build N qubit cluster states.

References

[1] M. F. Santos, M. Terra Cunha, R. Chaves and A. R. R. Carvalho, to appear in Phys. Rev. Lett. (2012).

[2] A. R. R. Carvalho and M. F. Santos, New J. Phys., **13**, 013010 (2011).

Informational power of quantum measurements

Michele Dall'Arno[1,2], **Giacomo Mauro D'Ariano**[2] **and Massimiliano F. Sacchi**[2,3]

[1]*ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, E-08860 Castelldefels (Barcelona), Spain*
[2]*Quit group, Dipartimento di Fisica "A. Volta", via A. Bassi 6, I-27100 Pavia, Italy*
[3]*Istituto di Fotonica e Nanotecnologie (INF-CNR), Piazza Leonardo da Vinci 32, I-20133, Milano, Italy*

The information stored in a quantum system is accessible only through a quantum measurement, and the postulates of quantum theory severely limit what a measurement can achieve. The problem of evaluating how much informative a measurement is has obvious practical relevance in several contexts, such as the communication of classical information over noisy quantum channels and the storage and retrieval of information from quantum memories. When addressing such problem, one can consider two different figures of merit: the probability of correct detection [1] (in a discrimination scenario) and the mutual information (in a communication scenario). The latter case is the aim of this contribution. We introduce [2] the *informational power* $W(\Pi)$ of a POVM Π as the maximum over all possible ensembles of states R of the mutual information between Π and R, namely

$$W(\Pi) = \max_R I(R, \Pi). \tag{1}$$

We prove [2] the additivity of the informational power. Given a channel Φ from an Hilbert space $\mathcal{H}$ to an Hilbert space $\mathcal{K}$, the *single-use channel capacity* is given by $C_1(\Phi) := \sup_R \sup_\Lambda I(\Phi(R), \Lambda)$, where the suprema are taken over all ensembles R in $\mathcal{H}$ and over all POVMs Λ on $\mathcal{K}$. A *quantum-classical channel* (q-c channel) Φ_Π (see [3]) is defined as $\Phi_\Pi(\rho) := \sum_j Tr[\rho \Pi_j]|j\rangle\langle j|$, where $\Pi = \{\Pi_j\}$ is a POVM and $|j\rangle$ is an orthonormal basis. We prove [2] that the informational power of a POVM Π is equal to the single-use capacity $C_1(\Phi_\Pi)$ of the q-c channel Φ_Π, i. e.

$$W(\Pi) = C_1(\Phi_\Pi). \tag{2}$$

The additivity of the informational power follows from the additivity of the single-use capacity of q-c channels.

We recast [2] the maximization of the informational power of a POVM to the maximization of the accessible information of a suitable ensemble. According to [4], the *accessible information* $A(R)$ of an ensemble $R = \{p_i, \rho_i\}$ is the maximum over all possible POVMs Π of the mutual information between R and Π, namely $A(R) = \max_\Pi I(R, \Pi)$. Given an ensemble $S = \{q_i, \sigma_i\}$, we define the POVM $\Pi(S)$ as $\Pi(S) := \left\{ q_i \sigma_S^{-1/2} \sigma_i \sigma_S^{-1/2} \right\}$. Given a POVM $\Lambda = \{\Lambda_j\}$ and a density matrix σ, we define the ensemble $R(\Lambda, \sigma)$ as $R(\Lambda, \sigma) := \left\{ Tr[\sigma \Lambda_j], \frac{\sigma^{1/2}\Lambda_j\sigma^{1/2}}{Tr[\sigma\Lambda_j]} \right\}$. We prove [2] that the informational power of a POVM $\Lambda = \{\Lambda_j\}$ is given by

$$W(\Lambda) = \max_\sigma A(R(\Lambda, \sigma)). \tag{3}$$

The ensemble $S^* = \{q_i^*, \sigma_i^*\}$ is maximally informative for the POVM Λ if and only if $\sigma_{S^*} = \arg\max_\sigma A(R(\Lambda, \sigma))$ and the POVM $\Pi(S^*)$ is maximally informative for the ensemble $R(\Lambda, \sigma_{S^*})$, as illustrated in the following commuting diagram. From this results it follows that for any given

$$
\begin{array}{ccc}
\Lambda & \xrightarrow{\sigma_{S^*}} & R(\Lambda, \sigma_{S^*}) \\
\downarrow & & \downarrow \\
S^* & \xleftarrow{\sigma_{S^*}} & \Pi(S^*)
\end{array}
$$

D-dimensional POVM there exists a maximally informative ensemble of M pure states, with $D \leq M \leq D^2$, a result similar to Davies theorem for accessible information [5]. For POVMs with real matrix elements [6], the above bound can be strengthened to $D \leq M \leq D(D+1)/2$.

We consider [2] some relevant examples. We prove that given a D-dimensional POVM $\Pi = \{\Pi_j\}_{j=1}^N$ with commuting elements, there exists a maximally informative ensemble $V = \{p_i^*, |i\rangle\}_{i=1}^M$ of $M \leq D$ states, where $|i\rangle$ denotes the common orthonormal eigenvectors of Π, and the prior probabilities p_i^* maximize the mutual information. We show how this results applies to the problem of the purification of noisy quantum measurements [7]. For some class of 2-dimensional and group-covariant POVM (namely, real-symmetric [6], mirror-symmetric, and SIC POVMs), we provide an explicit form for a maximally informative ensemble which enjoys the same symmetry. Finally, for any POVM we provide an iterative algorithm which is effective in finding a maximally informative ensemble.

The results we present have obvious relevance in the theory of quantum communication and measurement, and interesting related works [8, 9] recently appeared. In particular, in [8] Holevo extends the results we present to the relevant infinite dimensional case.

References

[1] N. Elron and Y. C. Eldar, IEEE Trans. Inf. Theory **53**, 1900 (2007).

[2] M. Dall'Arno, G. M. D'Ariano, and M. F. Sacchi, Phys. Rev. A **83**, 062304 (2011).

[3] A. S. Holevo, Russ. Math. Surv. **53**, 1295 (1998).

[4] A. S. Holevo, J. Multivariate Anal. **3**, 337 (1973).

[5] E. B. Davies, IEEE Trans. Inf. Theory **24**, 596 (1978).

[6] M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki, and O. Hirota, Phys. Rev. A **59**, 3325 (1999).

[7] M. Dall'Arno, G. M. D'Ariano, and M. F. Sacchi, Phys. Rev. A **82**, 042315 (2010).

[8] A. S. Holevo, arxiv:quant-ph/1103.2615.

[9] O. Oreshkov, J. Calsamiglia, R. Munoz-Tapia, and E. Bagan, New J. Phys. **13**, 073032 (2011).

Complete set of operational measures for the characterization of three–qubit entanglement

Julio I. de Vicente, **Tatjana Carle**, **Clemens Streitberger and Barbara Kraus**

Institut für Teoretische Physik, Universität Innsbruck, Austria

Entanglement is at the core of many of the applications of quantum information theory and quantum computation and plays a key role in the foundations of quantum mechanics. Therefore, a great amount of theoretical effort has been performed in recent years to grasp this phenomenon, in particular regarding its characterization and quantification as well as its convertibility properties [1]. Whereas bipartite entanglement is well understood, multipartite entanglement is much more subtle. In fact, our understanding of the nonlocal properties of many-body states is far from complete even in the simplest case of just three subsystems. Our knowledge of bipartite entanglement stems from the fact that in the asymptotic limit of many copies of any given state, there is a unique optimal rate at which it can be *reversibly* transformed into the maximally entangled state [2]. However, such an approach seems formidable in the multipartite regime [3].

A fundamental property of entanglement is that it is invariant under local unitary (LU) operations. This has led to the study of complete sets of (polynomial) invariants under this kind of operations [4] and the necessary and sufficient conditions for LU–equivalence have recently been provided [5]. However, a complete classification of LU classes with operationally meaningful measures was still lacking. In this contribution we solve this problem for the simplest nontrivial multipartite case: three qubits. That is, we provide a complete set of operational entanglement measures which characterize uniquely all 3–qubit states with the same entanglement properties [6].

To this end, we derive a new decomposition (up to LU operations) for arbitrary 3–qubit states which is characterized by five parameters. We show that these parameters are uniquely determined by bipartite entanglement measures. These quantities, which are easily computable, characterize the different forms of bipartite entanglement required to generate the state following a particular preparation procedure and, hence, have a clear physical meaning. Moreover, we show that the classification of states obtained in this way is strongly related to the one obtained when considering general local operations and classical communication, showing further the phisicality of this approach.

Our results provide a physical classification of pure multipartite entanglement and, hopefully, will pave the way for new applications of many-body states in the light of quantum information theory.

References

[1] M.B. Plenio and S. Virmani, Quantum Inf. Comput. **7**, 1 (2007); R. Horodecki *et al.*, Rev. Mod. Phys. **81**, 865 (2009).

[2] C.H. Bennett *et al.*, Phys. Rev. A **53**, 2046 (1996).

[3] C.H. Bennett *et al.*, Phys. Rev. A **63**, 012307 (2000).

[4] M. Grassl, M. Rotteler, and T. Beth, Phys. Rev. A **58**, 1833 (1998).

[5] B. Kraus, Phys. Rev. Lett. **104**, 020504 (2010); Phys. Rev. A **82**, 032121 (2010).

[6] J.I. de Vicente, T. Carle, C. Streitberger, and B. Kraus, Phys. Rev. Lett. **108**, 060501 (2012).

Universality in Topological quantum computing without the Dual space.

Simon. J. Devitt[1] **Alexandru. Paler**[2]**, Ilia. Polian**[2]**, and Kae Nemoto**[1]
[1]*National Institute for Informatics, 2-1-2, Hitotsubashi, Chiyoda-ku, Tokyo, Japan*
[2]*Department of Informatics and Mathematics, University of Passau, Innstr. 43, Passau, Germany*

Topological quantum codes have proven themselves to be arguably the most versatile for protecting quantum computers from the inevitable effect of coherent and incoherent errors. Not only do they exhibit one of the highest fault-tolerant thresholds known, but their local construction makes them amenable to realistic quantum computing architectures [1, 2]. The two most predominant topological codes used in large scale quantum architectures are the surface code [3] and its cluster state generalisation, commonly referred to as the Raussendorf code [4]. Universal computation with these models is achieved by encoding information into topologically protected degrees of freedom, known as defects, within a large entangled lattice of physical qubits. Quantum operations are then performed via the movement of such defects around each other, known as braiding.

The entangled state that defines the effective Hilbert space of the encoded space gives rise to two, interlaced lattices that are dual to each other (referred to as the primal and dual lattices). Qubit defects can be defined with respect to either of these lattices and valid braiding operations performed between two defects of *opposite type*. A large array of logic gates are therefore an interlaced network of braiding operations consisting of defect qubits of both types.

In this presentation we will illustrate how logic operations can be reformulated such that they can be performed directly between two defect qubits of the *same* type. This allows us to perform logical gates between qubits with only a single type of defect, giving rise to universality within the topological model *without* utilising both the primal and dual spaces. This reformulation replaces logical braiding of opposite type defects with logical junctions with the same type of defect and expanding the phenomenology to include more complicated circuit constructions with simple defect junctions.

Figure 1: Junction Identity from Ref. [4]. A closed Dual braid is contracted, forming a junction encaged by a Dual defect. The circuit equivalence is met by ensuring that the same correlation surfaces are supported.

The basic identity that gives rise to this result arises from the original junction rules of Raussendorf, Harrington and Goyal [4]. These junction rules allow braiding circuits to be rewritten as junctions. Illustrated in Fig. 1 is the defect configuration introduced by Raussendorf *et. al.* where a closed dual defect braiding with three pairs of primal defects is replaced by a junction of three primal defect pairs and a dual *cage* enclosing the junction. Given this general rule we can rewrite the structure of the braided CNOT gate [Fig. 2]. we have in each step utilised the numbered rules from the original work of Raussendorf *et. al.*. By inserting effective identity
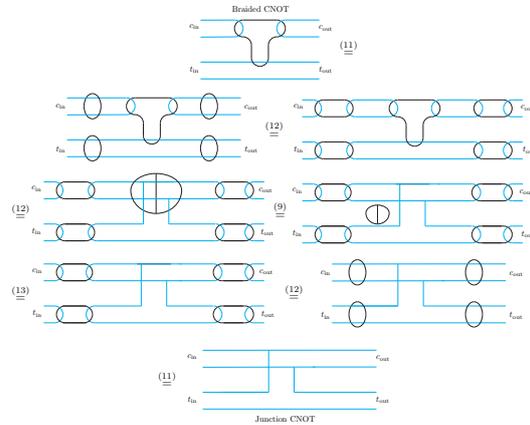
Figure 2: Braiding identities to convert a standard two-qubit CNOT gate into a junction. The respective moves are indicated and identical to the rules shown in Ref. [4]

operations on the target and control qubits, the dual cage that is formed when the CNOT is contracted into a junction can be removed completely. Reversing the identity operations leads to a junction based CNOT gate that *does not require any dual defects.*

Universality in the topological model comes about via the injection, distillation and teleportation of ancillary states for $R_z(\pi/4)$, $R_x(\pi/4)$ and $R_z(\pi/8)$ rotations on a logically encoded qubit (which are constructed via CNOT gates). These gates + the CNOT are sufficient for universality via the Solovay-Kitaev theorem. Consequently, universality is achieved without the need to utilise the dual space. Given this new construction, other useful circuit structures can be derived. This includes standard circuit identities and single and multi-qubit measurements in either the X or Z basis.

An additional benefit to achieving universality via defect junctions is that, in principle, two quantum computers are available for the price of one. As computation can be restricted exclusively to the primal space of the lattice, the Dual space is essentially empty. Therefore, an independent quantum circuit could be realised within the dual space using similar junction circuits.

References

[1] S. J. Devitt *et. al.*, New. J. Phys, **11**, 083032 (2009)

[2] N. Cody Jones *et. al.* arXiv:1010.5022 (2010).

[3] A.G. Folwer, A.M. Stephens and P. Groszkowsi, Phys. Rev. A. **80**, 052312 (2009).

[4] R. Raussendorf, J. Harrington and K. Goyal, New. J. Phys., **9**, 199 (2007).

Classical compilers for gate optimisation in fault-tolerant quantum computing.

Alexandru Paler[2], **Simon J. Devitt**[1], **Kae Nemoto**[1] and **Ilia Polian**[2]

[1]*National Institute for Informatics, 2-1-2, Hitotsubashi, Chiyoda-ku, Tokyo, Japan*
[2]*Department of Informatics and Mathematics, University of Passau, Innstr. 43, Passau, Germany*

The recent development of viable architectural designs for large scale quantum computing and the continued increase in precision reported by experimental groups suggests that large scale quantum information processing may soon become a reality. Advanced topological techniques for fault-tolerant universal computation have raised the threshold (the physical error rate at which error correction becomes effective) to a level comensurate with some of the most advanced experimental systems. Given the possibility that large scale qubit arrays could be built in the near future, the time has come to address the *classical* programming requirements of a quantum computer.

Some work has already been reported in this area [1, 2], focusing on the ability to efficiently and quickly perform error decoding within the topological error corrected model. Additional work has also occurred examining circuit optimisation for large quantum algorithms [3, 4]. However, a significant issue with these latter studies is that they focus on the optimisation of algorithms at the *logical* level (i.e. it is implicitly assumed that each logical gate in the representation is a valid fault-tolerant, error corrected, operation on some physical hardware). The primary purpose of a quantum computer is to perform error correction, actual computation represents a very small percentage of the active operations and the construction of fault-tolerant gates commonly requires resource intensive protocols such as state distillation, the Solovay-Kitaev algorithm and qubit transport.

The purpose of this presentation is to illustrate the framework for a *classical* programming model that is designed to decompose a large quantum algorithm into an appropriate set of valid encoded operations and to optimise the resources required to implement the algorithm of a physical computer. The model of computation that we focus on is those based on topological closes (specifically the surface code and the Raussendorf lattice [5]). Illustrated in Fig. 1 is an example of a small quantum circuit used to distill the encoded state $|0\rangle + i|1\rangle$ which is required to fault-tolerantly achieve $R_{x,z}(\pi/4)$ rotations. Each qubit in the topological model is defined via a pair of holes (or defects) in a large entangled lattice of physical qubits. Logic operations are achieved via the movement of these defects around each other (known as braiding). In terms of the physical resources required, the quantum hardware is designed to simply produce the large entangled state in which these operations occur. Hence resource requirements, in terms of total number of devices in the quantum hardware and the time required to execute an algorithm (which indirectly relates to the operational accuracy of the physical hardware), are directly related to how a given quantum circuit is converted and compacted into this series of braids. Even for only a small number of logic gates, the braiding sequences can be very large and ideally every part of the physical cluster should be occupied with a qubit defect such that resources are not wasted.
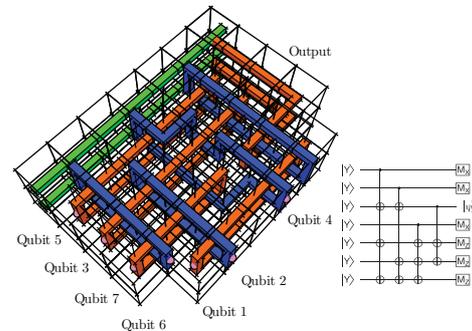
Figure 1: A representation of the state distillation and injection circuit in terms of braiding operations in the topological model. The efficiency of how braids are compactly constructed ultimately determines the spatial and temporal resources required by the quantum hardware. The goal of a classical compiler is to convert the quantum circuit *at the logical level* into this type of braiding sequence, constructed from valid fault-tolerant primitives. Even for a comparatively small algorithm, the total braiding representation is enormous.

The goal of the classical compiler is to determine a compact sequence of braiding movements that faithfully represent the quantum algorithm at the *logical* level, incorporating all valid circuit decompositions necessary to construct gates from the valid fault-tolerant primitives.

We will introduce the formalism necessary to represent a large braiding sequence, the general rules that lead to compactification of the computation and how both circuit identities and braiding identities are incorporated to optimise braiding. Finally we will present a comparison of several designs for state distillation circuits (which ultimately comprise the majority of operations within a large computation) which have been determined from the compiler and designed by hand.

References

[1] S. J. Devitt *et. al.*, I.J.Q.I. **8**:1-27 (2010).

[2] A.G. Fowler, A.C. Whiteside and L.C.L. Hollenberg, arXiv:1110.5133 (2011).

[3] M. Nielsen, M. Dowling, M. Gu, and A. Doherty, Science. **311**, 1133 (2006).

[4] V.V. Shende, S.S. Bullock, and I.L. Markov, Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, **25**, 1000-1010, (2006)

[5] R. Raussendorf, J. Harrington and K. Goyal, New. J. Phys., **9**, 199 (2007).

Fault-tolerant quantum computation and communication on a distributed 2D array of small local systems

Kieuske Fujii[1]**, Takashi Yamamoto**[1]**, Masato Koashi**[2] **and Nobuyuki Imoto**[1]

[1]*Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2]*Photon Science Center, The University of Tokyo, 2-11-16 Yayoi, Bunkyo-ku, Tokyo 113-8656, Japan*

In order to demonstrate advantages of quantum computation over classical computation, practically scalable architecture design is essential. Quantum fault-tolerance theory ensures scalable quantum computation with noisy quantum devices as long as the error probability of such devices is smaller than a threshold value (see Ref. [1] and references therein). The noise thresholds have been calculated to be about a few % for several fault-tolerant schemes under various assumptions [2, 3, 4]. However, the existing fault-tolerant schemes require many qubits live together in a single system and assume that the whole system can be controlled with the same accuracy regardless of its size. In experiment, however, the number of qubits in a single system is rather limited; if we increase the number of qubits in a single system, the control becomes more and more complex, which makes it hard to achieve the same accuracy.

In order to ensure practical scalability, it is natural to consider a distributed situation, where local systems with a small number of qubits are connected by quantum channels [5]. In this context, it has been reported that if the local system consists of only a single qubit, the tolerable rate of error in the quantum channel (or remote entangling operation) have to be as small as 0.01% [6, 7], although the success probability of the channel can be very small ~ 0.1. Then, a natural question is what happens if there are additional qubits in the local system. Here, we answer this question. We propose a distributed architecture for practically scalable quantum computation on a two-dimensional (2D) array of small local systems [8]. The local systems consist of only four qubits and connected with their nearest neighbors in 2D by quantum channels as depicted in Fig. 1. We show that the proposed architecture works well even with a gate error rate $\sim 0.1\%$. Furthermore, the quantum channel can be extensively noisy; the tolerable error rate is as high as 30% (fidelity 0.7), which are substantially higher than the case with the local system of a single qubit [6, 7]. These results are achieved by utilizing twofold error management techniques: entanglement purification [9] and topological quantum computation (TQC) [3]. The former is employed to implement a reliable two-qubit gate by using very noisy quantum channels with the help of quantum gate teleportation. In particular, we apply high-performance entanglement purification, so-called *double selection scheme* [9], which is essential for achieving the above result. TQC is used to handle the remaining errors and to archive quantum gate operations of arbitrary accuracy, which is required for large-scale quantum computation.

All key ingredients in the present architecture, (i) a four-qubit system, (ii) gate operations in the four-qubit system, and (iii) entangling operations between the separate systems, have already been demonstrated experimentally in various physical systems, such as trapped ions, nitrogen-vacancy centers in di-
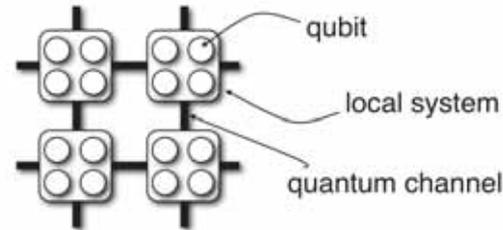
Figure 1: The proposed architecture for distributed quantum computation (see Ref. [8] for details).

amond, and superconducting qubits. In fact, the benchmarks in trapped ion systems are comparable to the requirements of the proposed architecture. We consider possible implementations of the proposed architecture by using trapped ions and nitrogen-vacancy centers in diamond [8]. The proposed scheme is further applied for the distribution of high-quality entanglement for long distance quantum communication on a distributed 2D quantum network.

These results push the realization of large-scale quantum computation and communication within reach of current technology. We believe that this work gives a good guideline and benchmark in the development of devices for quantum information processing.

References

[1] M. A. Nielsen and I. L. Chuang, (Cambridge University Press, 2000).

[2] E. Knill, Nature (London) **434**, 39 (2005).

[3] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007); R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).

[4] K. Fujii and K. Yamamoto, Phys. Rev. A **81**, 042324 (2010); Phys. Rev. A **82**, 060301(R) (2010).

[5] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Phys. Rev. A **59**, 4249 (1999).

[6] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, Phys. Rev. Lett. **105**, 250502 (2010).

[7] K. Fujii and Y. Tokunaga, Phys. Rev. Lett. **105**, 250503 (2010).

[8] K. Fujii, T. Yamamoto, M. Koashi, and N. Imoto, arXiv:1202.6588.

[9] K. Fujii and K. Yamamoto, Phys. Rev. A **80**, 042308 (2009).

Explorations in the efficiency of quantum factoring

__Omar Gamel__[1] and __Daniel F. V. James__[1]

[1]*Department of Physics and Center for Quantum Information and Quantum Control, University of Toronto, Toronto, Canada*

Shor's factoring algorithm [1] is held as one of the most promising and useful applications of quantum computing. It allows one to factor large numbers in polynomial time, undermining the most common cryptographic schemes in use today, such as RSA cryptography. The well known algorithm is based on the quantum fourier transform to find the period of a function, and also makes heavy use of the modular exponentiation operation, given by,

$$U : |a\rangle|0\rangle \rightarrow |a\rangle|x^a (mod N)\rangle, \qquad (1)$$

where N is the number to be factored, and x is a random positive integer coprime with N. The modular exponentiation is the bottleneck of the algorithm, the portion that uses the most time.

The generic algorithm can factorize any N in time order $(\log N)^3$, assuming sufficient memory space for intermediate calculations. Reducing the memory available (as long as it still lies above a certain threshold) increases the time taken by multiplicative factors, keeping its order the same in $\log(N)$.

However, for a given N, or class of N's to factorize, the generic algorithm may be suboptimal, and can be optimized to result in substantial savings in both memory needed and operation time [2, 3]. The different suboperations involved in modular exponentiation can be made more efficient using some known property of N. For example, multiplexed addition, repeated squaring, and multiplication block techniques.

There have also been experimental applications of these optimized algorithms for the simplest of N for which Shor's algorithm is applciable, $N = 15$. Experiments of this kind using a photonic architecture have been demonstrated to include entanglement [4].

We extend this body of work by finding optimization techniques for additional classes of N. In addition, we attempt to create a formula for the correct optimization structure for arbitrary N. We also propose experimental tests of the optimized factorization algorithm.

References

[1] P. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal of Computing 26, pp. 1484-1509 (1997).

[2] D. Beckman, A. Chari, S. Devabhaktuni and J. Preskill, *Efficient Networks for Quantum Factoring*, Phys. Rev. A. 54, 1034-1063 (1996).

[3] I. Markov, M. Saeedi, *Constant-Optimized Quantum Circuits for Modular Multiplication and Exponentiation*, Quantum Information and Computation, 12, 5-6, pp. 0361-0394 (2012)

[4] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, *Experimental Demonstration of a Compiled Version of Shors Algorithm with Quantum Entanglement*, Phys. Rev. Lett. 99, 250505 (2007).

Visibility bound caused by a distinguishable noise particle

Miroslav Gavenda,[1] Lucie Čelechovská,[1] Jan Soubusta,[2] Miloslav Dušek,[1] and Radim Filip[1]

[1]Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic
[2]Joint Laboratory of Optics of Palacký University and Institute of Physics of Academy of Sciences of the Czech Republic,
17. listopadu 50A, 779 07 Olomouc, Czech Republic

We investigate how distinguishability of a "noise" particle degrades interference of a "signal" particle. The signal, represented by an equatorial state of a photonic qubit, is mixed with noise, represented by another photonic qubit, via linear coupling on a beam splitter. The schema of the experiment is shown on figure 1. Signal source feeds the interferometer with single photon. The noise source produces another single photon which couple with source photon on the beam splitter with transmissivity T. As to measure again the single photon visibility at the verification stage we
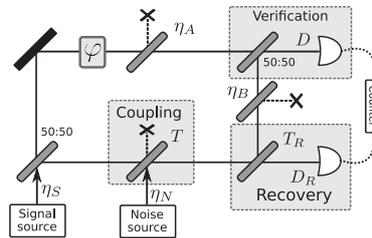
FIG. 1:

detach one photon from the bottom mode of the interferometer. We report on the degradation of the "signal" photon interference depending on the degree of indistinguishability between "signal" and "noise" photon. When the photons are principally completely distinguishable but technically indistinguishable (we are not able to technically measure the difference between distinguishable modes) the visibility drops to the value $1/\sqrt{2}$. As the photons become more indistinguishable the maximal visibility increases and reaches the unit value for completely indistinguishable photons. We have examined this effect experimentally using setup with fiber optics two-photon Mach-Zehnder interferometer.
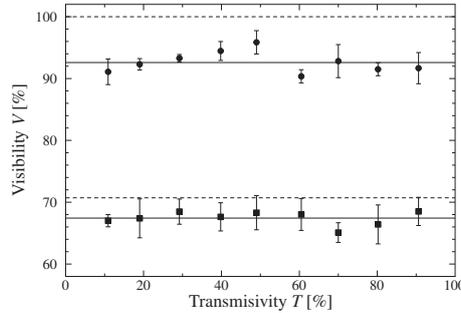
FIG. 2:

On the figure 2 are plotted measured visibilities for distinguishable and indistinguishable scenario dependent on the transmissivity T of the beam splitter (coupling strength). The visibilities are independent on T and the maximal visibility for distinguishable scenario reaches the value of $1/\sqrt{2}$. Main results were published in [1].

[1] M. Gavenda, L. Čelechovská, J. Soubusta, M. Dušek, and R. Filip, Phys. Rev. A **83**, 042320 (2011)

Calibration-robust entanglement detection beyond Bell inequalities

Oleg Gittsovich[1] and Tobias Moroder[2,3]

[1] *Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, N2L 3G1 Waterloo, Ontario, Canada*
[2] *Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Strasse 3, 57068 Siegen, Germany*
[3] *Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Technikerstrae 21A, A-6020 Innsbruck, Austria*

Entanglement verification represents one of the most important tools in quantum information. Besides its mere application in source or device testing it is often also a prerequisite sub-protocol in more concrete tasks like quantum key distribution [1] or teleportation as examples.

In its vast majority entanglement verification is examined either in completely characterized or totally device independent scenario. However, the assumptions imposed by these extreme cases are often either too weak or too strong for real experiments. Thus it is only natural to investigate intermediate scenarios, where only some partial knowledge of the employed devices is required. Besides, this investigation sheds some light on the question, which assumptions are more crucial than the others in entanglement verification. Moreover, the derived entanglement criteria are promised to be more robust against calibration errors, while still keeping a large detection strength, in particular when compared to Bell inequalities.

In this talk we investigate the detection task for the intermediate regime, where partial knowledge of the measured observables is known, and consider cases like orthogonal, sharp or only dimension bounded measurements [2]. We show that for all these assumptions it is not necessary to violate a corresponding Bell inequality in order to detect entanglement. The derived detection criteria can be directly evaluated for experimental data, and are even capable of detecting entanglement from bound entanglement states under the sole assumption of only dimension bounded measurements, or detecting the complete family of entangled two-qubit Werner states with already three dichotomic measurement settings per side under the same assumption.

In addition, we show by explicit examples that the above listed properties of orthogonality and sharpness are mutually exclusive, *i.e.*, there are cases for which the extra knowledge of the sharpness of observables is redundant if their orthogonality is already assumed and vice versa. Moreover we provide examples, where the extra knowledge of sharp and orthogonal measurements is irrelevant for the detection strength and already a dimension restriction suffices to verify exactly the same amount of entanglement. We demonstrate that the case of dimension bounded measurements bears a non-convex problem structure, which must be exploited.

An example of the strength of our detection criteria is shown in Fig. 1. Here we assume that the observed data can be written as

$$P(i,j|k,l) = \frac{1}{4}\left(1 + ijC_{kl}\right) \tag{1}$$

with dichotomic outcomes $i, j \in \pm 1$, two possible measurement settings per side $k, l \in 1, 2$, and C being the correlation matrix of these data characterized only by its two singular
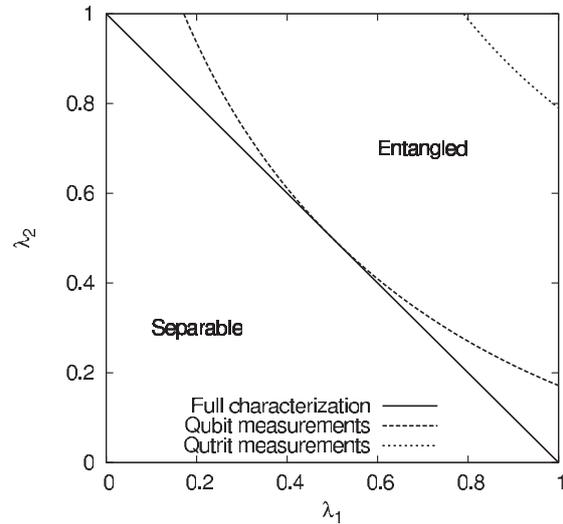
Figure 1: Different detection regions for observations given by Eq. 1 for different knowledge on the performed measurements. Full characterization stands for sharp, orthogonal qubit measurements. Let us point out that device independent verification is not possible.

values λ_1, λ_2.

Finally, we discuss the application of these results to quantum key distribution and prove that for an entanglement based BB84 protocol the familiar one-way key rate [3] is given by

$$R \geq 1 - 2h_2(e) \tag{2}$$

with h_2 being the binary entropy and e the symmetric bit error rate holds already if one of the parties is measuring a qubit; the additional knowledge that this party is measuring in two mutually unbiased basis, like σ_X and σ_Z, or even that the measurements are pure projectors, is not needed to ensure this rate.

References

[1] M. Curty, M. Lewenstein, N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[2] T. Moroder and O. Gittsovich, Phys. Rev. A **85**, 032301 (2012).

[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

Quantum limit to capacity and structured receivers for optical reading

Saikat Guha[1], **Ranjith Nair**[2], **Brent J. Yen**[2], **Zachary Dutton**[1] and **Jeffrey H. Shapiro**[3]

[1]*Disruptive Information Processing Technologies Group, Raytheon BBN Technologies, Cambridge, MA, United States*
[2]*National University of Singapore, Singapore*
[3]*Massachusetts Institute of Technology, Cambridge, MA, United States*

If our DVD disks and drives had no constraint on how the disks encode information (via some combination of amplitude and phase modulation of the probe light), and no constraints on the quantum states of light and receiver measurements that the drives could implement, what is the best achievable efficiency with which data could be read optically?

A K-mode transmitter sends N_S mean photons towards each memory pixel (see Fig. 1). Each pixel is effectively a beamsplitter, $\hat{a}_R^{(m,k)} = \sqrt{\eta_m} e^{j\theta_m} \hat{a}_S^{(m,k)} + \sqrt{1-\eta_m} \hat{a}_E^{(m,k)}$, with $\sum_{k=1}^{K} \langle \hat{a}_S^{(m,k)\dagger} \hat{a}_S^{(m,k)} \rangle \leq N_S$, with the environment modes $\hat{a}_E^{(m,k)}$ in vacuum states. With, (a) an optimal choice of probe (including entangled states), (b) an optimal modulation format for the pixels, (c) an optimal codebook, and (d) an optimal receiver (including joint-detection receivers that make a collective measurement on reflection from multiple pixels), how may bits $C(N_S)$ can be reliably read per pixel?
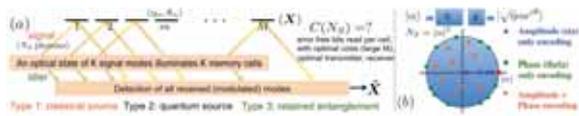
Figure 1: Memory pixels that encode classical information by modulating amplitude and/or phase of an optical probe.

We classify all optical transmitters into three *types*. Type 1 is a classical transmitter—either a coherent state or a mixture thereof. Types 2 and 3 are non-classical states. But, Type 3 retains idler modes $\hat{a}_I^{(m)}$ at the transmitter, entangled with the signal modes $\hat{a}_S^{(m)}$. We consider the case of $K = 1$, i.e., a single-mode probe state. In this case, the return modes from the M pixels can be looked upon as a codeword (spatial $\leftrightarrow$ temporal modes), and from the converse of the Holevo capacity theorem from Ref. [1], for Type 1 and Type 2 probes, we have, $C(N_S) \leq g(N_S)$ bits/pixel, where $g(x) = (1+x)\log(1+x) - x\log x$. However, reading is more constrained than communication, since, (a) the reading transmitter has less encoding/modulation control, and (b) the photon efficiency of reading is more constrained for amplitude modulation formats, since a modulated symbol with $\eta_m N_S$ photons consumes N_S transmitted photons (even for a lossless return-path channel—which we assume throughout in order to focus on the fundamental aspects of the problem).

We show that there is no fundamental upper limit to the number of information bits that could be read reliably per probe photon! However, using a noiseless coherent-state probe, an *on-off* amplitude-modulation pixel encoding, and signal-shot-noise-limited direct detection at the receiver (a *very* optimistic model for CD/DVD technology), the highest photon information efficiency (PIE) achievable is about 0.5 bit per transmitted photon. This is unlike optical communication, where on-off-keyed signaling and direct detection
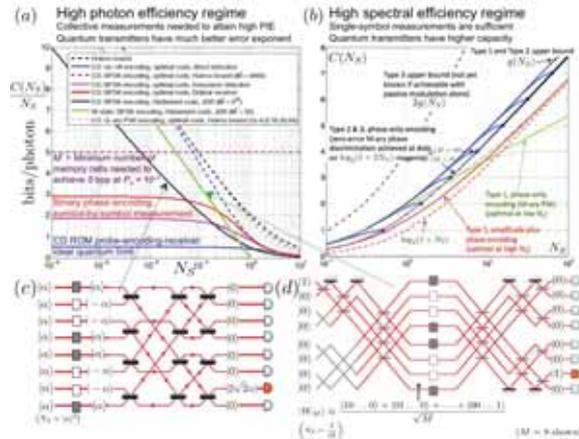
Figure 2: Photon efficiency and capacity of reading: Holevo and Shannon bounds for quantum and classical transceivers.

can attain unlimited PIE [2]. We then show that a coherent-state probe *can* read unlimited bits per photon, when, (a) the receiver is allowed to make joint (collective) measurements on the reflected light from a large block of pixels, and (b) phase modulation is allowed. We show that unlike in communication [1], coherent states cannot attain the Holevo bound. They come close in the high PIE ($N_S \ll 1$) regime, but there is a significant gap in the high capacity ($N_S \gg 1$) regime, even when both amplitude and phase modulation are allowed. We show examples of a Type 2 and a Type 3 (two-mode squeezed-vacuum) transmitter that *can* attain $C(N_S) = g(N_S)$ bits/pixel exactly, with a phase-only modulation. A sequential decoding receiver that uses beamsplitters, phase-sensitive amplifiers, phase plates, and a nondestructive *vacuum or not* measurement can achieve this capacity [3]. Finally, we construct a spatially-entangled (Type 2) probe, which can read unlimited number of error-free bits using a single photon prepared in a uniform superposition of multiple spatial locations, the so called *W-state*. The code, target and joint-detection receiver complexity required by a coherent state transmitter to achieve comparable photon efficiency is *much* higher than that of the W-state transceiver.

References

[1] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).

[2] S. Guha, Z. Dutton, J. H. Shapiro, arXiv:1102.1963v1 [quant-ph], ISIT (2011).

[3] S. Guha, S.-H. Tan, M. Wilde, arXiv:1202.0518v1 [quant-ph], *submitted to* ISIT (2012).

[4] S. Pirandola, *et al.*, New J. Phys. 13, 113012 (2011).

Characterizing multiparticle quantum correlations via exponential families

Otfried Gühne[1], **Sönke Niekamp**[1], and **Tobias Galla**[2]

[1]*Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Str. 3, D-57068 Siegen, Germany*
[2]*Complex Systems and Statistical Physics Group, School of Physics and Astronomy, University of Manchester, Manchester M13 9PL, United Kingdom*

Correlations between different parts of a physical system are ubiquitous in nature. The characterization of these correlations is important not only in quantum information theory, but also in other fields in physics, such as condensed matter theory or in the analysis of nonlinear dynamics and chaos.

For classical complex systems consisting of interacting particles an approach to characterize complexity with the help of exponential families has been developed [1, 2, 3]. For that, one considers a dynamical system composed of N particles each of which can be observed to be in one of two different states, referred to as 0 and 1. At any given time the state $\omega = (\sigma_1, \dots, \sigma_N)$ of the system is therefore found to be an element of $\Omega = \{0, 1\}^N$. Time averaging of the dynamics leads then to a stationary distribution $P(\cdot)$ of the system as a probability distribution over Ω.

Given such a distribution, $P(\cdot)$, one can ask whether or not it is the thermal state of a Hamiltonian with k-particle interactions only, i.e., whether one can write

$$P(\omega) = \frac{1}{Z} \exp[H^{(k)}(\omega)] \qquad (1)$$

where $H^{(k)}(\omega)$ is a Hamiltonian containing only j-particle terms with $j = 1, \dots, k$, and where Z is a constant ensuring normalisation. The set of all probability distributions of this type is called the exponential family $\mathcal{E}_k$.

If this is not the case, one can then use the distance D_k, quantified by the relative entropy from the set of all distributions generated by k-particle interactions as a measure of complexity of $P(\cdot)$. That is, one defines

$$D_k(P) := \inf_{Q \in \mathcal{E}_k} D(P||Q), \qquad (2)$$

where $D(P||Q)$ is the relative entropy or Kullback-Leibler distance

$$D(P||Q) = \sum_{\omega \in \Omega} P(\omega) \log_2 \frac{P(\omega)}{Q(\omega)}. \qquad (3)$$

This correlation measure has been used to investigate the behaviour of coupled iterated maps or cellular automata [2, 3]. Here, it is important to note that there are efficient numerical procedures to compute the optimum in Eq. (2).

For the quantum case, the same question can be asked: Given a multiparticle density matrix ϱ, can it be written as a thermal state of a k-particle Hamiltonian? And if not, how large is the distance to the closest state in the corresponding exponential family, now denoted by $\mathcal{Q}_k$? In Refs. [4, 5] some properties of the closest state and the resulting correlation measure have been derived.

In our contribution, we will first present a simple algorithm to compute the closest state in $\mathcal{Q}_k$. We will compare it with other algorithms which can in principle be used for this optimization and demonstrate that our approach leads to better results in most of the relevant cases.

Then, we will proceed and investigate the convex hull of the exponential family $\mathcal{Q}_k$. The set of all thermal states of one-particle Hamiltonians $\mathcal{Q}_1$ is the set of the states of the form

$$\varrho = \varrho_1 \otimes \varrho_2 \otimes \cdots \otimes \varrho_N, \qquad (4)$$

hence the convex hull equals set of all fully separable states, and a state which is not fully separable is called entangled. This notion is well studied in quantum information theory. In this sense, the investigation of the convex hulls of *all* $\mathcal{Q}_k$ leads to a natural generalization of the notion of multiparticle entanglement.

We will mainly investigate graph states, a family of multi-qubit states, which are of eminent importance for measurement-based quantum computation and quantum error correction. We will prove that no graph state is within $\mathcal{Q}_2$ or its convex hull. We will also present rigorous estimates on the fidelity of a graph state for states from $\mathcal{Q}_2$. It is well known that most graph states cannot be ground states of two-body Hamiltonians [6, 7], but our formalism allows to compute bounds on how well these states can be approximated by thermal states of two-body Hamiltonians. Moreover, our results lead to criteria which can be used experimentally to prove that a prepared state requires more than k-particle interactions for its generation.

References

[1] S. Amari, IEEE Trans. Inf. Theory **47**, 1701 (2001).

[2] T. Kahle, E. Olbrich, J. Jost, and N. Ay, Phys. Rev. E **79**, 026201 (2009).

[3] T. Galla and O. Gühne, Phys. Rev. E (in press), arXiv:1107.1180.

[4] D. L. Zhou, Phys. Rev. Lett. **101**, 180505 (2008).

[5] D. L. Zhou, Phys. Rev. A **80**, 022113 (2009).

[6] M. Van den Nest, K. Luttmer, W. Dür, and H. J. Briegel, Phys. Rev. A **77**, 012301 (2008).

[7] P. Facchi, G. Florio, S. Pascazio, and F.V. Pepe, Phys. Rev. Lett. **107** 260502 (2011).

Long-lived ion qubits in a microfabricated trap for scalable quantum computation

So-Young Baek, Emily Mount, Rachel Noek, Stephen Crain, Daniel Gaultney, Andre van Rynbach, Peter Maunz, and Jungsang Kim

Duke University, Durham, North Carolina, United States

Manipulation of atomic qubits in a chain of trapped ions utilizing Coulomb interaction among them is a promising way to construct a modest-size quantum register [1]. Quantum logic gates can be performed between two remote ions using entanglement generated via exchange of photons [2], which leads to the possibility of connecting two remote chains together to form a larger quantum information processor. These two physical mechanisms can be used to realize a quantum computer architecture where multiple ion chains are interconnected through a reconfigurable all-optical network [3].

Practical implementation of this architecture starts with a means to fabricate and operate the ion traps in a scalable way. Silicon microfabrication techniques can be applied to the design and batch fabrication of complex ion trap structures [4, 5]. In this work, we trap individual $^{171}Yb^+$ ions and demonstrate fundamental quantum information processing protocols in a microfabricated surface trap fabricated by Sandia National Laboratories. Figure 1 (a) shows a single Yb^+ ion trapped in the Sandia Thunderbird surface trap, which is a linear trap with a long open slot etched in the silicon substrate. The trapping fields are formed by two RF electrodes along the length of the slot, which is further segmented by a number of DC electrodes. The ion is trapped and cooled using a diode laser near 370nm, and optically pumped into the hyperfine ground state $|0\rangle$ (Fig. 1b). A single-qubit rotation can be induced either by a microwave field resonant with the qubit separation (hyperfine splitting of 12.6 GHz), or by two coherent optical fields with a frequency separation identical to the hyperfine splitting that drives a Raman transition. Alternatively, the Raman transition can be driven by a frequency comb whose repetition rate is stabilized to an integer fraction of the hyperfine splitting [6]. We use an off-resonant frequency comb generated by a frequency-doubled picosecond Ti:Sapphire pulsed laser to drive single qubit gates in an inherently scalable way. The qubit state can be measured by state-dependent fluorescence, with over 98% fidelity. Figure 1(c) shows the Rabi oscillation of the ion qubit using this method, with π-times of about $3\mu s$. The coherence time of the qubit is measured using Ramsey interferometry, where the qubit state $|0\rangle$ is first put in a coherent superposition state by a $\pi/2$-pulse and then driven into the $|1\rangle$ state with a second $\pi/2$-pulse after a time delay of τ. The fringe contrast of this process as a function of τ can be used to measure the coherence time of the qubit, which is determined to be approximately 600 ms (Fig. 1d).

A complete path to integration must include scalable solutions for both the qubit data path and classical controllers necessary to manipulate them. It is relatively straightforward to trap a chain of ions to expand the number of qubits in the system. Individual addressing of a linear chain of atoms can be achieved in a scalable way using a micro-electromechanical systems (MEMS)-based beam steering system [7], and a linear array of single photon detectors such as photomultiplier tubes can be used to parallelize the state detection process. Efficient optical interfaces for photon-mediated ion entanglement used to interconnect multiple chains can be realized by incorporating optical cavities into the ion trap structures. Integration of these technologies for the control of long-lived qubits in silicon microfabricated traps demonstrated in this work provides a promising platform for realizing scalable quantum information processors.
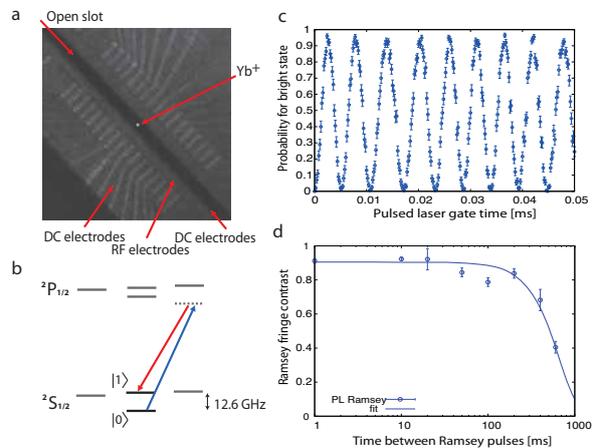
Figure 1: (a) A single Yb^+ ion trapped in the Sandia Thunderbird surface trap. (b) Simplified level scheme for the $^{171}Yb^+$ qubit. (c) Rabi oscillations induced by the repetition-rate stabilized pulsed laser. (d) Coherence time of the qubit ($\sim$600ms) measured using Ramsey interferometry.

References

[1] G.-D. Lin et al., Europhys. Lett. **86**, 60004 (2009).

[2] P. Maunz et al., Phys. Rev. Lett. **102**, 250502 (2009).

[3] J. Kim and C. Kim, Quant Inf. Comput. **9**, 0181 (2009).

[4] D.R. Leibrandt et al., arXiv:0904.2599v2 (2009)

[5] D. T. C. Allcock et al., arXiv:1105.4864 (2011).

[6] D. Hayes et al., Phys. Rev. Lett. **104**, 140501 (2010).

[7] C. Knoernschild et al., Appl. Phys. Lett. **97**, 134101 (2010).

Deterministic generation of non-classical states of light via Rydberg interactions

Erwan Bimbard[1], Jovica Stanojevic[1], Valentina Parigi [1], Rosa Tualle-Brouri[1], Alexei Ourjoumtsev[1] and Philippe Grangier[1]
[1]Laboratoire Charles Fabry, Institut d'Optique, Palaiseau, France

We investigate, both theoretically and experimentally, the deterministic generation of non-classical states of light by using giant non-linearities due to long-range interactions between Rydberg polaritons.

Atomic ensembles play a prominent role in quantum optics. For instance, a quantum state of light can be stored in an ensemble of cold atoms as a polarisation wave involving two long-lived atomic states. If one of these two is a Rydberg state, the evolution of this polariton will be strongly affected by long-range atomic interactions. As a result, a coherent pulse of light stored in the atomic medium should spontaneously turn into a non-classical polaritonic state. This state could be subsequently retrieved as a non-classical pulse of light by using a control laser nearly resonant with a third, short-lived atomic level.

We have theoretically investigated the evolution of a coherent optical pulse stored as Rydberg polaritons, and obtained simple analytical expressions describing this evolution at any time. One simple interesting result is that for long times, the interactions between Rydberg atoms should act as "quantum scissors" on the quantum state, and the retrieved optical pulse should become a coherent superposition of zero and one photon presenting a non-classical, negative Wigner function [1].

In order to observe this negative Wigner function in a homodyne measurement, the optical pulse must be retrieved not only with a high efficiency, but also in a well-defined spatial and temporal mode. We theoretically demonstrated that by using a low-finesse optical cavity and a well-adjusted readout laser pulse these constraints can be simultaneously satisfied [2]. The extraction efficiency as well as the modal purity can approach unity, and the non-classical Wigner function of the prepared state should be observable with realistic experimental parameters.

As a first step in this direction, we are currently experimentally investigating the response of the system shown on figure 1 (a Rydberg gas in a Rubidium cloud trapped inside the mode of an optical cavity) to a classical probe beam [3]. We analyze the transmission of this beam coupled to the lower transition through this system, in order to observe non-linear dispersion of the light induced by Rydberg-Rydberg interactions when the atomic medium is under the influence of a strong coupling beam [4].
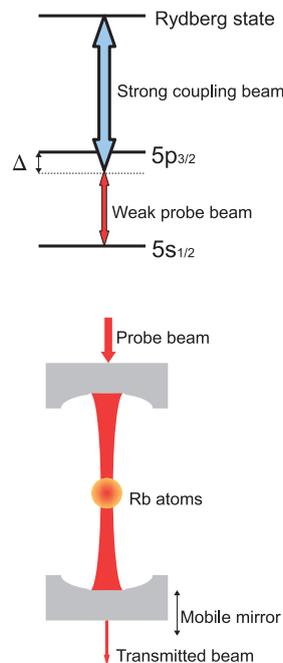
Figure 1: Rubidium level scheme and experimental system.

References

[1] J. Stanojevic, V. Parigi, E. Bimbard, A. Ourjoumtsev, P. Pillet and P. Grangier, preprint.

[2] J. Stanojevic, V. Parigi, E. Bimbard, R. Tualle-Brouri, A. Ourjoumtsev and P. Grangier, Phys. Rev. A **84**, 053830 (2011).

[3] J.D. Pritchard, D. Maxwell, A. Gauguet, K.J. Weatherill, M.P.A. Jones and C. S. Adams, Phys. Rev. Lett. **105**, 193603 (2010).

[4] S. Sevinçli, N. Henkel, C. Ates and T. Pohl, Phys. Rev. Lett. **107**, 153001 (2011).

Two component Bose-Einstein condensates and their applications towards quantum information processing

Tim Byrnes[1]

[1]*National Institute of Informatics, Tokyo, Japan*

In a recent set of experiments, two component BECs were realized on atom chips realizing full single qubit control on the Bloch sphere and spin squeezing [1]. Currently, the primary application for such two component BECs is for quantum metrology and chip based clocks. In this paper we discuss its applications towards quantum computation. Although BECs have been considered for quantum computation in the past, the results have shown to be generally been unfavorable for these purposes due to enhanced decoherence effects due to the large number of bosons N in the BEC. In this work we consider a different encoding of the quantum information, which to a large extent mitigates this problem. We develop the framework for quantum computation using this encoding, illustrated with several quantum algorithms.

Our basic procedure is to encode a standard qubit state $\alpha|0\rangle + \beta|1\rangle$ in the BEC in the state

$$|\alpha, \beta\rangle\rangle \equiv \frac{1}{\sqrt{N!}} \left(\alpha a^\dagger + \beta b^\dagger \right)^N |0\rangle, \quad (1)$$

where α and β are arbitrary complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. The state $|\alpha, \beta\rangle\rangle$ can be manipulated using Schwinger boson operators $S^x = a^\dagger b + b^\dagger a$, $S^y = -ia^\dagger b + ib^\dagger a$, $S^z = a^\dagger a - b^\dagger b$, which satisfy the usual spin commutation relations $[S^i, S^j] = 2i\epsilon_{ijk}S^k$, where ϵ_{ijk} is the Levi-Civita antisymmetric tensor. Despite the widespread belief that for $N \to \infty$ the spins approach classical variables, a two qubit interaction $H_2 = S_1^z S_2^z$ generates genuine entanglement between the bosonic qubits. As a measure of the entanglement, we plot the von Neumann entropy $E = -\text{Tr}(\rho_1 \log_2 \rho_1)$ in Figure 1a. For the standard qubit case ($N = 1$), the entropy reaches its maximal value at $\Omega t = \pi/4$. For the bosonic qubit case there is an initial sharp rise, corresponding to the improvement in speed of the entangling operation.

Such two qubit gates can be implemented via a cavity QED implementation realizing a quantum bus between qubits [2]. Together with one qubit gates, these can be shown to form a universal set of gates to perform an arbitrary quantum computation [2]. To illustrate this, we perform a simulation of Grover's algorithm in the continuous time formulation, which for BECs amounts to executing the Hamiltonian $H_G = N^2 \prod_{n=1}^{M} \frac{1}{2}\left[1 + \frac{S_n^x}{N}\right] + N^2 \prod_{n=1}^{M} \frac{1}{2}\left[1 + \frac{S_n^z}{N}\right]$. The bosonic qubits are prepared in the state $|X\rangle = \prod_{n=1}^{M} |\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\rangle\rangle_n$ and evolved in time by applying H. The system then executes Rabi oscillations between the initial state $|X\rangle$ and the solution state $|ANS\rangle$. The time required for a half period of the oscillation is found to be $t \sim \sqrt{2^M}/N$, which has the same square root scaling with the number of sites, but with a further speedup of N.

Finally, we consider decoherence effects due to the use of BEC qubits. Consider the simplest case when a quantum state

is stored in the system of qubits and no gates are applied, i.e. when the BEC qubits are used to simply store a state. The main channels of decoherence in this case are dephasing which can be modelled via the master equation

$$\frac{d\rho}{dt} = -\frac{\Gamma_z}{2} \sum_{n=1}^{M} [(S_n^z)^2 \rho - 2S_n^z \rho S_n^z + \rho(S_n^z)^2], \quad (2)$$

where Γ_z is the dephasing rate. For a standard qubit register, the information in a general quantum state can be reconstructed by $4^M - 1$ expectation values of $(I_1, S_1^x, S_1^y, S_1^z) \otimes \cdots \otimes (I_M, S_M^x, S_M^y, S_M^z)$. Examining the dephasing of the general correlation $\langle \prod_n S_n^{j(n)} \rangle$ where $j(n) = I, x, y, z$, we obtain the general decay relation $\langle \prod_n S_n^{j(n)} \rangle \propto \exp[-2\Gamma_z K_z t]$. Here K_z is the number of non-commuting $S_n^{j(n)}$ operators with S_n^z (i.e. $j(n) = x, y$), which is independent of N and is at most equal to M. The crucial aspect to note here is that the above equation does not have any N dependence. In fact the equation is identical to that for the standard qubit case ($N = 1$). This shows that for correlations of the form $\langle \prod_n S_n^{j(n)} \rangle$ there is in fact no penalty due to large N, showing that BECs can store quantum states. We also show the effects of decoherence during the execution of Grover's algorithm in Figure 1b. We observe that the fidelity of the algorithm is in fact improved with N, which can be understood as originating from the fast two qubit gate times which completes the gate before decoherence sets in. This work is supported by Navy/SPAWAR Grant N66001-09-1-2024.
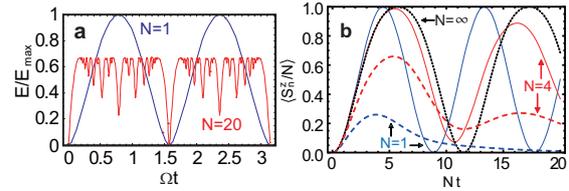
Figure 1: **a** The entanglement normalized to the maximum entanglement ($E_{max} = \log_2(N + 1)$) between two bosonic qubits for the particle numbers as shown. **b** Rabi oscillations executed by the Grover Hamiltonian for $M = 2$ for various boson numbers as shown. The dotted line shows the mean field result corresponding to the $N \to \infty$ limit, while dashed lines include dephasing of $\Gamma_z = 0.2$.

References

[1] P. Böhi *et al.*, Nature Phys. **5**, 592 (2009); M. Riedel *et al.*, Nature **464**, 1170 (2010).

[2] T. Byrnes, K. Wen, Y. Yamamoto, submitted (http://arxiv.org/1103.5512).

Gradient echo memory as a platform for manipulating quantum information

<u>Geoff Campbell</u>[1], Mahdi Hosseini[1], Ben Sparkes[1], Olivier Pinel[1], Tim Ralph[2], Ben Buchler[1] and Ping Koy Lam[1]

[1] *Centre for Quantum Computation and Communication Technology, Department of Quantum Science,*
The Australian National University, Canberra, Australia
[2] *Centre for Quantum Computation and Communication Technology, Department of Physics*
University of Queensland, St Lucia 4072, Australia

One of the key elements in an optical network for transmitting and manipulating quantum information is an optical memory that is capable of storing and recalling, on demand, optical states without significant loss or addition of noise. A candidate technique for the implementation of such a memory is the Λ gradient echo memory (Λ-GEM)[1], which uses an off-resonant Raman transition to couple an optical mode to a long-lived atomic spin coherence in a reversible manner. This technique has been demonstrated to store and recall quantum states of light beyond the quantum and no-cloning limits [2].

Optical quantum networks will also require active and passive linear optics to process the information in a manner that does not disrupt the quantum state of the light. These optical devices, required for operations such as state preparation, detection, multiplexing/demultiplexing and routing, consist of beam-splitters, delay-lines, phase-shifters, electro-optic modulators and other common components. Here we show that Λ-GEM can behave as a dynamically configurable linear optical network. Linear operations can be performed directly on time- or frequency-bin qubits while they are stored in the memory.

Figure 2: Numerical simulation of an arbitrary operation being performed by the memory on three optical modes. Three pulses, $\hat{\mathcal{E}}_1$-$\hat{\mathcal{E}}_3$, enter from the left and are stored into three memories via corresponding coupling fields which have amplitudes determined by the eigenvectors of a unitary operation. (a)-(c) are the optical modes in the original optical basis. (d)-(f) are the modes in the eigenbasis of the operation which is being performed. On recall, the phases of the coupling fields are changed such that the intended unitary operation is performed on the three frequency modes.

Figure 1: Numerical simulation of interference between an optical mode and the spin coherence of the atomic ensemble. The horizontal plane shows the optical modes. The vertical plane shows the spin coherence in the Fourier domain.

The memory can be used as a network of arbitrary beam-splitters operating on adjacent time-bin modes. Control over the coupling strength and phase between an optical pulse and a stored mode is effected by tuning the power and phase of the coupling field. A pulse can be stored in the memory, wholly or partially, and made to interfere with a pulse arriving at a later time with full control over the coupling amplitude. The portion of the two pulses that interferes into the coherence remains in the memory for future use. Numerical simulations, such as the one shown in figure 1, yield near unity fringe visibility and a visibility of 68% has been obtained experimentally [3].

The frequency selectivity of the coupling fields can also be used for operations in the frequency domain. An optical pulse can be stored from one frequency mode and recalled on another such that the memory can be used for frequency multiplexing and routing. The mode which is coupled to the memory, however, can also consist of an arbitrary superposition of frequencies. From this, arbitrary unitary operations can be performed directly on frequency multiplexed optical modes.

For N optical modes, we require N memories to perform an arbitrary operation. This is done by storing each eigenmode of the operation that is to be applied in a separate memory and then recalling it with a phase shift determined by the eigenvalue. In this manner any unitary operation can be performed by selecting the appropriate coupling field amplitudes. The operation can be as efficient as a storage and recall event and can yield near-unity fidelity. A numerical simulation is shown in figure 2. Experimentally, a fringe visibility of 73% was observed for a two-mode operation [3].

References

[1] G. Hétet, M. Hosseini, B. M. Sparkes, D. Oblak, P. K. Lam, B. C. Buchler, Opt. Lett., **20**, 2323-2325 (2008)

[2] M. Hosseini, G. Campbell, B. M. Sparkes, P. K. Lam, B. C. Buchler, Nat. Phys., **7**, 794798 (2011).

[3] G. Campbell, M. Hosseini, B. M. Sparkes, P. K. Lam, B. C. Buchler, New J. Phys., **14**, 033022 (2012).

NOVEL OPTICAL TRAPS FOR ULTRACOLD ATOMS

Cassettari D.
Bruce G. D., Harte, T., Richards, D., Bromely, S., Torralbo-Campo, L., Smirne, G.

SUPA, School of Physics and Astronomy, University of St Andrews, North Haugh, St Andrews, KY16 9SS, UK.

The use of a Spatial Light Modulator (SLM) to generate optical traps for ultracold atoms opens the possibility of forming non-periodic and non-trivial patterns of dipole traps to create trapping geometries not achievable using existing techniques. The SLM is an inherently dynamic tool that offers the opportunity to generate smooth, time-varying optical potentials that can in principle be employed to achieve full coherent control over the trapped gas. We outline the work in progress at St Andrews to achieve novel trapping geometries for ultracold atoms using an SLM.

[1] G D Bruce et al, *"Smooth, holographically generated ring trap for the investigation of superfluidity in ultracold atoms"*, arXiv: 1008.2140, Phys. Scr. **T143,** 014008 (2011).
[2] G D Bruce et al, *"Holographic power-law traps for the efficient production of Bose-Einstein condensates"*, Phys. Rev. A **84,** 053410 (2011).
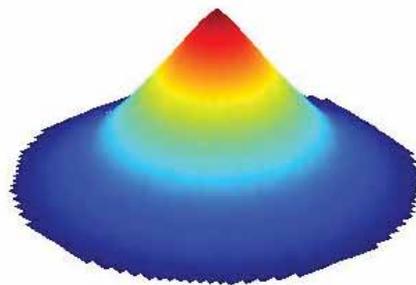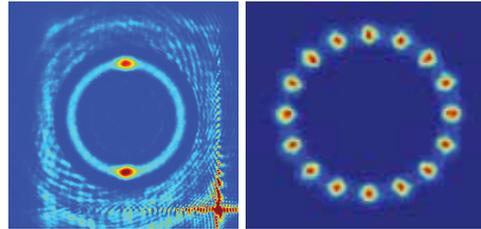
Demonstration of a state-insensitive, compensated nanofiber trap

A. Goban[1], **K. S. Choi**[1,2], **D. J. Alton**[1], **D. Ding**[1], **C. Lacroûte**[1], **M. Pototschnig**[1], **J. A. M. Silva**[1], **C. L. Hung**[1], **T. Thiele**[1†], **N. P. Stern**[1‡], **and H. J. Kimble**[1]

[1]*Norman Bridge Laboratory of Physics 12-33, California Institute of Technology, Pasadena, California 91125, USA*
[2]*Spin Convergence Research Center 39-1, Korea Institute of Science and Technology, Seoul 136-791, Korea*

An exciting frontier in quantum information science is the integration of otherwise "simple" quantum elements into complex quantum networks [1]. The laboratory realization of even small quantum networks enables the exploration of physical systems that have not heretofore existed in the natural world. Within this context, there is active research to achieve lithographic quantum optical circuits, for which atoms are trapped near micro- and nano-scopic dielectric structures and "wired" together by photons propagating through the circuit elements. Single atoms and atomic ensembles endow quantum functionality for otherwise linear optical circuits and thereby the capability to build quantum networks component by component.

Following the landmark realization of a nanofiber trap [2, 3], we report the implementation of a state-insensitive, compensated nanofiber trap for atomic Cesium (Cs) [4]. For our trap, differential scalar shifts δU_{scalar} between ground and excited states are eliminated by using "magic" wavelengths for both red- and blue-detuned trapping fields. Inhomogeneous Zeeman broadening due to vector light shifts δU_{vector} is suppressed by ≈ 250, by way of pairs of counterpropagating red- and blue-detuned fields.

A cloud of cold Cesium atoms (diameter ~ 1 mm) spatially overlaps the nanofiber. Cold atoms are loaded into U_{trap} during an optical molasses phase (~ 10 ms) and are then optically pumped to $6S_{1/2}, F = 4$ for 0.5 ms. The red- and blue-detuned trapping fields are constantly 'on' throughout the laser cooling and loading processes. For the transmission and reflection measurements, the trapped atoms are interrogated by a probe pulse with an optical power $P_{\text{probe}} \simeq 0.1$ pW and detuning δ relative to $F = 4 \leftrightarrow F' = 5$.

The compensation of scalar and vector shifts results in a measured transition linewidth $\Gamma/2\pi = 5.7 \pm 0.1$ MHz for Cs atoms trapped $r_{\text{min}} \simeq 215$ nm from the surface of an SiO_2 fiber of diameter 430 nm, which should be compared to the free-space linewidth $\Gamma_0/2\pi = 5.2$ MHz for the $6S_{1/2}, F = 4 \rightarrow 6P_{3/2}, F' = 5$ Cs transition. Compared to previous work with hollow-core and nano-fibers, the atoms are trapped with small perturbations to dipole-allowed transitions with resonant frequency shift by $\Delta/2\pi < 0.5$ MHz. Probe light transmitted through the 1D array of trapped atoms exhibits an optical depth $d_N = 66 \pm 17$ as shown in Figure 1. From the measurements of optical depth and number N of atoms, we infer a single-atom attenuation $d_1 = d_N/N \simeq 0.08$, as well as enhanced spontaneous emission rate $\Gamma_{1D} \simeq 0.2$ MHz into the waveguide.

The reflection from the 1D atomic array results from the backscattering of the electromagnetic field within the 1D system. The randomness in the distribution of N atoms among n_{sites} trapping sites can thus greatly affect the reflection spectrum $R_N(\delta)$. We observe $R_N(\delta)$ from the 1D atomic array,

where the measured Lorentzian linewidth Γ_R is significantly broadened from Γ_0 for large N (with $N \ll n_{\text{site}}$), in direct proportion to the entropy for the multiplicity of trapping sites. These advances provide an important capability for the implementation of functional quantum optical networks and precision atomic spectroscopy near dielectric surfaces.
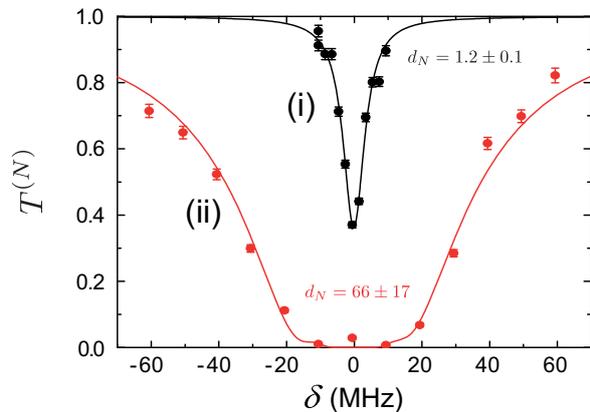
Figure 1: Probe transmission spectra $T^{(N)}(\delta)$ for N trapped atoms as a function of detuning δ from the $6S_{1/2}, F = 4 \rightarrow 6P_{3/2}, F' = 5$ transition in Cs. From fits to $T^{(N)}(\delta)$ (full curves), we obtain the optical depths d_N at $\delta = 0$ and linewidths Γ. $T^{(N)}(\delta)$ (i) at $\tau = 299$ ms with $d_N = 1.2 \pm 0.1$ and $\Gamma = 5.8 \pm 0.5$ MHz and (ii) at $\tau = 1$ ms with $d_N = 66 \pm 17$.

References

[1] H. J. Kimble, *Nature* **453**, 1023 (2008).

[2] E. Vetsch *et al.*, *Phys. Rev. Lett.* **104**, 203603 (2010).

[3] S. T. Dawkins *et al.*, *Phys. Rev. Lett.* **107**, 243601 (2011).

[4] C. Lacroute *et al. New J. Phys.* **14**, 023056 (2012).

[5] A. Goban *et al. arXiv.* 1203.5108 (2012).

Dynamical transport in correlated quantum dots:
a renormalization-group analysis

Sabine Andergassen[1], **Dirk Schuricht**[2], **Mikhail Pletyukhov**[2], **and H. Schoeller**[2]

[1]*Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Wien, Austria*
[2]*Institut für Theorie der Statistischen Physik, RWTH Aachen University*
and JARA - Fundamentals of Future Information Technology, 52056 Aachen, Germany

The theoretical description of strong correlations in the non-equilibrium transport through quantum dots represents a major challenge and require the development of suitable techniques. Using the real-time renormalization-group approach [1], we present results for the nonlinear transport and the time evolution into the stationary state for two paradigmatic model systems: the interacting resonant level model describing a quantum dot dominated by charge fluctuations [2, 3], and the Kondo model for a dot with spin fluctuations [4, 5]. In the stationary state, the finite bias voltage V driving the system out of equilibrium introduces new effects in the current and differential conductance as well as in the charge and spin susceptibilities due to the availability of additional transport channels.

Furthermore, we investigate the time evolution and relaxation in quantum dots. In particular, the derivation of relaxation and decoherence rates and their dependence on the microscopic system parameters is of fundamental importance for the use of quantum dot systems in future quantum information technology applications. For the considered model systems the analytic solution of the renormalization-group equations allows to identify the microscopic cutoff scales that determine these rates. Exploring the entire parameter space, we find rich non-equilibrium physics for the quench dynamics after a sudden switch-on of the level-lead couplings. The time evolution of the dot occupation and current is governed by an exponential relaxation modulating characteristic voltage-dependent oscillations, see Fig. 1.

In addition, the relaxation dynamics towards the steady state features an algebraic decay with interaction-dependent exponents. In the short-time limit we find universal dynamics for spin and current.

References

[1] H. Schoeller, Eur. Phys. J. Special Topics **168**, 179 (2009).

[2] C. Karrasch, S. Andergassen, M. Pletyukhov, D. Schuricht, L. Borda, V. Meden, and H. Schoeller, Europhys. Lett. **90**, 30003 (2010).

[3] S. Andergassen, M. Pletyukhov, D. Schuricht, H. Schoeller, L. Borda, Phys. Rev. B **83**, 205103 (2011).

[4] H. Schoeller and F. Reininghaus, Phys. Rev. B **80**, 045117 (2009).

[5] M. Pletyukhov, D. Schuricht, and H. Schoeller, Phys. Rev. Lett. **104**, 106801 (2010).
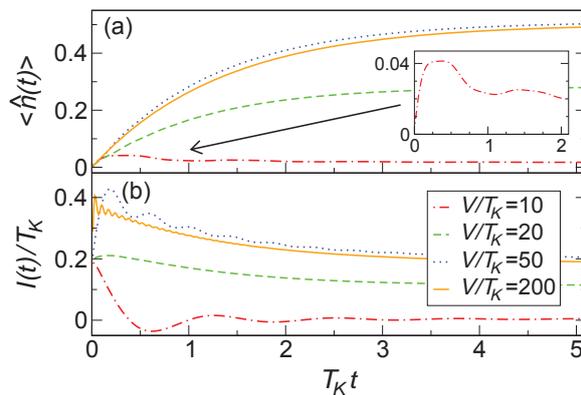
Figure 1: Time evolution of the dot occupation $< n(t) >$ and the current $I(t)$.

Concepts and applications of weak quantum measurements

Wolfgang Belzig[1]**, Christoph Bruder**[2]**, Abraham Nitzan**[3]**, and Adam Bednorz**[4]

[1]*Fachbereich Physik, Universität Konstanz, D-78457 Konstanz, Germany*
[2]*Department of Physics, University of Basel, Switzerland*
[3]*Department of Chemistry, Tel Aviv University, Tel Aviv, Israel*
[4]*Faculty of Physics, University of Warsaw, Hoża 69, PL-00681 Warsaw, Poland*

Realistic correlation measurements in quantum systems are in many cases not compatible with the standard projective measurement scheme. However, correlations can be addressed in the more general framework of weak measurements, which do not disturb the system but add detector noise instead to the quantum outcome. At present it is unclear how to characterize uniquely the non-disturbing limits of quantum measurements. The aim of our contribution is first to characterize weak measurements in general using a minimal set of physically motivated assumptions and second to apply the resulting concept of a quasiprobability to violate some novel sets of classical inequalities for continuous variables.

We first use minimal sets of physical assumptions for the measurement process and propose two generic descriptions of weak measurements leading to two distinct definitions of quasiprobabilities [1]. These quasiprobabilities are sometimes negative, but nevertheless meaningful because they are measurable after subtracting the unavoidable detector noise. Consequently, correlation functions of a quantum variable can be extracted from classically stored signals. There are infinitely many possible generalized measurement schemes equivalent to arbitrary chains of detection devices. We want to establish a clear-cut separation between the outcome of the measurement and the effects due to the detection process in the limit of a noninvasive measurement. We expect the probability of the detected outcome to be a convolution of external background detection noise (that is independent of the actual outcome), and intrinsic quantum signal fluctuations which – as we shall see – can be only described by a quasiprobability. To define a quasiprobability, we still need several assumptions which reflect the natural expected properties of the bare outcome of the quantum measurement. Since they cannot all be satisfied simultaneously, we will pursue two distinct possibilities: (i) we will assume the outcome depends locally in time on the observable. (ii) we will assume that systems and detector are in thermal equilibrium. Both are in agreement with already known theoretical applications of weak measurement and performed experiments [2]. The time-local measurement scheme is consistent with the intuition that the detector has no memory, i.e., registers only instant values of the outcome. The other scheme assumes some memory of the detector but is consistent with the expectation that no information can be transferred in thermodynamic equilibrium. The scheme (i) is consistent with the simplest classical measurement picture often found in experiment, while (ii) is often found in absorptive detectors (e.g. photodiode), where nonequilibrium fluctuations are absorbed without reflection far from the measured system.

If we assume classical macrorealism in quantum mechanics then the statistics of the outcomes with the detection noise subtracted in the limit of noninvasive measurement should correspond to a positive definite probability. In contrast, we show that the assumption of macrorealism is violated by demonstrating that our quasiprobability is somewhere negative. Such violation has been recently demonstrated experimentally [3]. In fact, if we additionally assume dichotomy or boundedness of the quantum outcomes, the violation can occur already on the level of second order correlations of a single observable as shown by Leggett, Garg and others [4]. However, without these additional assumptions, second order correlations are not sufficient to violate macrorealism. Instead, one needs at least fourth order averages to see this violation. We demonstrate that a special fourth order correlation function in the two-level system can reveal the negativity of the quasiprobability in this case and consequently can be used to violate macrorealism, without any additional assumptions [5].

The creation and detection of entanglement in solid state electronics is of fundamental importance for quantum information processing. We propose a general test of entanglement based on the violation of a classically satisfied inequality for continuous variables by 4th or higher order quantum correlation functions [6]. Our scheme can be used for example for current correlations in a mesoscopic transport setup and paves an experimental way to close the loophole based on the assumption of quantized detection of single electrons as required by entanglement test based on the usual Bell inequality.

References

[1] A. Bednorz and W. Belzig, Phys. Rev. Lett. **105**, 106803 (2010)

[2] E. Zakka-Bajjani *et al.*, Phys. Rev. Lett. **99**, 236803 (2007); J. Gabelli and B. Reulet, Phys. Rev. Lett. **100**, 026601 (2008); J. Stat. Mech. P01049 (2009); E. Zakka-Bajjani *et al.*, Phys. Rev. Lett. **104**, 206802 (2010); A. H. Safavi-Naeini, Phys. Rev. Lett. **108**, 033602 (2012).

[3] A. Palacios-Laloy, F. Mallet , F. Nguyen , P. Bertet, D. Vion,D. Esteve, and A.N. Korotkov, Nat. Phys. **6**, 442 (2010).

[4] A.J. Leggett and A. Garg, Phys. Rev. Lett. **54**, 857 (1985).

[5] A. Bednorz, W. Belzig, and A. Nitzan, New J. Phys **14**, 013009 (2012).

[6] A. Bednorz and W. Belzig, Phys. Rev. B **83**, 125304 (2011).

Delocalised Oxygen models of two-level system defects in superconducting phase qubits

Timothy C. DuBois, **Manolo C. Per, Salvy P. Russo and Jared H. Cole**

Chemical and Quantum Physics, School of Applied Sciences, RMIT University, Melbourne, 3001, Australia

Superconducting circuits based on Josephson junctions (JJ) are promising candidates for qubits, single electron transistors & SQUIDS. Decoherence in these systems is currently the largest obstacle that needs to be overcome before long coherence times can be realised. This decoherence is often suggested to come from environmental two-level systems (TLS) [1], which have been studied extensively in glassy systems [2].

Recent experiments in superconducting phase- and flux-qubits have shown that 'strongly-coupled' defects can also be observed [3, 4, 5]. These defects are stable, controllable and have relatively long decoherence times themselves. This provides an opportunity to study the nature of the defects in general.

Many TLS properties have been measured, but the microscopic origin of the defects has been quite elusive. Many phenomenological models have been put forward to describe them: charge dipoles coupled to the electric field [6], formation of Andreev bound states affecting the junctions' critical current [7], magnetic dipoles coupled to the magnetic field [8], TLS state changing the JJ transparency [9] & Kondo impurities [10]. Qualitative evaluation of these defect models unfortunately show that parameters for each model can be equally well fitted to experimental data and are therefore currently indistinguishable [11].

In this work we take an alternative approach: building a microscopic model from the bottom up. This allows us to make concrete predictions about the properties of these defects as a function of strain, temperature and stoichiometry; leading to better fabrication and design control over the defects.

A pertinent example defect in crystal Silicon is the Oxygen interstitial. For this defect, the harmonic approximation for atomic positions cannot be applied due to the rotational symmetry of the defect as Oxygen delocalises around the Si-Si bound axis. This forms an anharmonic system even in a "perfect" crystal [12].

Inspired by this defect, we consider delocalised Oxygen as an ansatz for two-level defects in amorphous Aluminium Oxide (a-AlO_x), which is generally used as the insulating barrier in Aluminium based JJs. Many different spacial configurations can exist beyond the trigonal symmetry of Corundum, although we initially consider a cubic lattice of six Aluminium atoms with an Oxygen atom at its centre as our prototype defect.

We build a one dimensional model and show that we can observe splitting energies of $2 - 45$ μeV for O-Al spacings of $|X| \approx |Y| \approx 2 - 4$ $\mathring{A}$. In this parameter regime, we see dipole element sizes of $\mathcal{O}(1\ \mathring{A})$, which compares well to that measured in experiments [6, 3, 11]. Similar energy scales are observed when the Oxygen is allowed to delocalise in two dimensions.

This model shows that such two-level defects can arise in a-AlO_x without any alien species present. This suggests changes in fabrication processes are required to eliminate such defects.
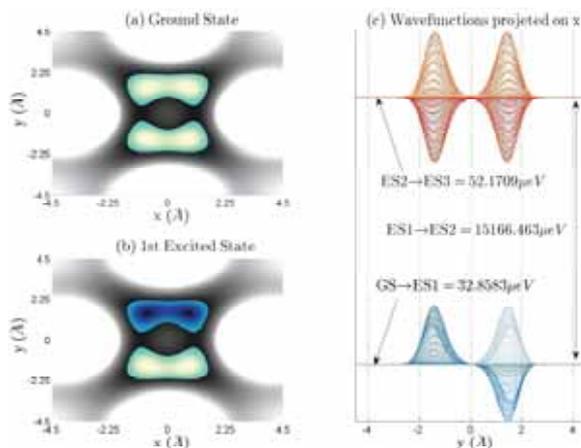
Figure 1: z projection of 2D potential (outer region) and wavefunction (central islands) showing the location probability of the Oxygen atom within the cluster when the system is in the (a) ground state and (b) first excited state. (c) x projection of lowest four wavefunctions and energies. Splitting energies are labeled for associated quasi-degenerate states.

References

[1] P. Dutta *et al.*, Rev. Mod. Phys., **53**, 497–516, (1981).

[2] P. W. Anderson *et al.*, Phil. Mag., **25**, 1–9, (1972).

[3] Y. Shalibo *et al.*, Phys. Rev. Lett., **105**, 177001, (2010).

[4] A. Lupaşcu *et al.*, Phys. Rev. B, **80**, 172506, (2009).

[5] J. Lisenfeld *et al.*, Phys. Rev. Lett., **105**, 230504, (2010).

[6] J. Martinis *et al.*, Phys. Rev. Lett., **95**, 210503, (2005).

[7] R. de Sousa *et al.*, Phys. Rev. B, **80**, 094515, (2009).

[8] S. Sendelbach *et al.*, Phys. Rev. Lett., **100**, 227006, (2008).

[9] L. Ku and C. Yu, Phys. Rev. B, **72**, 024526, (2005).

[10] L. Faoro *et al.*, Phys. Rev. B, **75**, 132505, (2007).

[11] J. H. Cole *et al.*, App. Phys. Lett., **97**, 252501, (2010).

[12] E. Artacho *et al.*, Phys. Rev. B, **51**, 7862–7865, (1995).

Using quantum state protection via dissipation in a quantum-dot molecule to solve the Deutsch problem

Márcio M. Santos[1], **Fabiano O. Prado**[1], **Halyne S. Borges**[1], **Augusto M. Alcalde**[1], **José M. Villas-Bôas**[1] **and** <u>**Eduardo I. Duzzioni**</u>[1]

[1]*Universidade Federal de Uberlândia, Uberlândia, Brazil*

The wide set of control parameters and reduced size scale make semiconductor quantum dots attractive candidates to implement solid-state quantum computation. Considering an asymmetric double quantum dot coupled by tunneling, we combine the action of a laser field and the spontaneous emission of the excitonic state to protect an arbitrary superposition state of the indirect exciton and ground state. As a by-product we show how to use the protected state to solve the Deutsch problem [1].

References

[1] M. M. Santos, F. O. Prado, H. S. Borges, A. M. Alcalde, J. M. Villas-Bôas and E. I. Duzzioni, Phys. Rev. A, **85**, 032323 (2012).

Diamond emitters in microcavities

Kathrin Buczak[1], Achim Bittner[2] ,Christian Koller[1], Tobias Nöbauer[1], Johannes Schalko[2], Ulrich Schmied[2], Michael Schneider[2], **Jörg Schmiedmayer**[1], **Michael Trupke**[1]

[1]*Vienna Center for Quantum Science and Technology, Atominstitut, TU Wien, 1020 Vienna, Austria*
[2]*Mikrosystemtechnik, Institut für Sensor- und Aktuatorsysteme, TU Wien, Gusshausstr. 27-29, 1040 Wien, Austria*

Nitrogen-vacancy or NV centres in diamond are among the most promising solid-state systems for quantum information processing as they possess convenient properties such as optical initialisation and read-out, a ZPL at 637 nm with transform-limited emission at low temperatures. Most importantly, the NV centre possesses a long room-temperature electron coherence lifetime [1]. It is on the order of 100 μs in natural diamond, and reaches values approaching 2 ms in artificial isotope-purified (spinless) carbon-12 diamonds.

It is possible to (probabilistically) create NV centres by implantation with a spatial resolution on the order of $\pm$ 25 nm [2]. It was furthermore shown that the electron spin can be entangled with the polarisation of a photon emitted by the NV centre if the emission occurs via the zero-phonon transition [3]. This lays the basis for an entanglement by projective measurement of remote NV centres. These experiments are hindered only by the weak zero-phonon transition of diamond, which makes up only 4 % of its radiative decay, but this transition can be strongly enhanced by coupling the NV centre to a microcavity.

Figure 1: (a) Level scheme for emitter-photon entangling sequence used for NV- [3]. (b) Proposed experimental setup for high-efficiency entanglement.

Here we will present our efforts to place NV centres into microcavities. These resonators are microfabricated [4] , directly fibre-coupled and individually actuated, and can be created in large numbers on a single chip.
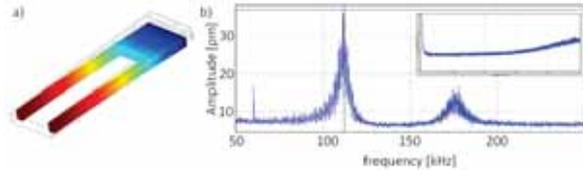
Figure 2: Cantilevers for micromirror actuation.
a) Finite-element simulation of a deflected cantilever. b) Measured oscillation spectrum of a fabricated cantilever with a length of 300 nm and a mirror pad of 50 nm × 50 nm under electrostatic driving. The first resonances of significant amplitude occur at frequencies above 100 kHz, i.e. far above the acoustic noise spectrum present in a standard laboratory environment. Inset: spectrum up to 1 MHz of the free-running cantilever.

References

[1] T. Ladd et al., Nature **464**, 45-53 (2010)

[2] M. Toyli et al., Nano Lett., **10** (8), 3168-3172, (2010)

[3] E. Togan et al., Nature **466**, 730-734 (2010)

[4] G. W. Biedermann et al., Appl. Phys. Lett. **97** 181110 (2010)

Experimental Demonstration of Blind Quantum Computing

Stefanie Barz[1,2], **Elham Kashefi**[3], **Anne Broadbent**[4,5], **Joseph F. Fitzsimons**[6,7], **Anton Zeilinger**[1,2], **Philip Walther**[1,2]

[1]*Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria*
[2]*Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria*
[3]*School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK*
[4]*Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1*
[5]*Department of Combinatorics & Optimization, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1*
[6]*Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore 117543*
[7]*School of Physics, University College Dublin, Belfield, Dublin 4, Ireland*

Quantum physics has revolutionized our understanding of information processing and enables quantum computers to achieve computational speed-ups that are unattainable using classical computers by harnessing quantum phenomena such as superposition and quantum entanglement. Theoretical and experimental efforts are focused on different experimental approaches for the realization of quantum computers. At present it seems that the intrinsic technical complexity may result in only a few powerful quantum computers that are operated only at specialized facilities. The challenge in using such central quantum computers to ensure the privacy of the client's data as well as the privacy of the computation.

Quantum physics provides a solution to this challenge and enables a new level of security in data processing [1]: The privacy of the data and the computation can be preserved while being computed at a remote servers, manifested in the blind quantum computing protocol. Combining the notions of quantum cryptography and quantum computation, the blind quantum computing protocol achieves the delegation of a quantum computation from a client with no quantum-computational power to an quantum server, such that the client's data remains perfectly private.

Remarkably, the preparation and sending of single qubits is the only quantum power that is required from the client. The protocol uses the concept of the measurement-based quantum computation which provides a conceptional framework, where the quantum and classical resources are clearly separated [2]. The user prepares blind qubits in a state $|\theta_j\rangle = 1/\sqrt{2}(|0\rangle + e^{\theta_j}|1\rangle)$ where the phase, θ_j, is chosen from the set $\{0, \pi/4, \dots, 7\pi/4\}$ and known only to himself ($|0\rangle$ and $|1\rangle$ are the computational basis of the physical qubits). These blind qubits are then send to to the quantum computer that entangles the qubits via controlled phase gates and creates blind cluster states. The actual computation is measurement-based: The user tailors measurement instructions to the particular state of each qubit and sends them to the quantum server. Without knowing the state of the blind qubits, these instructions appear random and do not reveal any information about the computation. The servers perform measurements according to these instructions and finally, the results of the computation are sent back to the user who can interpret and utilize the results of the computation.

Here we present the first such experimental blind quantum computation using a family of photonic blind cluster states, where the client's input, computation, and output remain secret [3]. We demonstrate the implementation of a universal of set of single-qubit and non-trivial two-qubit quantum logic gates, as well as examples of Deutsch-Jozsa's and Grover's algorithm, where the quantum-computing server cannot distinguish which kind of operation is performed.

Our experiment is a step towards unconditionally secure quantum computing in a client-server environment, where the client's computation remains hidden —a functionality not known to be achievable in the classical world alone [4, 5].
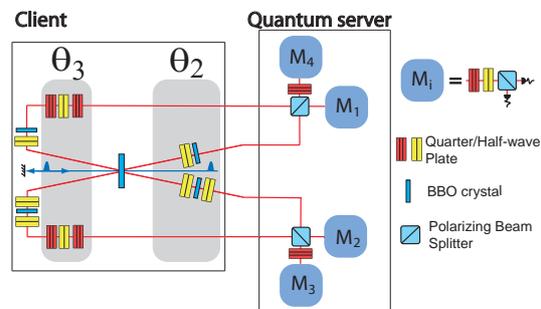
Figure 1: The experimental setup to produce (client) and measure (quantum server) blind cluster states, where the client has access to the blind phases θ_2 and θ_3 by adapting phase shifters.

References

[1] A. Broadbent, J. Fitzsimons, E. Kashefi, Proceedings of the 50th Annual Symposium on Foundations of Computer Science, 517–526 (2009).

[2] R. Raussendorf, H. J. Briegel, PRL **86**, 5188 (2001).

[3] S. Barz et al., Science **335**, 303 (2012).

[4] R. Rivest, L. Adleman, M. Dertouzos, Foundations of Secure Computation, 169–180 (1978).

[5] C. Gentry, Proceedings of the 41st annual ACM symposium on Theory of Computing, 169–178 (2009).

Multipartite photonic entanglement from polarization squeezing at 795 nm.

__Federica A. Beduini__[1], Yannick A. de Icaza Astiz[1], Vito G. Lucivero[1], Joanna A. Zielińska[1] and Morgan W. Mitchell[1]

[1]*ICFO - Institut de Ciències Fotòniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*

Many applications of the properties of quantum systems rely on multipartite entanglement, but it is still difficult to implement them experimentally with present techniques. For quantum networking and atomic quantum metrology applications, entangling many particles is not the only challenge: it is important also that the entangled photons can efficiently interact with atoms. Here we present a new technique that allows the generation of narrowband and atom-resonant multipartite entangled photons: starting from polarization squeezing, it is possible to achieve very bright states ($\sim 10^5$ pairs/(s MHz)) which are robust against losses.

Theoretical Results Spin squeezing implies entanglement of large numbers of particles [1], and spin-squeezed states with k-entanglement have been demonstrated [2]. These states cannot be written as a convex sum of density matrices with fewer than k particles. The evidence for this entanglement is, however, indirect, due to the difficulty of single-spin measurement. We use optical polarization squeezing, which is formally similar, and has the advantage that present photonic techniques allow both generation and characterization of multi-photon entanglement.

In order to show that polarization squeezing induces at least 2-entanglement, we derive the reduced two-photon density matrix of a polarization squeezed state and compute its concurrence. We consider a polarization squeezed state generated by combining in the same spatial mode a coherent state horizontally polarized (H) and a squeezed vacuum state with linear orthogonal polarization (V) that is generated by an optical parametric oscillator (OPO). Its reduced two-photon density matrix is proportional to the second order correlation matrix: $G^{(2)}_{jk,nm}(\tau) = \langle \hat{a}^\dagger_j(t) \hat{a}^\dagger_k(t+\tau) \hat{a}_m(t+\tau) \hat{a}_n(t) \rangle$, where the indices correspond to the two orthogonal linear polarization modes (H, V) and the diagonal elements correspond to the rate of detecting one photon in the $j = n$ mode at an instant t and another photon in the mode $k = m$ at the time $t + \tau$.

Our calculations show that a polarization squeezed state is always 2-entangled, but high amounts of entanglement are reached only for a limited range of values of the average photon flux for the squeezed vacuum and coherent beam (see Figure 1). The photons in the state are entangled even if they are not coincident, but they are separated in time up to an interval τ which is comparable to the inverse of the OPO bandwidth ($\delta\nu$). Realistic choices of the experimental parameters predict multipartite entangled states with large photon flux ($\sim 10^6$ entangled photons/s) as well as high entanglement (concurrence up to 0.64).

Experiment A squeezed vacuum state is generated by a sub-threshold OPO and it is combined at a polarizing beam splitter (PBS) with a coherent state: the resulting state is polarization squeezed [3].

A discrete quantum state tomography setup based on coincident photon detection allows us to recover experimentally
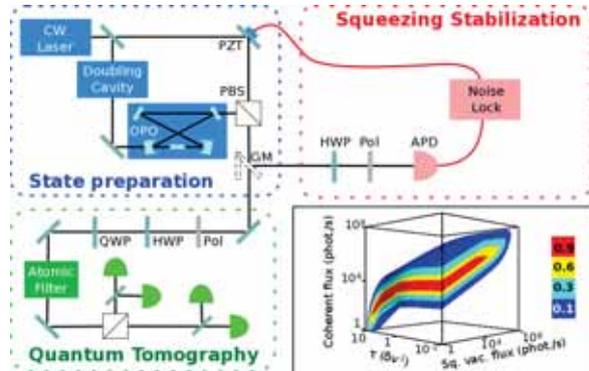
Figure 1: Schematic experimental setup. PZT: piezoelectric actuator. HWP(QWP): half(quarter)-waveplate. Inset: Isosurfaces of concurrence. $\delta\nu = 8$ MHz.

the two-photon reduced density matrix, so that we can measure its entanglement by computing the concurrence. In this way, losses do not affect the amount of entanglement, but they just correspond to lower detection rates.

In order to fix the squeezed Stokes component, we monitor the fluctuations of the $\hat{S}_2$ Stokes parameter: a noise lock circuit automatically adjusts the phase between the coherent and the squeezed vacuum state, so that the fluctuations are kept at their minimum. A galvanometer mirror (GM) sends alternatively the state either to the entanglement detection or to the squeezing stabilization part.

A polarizer (Pol) reduces the contribution from coherent photons by six orders of magnitude, so that the photon flux at the photon counters is maintained relatively low (< 1Mcps), while simultaneously the signal at the APD is sufficiently large (few nW) to assure shot-noise-limited detection. Remarkably, this does not interfere with the measurement of entanglement properties, as the polarizer affects each photon individually, performing a local operation. The filter, based on Faraday rotation [4] with a pass-band of ~ 500 MHz, passes the polarization squeezed state, but blocks non-degenerate OPO emission.

References

[1] A. Sørensen, L.-M. Duan, J. I. Cirac and P. Zoller, Nature **409**, 63 (2001).

[2] C. Gross, T. Zibold, E. Niklas, J .Esteve and M. Oberthaler, Nature 464, 1165-1169 (2010).

[3] F. Wolfgramm, A. Cerè, F. A. Beduini et al., Physical Review Letters **105**, 053601 (2010).

[4] J. A. Zielińska, F. A. Beduini, N. Godbout and M. W. Mitchell, Optics Letters, **37**, 524-526 (2012).

Conditional quantum teleportation of non-Gaussian non-classical states of light

Hugo Benichi[1,2], Shuntaro Takeda[1], Ladislav Mišta Jr.[3], Radim Filip[3] and Akira Furusawa[1]

[1]The University of Tokyo, Tokyo, Japan
[2]National Institute of Information and Communications Technology, Tokyo, Japan
[3]Palacký University, Olomouc, Czech Republic

Recently, [1] has reported on the successful experimental continuous variable teleportation[2] of non-classical non-Gaussian states of light produced with the photon subtraction protocol[3]. The successful quantum manipulation of a non-classical states in this experiment is defined in the sense of the negativity of the Wigner function: a quantum state with a negative Wigner function is teleported to the point where the fragile negativity of the Wigner function is preserved at the output of the teleporter. Although the negativity collapses in a way which can be quantified[4], the output teleported state is still a non-classical state without any ambiguity in [1].
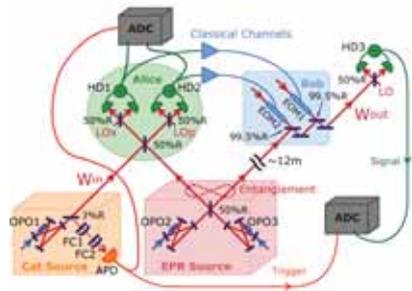
Figure 1: Experimental setup for conditional teleportation.

As was proposed in [5], conditional operations can improve the quality of the output teleported state and yield better negativities than what is achievable with deterministic operations. We present how to implement this conditional teleportation protocol to further enhance teleportation of non-classical features of the Wigner function (see Fig.1). We report on the experimental demonstration of this conditional teleportation scheme and show that the non-classicality of the Wigner function is enhanced by conditional operations where the teleportation succeeds only if a certain threshold condition is met: only when Alice's quadrature measurement results meet some chosen requisite conditions that teleportation will be considered successful. The conditioning scheme of our experimental setup is based on a simple threshold mechanism: if Alice's homodyne measurement $\xi = (\bar{x}_u + i\bar{p}_v)/\sqrt{2}$ falls inside a circle of radius L, then the output teleported state is accepted. In practice, the output negativity $W_{\text{out}}(0,0|L)$ is estimated using the inverse Radon transform with the detection events satisfying the condition $\bar{x}_u^2 + \bar{p}_u^2 \leq 2L^2$. The evolution with the control parameter L of both the output negativity $W_{\text{out}}(0,0|L)$ and the fraction of selected events can be evaluated for many different values of L with the same experimental data set after the experimental measurement has finished. With this analysis protocol, the experimental results shown in Fig.2 demonstrate the success of the conditional scheme and its improvement to $W_{\text{out}}(0,0|L)$. With conditional operations, the negativity is found to be stronger than what deterministic operations can achieve. Especially, we observe that conditional teleportation can pull out negativity from a state which appears to have a positive Wigner function with deterministic operations.
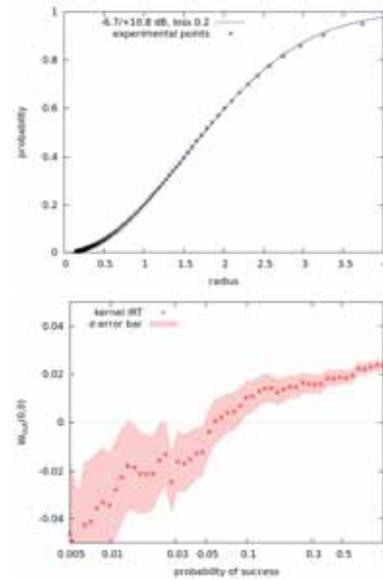
Figure 2: Top, probability of success of conditional teleportation $P(L)$ with the control parameter L, experiment (crosses) and theory (solid). Bottom, experimental improvement of $W_{\text{out}}(0,0|L)$ with $P(L)$.

References

[1] N. Lee *et al*, Science **332**, 330 (2011).

[2] S. L. Braunstein, H. J. Kimble, PRL **80**, 869 (1998).

[3] M. Dakna *et al*, PRA **55**, 3184 (1997).

[4] H. Benichi *et al*, PRA **84**, 012308 (2011).

[5] L. Mista *et al*, PRA **82**, 012322 (2010).

Cluster state generation with cylindrically polarized modes

Stefan Berg-Johansen[1,2], **Ioannes Rigas**[1,2], **Christian Gabriel**[1,2], **Andrea Aiello**[1,2], **Peter van Loock**[1,2], **Ulrik L. Andersen**[1,2,3], **Christoph Marquardt**[1,2] **and Gerd Leuchs**[1,2]

[1]*Max Planck Institute for the Science of Light, Erlangen, Germany*
[2]*Institute of Optics, Information and Photonics, University of Erlangen-Nuremberg, Erlangen, Germany*
[3]*Department of Physics, Technical University of Denmark, Lyngby, Denmark*

In the one-way model of quantum computing (QC) the computational resource is initially provided in the form of a multipartite, persistently entangled state, the cluster state [1]. Universal QC can be performed through consecutive measurements and feedforward on individual vertices of the cluster. The implementational effort is thus shifted away from creating a sequence of unitary quantum logic gates, as in the conventional circuit approach to QC, towards generating a highly entangled initial cluster. This conceptual difference makes cluster state QC promising with regard to scalability, but the efficient generation of the cluster itself still poses a challenge.

We present an approach to generating cluster states using cylindrically polarized modes (CPMs) of bright squeezed light. CPMs have a spatially varying polarization and intensity distribution which can be written as a superposition of horizontally (H) and vertically (V) polarized first-order Hermite-Gaussian basis modes (10 and 01). As an example, the decomposition of a radially polarized beam is shown in Figure 1a. Previously, we have shown that already in the classical picture the polarization and spatial degrees of freedom (DOFs) of these beams posess a Schmidt rank of 2 and therefore cannot be factorized [2]. In the quantum picture, quadrature squeezing leads to entanglement between the basis modes of the beam in the spatial and polarization DOFs and even across these two different DOFs, a feature referred to as *hybrid entanglement* [3].

Using squeezed CPMs as the initial resource, we design simple passive networks of polarizing beam splitters (PBS) and half-wave plates ($\lambda/2$) which spatially separate, rotate and possibly re-combine the basis modes. This results in a four-partite cluster state, the exact topology of which depends on the individual shape of the passive network. We note that each vertex of the final cluster state is physically represented by a unique spatio-polarization mode, allowing for a higher degree of addressability than with conventional lower-order modes. The DOF in which correlations are measured (spatial or polarization) can be chosen freely. Figure 1b shows an example of such a network. Applying the formalism of Gaussian graph states for finitely squeezed continuous-variable systems [4], the full covariance matrix of the cluster resulting from this particular example can be determined from the expression

$$\mathbf{Z}^{A/R} = i\mathbf{1}_4 + z\tilde{\mathbf{V}}^{A/R}, \tag{1}$$

where z quantifies the amount of squeezing and the adjacency matrix $\tilde{\mathbf{V}}^{A/R}$ has the form shown in Figure 1c (A/R indicates an azimuthally or radially polarized input mode). Remarkably, each vertex of the cluster is correlated to every other vertex, as can be seen from the corresponding diagrammatic representation in Figure 1d. Different network designs lead to other cluster topologies such as the simple "box" cluster.
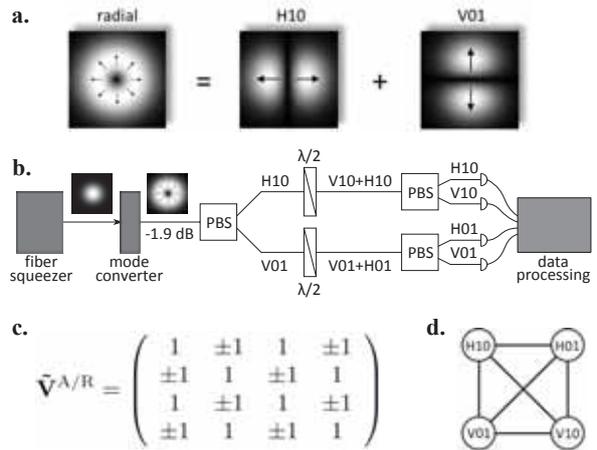
Figure 1: **a.** Hermite-Gauss decomposition for a radially polarized beam **b.** Experimental setup for the compact generation of a four-partite cluster state **c./d.** Adjacency matrix and graph representation for the cluster resulting from the setup in b.

The feasibility of the network shown in Figure 1b has been demonstrated experimentally. We employ an asymmetric nonlinear fiber Sagnac loop to achieve amplitude squeezing in a Gaussian beam which is subsequently converted into an azimuthally or radially polarized mode via a twisted nematic liquid crystal. The measured amplitude squeezing in the resulting CPMs is -1.9 dB below the quantum noise limit. The passive linear network has been implemented exactly as shown above. In a first characterization of the resulting cluster we measure amplitude correlations between all possible pairs out of the four output modes. These agree well with the theoretical predictions.

In conclusion, we show that cylindrically polarized modes are viable candidates for continuous-variable cluster state generation. Given one or more squeezed CPMs as the initial resource, various cluster topologies can be generated through a passive linear network. The resulting cluster vertices are uniquely addressable and multiply entangled across both polarization and spatial degrees of freedom.

References

[1] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett., **86**(22), 5188-5191 (2001)

[2] A. Holleczek *et al.*, Opt. Express, **19**(10) (2011)

[3] C. Gabriel *et al.*, Phys. Rev. Lett., **106**(6) (2011)

[4] N. C. Menicucci *et al.*, Phys. Rev. A, **83**(4) (2011)

Biphoton Interference and Phase Reconstruction of Time-Energy Entangled Photons through Spectral Amplitude and Phase Modulation

Bänz Bessire[1], **Christof Bernhard**[1], **André Stefanov**[1], and **Thomas Feurer**[1]

[1]*Institute of Applied Physics, University of Bern, Switzerland*

We demonstrate spectral amplitude and phase modulation of time-energy entangled photon pairs by means of a spatial light modulator (SLM) [1]. Coincidences are detected by sum frequency generation in a nonlinear crystal which has been applied in several experiments as an ultrafast coincidence detection method to temporally resolve entangled photons on a timescale of fs [2, 4]. By explicitly taking into account the properties of the detection crystal, we derive an expression for the sum frequency signal in the form of a second-order correlation function $G^{(1)}$ derived through perturbation theory [4].

In the experiment (Fig. 1), broadband entangled photons are generated via spontaneous parametric down-conversion by pumping a periodically poled nonlinear $KTiOPO_4$ (PPKTP) crystal. To compensate for group-velocity dispersion, the entangled photons are imaged from the SPDC crystal through a four-prism compressor in the middle of the up-conversion crystal. The intermediate plane of the prism compressor enables access to the spectrum of the entangled photons and provides the possibility to modulate spectral components in amplitude and phase with a SLM.
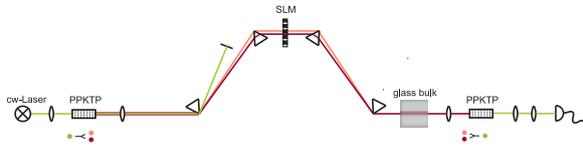
Figure 1: Experimental setup: Broadband entangled photons are generated in a PPKTP crystal, their spectrum is shaped by a SLM and coincidences are detected by up-conversion in another PPKTP crystal. In addition, a glass bulk is introduced in the entangled photon path.

The SLM allows to mimic various quantum optical experiments by suitably programming a time-stationary transfer function $\mathcal{M}(\Omega)$. To investigate biphoton interference, we implement the transfer function of a two path interferometer to perform an interferometric autocorrelation measurement (IAC). We are further able to measure an intensity-like autocorrelation (AC), only realizable by the use of an SLM (blue and red curves in Fig. 2).

Phase sensitivity of the IAC signal then enables the reconstruction of additional phase contributions due to various optical elements in the entangled photon path. We use a computer based optimization algorithm to determine relevant orders in the spectral biphoton phase. Each optimization step varies φ_n such that the RMS of the difference between measured IAC and

$$G^{(1)}(\tau) \propto \left| \int_{-\infty}^{\infty} d\Omega \, \Gamma(\Omega) \, \mathcal{M}(\Omega) \, \mathrm{e}^{2i \sum_{n=2r}^{\infty} \frac{\varphi_n}{n!} \Omega^n} \right|^2 , \quad r \in \mathbb{N},$$

converges to a minimum where $\Gamma(\Omega)$ denotes the coincidence photon amplitude. Fig. 2 shows experimental and theoretical results of a shaper based interferometric and intensity-like autocorrelation measurement with a fused silica glass bulk introduced in the entangled photon beam. In this case the optimization procedure determines the group-velocity Taylor coefficient $\varphi_2 = 1'281 fs^2$.
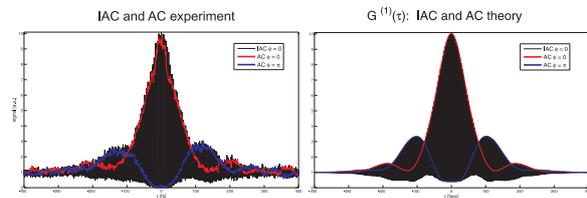
Figure 2: Experimental and theoretical results of a shaper based interferometric (black) and intensity-like (red, blue) autocorrelation measurement are shown. By applying a phase shift $\phi \in \{0, \pi\}$ in the corresponding transfer function, we are able to switch between the two output ports of an SLM based Mach-Zehnder interferometer.

By demonstrating the ability to coherently control the spectral amplitude and phase of entangled photons we contribute to the groundwork for SLM based experiments towards quantum processing and quantum information such as encoding qudits in the frequency domain.

References

[1] F. Zäh, M. Halder and T. Feurer, Optics Express, **16**, 21, 16452-16458 (2008)

[2] A. Pe'er, B. Dayan and Y. Silberberg, Phys. Rev. Lett., **94**, 073601 (2005)

[3] S. Sensarn, Irfan Ali-Khan, G. Y. Yin and S. E. Harris, Phys. Rev. Lett., **102**, 053602 (2009)

[4] K. A. O'Donnell and A. U. Ren, Phys. Rev. Lett., **103**, 123602 (2009)

Robust nonlocality tests with displacement-based measurements

Jonatan Bohr Brask[1] and Rafael Chaves[1]

[1]*ICFO-The Institute of Photonic Sciences, Av. Carl Friedrich Gauss, 3, 08860 Castelldefels (Barcelona), Spain*

According to quantum theory, experiments performed by space-like separated, independent observers may display correlations that do not comply with assumptions of local realism, i.e. which violate a Bell inequality. A decisive test of nonlocality is very desirable from a fundamental perspective, but also from an applied point of view, since nonlocality represents a physical resource which enables protocols such as device-independent quantum key distribution and random number generation.

In spite of steady theoretical and experimental progress, nonlocality has yet to be demonstrated in a loophole-free manner. All experiments to date suffer from either the locality loophole, meaning that the measurements performed by the observers are not space-like separated, or the detection loophole, which is opened when the efficiency of the detectors, transmission, or source coupling is insufficient. Both loopholes open for local-hidden-variable explanations of the observed data and compromise the security of cryptographic protocols. Closing the loopholes is thus important both from a fundamental and a technological perspective. To close the locality loophole, it is advantageous to work with optical systems since light can be distributed with relative ease among spatially separated parties and since optical detectors are fast. Various approaches have been considered towards closing the detection loophole in optical Bell tests. Two fundamental types of entangled states which may be used are polarisation-entangled states of fixed photon number, or states relying on superposition of one or few photons with the vacuum. Both approaches are hampered by low efficiency of source coupling and of most available single-photon detectors (although superconducting transition-edge sensors now do allow high efficiency). The former case has the advantage that projective measurements in any basis can be performed with linear optics. However, source and detector efficiencies are so far incompatible with the critical thresholds required for a bipartite Bell test. For the case of photon-number superpositions, entanglement generation can be achieved with relatively large efficiency since, in the simplest cases, it suffices to produce a two-mode squeezed state, or to split a single photon on a beam splitter. The disadvantage is that perfect projective measurements are not available in all bases, using linear optics and photon counting, since passive linear optics cannot change the energy of a state.

Here we present results demonstrating that with simple, displacement-based measurements, it is possible to attain good efficiency thresholds which in some cases exactly coincide with the thresholds for ideal qubit measurements in arbitrary bases. The measurement scheme is illustrated in Fig. 1 for a bipartite setup. We find that the scheme performs well for a weakly two-mode-squeezed state in which case it admits a combined efficiency threshold for coupling, transmission, and detection of 66.7%. That is, for efficiencies above this bound, a loophole-free test is possible. We also extend the scheme to atom-photon entanglement, where the threshold can be lowered to 43.7%, and to more parties sharing a single photon split between multiple modes. Finally, we consider a scheme to compensate imperfect transmission and coupling at the source by local filtering, based on single-photon amplification.
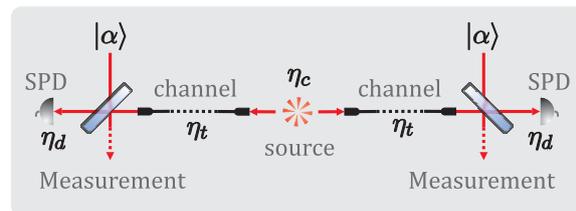
Figure 1: Bipartite Bell test with displacement-based measurements. A source distributes an entangled state of light to two separated parties. Each party applies a displacement by mixing the signal with a local oscillator on a highly transmissive beam splitter and then performs single-photon detection. Different measurement settings correspond to different choices of displacements. We account for losses in source coupling, transmission, and detection, here labelled by the efficiencies η_c, η_t, and η_d respectively.

Observation of topologically protected bound states in photonic quantum walks

T. Kitagawa[1†], M. A. Broome[3†], A. Fedrizzi[3], M. S. Rudner[1], E. Berg[1], I. Kassal[2], A. Aspuru-Guzik[2], E. Demler[1], A. G. White[3]

[1]Department of Physics, Harvard University, Cambridge MA 02138, United States
[2]Department of Chemistry and Chemical Biology, Harvard University, Cambridge MA 02138, United States
[3]ARC Centre for Engineered Quantum Systems and ARC Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane 4072, Australia
†These authors contributed equally to this work.

A striking feature of quantum mechanics is the appearance of new phases of matter with origins rooted in topology. The existence of bound states at the interface between different topological phases causes the robust macroscopic phenomena found in integer quantum Hall systems, topological insulators, and topological superconductors. Engineered quantum systems—notably in photonics, where the wavefunctions can be observed directly—provide versatile platforms for creating and probing a variety of topological phases. We use a photonic quantum walk to observe bound states between systems with different bulk topologies and demonstrate their robustness to small perturbations—the signature of topological protection. We can observe topological dynamics far from the static or adiabatic regimes—to which most previous work on topological phases has been restricted—where we discover a new phenomenon: a topologically protected pair of bound states unique to periodically driven systems.

Phases of matter have long been characterised by the symmetry properties of their ground-state wavefunctions, where breaking of symmetry results in a phase change. The discovery of the integer quantum Hall effect in the 1980's led to the insight that phases of matter could be characterised by their topology alone. Since then topological phases have been identified in physical systems ranging from condensed-matter and high-energy physics to quantum optics and atomic physics.

Topological phases of matter are parameterised by integer topological invariants. Since integers cannot change continuously, a frequent consequence is exotic behaviour at the interface between systems with different topological invariants. For example, a topological insulator supports conducting states at the surface precisely because its bulk topology is different to that of its surroundings. Creating and studying new topological phases remains a difficult task in a solid-state setting but might be easier in more controllable simulators.

Here we simulate one-dimensional topological phases using a discrete time quantum walk [2], a protocol for controlling the motion of quantum particles on a lattice. We create regions with distinct topological invariants and directly image the wavefunction of bound states at the boundary. The controllability of our system allows us to make small changes to the Hamiltonian and demonstrate the robustness of these bound states.

To probe the topological properties of the quantum walk we create a quantum walk Hamiltonian whose topology varies spatially across the walk lattice. If the two topologies are not compatible, i.e. they do not have the same topological invariant, the walker becomes trapped between these two phases. A sample of the results [4] are shown in Fig.1.
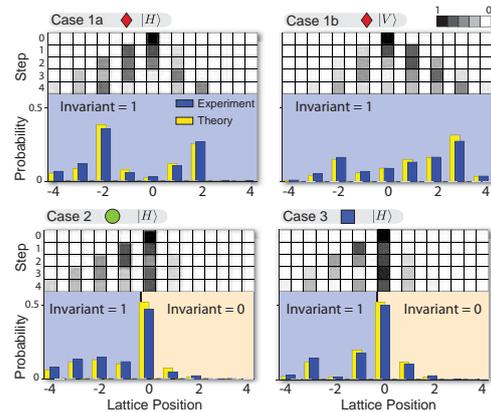
Figure 1: Experimental probability distributions. The quantum walk parameters are spatially inhomogeneous and therefore can have different topological invariants as shown in the figure. In case 1 the walker is initialised at the boundary between two phases, at lattice position $x=0$, here both sides of the lattice share the same topological invariant therefore bound states are not expected, and after four steps the walker spreads out ballistically. Case 2 shows the presence of a bound state with a pronounced peak near $x=0$ since each side of the lattice is a different topological phase. The bar graphs compare the measured (blue) and predicted (yellow) probabilities after the fourth step. Case 3 demonstrates that the presence of the bound state is robust against changes of parameters to case 2.

Topological effects, such as those present in topological insulators and many other fields of physics are currently one of the hottest topics in science and quantum simulation is equally well regarded as an exciting development in physics. This project combines these two topics elegantly, opening avenues for other proof-of-principle experiments in this area.

References

[1] M. A., Broome, *et. al.*, Phys. Rev. Lett., **104**, 153602 (2010).

[2] Y., Aharonov, *et. al.*, Phys. Rev. A, **48**, 1687 (1993).

[3] T., Kitagawa, *et. al.*, Phys. Rev. A, **82**, 033429 (2010).

[4] T., Kitagawa, *et. al.*, To appear in Nature Comms., e-print: arXiv:1105.5334v1 (2012).

Deterministic and Cascadable Conditional Phase Gate for Photonic Qubits

Christopher Chudzicki, Isaac Chuang, and Jeffrey H. Shapiro

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA

In optical quantum logic, qubit states are usually encoded using the presence or absence of a single photon in a preferred mode of the quantum electromagnetic field known as the principal mode. Logic gates can be high-fidelity only if they map input principal modes to output principal modes. Gates can be cascaded successfully if the input and output principal modes coincide. High-fidelity, cascadable single qubit-gates can be readily implemented using beam splitters and wave plates, but a significant challenge to implementing optical quantum information processing is the faithful realization of a deterministic and cascadable universal two-qubit photonic logic gate.

Cross-phase modulation (XPM) has often been proposed as a nonlinear optical process that might be used to construct such a universal gate, the conditional-phase gate, see, e.g., [1]. Although single-mode analyses of XPM-based gates are encouraging, continuous-time treatments [2] have shown that fidelity-degrading noise sources preclude high-fidelity π-rad conditional phase shifts at the single-photon level.

In this paper we present the continuous-time theory for a single-photon conditional-phase gate that, for sufficiently small nonzero ϕ, has high fidelity. Moreover, our gate is cascadable, in that it preserves the structure of the principal modes used to encode qubit information, and can therefore be cascaded to realize a high-fidelity conditional π-phase gate. The key components of our primitive gate are shown in Fig. 1 [3]. Horizontally-polarized and vertically-polarized rising-exponential principal modes—with space-dependent annihilation operators h_z and v_z—couple to a $\vee$-configuration atom trapped in a single-ended optical cavity. The control and target qubits are encoded as the presence or absence of single photons in these principal-mode polarizations. When only one photon—either h_z or v_z—illuminates the atom, the post-interaction photon carries an undesirable phase shift that is removed by using pulse-profile inverters ($\mathcal{I}$, accomplished by temporal imaging) to simulate a time-reversed interaction between the photon and an empty cavity. When both h_z and v_z photons illuminate the atom there is an additional nonlinear phase shift arising from the atom's inability to absorb more than one photon. Unfortunately, that desired nonlinear phase shift is accompanied by scattering out of the principal modes.
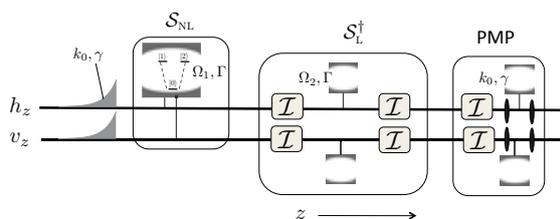
As shown in Fig. 2 [3], when the illumination is near resonance with the atom, a strong nonlinear phase shift is possible, but it comes with unacceptably low fidelity. The key to realizing a high-fidelity gate is then to employ off-resonance operation, wherein the nonlinear phase shift is small, but the fidelity lost to scattering out of the principal modes is even smaller. The quantum Zeno effect—enabled by the use of rising-exponential principal modes that are preferentially absorbed by an optical cavity—allows the principal-mode projection (PMP) stage in Fig. 1 to preclude coherent buildup of fidelity-reducing scattering from the principal modes. Cascading an appropriate number of our primitive gates could then yield a high-fidelity conditional π-phase gate. The weakness of XPM in a single $\vee$-configuration atom, however, makes this approach impractical. In particular, the fidelity of an N-gate cascade that realizes a conditional π-phase gate in this manner satisfies $F \approx 1 - 4.82 N^{-1/3}$, implying that more than 10^6 cascades will be required for 95% fidelity. Despite this drawback, we believe that PMP, based on the quantum Zeno effect, could be a valuable subroutine in the future of photonic quantum information processing. In particular, PMP together with stronger nonlinearities, e.g., the giant Kerr effect [4], could potentially realize a conditional π-phase gate with much more favorable scaling, i.e., $1 - F \propto N^{-1}$.
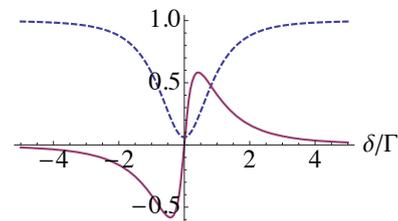
Figure 2: Nonlinear phase shift (solid line) and fidelity (dashed line) versus detuning δ normalized by the cavity decay rate Γ for the Fig. 1 system.

References

[1] I. L. Chuang and Y. Yamamoto, Phys. Rev. A **52,** 3489 (1995).

[2] J. H. Shapiro, Phys. Rev. A **73,** 062305 (2006); J. Gea-Banacloche, Phys. Rev. A **81,** 043823 (2010).

[3] C. Chudzicki, I. Chuang, and J. H. Shapiro, arXiv:1202.6640 [quant-ph].

[4] K. Koshino, S. Ishizaka, and Y. Nakamura, Phys. Rev. A **82,** 010301 (2010.)

Figure 1: Cascadable primitive gate with principal-mode wave number k_0, decay rate γ, and cavity decay rate Γ.

Ideal quantum reading of optical memories

Michele Dall'Arno[1,2], Alessandro Bisio[2] and Giacomo Mauro D'Ariano[2]

[1]*ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, E-08860 Castelldefels (Barcelona), Spain*
[2]*Quit group, Dipartimento di Fisica "A. Volta", via A. Bassi 6, I-27100 Pavia, Italy*

In the engineering of optical memories (such as CDs or DVDs), a tradeoff among several parameters must be taken into account. High precision in the retrieving of information is surely an indefeasible assumption, but also energy requirements, size and weight can play a very relevant role for applications. Clearly using a low energetic radiation to read information reduces the heating of the physical bit, thus allowing for smaller implementation of the bit itself. In the problem of *quantum reading* [1, 2, 3, 4, 5, 6] of optical memories one's task is to exploit the quantum properties of light in order to retrieve some classical digital information stored in the optical properties of a given media, making use of as few energy as possible. In practical implementations noise and loss can often be noticeably reduced, so that a theoretical analysis of the *ideal quantum reading*, namely lossless and noiseless, provides a theoretical insight of the problem and a meaningful benchmark for any experimental realization.

In this hypothesis two different scenarios can be distinguished. A possibility is the on-the-fly retrieving of information (e.g. multimedia streaming), where one requires that the reading operation is performed fast - namely, only once, but a modest amount of errors in the retrieved information is tolerable. In this context, denoted as *ambiguous quantum reading*, the relevant figure of merit is the probability P_e to have an error in the retrieved information. On the other hand for highly reliable technology the perfect retrieving of information is an issue. Then, *unambiguous quantum reading*, where one allows for an inconclusive outcome (while, in case of conclusive outcome, the probability of error is zero) becomes essential. Here, the relevant figure of merit is clearly the probability P_i of getting an inconclusive outcome.

We provide [2, 5] the optimal strategies for both scenarios, which exploit fundamental properties of the quantum theory such as entanglement, allowing for the ambiguous (unambiguous) discrimination of beamsplitters with probability of error P_e (probability of failure P_i) under any given threshold, while minimizing the energy requirement. The most general strategy for performing quantum reading consists in preparing a bipartite input state ρ (we allow for an ancillary mode), applying locally the unknown device and performing a bipartite POVM on the output state. So the problem of quantum reading can be formally stated as follows. For any set of two optical devices $\{U_1, U_2\}$ and any threshold q in the probability of error (failure), find the minimum energy input state ρ^* that allows to ambiguously (unambiguously) discriminate between U_1 and U_2 with probability of error P_e (probability of failure P_i) not greater than q, namely

$$\rho^* = \arg \min_{\rho \text{ s.t. } P(\rho,U) \leq q} E(\rho). \quad (1)$$

where $P(\rho, U)$ can either be given by P_e or P_i.

We prove [2, 5] that without loss of generality, the optimal input state ρ^* for (ambiguous or unambiguous) quantum reading can be taken pure and no ancillary modes are required. For the quantum reading of beamsplitters, we prove that the optimal input state ρ^* is given by a superposition of a NOON state and the vacuum, namely

$$|\psi^*\rangle = \frac{1}{\sqrt{2}}\alpha(|0, n^*\rangle + |n^*, 0\rangle) + \sqrt{1 - \alpha^2}|00\rangle, \quad (2)$$

where α and n^* depend on U_1 and U_2 [2, 5].

We compare [2] the optimal strategy for ambiguous quantum reading with a *coherent strategy*, reminiscent of the one implemented in common CD readers, showing that the former saves orders of magnitude of energy, moreover allowing for perfect discrimination with finite energy (see Fig. 1). Then, we present [5] experimental setups implementing ambiguous and unambiguous optimal strategies which are feasible with present day quantum optical technology, in terms of preparations of single-photon input states, linear optics and photodetectors.
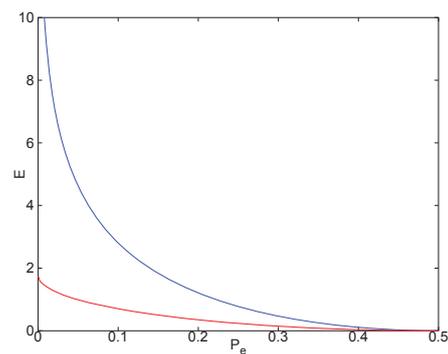
Figure 1: Tradeoff between energy E (expressed as the average number of photons) and probability of error P_e in the ambiguous quantum reading of $50/50$ beamsplitters with optimal strategy (lower line) and coherent strategy (upper line).

References

[1] S. Pirandola, Phys. Rev. Lett. **106**, 090504 (2011).

[2] A. Bisio, M. Dall'Arno, and G. M. D'Ariano, Phys. Rev. A **84**, 012310 (2011).

[3] S. Pirandola, C. Lupo, V. Giovannetti, S. Mancini, and S. L. Braunstein, New J. Phys. **13**, 113012 (2011).

[4] O. Hirota, arXiv:quant-ph/1108.4163v2.

[5] M. Dall'Arno, A. Bisio, G. M. D'Ariano, M. Miková, M. Ježek, and M. Dušek, Phys. Rev. A **85**, 012308 (2012).

[6] A. Bisio, M. Dall'Arno, G. M. D'Ariano, P. Perinotti, and M. Sedlak, (in preparation).

Experimental Demonstration of Quantum Digital Signatures

Patrick J. Clarke[1], **Robert J. Collins**[1], <u>**Vedran Dunjko**</u>[1], **Erika Andersson**[1], **John Jeffers**[2], **Gerald S. Buller**[1]

[1]*SUPA, School of Engineering and Physical Sciences, David Brewster Building, Heriot Watt University, Edinburgh, EH14 4AS, UK*
[2]*SUPA, Department of Physics, John Anderson Building, University of Strathclyde, 107 Rottenrow, Glasgow, G4 0NG, UK*

Quantum cryptography offers a promise that certain security-sensitive tasks can be performed *better* by exploiting quantum effects. Ideally, the security foundations of protocols realizing these tasks can be upgraded from the conjectural hardness of certain mathematical problems to information-theoretic grounds and the principles of quantum mechanics. A prime example where this has been achieved is Quantum Key Distribution (QKD) [1], which has been extensively studied for the last 28 years.

Here, we report the first experimental demonstration of Quantum Digital Signatures (QDS) [2] which also delivers on the aforementioned promise. QDS is the quantum answer to the task of the distribution and authentication of digital signatures, an increasingly relevant task in the modern information age. QDS offers a security based on the well-established quantum principles which, unlike in the case of classical known protocols for this task, can no longer be compromised given sufficient raw computing power, or perhaps yet to be discovered clever algorithms.

In all message verification schemes the security is based on existence of specific knowledge, reserved to the honest sender alone. In QDS, this knowledge is the classical description of quantum states ('quantum signatures') which are distributed to future message recipients. The message authentication is performed by checking whether the later disclosed classical descriptions match initially distributed quantum signatures.

We have constructed an experimental system permitting the sharing of quantum digital signatures, and the subsequent message authentication. The quantum signatures comprise a sequence of coherent states, the phase of which is known to the sender Alice alone. The schematic diagram of our set-up is given in Figure 1. The QDS protocol ensures security against forging - no message devised by an unauthorised sender will be authenticated by the recipients, and against repudiation - a message accepted by one recipient will also be accepted by all others. We have performed a detailed security analysis of our system. In the analysis of security against forging we identify two classes of attacks: *passive* and *active*. In the restrictive case of passive attacks the forger is honest throughout the signatures distribution phase. For this case, we prove the desired exponential decay of successful forging probabilities in terms of the signature length L:

$$p_{forging}^{passive} \leq 2 \exp\left(-\frac{2}{9} g^2 L\right) \qquad (1)$$

The parameter g is derived directly from experimental data, and for our system yields $g \approx 8 \times 10^{-4}$. The active attacks comprise individual and coherent strategies, akin to cases identified in QKD. We show that active individual attacks effectively decrease the parameter g in Equation by a value which can be made arbitrarily small given a sufficiently large L. Thus, the exponential decay of successful forging proba-
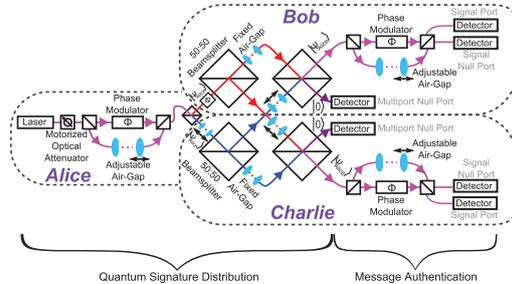
Figure 1: A diagram of the fiber-based experimental demonstration of quantum digital signatures. The core of the system realizes Quantum Signature Distribution, in which Alice (the sender) generates time multiplexed phase signal and reference coherent pulses, split into Bob's and Charlie's (the recipients) copies of quantum signatures. The quantum signatures are compared using a *multiport* realized by the four linked central balanced beam splitters. The multiport compares the quantum signatures, which is required for security against message repudiation. Finally, the signatures are validated in the Message Authentication component. Due to a lack of quantum memory, our system performs verification in run-time.

bilities can still be guaranteed. For the most general coherent active attacks we give arguments that they hold no advantage over active individual attacks. A full formalized proof is under current research.

For the security against repudiation, we identify separable and coherent (general) classes of attacks, and prove that in this case coherent strategies cannot help. We show that the successful repudiation probability decays exponentially quickly in L as

$$p_{repudiation} \leq d^{\frac{1}{3} g L} \qquad (2)$$

where the parameter g appears in the expression for security against forging in Eq. (1). The parameter d in Eq. (2) is a probability, and depends on the imperfections of our experimental realization. Based on a series of experiments and theoretical modelling this value was estimated at $d \approx 0.9$. Even for much larger values of d an upper bound of overall security of our system is dominated by the forging probability.

References

[1] C. Bennett and G. Brassard. *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, **175**:175–179, 1984.

[2] D. Gottesman and I. Chuang. *arXiv:quant-ph/0105032v2*, 2001.

[3] E. Andersson, M. Curty, and I. Jex. *Phys. Rev. A*, **74**:022304, 2006.

Quantum tomography of inductively created multi-photon states

E. Megidish, A. Halevy, T. Shacham, T. Dvir, L. Dovrat, and H. S. Eisenberg

Racah Institute of Physics, Hebrew University of Jerusalem, Jerusalem, Israel

Measuring the state of a quantum system is a task of high complexity. It requires many copies of the system at an identical state. Construction of the state's density matrix is achieved by projection measurements onto different states. If the quantum system is composed of n qubits, it is 2^n-dimensional and the number of required settings is 4^n. Even after sufficient amount of data about the state has been collected, the numerical process that is required to calculate the density matrix from the results scales as 16^n. The result of this scalability problem is that the largest state that has been fully characterized up-to-date is a W-state of 8 qubits [1].

We have recently introduced a resource efficient setup that can combine many polarization entangled photon pairs, generated at a single nonlinear crystal by type-II parametric down-conversion, into a multi-photon entangled state. As the pump laser is pulsed, consequent pump pulses can create consequent photon pairs. By delaying one of the two photons of each pair until the next pair is generated (see Fig. 1a), consequent pairs are fused on a polarizing beam-splitter (PBS). For example, if the delayed photon from the first pulse arrives at the PBS together with the photon on the short path from the second pair, selecting the outcome when each photon exits the PBS from a different port projects the four photons of the two pairs onto a four-photon GHZ state. The main advantage of this configuration is that without any addition of optical elements, it can keep entangling more pairs with this state if they are generated consequently.

The created GHZ states possess an interesting property. They are assembled from a few pairs by two-photon projecting fusion operations. Nevertheless, all of the pairs originate from the same source and all of the projection operations happen at the same PBS. As a result, the quantum state of all of the entangled pairs, described by their density matrix, is identical. Furthermore, the quantum process of all of the projections, described by a process matrix, is identical as well. Thus, by measuring these two matrices, the full knowledge of states of any photon number is achieved, even without accumulating their full statistics. The density matrix of these states can be precisely extrapolated by combining identical two-photon states with identical projections.

The quantum state tomography (QST) of the polarization entangled pairs (the delayed photon and the photon from the short path) resulted with 94% fidelity to a $|\psi^+\rangle$ state. The projection process matrix was measured using an ancilla assisted quantum process tomography. As the projection operates on two photons, where each of them is a part of an entangled state, the four-photon density matrix contains all the information about the two-photon process matrix. This is a result of the Choi-Jamiołkowski isomorphism. The four-photon density matrix requires 256 measurement settings. The first photon from the first pair and the last photon from the second pair share paths with the two middle photons. Thus, in order to individually rotate them we induced rotations through
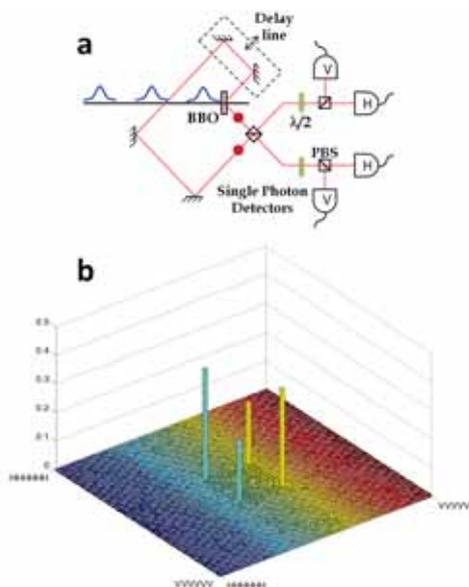
Figure 1: a: The multi-photon entangling setup. b: The calculated six-photon density matrix.

the non-locality of the entangled pairs. These rotations are not sufficient to cover all possible polarization projections. Therefore, 4 of the 16 settings of these two photons involved elliptical polarizations. The overall number of projections we have to perform is 272 in order to gather all of the required information.

After extracting the projection process matrix, we applied it again to combine an extra third pair to the four-photon measured state. The calculated six-photon density matrix is presented in Fig. 1b. The fidelity with a six-photon GHZ state is 64%, enough for the demonstration of genuine six-photon entanglement. We continued to add more pairs and calculated the density matrices for the eight- and ten-photon GHZ states. The fidelities of the density matrices from four photons to ten are $77\%, 64\%, 52\%$ and 45%, respectively. The corresponding visibilities at a $45°$ rotated polarization basis are $65\%, 47\%, 36\%$ and 26%. Genuine multi-partite entanglement for GHZ states requires fidelities above 50% and thus we currently satisfy this condition up to eight photons. A simple non-locality criterion that was derived by Mermin [2] is well satisfied for all the calculated visibilities. In order to interpret these results well, the measurement errors are required. We are currently working on this calculation.

References

[1] H. Häffner *et al.*, Nature **438**, 643 (2005).

[2] N.D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).

Experimental emulation of coherent quantum effects in biology

Devon N. Biggerstaff[1], Thomas Meaney[2], Ivan Kassal[1], <u>Alessandro Fedrizzi</u>[1], Martin Ams[2], Graham D. Marshall[2], Michael J. Withford[2] and Andrew G. White[1]

[1]ARC Centre for Engineered Quantum Systems, ARC Centre for Quantum Computer and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane, QLD 4072, Australia
[2]ARC Centre for Ultrahigh Bandwidth Devices for Optical Systems, Centre for Quantum Science and Technology, MQ Photonics Research Centre, Department of Physics and Astronomy, Macquarie University, North Ryde, NSW 2109, Australia

The discovery of quantum coherence in photosynthetic processes [1] has sparked enormous interest in the exact role of quantum effects in biology. Some of the biggest open questions are how robust the coherent dynamics in photosynthesis is; whether it really assists energy transport; and whether it is optimised by natural selection or just a random by-product. These questions are difficult to address experimentally, since the structure of a biological complex cannot usually be modified. Our goal is to build emulators that allow us to easily vary the structure, the degree of coherence, and the environment with the goal of understanding how these factors interact in modifying quantum transport.

Here we report the coherent simulation in a 3D direct-write waveguide array of the exciton delocalization dynamics in a well-studied photosynthetic complex, the B850 subunit of the light-harvesting system II (LHII) of *Rhodobacter sphaeroides* purple bacteria, see figure 1(a). When a photon is absorbed in one of these bacteria, it creates electronic excitations, quantised as excitons, in complexes of chromophores. These chromophores are coupled via the Coulomb interaction and electron exchange, which allows excitons to move between sites until the they are either lost through recombination or successfully trapped at target receptor sites and turned into useful chemical energy. Ignoring environmentally-induced decoherence and absorption, and considering the case where only one exciton is present in the system—which is often the only relevant scenario for photosynthetic organisms—the dynamics of such a system can be described by a Hamiltonian which contains the excitation energies of the individual sites along the diagonal and the coupling terms in the off-diagonal elements. With a reasonable cutoff of small coupling parameters, this type of Hamiltonian can be emulated by photonic evolution in an array of evanescently coupled waveguides, where the site energies correspond to the effective waveguides refractive indices, and the coupling terms to the inter-waveguide coupling. These arrays can be written into glass using a femtosecond-laser, direct-write process—a powerful technique which has been proven useful for photonic quantum information [2] and quantum walk applications [3].

We used this technique to write 16 straight waveguides arranged along two concentric circles, with the waveguide positions determined by 3 parameters, figure 1(b). We analytically and numerically optimised these parameters to obtain the best possible approximation of the spectroscopically determined *Rhodobacter* Hamiltonian. Measurements of coherent 820 nm light launched into the resulting waveguide array at different simulation lengths allowed us to observe the coherent evolution of light governed by the approximated Hamiltonian and to confirm that our dynamics of our photonic
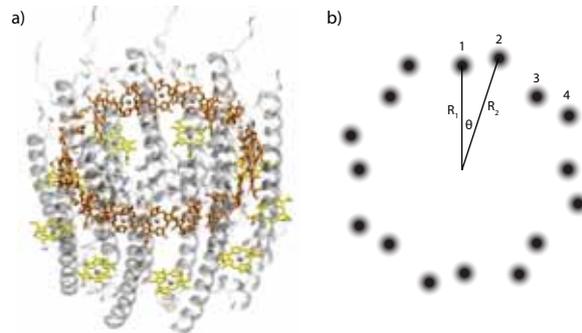
Figure 1: a: The LH-2 complex responsible for harvesting light in purple bacteria. The chlorophyll molecules (in orange) are described by a 16×16 Hamiltonian which has been experimentally determined. b: Geometry of an array of 16 waveguides approximating the rhodobacter Hamiltonian. The coupling between individual waveguides i and j is proportional to e^{-r_{ij}/r_0}, wherer r is the inter-waveguide distance. We arranged the geometry such that the effective waveguide Hamiltonian is as close as possible to the biological Hamiltonian.

emulation achieved good overlap with the target Hamiltonian.

Our results show that waveguide photonics can emulate real-world Hamiltonians, providing a controlled laboratory setting for studying quantum effects in biology. While we restricted our measurements to the realistic case of single-photon excitations, it is feasible to extend this work to the study of multi-photon processes [3] and of the potential generation of entanglement or other non-classical correlations in biological processes [4].

References

[1] E. Harel and G. S Engel, *Proceedings of the National Academy of Sciences* **109**, 706–711 (2012)

[2] G. D. Marshall, A. Politi, J. C. F. Matthews, P. Dekker, M. Ams, M. J. Withford and J. L. O'Brien *Optics Express* **17** 1254654 (2009)

[3] J. O. Owens, M. A. Broome, D. N. Biggerstaff, M. E. Goggin, A. Fedrizzi, T. Linjordet, M. Ams, G. D. Marshall, J. Twamley, M. J. Withford and A. G. White, *New Journal of Physics* **13**, 075003 (2011).

[4] K. Bradler, M. M. Wilde, S. Vinjanampathy, D. B. Uskov, *Physical Review A* **82**, 062310 (2010).

Heralded processes on continuous-variable spaces as quantum maps

Franck Ferreyrol[1,2], **Nicolò Spagnolo**[3], **Rémi Blandino**[1], **Marco Barbieri**[1], **Rosa Tualle-Brouri**[1,4] **and Philippe Grangier**[1]

[1]*Groupe d'Optique Quantique, Laboratoire Charles Fabry, Institut d'Optique, CNRS, Université Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau cedex, France*
[2]*Centre for Quantum Dynamics and Centre for Quantum Computation and Communication Technology, Griffith University, Brisbane 4111, Australia*
[3]*Dipartimento di Fisica, Sapienza Universita di Roma and CNISM, I-00185, Roma, Italy*
[4]*Institut Universitaire de France, 103 boulevard Saint-Michel, 75005 Paris, France*

Maps and quantum process tomography are commonly used to describe quantum processes in discrete-variable space, but much rarer in the continuous-variable domain. A tomographic technique that can be used in continuous-variable experiments, including heralded processes, has been proposed [1], but it still uses the tensorial form $\mathcal{E}_{l,k}^{n,m}$ of quantum maps, which is not well adapted to continuous variables. This technique is based around transformations of the density matrix which, despite is great usefulness for discrete variables, does not clearly express some aspects of continuous-variable systems. And as some basic continuous-variable states are barely recognisable from the density matrix, some basic processes — for example squeezing, phase rotation and displacement operators — are hard to recognise in the tensor form.

The Wigner function circumvent those difficulties for quantum states, so a better way to represent continuous-variable maps would be to have a tool for transforming the Wigner function. Such a representation exists [2], but it has only been used for process corresponding to a unitary operator, and never to heralded processes. We propose a technique for representing generic maps that generalizes this formalism and explicitly related it to the tensor expression and the Kraus decomposition.

In this formalism, the map is expressed as a transfer function which transforms a Wigner function into another Wigner function. The discrete sum on all the elements of the density matrix, in the tensor form, is replaced by an integral on the whole phase-space:

$$W'(x', p') = \int f(x', p', x, p) W(x, p) dx dp \qquad (1)$$

which is close to the probability transition used for Markovian process in phase-space, and has similar properties. Nevertheless, as for the Wigner function, the quantum transfer function can take negative values, and so it cannot be interpreted as a true probability transition.

We have developed the methods for building an analytic expression for the transfer function that models a particular experiment, starting with some simple transfer functions corresponding to some elementary processes and then combining them in order to build the complete function. We have also studied the case of wrong heralding, which is generally modelled with the use of some non-linear operations, and showed that it can be expressed as linear operations, and thus can be included in the transfer function.

Finally, we have reconstructed the transfer function of two recent experimental heralded processes : the noiseless amplifier [3] and photon addition [4]. In both cases, since the process doesn't depend of the phase of the input state, the transfer function can be expressed as a function $f(r', r, \theta)$ of the radial quadratures ($r' = \sqrt{x'^2 + p'^2}$ and $r = \sqrt{x^2 + p^2}$) and the phase between the input and the output ($\theta = \cos^{-1}\left(\frac{\vec{r} \cdot \vec{r'}}{r r'}\right)$).
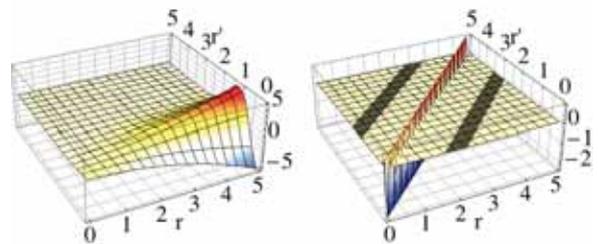
Figure 1: a: map of the noiseless amplifier without experimental imperfections for $\theta = 0$. b: map of photon addition with experimental imperfections for $\theta = 0$.

From the resulting graphs (fig. 1) it is possible to directly observe the main features of the process: variation of the success probability with the input amplitude through height of the peaks, relation between the output and input amplitude represented by the position of positive peaks, introduction of negativity with the negatives peaks. All those characteristics are hardly visible in the tensor form. As for the Wigner function, the negativity of the transfer function is a sign of the quantumness of the process, however the negativity of the transfer function seems to be more important and more resistant to experimental imperfections than the negativity of the Wigner function of output states.

Our quantum maps formalism for continuous variable is therefore particularly clear and useful for the analysis of the process. It gives a way of quantifying not only the effect of the process but also the parasite effects of imperfections in an input-independent way, is adapted to the specificity of continuous variables, and is linked to the common tools used in this domain.

References

[1] M. Lobino et al., Science, **322**, 563 (2008)

[2] M.V. Berry et al., Ann. Phys, **122**, 26 (1979)

[3] F. Ferreyrol et al., Phys. Rev. Lett. **104**, 123603 (2010)

[4] M. Barbieri et al., Phys. Rev. A **82**, 063833 (2010)

Photon-detection-induced Kennedy receiver for binary-phase coded PPM

__Jian Chen__[1], Jonathan L. Habif[1], Zachary Dutton[1], and Saikat Guha[1]

[1]*Disruptive Information Processing Technologies Group, Raytheon BBN Technologies, Cambridge, MA 02138, USA*

Discriminating two coherent states is impossible since their quantum states are never mutually orthogonal. Achieving the ultimate quantum limit for capacity, the Holevo capacity, is possible via coherent states using joint-detection measurements on long codeword blocks [1], although optical implementations remain unknown. We report the experimental demonstration of a joint-detection receiver for demodulating binary-phase-coded (BPSK) pulse-position-modulation (PPM) codewords (that is, PPM codewords along with their π-phase-shifted counter-parts), which was recently shown to be able to achieve fundamentally superior channel capacity to any symbol-by-symbol measurement scheme [2, 3].

The receiver proposed in [2] can take input states as phase-coded PPM. It proceeds by performing direct detection (DD) to determine the pulse slot, followed by using the Dolinar receiver on the remainder of the pulse energy in that slot. In [3] it was shown that this is indeed the optimal receiver, from a capacity point of view, for this modulation format. The red curve in Fig. 1 shows the photon information efficiency (PIE)—capacity (in bits per slot) divided by mean photon number $\bar{n}$ per time slot, as a function of $\bar{n}$. It exceeds the Shannon capacities of on-off-keyed (OOK) modulation with DD (black curve), and that of PPM with DD by a somewhat larger margin (blue curve). In place of the Dolinar receiver, a Generalized-Kennedy (GK) receiver [4] can be employed to achieve nearly the same performance, which is the approach we take here. Combined with the optical *Green-Machine* [2], this receiver can also demodulate the BPSK first-order Reed-Muller code. In this case, the capacity achieved by our receiver far exceeds that of BPSK paired with either the homodyne receiver (magenta curve) or even the Dolinar receiver (green curve)—the latter being the receiver which can discriminate the single-copy BPSK coherent states with the minimum probability of error.
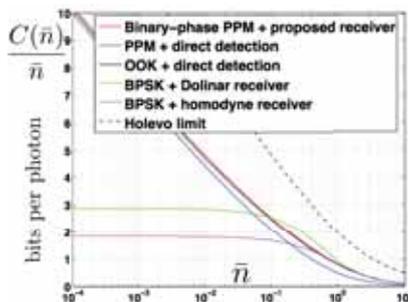
Figure 1: PIE of our receiver acting on phase coded PPM (red curve) vs. $\bar{n}$, PPM with DD (blue curve), and unconstrained OOK with DD (black curve). The green and magenta curves show, respectively, the Shannon limits for BPSK with a Dolinar receiver and homodyne receiver.

Fig. 2 shows the experimental setup where a flat-top pulse train with pulse duration of 200 ns and repetition rate of 1 MHz is generated by a SWL at 688 nm and an I-EOM1. The pulse train is then divided into a signal arm and a nulling arm by a free-space beamsplitter. BPSK-PPM codewords are implemented via P-EOM and I-EOM3. I-EOM2 acts as a high-speed shutter on the nulling arm. Demodulation is implemented by a single-photon-detection triggered GK receiver. Nulling of the GK receiver happens at a fiber coupler which transmits 99% of the signal. An FPGA circuit opens the I-EOM2 shutter every time a click is generated by the SPD.
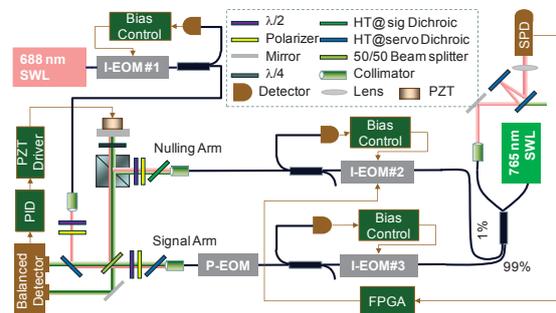
Figure 2: Experimental setup. SWL: single wavelength laser, PZT: Piezoelectric Transducer, I(p)-EOM: electro-optic intensity (phase) modulator, SPD: single photon detector, FPGA: field-programmable gate array.

Since carrier phase and pulse amplitude noise degrades the nulling quality, hence probability of error, active locking is introduced to stabilize the relative phase between the nulling and signal arms and DC bias points of the EOMs. A servo SWL delivers a 765 nm signal into the nulling system from reverse direction to minimize optical noise from the servo laser. Balanced detection and a PZT driven mirror are used in to detect and compensate the phase noise. DC bias points of the EOMs are locked by dithering the EOM at 1 kHz around the desired locking points and tapping out the servo laser as the control signal to the locking electronics.

In conclusion, we report the first experimental demonstration of a joint-detection receiver able to exceed the Shannon capacity of any symbol-by-symbol optical measurement.

References

[1] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).

[2] S. Guha, Z. Dutton, J. H. Shapiro, p.274, ISIT 2011.

[3] B. I. Erkmen, K. M. Birnbaum, B. E. Moision and S. J. Dolinar, to appear in Proceedings of the SPIE in 2011.

[4] K. Tsujino, *et al.*, Phys. Rev. Lett. **106**, 250503 (2011).

Narrowband Source of Correlated Photon Pairs via Four-Wave Mixing in Atomic Vapour

Bharath Srivathsan[1]**, Gurpreet Kaur Gulati**[1]**, Chng Mei Yuen Brenda**[1]**, Gleb Maslennikov**[1]**, Dzmitry Matsukevich**[1, 2]**, Christian Kurtsiefer**[1, 2]

[1]*Centre for Quantum Technologies, National University of Singapore, Singapore 117543*
[2]*Department of Physics, National University of Singapore, Singapore 117542*

Many quantum communication protocols require entangled states of distant qubits which can be implemented using photons. To efficently transfer entanglement from photons to stationary qubits such as atoms, one requires entangled photons with a frequency bandwidth matching the absorption profile of the atoms. In our setup, a cold Rb^{87} atomic ensemble is pumped by two laser beams (780nm and 776nm) resonant with the $5S_{1/2} \to 5P_{3/2} \to 5D_{3/2}$ transition. This generates time-correlated photon pairs (776nm and 795nm) by nondegenerate four-wave mixing via the decay path $5D_{3/2} \to 5P_{1/2} \to 5S_{1/2}$. Coupling the photon pairs into single mode fibres and using silicon APDs, we observe $g^{(2)}$ of about 2000 and pairs to singles ratio of 11.2

References: Willis, R. T. et al. Phys. Rev. A 79, 033814 (2009) Du, S-W. et al. Phys. Rev. Lett. 100, 183603 (2008) Chaneliere, T et al. Phys. Rev. Lett. 96, 093604 (2006)

Interfacing Microwave Photons with Rydberg Atoms on a Superconducting Chip

S. Filipp[1], T. Thiele[1], S. D. Hogan[2], J. A. Agner[2], F. Merkt[2] and A. Wallraff[1]

[1]*Quantum Device Lab, ETH Zurich, CH-8093 Zurich, Switzerland*
[2]*Laboratory of Physical Chemistry, ETH Zurich, CH-8093 Zurich, Switzerland*

A major challenge in the field of quantum information processing is to combine a fast quantum processor – potentially based on solid state electronic devices – with a long-lived quantum memory realized for example in electronic or spin states of atoms. We are pursuing the goal to form such a hybrid quantum system by combining superconducting qubits and atoms in highly-excited Rydberg states on a single chip device. For both systems, suitable qubit transitions are available in the microwave domain, suggesting the use of quasi-one-dimensional microwave resonators as a photonic interface to transfer coherent quantum information between atoms and solid-state qubits.

As a first step we have induced transitions between atomic Rydberg states by microwave photons from a coplanar transmission line [1]. In our setup – shown in Figure 1 – metastable Helium atoms are produced by an electric discharge after a pulsed supersonic beam expansion. The atoms are excited to their $33p$ Rydberg state by a 313 nm UV-laser inside a cold chamber. The cryogenic region can be cooled to temperatures below 5 K, at which blackbody transitions between different Rydberg states, a major relaxation channel at room temperature, can be significantly reduced. The atoms then pass over a printed circuit board (PCB) containing the coplanar transmission line. Applying a resonant microwave pulse at 30.7 GHz results in Rabi oscillations between the $33p$ and $33s$ state with a typical period of 30 ns when varying the duration of the pulse (Figure 2).

The observed coherence time is limited by microwave field inhomogeneities across the dimension of the Rydberg ensemble as well as by stray electric fields emanating from the PCB surface. Spectroscopic measurements of narrow-linewidth microwave transitions between Rydberg states together with atom trajectory simulations support the theoretically predicted dependence of the stray electric field strength on the inverse square of the atom-surface distance [2]. Additional dephasing at a timescale of ≈ 250 ns is attributed to the atomic motion in inhomogeneous electric fields. Rydberg atoms can thus serve as sensitive probes of surface electric fields.
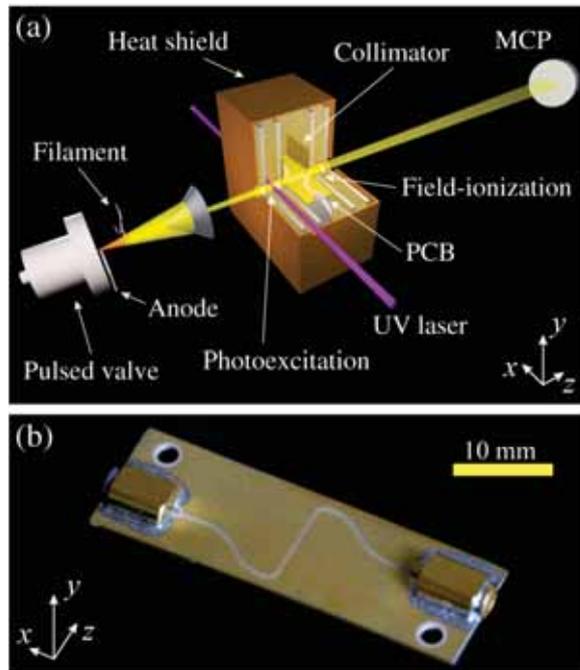
Figure 1: (a) Schematic diagram of the experimental apparatus. (b) Printed circuit board (PCB) containing the coplanar microwave waveguide.

Figure 2: Rabi oscillations in the population of the $33s$ state. An increase of the microwave power from (a) 4 μW to (b) 10 μW leads to a corresponding increase in the oscillation frequency.

To coherently couple Rydberg atoms to microwave photons at the level of single energy quanta, a superconducting coplanar waveguide resonator has to be used. We have fabricated resonators on a niobium-titanium-nitride (NbTiN) coated sapphire chip and measured quality factors up to 4000 at a temperature of 4 K and a frequency of 20 GHz, matching the transition frequency between $38p$ and $38s$ states of Helium. Passing the atoms over the resonator will then lead to a modified transmission of microwave signals through the resonator due to the large collective dipole coupling between Rydberg atoms and microwave photons. In further experiments, on-chip trapping, collimation and guiding elements will be realized to gain control over position and size of the atomic ensemble as the next step towards hybrid quantum computation.

References

[1] S. D. Hogan, J. A. Agner, F. Merkt, T. Thiele, S. Filipp, A. Wallraff, Phys. Rev. Lett, **106**, 063004 (2012).

[2] J. D. Carter and J. D. D. Martin, Phys. Rev. A **83**, 032902 (2011).

Qubus ancilla-driven quantum computation

Katherine Louise Brown[a,b]**, Suvabrata De**[a]**, <u>Viv Kendon</u>**[a]** and Bill Munro**[c,d]

[a]*School of Physics and Astronomy, University of Leeds, LS2 9JT, United Kingdom*
[b]*School of Physics and Astronomy, Louisiana State University, Baton Rouge, LA 70808, United States*
[c]*National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*
[d]*NTT Basic Research Laboratories, 3-1, Morinosato Wakamiya Atsugi-shi, Kanagawa 243-0198, Japan*

Using an ancilla (qubit or other quantum system) to enact the gates between qubits provides several advantages over direct interactions. Qubits do not need to be moved next to each other for gates (the ancilla moves instead), and multiqubit gates can often be performed with a single ancilla interaction per qubit. While our results are relevant for ancilla systems in general [1], we have focused on the qubus quantum computer [2, 3] which uses a continuous-variable ancilla, such as a coherent state of light. The qubus system generates gates between qubits deterministically without the need for measurement, but does require an interaction between the field and a matter qubit [3]. By entangling one qubit to each quadrature, then disentangling them in the same order, a geometric phase gate is performed between the qubits leaving the coherent state disentangled, see figure 1.

(a)   (b)
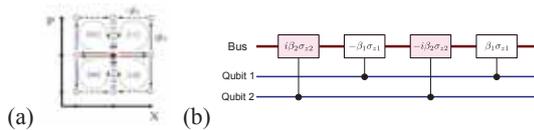
Figure 1: The basic qubus controlled-phase gate: (a) the phase-space displacements of the bus, (b) the operation sequence, shaded operations are on the momentum quadrature.

The qubus has advantages over single particle ancillas since coherent states are easier to produce, control and measure, and are robust against certain types of loss [4]. A coherent state can entangle an arbitrary number of qubits to each of its two quadratures, and this can provide significant extra efficiencies compared with single particle ancillas of fixed dimension. We have demonstrated how to obtain these efficiencies in detail for building cluster states [4, 5], and for quantum simulation [6]. Performing a QFT on n qubits requires
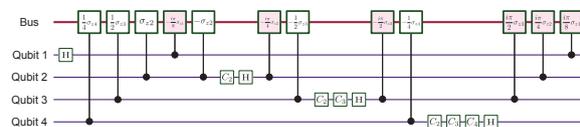
Figure 2: QFT on 4 qubits using qubus operations.

a total of $\frac{n(n-1)}{2}$ controlled-rotation gates. With the qubus, these can be performed using a controlled-phase gate plus single-qubit corrections on each qubit [6]. In a naïve implementation, where each controlled-phase gate requires four operations to perform, we would require $2n(n-1)$ interactions with the bus. Savings are obtained by leaving the qubits entangled with the bus for several consecutive operations, with the constraint that we need to apply Hadamard gates between each set of controlled-phase operations (since they don't commute).

We have demonstrated how to reduce the number of operations required when performing a QFT on the qubus quantum computer to $4n - 2$ per QFT. This is linear in the number of qubits n, compared with $n^2 + n$ for the simple gate sequence, and $n \log n$ for the best known gate sequence [7]. This implies that continuous-variable ancillas are equivalent to the quantum circuit model with unbounded fan-out, and measurement-based quantum computing [8]. These efficiencies using the qubus will thus apply in a wide range of situations.

References

[1] J. Anders, D. K. L. Oi, E. Kashefi, D. E. Browne, and E. Andersson. Ancilla-driven universal quantum computation. *Phys. Rev. A*, 82(2):020301, 2010.

[2] P. van Loock, W. J. Munro, Kae Nemoto, T. P. Spiller, T. D. Ladd, Samuel L. Braunstein, and G. J. Milburn. Hybrid quantum computation in quantum optics. *Phys. Rev. A*, 78:022303, 2008.

[3] T. P. Spiller, Kae Nemoto, Samuel L. Braunstein, W. J. Munro, P. van Loock, and G. J. Milburn. Quantum computation by communication. *New J. Phys.*, 8:30, 2006.

[4] Clare Horsman, Katherine L. Brown, William J. Munro, and Vivien M. Kendon. Reduce, reuse, recycle for robust cluster-state generation. *Phys. Rev. A*, 83(4):042327, Apr 2011.

[5] K. L. Brown, C. Horsman, V. M. Kendon, and W. J. Munro. Layer by layer generation of cluster states, 2011. http://arxiv.org/abs/1111.1774v1.

[6] Katherine L. Brown, Suvabrata De, Viv Kendon, and William J. Munro. Ancilla-based quantum simulation. *New J. Phys.*, 13:095007, 2011.

[7] L. Hales and S. Hallgren. In *Proc. 41st FoCS*, 515, 2000.

[8] D. Browne, E. Kashefi, and S. Perdrix. In *TQC*, volume 6519 of *LNCS*, 35–46. Springer, 2010.

Time-bin photonic state transfer to electron spin state in solids

Hideo Kosaka[1*], **Takahiro Inagaki**[1], **Ryuta Hitomi**[1], **Fumishige Izawa**[1], **Yoshiaki Rikitake**[2], **Hiroshi Imamura**[3], **Yasuyoshi Mitsumori**[1] **and Keiichi Edamatsu**[1]

[1]*Research Institute of Electrical Communication, Tohoku University, Sendai 980-8577, Japan*
[2]*Sendai National College of Technology, Sendai 989-3128, Japan*
[3]*Nanosystem Research Institute, AIST, Tsukuba 305-8568, Japan*

Time carried with photons can be a superposition state of two time bases, which is called a time-bin state and is used to secure communication. In the same way, spin carried with electrons can be a superposition state of up/down spin bases and offers the promise of universal computation. Here we demonstrate the direct superposition-state transfer from a time-bin state of photons to a spin state of electrons in a semiconductor nanostructure.

The transfer is based on the relative difference in spin dynamics between an electron and hole that are pair-created by a photon forming a coherent exciton and are naturally entangled but can be disentangled after their different time evolutions in the spin Bloch space. The photonic state encoded on time is decoded by dynamically erasing "which-path" information on the hole spin to restore the state into only the electron spin with the help of time-spin hybrid interference. The developed time-bin transfer scheme is applicable for quantum media conversion [1,2] from any energy-range of photons to various solid-state qubit media.

We experimentally demonstrate that not only the population of the up/down spin states but also an arbitrary coherent superposition state can be created by the transfer. The transfer is achieved in two extreme cases: an electron-precession (EP) case, where the electron spin precesses while the hole spin stays fixed, and a hole-precession (HP) case, where the hole spin precesses while the electron spin stays fixed. The obtained transfer fidelity amounts to 82% in the EP case (Fig. 1) and 58% in the HP case [3].

Operating principle of the time-bin transfer scheme is as follows. The targeting process is $\alpha|0\rangle_{ph} + \beta|1\rangle_{ph} \rightarrow \alpha|\uparrow\rangle_e + \beta|\downarrow\rangle_e$, where $|0\rangle_{ph}$ and $|1\rangle_{ph}$ are the first/second photon time-bin states, $|\uparrow\rangle_e$ and $|\downarrow\rangle_e$ are the up/down electron spin states. In the EP case, two input pulses are co-polarized to create the same spin state: $|0\rangle_{ph} \rightarrow |\downarrow\rangle_e \otimes |\Uparrow\rangle_h$ and $|1\rangle_{ph} \rightarrow |\downarrow\rangle_e \otimes |\Uparrow\rangle_h$. Without any spin dynamics, the input pulses always generate the same spin state. However, if the time separation t_s between two pulses is synchronized with the electron spin precession to flip up leaving the hole spin unchanged, the spins created at time-bin 0 evolve into $|\uparrow\rangle_e \otimes |\Uparrow\rangle_h$ by time-bin 1. The input time-bin state will then be transferred to the spin state of the electron with the fixed hole spin:

$$\alpha|0\rangle_{ph} + \beta|1\rangle_{ph} \rightarrow (\alpha|\uparrow\rangle_e + \beta|\downarrow\rangle_e) \otimes |\Uparrow\rangle_h, \quad (1)$$

where the electron and hole spin states are in a separable product state. In the HP case, two input pulses are cross-polarized to create different spin states: $|0\rangle_{ph} \rightarrow |\uparrow\rangle_e \otimes |\Downarrow\rangle_h$ and $|1\rangle_{ph} \rightarrow |\downarrow\rangle_e \otimes |\Uparrow\rangle_h$. Without any spin dynamics, entangled spin states are generated:

$$\alpha|0\rangle_{ph} + \beta|1\rangle_{ph} \rightarrow \alpha|\uparrow\rangle_e|\Downarrow\rangle_h + \beta|\downarrow\rangle_e|\Uparrow\rangle_h, \quad (2)$$

where the hole decoherence or extraction drives the electron in an incoherent mixed state. However, the synchronization of t_s with the hole precession time to flip up results in the same coherent transfer as in eq. (1).

In experiments, we used a non-doped single quantum well structure made of $Ga_{0.35}Al_{0.65}As/GaAs(20nm)/Ga_{0.35}Al_{0.65}As$, which allows the two extreme cases mentioned above. A heavy hole, which does not precess under an in-plane magnetic field, was used in the EP case, while a light hole, which precesses much faster than the electron spin, was used in the HP case.

From measurements, we inferred the spin Bloch vectors of the transferred state (**Fig. 1(b)**). Although the dephasing of the exciton distorts spherical photonic Bloch space (**Fig. 1(a)**) into an ellipsoid, coherence is maintained after the transfer.

Since the developed time-bin transfer scheme requires only a two-level system with different state dynamics, the potentially applicable materials include quantum dots, donor impurities in semiconductors, and color centers in diamond. The scheme is especially useful when polarization modes are not well degenerate in structures such as photonic crystal waveguides, microwave striplines, cavities and quantum dots. The scheme allows us to interface any frequency range of photons, including visible, infrared, microwave and radiofrequency, with various kinds of spin, including a hole spin, nuclear spin and superconducting flux qubit, for the purpose of building hybrid quantum systems including quantum repeaters.
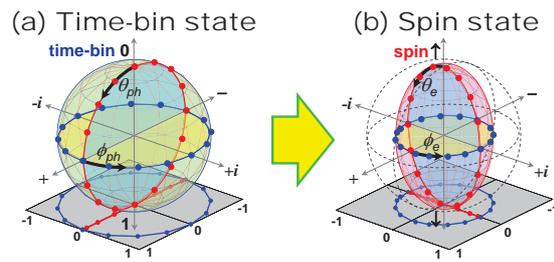
Figure 1: Bloch sphere representations of the input time-bin photonic state (a) and the transferred electron spin state (b). Dotted lines show the ideal Bloch sphere.

References

[1] H. Kosaka et al., Phys. Rev. Lett. **100**, 096602 (2008).

[2] H. Kosaka et al., Nature, **457**, 702 (2009).

[3] H. Kosaka et al., Phys. Rev. A, in printing.

Atoms and molecules in arrays of coupled cavities

Guillaume Lepert[1], **Michael Trupke**[1], **Ed Hinds**[1], **Jaesuk Hwang**[1], **Michael Hartmann**[2] **and Martin Plenio**[3]

[1]*Centre for Cold Matter, Imperial College London*
[2]*Technische Universität München*
[3]*Universität Ulm*

The field of cavity QED has witnessed spectacular progress over the last couple of decades: photon blockade, single photon non-linearities, phase gates, strong coupling have all been successfully demonstrated with cold atoms, and state-of-the art cavities showcase finesses close to 10^6.

Further significant advances in cavity QED will be based on the interconnection of many cavities into complex networks (**coupled-cavities QED**), but this will require a major technological shift from bulky free space optical systems towards integrated photonics. Significant steps have already been taken in that direction, such as the successful operation of fibred micro-cavities [1]. Such systems typically do not reach the very high finesse of bulky cavities, but this is compensated by mode volumes smaller by an order of magnitude.

We present here an extension of these microcavities where the fibres have been replaced by waveguide chips [2] (see Figure 1). Atoms sit in free space microcavities, facing waveguides. The latter can be routed and coupled to each other to connect a potentially very large number of microcavities. This design offers a degree of control unavailable to other proposed coupled-cavities system like photonic crystals, since each of the atom-microcavity couplings and each of the waveguide-waveguide couplings can be individually adjusted (using piezo or capacitive actuators and integrated thermal phase shifters, respectively).

In such a **hybrid quantum system**, the atoms effectively mediate photon-photon interactions by exploiting the cavity field enhancement which, by saturating the atomic transition even when only one photon is present inside the cavity, generates a non-linear phase shift. We describe the basic operating principles of the device and demonstrate successful operation of some of the basic building blocks, such as:

- optimisation of UV-written waveguide chips for operation at 780nm (Rubidium)
- on-chip cross-couplers
- phase shifters
- strong coupling between a waveguide resonator and a microcavity.

The waveguide chips are fabricated at the University of Southampton by UV-writing [3], a technique that offers rapid prototyping, low cost and high flexibility and is therefore an ideal platform in a research environment.

Atoms are not the only quantum system that can be placed in our array of microcavities. Quantum dots and diamonds NV centres are also suitable, and we are currently investigating cryogenic dye molecules [4].

We also theoretically explore experiments that could be performed with the finished device. Detailed analysis of two basic scenarios with two coupled cavities are presented: spectroscopy of a Jaynes-Cummings system, and dynamics of a spin system. Our device would also be ideal for more advanced physics, including quantum phase transitions in a Bose-Hubbard model [5], high fidelity entanglement transport along a tailored spin chain [6], many-photon fast entanglement and cluster state generation, and more generally as a quantum emulator.
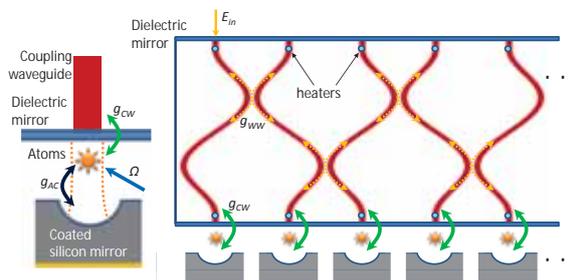
Figure 1: Schematic representation of the device under construction. Left is a close-up of the free space microcavity with atoms, coupled to a waveguide. Right shows the cavity array. Both end facets of the chip are coated with a dielectric mirror, so that each waveguide is an additional resonator, thus confining photons within the device, while waveguides are evanescently coupled to each other.

References

[1] M. Trupke et al, Atom Detection and Photon Production in a Scalable, Open, Optical Microcavity, *Physical Review Letters* **99**, 063601 (2007).

[2] G. Lepert et al, Arrays of waveguide-coupled optical cavities that interact strongly with atoms. *New Journal of Physics* **13**(11), 113002 (2011).

[3] G. Lepert et al, Demonstration of UV-written waveguides, Bragg gratings and cavities at 780 nm, and an original experimental measurement of group delay, *Optics Express* **19**, 24933 (2011).

[4] J. Hwang and E. Hinds, Dye molecules as single-photon sources and large optical nonlinearities on a chip, *New Journal of Physics* **13**, 085009 (2011).

[5] M. Hartmann et al, Quantum many-body phenomena in coupled cavity arrays, *Laser & Photonics Review* **2**, 527-556 (2008).

[6] S. Giampaolo, and F. Illuminati, Long-distance entanglement and quantum teleportation in coupled-cavity arrays, *Physical Review A* **80**, 4-7 (2009).

Photon number discrimination using only Gaussian resources and measurements

H. M. Chrzanowski[1], **J. Bernu**[1], **B. Sparkes**[1], **B. Hage**[1], **A. Lund**[2], **T. C. Ralph**[3], **P. K. Lam**[1] **and T. Symul**[1]

[1]*Centre for Quantum Computation and Communication Technology, The Australian National University*
[2]*Centre for Quantum Computation and Communication Technology, Griffith University*
[3]*Centre for Quantum Computation and Communication Technology, University of Queensland*

Central to the weirdness of quantum mechanics is the notion of wave-particle duality, where classical concepts of particle or wave behaviour alone cannot provide a complete description of quantum objects. When investigating quantum systems, information concerning one description is typically sacrificed in favour of the other, depending on which description fits your endeavour. Perhaps unjustly, probing the continuous variables of an infinite Hilbert space, such as the amplitude and phase of a light field, often viewed as less interesting than probing the quantized variables of a quantum system, due to the fact that when probing the continuous variables of a quantum system alone, one is restricted to transformations that map Gaussian states onto Gaussian states. Nevertheless, the idea of measuring the corpuscular nature of light with only CV techniques has been theoretically [1, 2] and experimentally [3, 4, 5] investigated.

We present a continuous variable technique enabling us to exploit the quantized nature of light, and present an application of the technique in accessing the statistics of the non-Gaussian k photon subtracted squeezed vacuum (PSSV) states. CV techniques combined with linear optics are known to be insufficient to prepare non-Gaussian states with negativity in their Wigner functions. Here we extend these ideas and show how the necessity of a photon counting measurement can be replaced by CV measurements for the reconstruction of the statistics of non-Gaussian states. Although the k-PSSV states are not heralded, remarkably, we still extract their quantum statistics.

Our scheme replaces a would-be photon counting measurement with homodyne measurements of the field quadrature [6]. We present two different approaches to this measurement: one that focuses on sampling polynomials of the number operator implemented with a heterodyne measurement, and a second approach where the pattern functions developed by Leonhardt [1] and a single phase-randomised homodyne form the conditioning measurement. Both techniques allow for photon number discrimination in the reconstruction of the non-Gaussian states, allowing us to unambiguously reconstruct the 1, 2, and 3-PSSV states. The Wigner functions, shown in Figure 1, are obtained directly from raw data using the inverse Radon transform without correction or assumption. All reconstructions present clear negativity, testifying to the non-classical nature of the reconstructed states. In addition to enabling us to reconstruct larger states, the ability of our scheme to discriminate photon number also allows us to remove spurious contributions from unwanted higher order subtraction events.

Whilst this scheme does not allow access to heralded non-Gaussian states, it may prove useful for approaches focused on average outcomes. This notion of probing the quantized nature of the quantum system via measurement of its contin-
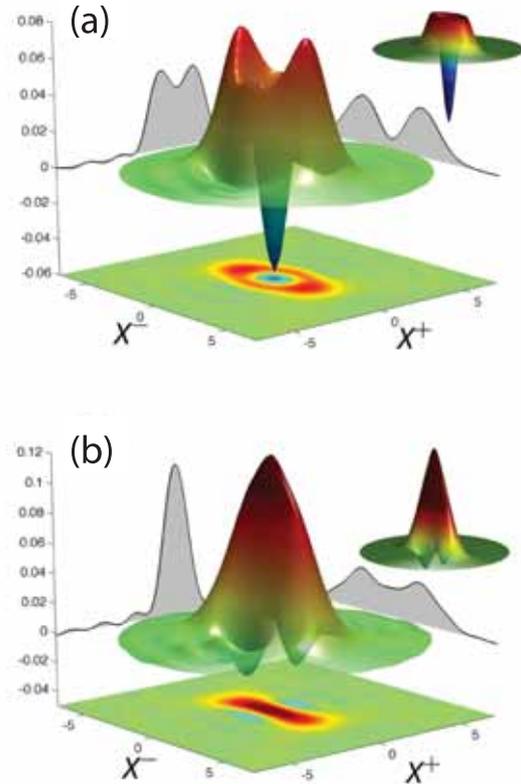
Figure 1: Experimentally reconstructed Wigner function for the (a) 1-PSSV state, and the (b) 2-PSSV state. The insets display the corresponding calculated PSSV states assuming pure initial squeezed states and ideal photon subtraction.

uous variables could also prove interesting for elds such as optomechanics, where direct measurements of the quantization are unavailable or technically difficult.

References

[1] U. Leonhardt, *et al.*, Opt. Comm. **127**, 1-3 (1996).

[2] T. C. Ralph, W. J. Munro, and R. E. S. Polkinghorne, Phys. Rev. Lett. **85**, 2035 (2000).

[3] M. Vasilyev, S. K. Choi, P. Kumar, and G. M. D'Ariano, Phys. Rev. Lett. **84**, 11 (2000).

[4] J. G. Webb, T. C. Ralph, and E. H. Huntington, Phys. Rev. Lett. **73**, 033808 (2006).

[5] N. B. Grosse *et al.*, Phys. Rev. Lett. **98**, 153603 (2007).

Arbitrary shaping of light pulses at the single-photon level.

Eden Figueroa[1], **Tobias Latka**[1], **Andreas Nezner**[1], **Christian Nölleke**[1], **Andreas Reiserer**[1], **Stephan Ritter**[1] and **Gerhard Rempe**[1]

[1]*Max Planck Institute of Quantum Optics, Hans-Kopfermann-Str. 1, 85748 Garching, Germany*

Quantum interconnects between light and matter are essential for future applications of quantum information science. For example, they are important ingredients of long-distance quantum networks, in which remote quantum nodes are connected by light pulses carrying quantum information. A technologically appealing system for the realization of such quantum interconnects is provided by an optically dense room-temperature atomic ensembles where quantum pulses of light are manipulated using electromagnetically induced transparency (EIT).

Despite the remarkable experimental progress demonstrated recently using single atoms in optical cavities as quantum nodes and node-connecting single photons [1], several requirements remain unfulfilled in order to implement a truly practical quantum network. One of them is the capability to easily restore the quality of an input signal so that degradations in signal quality do not propagate through the network [2]. For photon-linked quantum networks, in particular, it is necessary to preserve the temporal envelope of a light pulse containing a single information-carrying photon. We therefore aim to develop a practical device which allows one to control the temporal envelope of a light pulse on the fly.

Towards this goal, we have set up an EIT-based light storage experiment using a ^{87}Rb vapour cell. The classical signal field is obtained from a diode laser and attenuated to the single-photon level. The control field comes from an additional diode laser phase locked to the signal in order to ensure a two-photon resonance. We use linear orthogonal polarizations for the two lasers, and the time-dependent field intensities are controlled using acousto-optical modulators.

In order to prove that our system is able to control light pulses at the single-photon level, we have implemented a stack of filtering stages for the control-field photons. Filtering is particularly important because typically one signal photon has to be distinguished from 10^{11} control photons. In our experiment, the filtering is provided by polarization optics and two temperature-controlled silica etalons. Overall we have achieved 131 dB control-field suppression while only having 10 dB signal losses. This results in an effective control suppression of 121 dB which is almost two orders of magnitude better than results reported in recent experiments [3, 4]. Additional measures have also been taken to minimize control-field induced noise photons produced at the signal frequency.

We have then performed EIT storage experiments at the single-photon level and recorded the results over many experimental runs using a single-photon counting module. The resulting histogram of click-events contains information regarding the storage process, but also events associated to control-field induced noise photons (*storage histogram*). Additionally, we have repeated the storage sequence but only with the control field present, thereby obtaining a histogram of clicks associated exclusively to the noise photons (*noise histogram*). Subtracting both sets of experimental measurements yields the histogram of counts provided only by the
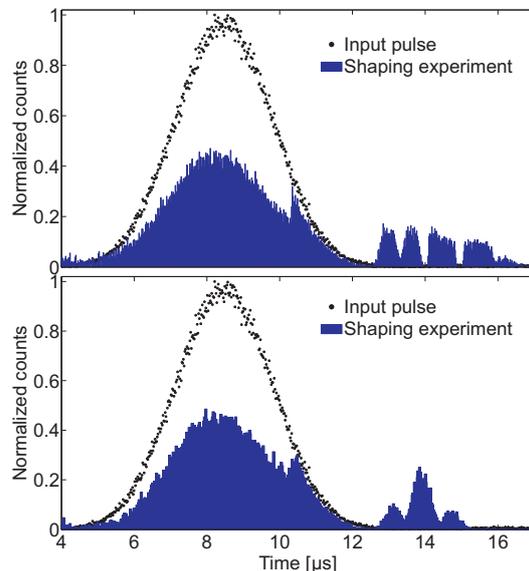
Figure 1: *Noise-free storage histograms* with arbitrarily-shaped retrieval for input pulses containing on average one single-photon (see text for details).

storage and retrieval of the signal field (*noise-free storage histogram*). Finally, we have determined the ratio between the total number of counts in the *noise-free storage histogram* during the time-interval associated to the retrieval, and the total number of counts in the *noise histogram* during the same time-interval. This yields our *measured* signal-to-noise-ratio (an adequate measure of the performance of the device at the single-photon level) of 1.5. This is to the best of our knowledge the first time that such high *measured* signal-to-noise-ratio has been achieved in a vapour experiment.

Moreover, we have stored single-photon level light pulses with a given temporal envelope in the medium and engineered their retrieval with an arbitrary shape (see Fig. 1). This is achieved by means of dynamically manipulating the intensity of the control field during read-out, thus coherently modulating the group velocity of the propagating light pulse. The latter experiment opens up realistic avenues for the optically controlled manipulation of the temporal wave-function of true single-photon fields.

References

[1] S. Ritter *at al.*, Nature (in press)

[2] D. A. B. Miller, Nature Photonics, **4**, 3 (2010)

[3] D. Hoeckel *et al.*, Phys. Rev. Lett., **105**, 153605 (2010).

[4] K. F. Reim *et al.*, Phys. Rev. Lett., **107**, 052603 (2011).

A Versatile Single Photon Source for Quantum Information Processing

Michael Förtsch[1,2,3], **Josef Fürst**[1,2], **Christoffer Wittmann**[1,2], **Dmitry Strekalov**[1], **Andrea Aiello**[1,2], **Maria V. Chekhova**[1,2], **Christine Silberhorn**[1], **Gerd Leuchs**[1,2] and **Christoph Marquardt**[1,2]

[1]*Max Planck Institute for the Science of Light, Erlangen, Germany*
[2]*Institut für Optik, Information und Photonik, Erlangen, Germany*
[3]*SAOT, School in Advanced Optical Technologies, Erlangen, Germany*

The generation of high-quality single photon states with controllable narrow spectral bandwidths and central wavelength is key to facilitate efficient coupling of any atomic system to non-classical light fields. Among others, such interaction is essential for applications in the fields of linear quantum computing and optical quantum networking. In order to be compatible with all of these experiments, a versatile single-photon source should allow for tuning of the spectral properties (wide wavelength range and narrow bandwidth), while retaining high efficiency.

For the first time, we realized an efficient $(1.3 \cdot 10^7$ pairs/(s mW 13 MHz)) narrow-band heralded single photon source, readily tunable in all spectral properties at once. We successfully implemented a cavity assisted spontaneous parametric down-conversion process with a crystalline whispering gallery mode resonator (WGMR). In essence, our system is comparable to a triply resonant optical parametric oscillator[3] operated far below the pump threshold. A green pump light is coupled to the resonator using a prism placed in closed vicinity to the resonator. The variable spacing between the prism and the WGMR forms the basis for the adjustable decay times of the down-converted single photon pairs. By controlling the temperature of the WGMR we control the phase-matching between the pump and the down-converted photons (natural Type I phase matching). An additional con-

trol over the phase matching is realized by a voltage applied to the resonator.

The down-converted light is characterized by evaluating the normalized Glauber inter-beam and intra-beam correlation function, respectively. This gives us a measure for the bandwidth of the emitted photons and the purity of the generated single photon states. We verify a bandwidth tunability of almost a factor of two starting from the smallest experimentally determined bandwidth of 7.2 MHz (Fig.1A). The corresponding purity indicates the presence of only three effective modes. We want to point out that this purity is achieved without the need for (lossy) filtering. By heralding on the idler photon, we investigated the normalized Glauber intra-beam correlation. The minimum of this correlation function is sensitive to the non-classical correlations and tends to zero for single photon states. In Fig.1B the characteristic anti-bunching is clearly visible and shows that our source generates non-classical correlations between two photons in two different modes. By changing the resonators temperature over 3 °C we observe a wavelength detuning of 100 nm (Fig.2). Furthermore we demonstrate that a change of the applied resonator voltage over a range of 4 V results in a mode-hop-free wavelength detuning of 150 MHz.

Figure 2: Wavelength detuning via temperature phase-matching.

Figure 1: (A) The normalized Glauber inter-beam correlation functions for different coupling distances. (B) The normalized Glauber intra-beam correlation function conditioned on an idler event.

References

[1] E. Knill, R. Laflamme, G. J Milburn, Nature **409**, 46 (2001)

[2] J. I Cirac, P. Zoller, H. J. Kimble, H. Mabuchi, PRL **78**, 3221 (1997)

[3] J. Fürst, D. Strekalov, D. Elser, A. Aiello, U. Andersen, Ch. Marquardt, G. Leuchs, PRL **105**, 263904 (2010)

Transition edge sensors with low jitter and fast recovery times

<u>Antia Lamas-Linares</u>[1], Nathan Tomlin[1], Brice Calkins[1], Adriana E. Lita[1], Thomas Gerrits[1], Joern Beyer[2], Richard Mirin[1], Sae Woo Nam[1]

[1]*National Institute of Standards and Technology, 325 Broadway St., Boulder, USA*
[2]*Phys.-Tech. Bundesanstalt (PTB), Berlin, Germany*

Superconducting transition edge sensors (TES) for single photon detection have been shown to have almost perfect quantum efficiency (98%) at a wide range of wavelengths[1, 2, 3]. Their high quantum efficiency combined with their ability to intrisically measure the energy of the absorption event results in a detector that is able to distinguish photon number with high fidelity and without any multiplexing structure. These are highly desired properties in quantum optics experiments, however, the wider adoption of TESs has been hindered by relatively poor timing performance, both in recovery time and in timing resolution (jitter).

We will show how both these aspects can be addressed by material and thermal engineering and appropriate readout configurations, while maintaining the high efficiency and the photon number resolution.

Timing resolution A common figure quoted for TES for optical photons is a jitter of ≈ 100 ns[6], with best reported values of 28 ns[3]. These are orders of magnitude worse than commercial APDs and constitute a serious obstacle in their practical application to coincidence based experiments or the many setups built around a 80 MHz clocked laser.

Recently[4] we have obtained values as short as 2.5 ns for 800 nm light by using low inductance SQUID amplifiers[5] with "conventionally" fabricated TES. This brings TES to a much more useful regime for their integration in practical experiments.

Recovery time Another aspect of timing performance where TES lag behind is in their recovery times. While a typical APD has a dead time of ≈ 100 ns and a superconducting nanowire will recover in ≈ 50 ns, a TES' recovery time is given in μs, with 4 μs being a typical figure. We have shown recently[7] that engineering the thermal links using a normal metal, in addition of the tungsten used as main TES material, results in much improved timing performance.

Low timing jitter and fast recovery Ideally we would like a device that maintains the high efficiency and photon number resolving characteristics of the TES, while improving on both aspects of its timing performance. Here we report on tungsten devices with inherent low jitter (< 12 ns) and that have been engineered by addition of gold patches to improve the recovery time (< 500 ns). The devices also maintain photon number resolution and an efficiency $> 90\%$. The combination of the readout configuration optimized for low jitter plus the addition of a small amount of normal metal results in a device that is particularly well matched to the requirements of experiments in quantum optics.

Figure 1: Histogram of "time of arrival" information for a W-TES with a low inductance readout. The three curves correspond to the jitter for 1, 2 and 3 photons at 1550 nm respectively from left to right, but can also be interpreted as the expected jitter for 1 photon signals at 1550 nm, 775 nm and 516 nm.

[2] A. E. Lita, B. Calkins, L. A. Pellouchoud, A. J. Miller and S. W. Nam, Proc. SPIE **7681**, 76810D (2010).

[3] D. Fukuda et al., IEEE Trans. of Appl. Superconductivity **21**, 241 (2011).

[4] Manuscript in preparation; Presentation at CLEO 2012.

[5] D. Drung et al., IEEE Trans. of Appl. Superconductivity **17**, 699 (2007).

[6] M. D. Eisaman et al., Rev. Sci. Instrum. **82**, 071101 (2011).

[7] B. Calkins, A. E. Lita, A. E. Fox and S. W. Nam, Appl. Phys. Lett. **99**, 241114 (2011).

References

[1] A. E. Lita, A. J. Miller and S. W. Nam, Opt. Express **16**, 3032 (2008).

Discerning EIT from ATS: an experiment with cold Cs atoms

Lambert Giner[1], **Lucile Veissier**[1], **Ben Sparkes**[2], **Alexandra Sheremet**[1], **Adrien Nicolas**[1], **Oxana Mishina**[1], **Michael Scherman**[1], **Sidney Burks**[1], **Itay Shomroni**[3], **Ping Koy Lam**[2], **Elisabeth Giacobino**[1] **and Julien Laurat**[1]

[1] *Laboratoire Kastler Brossel, Université Pierre et Marie Curie, Ecole Normale Supérieure, CNRS,*
Case 74, 4 place Jussieu, 75005 Paris, France
[2] *Centre for Quantum Computation and Communication Technology, The Australian National University, Canberra*
[3] *Chemical Physics Department, Faculty of Chemistry, Weizmann Institute of Science, Rehovot, Israel*

If in general the transparency of an initially absorbing medium for a probe field is increased by the presence of a control field on an adjacent transition, two very different processes can be invoked to explain it. One of them is a quantum Fano interference between two paths in the three level system, which occurs even at low control intensity and gives rise to EIT, the other one is the appearance of two dressed states in the excited level at higher control intensity, corresponding to the Autler Townes splitting (ATS). This distinction is particularly critical for instance for the implementation of slow light or optical quantum memories. In a recent paper, P.M. Anisimov, J.P. Dowling and B.C. Sanders proposed a quantitative test to objectively discerning ATS from EIT [1] . We experimentally investigated this test with cold Cs atoms.

In this study, we use an ensemble of cold Cesium atoms trapped in a MOT, interacting with light via a lambda-type scheme on the D2 line. Absorption profiles are obtained for various values of the control Rabi frequency Ω_C between 0.1Γ and 4Γ, where Γ is the natural linewidth, and as a function of the two-photon detuning δ. The width of the transparency window increases when Ω_C/Γ becomes larger.
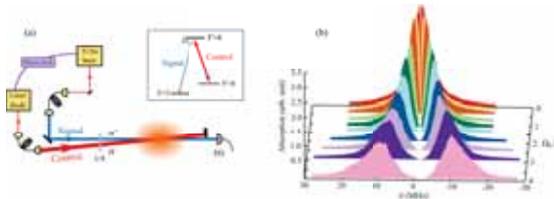
Figure 1: EIT features in a Λ-type system. (a) The experimental EIT setup involves a weak signal beam and a control beam interacting in a cloud of cold cesium atoms prepared in a MOT. (b) Absorption profiles are displayed for various values of the control Rabi frequency Ω_C between 0.1Γ and 4Γ, where Γ is the natural linewidth, and as a function of the two-photon detuning δ.

To analyze the absorption curves, data are fitted using two different models. The first one, related to EIT, is the difference between two Lorentzian curves centered at the same frequency : a positive one with a large width and a negative one with a very small width corresponding to the transparency peak. The second model, related to Autler-Townes splitting, is the sum of two Lorentzian curves with similar widths and separated by a frequency that is of the order of the Rabi Frequency of the control field.

As proposed by Anisimov *et al.* [1], the first method to test the quality of the fits is to calculate for both EIT and ATS models the relative weights ω_{EIT} and ω_{ATS} which are

estimated from "Akaike information criterion" (AIC). Those weights give relative measurements of the likelihood of fits and enable us to determine which model is the best for the experimental data for various values of the control field. The second method is based on mean relative weights $\overline{\omega}_{EIT}$ and $\overline{\omega}_{ATS}$ calculated from mean AIC per point. This method shows a smooth but clear transition between the two regimes and gives more information about the agreement between the models and experimental data, compared with the first method (see fig. 2).
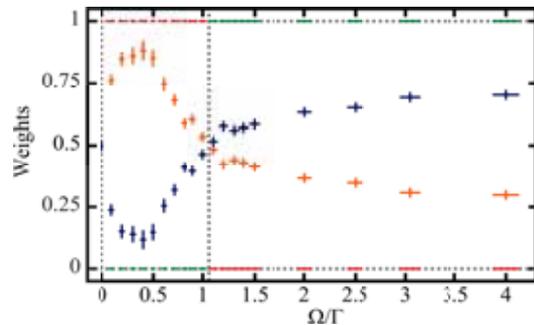
Figure 2: Relative weights ω_{EIT} (red dots) and ω_{ATS} (green dots) are crossing abrupty around $\Omega/\Gamma = 1.1$ while mean weights $\overline{\omega}_{EIT}$ (orange dots) and $\overline{\omega}_{ATS}$ (blue dots) show a smooth transition around the same crossing point.

In conclusion, we have tested the EIT versus ATS test proposed in Ref.[1] in a well controlled experimental case. The criteria have been calculated and give consistent conclusion for the boundary between the two regimes. The observed differences as compared to the model, e.g the crossing point and behavior at large Rabi frequency, can be explained by the specific atomic structure which involves multiple excited levels [2].

References

[1] P.M. Anisimov, J.P. Dowling, and B.C. Sanders, Phys. Rev. Lett. **107**, 163604 (2011).

[2] O. Mishina *et al.*, Phys. Rev. A **83**, 053809 (2011).

Fast light images and the arrival time of spatial information in optical pulses with negative group velocity.

Ryan T. Glasser[1,2], Ulrich Vogl[1,2] and Paul D. Lett[1,2]

[1]*National Institute of Standards and Technology, Gaithersburg, MD, United States*
[2]*Joint Quantum Institute, NIST and the University of Maryland, College Park, MD, United States*

We present the experimental demonstration of superluminal pulse generation via noncollinear four-wave mixing in hot rubidium vapor [1]. In the four-wave mixing double-Λ scheme an injected seed is blue detuned ≈ 6 GHz relative to the conjugate, which is generated on the wing of an absorption line. The two steep gain features result in a large dispersion near the gain lines, resulting in both slow and fast light effects. Near the wings of the gain lines, large negative group indices are obtained with nearly linear dispersion over a typical bandwidth of ≈ 10 MHz. By injecting seed pulses of similar bandwidths we observe group velocities of up to -1/2000 c for the amplified injected beam. A novel feature of this system is that the generated conjugate propagates with a different k-vector, and can also be superluminal. The group velocities of the seed and conjugate pulses can be tuned over a wide range via the two-photon detuning of the seed, as well as by varying the input seed power.

Due to the lack of a cavity in the experiment, we are able to impart an image on the injected seed pulse, and show that the multi-spatial mode pulse also propagates with negative group velocity. Different spatial regions of the image are shown to propagate with different group velocities, all superluminal. Experimental limitations on the amount of pump power available require focusing the pump beam, resulting in some spatial distortion of the images. Because of this, there is a trade-off between the amount of relative pulse peak advancement and output image quality. Large relative pulse peak advancements of >60% are shown, in the case when image quality is not a concern.

This scheme allows us to investigate the propagation of spatial information through a medium of anomalous dispersion. By encoding information in the spatial degree of freedom, we can address the arrival time of the experimentally detectable information without introducing temporal waveforms that explicitly contain points of non-analyticity. This allows for the majority of the pulse bandwidth to fit in the linear region of anomalous dispersion. We show that given a realistic detector with sub-unity quantum efficiency, the arrival time of the spatial information is advanced when propagating through the region of anomalous dispersion [2].

The seed and conjugate beams in the noncollinear four-wave mixing scheme in hot rubidium vapor have been shown to exhibit nonclassical correlations and entanglement [3]. The present results should allow investigating the effects of anomalous dispersion on quantum correlations between the generated twin beams.

Figure 1: Relative pulse peak advancement of the seed (triangles) and conjugate (circles) pulses versus two-photon detuning. The curves are fits derived from a Lorentzian gain line with an absorption line on the wing, for the conjugate mode, and an asymmetric Lorentzian gain line for the seed mode. The inset shows the modeled and measured gain lines for the conjugate mode.
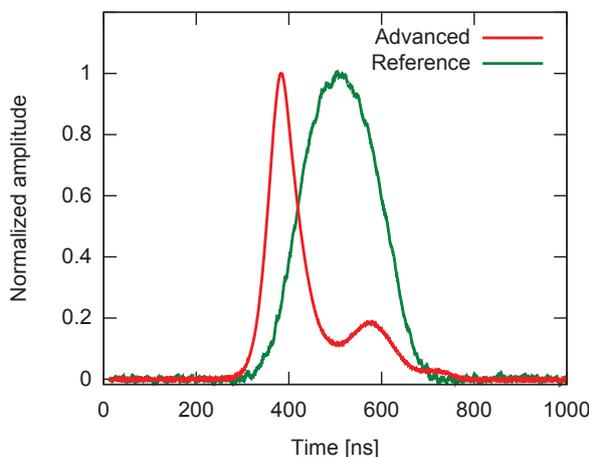
Figure 2: Typical trace of a reference pulse propagating at c (green line) and an advanced pulse propagating with a negative group velocity (red).

References

[1] R.T. Glasser, U. Vogl, and P. D. Lett, Phys. Rev. Lett, in press (2012).

[2] U. Vogl, R. T. Glasser, and P. D. Lett, in preparation.

[3] V. Boyer, A. M. Marino, R. C. Pooser and P. D. Lett, Science, **321**, 5888 (2008).

Phase property measurements with an ultrafast pulsed Sagnac source of polarization-entangled photon pairs

Ana Predojević[1], **Stephanie Grabher**[1] and Gregor Weihs[1]

[1]*Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, 6020 Innsbruck, Austria*

Entangled photons are basic ingredients for applications in linear optics quantum computation [1] and various schemes in quantum information which employ teleportation [2] and entanglement swapping [3].

Here, we present a pulsed down-conversion source of polarization-entangled photon pairs that consists of a non-linear crystal embedded in a Sagnac-type interferometer [4]. The conversion takes place in a type-II periodically poled KTP crystal with a poling period of $9.825\mu m$ and a length of 15mm. Laser pulses at 808nm with a duration of about 2ps from a Ti:Sapphire laser are frequency-doubled to 404nm in a BIBO crystal and sent into the Sagnac loop.

Our experimental setup is shown schematically in Fig.1 (a). The pump beam is reflected off a dichroic mirror and enters the interferometer. Depending on its polarization it travels clockwise or counter-clockwise through the loop before it is down-converted in the type-II ppKTP crystal. The created photons propagate through the loop and exit at the polarizing beam splitter. Depending on their polarization, the single photons are reflected or transmitted by the beamsplitter and travel along two different paths before they are coupled into single-mode fibers and detected. The dual-wavelength half wave-plate in the loop erases the temporal walk-off which is typical for type-II down-conversion. A dichroic mirror in front of the loop reflects the pump light and transmitts the down-converted photons.

of the photon pairs and that the source is wavelength-tunable and can be run in a cw [5] or pulsed [6] configuration.

The visibility of our created Ψ^+-Bell-state is shown in Fig.1 (b). We achieved very high visibilities of $98.70(9)\%$ in the AD-basis and $99.88(3)\%$ in the HV-basis. Moreover, we did a full quantum state tomography on our measured state and received a tangle of $96.50(83)\%$ and a fidelity $98.20(70)\%$.

In addition, we investigated the phase properties of this source geometry. In [5] it was shown that the phase of the generated biqubit state does not depend on the position of the crystal in the loop. Yet, this claim is only correct for plane waves propagating in vacuum. In a real source the phase of the generated state will be affected by two factors: the dispersion of air and the Gouy phase-shift which occurs in Gaussian beams. While the dispersion of the air is linear and trivial to solve, the Gouy phase-shift is somewhat more complicated. Boyd and Kleinman showed in [7] that the the Gouy phase-shift acts destructively on the conversion unless it is compensated for by an appropriate phase mismatch. However, even for relatively weak focusing, the compensation cannot be perfect. The contribution of the Gouy phase-shift along with the influence of the dispersion of air are evident when moving the crystal in the loop. Fig.1 (c) shows that we performed a full quantum state tomography on the output state to obtain its phase. The residual Gouy phase-shift after subtracting the contribution of the dispersion of air, was measured in Fig.1 (d) (black dots) and compared to theory (red curve).

References

[1] E. Knill, R. Laflamme and G. J. Milburn, Nature, **409** (2001)

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett., **70**, 13 (1993).

[3] H. de Riedmatten, I. Marcikic, J. A. W. van Houwelingen, W. Tittel, H. Zbinden and N. Gisin, Phys. Rev. A, **71**, 050302 (2005).

[4] B. Shi and T. Tomita, Phys. Rev. A, **69**, 013803 (2004).

[5] T. Kim, M. Fiorentino and F. N. C. Wong, Phys. Rev. A, **73**, 012316 (2006).

[6] O. Kuzucu and F. N. C. Wong, Phys. Rev. A, **77**, 032314 (2008).

[7] G. D. Boyd and D. A. Kleinman, J. Appl. Phys., **39**, 8 (1968).

Figure 1: **(a)** Schematic picture of the experimental setup **(b)** Visibility of the Ψ^+-state; AD=$98.70(9)\%$, HV=$99.88(3)\%$ **(c)** Fidelity of the output state depending on the crystal position **(d)** Gouy phase-shift depending on the position of the focus

The major advantage of the Sagnac source is the intrinsic phase-stability [5] of the interferometer. Other advantages are that there is no need for spatial, temporal or spectral filtering

A High-Speed Quantum Random Number Generator Based on the Vacuum State

Christian Gabriel[1,2,*], **Christoffer Wittmann**[1,2], **Bastian Hacker**[1,2], **Wolfgang Mauerer**[3], **Elanor Huntington**[4,5], **Metin Sabuncu**[1,6], **Christoph Marquardt**[1,2] and **Gerd Leuchs**[1,2]

[1] Max Planck Institute for the Science of Light, Guenther-Scharowsky-Str. 1, D-91058 Erlangen, Germany
[2] Institute of Optics, Information and Photonics, University Erlangen-Nuremberg, Staudtstr. 7/B2, D-91058 Erlangen, Germany
[3] Siemens AG, Corporate Technology, Otto-Hahn-Ring 6, 81739 München, Germany
[4] Centre for Quantum Computation and Communication Technology, Australian Research Council
[5] School of Engineering and Information Technology, The University of New South Wales, Canberra, Australian Capital Territory
[6] Department of Electrical and Electronics Engineering, Dokuz Eylül University, Tinaztepe, Buca, 35160 Izmir, Turkey

Random number generators (RNGs) are important in many fields ranging from simulations to cryptography. In quantum cryptography random numbers are essential for an unconditional secure key distribution [1]. RNGs based on computer algorithms or classical physical systems produce bit sequences that might seem random, however they in principle still rely on a purely deterministic nature. Quantum mechanics can overcome this hurdle as the quantum measurement process can yield completely random outcomes. This has the additional advantage that the numbers are unique, i.e. that no potential adversary has knowledge over the generated bit string. One can assure this by either utilizing pure states [2], a detection-loophole free Bell test [3] or a tomographical complete measurement [4].

Our quantum RNG scheme[2] employs a homodyne detection system to measure the quantum fluctuations of a pure vacuum state. We here present an implementation that uses a high speed homodyne detector and novel data-post processing that is able to improve the speed of the quantum RNG to the Gbit/s range.

The experimental setup (s. Fig. 1a) consists of a balanced homodyne setup that uses a combination of a half-wave plate and a polarizing beam splitter to substitute the actual beam splitter in order to assure an exact splitting ratio of the local oscillator of 50%. The detected signals are subtracted and fed into an oscilloscope with a 4 GHz analog bandwidth and a 20 GS/s sampling rate. By subtracting the two currents, a quadrature amplitude of the vacuum state is measured. As the electronic noise and gain of the detector and oscilloscope modify the signal with their non-uniform, frequency-dependent spectrum we perform the data extraction with the quantum fluctuations occurring at each single frequency respectively (omitting pick-up signal from external noise sources, for example mobile phone up- and down-links). For this purpose we apply a discrete Fourier transform (DFT) with a resolution bandwidth of 0.1 MHz to the measured time signal (the power spectrum is shown in Fig. 1b). At each frequency component the amplitude fluctuations follow a Gaussian probability distribution.

To extract bits from the measured signal an equidistant spacing of width b is applied to a length $B = b \cdot 2^n$ of each of the probability distributions. Here n is the number of bits assigned to each measurement value within one bin of width b. The pattern is repeated after each length B. This scheme has the advantage that if B is chosen small enough a uniform distribution is achieved, i.e. that the numbers are not biased. We determine the conditional Min-entropy in the system , allowing us to carefully characterize how much information is
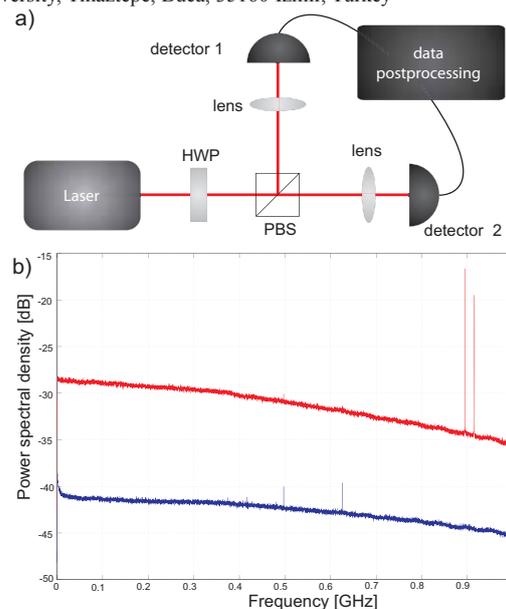
Figure 1: a) The experimental setup of the QRNG (HWP = half-wave plate, PBS = polarizing beam splitter). b) The power spectrum of the homodyne measurement data of the vacuum fluctuations (red) and the electronic noise (blue).

suited for true random number generation. Furthermore, the extractable information of the generated bit string is determined. A one-way hashing function has to be applied to the raw bit strings to reduce its information content by the appropriate amount. After that the resulting bits only contain information from quantum effects.

The high-speed detector and the new bit extraction method allow an expected random bit extraction speed of up to 10 GBit/s.

References

[1] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145–195 (2002).

[2] C. Gabriel *et al.*, Nature Photonics **4**, 711–715 (2010).

[3] S. Pironio *et al.*, Nature **464**, 1021–4 (2010).

[4] M. Fiorentino *et al.*, Phys. Rev. A **75** (2007).

Poster session 2 Tuesday abstracts

Single spontaneous photon as a coherent beamsplitter for an atomic matter-wave

Jiří Tomkovič[1], Michael Schreiber[2], Joachim Welte[1], Martin Kiffner[3], Jörg Schmiedmayer[4], Markus K. Oberthaler[1]

[1] *Kirchhoff-Institut für Physik, Universität Heidelberg, Im Neuenheimer Feld 227, 69120 Heidelberg, Germany*
[2] *Ludwig-Maximilians-Universität, Schellingstr. 4, 80799 München, Germany*
[3] *Physik Department I, Technische Universität München, James-Franck-Straße, 85747 Garching, Germany*
[4] *Vienna Center for Quantum Science and Technology, Atominstitut, TU Wien, 1020 Vienna, Austria*

In spontaneous emission an atom in an excited state undergoes a transition to the ground state and emits a single photon. Associated with the emission is a change of the atomic momentum due to photon recoil [1]. In free space, a spontaneous emission destroys motional coherence [2, 3].

Photon emission can be modified close to surfaces [4] and in cavities [5]. In the experiment reported here [6] we show that motional coherence can be *created* by a single spontaneous emission event close to a mirror surface.

For emission very close to a mirror surface directions of the emitted photon become indistinguishable due to reflection. A single spontaneous emission event in front of a mirror therefore creates a coherent superposition of freely propagating atomic matter waves, without any external coherent fields involved. The coherence in the free atomic motion can be verified by atom interferometry [7]. We observe coherence only when the photon cannot carry away which-path information (see Figure 1).

In our experiment the emitted single photon can be regarded as the ultimate light weight beamsplitter for the atomic matter wave and consequently our experiment extends the original recoiling slit Gedanken experiment by Einstein [8] to the case where the slit can be in a coherent superposition of the two recoils associated with the two paths of the quanta.

In free space the momentum of the emitted photon allows to measure the path of the atom. This corresponds to a well defined motional state of the recoiling slit beamsplitter and no coherence is observed. Close to the mirror reflection renders paths with opposite momentum indistinguishable realizing a coherent superposition of the beamsplitter in two motional states. The large mass of the mirror ensures that even in principle the photon recoil on the mirror cannot be seen, and therefore erases the entanglement between the photon and the path of the atom. Thus the atom is in a coherent superposition of the two paths and interference is observed.

Figure 1: Experimental confirmation of coherence induced by spontaneous emission [6]. A spontaneous emission event is employed as the first beamsplitter of an atom interferometer which is completed by Bragg scattering from a standing light wave. The relative phase of the two paths can be changed by moving the 'Bragg mirror' which forms the standing wave as indicated. In the case of large distance ($54~\mu m$) between atoms and the mirror (upper graph) no interference signal is observed confirming the free space limit. For short distance ($2.8~\mu m$) the mirror erases the *which path information* carried by the photon, the single emitted photon acts as a coherent beamsplitter and interference is observed. The inset depicts the position of the mirror to the atomic beam.

References

[1] Milonni, P. W., *The quantum vacuum*, Academic Press, Boston, (1994).

[2] Pfau, T., Spälter, S., Kurtsiefer, C., Ekstrom, C. R., Mlynek, J., *Loss of spatial coherence by a single spontaneous emission*, Phys. Rev. Lett. **73**, 1223 (1994).

[3] Chapman, M. S. *et al.*, *Photon scattering from atoms in an atom interferometer: Coherence lost and regained*, Phys. Rev. Lett. **75**, 3783 (1995).

[4] Drexhage, K. H. *Progress in Optics* Vol. 12, 163-192, 192a, 193-232 (Elsevier, 1974).

[5] Goy, P., Raimond, J., Gross, M., Haroche, S. *Observation of cavity-enhanced single-atom spontaneous emission*, Phys. Rev. Lett. **50**, 1903 (1983).

[6] Tomkovič J. *et al.*, *Single spontaneous photon as a coherent beamsplitter for an atomic matter-wave*, Nature Physics **7**, 379 (2011).

[7] Oberthaler, M. *et al.*, *Dynamical diffraction of atomic matter waves by crystals of light*, Phys. Rev. A **60**, 456 (1999).

[8] Bohr, N.,*Albert Einstein: Philosopher Scientist*, (ed. Schilpp, P.A.) (Library of Living Philosophers, Evanston, 1949); reprinted in *Quantum Theory and Measurement* (eds Wheeler, J. A. and Zurek, W. H.) 949 (Princeton Univ. Press, 1983).

Generation of entanglement with highly-mixed systems

Minsu Kang[1], **M. S. Kim**[2] **and Hyunseok Jeong**[1]

[1]*Center for Macroscopic Quantum Control, Department of Physics and Astronomy, Seoul National University, Seoul, 151-742, Korea*
[2]*QOLS, Blackett Laboratory, Imperial College London, London SW7 2BZ, United Kingdom*

We investigate entanglement production with highly-mixed states. We show that entanglement between highly mixed states can be generated via a direct unitary interaction even when both the states have purities arbitrarily close to zero [1]. This indicates that purity of a subsystem is not required for entanglement generation, and this result is in contrast to previous studies where the importance of the subsystem purity was emphasized.

Entanglement is considered a genuine quantum correlation that cannot be described by any classical means. In general, generating entanglement using a classical system such as a thermal state is much more difficult than using a nonclassical state. On the other hand, it is still possible to generate entanglement with highly mixed thermal states under certain conditions [2, 3, 4, 5, 6]. For example, Bose *et al.* showed [3] that entanglement always arises between a two-level atom and a thermal field inside a cavity irrespective of the temperature of the thermal state as far as the atom was initially in a pure excited state.

However, these are not the bottom of the investigations. For example, it would be an interesting question whether a thermal state at an arbitrarily high temperature can ever be entangled with a mixed atomic state by a direct unitary interaction. In fact, it is possible to prepare the initial atomic state in an independent manner from the temperature of the field. We consider an atomic state, $p |e\rangle\langle e| + (1 - p) |g\rangle\langle g|$ with $0 \leq p \leq 1$, and a thermal-field state, $\rho^{th} = (1 - \lambda) \sum_n \lambda^n |n\rangle\langle n|$, where $|g\rangle (|e\rangle)$ is the ground (excited) state of the atom and $|n\rangle$ is the photon number state of the field. We note that $\lambda = \exp[-\hbar\omega/k_B T]$, k_B is the Boltzman constant, T is the temperature, and ω is the frequency of the optical field. In our analysis, the purity of state ρ is quantified by the linear entropy $\text{Tr}[\rho^2]$. The purities of the atomic and field states are then $\mathcal{P}_{atom} = 2(p - 1/2)^2 + 1/2$ and $\mathcal{P}_{field} = (1 - \lambda)/(1 + \lambda)$, respectively. We take p and λ as independent control parameters of purities of the atom and the field. The initial states evolve through a Jaynes-Cummings interaction, $H_{JC} = g(|e\rangle\langle g| a + |g\rangle\langle e| a^\dagger)$, where g is the coupling strength and a ($a^\dagger$) is the annihilation (creation) operator of the field mode. Our numerical analysis based on the negativity of partial transpose [7, 8, 9] suggests that a certain degree of purity for the atom is required to generate entanglement.

It also remains unanswered whether entanglement may be generated between thermal states at arbitrarily high temperatures by a direct unitary interaction. We here prepare two identical displaced thermal states, $D(d)\rho^{th}D^\dagger(d)$, where $D(d) = e^{d\hat{a}^\dagger - d^*\hat{a}}$ and then apply a cross-Kerr interaction directly. The cross-Kerr interaction between modes a and b is described by an interaction Hamiltonian $H_{\text{Kerr}} = \chi a^\dagger a b^\dagger b$ where χ is the nonlinear interaction strength. Here, the purity (and the temperature) of a thermal state is characterized solely

by its variance V. The purity of a thermal state approaches zero (and the temperature approaches infinity) for $V \to \infty$. As shown in Fig. 1, interestingly, we observe that two thermal states at arbitrarily high temperatures are entangled through a direct unitary interaction as far as the displacement d of the thermal states is sufficiently larger than the variance of the thermal states, *i.e.*, $d \gg \sqrt{V}$.

Our results reveal some interesting facts concerning the generation of entanglement involving highly mixed systems. The purity of initial states is not necessarily a prerequisite for entanglement generation. It rather depends on the model of the interaction between the initial states. In particular, entanglement between thermal states can be generated via a direct unitary interaction even when both the states have purities arbitrarily close to zero.
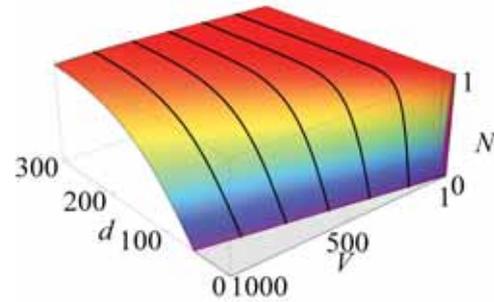
Figure 1: Entanglement (negativity of partial transpose) N of a state generated by a direct cross Kerr interaction between two displaced thermal states with variance V and displacement d.

References

[1] M. Kang, M. S. Kim and H. Jeong, to be published in Phys. Rev. A.

[2] R. Filip *et al.*, Phys. Rev. A **65**, 043802 (2002).

[3] S. Bose *et al.*, Phys. Rev. Lett. **87**, 050401 (2001).

[4] M. S. Kim, *et al.*, Phys. Rev. A **65**, 040101(R) (2002).

[5] A. Ferreira *et al.*, Phys. Rev. Lett. **96** (2006) 060407.

[6] H. Jeong and T.C. Ralph, Phys. Rev. Lett. **97**, 100401 (2006); Phys. Rev. A **76**, 042103 (2007).

[7] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[8] M. Horodecki *et al.*, Phys. Lett. A **223**, 1 (1996).

[9] J. Lee *et al.*, J. Mod. Opt. **47**, 12 (2000).

Creating and Detecting Momentum Entangled States of Metastable Helium Atoms

Michael Keller[1][2], Max Ebner[1][2], Mateusz Kotyrba[1][2], Mandip Singh[1], Johannes Kofler[1][3] and Anton Zeilinger[1][2]

[1] Institute for Quantum Optics and Quantum Information (IQOQI) Vienna, Austria
[2] University of Vienna, Quantum Optics, Quantum Nanophysics, Quantum Information, Austria
[3] Max-Planck Institute for Quantum Optics (MPQ), Garching, Germany

We present a possible scheme for creating and detecting entangled states in momentum space for neutral metastable Helium (He*) atoms.

Starting from a Bose-Einstein condensate (BEC) one can use two-photon Raman pulses to transfer momentum to the atoms. Using this to put the atoms in a superposition of two counterpropagating momentum states one can induce collisions between atoms to create entangled atom pairs [1]. Very close to the original proposal by Einstein, Podolski and Rosen [2], those pairs are anti-correlated in their motional degree of freedom.

A position resolved micro-channel plate (MCP) detector can be used for detecting individual He* atoms. The high internal energy of He* atoms of almost 20 eV per atom allows for creating an electron avalanche in the MCP channels that is subsequently hitting a delay-line Anode. Very precise detection of the arrival times of the electronic pulses on the ends of the delay-lines of sub 500 ps resolution allows for precise detection in space ($< 50\ \mu m$) and time, thereby gaining full 3D information on an individual atom. Due to the large surface area of the detector (80 mm in diameter) we can mount it more than 80 cm below the magnetic trap center which increases the resolution in momentum space. Four independent quadrants of the detector enable us to detect two particles on opposite detector sides in a truely simultaneous manner.
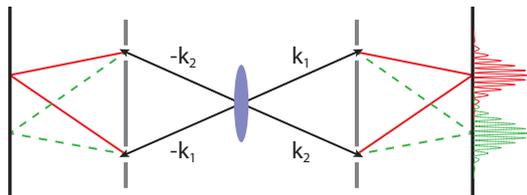
Figure 1: With momentum correlated atom pairs, single particle interference patterns don't occur, since the correlated partner particle could in principle be used for gaining which path information. In a double double-slit configuration, however, a second double slit is used to erase that information and interference fringes appear when detecting the particles in coincidence.

Those tools open up the way for experiments to proof that the atoms are actually entangled, for example in a double double-slit experiment (see Fig. 1) [3, 4, 5]. We analyze requirements and restrictions for such an experiment, for example on detector resolution and source size, and show that it should be in principle achievable in our current setup.

References

[1] A. Perrin, H. Chang, V. Krachmalnicoff, M. Schellekens, D. Boiron, A. Aspect and C. I. Westbrook, Phys. Rev. Lett. **99**, 150405 (2007).

[2] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).

[3] M. A. Horne and A. Zeilinger, "A Bell-Type EPR Experiment Using Linear Momenta", Symposium on the Foundations of Modern Physics, Joensuu, P. Lahti and P. Mittelstedt (Eds.), World Scientific Publ. (Singapore), 435 (1985).

[4] M. Horne and A. Zeilinger, "A Possible Spin-Less Experimental Test of Bell's Inequality", Microphysical Reality and Quantum Formalism, Kluwer (1988).

[5] J. G. Rarity and P. R. Tapster, Phys. Rev. Lett. **64**, 2495 (1990).

Violation of macroscopic realism without Leggett-Garg inequalities

__Johannes Kofler__[1], and Časlav Brukner[2,3]

[1]*Max Planck Institute of Quantum Optics (MPQ), Garching/Munich, Germany*
[2]*University of Vienna, Vienna, Austria*
[3]*Institute for Quantum Optics and Quantum Information (IQOQI), Vienna, Austria*

In 1985, Leggett and Garg put forward the concept of macroscopic realism (macrorealism) and, in analogy to Bell's theorem, derived a necessary condition in terms of inequalities, which are now known as the Leggett-Garg inequalities. In this paper, we discuss another necessary condition called *statistical non-invasive measurability*. Its structure intuitively encompasses the physical meaning of macrorealism and allows for an experimental test in situations where the paradigm of Leggett-Garg inequalities cannot be implemented. It solely bases on comparing the probability distribution for a macrovariable at some time with the distribution in case a previous measurement was performed. Although the concept is analogous to the no-signaling condition in the case of Bell tests, it can be violated according to quantum mechanical predictions. We show this with the example of the double slit experiment.

Experimental non-classicality of an indivisible quantum system

Radek Lapkiewicz[1,2]**, Peizhe Li**[1]**, Christoph Schaeff**[1,2]**, Nathan K. Langford**[1,2]**, Sven Ramelow**[1,2]**, Marcin Wiesniak**[1]
& Anton Zeilinger[1,2]

[1] *Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Boltzmanngasse 5, Vienna A-1090, Austria*
[2] *Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, Vienna A-1090, Austria*

In Quantum Mechanics (QM) not all properties can be simultaneously well defined. An important question is whether a joint probability distribution can describe the outcomes of all possible measurements, allowing a quantum system to be mimicked by classical means. Klyachko, Can, Binicioglu and Shumovsky (KCBS) [1] derived an inequality which allowed us to answer this question experimentally. The inequality involves only five measurements and QM predicts its violation for single spin-1 particles. This is the simplest system where such a contradiction is possible. It is also indivisible and as such cannot contain entanglement. In our experiment with single photons distributed among three modes (isomorphic to stationary spin-1 particles) we obtained a value of -3.893(6), which lies more than 120 standard deviations below the "classical" bound of -3.081(2). Our results illustrate a deep incompatibility between quantum mechanics and classical physics that cannot at all result from entanglement [2].
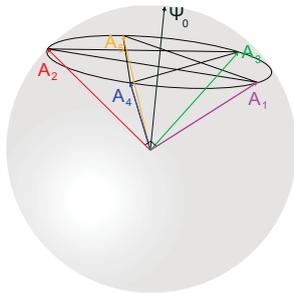
Figure 1: Representation of the measurements and a state providing maximal violation of the KCBS inequality [1] by directions in three-dimensional space.

Figure 2: The conceptual scheme of the experiment with the preparation and five successive measurement stages. Straight, black lines represent the optical modes (beams), gray boxes represent transformations on the optical modes. a) Single photons are distributed among three modes by transformations T_A and T_B. This preparation stage is followed by one of the five measurement stages: b)-f).

References

[1] A. A. Klyachko, M. A. Can, S. Binicioglu, and A. S. Shumovsky, PRL , **101**, 020403 (2008).

[2] R. Lapkiewicz, P. Li, C. Schaeff, N. K. Langford, S. Ramelow, M. Wiesniak, and A. Zeilinger, Nature, **474**, 490 (2011).
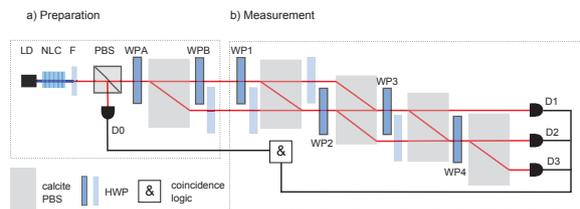
Figure 3: Experimental setup. a) Preparation of the required single-photon state. b) The measurement apparatus: half-wave plates $WP_1 - WP_4$ realize the transformations $T_1 - T_4$ on pairs of modes.

Time reversibility in the quantum frame

Fatima Masot-Conde

Dpt. Applied Physics III, University of Seville, Seville, Spain

There is no shadow of doubt about the time reversible character of classic Mechanics. The theoretical time invariance of classic Electromagnetism, though, is questioned, due to the collision with the obvious irreversible physical behaviour of radiation, (the so-called Loschmidt paradox[1, 2, 3]). Both classic Mechanics and Electromagnetism share the same concept of *motion* (either of mass or charge), as the basis of time reversibility in their own fields [4]. This is precisely the topic of this work: time reversibility from the point of view of motion. In particular, the study focuses on the relationship between mobile geometry and motion reversibility. The goal is to extrapolate the conclusions to the quantum frame, where "matter" and "energy" behave just as elementary mobiles. The possibility that the asymmetry of Time (Time's arrow) is an effect of a fundamental asymmetry of elementary particles, turns out to be a consequence of the discussion.

References

[1] F. Arntzenius, The Classical Failure to Account for Electromagnetic Arrows of Time, in G. Massey, T. Horowitz and A. Janis (*eds.*) *Scientific Failure*, (Lanham: Rowman & Littlefiled), 29-48 (1993).

[2] L. Maccone, Phys. Rev. Lett. **103**, 080401 (2009).

[3] J. Loschmidt, Sitzungsber, Kais. Akad. Wiss. Wien, Math Naturewiss. Classe II, **73**, 128 (1876).

[4] J. Sakurai, *Modern Quantum Mechanics* (Reading, MA: Addison Wesley) 266 (1994).

Entanglement between photons that never co-existed

E. Megidish, A. Halevy, T. Shacham, T. Dvir, L. Dovrat, and H. S. Eisenberg

Racah Institute of Physics, Hebrew University of Jerusalem, Jerusalem, Israel

Entanglement between quantum systems is the most puzzling property of quantum mechanics. It results in non-classical correlations between systems that are separated in time and space. Photons are useful realizations of quantum particles as they are easily manipulated and preserve their coherence for long times.

In this work we demonstrate the creation of entanglement between photons that never interacted, and even more importantly, never co-existed. Entanglement is swapped [1] between temporally separated photon pairs that exist in separate times. A pulsed laser pumps a single parametric down-conversion polarization-entangled photon source [2]. Two pairs are created at the same source but from different pulses, separated in time by τ:

$$|\psi^-\rangle_{1,2}^{0,0} \otimes |\psi^-\rangle_{1,2}^{\tau,\tau} =$$
$$\frac{1}{\sqrt{2}}(|h_1^0 v_2^0\rangle \pm |v_1^0 h_2^0\rangle) \otimes \frac{1}{\sqrt{2}}(|h_1^\tau v_2^\tau\rangle \pm |v_1^\tau h_2^\tau\rangle) \quad (1)$$

The uppercase designation is for the time-label of the photon. Projecting two photons, one from each pair onto a maximally entangled Bell state creates entanglement between the remaining two photons. Bell measurement is realized by inserting the two photons into a polarization beam-splitter (PBS) from different input ports and post-selecting [1] the cases when they exit from different output ports. One photon from the first pair is delayed until a photon from the second pair arrives simultaneously to the PBS (see Fig.1 a). The same delay is also applied to the other photon of the second pair. The first photon from the first pair and last photon from the second pair, that did not share between them any correlations before, become entangled.

Entanglement between the first and the last photons is created gradually. First, one entangled pair is created, then the second, and finally, the swapping between them is performed. The timing of each photon is merely an additional label to discriminate between the different photons. It is thus clear that the time of the measurement of each photon has no effect on the final outcome. In previous demonstrations, all photons were first created, and only then measured. In our scheme, the first photon from the first pair is measured even before the second pair is created. After the creation of the second pair, the Bell projection occurs by a measurement of a photon from each of the pairs. Only after another delay period, the last photon from the second pair is detected. As entanglement swapping creates correlations between the first and last photons non-locally, the fact that the first photon has been measured even before it was linked to the last photon has no effect on the final outcome. Quantum correlations are only established a posteriori, after measurement of all the photons is completed.

We used the experimental setup presented in Fig.1 a. A doubled Ti:Sapphire laser beam with 400 mW at a wavelength of 390 nm and a repetition rate of 76 MHz pumps a BBO non-
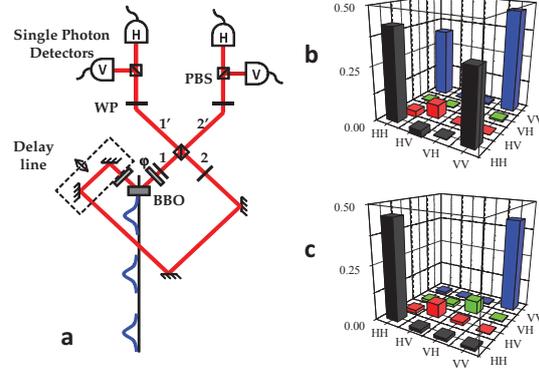
Figure 1: a: Experimental setup. b,c: Real part of the density matrices of the first and last photons when the two middle photons are projected onto the $|\phi^+\rangle$ state (b) and when the projection fails due to temporal distinguishability (c).

linear crystal. By type-II non-collinear PDC, polarization entangled pairs are created in the state $|\psi^-\rangle$ with low-power visibility above 90% in the H/V and P/M bases. The free-space delay line is 31.5 m long (105 ns), such that entanglement swapping occurs between pairs created by pump pulses that are 8 pulses apart. The delay time is longer than the 50 ns single-photon detectors' dead-time. This delay time is sufficient to ensure that the first photon detection is completed before the second pair is created.

In order to demonstrate the entanglement created between the first and last photons we performed quantum state tomography (QST) [3] with a maximal likelihood procedure of these two photons' state, conditioned on the detected state of the two middle photons. The results presented in Figs. 1b and 1c are for the condition that the two middle photons at time τ were projected onto the $|\phi^+\rangle_{1,2}^{\tau,\tau}$ state. In Fig. 1b the projected middle photons are temporally indistinguishable, as they arrive at the PBS simultaneously, while in Fig. 1c distinguishability is introduced by an extra time delay. When the projected photons are indistinguishable, the measured state of the first and last photons has fidelity of $77 \pm 1\%$ with a pure $|\phi^+\rangle_{1,2}^{0,2\tau}$ state. When the projected photons are distinguishable, the off-diagonal coherence elements vanish. We also performed QST when the two middle photons were projected on the $|\phi^-\rangle$ state. In this case, the sign of the off-diagonal elements was changed as expected.

References

[1] J.-W. Pan *et al.*, *Phys. Rev. Lett.* **80**, 3891 (1998).

[2] P. G. Kwiat *et al.*, *Phys. Rev. Lett.* **75**, 4337 (1995).

[3] D. F. V. James *et al.*, *Phys. Rev. A* **64**, 052312 (2001).

Characterizing and Quantifying Frustration in Quantum Many-Body systems

S.M. Giampaolo[1]**, G. Gualdi**[1]**, Alex Monras**[1]* **and F. Illuminati**[1]

[1]*Università degli Studi di Salerno, Via Ponte don Melillo, I-84084 Fisciano (SA), Italy*
*Presently at: Centre for Quantum Technologies, National University of Singapore, 117543, Block S15, 3 Science Drive 2 Singapore

We present a general scheme for the study of frustration in quantum systems. We introduce a universal measure of frustration for arbitrary quantum systems and relate it to a class of entanglement monotones via a sharp inequality. We introduce sufficient conditions for a quantum spin system to saturate such bounds. These conditions provide a generalization to the quantum domain of the Toulouse criteria for classical frustration-free systems. The models satisfying these conditions can be reasonably identified as geometrically unfrustrated and subject to frustration of purely quantum origin, in accordance with the equality between entanglement and frustration measures. Our results therefore establish a unified framework for studying the intertwining of geometric and quantum contributions to frustration.

In recent years it has become well understood that frustration in quantum systems arises even in the abscence of geometric frustration (GF) [2]. Although it is widely assumed that GF is responsible for the existence of exotic states of matter [3], the very notion of GF is based on classical notions [4] and its implications for quantum systems are yet to be fully understood.

Given an N-body system described by a generic Hamiltonian

$$H = \sum_S h_S \tag{1}$$

where h_S indicate interaction among $S \subset \{1, \ldots, N\}$ bodies, a frustration measure for each subsystem S can be defined as follows. Let $\rho = |G\rangle\langle G|$ be the ground state of H and let Π_S be the projector onto the ground subspace of h_S. Then

$$f_S = 1 - \text{tr}[\rho \Pi_S] \tag{2}$$

With this definition, a system is *frustration free* if and only if $f_S = 0$ for all subsystems S.

Also, the d-rank Geometric Entanglement [5] between subsystem S and the rest of the system (its complement $\bar{S}$) is given by

$$E_S^{(d)} = 1 - \sum_{i=1}^d \lambda_i^\downarrow(\rho_S) \tag{3}$$

where ρ_S is the reduced state $\rho_S = \text{tr}_{\bar{S}}\rho$.

These quantities, although capturing essentially different phenomena, are related by the simple sharp inequality

$$f_S \geq E_S^{(d)} \tag{4}$$

for all subsystems S, when d is chosen to be the rank of Π_S. The fact that this inequality is sharp suggests that with the chosen quantifiers, entanglement and frustration are measured in equal footing.

In order to undertand the interplay between frustration and entanglement exhibited by Inequality (4), we explore under which conditions does this saturate. To this aim, we focus on nondegenerate two-body interactions with (possibly inhomogeneous, anisotropic) Heisenberg interactions,

$$H = -\sum_{ij} \left(J_{ij}^x X_i X_j + J_{ij}^y Y_i Y_j + J_{ij}^z Z_i Z_j \right). \tag{5}$$

We find sufficient conditions for saturation of Inequality (4) and notice that these are a simple generalizations of Toulouse's criterion for the abscence of Geometric Frustration.

Our analysis reveals that the quantum nature of the model affects the very notion of geometric frustration, and in fact, the generality of the considered models points out cases which turn out to be geometrically frustration-free, although a classical analysis would not give conclusive answers. We point out that a deeper understanding of our findings may reveal generic properties which so far failed to be properly generalized. Also, saturation of Inequality (4) has very specific consequences for the spectrum of the two-body reduced density matrices, with potential applications to renormalization algorithms.

References

[1] S. M. Giampaolo, G. Gualdi, A. Monras, and F. Illuminati, *Characterizing and Quantifying Frustration in Quantum Many-Body Systems*, Phys. Rev. Lett. **107**, 260602 (2011).

[2] M. M. Wolf, F. Verstraete, and J. I. Cirac, Int. J. Quant. Inf. **1**, 465 (2003). N. de Beaudrap, M. Ohliger, T. J. Osborne, and J. Eisert, Phys. Rev. Lett. **105**, 060504 (2010). A. Ferraro, A. García-Saez, and A. Acin, Phys. Rev. A **76**, 052321 (2007).

[3] P. Lacorre, J. Phys. C **20**, L775 (1987); A. Sen De, U. Sen, J. Dziarmaga, A. Sanpera, and M. Lewenstein, Phys. Rev. Lett. **101**, 187202 (2008). L. Balents, Nature Phys. **464**, 199 (2010). A. P. Ramirez, Annu. Rev. Mater. Sci. **24**, 453 (1994).

[4] G. Toulouse, Commun. Phys. **2**, 115 (1977).

[5] K. Uyanık and S. Turgut, Phys. Rev. A **81**, 032306, (2010).

Entanglement of phase-random states

Yoshifumi Nakata[1], **Peter S. Turner**[1] **and Mio Murao**[1,2]

[1]*Department of Physics, Graduate School of Science, University of Tokyo, Tokyo 113-0033, Japan*
[2]*Institute for Nano Quantum Information Electronics, University of Tokyo, Tokyo 153-8505, Japan*

Introduction.– Recently, statistical properties of an ensemble of states have been studied in quantum information science, as well as in traditional statistical physics. The most well-studied ensemble of states is that of *random states*, the set of pure states in Hilbert space selected randomly from the unitarily invariant distribution. Random states are useful for performing quantum tasks, and are also studied more generally [1, 2]. It has also been shown that they have extremely high entanglement on average [3],

The studies of random states are reasonable when we analyze generic properties of uniform systems. But, when the system is restricted by constraints such as symmetries or rules of time-evolutions, the set of realizable states is limited. In particular, we consider a system evolving under a time-independent Hamiltonian, where the time evolution changes only the phases of the expansion coefficients in the Hamiltonian's eigenbasis. Our aim is to study random states in such a system, namely, an ensemble of states where the randomness is restricted to the phase of the complex expansion coefficients in a given basis, which we call *phase-random states*.

Phase-random states.– A formal definition of phase-random states is given by the following. *For a given basis $\{|u_n\rangle\}$ of N-qubit Hilbert space, a set of states $\{|\Psi\rangle = \sum_{n=1}^{2^N} r_n e^{i\phi_n}|u_n\rangle\}_{\phi_n}$, where the amplitudes $\{r_n | \sum_n r_n^2 = 1, 0 \leq r_n \leq 1\}$ are fixed and the phases $\{\phi_n\}$ are randomly distributed according to the Lebesgue measure on $[0, 2\pi]$, is said to be a set of phase-random states.*

Phase-random states are closely related to studies of typical properties in statistical mechanics, where derivations of micro-canonical and canonical distributions under time evolution in closed systems are often discussed. It is often assumed that the phases of the expansion coefficients in Hamiltonian eigenstates are randomly distributed after sufficiently long time, which is referred to as *phase ergodicity*. All studies assuming phase ergodicity are equivalent to investigations of statistical properties of phase-random states with corresponding amplitudes and basis. Based on the results in Ref. [2], we give an explicit condition for initial states to give rise to canonical distributions in subsystems by time evolution [4].

Entanglement and simulatability.– Next, we investigate the entanglement properties of phase-random states, which can reveal if the state is simulatable by matrix product states (MPSs). Consider a N-qubit system divided into two subsystems A and $\bar{A}$, composed of N_A and $N_{\bar{A}}$ qubits, respectively. For a given pure state $|\phi\rangle$ and subsystem A, the amount of entanglement in terms of the linear entropy is given by $E_L^{(A)}(|\phi\rangle) = 1 - \text{Tr}(\text{Tr}_{\bar{A}}|\phi\rangle\langle\phi|)^2$. We consider the average amount of entanglement of phase-random states $\langle E_L^{(A)}\rangle_{\text{phase}}$. By denoting the mutual information of $\Phi = \sum r_n^2 |u_n\rangle\langle u_n|$ between A and $\bar{A}$ in terms of the linear entropy by $I_L^{(A)}(\Phi)$, $\langle E_L^{(A)}\rangle_{\text{phase}}$ is given by [4]
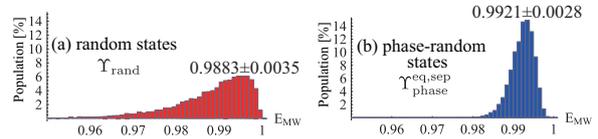
Figure 1: The distributions for $N = 8$ of the amount of entanglement for two ensembles, (a) random states and (b) phase-random states with equal amplitudes and a separable basis, using the Meyer-Wallach measure of entanglement $E_{\text{MW}}(|\phi\rangle) := \frac{2}{N}\sum_{k=1}^{N} E_L^{(\{k\})}(|\phi\rangle)$, where k labels single-qubit subsystems. The number of samples is 10^4, binned in intervals of 0.002.

$$\langle E_L^{(A)}\rangle_{\text{phase}} = I_L^{(A)}(\Phi) - \sum_{n=1}^{2^N} r_n^4 E_L^{(A)}(|u_n\rangle). \quad (1)$$

This result has implications for the simulatability of the dynamics under *time-independent* Hamiltonian in spin systems. By assuming phase ergodicity, the time-average of the amount of entanglement is identified with Eq. (1). In particular, when the Hamiltonian is composed of separable eigenstates and the initial state is a superposition of all eigenstates with equal amplitudes, leading to a separable initial state, the average entanglement is, from Eq. (1), $\langle E_L^{(A)}\rangle_{\text{phase}} = 1 - \frac{2^{N_A} + 2^{N_{\bar{A}}} - 1}{2^N}$. This average is greater than that of random states (see also Fig. 1). It is also shown that entanglement concentrates around its average during the time evolution. Since we can show that a state with such high entanglement is not simulatable by MPSs with a constant matrix size, we conclude that the time evolution cannot be simulated by MPSs [4]. This is surprising at first because all eigenstates as well as the initial state are separable, however the dynamics generate extremely high entanglement and, is therefore difficult to simulate.

References

[1] C. H. Bennett, *et. al.*, IEEE Trans. Inform. Theory, vol. 51, no. 1, pp 56-74 (2005); B. M. Terhal, *et. al.*, Phys. Rev. Lett. 86, 5807-5810 (2001).

[2] N. Linden, *et. al.*, Phys. Rev. E 79, 061103 (2009).

[3] P. Hayden, *et. al.*, Commun. Math. Phys. 250(2):371-391(2004).

[4] Y. Nakata, P. S. Turner and M. Murao, arXiv:1111.2747 (2011).

Quantum dynamics of damped oscillators

T.G. Philbin

School of Physics and Astronomy, University of St Andrews, UK

The quantum theory of the damped harmonic oscillator has been a subject of continual investigation since the 1930s. The obstacle to quantization created by the dissipation of energy has been tackled in various ways, the most popular being to include a reservoir that takes up the dissipated energy. The reservoir generally used consists of a discrete number of harmonic oscillators, and the resulting dynamical system does not directly give a damping proportional to velocity. We show that the use of a continuum reservoir allows an exact canonical quantization of the damped harmonic oscillator with damping proportional to velocity, as well as other damping behaviours. The significance of the results for the theory of nanomechanical oscillators is discussed.

Quantum optics meets real-time quantum field theory: generalised Keldysh rotations, propagation, response and tutti quanti

L.I. Plimak[1] **and S. Stenholm**[1,2,3]

[1] *Institut für Quantenphysik, Universität Ulm, 89069 Ulm, Germany*
[2] *Physics Department, Royal Institute of Technology, KTH, Stockholm, Sweden.*
[3] *Laboratory of Computational Engineering, HUT, Espoo, Finland.*

The connection between real-time quantum field theory (RTQFT) [1] and phase-space techniques [2] is investigated. The Keldysh rotation that forms the basis of RTQFT is shown to be a phase-space mapping of the quantum system based on the symmetric (Weyl) ordering. Following this observation, we define generalised Keldysh rotations based on the class of operator orderings introduced by Cahill and Glauber [3]. Each rotation is a phase-space mapping, generalising the corresponding ordering from free to interacting fields. In particular, response transformation [4] extends the normal ordering of free-field operators to the time-normal ordering of Heisenberg operators. The key property of the normal ordering, namely, cancellation of zero-point fluctuations, is inherited by the response transformation. In this representation, dynamics of the electromagnetic field looks essentially classical (field radiated by current), without any contribution from zero-point fluctuations.

References

[1] A. Kamenev and A. Levchenko, Advances in Physics **58**, 197 (2009), also available as e-print arXiv:0901.3586v3.

[2] E. Wolf and L. Mandel, *Optical Coherence and Quantum Optics* (Cambridge University Press, 1995).

[3] K. E. Cahill and R. J. Glauber, Phys. Rev. **177**, 1882 (1969).

[4] L. I. Plimak and S. Stenholm, Ann. Phys. (N.Y.) **323**, 1989 (2008).

Experimental investigation of the uncertainty principle in the presence of quantum memory

Robert Prevedel[1,2], **Deny R Hamel**[1], **Roger Colbeck**[3], **Kent Fisher**[1] and **Kevin J Resch**[1]

[1] *Department of Physics and Astronomy and Institute for Quantum Computing, University of Waterloo, Waterloo, Canada*
[2] *Research Institute for Molecular Pathology and Max F. Perutz Laboratories GmbH, Vienna, Austria*
[3] *Perimeter Institute for Theoretical Physics, Waterloo, Canada*

Consider an experiment in which one of two measurements is made on a quantum system. In general, it is not possible to predict the outcomes of both measurements precisely, which leads to uncertainty relations constraining our ability to do so. Such relations lie at the heart of quantum theory and have profound fundamental and practical consequences. However, if the observer has access to a particle (stored in a quantum memory) which is entangled with the system, his uncertainty is generally reduced. This effect has recently been quantified by Berta et al. [3] in a new, more general uncertainty relation. Using entangled photon pairs, an optical delay line serving as a quantum memory and fast, active feed-forward we experimentally probe the validity of this new relation. The behaviour we find satisfies the new uncertainty relation. In particular, we find lower uncertainties about the measurement outcomes than would be possible without entanglement.

The first uncertainty relation was formulated by Heisenberg for the case of position and momentum [1]. More recently, driven by information theory, uncertainty relations have been developed in which the uncertainty is quantified by the Shannon entropy [2], rather than the standard deviation. Interestingly, these relations do not apply to the case of an observer holding quantum information about the measured system. In the extreme case that the observer holds a particle maximally entangled with the quantum system, he is able to predict the outcome precisely for both choices of measurement. This dramatically illustrates the need for a new uncertainty relation, which was put forward by Berta *et al.* [3]

$$H(R|B) + H(S|B) \geq \log_2 \frac{1}{c} + H(A|B), \qquad (1)$$

Here the measurement (R or S) is performed on a system, A, and the additional quantum information held by the observer is in B, while the term $1/c$ quantifies the *complementarity* of the observables. The Shannon entropy of the outcome distribution is replaced by $H(R|B)$, the conditional von Neumann entropy, quantifying the uncertainty about the outcome of a measurement of R given access to B. This relation is a strict generalization of [2] and features an additional term on the right-hand-side. This term is a measure of how entangled the system A is with the observer's particle, B, expressed via $H(A|B)$. Note that this quantity can be *negative* for entangled states and in this case lowers the bound on the sum of the uncertainties. In particular, if ρ_{AB} is maximally entangled, $H(A|B) = -\log_2 d$, where d is the dimension of the system. Since the RHS of (1) cannot be greater than zero for a maximally entangled state, both R and S are perfectly predictable in such a case. From a fundamental point of view, this highlights the additional power an observer holding quantum information about the system has compared to
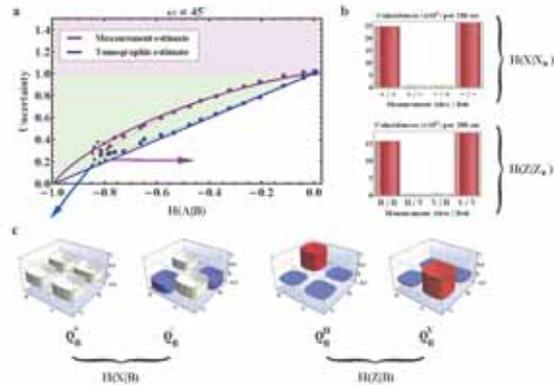
Figure 1: Experimental results. In (a) we plot the left-hand side (LHS) of the new inequality (1) for the case where $R = X$ and $S = Z$ with varying entanglement $H(A|B)$. To calculate $H(X|B) + H(Z|B)$ we evaluate the entropies of the conditional single-qubit density matrices of Bob's qubit which we obtain through quantum state tomography (blue dots), see (c). We also perform projective measurements on Bob's side, obtaining $H(X|X_B) + H(Z|Z_B)$ (purple dots) directly from the obtained coincidence count rates (b). Solid lines represent the theoretical bounds, while the dashed lines are simulations. Figure taken from [4].

an observer holding classical information.

In our work [4], we test the new inequality of Berta *et al.* experimentally using entangled photon states and an optical delay serving as a simple quantum memory. Entanglement allows us to achieve lower uncertainties about both observables than would be possible with only classical information over a wide range of experimental settings. This shows not only that the reduction in uncertainty enabled by entanglement can be significant in practice, but also demonstrates the use of the inequality to witness entanglement. Our work addresses a cornerstone relation in quantum mechanics and, to the best of our knowledge, is the first to test one of its entropic versions.

References

[1] W. Heisenberg, Z. Phys. **43**, 172 (1927).

[2] H. Maassen and J. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

[3] M. Berta *et al.*, Nature Physics, **6**, 659 (2010).

[4] R. Prevedel *et al.*, Nature Physics, **7**, 757 (2011).

Entanglement and Quality of Composite Bosons

Pawel Kurzynski,[1,2] **Ravishankar Ramanathan,**[1] Akihito Soeda,[1]
Tan Kok Chuan,[1] Marcelo F. Santos,[3] and Dagomir Kaszlikowski[1,4,*]

[1]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2]*Faculty of Physics, Adam Mickiewicz University, Umultowska 85, 61-614 Poznań, Poland*
[3]*Departamento de Física, Universidade Federal de Minas Gerais,*
Belo Horizonte, Caixa Postal 702, 30123-970, MG, Brazil
[4]*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*

Most particles in Nature are not elementary, and are in fact composed of elementary fermions and bosons. These composite particles can exhibit a variety of behaviors ranging from fermionic to bosonic depending on the the state of the system and the physical situation at hand. The bosonic behavior of composite bosons such as excitons, especially in the context of Bose-Einstein condensation has been studied (see for example [1]), and it is found that excitons behave as bosons when their density is low so that the overlap of the fermionic wave functions can be neglected. A careful analysis of the wave functions of experimentally achieved condensates clearly indicates entanglement between certain degrees of freedom of the constituent fermions. This fact was first investigated in [2, 3] where it was hypothesized that the amount of entanglement between the constituent fermions plays a substantial role.

Let us consider the simple scenario of a composite boson made of two distinguishable fermions such as an exciton, hydrogen atom, positronium, etc. Each fermion is described by a single internal degree of freedom (spin or energy eigenstates of a confining trap). In general, the state of a composite boson made of two distinguishable fermions of type A and B is

$$|\psi\rangle_{AB} = \sum_n \sqrt{\lambda_n} a_n^\dagger b_n^\dagger |0\rangle,$$

where $a_n^\dagger (b_n^\dagger)$ creates a particle of type A (B) in mode n, and λ_n is the probability of occupation of mode n. Standard anti-commutation rules apply, i.e., $\{K_n, K_m^\dagger\} = \delta_{nm}$ ($K = a, b$). The number of non-zero coefficients λ_n is the Schmidt number of this state and the state is entangled when it is larger than one. It has been shown [2–4] that the bosonic behavior of composite particles made of two distinguishable fermions is related to the amount of entanglement between the two fermions. The quality of bosonic behavior was measured by the deviation from identity in number states of the commutator between the annihilation and creation operators. It was shown that as the entanglement increases, the commutation relation for the annihilation and operators of these composite particles approaches that for ideal bosons. However, in general the behavior of these systems is more complicated and not entirely captured by the average value of the commutator in the number state. These particles can in fact exhibit a variety of behavior in two-particle interference and particle addition-subtraction experiments which is not detected by the commutator approach.

In this talk, we will refine and further develop the hypothesis linking entanglement and bosonic behavior and show that a large amount of entanglement, while necessary, is not sufficient for the display of bosonic behavior. Unlike in the previous approaches which focused on mathematical aspects such as the commutation relations, we concentrate on the physical aspect of the display of bosonic properties, such as the formation of a condensate. Fermionic and bosonic behavior of composite particles are captured by the fundamental operations of addition and subtraction of single composite particles. For fermions, addition to an already occupied state is forbidden by the Pauli principle while for bosons, it is easier to add a particle to an already occupied state than for distinguishable particles. The operations of single particle addition and subtraction are known to be probabilistic and are best described by the language of completely positive maps and Kraus operators. The success probability of these operations is related to the quality of fermionic or bosonic behavior of the particles. Another physical situation that we will consider is two-particle interference, where bosonic behavior is captured by the tendency of particles to bunch, while fermionic behavior is related to their tendency to anti-bunch. This approach clarifies the importance of entanglement and allows us to link it to other criteria discussed in the literature.

---

[1] *Bose-Einstein Condensation*, edited by A. Griffin, D. W. Snoke, and S. Stringari (Cambridge University Press, Cambridge, 1995).
[2] C. K. Law, Phys. Rev. A **71**, 034306 (2005).
[3] C. Chudzicki, O. Oke, W. K. Wootters, Phys. Rev. Lett. **104**, 070402 (2010).
[4] R. Ramanathan, P. Kurzynski, T. K. Chuan, M. F. Santos and D. Kaszlikowski, Phys. Rev. A **84**, 034304 (2011).
[5] P. Kurzynski, R. Ramanathan, A. Soeda, T. K. Chuan and D. Kaszlikowski, arXiv/quant-ph: 1108.2998 (2011).

The elusive Heisenberg limit in quantum enhanced metrology

Rafal Demkowicz-Dobrzanski[1], **Jan Kolodynski**[1] **and Madalin Guta**[2]

[1] *University of Warsaw, Faculty of Physics, Warsaw, Poland*
[2] *University of Nottingham, School of Mathematical Sciences, Nottingham, UK*

Quantum precision enhancement is of fundamental importance for the development of advanced metrological experiments such as gravitational wave detection and frequency calibration with atomic clocks. Precision in these experiments is limited by the $1/\sqrt{N}$ *shot-noise scaling* (SS) with N being the number of probes (photons, atoms) employed in the experiment. The bound is due to the independent character of the sensing process for each of the probes and can only be overcome when the probes are prepared in an appropriately entangled state, as schematically depicted in Fig. 1**a**. In an ideal scenario, i.e. the case of a unitary evolution, it is then possible to beat $1/\sqrt{N}$ and achieve the *Heisenberg scaling* (HS) of precision $1/N$.
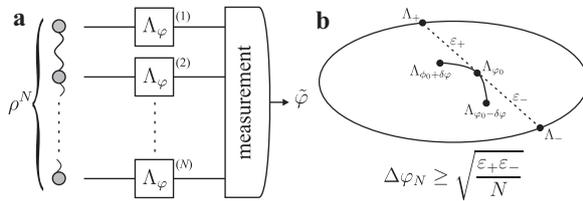
Figure 1:
a: General scheme for quantum enhanced metrology. N-probe quantum state fed into N parallel channels is sensing an unknown channel parameter φ. An estimator $\tilde{\varphi}$ is inferred from a measurement results on the output state.
b: Schematic representation of a local classical simulation of a channel that lies *inside* the convex set of quantum channels. The construction instantly provides a lower bound on the estimation precision, $\Delta\varphi_N$, for N channels used in parallel.

To the contrary, in article [1], we show that if *almost any* type of arbitrarily weak decoherence is taken into account, the $1/N$ scaling is lost. Such behavior has already been proved for the cases of optical interferometry with photonic losses [2, 3] and atomic spectroscopy with noise modeled as dephasing [4]. We generalize those results by developing the methods of [5, 6], in order to establish a universal scheme for deriving upper bounds on the achievable precision in quantum metrological schemes. In particular, for some models, e.g. atomic clocks frequency calibration with dephasing, the calculation becomes straightforward and may be performed using an intuitive geometric picture. All that is necessary is the distance of a point representing the decoherence process from the boundary of the set of all quantum channels, as schematically represented in Fig. 1**b**. Our results prove that in the asymptotic limit of infinite resources, $N \to \infty$, even infinitesimally small noise turns HS into SS, so that the quantum gain amounts then at most to a constant factor improvement, e.g. the $\mathrm{const}/\sqrt{N}$ factor for the optical interferometer case plotted in Fig. 2.

Furthermore, we demonstrate that SS bounds can be de-
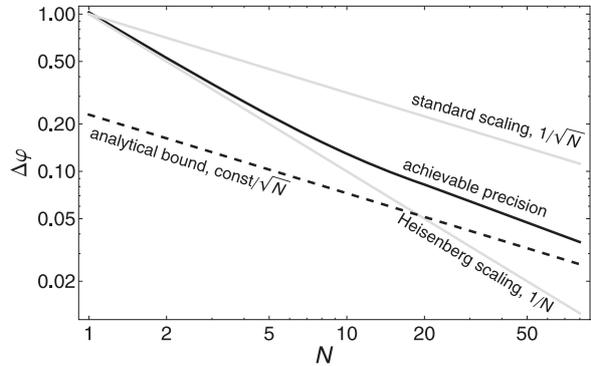
Figure 2: Log-log plot of the dependence of quantum enhanced phase estimation uncertainty on the number of photons N in a Mach-Zehnder interferometer with 5% losses in both arms.

rived for nearly all types of decoherence models by analyzing the structure of a single use of the decoherence channel, regardless of both the choice of input states and the measurement strategies of estimation. While in [5, 6] it has been proved that SS bounds can be derived for all full rank channels, i.e. the ones that do not lie at the boundary of the set of all physical channels, we show that those methods may be applied to a more general class including the ones lying on the boundary of the set.

Finally, employing our results, we calculate SS bounds for the most important decoherence models in quantum metrology such as: dephasing, depolarization, spontaneous emission and losses inside an interferometer. These are compared with the ones obtained previously in the literature using systematic, but much more computationally demanding, methods such as [4].

References

[1] R. Demkowicz-Dobrzanski, J. Kolodynski and M. Guta, ArXiv e-prints, 1201.3940 (2012).

[2] J. Kolodynski and R. Demkowicz-Dobrzanski, Phys. Rev. A, **82**, 053804 (2010).

[3] S. Knysh, V. N. Smelyanskiy and G. A. Durkin, Phys. Rev. A, **83**, 021804(R) (2011).

[4] B. M. Escher, R. L. de Matos Filho, and L. Davidovich, Nature Physics, **7**, 406 (2011).

[5] K. Matsumoto, ArXiv e-prints, 1006.0300v1 (2010).

[6] A. Fujiwara and H. Imai, J. Phys. A: Math. Theor., **41**, 255304 (2008).

A micropillar for cavity optomechanics

Aurélien G. KUHN[1], Emmanuel Van Brackel[1], Leonhard NEUHAUS[1], Jean TEISSIER[1], Claude CHARTIER[2], Olivier DUCLOUX[2], Olivier Le TRAON[2], Christophe MICHEL[3], Laurent PINARD[3], Raffaele FLAMINIO[3], Samuel DELEGLISE[1], Tristan BRIANT[1], Pierre-François COHADON[1] and Antoine HEIDMANN[1]

[1]*Laboratoire Kastler Brossel, École Normale Supérieure - Université Pierre et Marie Curie - CNRS, Paris, France.*
[2]*ONERA, Châtillon, France.*
[3]*Laboratoire des Matériaux Avancés, IN2P3 - CNRS, Lyon, France.*

Reaching the quantum ground state of a macroscopic mechanical object is a major experimental challenge in physics at the origin of the rapid emergence of the cavity optomechanics research field. Many groups have been targeting this objective for a decade using a wide range of resonators and different techniques of displacement sensing. The development of a very sensitive position sensor combined with a mechanical resonator in its ground state would have important consequences not only for fundamental aspects in quantum physics such as entanglement and decoherence of mechanical resonators but also for potential applications such as the detection of very weak forces.

Two conditions have to be fulfilled in order to reach and demonstrate the mechanical ground state. The thermal energy $k_B T_c$ has to be small with respect to the zero-point quantum energy $h\nu_m$. For a resonator oscillating at a frequency $\nu_m = 4$ MHz, T_c is in the sub-mK range and conventional cryogenic cooling has to be combined with novel cooling mechanisms such as radiation pressure cooling. The second requirement is to be able to detect the very small residual displacement fluctuations associated with the quantum ground state. The measurement sensitivity must be better than the expected displacement noise at resonance, which scales as:

$$S_x^{zpm}[\nu_m] = \frac{25\mu g}{M} \frac{Q_c}{2\,000} \left(\frac{4\text{MHz}}{\nu_m}\right)^2 10^{-38} \text{m}^2/\text{Hz}, \quad (1)$$

where M is the effective mass of the resonator and Q_c its mechanical quality factor.

We have developed experiments based on high finesse optical cavities (up to 50 000) where the displacement of the moving micromirror is monitored with a sensitivity at the 10^{-38} m²/Hz level. Our group has already performed optical cooling [1] of the micromirror both at room temperature and at 4 K. As all active cooling mechanisms increase the damping, Q_c in equation (1) is the final quality factor related to the quality factor Q of the resonator by $Q_c T_c = QT$, where T_c/T is the cooling ratio. We have therefore developed a new generation of micro-resonator with an ultra-high Q, up to 2 000 000, suitable for a cryogenic temperature of 100 mK in order to ensure a sufficient $Q_c \approx 1000$ at the final effective temperature [2].

The resonator consists in a 1 mm-long micropillar mechanically decoupled from the wafer by a dynamical frame and clamped at its center by a thin membrane [3]. A high-reflectivity mirror is coated on top of the pillar, allowing us to build a high-finesse cavity for interferometric sensing of the resonator vibrations. This requires the use of a small optical beam waist (10 μm), compatible with the pillar transverse size of 100 μm. We thus developed coupling mirrors with small radius of curvature (1 mm) integrated in a 500-μm length and high-finesse (50 000) Fabry-Perot cavity. We finally developed a specific dilution fridge with optical accesses and working at a base temperature of 100 mK with 500 W of incident laser power.

We have observed the thermal noise spectrum both at room temperature and in the dilution fridge environment at about 100 mK, using a quantum-limited interferometric measurement (see figure).
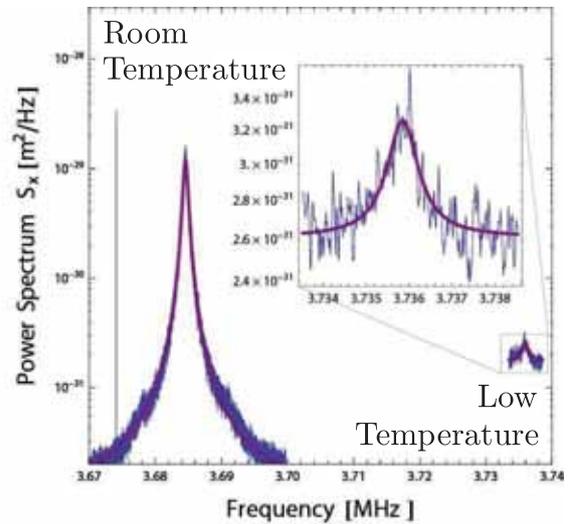
We expect to reach the ground state of such a low mass and ultra-high quality factor micropillar by using an active cooling technique, and then be able to observe its quantum fluctuations thanks to the sensitivity of the high-finesse cavity.

References

[1] O. Arcizet *et al.*, Radiation-pressure cooling and optomechanical instability of a micromirror, Nature, **444**, 71 (2006).

[2] A. G. Kuhn *et al.*, A micropillar for cavity optomechanics, Applied Physics Letters, **99**, 121103 (2011).

[3] M. Bahriz and O. Le Traon, French Patent, **FR 10 02 829** (2010).

Calculating errors in quantum tomography: diagnosing systematic vs statistical errors

Nathan K. Langford[1]

[1]*Royal Holloway University of London, Egham, United Kingdom*

One of the greatest challenges associated with experimentally demonstrating some quantum information processing (QIP) protocol is to be able to verify and quantify its successful operation. In some cases, such as Bell [1] and steering [2] tests of nonlocal quantum phenomena and Kochen-Specker tests of noncontextuality [3], this can be achieved by violating a measurement inequality. In other cases, such as Shor's factoring algorithm [4], the success of the protocol can be readily tested after the fact via a simple test of the "correctness" of the outcome or answer. Often the answer is not so clear cut [5], however, and quantum tomography can be a valuable tool for achieving this goal. This might, for example, take the form of measuring the process directly via quantum process tomography (QPT) [6], or characterising the state at key stages of the protocol via quantum state tomography (QST) [7].

When wishing to verify the success of a protocol or quantify its reliability, it is critical to have a rigorous and comprehensive recipe for calculating experimental errors. In Bayesian approaches to tomography, such as Bayesian mean estimation [8] or Kalman filtering reconstruction [9], the method provides errors automatically as part of the reconstruction output. Currently, the most commonly used method of tomographic reconstruction, however, is maximum-likelihood estimation [10, 11]. The formal output of this approach, however, is a single quantum state, the state which mathematically maximises the likelihood function, with no intrinsic uncertainty. Maximum-likelihood tomography therefore needs to be augmented in some way to allow the experimenter to estimate errors. In the last decade or so, as ever more experiments have relied on tomography in their results, this idea has gradually received more attention. In the last few years, several methods have been proposed for doing this, e.g., [12, 13]. Perhaps the most common way to calculate errors in maximum-likelihood tomography is to use Monte-Carlo methods. Here, I explore this approach from a pragmatic, experimentalist's perspective, with particular attention to the different types of errors that arise in an experimental tomography scenario. I discuss the limitations of Monte-Carlo error estimation and introduce a simple measure of "fit quality" which can be used to overcome some of these limitations.

There are three main sources of error that arise during a tomographic procedure. Firstly, errors may be introduced as a result of inaccuracies in the measurement system, either detection or preparation (in the case of QPT). Secondly, statistical errors arise automatically from the finite precision of any measurement made on a finite number of system copies. Finally, in any procedure involving data fitting, there will be some error associated with how poorly or how well the data fit is achieved. Ultimately, all of these errors will combine to affect any experimental estimates of physical quantities derived from the density matrix, such as entanglement and en-
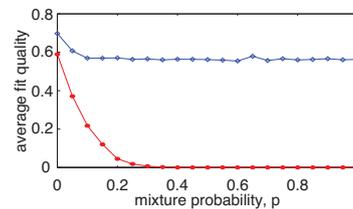
Figure 1: Fit quality for minimum (red) and over-complete (blue) tomographies as a function of mixture probability.

tropy for quantum states. To date, most errors reported in QIP experiments consider only the second type of error and ignore errors which arise, for example, as a result of inaccurate measurements. Doing this can be reasonably well justified is some cases where statistical errors are the dominant source of noise. For example, in photonic experiments involving polarisation qubits, the measurement operations can be made using extremely high-precision wave plates and polarisers and are very well characterised and understood. This is arguably much less reasonable in the case of superconducting quantum circuits, however, where systematic errors and imprecision in measurement settings can strongly dominate over statistical errors. I discuss how the fit quality parameter can be used in conjunction with the Monte-Carlo method to diagnose, for example, the presence of unexpected systematic measurement errors and to probe the level of effect of physicality constraints are imposing on the reconstruction. Finally, I look at how this parameter can be used to influence tomographic measurement design (Fig. 1).

References

[1] J. F. Clauser *et al.*, Phys. Rev. Lett. **23**, 880 (1969)

[2] H. M. Wiseman *et al.*, Phys. Rev. Lett. **98**, 140402 (2007)

[3] A. A. Klyachko *et al.*, Phys. Rev. Lett. **101**, 020403 (2008)

[4] P. W. Shor, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, p124 (1994)

[5] A. G. White *et al.*, J. Opt. Soc. Am. B **24**, 172 (2007)

[6] I. L. Chuang and M. A. Nielsen, J. Mod. Opt. **44**, 2455 (1997)

[7] D. T. Smithey *et al.*, Phys. Rev. Lett. **70**, 1244 (1993)

[8] R. Blume-Kohout, New J. Phys. **12**, 043034 (2010)

[9] K. M. R. Audenaert and S. Scheel, New J. Phys. **11**, 023028 (2009)

[10] Z. Hradil, Phys. Rev. A **55**, R1561 (1997)

[11] D. F. V. James *et al.*, Phys. Rev. A **64**, 052312 (2001)

[12] R. Blume-Kohout, Phys. Rev. Lett. **105**, 200504 (2010)

[13] R. Blume-Kohout, arXiv:1202.5270 (2012)

Quantum measurement bounds beyond the uncertainty relations

Vittorio Giovannetti[1], Seth Lloyd[2], __Lorenzo Maccone__[3]

[1]*NEST, Scuola Normale Superiore and Istituto Nanoscienze-CNR, piazza dei Cavalieri 7, I-56126 Pisa, Italy*
[2]*Dept. of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[3]*Dip. Fisica "A. Volta", INFN Sez. Pavia, Università di Pavia, via Bassi 6, I-27100 Pavia, Italy*

This talk is based on the research presented in [1] and [2].

Quantum mechanics limits the accuracy with which one can measure conjugate quantities: the Heisenberg uncertainty relations [3, 4] and the quantum Cramér-Rao inequality [5, 6, 8, 7] show that no procedure for estimating the value of some quantity (e.g., a relative phase) can have a precision that scales more accurately than the inverse of the *standard deviation* of a conjugate quantity (e.g., the energy) evaluated on the state of the probing system. Here we present a new bound on quantum measurement: we prove that the precision of measuring a quantity cannot scale better than the inverse of the *expectation value* (above a 'ground state') of the conjugate quantity. We use the bound to resolve an outstanding problem in quantum metrology [9]: in particular, we prove the longstanding conjecture of quantum optics [10, 11, 12, 13, 14, 15] – recently challenged [16, 17, 18] – that the ultimate limit to the precision of estimating phase in interferometry is bounded below by the inverse of the total number of photons employed in the interferometer.

The new bound is derived using an extension [19] to the Margolus-Levitin theorem [20] that limits the speed of evolution of any quantum system (the "quantum speed limit"). We first connect the fidelity between the initial and final state of the probe systems to the error in the estimation through the Tchebychev inequality, and then we use the quantum speed limit to connect the fidelity with the expectation value of the generator of translations (i.e. the "conjugate" quantity) of the parameter to be estimated.

I then report how the newly proposed sub-Heisenberg strategies can bypass our bound, by considering situations where the prior information is very large. However, such estimations are basically useless [2]: one can achieve a comparable precision without performing any measurement, just using the large prior information that sub-Heisenberg strategies require. For uniform prior (i.e. no prior information), we prove that these strategies cannot achieve more than a fixed gain of about 1.73 over Heisenberg-limited interferometry. Analogous results hold for arbitrary single-mode prior distributions, and also beyond interferometry: the effective error in estimating any parameter is lower bounded by a quantity proportional to the inverse expectation value (above a ground state) of the generator of translations of the parameter.

References

[1] V. Giovannetti, S. Lloyd, L. Maccone, arXiv:1109.5661 (2011).

[2] V. Giovannetti, L. Maccone, arXiv:1201.1878 (2012).

[3] W. Heisenberg, *Zeitschrift für Physik* **43**, 172 (1927), English translation in Wheeler J.A. and Zurek H. eds., *Quantum Theory and Measurement* (Princeton Univ. Press, 1983), pg. 62.

[4] H.P. Robertson, *Phys. Rev.* **34**, 163 (1929).

[5] A.S. Holevo, *Probabilistic and Statistical Aspect of Quantum Theory* (Edizioni della Normale, Pisa 2011).

[6] C.W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[7] S.L. Braunstein, C.M. Caves, *Phys. Rev. Lett.* **72**, 3439 (1994).

[8] S.L. Braunstein, C.M. Caves, G.J. Milburn, *Annals of Physics* **247**, 135 (1996).

[9] V. Giovannetti, S. Lloyd, L. Maccone, *Nature Phot.* **5**, 222 (2011).

[10] S.L. Braunstein, A.S. Lane, C.M. Caves, *Phys. Rev. Lett.* **69**, 2153 (1992).

[11] B. Yurke, S.L. McCall, J.R. Klauder, Phys. Rev. A **33**, 4033 (1986).

[12] B.C. Sanders, G.J. Milburn, *Phys. Rev. Lett.* **75**, 2944 (1995).

[13] Z.Y. Ou, *Phys. Rev. A* **55**, 2598 (1997); Z.Y. Ou, *Phys. Rev. Lett.* **77**, 2352 (1996).

[14] J.J. Bollinger, W.M. Itano, D.J. Wineland, D.J. Heinzen, *Phys. Rev. A* **54**, R4649 (1996).

[15] P. Hyllus, L. Pezzé, A. Smerzi, *Phys. Rev. Lett.* **105**, 120501 (2010).

[16] P.M. Anisimov, et al., *Phys. Rev. Lett.* **104**, 103602 (2010).

[17] A. Rivas, A. Luis, arXiv:1105.6310v2 (2011).

[18] Y.R. Zhang, et al., arXiv:1105.2990v2 (2011).

[19] V. Giovannetti, S. Lloyd, L. Maccone, *Phys. Rev. A* **67**, 052109 (2003).

[20] N. Margolus, L.B. Levitin, *Physica D* **120**, 188 (1998).

Noiseless Image Amplification

__Alberto M. Marino__[1], __Neil Corzo__[1,2], __Kevin M. Jones__[3]__, and Paul D. Lett__[1]

[1]*Joint Quantum Institute, National Institute of Standards and Technology and the University of Maryland, Gaithersburg, MD 20899 USA*
[2]*Departamento de Física, CINVESTAV-IPN, México D.F., 07360, México*
[3]*Department of Physics, Williams College, Williamstown, MA 01267 USA*

Introduction

Quantum mechanics predicts that any optical amplifier must add a certain level of noise [1]. It is, however, possible to implement an amplifier, known as a phase-sensitive amplifier (PSA), in which both the signal and the noise are amplified by the same amount. This leaves the signal-to-noise ratio (SNR) unchanged after the amplification process and thus the PSA acts as a noiseless amplifier. The ability to implement such an amplifier is of practical importance for applications that range from communication systems to enhanced sensitivity of measurements and has been an active area of research for a long time. There is also significant interest in performing noiseless amplification of multiple spatial modes simultaneously, thus making it possible to noiselessly amplify an image. We show that four-wave mixing (4WM) in rubidium atomic vapor can act as a PSA that supports hundreds of spatial modes and operates near the ideal limit of a noiseless amplifier.

Phase-sensitive amplifier

To implement a PSA we use a 4WM process in a double-Λ scheme [2, 3]. In this configuration two strong pump beams and a weak probe beam are combined at a slight angle inside a rubidium cell. When the phases of the fields are properly selected, the 4WM leads to a transfer of one photon from each of the two pumps to two photons of the probe and thus gain.

The performance of the amplifier is quantified with the noise figure, $NF = SNR_{in}/SNR_{out}$. Since an ideal PSA conserves the SNR of the input, it will have $NF = 1$ independent of its gain. In practice the efficiency of the detection system needs to be taken into account. This leads to a reduction of the NF, making values slightly less than one possible. The gain of the 4WM-based PSA can be changed by modifying a number of different experimental parameters, such as the frequency of the fields, the power of the pumps, or the temperature of the cell. We have explored this parameter space and measured NFs as low as 0.98 for gains of the order of 4 with a detection efficiency of 91%.

Multi-Spatial-Mode Properties

One of the most important properties of the 4WM-based PSA is its multi-spatial-mode character. To illustrate this point we image an "N"-shaped beam into the amplifier and characterize the amplified output, shown in the inset of Fig. 1. For this image we have measured $NF = 0.98$ for a gain of 4.6 and a detection efficiency of 88%. The fact that the PSA preserves the NF for different spatial patterns is an indication of its multi-spatial-mode character. To unambiguously show the multi-spatial-mode behavior of the amplifier, we performed measurements of the NF as a function of spatial losses, as shown in Fig. 1. For a single-spatial-mode PSA the
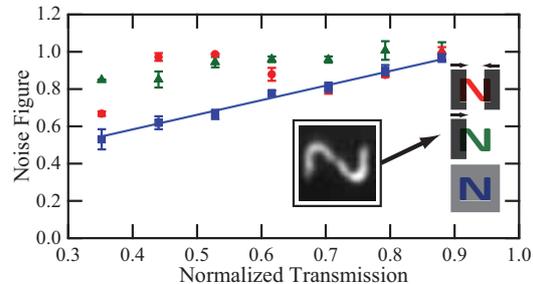
Figure 1: Noise figure as a function of normalized transmission after attenuation with an ND filter (blue squares), cutting with a slit (red circles), and cutting with a razor blade from one side (green triangles). The blue line shows the expected behavior for a single-spatial-mode PSA.

NF should always scale linearly with attenuation (blue line), independent of its origin. Any deviation from this behavior shows the multi-spatial-mode nature of the amplifier. We performed three different measurements on the output "N"-shaped beam: attenuation of the whole image with an ND filter (blue squares), cutting with a slit (red circles), and cutting with a razor blade from one side (green triangles). As can be seen from Fig. 1, attenuating with an ND filter leads to the linear behavior expected for a single mode, as a result of having all the spatial modes equally attenuated. When spatially clipping, however, the behavior of the NF deviates from the expected one for a single spatial mode. Although a greater knowledge of the mode structure of the PSA is needed to fully understand the behavior shown in Fig. 1, the difference in behavior between the three different methods is a signature of the multi-mode nature of the PSA.

To obtain a quantitative measure of the number of modes supported by the amplifier we measured the spatial resolution and the area of the gain region of the PSA. From these measurements we found that the amplifier can support over 35 line pairs per millimeter in each of the transverse directions and that the gain region has an area of approximately 0.21 mm^2. This leads to an estimate of the spatial bandwidth product of over 1000 for the 4WM-based amplifier.

References

[1] C. M. Caves, Phys. Rev. D **26**, 1817 (1982).

[2] V. Boyer, A. M. Marino, and P. D. Lett, Phys. Rev. Lett. **100**, 143601 (2008).

[3] R. C. Pooser, A. M. Marino, V. Boyer, K. M. Jones, and P. D. Lett, Phys. Rev. Lett. **103**, 010501 (2009).

A complete characterization of the OPO, leading to hexapartite entanglement

Felippe A. S. Barbosa[1], **Antônio S. Coelho**[1], **Alessandro Villar**[2], **Katiúscia N.Casemiro**[2], **Paulo Nussenzveig**[1], **Claude Fabre** [2], and **Marcelo Martinelli**[1]

[1]*Instituto de Física - USP, São Paulo, Brazil*
[2]*Departamento de Física - UFPE, Recife, Brazil*
[3]*Laboratoire Kastler-Brossel - UPMC-Paris 6, France*

Homodyne detection, combined with heterodyne electronic demodulation [1], has been at the heart of many measurements of continuous variables in quantum optics. From a given mode of the field at frequency ω, homodyne detection gives the measurement of the quadrature $\hat{X}_\theta(t) = \hat{a}(t)e^{i\theta} + \hat{a}^\dagger(t)e^{-i\theta}$, given in terms of creation and annihilation operators, and the relative phase θ between the mode under study and the optical local oscillator of the same frequency. While this measurement technique can be used to obtain a complete reconstruction of the state at a given frequency ω by tomographic methods, there is the challenge of overcoming the classical noise of the light sources around the local oscillator optical frequency.

These classical sources of noise are the reason why many systems involved in entanglement or squeezing measurements use the demodulation of the measured photocurrent with the help of an electronic reference at frequency Ω. In this case, the resulting measurement corresponds to the beat-note of the sideband modes at frequencies $\omega \pm \Omega$ with the central carrier. Therefore, the resulting evaluation is always obtained for a combination of creation and annihilation operators at these sidebands frequencies. Although it is widely used by the community, the resulting measurement cannot be considered complete, unless strict symmetries between the sidebands are assumed, involving balanced number of photons on the detected sidebands, as well as the stability of the involved fields over the measurement process.

While these symmetries are supposed to be valid for many situations dealing with squeezed vacuum, there are still many states for which those conditions are not satisfied, and the reconstruction is incomplete[2]. As an example, we investigate the case of the optical parametric oscillator, in above threshold operation.

In this case, the production of pairs of photons in signal and idler beams occurs inside the bandwidth of the optical cavity by annihilation of pump photons. While this process should produce balanced states which are in principle completely measurable by the homodyning technique, the process of exchange of photons between signal and pump modes, assisted by idler photons, and its counterpart involving exchange of idler and pump photons, produces intrinsically unbalanced modes.

A way to completely recover the information of the sidebands involves the use of analysis optical cavities[3] in a self homodyne technique. In this case, the phase of each sideband mode and carrier are shifted independently, enabling a complete reconstruction of the modes in the sideband description. The measurement can now be considered complete, if the state is considered to be stable (i.e. free of phase diffusion) during the measurement process, a much less stringent

demand that can be experimentally tested.

We apply this technique to the complete reconstruction of the field modes produced by the OPO dynamics. We perform the complete measurement of the pair of sidebands of each mode (pump, signal and idler), recovering the complete hexapartite covariance matrix of the sidebands modes produced by the OPO at the detected sideband frequency. For Gaussian states the covariance matrix gives the complete information of the density operator.

Using the covariance matrix, we test different bipartitions of the system, in this manner experimentally probing the structure of entanglement present in this case[4]. We observe hexapartite entanglement directly generated in the OPO. We analyze different combinations of partitions, and compare the results with those from usual homodyne techniques. Consequences of this higher order entanglement are discussed for other systems, as well as its application for quantum information processing.
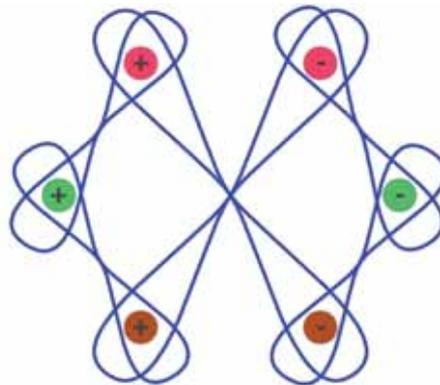
Figure 1: A pictoric view of hexapartite entanglement in the above threshold OPO, generated by exchange of photons between upper bands (+) of pump and idler modes, or pump and signal modes [and their counterpart for the lower bands (-)], and pair production in upper band of signal and lower band of idler modes (and vice versa).

References

[1] J. H. Shapiro, IEEE J. Quantum Electr. **21**, 237 (1985).

[2] T. Golubeva, Yu. Golubev, C. Fabre, and N. Treps, Eur. Phys. J. D **46**, 179 - 193 (2008).

[3] A. S. Villar, Am. J. Phys. **76**, pp. 922-929 (2008).

[4] R. F. Werner, M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).

QCMC 2012
Vienna, Austria

High Resolution Measurement of Polarization Mode Dispersion (PMD) in Telecom Switch using Quantum Interferometry

<u>O.V. Minaeva</u>[1,2], A.M. Fraine[1], R. Egorov [1], D. S. Simon[1,4], and A. V. Sergienko[1,3]

[1]*Dept. of Electrical & Computer Engineering, Boston University, Boston, Massachusetts 02215*
[2]*Dept. of Biomedical Engineering, Boston University, Boston, Massachusetts 02215*
[3]*Dept. of Physics, Boston University, Boston, Massachusetts 02215*
[4]*Dept. of Physics and Astronomy, Stonehill College, 320 Washington Street, Easton, MA 02357*

The need for high-resolution dispersion measurements is drastically increasing with current trends in fiber optic networks adopting 40Gb, 100 Gb and even greater speed. The size of metropolitan network components such as modern optical routers and switches decreases while the amount of data transmitted over fiber optic networks is getting greater and greater. The aggregate effect of many components in a network is becoming substantial for endangering a clear signal delivery, so it is important to measure the contribution from each individual component since the optical paths of two pulses with the same origin and destination may differ.

The use of quantum interferometry using polarization entangled states has been shown to provide a new ground for an accurate measurement of PMD [1, 2, 3] that has the potential to go beyond the limitations of classical techniques such as white light interferometry [5] and the Jones Matrix Eigenanalysis (JME) method [6]. In this paper, a quantum interferometric measurement of the PMD of a commercially available wavelength selective switch (WSS) is presented.

To demonstrate the use of quantum interferometry for high-resolution PMD measurements, we measure the group delay from a (1x9) 96 channel MEMS-based WSS with 50 GHz channel spacing [4]. We exploit the properties of collinear Type II spontaneous parametric down conversion that produces correlated orthogonally polarized photons. By sending this state into a non-polarization dependent beam splitter, a superposition of modes allows for the post-selection of a polarization-entangled state through coincidence detection. By measuring the timing delay between these two photons through a sample, the differential group delay is extracted (see Fig. 1).

Figure 2: Comparison of interferogram before (a) and after (b) the switch is introduced.

tum interferometric technique using polarization-entangled states to evaluate the PMD of a commercially available telecom device (see Fig. 2) Several additional improvements will be required in order to fully introduce quantum interferometry into an industrial setting and to exploit the unique features of the quantum states of light such as even order dispersion cancellation. Despite this, an upper bound on the PMD of this particular telecom device (WSS) was determined at the level sufficiently below the resolution of commercially available measurement devices tailored for the traditional task of measuring large differential group delays in optical fibers.

References

[1] E. Dauler, G. Jaeger, A. Muller, A.L. Migdall, A.V. Sergienko, J. Res. Natl. Inst. Stand. Technol., **104**, 1 (1999).

[2] D. Branning, A.L. Migdall, A.V. Sergienko, Phys. Rev. A, **62**, 063808 (2000).

[3] A. Fraine, D.S. Simon, O. Minaeva, R. Egorov, A.V. Sergienko, Opt. Exp., **19**, 22820 (2011).

[4] A. Fraine, O. Minaeva, D.S. Simon, R. Egorov, and A.V. Sergienko, Optics Express, v. **20**, pp. 2025-2033 (2012).

[5] S. Diddams, J. Diels, J. Opt. Soc. Am. B 13, 1120 (1996).

[6] B.L. Heffner, IEEE Phot. Tech. Lett., 5, 787 (1993).

Figure 1: Setup for PMD measurement in MEMS-based WSS.

We have demonstrated the first results of applying a quan-

Four-State Discrimination via a Hybrid Receiver

<u>C. R. Müller</u>[1,2], M. A. Usuga[3,1], C. Wittmann[1,2], M. Takeoka[4], Ch. Marquardt[1,2], U. L. Andersen[3,1] and G. Leuchs[1,2]

[1]*Max Planck Institute for the Science of Light, Erlangen, Germany*
[2]*Department of Physics, University of Erlangen-Nuremberg, Germany*
[3]*Department of Physics, Technical University of Denmark, Kongens Lyngby, Denmark*
[4]*National Institute of Information and Communications Technology, Tokyo, Japan*

According to the basic postulates of quantum mechanics, perfect discrimination of nonorthogonal quantum states is impossible [1]. On the one hand this result allows for new applications such as quantum key distribution [2] but on the other hand it also imposes ultimate limits to the channel capacity in communication protocols [3]. In both cases, the development of optimal or near-optimal detection schemes for a given set of states is of outstanding importance. Not only is the channel capacity increased if the error rate of the detection system is lowered, but it has also been shown that the feasible secret key rate of a quantum key distribution system can be largely increased by optimizing the receiver scheme [4]. While a lot of attention has already been devoted to the development of optimized receivers for the elementary binary alphabet, four-state protocols have hardly been considered.

We present a discrimination scheme for the quadrature phase-shift keyed (QPSK) alphabet, which comprises four states with equal amplitude but with a phase shift of $\pi/2$.

$$\alpha_i = |\alpha| \cdot e^{i\,(n-\frac{1}{2})\frac{\pi}{2}} \qquad (1)$$

This encoding technique is nowadays widely used in applications such as wireless networks for mobile phones or backbone fiber networks, but has also been considered for applications in QKD [2, 5].

We prove in theory and provide experimental evidence, that our approach outperforms the error probability of the standard scheme - heterodyne detection - for any signal power. We show that our receiver provides the hitherto smallest error probability in the domain of highly attenuated signals. The discrimination is composed of a quadrature measurement, a conditional displacement and a threshold detector.

The strategy is to split the state and to perform two successive measurements on the individual parts. The first measurement is a quadrature projection via a homodyne detector (HD) and allows to reduce the set of possible states from four to two. The outcome is subsequently forwarded to a displacement stage, that optimally tunes the remaining pair of states for the discrimination via a photon counting detector. In this way, both the wave nature (homodyne) and the particle nature (photon counting) of the quantum states are considered.

We implemented this hybrid receiver with two different photon counting stages: the Kennedy [6] and the optimized displacement receiver [7]. In both receivers, the remaining part of the quantum state is first subject to a displacement that shifts one of the states to or close to the vacuum. Subsequently, the states are detected and identified by observing whether or not a click event was recognized by the detector. The experimental results for the error probability relative to the heterodyne detector are presented in Fig.1. While the HD-Kennedy receiver can not outperform the standard scheme
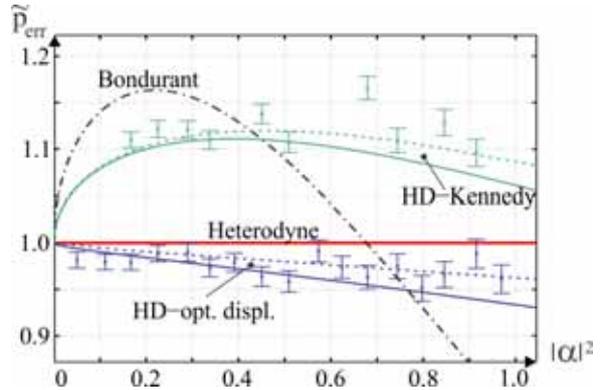
Figure 1: Error probabilities for different receiver schemes relative to a heterodyne detector. Our hybrid receiver outperforms heterodyne detection for any amplitude and provides the smallest error probabilities in the domain of highly attenuated signals. Solid lines correspond to the theoretical prediction and the dashed curves account for the detrimental effects of dark counts.

in the measured range of amplitudes, the HD-optimized displacement receiver is superior for any input amplitude. Additionally, we show the error probabilities of the Bondurant receiver [8], which provides the hitherto smallest error rates in the regime of conventional signal powers. The comparison shows, that our hybrid receiver is superior for signals with mean photon number $|\alpha|^2 < 0.75$.

References

[1] C. W. Helstrom, Inform. Control **10** (1967)

[2] S. Lorenz, N. Korolkova and G. Leuchs, Appl. Phys. B **79** (3), 273-277 (2004)

[3] V. Giovannetti et al., Phys. Rev. Lett. 92, 027902 (2004)

[4] C. Wittmann et al., Phys. Rev. Lett. **104**, 100505 (2010)

[5] D. Sych and G. Leuchs, New. J. Phys. **12**, 053019 (2010)

[6] R. S. Kennedy, Research Laboratory of Electronics, MIT, Quarterly Progress Report No. **108**, p. 219 (1973)

[7] C. Wittmann et al., Phys. Rev. Lett.**101**, 210501 (2008)

[8] R. S. Bondurant, Opt. Lett. **18**, 22, 1896-1898 (1993)

Fundamental limits on the accuracy of optical phase estimation from rate-distortion theory

Ranjith Nair

Department of Electrical and Computer Engineering, National University of Singapore, 4 Engineering Drive 3, Singapore 117583

The "Heisenberg limit" (H limit) [1] for optical phase estimation provides an asymptotic lower bound on the mean-squared error (MSE) $\delta\Phi^2 \sim 1/N^2$ of any lossless estimation scheme, where N is the mean number of photons in the probe state. Following the recent intriguing claims, based on the quantum Cramér-Rao bound, that the H limit may be beaten in optical interferometry [2], several authors have shown this is not the case by giving rigorous proofs of non-asymptotic lower bounds with H limit behavior [3]. Interestingly, these proofs use diverse techniques such as the speed limit on quantum evolutions, the entropic uncertainty relations, and the quantum Ziv-Zakai bound. In this work, we first give a very simple proof of a lower bound for optical phase estimation using classical rate-distortion theory that is valid for all values of N and any prior probability density for the phase. Further, we illustrate the generality of the approach by showing that, when any nonzero loss is present, an uncoded system cannot achieve better than shot-noise scaling [1].

Rate-distortion theory is the theoretical basis for lossy data compression and was introduced by Shannon in his famous 1948 paper and elaborated in [4]. In this approach, the unknown phase random variable Φ, with probability density $P_\Phi(\phi)$, is considered as a data source and the MSE between Φ and our estimate $\hat{\Phi}$ is considered as a distortion measure $d(\Phi, \hat{\Phi}) := E[(\Phi - \hat{\Phi})^2]$. For a given source and distortion measure, we can compute the *rate-distortion function* $R(D)$ given by a minimization over conditional densities $P_{\hat{\Phi}|\Phi}(\hat{\phi}|\phi)$:-

$$R(D) = \min_{P_{\hat{\Phi}|\Phi}(\hat{\phi}|\phi):d(\Phi,\hat{\Phi})\leq D} I(\Phi;\hat{\Phi}), \qquad (1)$$

where $I(\Phi; \hat{\Phi})$ is the mutual information. The Information Transmission Inequality (Theorem 1 of [4]) in the form corresponding to an uncoded system reads:- Given a source Φ
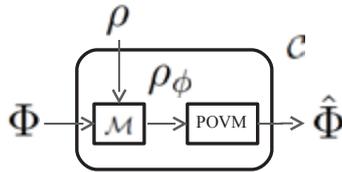
Figure 1: Quantum-mechanical realization of the system to which the Information Transmission Inequality applies.

with prior distribution $P_\Phi(\phi)$, a distortion measure $d(\Phi, \hat{\Phi})$ and the rate-distortion function $R(D)$ (in nats/symbol) of the source. Suppose Φ is transmitted over a channel $\mathcal{C}$ with capacity C nats/use. Let the channel output be $\hat{\Phi}$. We then have

$$d(\Phi, \hat{\Phi}) \geq D(C), \qquad (2)$$

where $D(\cdot)$ is the function inverse to $R(D)$.

The application of this result to quantum metrology, first suggested in [5], is made by considering the classical channel $\mathcal{C}$ as being realized through selection of a probe state ρ, a modulation map $\mathcal{M}$ and a POVM to yield the output estimate (Fig. 1). Using a result of [6] on the form of the optimum probe state, and the known capacity of a single-mode bosonic channel [7], we obtain from (2) a H limit for lossless phase estimation

$$\delta\Phi^2 \geq Q_\Phi / \left[e(N+1) \right]^2, \qquad (3)$$

where Q_Φ is the entropy power of the prior distribution P_Φ.

When any finite amount of loss $1 - \eta > 0$ is present in the probe mode, (3) is no longer tight. Again using the optimal form of the probe state from [6] and a result of [8] on the minimum entropy gain of a loss channel, we overbound the achievable capacity C under phase modulation to obtain the lower bound

$$\delta\Phi^2 \geq \frac{Q_\Phi(1-\eta)^2}{2\pi e\left[\eta(1-\eta)N + 1/12\right]}, \qquad (4)$$

which shows shot-noise scaling similar to a coherent-state probe. Details of the derivations may be found in [9].

References

[1] B. Yurke, S. L. McCall, J. R. Klauder, Phys. Rev. A **33**, 4033 (1986); B. C. Sanders, G. J. Milburn, Phys. Rev. Lett. **75**, 2944 (1995); Z. Y. Ou, Phys. Rev. Lett. **77**, 2352 (1996).

[2] P. M. Anisimov, et al., Phys. Rev. Lett. **104**, 103602 (2010); A. Rivas, A. Luis, arXiv:1105.6310v2 (2011); Y. R. Zhang, et al., arXiv:1105.2990v2 (2011).

[3] V. Giovannetti, S. Lloyd, L. Maccone, arXiv:1109.5661 (2011); M. J. W. Hall *et al.*, arXiv:1111.0788v2 (2012); M. Tsang, arXiv:1111.3568v3 (2011); V. Giovannetti, L. Maccone, arXiv:1201.1878 (2012); M. J. W. Hall, H. M. Wiseman, arXiv:1201.4542v1 (2012).

[4] C. E. Shannon, IRE Intntl. Conv. Rec., **7**, 325 (1959).

[5] H. P. Yuen, in Chap. 7 of *Quantum Squeezing*, Eds. P. D. Drummond and Z. Ficek, Springer Verlag (2004).

[6] R. Nair, B. J. Yen, Phys. Rev. Lett. **107**, 193602 (2011).

[7] H. P. Yuen, M. Ozawa, Phys. Rev. Lett. **70**, 363 (1993).

[8] A. S. Holevo, Dokl. Math. **82** 730 (2010); arXiv:1003.5765v1 (2010).

[9] R. Nair, arXiv.org: to appear in early April 2012.

A generalized Dolinar receiver with inconclusive results

Kenji Nakahira[1], **Tsuyoshi Sasaki Usuda**[2]

[1] *Yokohama Research Laboratory, Hitachi, Ltd., Japan*
[2] *School of Information Science and Technology, Aichi Prefectural University, Japan*

Quantum optical coherent state discrimination is a critical problem in quantum optics and quantum information theory. In particular, in optical communications it is necessary to discriminate as accurately as possible between binary pure coherent states, which can be generated by an ideal laser. Dolinar showed that the optimal receiver for these states without inconclusive results can be implemented using only a beam splitter, a local coherent light source, a photon detector, and a feedback circuit [1]. We propose an extension of the Dolinar receiver that realizes optimal performance for any fixed probability of an inconclusive result.

Several studies have sought to find a measurement that maximizes the probability of correct detection. Recently, a more generalized measurement that maximizes the probability of correct detection for a fixed probability of an inconclusive result, which we refer to as the optimal inconclusive measurement, has been considered [2]. The optimal inconclusive measurement has been derived for binary pure states with any prior probabilities (e.g., [3]).

Unfortunately, the analytical expression for optimal measurements does not yield receiver implementations that attain the optimal performance. Thus, it is a nontrivial problem to determine how to implement such an optimal receiver in practice. In 1973, Dolinar proposed an optimal receiver without inconclusive results for binary coherent states [1]. Recently, an experimental realization of the Dolinar receiver has been demonstrated [4]. However, to the best of our knowledge, an optical implementation of a theoretically optimal inconclusive receiver for an arbitrary probability of an inconclusive result has not been found.

Here, we propose an optimal inconclusive receiver for binary coherent states with any prior probabilities and for any probability of an inconclusive result using only a beam splitter, a local coherent light source, a photon detector, and a feedback circuit. Although the optimal inconclusive measurement can be expressed by three measurement operators in a two-dimensional Hilbert space and thus is not a von Neumann measurement, this receiver can be implemented using the same optical components as the Dolinar receiver.

Consider two pure optical coherent states $\{|\alpha_0\rangle = |\alpha\rangle, |\alpha_1\rangle = |-\alpha\rangle\}$ occurring with the prior probabilities ξ_0 and $1-\xi_0$. For notational simplicity, we normalize the pulse duration of the input signal to be $T = 1$. We assume that the measurement starts at time $t = 0$. The output of the photodetector, which has the same components as the Dolinar receiver, is a conditionally Poisson counting process with a rate $\lambda(t) = |\pm\alpha - u(t)|^2$, where $u(t)$ is the displacement quantity controlled by the local coherent light source. The displacement quantity of the Dolinar receiver is represented by $u(t) = (-1)^{N(t)}u_0(t)$, where

$$u_0(t) = \frac{\alpha}{\sqrt{1 - 4C^2}}. \qquad (1)$$

Here, $C = \sqrt{\xi_0(1 - \xi_0)}\exp(-2|\alpha|^2)$, and $N(\tau)$ is the number of photons detected over the time interval $0 \le t \le \tau$.

An inconclusive measurement discriminates the following three possibilities: $|\alpha_0\rangle$, $|\alpha_1\rangle$, and inconclusive result. Our proposed receiver switches between the following two modes: discriminating between the two states $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ and determining whether the measurement result is inconclusive. Our receiver applies the displacements of Eq. (1) during the time interval $0 \le t \le t_1$, where

$$t_1 = \frac{1}{4|\alpha|^2}\ln\left(\frac{2\xi_0(1 - \xi_0)}{2C^2 - 2P_1C + P_1}\right) \qquad (2)$$

and P_1 is the probability of an inconclusive result. Let $j = 0$ when $N(t_1)$ is even and $j = 1$ when $N(t_1)$ is odd. During the time interval $t_1 < t \le 1$, the discrimination between $|\alpha_j\rangle$ and an inconclusive result is performed. This discrimination task is accomplished by the Dolinar receiver for the states $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ with prior probabilities v and $1-v$, respectively. v is a certain value obtained from ξ_0, α, and P_1.

Figure 1 shows two examples of optimal displacement amplitudes $u_0(t)$ with $\alpha = \sqrt{0.2}$, and with $(\xi_0, P_1) = (0.5, 0.2)$ and $(0.7, 0.2)$, respectively. From Eq. (2), t_1 becomes 0.678 and 0.572, respectively. When the optical devices have ideal properties (for example, an ideal coherent-state local field, a photon detector with a quantum efficiency of unity and no dark current, and an ultra-fast feedback circuit), our receiver achieves optimal performance.
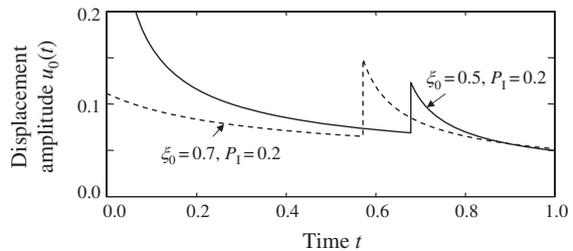
Figure 1: Examples of optimal displacement amplitudes.

References

[1] S. J. Dolinar, MIT Res. Lab. Electron. Quart. Prog. Rep. **111**, 115 (1973).

[2] A. Chefles and S. M. Barnett, J. Mod. Opt. **45**, 1295 (1998).

[3] H. Sugimoto, T. Hashimoto, M. Horibe, and A. Hayashi, Phys. Rev. A **80**, 052322 (2009).

[4] R. L. Cook, P. J. Martin, and J. M. Geremia, Nature **446**, 774 (2007).

Measuring Nothing

Daniel K. L. Oi[1], **Václav Potoček**[2] **and John Jeffers**[1]

[1] *SUPA Department of Physics, University of Strathclyde, Glasgow G4 0NG, United Kingdom*
[2] *Czech Technical University in Prague, Faculty of Nuclear Sciences and Physical Engineering, Department of Physics, Břehová 7, 115 19 Praha 1, Czech Republic*

Measurement is crucial for transforming information embodied in a quantum system into classical signals. In sequential protocols [1], non-destructive (or indirect) means of measuring a state are required [2]. The projection onto the vacuum or its complementary subspace is a novel measurement utilised in sequential decoding by quantum communication protocols saturating the Holevo bound with coherent signal states [3, 4]. Detecting the vacuum is trivial, conventional photodetection measures the vacuum as an absence of counts, but the converse result (not vacuum) leads to the destruction of the state making it unsuitable for such sequential measurement procedures.

Here, we show how to implement the ideal "vacuum or not" projection preserving the post-measurement non-vacuum state with no leakage of information about photon number (Fig.1). The measurement utilises adiabatic conditional evolution of a three level probe coupled to a cavity system, similar to vacuum stimulated Ramann adiabatic passage (V-STIRAP) [5], but extended to arbitrary field states. Adiabatic evolution eliminates photon number dependent dynamics which would leak information from the non-vacuum subspace and change the relative amplitudes of the photon number basis states or else destroy their coherence as in non-destructive photon counting [6]. We discuss how the measurement may be achieved experimentally in cavity QED (Fig. 2) or circuit QED systems including the effect of non-idealities, i.e. photon loss and non-adiabaticity.

Additionally, the protocol can be adapted to create unusual quantum states of light through the application of the bare raising and lowering operators [7]. These have not previously been implemented in quantum optical experiments and may open up new avenues for manipulating continuous variable systems. It is also possible to generalise the measurement to project onto the joint vacuum state of multiple modes or the complementary subspace which may have application in quantum communication and computation.

References

[1] E. Andersson, D. K. L. Oi, PRA **77**, 052104 (2008)

[2] P. Grangier et al., Nature **396**, 537 (1998)

[3] P. Sen, arXiv:1109.0802v1

[4] S. Guha, S.-H. Tan, M. M. Wilde, arXiv:1202.0518v1

[5] A. Kuhn et al., Appl. Phys. B **69**, 373 (1999)

[6] C. Guerlin *et al.*, Nature **448**, 889 (2007)

[7] L. Susskind and J. Glogower, Physics **1**, 49 (1964).
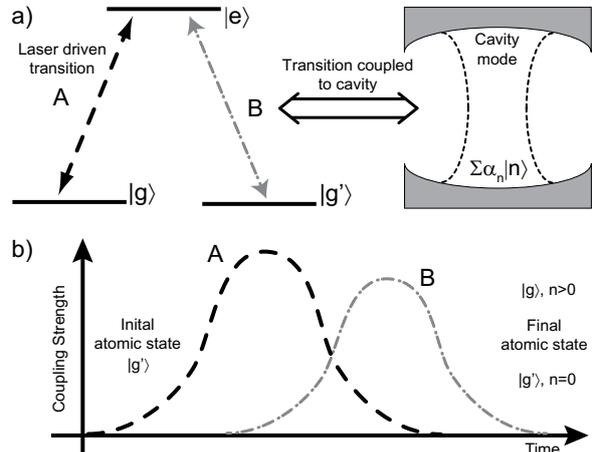
Figure 1: a: Lambda atomic system coupled to cavity. A probe three level atom with two ground states ($|g\rangle$, $|g'\rangle$) and a single excited level ($|e\rangle$) is coupled to the field to be measured. b: Counter-intuitive coupling sequence. For $n \geq 1$ photons in the field, the atom-cavity adiabatically follows the dark-state manifold $\sin\theta|g, n-1\rangle + \cos\theta|g', n\rangle$, $\theta = 0 \to \pi/2$ leaving the final state of the system as $|g, n-1\rangle$. After measuring the atom in $|g\rangle$, we replace the photon by reversing the coupling sequence. If the cavity was originally vacuum ($n = 0$), the final state of the atom remains as $|g'\rangle$.
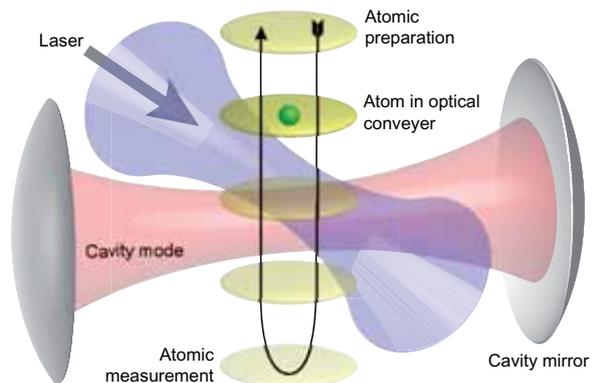
Figure 2: Proposed realisation. An optical lattice traps and controls the position, hence coupling, of the atom with the driving laser and cavity mode. The atom, initially in $|g'\rangle$, adiabatically interacts with laser and mode and is then measured in $|g'\rangle$ (vacuum) or $|g\rangle$ (not vaccum). To perform the ideal $(\mathbb{I} - |0\rangle\langle 0|)$ operation in latter case, the motion of the atom is reversed to replace the photon extracted from the cavity.

Photon-number statistics of twin beams: self-consistent measurement, reconstruction, and properties

__Jan Peřina Jr.__[1], __Ondřej Haderka__[1], __Václav Michálek__[2] __and Martin Hamar__[2]

[1]*RCPTM, Joint Laboratory of Optics of Palacký University and Institute of Physics of Academy of Science of the Czech Republic, Faculty of Science, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic.*
[2]*Institute of Physics of Academy of Sciences of the Czech Republic, Joint Laboratory of Optics of Palacký University and Institute of Physics of AS CR, 17.listopadu 12, 772 07 Olomouc, Czech Republic.*

A method for the determination of photon-number statistics of twin beams using the joint signal-idler photocount statistics measured by an iCCD camera is suggested [1, 2]. Also absolute quantum detection efficiency of the camera is obtained. In the method, the measured histograms of joint signal-idler photocount statistics are fitted by a general six-parameter function arising from a paired variant of quantum superposition of signal and noise [3]. Values of these parameters together with the inquired quantum detection efficiencies in the signal- and idler-field paths are given combining the five first- and second-order experimental photocount moments and the requirement of least-square declinations from the experimental histogram. The obtained joint signal-idler photon-number distributions reveal a paired character of twin beams that is responsible for the violation of classical inequalities as well as a teeth-like character of the distribution of the sum of signal and idler photon numbers. Using quasi-distributions of integrated intensities, the transition from fully quantum to classical description of twin beams is studied. From the metrology perspective, the method overcomes the usual approaches of absolute detector calibration [4] in precision due to the identification and elimination of noisy parts of twin beams.

References

[1] O. Haderka, J. Peřina Jr., M. Hamar, and J. Peřina, Phys. Rev. A, __71__, 033815 (2005).

[2] J. Peřina, J. Křepelka, J. Peřina Jr., M. Bondani, A. Allevi, and A. Andreoni, Phys. Rev. A, __76__, 043806 (2007).

[3] J. Peřina and J. Křepelka, J. Opt. B: Quant. Semiclass. Opt., __7__, 246 (2005).

[4] G. Brida, I. P. Degiovanni, M. Genovese, M. L. Rastello, and I. R. Berchera, Opt. Express, __18__, 20572 (2010).

How to make optimal use of maximal multipartite entanglement in clock synchronization

Changliang Ren[1,2], Holger F. Hofmann[1,2]

[1]Graduate School of Advanced Sciences of Matter, Hiroshima University, Kagamiyama 1-3-1, Higashi Hiroshima 739-8530, Japan
[2]JST, CREST, Sanbancho 5, Chiyoda-ku, Tokyo 102-0075, Japan

Entanglement is very useful for clock synchronization, since entangled states can achieve the maximal sensitivity to time differences between local parties when the parties perform time dependent measurements. The two-party quantum clock synchronization protocol initially proposed by Jozsa et al. [1] shows how bipartite entangled states can be used for efficient clock synchronization between two parties. This idea has been extended to multiparty clock synchronization protocols by using W-states or symmetric Dicke states to simultaneously establish bipartite entanglement between all the parties [2, 3]. However, for such states, the amount of bipartite entanglement available for the clock synchronization protocol decreases rapidly as the number of clocks increases. The reason is that multipartite entanglement decreases the bipartite entanglement available to any two parties. To achieve optimal efficiency in multiparty protocols, it would therefore be desirable to directly use the characteristic multiparty correlations of genuine multipartite entanglement in clock synchronization.

In this presentation, we show how the maximal multipartite entanglement of GHZ-type states can be used for multiparty clock synchronization [4]. Two problems need to be solved to achieve this. Firstly, it is necessary to define GHZ-type states that are energy eigenstates, to avoid any dependence on state distribution times. Secondly, it is necessary to extract information on individual clock times from the collective information on multiparty measurement correlations.

The first problem can be solved by converting a standard GHZ-state in the energy eigenbasis into an energy eigenstate by flipping exactly one half of the local energies by appropriate local unitaries. If the qubits are arranged so that the first half of the qubits is unflipped and the second half of the qubits is flipped, this N-partite entangled energy eigenstate can be written as

$$| \Psi_N \rangle = \frac{1}{\sqrt{2}} \left(| 0 \rangle^{\otimes \frac{N}{2}} | 1 \rangle^{\otimes \frac{N}{2}} + | 1 \rangle^{\otimes \frac{N}{2}} | 0 \rangle^{\otimes \frac{N}{2}} \right). \quad (1)$$

This initial state unavoidably divides the qubits into two groups. Since this division into groups lifts the symmetry between the parties, it can actually be used to solve the second problem. In each distribution, every party will receive a flipped or an unflipped qubit, making it a member of the flipped or the unflipped group. By using different group assignments, it becomes possible to extract the necessary information about local clock times. If no two parties are always members of the same group, each local clock can be properly synchronized. Hence, the most simple solution is to assign each qubit of the initial state to the clock owners randomly, so that each party sometimes receives a qubit from the unflipped group, and sometimes receives a qubit from the flipped group. To describe each distribution, we can define a sequence $\{f_i\}$,

where $i = 1, ..., N$. If the qubit of the $i-th$ clock owner is a flipped qubit, $f_i = 1$, if not, $f_i = 0$. To keep track of the different distributions, we assign an index j to each, so that the elements of each sequence are given by $f_i(j)$.

After the distribution of the qubits to the locations of the different clocks, each of the parties measures a time dependent observable $\hat{X}(t)$ on its qubit when their local clock points to a specific time. If the actual measurement times of the parties are given by $\{t_1, t_2, ..., t_N\}$, the expectation value of this product is

$$\langle \hat{X}^{\otimes N} \rangle = \cos \left(\sum_i^N (-1)^{f_i} \omega t_i \right). \quad (2)$$

The total time difference that defines the phase shift in the multipartite interference fringe observed in the $\hat{X}^{\otimes N}$ measurement of the distribution with index j is then

$$T_j = \sum_{i=1}^N (-1)^{f_i(j)} t_i. \quad (3)$$

After sharing the results of a sufficiently large number of measurements for the different distributions $\{f_i(j)\}$, all parties can obtain the same estimates for the time differences T_j. Each clock owner can then estimate and adjust the time difference between his or her respective local clock and the average time of all the clocks by considering the linear dependence of all T_j on the local clock times t_i.

For comparison with the previous multiparty protocols, the efficiency of this protocol can be evaluated in terms of the statistical errors in the estimation of time differences. We find that the present protocol has the highest efficiency in terms of the accuracy achieved with a given number of qubits, performing about twice as well as the parallel distribution of entangled pairs, and four times as well as the symmetric Dicke states. This analysis confirms that the genuine multipartite entanglement of GHZ-type states can indeed be used to improve the efficiency of clock synchronization beyond that achieved by protocols that only use the bipartite entanglement available between two parties each. Thus, multipartite entanglement is a resource that requires cooperation between all the parties to realize its full potential.

References

[1] R. Josza et al., Phys. Rev. Lett. 85 2010 (2000).

[2] M. Krco and P. Paul, Phys. Rev. A 66 024305 (2002).

[3] R. Ben-Av and I. Exman, Phys. Rev. A 84, 014301 (2011).

[4] C. L. Ren and H. F. Hofmann, arXiv: 1203.4300 .

Local non-realistic states observed via weak tomography - resolving the two-slit paradox

Dylan J. Saunders[1], Pete J. Shadbolt[2], Jeremy L. O'Brien[2] and Geoff J. Pryde[1]

[1]Centre for Quantum Computation and Communication Technology (Australian Research Council), Centre for Quantum Dynamics, Griffith University, Brisbane, Queensland 4111, Australia
[2]Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK

A Mach-Zehnder (MZ) interferometer, like a double slit experiment, has at its heart many of the mysterious properties of quantum theory [1]. Recently, 100 years after the original double slit experiment, there have been exciting experimental [2] and theoretical [3] results implementing weak measurement, offering new insight into quantum theory. The theory result, by Hofman, introduced a framework for weak tomography which can be used to describe transient states, that is, the state between initial preparation and final measurement. This formalism provides a surprising answer to the question - "what is the state of a photon (or particle) while in transit through a double slit apparatus?".

We present an experiment using weak tomography where we have measured single qubit transient states passing through a two-path MZ interferometer analogous to a double slit. We observe states that reveal the quantum system travels through a single slit (a particle property) while maintaining coherence (a wave property) with "not going through the other slit". Despite these states being non-realistic they are measurable within the framework of weak tomography by implementing sufficiently weak measurements [3].

The transient quantum state, $\hat{R}_{if}$, observed by weak tomography exists between a pre-selection, i, and post selection, f. Any input state $|\psi_i\rangle$ can be written as $|\psi_i\rangle = \sum_i p(f)\hat{R}_{if}$, where $p(f)$ is the probability of obtaining post selection f. All the properties of $|\psi_i\rangle$, between i and f, are described by a statistical mixture of non-realistic transient states, where the result of the final measurement f acts like a classical Bayesian updating. This leads to a consistent non-realistic interpretation of quantum theory [3].

Following Hofman [3], we derive a procedure to reconstruct transient states by generalising strong measurement tomography to include weak measurements, in particular, weak POVM measurements. Using an informationally complete set of weak POVMs, $\{_i\hat{\Pi}_f\}$, we can infer a single transient state that is consistent with the observed weak values. One important assumption in this theory is that the measurement strength, ϵ, satisfy $\epsilon \ll 1$, otherwise measurement back-action will perturb the state after the weak measurement and give inaccurate weak tomography reconstructions. We investigated the effect of back-action using a numerical simulation for single qubit states. We found, that unlike normal strong measurement tomography, the size of the back-action strongly depends on the chosen basis set $\{_i\hat{\Pi}_f\}$. To resolve the effect of measurement strength on the fidelity of the reconstructed transient states, we implemented a large Monte-Carlo simulation over randomly chosen mutually un-biased weak POVM sets, effectively averaging over any basis biasing. We found an experimentally accessible region (in white)

where meaningful transient states can be reconstructed.

Our weak measurement device is a linear optics CNOT gate that implements a variable strength measurement on one arm (slit) of a MZ interferometer. The circuit is realised in a reconfigurable wave guide photonic circuit with eight voltage controlled phase shifters [4]. The photonic circuit is a path encoded MZ controlled-NOT gate, where the double slit is the MZ interferometer used for the control bit. We implement the weak measurement using the entangling properties of the gate, where the which-way information is entangled with the meter qubit [5]. By varying the strength of this entangling operation, and by strongly measuring the meter qubit, we can implement varying strength POVMs in the $\hat{\sigma}_Z$ on the control qubit. Rotating the state of the control qubit before and after the CNOT generalises the device to be able to perform any arbitrary weak POVM. Using the corresponding weak values, we reconstruct the transient states of the control qubit during propagation through the MZ interferometer. For an example of a pair of experimentally observed transient states see Figure 1a. The observed transient states are non-realistic (negative eigenvalues) because they strongly address the "which slit" question, which would normally collapse the superposition, however, by weakly measuring the state at the slit beforehand, we still observe all wave properties simultaneously.
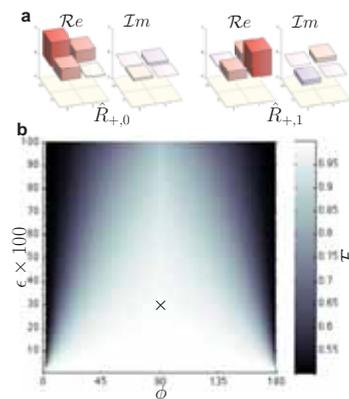
Figure 1: a. Experimentally reconstructed single qubit transient states with negative eigenvalues for input state $|+\rangle$, post selected on the logical 0 and 1 states, with $\epsilon \approx .3$ - position $\times$ in figure (b). **b.** Simulation showing the effect of back-action. ϵ is varied from 0 to 1 for a range of input states parametrized by ϕ (azimuthal angle between the input state and post selection basis), for a fixed post selection basis $\hat{\sigma}_Z$.

References
[1] R. Feynman, The Feynman Lectures on Physics (1989)
[2] S. Kocsis, et. al. Science, **332** 1170-1173 (2011)
[3] H. Hofman, Phys. Rev. A **81**, 012103 (2010)
[4] P. J. Shadbolt, et. al. Nature Phot. **6**, 45-49 (2012).
[5] G. J. Pryde et. al., Phys. Rev. Lett. **94** 220405 (2005)

Matter wave Mach-Zehnder interferometry on an atom chip

Jean-François Schaff, Tarik Berrada, Sandrine van Frank, Robert Bücker, Thorsten Schumm, and Jörg Schmiedmayer

Vienna Center for Quantum Science and Technology, Atominstitut, TU Wien, 1020 Vienna, Austria

We have implemented an atomic Mach-Zehnder interferometer in a fully trapped configuration on an atom chip.

We start with a Bose-Einstein condensate (BEC) of ^{87}Rb atoms in a magnetic trap, which is first coherently split by turning the initial trap into a double-well potential by means of radio-frequency dressing [1]. This constitutes the first beam splitter of the interferometer, the two clouds being completely decoupled after splitting.

We imprint a relative phase between the two condensates by tilting the double well. The phase thus evolves as $\phi = Et_\phi/\hbar$, where t_ϕ is the phase accumulation time, and E the energy difference between the ground state of each well.

In a third step, the spacing between the wells is abruptly reduced in order to accelerate the two clouds towards the potential barrier. Both condensates are partially reflected on the tunnel barrier and partially transmitted. The reflected component arising from one cloud overlaps with the transmitted part coming from the other cloud. Depending on the initial relative phase between the two BECs, the interference can either be constructive or destructive. In the absence of interactions, one can show that the population imbalance z, defined as the difference of atom numbers between the two wells over the sum, is given by

$$z = C(t_{\mathrm{BS}})\sin(\phi), \tag{1}$$

where ϕ is the initial relative phase, and $-1 \leq C(t_{\mathrm{BS}}) \leq 1$ is a non trivial function of the time t_{BS} spent in the coupled double well. This contrast also depends on the initial wave functions and precise shape of the double-well potential.

As a whole, this sequence thus converts a relative phase between two condensates containing the same number of atoms into a population imbalance, and can thus be used as the output beam splitter of our interferometer. It was optimized by adjusting both the barrier height of the coupled trap and the duration t_{BS} in order to maximize the contrast C after having prepared an initial relative phase of $\pi/2$. This yields a contrast of 40%, as can be seen on Figure 1. The population imbalance is finally measured by raising the tunnel barrier in order to clearly separate the two wells, and imaging the two clouds after time of flight (cf. insets of Figure 1).

The fringes observed when the phase accumulation time t_ϕ is varied are presented in Figure 1.

The particles are trapped during the whole sequence, which allows long interrogation times. Since the interferometry is performed on the external degrees of freedom, such an interferometer can be used as a gravimeter or gyrometer. Phase estimation is also known to be easier with atom counting [2] than with the usual continuous variable measurement performed on atom chips [3] (readout of the interference pattern after time of flight). While we control the relative population at the atomic shot noise level, and even observe number squeezing during the splitting stage, the relative phase is broadened by technical fluctuations, with a variance typically 25 times larger than that expected from the Heisenberg limit, subsequently reducing the contrast of the interferometric signal.

By using a new scheme involving two such beam splitters, and improving number squeezing during the first splitting stage, for instance by using optimal control of the double well [4], one could in principle reach the Heisenberg scaling of the phase sensitivity [5] in this trapped configuration [2, 6].
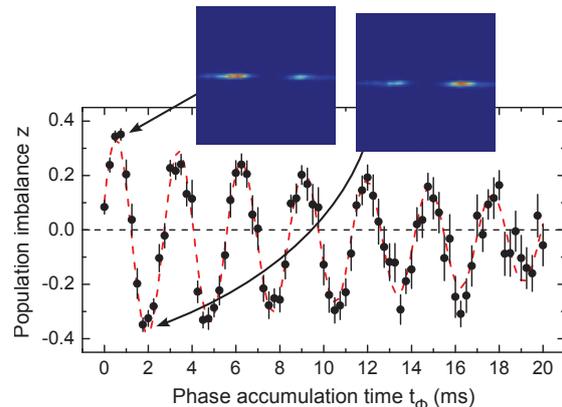
Figure 1: Interferometric signal at the output of the matter wave Mach-Zehnder interferometer. The population imbalance (see text) oscillates at 350 Hz, which corresponds to a difference of altitude of 160 nm induced by a tilt of the double well potential by a few degrees during the phase accumulation time. The contrast approaches 40% which is due to the limited mode matching of the two wave packets on the output beam splitter. Its decay is still under investigation and may be a consequence of phase diffusion occuring during the phase accumulation time. The points are the mean values of 20 shots, the error bars represent ± the standard error of the mean, and the dashed red line is an exponentially damped sine fit to the data.

References

[1] I. Lesanovsky *et al.*, PRA **73**, 033619 (2006); S. Hofferberth *et al.*, PRA **76**, 013401 (2007).

[2] J. Chwedenczuk *et al.*, PRA **82**, 051601(R) (2010); J. Chwedenczuk *et al.*, New Journal of Physics **13**, 065023 (2011).

[3] T. Schumm *et al.*, Nature Physics **1**, 57 (2005).

[4] J. Grond *et al.*, PRA **79**, 021603(R) (2009).

[5] V. Giovannetti *et al.*, Science **306**, 1330 (2004).

[6] J. Grond *et al.*, PRA **84**, 023619 (2011).

Enhancing Quantum Effects via Periodic Modulations in Optomechanical Systems

Alessandro Farace[1] **and Vittorio Giovannetti**[1]

[1]*NEST-CNR-INFM & Scuola Normale Superiore, Piazza dei Cavalieri 7, I-56126 Pisa, Italy*

One of the main goals in today quantum science is controlling nano- and micromechanical oscillators at the quantum level. Quantum optomechanics [1, 2, 3], i.e. studying and engineering the radiation pressure interaction of light with mechanical systems, comes as a powerful and well-developed tool to do so: first, radiation pressure interaction can cool a (nano)micromechanical oscillator to the ground-state [4, 5, 6], counteracting thermalization and decoherence; second, many optomechanical effects find an interpretation in terms of non-linear quantum optics, so that quantum control protocols are already at hand and need only an appropriate translation.

In the last two decades many interesting applications have been proposed [7], ranging from the generation of entanglement (key resource in quantum information processing) between one moving mirror and the radiation in a Fabry-Perot (FP) cavity [8] to the generation of position-squeezed mechanical states [9] (helpful in increasing the precision of interferometry and detection experiments). Experimental realizations are still pursued, mainly because the attainable levels of light-matter interaction are not sufficiently high to enter the so called strong coupling regime, with first steps forward being moved only most recently [10]. Therefore, without waiting for technological advances, we would like to find a way of enhancing the visibility of the desired quantum properties.

A possible solution was first proposed in Ref. [9, 11], which relies on applying a periodic modulation to some of the system parameters: this induces a modulation on the system response and in turn, quantum effects are found to be periodically stronger with respect to the unmodulated case. Bringing on this idea, we ask ourselves whether there is an optimal modulation, for which this increase its maximal, and whether there is a substantial difference in modulating only one or more parameters at the same time.

To tackle these issues we consider the case of a FP cavity with a movable mirror, which evolves under the action of thermal noise and of the radiation pressure exerted by the photons of an externally driven optical mode. We first apply a modulation on the mirror oscillation frequency of the form $\omega_M(t) = \omega_M^0(1 + \epsilon cos(\Omega_1 t))$, to study the single modulation picture, and we then add a second modulation on the input laser power $P(t) = P^0(1 + \eta cos(\Omega_2 t + \phi))$ (as originally done in [9]), to study the interplay between the two. Fixing all parameters to state-of-the art values, we simulate the system dynamics and characterize the quantum properties in the asymptotic stationary regime [12].

When only one modulation is activated, we find that setting the corresponding frequency $\Omega_1, \Omega_2 \sim 2\omega_M^0$ gives the best performance. Moreover, quantum effects increase monotonically with respect to the associated modulation strengths ϵ and η, up to a threshold value where the system becomes unstable. We can explain this behavior as a resonance between the modulation frequency and the natural frequency of evolution of the system correlations, which for our case is actually $2\omega_M^0$; when the modulation is too strong, the energy absorbed by the system is not compensated by dissipation and the evolution has no asymptotic steady-state.

When both modulations are applied at the same time we notice the arising of interference patterns between the two. In particular setting the frequencies at the optimal values which yield the best performances in the single modulation scenario, (i.e. $\Omega_1 = \Omega_2 = 2\omega_M^0$) we notice that the quantum properties of the system are strongly affected by the relative phase ϕ of the two modulations. Specifically, while the entanglement between the mirror and the cavity mode is affected very little, we find rather drastic changes if we look at the mirror squeezing or at its energy, with evident constructive/destructive interference effects showing up.

References

[1] G. J. Milburn and M. J. Woolley, Acta. Phys. Slov. **61**, 5 (2012).

[2] F. Marquardt and S. M. Girvin, Physics **2**, 40 (2009).

[3] M. Aspelmeyer, S. Gröblacher, K. Hammerer and N. Kiesel, J. Opt. Soc. Am. B **27**, A189 (2010).

[4] C. Genes *et al*, Phys. Rev. A **77**, 033804 (2008).

[5] S. Gröblacher *et al*, Nat. Phys. **5**, 485-488 (2009).

[6] J. Chan *et al*, Nature **478**, 89 (2011).

[7] C.Genes, A. Mari, D. Vitali and S. Tombesi, Adv. At. Mol. Opt. Phys. **57**, 33 (2009).

[8] D. Vitali *et al*, Phys. Rev. Lett. **98**, 030405 (2007).

[9] A. Mari and J. Eisert, Phys. Rev. Lett. **103**, 213603 (2009).

[10] E. Verhagen *et al*, Nature **482**, 63 (2012).

[11] A. Mari and J. Eisert, Eprint arXiv:1111.2415v1 [quant-ph] (2011).

[12] A. Farace and V. Giovannetti, Eprint arXiv:1204.0406v1 [quant-ph] (2012).

Optimal control of a qubit in a non-Markovian environment

Bin Hwang, and Hsi-Sheng Goan

Department of Physics and Center for Quantum Science and Engineering, National Taiwan University, Taipei, Taiwan

Quantum optimal control theory (QOCT) is a powerful tool that provides a variational framework for calculating the optimal shaped pulse to maximize a desired physical objective (or minimize a physical cost function). Compared to the dynamical-coupling-based method [1] in which a succession of short and strong pulses designed to suppress decoherence is applied to the system, QOCT [2, 3, 4] is a continuous dynamical modulation with many degrees of freedom for selecting arbitrary shapes, durations and strengths for time-dependent control, and thus allows significant reduction of the applied control energy and the corresponding quantum gate error. Reference [2] investigated the optimal control of a qubit coupled to a two-level system that is exposed to a Markovian heat bath. Although this may mimic the reduced non-Markovian dynamics of the qubit, it is by no means a model of a qubit coupled directly to a non-Markovian environment. References [3, 4] investigated optimal quantum gate operations in the presence of a non-Markovian environment. However, to combine QOCT with a non-Markovian master equation involving time-ordered integration of the nonunitary (dissipation) terms for noncommuting system and control operators, and for a nonlocal-in-time memory kernel, the numerical treatment is rather mathematically involved and computationally demanding. All of the QOCT approaches mentioned above [2, 3, 4] for open quantum systems employed gradient-based algorithms for optimization.

A somewhat different QOCT approach from the standard gradient optimization methods is the Krotov iterative method [5]. The Krotov method has several appealing advantages [5] over the gradient methods: (a) monotonic increase of the objective with iteration number, (b) no requirement for a line search, and (c) macrosteps at each iteration. Here, we provide a novel and efficient QOCT approach based on the Krotov method and an extended Liouville space quantum dissipation formulation to deal with the non-Markovian open quantum systems [6]. We apply the developed QOCT method to find the control sequences for high-fidelity Z-gates and identity-gates of a qubit embedded in a non-Markovian bath. Our results illustrate that the control parameter can be engineered to efficiently counteract and suppress the environment effect for non-Markovian open systems with long bath correlation times (long memory effects). Z-gates and identity-gates with errors less than 10^{-5} (smaller than the error threshold for fault-tolerant quantum computation) for a wide range of bath decoherence parameters can be achieved with control over only σ_z term [6]. The control-dissipation correlation, and the memory effect of the bath are crucial in achieving the high-fidelity gates. This is in contrast to the cases in the literature [2, 3, 4], where the non-Markovian systems were mainly studied in a parameter regime very close to Markovian systems, and thus no significant reduction of the quantum gate errors was observed.

Our study yields several computational and conceptual in-novations [6] : (a) Our QOCT approach transforms the time-ordered non-commuting integro-differential master equation into a set of time-local coupled differential equations with the small price of introducing auxiliary density matrices in an extended auxiliary Liouville space. As a result, incorporation of the resultant time-local equations with the Krotov optimization method becomes effective. (b) Our approach of decomposing the bath correlation function directly into multi-exponential form has a great computational advantage over the commonly used spectral density parametrization approach at low bath temperatures [7]. (c) The constructed QOCT, which retains the merits of the Krotov method, is extremely efficient in dealing with the time-nonlocal non-Markovian equation of motion. Compared to the calculations performed on a 40-node SUN Linux cluster via the gradient-based approach to tackle the nonlocal kernel directly [3], the calculations using our approach for a similar problem can be performed on a typical laptop PC with ease, thus opening the way for investigating two-qubit and many-qubit problems in non-Markovian environments. (d) Our study of optimal control reveals the strong dependence of the gate errors on the bath correlation time, and exploits this non-Markovian memory effect for high-fidelity quantum gate implementation and arbitrary state preservation in an open quantum system. The presented QOCT is shown to be a powerful tool, capable of facilitating new implementations of various quantum information tasks against decoherence. The required information is knowledge of the bath or noise spectral density, which is experimentally accessible [8]. By virtue of its generality, our method will find useful applications in many different branches of the sciences. Recent experiments on engineering external environments, simulating open quantum systems and observing non-Markovian dynamics could facilitate the experimental realization of the QOCT in non-Markovian open quantum systems in the near future.

References

[1] J. R. West et al., Phys. Rev. Lett. **105**, 230503 (2010).

[2] P. Rebentrost et al., Phys. Rev. Lett. **102**, 090401 (2009).

[3] M. Wenin and W. Pötz, Phys. Rev. A **78**, 012358 (2008); Phys. Rev. B **78**, 165118 (2008); M. Wenin et al., J. Appl. Phys. **105**, 084504 (2009).

[4] R. Roloff and W. Pötz, Phys. Rev. B **79**, 224516 (2009); M. Wenin and W. Pötz, Phys. Rev. A **74**, 022319 (2006).

[5] R. Eitan et al., Phys. Rev. A, **83**, 053426 (2011).

[6] B. Hwang et al., Phys. Rev. A **85**, 032321 (2012).

[7] C. Meier et al., J. Chem. Phys. **111**, 3365 (1999); U. Kleinekathöfer, *ibid.* **121**, 2505 (2004).

[8] J. Bylander et al., Nat. Phys. **7**, 565 (2011).

Modeling spin entanglement with an optical frequency comb of atoms confined on atom-chip traps

Qudsia Quraishi, Vladimir Malinovsky and Patricia Lee

Army Research Laboratory, Adelphi, MD 20783

Cold atomic gases are a versatile environment to test quantum physics, quantum information and quantum control. Various schemes have been devised to leverage the cold atom physics for quantum information processing [1], including, trapping of cold atomic ensembles on miniature traps for atom interferometry [2]. In order to manipulate the internal state of the atoms, typically a combination of microwave, rf and optical fiields are used. However, an all optical approach has distinct advantages for coherent control which involves momentum transfer to the atomic cloud. The optical fields must bridge (relatively large) hyperfine frequency differences within the atom, that is, couple states differing by optical frequencies and simultaneously couple states at microwave frequencies which store the qubit. Optical frequency combs (OFCs), emitted by ultrafast modelocked pulsed lasers, are excellent tools to perform quantum coherent control in multi-level atoms. The spectral purity, large bandwidth and high pulse powers makes these sources attractive for precision control of multi-level atoms.

Recent experiments have shown that an OFC can be used to coherently control and entangle trapped ion qubits by means of off-resonant Raman transitions [3, 4]. Here, we propose to extend this technique to neutral atoms confined on an atom chip and propose to implement an all-optical technique for hyperfine qubit manipulation using OFCs. Atom-chips offer a compact and robut system for coherent quantum control of atomic systems [5]. We envisage using pairs of OFC modes to drive stimulated Raman transistions between the two hyperfine clock states $5S_{1/2}|F = 2, m_F = +1\rangle$ and $5S_{1/2}|F = 1, m_F = -1\rangle$ at 3.2 G field in ^{87}Rb confined on an atom chip. The Raman transitions will be driven using a four photon technique whereby the first photon pair drives off-resonantly to the intermediate state $5S_{1/2}|F = 2, m_F = 0\rangle$ and then a second photon pair resonantly drives to $5S_{1/2}|F = 2, m_F = +1\rangle$.

Our upcoming efforts will be focused on performing spin flips with co-propogating optical beams from the modelocked pulsed laser. Following this, we plan to do spin-dependent kicks by using a counter-propogating geometry for the optical beams so that we can impart two photon recoil momenta from these beams. In this way, we plan to entangle the atomic spin with the external motion. The coherence of the clouds as a function of the clouds' separation will be studied using atom inteferometry. We foresee that inhomogeneities in the magnetic trapping potentials may restrict control over the spatial extent of the ultracold gas. Hence, we plan to tailor the optical pulses to drive stimulated Raman adiabatic passage (STIRAP). STIRAP can potentially mitigate both decoherence effects and optimize the entanglement operation.

In particular, we will apply a STIRAP scheme [6, 7, 8] which potentially allows mitigating deleterious effects on the atom spin states due to inhomogeneities in the trapping magnetic field. The technique uses well timed optical pulses to drive optical transitions between initial and target states without populating intermediate levels [9]. Here we will discuss our theoretical work to optimize the Raman transitions using an optical frequency comb to coherently control hyperfine atomic qubits.

References

[1] J. J. Garcia-Ripoll, P. Zoller and J. I. Cirac, J. Phys. B 38, S567 (2004).

[2] Y. Wang, et al, Phys. Rev. Lett. 94, 090405 (2005).

[3] D. Hayes, D. N. Matsukevich, P. Maunz, D. Hucul, Q. Quraishi, S. Olmschenk, W. Campbell, J. Mizrahi, C. Senko, and C. Monroe, Phys. Rev. Lett. 104, 140501 (2010).

[4] W. C. Campbell, J. Mizrahi, Q. Quraishi, C. Senko, D. Hayes, D. Hucul, D. N. Matsukevich, P. Maunz, and C. Monroe, Phys. Rev. Lett. 105, 090502 (2010).

[5] P. D. D. Schwindt, E. A. Cornell, T. Kishimoto, Y. Wang, and D. Z. Anderson, Phys. Rev. A 72, 023612 (2005).

[6] J.Oreg, F.T. Hioe, and J.H.Eberly, Phys. Rev. A, 29, 690 (1985).

[7] U. Gaubatz, P. Rudecki, S. Schiemann, and K. Bergmann, J. Chem.Phys., 92, 5363 (1973).

[8] W. Shi and S. Malinovskaya, Phys. Rev. A, **82**, 013407 (2010).

[9] P.R. Berman and V.S.Malinovsky, Principles of Laser Spectroscopy and Quantum Optics, Princeton University Press, Princeton, NJ (2011).

Investigating the feasibility of a practical Trojan-horse attack on a commercial quantum key distribution system

Nitin Jain[1,2], Elena Anisimova[3,4], Christoffer Wittmann[1,2], Christoph Marquardt[1,2], Vadim Makarov[3,4] and Gerd Leuchs[1,2]

[1]*Max Planck Institute for the Science of Light, Erlangen, Germany*

[2]*Institut für Optik, Information und Photonik, University of Erlangen-Nürnberg, Germany*

[3]*Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, N2L 3G1 Canada*

[4]*Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491, Trondheim, Norway*

As of today, quantum key distribution (QKD) is the most promising and pervasive application of quantum information technology. It offers unconditional security based on the laws of quantum mechanics: an eavesdropper *Eve* introduces errors while listening to the key-exchange between two legitimate parties, *Alice* and *Bob*, which disclose her presence. However, if the theoretical model is not properly implemented or if it fails to provide a complete description of the implementation, loopholes may arise (such as from technological deficiencies or operational vulnerabilities), that allow Eve to successfully breach the security.

An optical component inside a QKD system may be probed from the quantum channel by sending in sufficiently-intense light and analyzing the back-reflected light. This forms the basis of a Trojan horse attack [1]. We experimentally review the feasibility of such an attack on Clavis2, a commercially available QKD system from ID Quantique [2]. The objective is to read Bob's phase modulator (PM) to acquire knowledge of his basis choice, as this information suffices for constructing the raw key in the Scarani-Acin-Ribordy-Gisin 2004 (SARG04) protocol [3].

The principal idea is to send in a bright coherent pulse at a suitable wavelength λ and appropriately-chosen time τ, such that its back-reflection would've traversed through Bob's PM when it was activated (with frequency $f_{\text{Clavis2}} = 5$ MHz). This back-reflection, essentially a weak coherent state $|\alpha(\lambda)\rangle$, carries an imprint of Bob's randomly-chosen phase of 0 or $\frac{\pi}{2}$. Eve's task is then to be able to distinguish between two weak coherent states with some angle $\theta(\lambda)$ between them. This can be accomplished by, e.g., homodyne detection. The prior information that Eve requires is: when to send in the pulse (τ), and how many photons on average ($|\alpha(\lambda)|$) to expect. These can be readily estimated by techniques such as optical time domain reflectometry (OTDR) [1, 4].

We first prepared OTDR maps of the Bob module at three different wavelengths: 806, 1310 and 1550 nm. In fig. 1(a), we present the reflection maps at two of them. We find that the highest back-reflection level that could be utilized for an attack is only around -60 dB, implying that Eve needs to send in a bright pulse to obtain *at least* a few photons in the back-reflected pulse (a higher $|\alpha|$ would reduce probability of discrimination error).

With such a chosen intensity of Eve's input light, we find that strong afterpulsing occurs in Bob's detectors (see fig. 1(b)). Since this would cause a high QBER that would stop the QKD exchange, we are currently exploring the long wavelength $(1600 - 2000$ nm$)$ regime where we conjecture that a low detector sensitivity and/or high back-reflection level would mitigate the afterpulsing effects. The idler output
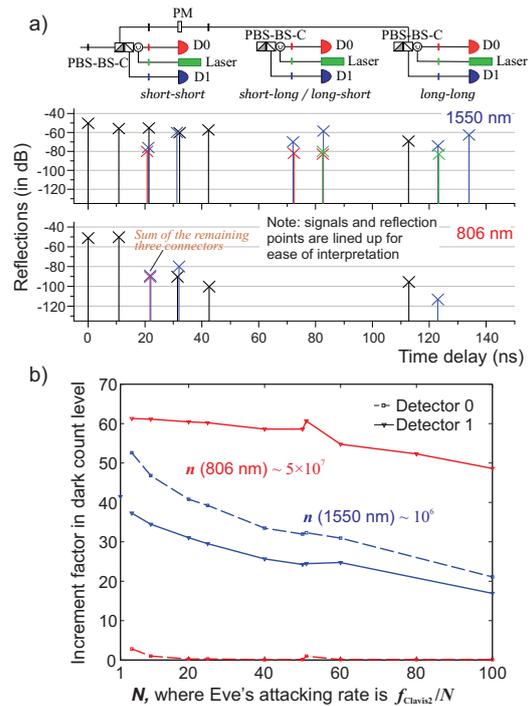
Figure 1: a) Reflection maps obtained using the OTDR technique at 806 nm and 1550 nm. b) Increase in dark count rate of Bob's detectors due to afterpulsing effects.

of an optical parametric oscillator, or supercontinuum light serve as two possible light sources to perform such a broadband spectral characterization. We report on the first results obtained with these sources and the feasibility to craft and execute a successful attack.

Several technical countermeasures such as watchdog detectors, optical isolators/filters, etc. have been proposed and need to be taken into account for security proofs.

References

[1] N. Gisin *et al.*, Phys. Rev. A **73**, 022320 (2006).

[2] Datasheet of Clavis2, available at ID Quantique website http://www.idquantique.com

[3] V. Scarani, A. Acin, G. Ribordy and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[4] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).

Programmable Multi-mode Quantum Networks

J. Janousek[1], **S. Armstrong**[1,2], **B. Hage**[1], **J-F. Morizur**[3], **P. K. Lam**[1], **H-A. Bachor**[1]

[1]*Centre for Quantum Computation and Communication Technology, The Australian National University, Canberra ACT Australia*
[2]*Department of Applied Physics, The University of Tokyo, Tokyo, Japan*
[3]*Laboratoire Kastler Brossel, Universit Pierre et Marie Curie, Paris, France*

We report on the experimental preparation of various multi-mode entangled states, with the ability to switch between them in real-time. Up to N-mode entanglement is measured with just one detector, here N = 8.

New continuous variable quantum protocols such as cluster state computation [1] and quantum error correction [2] require an increasing number of modes to be entangled in a specific way. Current multi-partite entanglement schemes tend to employ one detection scheme per entangled mode, which introduces an inherent lack of flexibility and is detrimental to its scalability. These optical setups are built to produce one set of outputs or to perform one given protocol; in order to change the output the optical hardware itself must be modified. Here, we demonstrate a system which offers the flexibility to switch between desired outputs, by measuring all of the entangled modes simultaneously with just one detection system. The switching is done in real time, via software only, requiring no modification of the optical setup. This is achieved by applying calculated electronic gain functions to spatial regions of optical modes co-propagating in one beam.

Entanglement between co-propagating modes has been demonstrated previously by this group [3]. In the current work we extend the idea of one-beam entanglement by introducing the notion of emulating linear optics networks, by programming virtual networks that mix together different spatial regions of the detected light beam, as shown in Fig. 1. By defining our modes to be combinations of different spatial regions of the beam, we may use just one pair of multi-pixel detectors and one local oscillator to measure an orthogonal set of modes. The software based networks calculate the precise weighted combinations of the spatial regions required to emulate the physical networks.

The virtual networks are fully equivalent to the physical linear optics networks they are emulating. We show that up to N-mode entanglement is measurable given just one pair of detectors each with N photodiodes, and demonstrate N=2 up to N=8 entangled modes, the results of which are shown in Fig. 2. Our approach introduces flexibility and scalability to multi-mode entanglement, two important attributes that are presently lacking in state of the art devices.

Figure 1: Spatial mode patterns. Measured modes are defined as spatial patterns of electric field amplitudes. Here an input mode basis (middle row) is projected on to bases of entangled modes. The top row shows the EPR or 2-mode basis, while the bottom row shows the 8-mode basis. The projection is done via electronic gains, calculated using virtual networks. Shown in the pattern creation box is an example of how the spatial mode pattern for input mode $\hat{a}_5$ is created by applying 8 electronic gain values to the detected light.
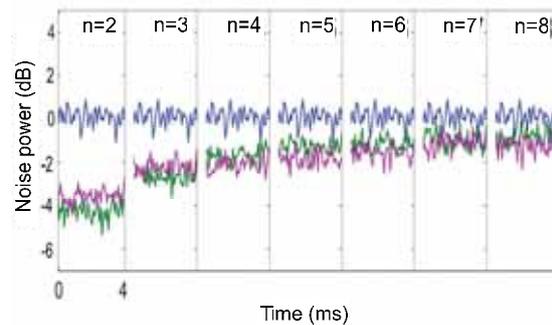
Figure 2: Correlations between entangled modes. The variances of quadrature amplitude combinations here are shown to be below 0dB, defined to be the classical bound of separability. Hence we measure entanglement for states up to N=8, with the strength of inseparability diminishing due to increased amount of vacua noise penalty introduced in to the virtual networks with higher N. The green trace shows the amplitude quadrature correlations, x, and the purple trace shows momentum quadrature correlations, p.

References

[1] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, P. van Loock, Physical Review A **79**, 062318 (2009)

[2] T. Aoki, G. Takahashi, T. Kajiya, J. Yoshikawa, S. L. Braunstein, P. van Loock, A. Furusawa, Nature **5**, 541-546 (2009)

[3] J. Janousek, K. Wagner, J-F. Morizur, N. Treps,. P. K. Lam, C. C. Harb, H-A. Bachor, Nature Photonics **3**, 399-403 (2009)

Ultra narrowband telecom polarisation entanglement source for future long distance quantum networking

Florian Kaiser, **Lutfi Arif Ngah**, **Amandine Issautier**, **Olivier Alibart**, **Anthony Martin** and **Sébastien Tanzilli**

Laboratoire de Physique de la Matière Condensée, CNRS UMR 7336, Université de Nice - Sophia Antipolis, France

Entanglement has evolved from being a *spooky* interaction towards a key resource of real-life applications such as absolute secure communication. Today, quantum networking devices are commercially available, typically taking advantage of time-bin or polarisation entanglement, the latter one doubtlessly being easier to analyse thanks to interferometer free set-ups. The communication distance of such systems is generally limited to a few hundreds of kilometres due to intrinsic fibre transmission losses and imperfect detectors. It was shown that the communication distance can be greatly increased when combining entangled pairs of photons and quantum memories [1]. But the narrow absorption bandwidth of current quantum memories is in contrary to the widely used broadband entanglement sources based on non linear interactions. More precisely, there is a lack of ultra narrowband sources in the telecom C-band, where fibre losses are minimal and high performance guided-wave optics are available. In the following we introduce a high quality polarisation entanglement engineering scheme based on a birefringent delay line (BDL). This BDL is applied to generate polarization entanglement from a high efficiency ultra narrowband telecom photon pair source where no polarisation entanglement is available initially.

The BDL scheme is shown in Figure 1. A pair of incoming photons is sent to an actively stabilised 18 m unbalanced Mach-Zehnder interferometer like birefringent delay line made of a fibre polarising beam splitter (f-PBS) at the input and output, respectively. In this particular realisation the $|H\rangle$ polarisation component is delayed by 76 ns compared to the $|V\rangle$ counterpart. Via post selection of simultaneously arriving pairs of photons a polarisation entangled state of the form $\psi(\phi) = \alpha|H\rangle_1|H\rangle_2 + e^{i\phi}\beta|V\rangle_1|V\rangle_2$ is generated. Note that all parameters of this state are easily accessible *i.e.* α and β via control on the pair's input polarisation state and the phase ϕ by fine tuning of the path lengths. Therefore any superposition of maximally entangled Bell states $|\Phi^{\pm}\rangle$ can be generated. The BDL is applied to a high efficiency type-0 periodically poled lithium niobate waveguide (PPLN/W) source pumped by a 780 nm laser. The pairs at the output ($|V\rangle_1|V\rangle_2$) are collected using a single mode fibre and filtered down to 25 MHz thanks to a phase shifted fibre Bragg grating. In order to engineer polarisation entanglement, the paired photons are rotated to the diagonal state $|D\rangle_1|D\rangle_2$ using a polarisation controller and sent to the BDL, where simultaneously exiting pairs are projected onto a maximally entangled polarisation Bell state. The source quality is measured by violation of Bell's inequalities. High visibilities ($> 99\%$) for several filtering bandwidths, *i.e.* 100 GHz (ITU channel), 540 MHz (absorption of some solid state quantum memories) and 25 MHz (atomic quantum memories) show the versatility of our approach (see Figure 2). In order to render our source compatible with current quantum memories, the wavelength of the emitted pairs has to be converted from telecom to visible, where most quantum memories operate. Such wavelength converters already exist, showing low noise and high efficiency [2]. We state that starting with a source of entangled photons in the visible is disadvantageous due to extremely high fibre losses at these wavelengths. Therefore long distance distribution of narrowband *telecom* photons and wavelength conversion only in front of the desired quantum memory is the preferred strategy. A non negligible side effect is that narrowband photons are less sensitive to fibre chromatic dispersion. We believe that our approach will play an important role for future quantum networks in which photons and quantum memories are to be combined.

Figure 2: Left: Temporal response of the filtered entangled photons for several filtering bandwidths. Note that for 100 GHz the temporal response is given by the detector's timing jitter. Right: Violations of Bell's inequalities when performing a phase scan in the diagonal analysis basis. The same high visibilities are also obtained when performing the classical polarisation measurements.

Figure 1: Set-up. Starting from a narrowband photon pair source, polarisation entanglement is engineered using a birefringent delay line and measured with a Bell state analyser.

References

[1] N. Sangouard *et al.*, Rev. Mod. Phys., **83**, 33 (2011).

[2] S. Tanzilli *et al.*, Nature, **437**, 116 (2005).

Long distance continuous-variable quantum communication

Imran Khan[1,2], Christoffer Wittmann[1,2], Nitin Jain[1,2], Nathan Killoran[3,4], Norbert Lütkenhaus[3,4], Christoph Marquardt[1,2] and Gerd Leuchs[1,2]

[1]*Max Planck Institute for the Science of Light, Erlangen, Germany*
[2]*Institute of Optics, Information and Photonics, University of Erlangen-Nürnberg, Erlangen, Germany*
[3]*Institute for Quantum Computing, Waterloo, Canada*
[4]*Department of Physics & Astronomy, University of Waterloo, Waterloo, Canada*

Quantum correlations are at the heart of all quantum communication. In experimental data, such correlations can be investigated using the concept of effective entanglement [1, 2]. In a former experiment, we have witnessed the distribution of effective entanglement over a 2 km fiber channel by simultaneous measurement of conjugate Stokes operators [3]. We now present our results on the quantification of effective entanglement employing a simultaneous measurement of conjugate quadrature operators $\hat{X}$ and $\hat{P}$. With channel lengths of up to 40 km this sets, to our knowledge, a new record for continuous-variable quantum communication.
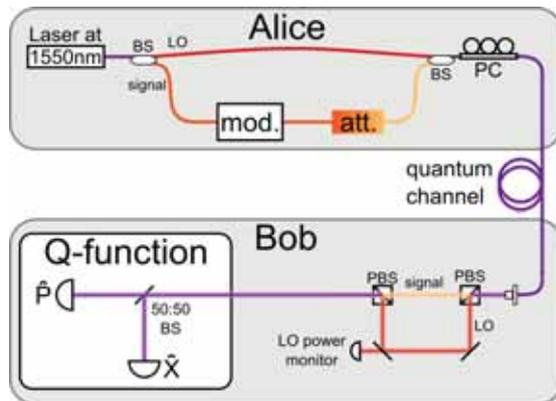
Figure 1: A schematic of the setup. Alice (fiber-integrated): beam splitter (BS), local oscillator (LO), Mach-Zehnder modulator (mod.), optical attenuator (att.), polarization controller (PC); Bob (free space): polarization beam-splitter (PBS), $\hat{X}$ and $\hat{P}$ homodyne detectors.

In our experimental setup (Figure 1), a 1550 nm laser is used for the generation of pulses at a repetition rate of 1 MHz. The pulses are then split up asymmetrically into a local oscillator (LO) and a signal line. The larger portion of the beam is directed to the LO line to provide a strong phase reference for the weak signal beam. The signal preparation line uses a Mach-Zehnder modulator to generate the quantum state alphabet and an optical attenuator to attenuate them to a quantum level. Once recombined, both signal and LO enter the quantum channel with orthogonal polarizations. At Bob's side, signal and LO are split up to allow for temporal mode matching and monitoring of the LO power. Finally the states enter the detection setup, where double homodyne detection, which corresponds to a measurement of the Q-function, is used to characterize the signal states.

To probe the quantum channel, Alice prepares two weak coherent states $|\alpha\rangle$ and $|-\alpha\rangle$ ($|\alpha| \approx 0.5$). By analyzing the first and second moments of the measured Q-functions we can estimate the received signal amplitudes and the excess noise acquired by the channel. The obtained information is then used to quantify the remaining quantum correlations of our quantum states after propagation through the channel. In order to be useful for quantum communication, a channel must preserve entanglement, which we study using the concept of effective entanglement [4]. The entanglement is quantified using the negativity $\mathcal{N}$, which distinguishes between separable ($\mathcal{N} = 0$) and entangled ($\mathcal{N} > 0$) states. Using the described set of states and our setup we recorded data for varied experimental parameters, such as the length of fiber channel or the amplitudes of our coherent states (Figure 2). This allowed us to find the limits of our continuous-variable quantum communication setup with regard to effective entanglement.
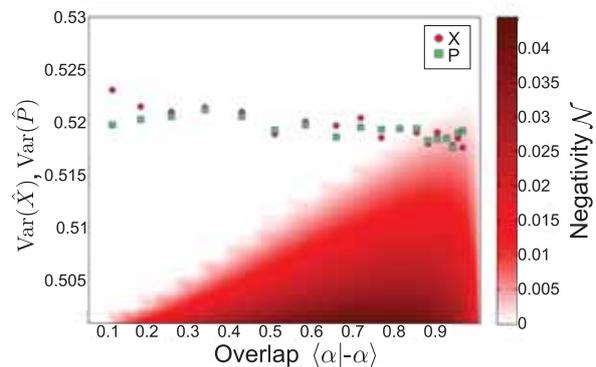
Figure 2: Effective entanglement over a 40 km channel: The quantum channel has been probed for different signal overlaps $\langle\alpha|-\alpha\rangle$. The recorded data shows a quadrature variance of around 0.52, where 0.50 would be the shot noise level, thus indicating 4% of excess noise for our system. Non-zero effective entanglement is witnessed and quantified for high overlaps, demonstrating that the 40 km fiber channel is able to preserve the correlations necessary for quantum communication.

References

[1] J. Rigas et al., Phys. Rev. A 73, 012341 (2006)

[2] H. Häseler et al., Phys. Rev. A 77, 032303 (2008)

[3] C. Wittmann et al., Opt. Express 18, 4499 (2010)

[4] N. Killoran et al., Phys. Rev. A 83, 052320 (2011)

Entanglement of Ince-Gauss Modes of Photons

Mario Krenn[1]**, Robert Fickler**[1]**, William Plick**[1]**, Radek Lapkiewicz**[1]**, Sven Ramelow**[1]**, Anton Zeilinger**[1]

[1]*University of Vienna, Faculty of Physics, IQOQI Vienna, Austrian Academy of Sciences, Austria*

Ince-Gauss modes are solutions of the paraxial wave equation in elliptical coordinates [1]. They are natural generalizations both of Laguerre-Gauss and of Hermite-Gauss modes, which have been used extensively in quantum optics and quantum information processing over the last decade [2].

Ince-Gauss modes are described by one additional real parameter - ellipticity. For each value of ellipticity, a discrete infinite-dimensional Hilbert space exists. This conceptually new degree of freedom could open up exciting possibilities for higher-dimensional quantum optical experiments. We present the first entanglement of non-trivial Ince-Gauss Modes.

In our setup, we take advantage of a spontaneous parametric down-conversion process in a non-linear crystal to create entangled photon pairs. Spatial light modulators (SLMs) are used as analyzers.

References

[1] Miguel A. Bandres and Julio C. Gutirrez-Vega "Ince Gaussian beams", Optics Letters, Vol. 29, Issue 2, 144-146 (2004).

[2] Adetunmise C. Dada, Jonathan Leach, Gerald S. Buller, Miles J. Padgett, and Erika Andersson, "Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities", Nature Physics 7, 677-680 (2011).

Security of practical quantum cryptography with heralded single photon sources

Mikolaj Lasota[1], **Rafal Demkowicz-Dobrzanski**[2] and **Konrad Banaszek**[2]

[1] *Faculty of Physics, Astronomy and Applied Informatics, Nicolaus Copernicus University, Torun, Poland*
[2] *Faculty of Physics, University of Warsaw, Warsaw, Poland*

The theoretically unconditional security of quantum key distribution (QKD) can be compromised in practical implementations due to imperfections of available components, such as limited quantum efficiency and dark counts of detectors, attenuation of light transmitted through a fiber, and multiphoton events generated by non-ideal single photon sources. Nevertheless, even under pessimistic assumptions QKD can be shown to remain secure for realistic parameters of the devices. The imperfections impose a lower bound on the power transmission T of the optical channel linking the communicating parties, which in turn defines the maximum distance over which QKD is possible. A more detailed characteristics of interest is the key rate as a function of transmission T.

In this contribution, we analyse theoretically the application of photon number resolving (PNR) detectors to improve the quality of heralded single photon sources based on spontaneous parametric down-conversion (SPDC). This generalizes the work of Brassard *et al.* [1] who analyzed the performance of the BB84 QKD protocol [2] using ideal single photons (SGL), weak coherent pulses (WCP) derived from an attenuated laser, and SPDC with binary on/off heralding detector. The motivation for our work is the rapid progress in the field of PNR detectors [3] which however exhibit new types of imperfections, and the introduction of novel QKD protocols such as SARG04 [4].

First, we demonstrate that for a realistic PNR detector used for heralding single photons from an SPDC source, the minimum transmission $T_{\min}$ required to establish a secure key is given by

$$T_{\min} \approx T_{\min}^{\text{SGL}} + T_{\min}^{\text{WCP}} \left(\frac{q_0 q_2}{q_1^2} \right)^{1/2}, \tag{1}$$

where $T_{\min}^{\text{SGL}}$ and $T_{\min}^{\text{WCP}}$ are minimum transmissions for the same protocol implemented with single photons and weak coherent pulses, and q_0, q_1, and q_2 are conditional probabilities that the PNR detector will generate the correct heralding signal when fed with zero, one, or more than one photons. The above formula defines the usefulness of a particular PNR detector to increase the QKD distance. An an example, for a multiplexing device composed of N individual detectors, each characterized by the dark count probability d_A and the quantum efficiency η_A, we have

$$\frac{q_0 q_2}{q_1^2} \approx d_A \left(1 + 2N \frac{1 - \eta_A}{\eta_A} \right) \tag{2}$$

in the regime when $d_A \ll 1$. This implies that increased dark count rates override the benefit of partial photon number resolution.

However, multiplexing detectors can be used to increase the key rates over short and medium distances. To demonstrate this we carried out a complete calculation of the key rate

k as a function of the channel transmission T for BB84 and SARG04 protocols based on the method presented by Renner *et* al. [5], including optimisation over the pumping strength of the non-linear medium. We considered a tree-like multiplexing arrangement with imperfect splitters. As shown in Fig. 1, for realistic parameters multiplexed heralding is capable of increasing the key rate by up to 40% for moderate distances.
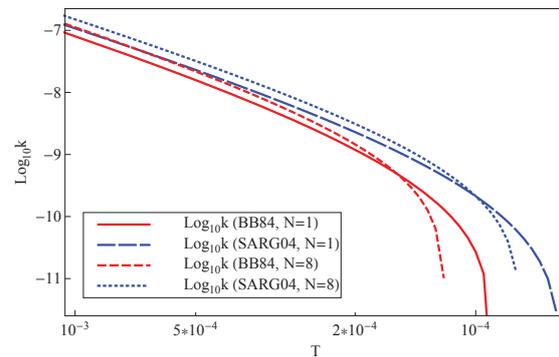
Figure 1: The optimized key rate k as a function of the channel transmission T for the BB84 and SARG84 protocols with a SPDC source employing a single ($N=1$) heralding detector and a multiplexed scheme with $N=8$ detectors. An individual heralding detector is assumed to have 60% efficiency and 10^{-6} dark count probability, with 2% insertion loss for each splitter in the tree-like multiplexing arrangement. The dark count probability for the receiver detectors is equal 10^{-5}, and their efficiency is included in T.

References

[1] G. Brassard, N. Lutkenhaus, T. Mor and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[2] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175–179, Institute of Electrical and Electronics Engineers, New York (1988).

[3] R.H. Hadfield, Nature Photon. **3**, 696 (2009).

[4] V. Scarani, A. Acin, G. Ribordy, N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[5] R. Renner, N. Gisin, B. Kraus, Phys. Rev. A **72**, 012332 (2005).

Guaranteed violation of a Bell inequality
without aligned reference frames or calibrated devices

Peter Shadbolt[1], Tamás Vértesi[2], Yeong-Cherng Liang[3], Cyril Branciard[4], Nicolas Brunner[5] and Jeremy L. O'Brien[1]

[1]*Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Bristol, United Kingdom*
[2]*Institute of Nuclear Research of the Hungarian Academy of Sciences, Debrecen, Hungary*
[3]*Group of Applied Physics, University of Geneva, Geneva, Switzerland*
[4]*School of Mathematics and Physics, The University of Queensland, Australia*
[5]*H.H. Wills Physics Laboratory, University of Bristol, Bristol, United Kingdom*

Bell tests [1] — the experimental demonstration of a Bell inequality violation — are central to understanding the foundations of quantum mechanics, underpin quantum technologies, and are a powerful diagnostic tool for technological developments in these areas. In a quantum Bell test, two (or more) parties perform local measurements on an entangled quantum state. After accumulating enough data, both parties can compute their joint statistics and assess the presence of quantum nonlocality by checking for the violation of a Bell inequality. Although entanglement is necessary for obtaining nonlocality it is not sufficient. Even for sufficiently entangled states, one needs judiciously chosen measurement settings. Thus although nonlocality reveals the presence of entanglement in a device-independent way, that is, irrespectively of the detailed functioning of the measurement devices, one generally considers carefully calibrated and aligned measuring devices in order to obtain a Bell inequality violation. This in general amounts to having the distant parties share a common reference frame and well calibrated devices.

Although this assumption is typically made implicitly in theoretical works, establishing a common reference frame, as well as aligning and calibrating measurement devices in experimental situations are never trivial issues. For instance, in the context of quantum communications via optical fibers, unavoidable small temperature changes induce strong rotations of the polarization of photons in the fiber. This makes it challenging to maintain a good alignment, which in turn severely hinders the performance of quantum communication protocols in optical fibers [2]. Also, in the field of satellite based quantum communications [3], the alignment of a reference frame represents a key issue given the fast motion of the satellite and the short amount of time available for completing the protocol. Finally, in integrated optical waveguide chips, the calibration of phase shifters is a cumbersome and time-consuming operation. As the complexity of such devices is increased, this calibration procedure will become increasingly challenging.

It is therefore an interesting and important question whether the requirements of having a shared reference frame and calibrated devices can be dispensed with in nonlocality tests. Here, we further develop the idea proposed in Ref. [4] and show [5] that neither of these operations are necessary: violation of the Clauser-Horne-Shimony-Holt-Bell inequalities without a shared frame of reference, and even with uncalibrated devices, can be achieved with near-certainty by performing local measurements in randomly chosen bases. We first show that whenever two parties perform three mutually unbiased (but randomly chosen) measurements on a maximally entangled qubit pair, they obtain a Bell inequality violation with certainty—a scheme that requires no common reference frame between the parties, but only a local calibration of each measuring device. We further show that when all measurements are chosen at random (*i.e.*, calibration of the devices is not necessary anymore), although Bell violation is not obtained with certainty, the probability of obtaining nonlocality rapidly increases towards one as the number of different local measurements increases.

Experimentally, we verify the feasibility of these schemes by performing these random measurements on the singlet state of two photons using a reconfigurable integrated waveguide circuit [6], based on voltage-controlled phase shifters. The data confirm the near-unit probability of violating an inequality as well as the robustness of the scheme to experimental imperfections—in particular the non-unit visibility of the entangled state—and statistical uncertainty. These new schemes exhibit a surprising robustness of the observation of nonlocality that is likely to find important applications in diagnostics of quantum devices (*e.g.*. removing the need to calibrate the reconfigurable circuits used here) and quantum information protocols, including device independent quantum key distribution [7] and other protocols based on quantum nonlocality [8] and quantum steering [9].

References

[1] A. Aspect, Nature **398**, 189 (1999).

[2] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145195 (2002).

[3] M. Aspelmeyer *et al.*, IEEE J. Sel. Top. Quantum Electron. **9**, 1541 (2003).

[4] Y.-C. Liang *et al.*, Phys. Rev. Lett. **104**, 050401 (2010); J. J. Wallman *et al.*, Phys. Rev. A **83**, 022110 (2011).

[5] P. Shadbolt *et al.*, arXiv:1111.1853 (2011).

[6] P. J. Shadbolt *et al.*, Nature Photon. **6**, 45 (2012).

[7] A. Acín *et al.*, Phys. Rev. Lett. **98**, 230501 (2007).

[8] S. Pironio *et al*, Nature **464**, 1021 (2010); R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2011); R. Rabelo *et al.*, Phys. Rev. Lett. **107**, 050502 (2011).

[9] C. Branciard *et al.*, Phys. Rev. A **85**, 010301(R) (2012).

Long-distance quantum key distribution with imperfect devices

Nicoló Lo Piparo[1] **and Mohsen Razavi**[1]

[1] *School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK*

Quantum key distribution (QKD), over long distances, relies on quantum repeaters to share entangled states between two remote parties. A practical way to implementing quantum repeaters is to use probabilistic schemes, which can possibly operate using imperfect devices [1-5]. Here, we compare two such schemes in terms of their secure key generation rates per memory, R_{QKD}, under practical assumptions.

The schemes we consider are the one proposed by Duan, Lukin, Cirac and Zoller [2], denoted by DLCZ hereafter, and the single-photon-source protocol, denoted by SPS, proposed in [3]. The DLCZ protocol uses atomic ensembles as quantum memories (QMs); see Fig. 1(a). By coherently pumping these QMs, they may undergo Raman transitions emitting photons and leaving atoms in symmetric collective states. A single detection at the middle site heralds entanglement generation between QMs. Within the DLCZ scheme, it is possible that both QMs store excited states-a non-entangled state-leading to lower values for R_{QKD}. The SPS protocol, instead, is not ideally affected by this limitation. As shown in Fig. 1(b), entanglement is distributed by ideally generating single photons and directing them toward the middle measurement site via beam splitters with transmission coefficients η. The other ports are directed to and stored in QMs. Again, a single click in the middle heralds entanglement.

In this paper, we consider various sources of imperfection in the SPS protocol, such as a nonzero double-photon probability, p, for the source, channel loss and inefficiencies in photodetectors and memories, to find R_{QKD} under two scenarios. In the first scenario, entangled pairs are generated over a distance L using the scheme in Fig. 1(b). In the second one, we use a quantum repeater link, as shown in Fig. 1(c). In both cases, photons are retrieved from QMs and QKD measurements are performed on these photons according to the protocol described in [5]; see Fig. 1(c). We assume a multimemory configuration, in which the above procedure can be repeated in parallel in a cyclic way [4]. R_{QKD} is then a normalized figure of merit that accounts for the number of memories used. Finally, we compare our results with that of the DLCZ protocol as reported in [5].

Figure 2(a) shows R_{QKD} versus η, in Fig. 1(b), for the SPS protocol. We have considered both photon-number resolving detectors (PNRDs) and non-resolving photon detectors (NRPDs). We find that there exists an optimum value of η, which maximizes R_{QKD}. It turns out that this optimum value is insensitive to distance. Using the optimum value for η, in Fig. 2(b), we have plotted R_{QKD} versus p. It can be seen that for $p > 0.03$, in the no-repeater case, and $p > 0.006$, in the repeater case, we cannot guarantee secure key exchange. Nevertheless, these are practical limits for the current technology of single-photon sources. Figures 2(a) and 2(b) also show that it is not crucial to use PNRDs. Finally, in Fig. 2(c), we compare the SPS and DLCZ schemes. It turns out that the SPS outperforms DLCZ for practical values of p. The
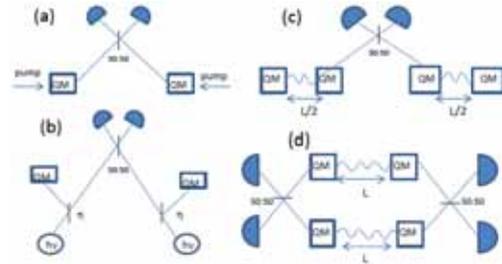
Figure 1: (a) Entanglement distribution scheme for DLCZ protocol; (b) entanglement distribution scheme for SPS protocol; (c) quantum repeater scheme; and (d) QKD scheme.
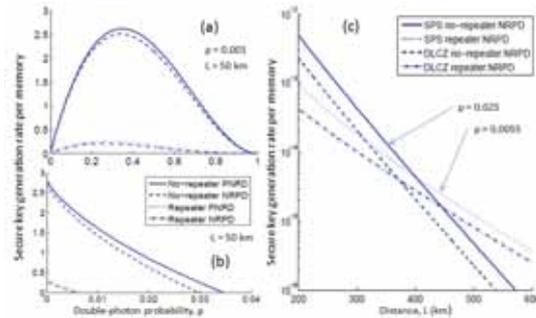
Figure 2: R_{QKD} versus (a) η and (b) p in the repeater and no-repeater cases when PNRDs and NRPDs are used. (c) R_{QKD} for DLCZ and SPS protocols versus distance. In all graphs, the channel loss is 0.17dB/km, the writing (reading) efficiency of QMs is 0.9 (0.7), and quantum efficiency is 0.5.

crossover distance, where quantum repeaters outperform the direct link, is reduced in the SPS case, where the repeater nodes are apart by 100 km at $p = 0.002$ and when NRPDs are used.

References

[1] N. Sangouard *et al.*, Rev. Mod. Phys., **83**, 33 (2011).

[2] L. M. Duan, M.D. Lukin, J. I. Cirac and P. Zoller, Nature (London), **414**, 413 (2001).

[3] N. Sangouard *et al.*, Phys. Rev. A, **76**, 050301 (2007).

[4] M. Razavi, M. Piani and N. Lütkenhaus, Phys. Rev. A, **80**, 032301 (2009).

[5] J. Amirloo, M. Razavi and A. H. Majedi, Phys. Rev. A, **82**, 032304 (2010).

Continuous variable quantum key distribution with optimally modulated entangled states

Vladyslav C. Usenko[1,3], **Lars S. Madsen**[2], **Mikael Lassen**[2], **Radim Filip**[1] and **Ulrik L. Andersen**[2]

[1]*Department of Optics, Palacky University, Olomouc, Czech Republic*
[2]*Department of Physics, Technical University of Denmark, Kongens Lyngby, Denmark*
[3]*Bogolyubov Institute for Theoretical Physics of National Academy of Sciences, Kiev, Ukraine*

Quantum key distribution (QKD) enables two remote parties to grow a shared key which they can use for unconditionally secure communication. Being first proposed on the basis of single qubits and qubit pairs, QKD was recently developed on the basis of continuous-variable (CV) quantum states of light, in particular, coherent [1] and squeezed states [2].

The applicability of the CV QKD protocols depends of the loss and noise of the quantum channel, connecting two trusted parties. Most of the schemes based on the coherent states and CV measurements are resilient to high loss in the channel, but are sensitive to the small amounts of the channel noise.

In the present work we propose and experimentally address a CV QKD protocol which uses entangled states optimally combined with a large coherent modulation. The protocol is based on the preparation of the two-mode entangled state, by coupling two orthogonally squeezed states, and application of the optimized correlated Gaussian displacement on its modes. Trusted parties are then performing homodyne measurements on their modes and are supposed to process the data in the reverse reconciliation scenario.

Following the Gaussian security proofs we show that additional modulation of entangled states greatly enhances the robustness of the protocol to channel noise and, accordingly, increases the applicable distance of the protocol. The peculiarity of our protocol is that due to the optimal modulation the trusted parties are gaining from any amount of nonclassicality, which is present in the source.

The experimental data obtained on the modulated entangled states well confirm the theoretical security predictions and show possibility to fully implement the proposed protocol.

We also show that the improvement by optimal coherent modulation is preserved upon limited post-processing efficiency [4]. Thus, our scheme represents a very promising method for extending the applicability of the practical CV QKD.

References

[1] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002); Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002); F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003); C. Weedbrook et al., Phys. Rev. Lett. **93** 170504 (2004).

[2] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999); M. Hillery, Phys. Rev. A **61**, 022309 (2000); N.J. Cerf, M. Levy and G. Van Assche, Phys. Rev. A **63**, 052311 (2001); D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).

[3] M.M. Wolf, G. Giedke and J.I. Cirac, Phys. Rev. Lett. **96** 080502 (2006); M. Navascues, F. Grosshans and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006); R. García-Patron and N.J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[4] V. C. Usenko and R. Filip, New J. Phys. **13** 113007 (2011)

Quantum Key Distribution Software maintained by AIT

Oliver Maurhart[1], Christoph Pacher[1], Andreas Happe[1], Thomas Lorünser[1], Gottfried Lechner[2], Cristina Tamas[1], Andreas Poppe[1] and Momtchil Peev[1]

[1]*AIT Austrian Institute of Technology, Donau-City-Strasse 1, 1220 Vienna, Austria*
[2]*University of South Australia, Institute for Telecommunications Research (ITR), Mawson Lakes, SA 5095, Australia*

Quantum Key Distribution has come of age. After the first proof-of-principe realizations, many different implementations, based on different physical principles, have been proposed. Subsequently these have been scrutinized in an ongoing security and efficiency analysis effort (see Ref.[1] for a recent review). Currently the landscape of QKD includes three main classes of systems coming in a variety of realization types and flavors. While the breadth of the field is impressive critical mass has been accumulated only in very few cases, hindering thus broader practical adoption. It must, however be stressed that whatever the "physical layer" of QKD is, it provides in the end a pair of strongly correlated bit strings that have then to be distilled by a fundamentally universal postprocessing protocol to yield Information Theoretically Secure (ITS) key. Post-processing is an obvious target for providing standard cryptographic, coding and software implementation realizations. This task has however been often underestimated for a seeming lack of fundamental importance, or immediate interest in an typically experimental physics environment.

Building on a broad collaboration between experimentalists, quantum information theorists and cryptographers, the AIT team initiated in the framework of the European project SECOQC (2004-2008) a common "software level" approach to QKD [2] to combine many independent quantum links into a QKD Network. Later this network-centric effort was extended to include universal aspects of QKD post-processing and currently aims also to include general mechanisms for management and control of different QKD physical-layer realizations. This contribution focuses on the present stage of this development, the current approach aiming to make it a joint effort of the community, and the foreseeable next steps.

The QKD software can be be generally subdivided in several logical segments: the **QKD Network software**, the **QKD Node/Link software**, the **QKD postprocessing stack**, and the **QKD management tools**.

The QKD Network software originates from the SECOQC times and aims at establishing a trusted repeater network of independent QKD links, the objective being to allow for ITS routing and ITS (key-material) transport. The QKD Node/Link software is also a SECOQC architectural design, operating the Q3P protocol and allowing for an effective encapsulation of the point-to-point classical communication of QKD peers linked by a quantum channel. The design of these two basic software segments was discussed in some detail in Ref.[2]. In this contribution we give an update of the development in this domain and the plans for next steps.

The QKD postprocessing stack, originally designed and developed internally for being used with the AIT QKD systems has been opened to the scientific community. The stack operates as a series of separate processes each taking its input from the previous process, and posting its output to the next process, much like pipes in standard UNIX. Every process exhibits a certain interface qualifying it to be a *QKD Module*. A QKD Module **read**s a *QKD Key* from the previous module, **send**s and **recv**(receives) *QKD Messages* with the same module on the peer side and finally **write**s the modified QKD Key as output. The main functions `read`, `write`, `send` and `recv` are provided by the *QKD Framework* and are similar to the well know POSIX pendants. The stack includes algorithms for all necessary steps for BB84 post processing: sifting, error correction, confirmation, and privacy amplification. New modules can readily be included in the Framework.

In the contribution we discuss both the Framework, the generic module design and highlight implemented algorithms. In particular for *reconciliation* we have used density evolution to optimize LDPC codes for different code rates for the BSC. In addition, a set of different LDPC encoders including different approaches to deal with varying channel conditions has been implemented. We compare their efficiencies (gap to the channel capacity) and performance (bit/s) as function of code rate, block size, and channel conditions. *Confirmation* is performed with different families of almost universal hash functions. For *privacy amplification* we use the well-known Toeplitz hashing which is implemented using the number theoretic transform in GF(p) with $p = 15 * 2^{27} + 1$. This gives an upper limit of the blocksize of $l = 2^{27}$ which is 16 MiByte. We discuss the performance as a function of different block sizes.

We further present the QKD management tools that allow to orchestrate all QKD Modules and to react to hardware events. Central management facilities are the *OID-Store* in conjunction with *DBus*. The OID-store collects and makes process variable values accessible outside their original process space. The Distributed Bus (DBus) is a standard Inter Process Communication mechanism for process variables' transport, allowing management observation and control of the system in operation by the main control instance - the *qkd-control-daemon*.

AIT aims at encouraging the research community access to the QKD software software in order to provide a background framework and thus focusing of efforts on really open instead of technical questions. The software is licensed as open source under the GNU GPL V2 and GNU LGPL V2.1. The motivation, details and impacts of this policy are also be discussed in the contribution.

References

[1] V. Scarani et al. Security of Practical Quantum Key Distribution, Rev. Mod. Phys., **81**, 1301 (2009).

[2] M. Peev et al. The SECOQC Quantum Key Distribution Network in Vienna, New J. Phys., **11**, 075001 (2009).

Noiseless loss suppression in quantum optical communication

Michal Mičuda[1], Ivo Straka[1], Martina Miková[1], Miloslav Dušek[1], Nicolas J. Cerf[2], Jaromír Fiurášek[1], and Miroslav Ježek[1]

[1]*Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic*
[2]*Quantum Information and Communication, Ecole Polytechnique de Bruxelles, CP 165/59, Université Libre de Bruxelles, 1050 Brussels, Belgium*

Quantum communication holds the promise of unconditionally secure information transmission. Unfortunately, the range of current point-to-point quantum key distribution systems is restricted to several tens of kilometers due to unavoidable losses in optical links. Losses, as well as errors or decoherence, may in principle be overcome by the sophisticated techniques of quantum error correction, entanglement distillation, and quantum repeaters. However, these techniques typically require encoding information into complex multimode entangled states, processing many copies of an entangled state, and – even more challenging – using quantum memories. Recently, the concept of noiseless amplification of light[1, 2, 3, 4, 5] has emerged as a promising tool for quantum optical communication. Here, we introduce a dual process called noiseless attenuation, which, combined with noiseless amplification, enables the conditional suppression of optical losses to an arbitrary extent without adding noise, hence keeping quantum coherence. The method is remarkably simple since it only requires single-mode operations. We experimentally demonstrate it in the subspace spanned by vacuum and single-photon states, and consider its applicability to arbitrary input states.

References

[1] T.C. Ralph and A.P. Lund, Nondeterministic Noiseless Linear Amplification of Quantum Systems, in *Quantum Communication Measurement and Computing*, Proceedings of 9th International Conference, Ed. A. Lvovsky, 155-160 (AIP, New York 2009); arXiv:0809.0326.

[2] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Heralded noiseless linear amplification and distillation of entanglement, *Nature Phot.* **4**, 316-319 (2010).

[3] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Implementation of a Nondeterministic Optical Noiseless Amplifier, *Phys. Rev. Lett.* **104**, 123603 (2010).

[4] M.A. Usuga, C.R. Muller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U.L. Andersen, Noise-powered probabilistic concentration of phase information, *Nature Phys.* **6**, 767-771 (2010).

[5] A. Zavatta, J. Fiurášek, and M. Bellini, A high-fidelity noiseless amplifier for quantum light states, *Nature Phot.* **5**, 52-56 (2011).

Do the Ince-Gauss Modes of Light Give Keys New Places to Hide?

William Plick[1], Mario Krenn[1], Sven Ramelow[1], Robert Fickler[1], and Anton Zeilinger[1]

[1]*Institute for Quantum Optics and Quantum Information, Vienna, Austria*

The Ince-Gauss light modes, recently discovered, are the solutions to the paraxial wave equation in elliptical coordinates. In addition to the radial, and charge, quantum numbers they posses an additional parameter - the ellipticity of the solutions. We study how the orbital angular momentum of these beams varies with the ellipticity and discover several compelling features, including: non-monotonic behavior, stable beams with fractional orbital angular momentum, and modes for whom both quantum mode numbers differ but the orbital angular momentum is the same. These features may have application to atom trapping, quantum key distribution, and quantum informatics in general – as the ellipticity opens up a new parameter space. We address the question of whether or not this parameter space may be used to hide information and make Quantum Key Distribution Schemes more robust.

Polaractivation of Quantum Channels

L. Gyongyosi[1] **and S. Imre**[1]
[1]*Quantum Technologies Laboratory, Budapest University of Technology and Economics, Budapest, Hungary*

In this work a new phenomenon called *polaractivation* is introduced. Polaractivation is based on quantum polar encoding and the result is similar to the *superactivation* effect [4]— positive capacity can be achieved with noisy quantum channels that were initially completely useless for communication. However, an important difference that polaractivation is *limited neither* by any preliminary conditions on the initial private capacity of the channel nor on the maps of other channels involved to the joint channel structure. We prove that the polaractivation of quantum channel capacities requires only the proposed quantum polar encoding scheme and the *multiple uses* of the same arbitrary quantum channel.

Polar channel coding is a revolutionary encoding and decoding scheme that makes possible the construction of codewords to achieve the symmetric capacity of noisy channels. The symmetric capacity is the highest rate at which the channel can be used for communication if the input probability distribution is equal [1,2,3].

We demonstrate that quantum polar coding can be used for the polaractivation of *private classical capacity* of any quantum channels, and the private classical capacity of quantum channels is *polaractive*.

Due to our proposed polaractivation effect any quantum channel that had zero private classical capacity initially, can be used for private classical communication. Our polar encoding scheme enables *arbitrary* noisy quantum channels and the parties can use either the amplitude or the phase to encode classical information; however, the transmission of private classical information requires both amplitude and phase coding simultaneously. This encoding scheme is possible for quantum channels, since the polarization can occur in both amplitude and phase, denoted by the quantum channels $\mathcal{N}_{amp}$ and $\mathcal{N}_{phase}$ [2].

In Fig. 1 we show the polarized channel structure: the channels can be separated into 'bad' channels $\mathcal{B}$ (Fig. 1(a)), and 'good' channels $\mathcal{G}$ (Fig. 1(b)). The difference between the two channels is the knowledge of input u_1 on Bob's side. For the 'bad' channel $\mathcal{B}$ the input u_1 is unknown. In Fig. 1(c), the second-level channel $\mathcal{N}_4$ is shown, which is the combination of the two first-level channels $\mathcal{N}_2$. The scheme also contains a permutation operator R [1,2,3].

The set of polar codewords that can transmit private classical information is defined as $S_{in} = \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)$, where $\beta < 0.5$ is a fixed constant. The 'partly good' (i.e., can be used for non-private classical communication) input codewords are defined as $\mathcal{P}_1$ and $\mathcal{P}_2$. The set of polar codewords that are useless for both the transmission of the amplitude and phase is denoted by $\mathcal{B}$.

Initially the quantum channel $\mathcal{N}$ cannot transmit any private classical information, i.e., $S_{in} = \varnothing$.
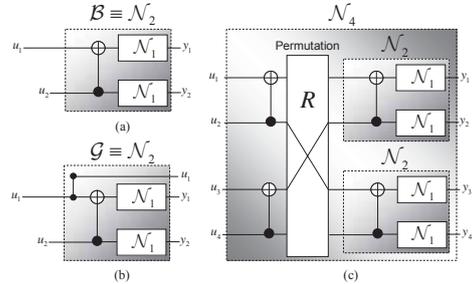
Figure 1. (a): The polaractivation scheme: for the 'bad' channel the input u_1 is not known by Bob. (b): For the 'good' channel, the input is also known on Bob's side. (c): The recursive polar channel construction.

As we have proved by using quantum polar codes, the *polaractivation*, i.e., the transformation of $S_{in} = \varnothing$ into $S_{in} \neq \varnothing$ can be achieved. Our results on the polar codeword-set construction are summarized in Fig. 2. After the polaractivation effect is realized on the channels, the channels will be able to transmit private classical information, i.e., $S_{in} \neq \varnothing$.
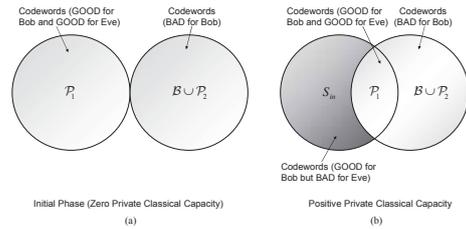
Figure 2 (a). The brief summarization of our polar codeword-set construction. In the initial phase, the input channels cannot transmit classical information privately. (b) Our quantum polar coding scheme makes it possible to construct codewords capable of transmitting private classical information between Alice and Bob.

In this work, we introduced the term polaractivation, which is the polar encoding based superactivation of quantum channels without the necessary preliminary conditions of the originally defined superactivation effect. We have shown that the private classical capacity is polaractive. We also gave an exact lower bound on the symmetric classical capacity required for the polaractivation.

References
[1] E. Arikan. Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels. IEEE Transactions on Information Theory, 55(7):3051–3073, arXiv:0807.3917, (2009).
[2] J. M. Renes, Frederic Dupuis, and Renato Renner, Efficient Quantum Polar Coding, arXiv:1109.3195v1, (2011).
[3] S. Imre, L. Gyongyosi: Advanced Quantum Communications: An Engineering Approach, Wiley-IEEE Press, (2012).
[4] G. Smith, J. Yard, Quantum Communication with Zero-capacity Channels. Science 321, 1812-1815 (2008).

Quasi-Superactivation of Zero-Capacity Quantum Channels

L. Gyongyosi[1] and S. Imre[1]
[1]*Quantum Technologies Laboratory, Budapest University of Technology and Economics, Budapest, Hungary*

The phenomenon called superactivation is rooted in the extreme violation of additivity of the channel capacities of quantum channels. The superactivation of zero-capacity quantum channels makes it possible to use two zero-capacity quantum channels with a positive joint capacity [1,2,3]. In this work the term *quasi-superactivation* is firstly introduced. While the superactivation of classical capacity of quantum channels is trivially not possible, here we prove that the quasi-superactivation of classical capacity of *any* quantum channels is possible, and the classical capacity of zero-capacity quantum channels is *quasi-superactive.*

Our result is similar to the superactivation effect—information can be transmitted over zero-capacity quantum channels. An important difference that quasi-superactivation is restricted neither by any preliminary conditions on the quantum channels of the joint channel structure. The quasi-superactivation works for the most generalized quantum channel models (*even for arbitrary quantum channels*) and requires only the most natural physical processes that occur during *stimulated emission*.

As we proved, while individually quantum channel $\mathcal{M}$ cannot used to transmit any classical information (Fig. 1(a)), positive joint classical capacity can be achieved if two of these zero-capacity channels $\mathcal{M}_1$ and $\mathcal{M}_2$ are combined and used together (Fig. 1(b)). In the joint combination each channel $\mathcal{M}_i$, $i = 1, 2$ is constructed from an *arbitrary* zero-capacity quantum channel. As we have found, two zero-capacity quantum channels in a joint structure $\mathcal{M}_1 \otimes \mathcal{M}_2$ can activate each other, and the joint classical capacity will be positive, $C(\mathcal{M}_1 \otimes \mathcal{M}_2) > 0$, while for the individual classical capacities $C(\mathcal{M}_1) = C(\mathcal{M}_2) = 0$.
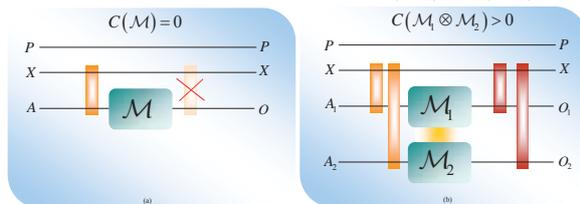
Figure 1. (a): Individually quantum channel $\mathcal{M}$ cannot transmit any classical information, i.e., $C(\mathcal{M}) = 0$. The channel destroys every classical correlation between Alice's classical register X and channel output O. (b): For the joint combination of the two zero-capacity quantum channels $\mathcal{M}_1$ and $\mathcal{M}_2$ with classical capacities $C(\mathcal{M}_1) = C(\mathcal{M}_2) = 0$, the joint classical capacity will be positive, i.e., $C(\mathcal{M}_1 \otimes \mathcal{M}_2) > 0$. Any correlation between classical register X and output systems O_1 and O_2 will occur that result in positive classical capacity.

We also revealed that the channel construction $\mathcal{M}_1 \otimes \mathcal{M}_2$ of zero-capacity channels can be used for transmission of classical information only in a very small parameter domain. Fig. 2 illustrates the *quasi-superactivation* of classical capacity of arbitrary quantum channels.
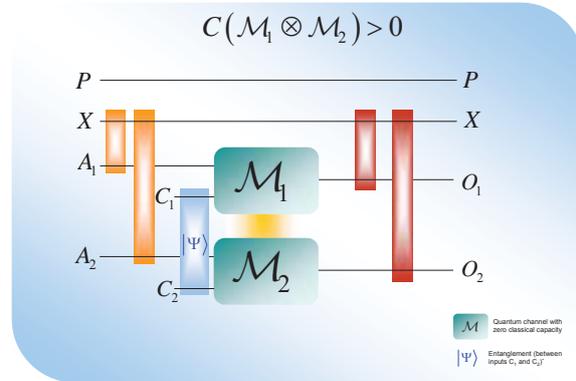
Figure 2. The detailed view of joint channel construction $\mathcal{M}_1 \otimes \mathcal{M}_2$ helps to reveal the quasi-superactivation effect. Individually, neither $\mathcal{M}_1$, nor $\mathcal{M}_2$ can transmit any classical information. On the other hand, if we use entangled auxiliary input and the amount of entanglement in the input qubits is chosen from a very limited domain, the two channels can activate each other and classical information can be transmitted. Using input states with this special amount of entanglement, the outputs of the joint channel construction will be correlated with each other and some correlation will also occur with the classical register X. However, individually every classical correlation will vanish, jointly some correlation can be produced at the channel output which leads to positive classical capacity.

The superactivation of the classical capacity of quantum channels is trivially not possible. Before our work the transmission of classical information over zero-capacity quantum channels was also seemed to be impossible. We proved that the quasi-superactivation of the classical capacity of quantum channels is possible. Besides that there exists zero-capacity channels with positive joint quantum capacity, using the quasi-superactivation it is also possible to find zero-capacity quantum channels with individually zero classical capacities, which if employed in a joint channel construction can transmit classical information.

An advance of the proposed quasi-superactivation in comparison to superactivation that our effect is limited neither by any preliminary conditions on the initial private classical capacity of the channel nor on the maps of other channels involved to the joint channel structure.

References
[1] S. Imre, L. Gyongyosi: Advanced Quantum Communications: An Engineering Approach, Wiley-IEEE Press, (2012).
[2] G. Smith, J. Yard, Quantum Communication with Zero-capacity Channels. Science 321, 1812-1815 (2008).
[3] L. Gyongyosi, S. Imre: Algorithmic Superactivation of Asymptotic Quantum Capacity of Zero-Capacity Quantum Channels, Information Sciences, Elsevier, ISSN: 0020-0255; (2011).

Quantum Polar Coding for Probabilistic Quantum Relay Channels

L. Gyongyosi[1] **and S. Imre**[1]
[1]*Quantum Technologies Laboratory, Budapest University of Technology and Economics, Budapest, Hungary*

The superactivation effect originally was intended to use zero-capacity quantum channels for communication [1,2,4]. In this work we firstly demonstrate that the superactivation effect can be exploited for a completely different propose. We will use the superactivation-effect to construct deterministic quantum relay encoders from probabilistic quantum relay encoders. To achieve the private classical capacity of the superactivation-assisted quantum relay channel we construct quantum polar codewords.

In classical communication systems, the relay encoder is an unreliable probabilistic device which is aimed at helping the communication between the sender and the receiver. Here we show that in the quantum setting the probabilistic behavior can be completely eliminated using our superactivation-assisted quantum relay encoder.

The polar coding is a revolutionary channel coding technique, which makes it possible to achieve the symmetric capacity of a noisy communication channel [3]. We also show how to combine the results of quantum polar encoding with superactivation-assistance in order to achieve secure communication over probabilistic quantum relay channels.

Our proposed quantum relay encoder $\mathcal{E}_2$ is depicted in Fig. 1. Alice would like to send her *l*-length private message M to Bob. The first encoder $\mathcal{E}_1$ can encode only phase information, while the quantum relay encoder $\mathcal{E}_2$ can encode only amplitude information.

The quantum relay encoder $\mathcal{E}_2$ can add the amplitude information to the message A received from $\mathcal{E}_1$ only with success probability $0 < p_{\mathcal{E}_2} < 1$. In the first step, her encoder $\mathcal{E}_1$ outputs the *n*-length *phase* encoded message A. The second encoder $\mathcal{E}_2$ gets input on the channel output B', which will be amended with *amplitude* information. The relay quantum encoder $\mathcal{E}_2$ outputs A' to the channel, and Bob will receive message B.

The goal of the whole structure is to help Bob's encoder $\mathcal{D}$, by the quantum relay encoder $\mathcal{E}_2$ to cooperate with $\mathcal{E}_1$, to send the private message M from Alice to Bob. The quantum relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$, which includes Alice's first encoder $\mathcal{E}_1$ and the relay encoder $\mathcal{E}_2$ is defined as $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}} = \mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$, where $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}$ is the quantum channel between encoder $\mathcal{E}_1$ and the quantum relay encoder $\mathcal{E}_2$, while $\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$ is the quantum channel between the quantum relay encoder $\mathcal{E}_2$ and Bob's decoder $\mathcal{D}$.

As we will prove, using *superactivation-assistance* in the relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$, the reliability of $\mathcal{E}_2$ will be $p_{\mathcal{E}_2} = 1$; however, the rate of private communication will be lower.
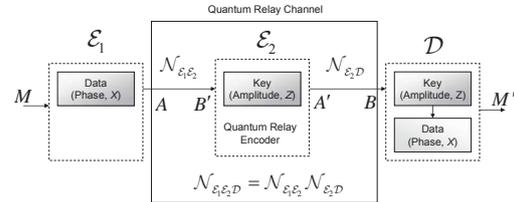
Figure 1. The quantum relay channel with the relay encoder. The first encoder encodes only phase information, the second adds only the amplitude information. The quantum relay encoder is not reliable, it works with success probability $0 < p_{\mathcal{E}_2} < 1$.

The quantum relay encoder $\mathcal{E}_2$ with superactivation-assistance is illustrated in Fig. 2. The joint channel construction $\mathcal{M}_1 \otimes \mathcal{M}_2$ realizes the quantum relay encoder $\mathcal{E}_2$ with $p_{\mathcal{E}_2} = 1$. Using this scheme, the rate of private communication between Alice and Bob can be increased if initially the $p_{\mathcal{E}_2}$ success probability of $\mathcal{E}_2$ was $0 < p_{\mathcal{E}_2} < 0.5$, while the reliability of the quantum relay encoder can be maximized to the $p_{\mathcal{E}_2} = 1$.
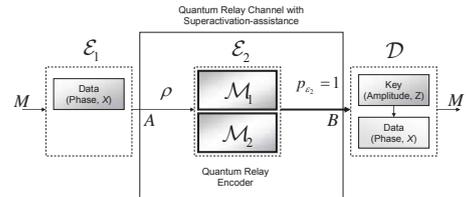
Figure 2. The quantum relay encoder with superactivation-assistance. The rate of private communication can be increased if the initial reliability $p_{\mathcal{E}_2}$ was in $0 < p_{\mathcal{E}_2} < 0.5$. In the joint channel structure the reliability of the quantum relay encoder will be $p_{\mathcal{E}_2} = 1$.

In this work we have shown that by combining the polar coding with superactivation-assistance, the reliability of the quantum relay encoder can be increased and the rate of the private communication over the superactivation-assisted relay quantum channel can be maximized at the same time. The proposed encoding scheme can be a useful tool in quantum cryptographic protocols.

References
[1] S. Imre, L. Gyongyosi: Advanced Quantum Communications: An Engineering Approach, Wiley-IEEE Press, (2012).
[2] G. Smith, J. Yard, Quantum Communication with Zero-capacity Channels. Science 321, 1812-1815 (2008).
[3] E. Arikan. Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels. IEEE Transactions on Information Theory, 55(7):3051–3073, July 2009.
[4] L. Gyongyosi, S. Imre: Algorithmic Superactivation of Asymptotic Quantum Capacity of Zero-Capacity Quantum Channels, Information Sciences, Elsevier, ISSN: 0020-0255; (2011).

Direct evaluation of entanglement in graph states

Michal Hajdušek[1] **and Mio Murao**[1,2]

[1]*Department of Physics, Graduate School of Science, University of Tokyo, 113-0033, Japan*
[2]*Institute for Nano Quantum Information Electronics, University of Tokyo, 153-8505, Japan*

Entanglement quantification in multipartite states is one of the fundamental problems in quantum information theory. Most multipartite entanglement measures are defined using hard optimization over some Hilbert space and are therefore extremely difficult to compute analytically for general states. Examples of states for which this can be done are rare and usually include some form of symmetry that simplifies the problem such as the permutationally symmetric and anti-symmetric states.

We investigate how entanglement can be quantified directly in pure graph states by considering three multipartite measures of entanglement, namely the relative entropy of entanglement E_R, geometric measure E_G and the Schmidt measure E_S. Graph states have an interesting property that for a large number of them the lower and upper bounds for these measures coincide [1, 2]. We explicitly demonstrate how to construct the closest separable state (CSS) ω, the closest product state (CPS) $|\phi\rangle$ and the minimal linear decomposition into product states of a pure graph state $|G\rangle$. We achieve this by mapping the problem of entanglement evaluation in graph states to a single problem in graph theory, namely that of determining the *maximum independent set* $\alpha(G)$ of the corresponding graph G.

Consider a graph state described by stabilizer $\mathcal{S} = \langle g_1, \ldots, g_N \rangle$ generated by N correlation operators

$$g_i := X_i \bigotimes_{j \in N_i} Z_j, \tag{1}$$

where X and Z are Pauli matrices and N_a is the neighborhood of qubit a. Now imagine the scenario of discarding k generators from $\mathcal{S}$. The new stabilizer is given by $\mathcal{S}_{N-k} = \langle g_1, \ldots, g_{N-k} \rangle$ where we have relabeled the remaining generators for convenience. Because we no longer have a full set of N generators $\mathcal{S}_{N-k}$ stabilizes a set of states $\{|\psi_1\rangle, \ldots, |\psi_D\rangle\}$ that span a D-dimensional subspace $\mathcal{H}_A$. The dimensionality of the subspace depends on the structure of the generators $g_i \in \mathcal{S}_{N-k}$ and the states spanning the stabilized subspace may or may not be entangled.

Natural question to ask is what is the most efficient way of discarding generators from $\mathcal{S}$ so that $\mathcal{H}_A$ is spanned by a set of product states $\{|\psi_1\rangle, \ldots, |\psi_D\rangle\}$. Crucial observation needed to answer this question is that when two generators $g_i, g_j \in \mathcal{S}_{N-k}$ act non-trivially on the same qubit and one of them acts with X and the other with Z then the resulting state that they stabilize is entangled. Therefore in order for $\mathcal{S}_{N-k}$ to stabilize a space spanned by product states, it has to contain generators that act on the same qubit either trivially or both with Z or both with X. Therefore $\mathcal{S}_{N-k}$ can only contain generators that act on non-adjacent qubits. Finally in order to make this procedure as efficient as possible we require to discard the smallest possible number of generators or equivalently to make the cardinality of $\mathcal{S}_{N-k}$ as large as possible.

This can be achieved by identifying the maximum independent set $\alpha(G)$ of the underlying graph G. Therefore we only keep generators corresponding to $\alpha(G)$ and discard generators corresponding to the *minimum vertex cover* $\beta(G)$. Note that $|\alpha(G)| + |\beta(G)| = N$.

Now the CSS ω can be easily constructed by summing over all the elements of $\mathcal{S}_\alpha$, the stabilizer corresponding to qubits in $\alpha(G)$, or equally mixing the basis product states of $\mathcal{H}_\alpha$

$$\omega = \frac{1}{2^N} \sum_{\sigma \in \mathcal{S}_{N-k}} \sigma = \frac{1}{D} \sum_{i=1}^{D} |\psi_i\rangle\langle\psi_i|. \tag{2}$$

The relative entropy of entanglement is then easily computed as $E_R(|G\rangle) = \log D$.

The minimal linear decomposition of $|G\rangle$ into product states can be achieved by equal superposition of the basis product states of $\mathcal{H}_\alpha$

$$|G\rangle = \frac{1}{\sqrt{D}} \sum_{i=1}^{D} |\psi_i\rangle. \tag{3}$$

The Schmidt measure can be quickly obtained from this form to be $E_S(|G\rangle) = \log D$.

Finally knowing the minimal decomposition into product states we can see that the CPS is given by any product state from the basis spanning $\mathcal{H}_\alpha$

$$|\phi\rangle = |\psi_i\rangle \qquad \forall i \in \{1, \ldots, D\}. \tag{4}$$

The geometric measure is then given by $E_G(|G\rangle) = \log D$ as $\langle\psi_i|\psi_j\rangle = \delta_{ij}$.

We also present alternative approaches to describing the CSS ω. One such approach uses a construction similar to projected entangled pairs technique [3]. This way we open up the possibility to study entanglement measures in the case of graph related states that do not admit a stabilizer description such as weighted graph states.

Another approach we present investigates how entanglement can be destroyed optimally by introduction of noise. We show that states with the same amount of entanglement are differently susceptible to this noise. We also outline how the entanglement of the system can be partially protected by application of local Clifford unitaries.

References

[1] D. Markham, A. Miyake and S. Virmani, New. J. Phys. **9**, 194 (2007)

[2] M. Hein, J. Eisert and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004)

[3] F. Verstraete and J. I. Cirac, Phys. Rev. A. **70**, 060302(R) (2004)

Absolutely Maximal Entanglement and Quantum Secret Sharing

Wolfram Helwig[1], **Wei Cui**[1], **José Ignacio Latorre**[2], **Arnau Riera**[3,4] **and Hoi-Kwong Lo**[1]

[1]*Center for Quantum Information and Quantum Control (CQIQC), Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*
[2]*Dept. d'Estructura i Constituents de la Matèria, Universitat de Barcelona, 647 Diagonal, 08028 Barcelona, Spain*
[3]*Max Planck Institute for Gravitational Physics, Albert Einstein Institute, Am Mühlenberg 1, D-14476 Golm, Germany*
[4]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*

We study the concept of absolutely maximally entangled (AME) states in quantum mechanics, which are states with genuine multipartite entanglement, characterized by being maximally entangled for all bipartitions of the system. We show how the high degree of entanglement can be used in a novel parallel teleportation protocol, which teleports multiple states between groups of senders and receivers. The notable features of this protocol are that the partition into senders and receivers can be chosen after the state has been distributed, and one group has to perform joint quantum operations, while the parties of the other group only have to act locally on their system. Further investigation of these features leads us to discovering the remarkable equivalence of pure state quantum secret sharing schemes and AME states shared between an even number of parties. This equivalence also allows us to prove the existence of AME states for an arbitrary number of parties due to known results about the existence of quantum secret sharing schemes.

Nonlocality as a Benchmark for Universal Quantum Computation in Ising Anyon Topological Quantum Computers

Mark Howard[1], **Jiri Vala**[1,2]

[1]*Department of Mathematical Physics, National University of Ireland, Maynooth, Ireland*
[2]*Dublin Institute for Advanced Studies, School of Theoretical Physics, 10 Burlington Road, Dublin, Ireland*

An obstacle affecting any proposal for a topological quantum computer based on Ising anyons is that quasiparticle braiding can only implement a finite (non-universal) set of quantum operations. The computational power of this restricted set of operations (often called stabilizer operations) has been studied in quantum information theory, and it is known that no quantum-computational advantage can be obtained without the help of an additional non-stabilizer operation.

Similarly, a bipartite two-qubit system based on Ising anyons cannot exhibit non-locality (in the sense of violating a Bell inequality) when only topologically protected stabilizer operations are performed. To produce correlations that cannot be described by a local hidden variable model again requires the use of a non-stabilizer operation.

Using geometric techniques, we relate the sets of single-qubit operations that enable universal quantum computing (UQC) with those that enable violation of a Bell inequality. Motivated by the fact that non-stabilizer operations are expected to be highly imperfect, our aim is to provide a benchmark for identifying UQC-enabling operations that is both experimentally practical and conceptually simple. We show that any (noisy) single-qubit non-stabilizer operation that, together with perfect stabilizer operations, enables violation of the simplest two-qubit Bell inequality can also be used to enable UQC. This benchmarking requires finding the expectation values of two distinct Pauli measurements on each qubit of a bipartite system.

References

[1] M. Howard and J. Vala, Nonlocality as a benchmark for universal quantum computation in Ising anyon topological quantum computers, Physical Review A **85** 022304 (2012).
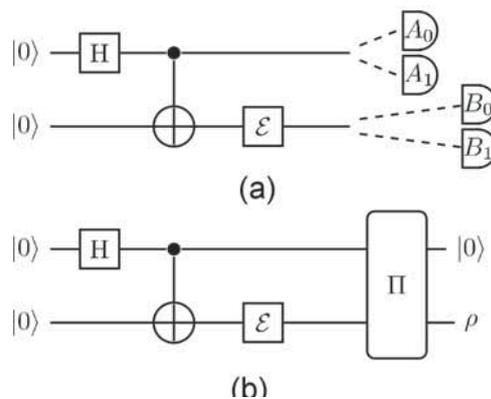
Figure 1: **Using a non-stabilizer operation, $\mathcal{E}$, to achieve a non-classical task**

(a) A simple set-up to detect nonlocality: Here, two possible measurement settings for the first (second) qubit are denoted A_i (B_j). When A_i and B_j are constrained to be Pauli operators, then $\mathcal{E}$ must be a non-stabilizer operation if any Bell inequality (e.g., a CHSH inequality of the form $\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2$) is to be violated.

(b) A circuit to help achieve universal quantum computation via magic state distillation: Every element of this circuit except $\mathcal{E}$ is implementable using stabilizer operations. When $\mathcal{E}$ exhibits nonlocality in the setup of subfigure 1(a), then $\mathcal{E}$ used in the circuit of 1(b) produces ancillas ρ that are useful for a magic state distillation subroutine (MSD circuit not depicted). The block containing Π stands for a two-qubit Pauli measurement (e.g. parity measurement) wherein we postselect on the desired outcome.

Randomizing quantum states in Shatten p-norms

Kabgyun Jeong

[1]*Korea Institute for Advanced Study, Seoul, Korea*

Randomizing quantum states in Quantum Information Theory has many applications in quantum communications such as super-dense coding [1], data hiding [2] and proof of the additivity violation for the classical capacity on quantum channels [3]. Following Hayden, Leung, Shor and Winter's result [2] and Dickinson and Nayak's [4], we would like to make a special formula for the randomization of all quantum states. In this study, actually we formularize a method for randomizing quantum states with respect to the Shatten p-norms in trace class [5].

Preliminaries Let $\mathcal{B}(\mathbf{C}^d)$ be the space of (bounded) linear operators and $\mathcal{U}(d) \subset \mathcal{B}(\mathbf{C}^d)$ the unitary group on the d dimensional Hilbert space $\mathbf{C}^d$, and $\mathbf{I}$ stands for the $d \times d$ identity operator on the space. Let $\mathcal{P}(\mathbf{C}^d)$ denote the set of all pure states i.e., unit vectors on $\mathbf{C}^d$. The Shatten p-norm can be described in trace class by $\|A\|_p = \left(tr(A^\dagger A)^{p/2}\right)^{1/p}$ for any matrix A.

Now, let's define an ϵ-randomizing maps with respect to the Shatten p-norm: A completely positive and trace-preserving map $\mathcal{R} : \mathcal{B}(\mathbf{C}^d) \to \mathcal{B}(\mathbf{C}^d)$ is *ϵ-randomizing* with respect to the Shatten p-norm $\|\cdot\|_p$ if, for all states $\rho \in \mathcal{B}(\mathbf{C}^d)$,

$$\left\| \mathcal{R}(\rho) - \frac{\mathbf{I}}{d} \right\|_p \leq \frac{\epsilon}{\sqrt[p]{d^{p-1}}}. \tag{1}$$

If ϵ is equal to zero, the map $\mathcal{R}$ is called by completely randomizing map. Above definition of ϵ-randomizing map is well defined for some special cases p. Since, for the map $\mathcal{R}$ with respect to the trace norm, the ϵ-randomizing map is defined by the condition $\|\mathcal{R}(\rho) - \mathbf{I}/d\|_1 \leq \epsilon$. Similarly, for $p = \infty$ case, the condition is naturally defined as $\|\mathcal{R}(\rho) - \mathbf{I}/d\|_\infty \leq \epsilon/d$.

Main result We are interesting to approximating the randomizing map $\mathcal{R}$ by mapping with small cardinality of unitary operators, and reproducing the known two results [2, 4] exactly. Next statement is our *main theorem*.

Let φ be a pure state in $\mathcal{P}(\mathbf{C}^d)$, and μ be the Haar measure on the unitary group $\mathcal{U}(d)$. For all $\epsilon \geq 0$ and sufficiently large d, there exists a choice of unitaries in $\mathcal{U}(d)$, $\{U_i | 1 \leq i \leq m\}$ with $m \geq \frac{c_p \cdot d}{\epsilon^2} \log\left(\frac{10d^{(p-1)/p}}{\epsilon}\right)$, which is independent μ-distributed random matrices, such that the map

$$\mathcal{R}(\varphi) = \frac{1}{m} \sum_{i=1}^{m} U_i \varphi U_i^\dagger \tag{2}$$

on $\mathcal{B}(\mathbf{C}^d)$ is ϵ-randomizing with respect to the Shatten p-norms for all $p \geq 1$ with probability at least $1 - e^{-m}$, and c_p is an absolute constant.

Let c_1 and c_∞ be absolute constants. Notice that if $p = 1$, the map $\mathcal{R}$ is ϵ-randomizing with respect to the trace norm with the cardinality $m = \mathcal{O}\left(\frac{c_1 \cdot d}{\epsilon^2} \log\left(\frac{10}{\epsilon}\right)\right)$ in Ref. [4]. If $p = \infty$, then $m = \mathcal{O}\left(\frac{c_\infty \cdot d}{\epsilon^2} \log\left(\frac{10d}{\epsilon}\right)\right)$ in Ref. [2]. See the proof of above theorem in Ref. [5]. The scheme of main proof is similar to the References [2, 4]. For the proof, we make use of two key-lemmas known as McDiarmid's inequality [6] and η-net argument. The first one is a large deviation estimates and the second is a method for discretization of all pure quantum states.

In conclusion, we can obtain a formula for randomizing quantum states with respect to the Shatten p-norms on d dimensional Hilbert space. That is, there exists a choice of unitary operators in $\mathcal{U}(d)$ selected according to the Haar measure, $\{U_i\}_{i=1}^{m}$ with $m = \mathcal{O}(d \log(d^{(p-1)/p}/\epsilon)/\epsilon^2)$ such that the completely positive and trace-preserving map $\mathcal{R}(\varphi) = \frac{1}{m} \sum_{i=1}^{m} U_i \varphi U_i^\dagger$ on $\mathcal{B}(\mathbf{C}^d)$ is ϵ-randomizing with respect to the p-norm with high probability.

References

[1] A. Harrow, P. Hayden, and D. Leung, Phys. Rev. Lett. **92**, 187901 (2004).

[2] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Commun. Math. Phys. **250**, 371–391 (2004).

[3] M. B. Hastings, Nature Physics **5**, 255–257 (2009).

[4] P. Dickinson and A. Nayak, In AIP Conference Proceedings **864**, 18–36 (2006).

[5] K. Jeong, The manuscript was submitted to J. Math. Phys. (2012).

[6] C. McDiarmid, Surveys in Combinatorics **141**, 148–188 (1989).

Minimax Discrimination of Quasi-Bell States

Kentaro Kato[1]

[1]*Quantum ICT Research Institute, Tamagawa University, Tokyo, JAPAN*

It is well-known that nonorthogonal quantum states can not be distinguished without error [1]. Therefore, optimization of quantum measurement for nonorthogonal states is one of key problems in quantum information processing. It is also well-known that quantum entanglement and its unique features make it possible to produce new functions such as teleportation [2]. In this study, we are interested in an optimal measurement process for particular entangled states called quasi-Bell states.

The quasi-Bell states based on entangled coherent states of light are defined as follows [3]:

$$|H_1\rangle = h_1\Big[|\alpha\rangle_1|-\alpha\rangle_2 + |-\alpha\rangle_1|\alpha\rangle_2\Big], \quad (1)$$

$$|H_2\rangle = h_2\Big[|\alpha\rangle_1|-\alpha\rangle_2 - |-\alpha\rangle_1|\alpha\rangle_2\Big], \quad (2)$$

$$|H_3\rangle = h_3\Big[|\alpha\rangle_1|\alpha\rangle_2 + |-\alpha\rangle_1|-\alpha\rangle_2\Big], \quad (3)$$

$$|H_4\rangle = h_4\Big[|\alpha\rangle_1|\alpha\rangle_2 - |-\alpha\rangle_1|-\alpha\rangle_2\Big], \quad (4)$$

where the normalizing constants are respectively given by $h_1 = h_3 = 1/\sqrt{2(1+\kappa^2)}$ and $h_2 = h_4 = 1/\sqrt{2(1-\kappa^2)}$, and where $\kappa = \langle\alpha|-\alpha\rangle$. Then the Gram matrix of the quasi-Bell states is given as

$$G = \begin{bmatrix} 1 & 0 & D & 0 \\ 0 & 1 & 0 & 0 \\ D & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

where $D = 2\kappa/(1+\kappa^2)$. Thus, the set of the states contains a nonorthogonal pair, $|H_1\rangle$ and $|H_3\rangle$. Our problem is to design an optimal measurement for these four states. If *a priori* probabilities of the states are given, one can employ quantum Bayes strategy that minimizes the average probability of detection error [4]. However, one might not be able to or not need to specify the probabilities if it is convenient. So, we assume that the probabilities of the states are unknown to the designer. In this scenario, the designer must employ quantum minimax strategy, instead of the Bayes strategy. The necessary and sufficient conditions for the minimax strategy of a finite number of decisions were first studied by Hirota and Ikehara [5]. In order to design the minimax measurement for the quasi-Bell states above, we will show a simple extension of their result. Using this extended version of the necessary and sufficient conditions, it will be shown that the square-root measurement for the quasi-Bell states is an optimal measurement in terms of the quantum minimax strategy. In addition, we attempt to apply the minimax measurement to teleportation scheme that uses a quasi-Bell state as a resource [6, 7, 8]. Through this application, we will discuss the relationship between quantum detection theory and teleportation.

References

[1] C. W. Helstrom, Quantum Detection and Estimation Theory (Academic Press, New York, 1976).

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[3] O. Hirota, S. J. van Enk, K. Nakamura, M. Sohma and K. Kato, arXiv:quant-ph/0101096v1 (2001).

[4] A. S. Holevo, J. Multivar. Analys. **3**, 337 (1973).

[5] O. Hirota and S. Ikehara, Trans. IECE of Japan **E65**, 627 (1982).

[6] S. J. van Enk and O. Hirota, Phys. Rev. A **64**, 022313 (2001).

[7] H. Jeong, M. S. Kim and J. Lee, Phys. Rev. A **64**, 052308 (2001).

[8] H. Prakash and M. K Mishra, arXiv:1107.2533v1 (2011).

Quantum walk computation

Viv Kendon[1]

[1] *School of Physics and Astronomy, University of Leeds, LS2 9JT, United Kingdom*

Quantum versions of random walks have diverse applications that are motivating experimental implementations as well as theoretical studies. However, the main impetus behind this interest is their use in quantum algorithms, which have always employed the quantum walk in the form of a program running on a quantum computer. Like random walks in classical computation, these have the position stored as a binary number labelling the vertex, an exponentially more efficient representation than a physical quantum walk. Recent results [1, 2] showing that quantum walks are "universal for quantum computation" relate entirely to algorithms, and do not imply that a physical quantum walk could provide a new architecture for quantum computers.

Quantum versions of random walks were introduced in the late 80s. In the simplest setting of a line or a Cartesian lattice, on which the walker hops between integer sites, a quantum walk spreads quadratically faster than a classical random walk, see figure 1. This provides the speed up in
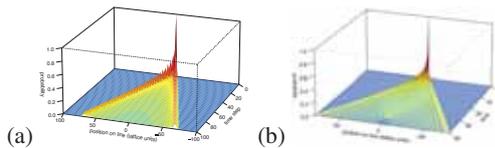
Figure 1: Probability distribution evolving in time for (a) a discrete-time quantum walk, and (b) a continuous-time quantum walk on the line. Linear spreading is clearly seen in both.

many quantum walk algorithms, e.g., searching. Exponential speed up has been proved for transport: crossing a hypercube or a particular "glued trees" graph exponentially faster. Quantum walks provide useful models of physical phenomena such as spin chains or energy transport in biomolecules. Certain combinations of parameters can achieve perfect quantum state transfer (reviewed in [3]), of interest for building quantum wires in quantum computers. Highly efficient transport can be obtained by using imperfect quantum walks where the amount of decoherence is tuned to optimize the quantum walk properties [4].

For experiments that could perform useful computation, we should compare with classical computational capabilities. Classically, as with any full simulation of a quantum system, it is necessary to store and manipulate all of the complex amplitudes describing the wavefunction. Each amplitude requires two floating point numbers (real and imaginary parts). Using 32 bits (4 bytes) for each floating point number, we can store 2^{27} amplitudes in 1 Gbyte of memory. A quantum walk on the line of a million steps, needing 22 qubits in a quantum computer, can be described by 2^{22} amplitudes, which requires about 4 Mbyte of memory, and this computation is quick and easy on a desktop computer. Single quantum walkers, even with decoherence, can be efficiently simulated on classical computers for many more steps than current experiments can

achieve, due to the efficiency gained by binary encoding of the position labels, and limited experimental coherence times.

Quantum walks with multiple walkers extend the paradigm beyond the standard algorithmic applications. If the walkers are distinguishable and don't interact, the classical simulation can still be done efficiently, it is given by the solution for a single walker. Interacting quantum walkers are a special case of quantum cellular automata [5], known to be universal for quantum computation. They are particularly suited to optical lattice implementations [6]. The Hilbert space now grows exponentially, for m walkers on L locations, the full Hilbert space is of size L^m. Classical simulation of such interacting walkers can only be done for a few walkers and locations: six walkers on eight locations is already close to the limit.

Indistinguishable but non-interacting bosons can have intermediate computational power [7]. However, multiple non-interacting bosonic walkers starting from a single location do not generate a hard instance of the "boson sampling problem". While they will be interesting experiments, requiring accurate photon counting detectors, the classical computations to verify the results will be tractable for current experimental capabilities [8].

References

[1] A. M. Childs, Universal computation by quantum walk, Phys. Rev. Lett. **102**, 180,501 (2009).

[2] N. B. Lovett, S. Cooper, M. Everitt, M. Trevers, and V. Kendon, Universal quantum computation using the discrete time quantum walk, Phys. Rev. A **81**, 042330 (2010).

[3] V. M. Kendon and C. Tamon, Perfect state transfer in quantum walks on graphs, J. Comp. Theor. Nanoscience **8**, 422–433 (2010).

[4] V. Kendon and B. Tregenna, Decoherence can be useful in quantum walks, Phys. Rev. A **67**, 042,315 (2003).

[5] K. Wiesner, Quantum Cellular Automata, in Springer Encyclopedia of Complexity and System Science, , A. Adamatzky, ed. (Springer, 2009).

[6] A. Ahlbrecht, A. Alberti, D. Meschede, V. B. Scholz, A. H. Werner, and R. F. Werner, Bound molecules in an interacting quantum walk, (2011). Arχiv:1105.1051v1[quant-ph].

[7] S. Aaronson and A. Arkhipov The computational complexity of linear optics Arχiv:1011.3245v1[quant-ph].

[8] V. Kendon, Where to quantum walk, (2011). Arχiv:1107.3795v1[quant-ph].

Quantum Annealing in Hopfield Model

Sergey Knysh[1] and **Vadim N. Smelyanskiy**[2]

[1]*Mission Critical Technologies, NASA Ames Research Center, Moffett Field, CA 94035, USA*
[2]*NASA Ames Research Center, Mofferr Field, CA 94035*

It has been suggested that quantum adiabatic algorithm (QAA) [1] based on the idea of quantum annealing [2] would outperform its classical counterpart — simulated annealing. The implementation uses quantum spins with Ising interactionss subjected an external transverse magnetic field Γ that varies from a very large value to zero.

$$\hat{H} = -\frac{1}{2} \sum_{i \neq k} J_{i,k} \hat{\sigma}_i^z \hat{\sigma}_k^z - \sum_i h_i \hat{\sigma}_i^z - \Gamma \sum_i \hat{\sigma}_i^x. \quad (1)$$

At the end of the algorithm the system is found in a state that minimizes the interaction term provided that one starts from the ground state at large Γ (easily prepared symmetric superposition of all spin configurations) and proceeds at sufficiently slow rate so as to satisfy the adiabatic theorem. The performance of the algorithm is determined by the smallest value of the energy gap between the ground state and the first excited state.

We investigate the performance of QAA for Hopfield model of neural network theory [3, 4], where $h_i = 0$ and

$$J_{i,k} = \sum_{\alpha=1}^p \xi_i^{(\alpha)} \xi_k^{(\alpha)} \quad (2)$$

with $\{\xi_i^{(\alpha)}\}_i$ representing "patterns" to be recalled. We assume that patterns are Gaussian-distrbuted in contrast to customary choice $\xi_i^{(\alpha)} = \pm 1$. Corresponding model has rich structure for as few as $p = 2$ patterns which is the example we consider, although our analysis can be generalized to any finite number $p \ll N$.

Whereas earlier work [5] on quantum Hopfield model investigated only static properties in the thermodynamic limit, we study the spectrum of low energy excitations for large but finite value of N. For the Gaussian Hopfield model, the extensive part of the free energy is given by the minimum of the effective potential

$$V(\vec{m}) = \frac{N}{2} \vec{m}^2 - \frac{N\Gamma}{\pi\sqrt{2}} \sqrt{z} e^z \left[K_0(z) + K_1(z) \right], \quad (3)$$

where $z = \Gamma^2/4\vec{m}^2$ and $\vec{m}$ is the order parameter (a p-dimensional vector).

$\Gamma_c = 1$ is the quantum critical point below which the order paramater acquires non-zero value (see Fig. 1). The gap for $\Gamma > \Gamma_c$ and the singular component of the free energy scale as $\sqrt{\Gamma - \Gamma_c}$ and $(\Gamma - \Gamma_c)^2$ respectively. Using hyperscaling relations, gap at criticality is conjectured to scale as $N^{-1/3}$.

Low-energy excitations in the spin-glass phase $(\Gamma < \Gamma_c)$ are the Goldstone modes of the broken continuous rotational symmetry. Disorder realization–dependent $O\left(\sqrt{N}\right)$ corrections to the effective potential become relevant in this regime as they are not invariant with respect to rotations. It is shown
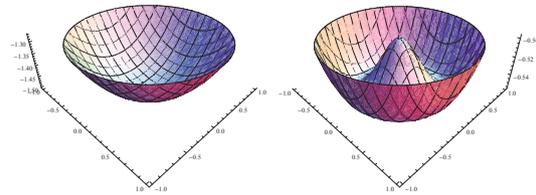
Figure 1: Effective potential above (left: $\Gamma = 1.5$) and below (right: $\Gamma = 0.5$) the phase transition.

that the low-energy spectrum is equivalent to that of quantum-mechanical particle on a ring moving in random potential which allows to study the spectrum of many-body system rigorously. We corroborate the above-mentioned scaling of the gap at $\Gamma = \Gamma_c$. For $\Gamma < \Gamma_c$ the gap to the first excited state scales as $\exp\left(-cN^{3/4}/\Gamma\right)$ and the typical value of the gap to the second excited state is $\sim \Gamma N^{-1/4}$. The latter is more relevant for QAA since non-adiabatic transitions to first excited state are not allowed due to global spin-inversion symmetry.

Although the typical gap for fixed Γ is polynomial, this leaves open a possibility that exponentially small gaps occur during the evolution of the effective potential with Γ as its landscape becomes increasingly more rugged. We investigate the probability of global bifurcation events for $\Gamma < 1$. It is related to the properties of positive Langevin process to which the effective potential converges as $\Gamma \to 0$. The implicit cutoff is at $\Gamma \sim 1/N^{1/4}$ where discreteness of the model comes into effect as the wavefunction becomes localized.

References

[1] E. Farhi, J. Goldstone, S. Gutman, J. Lapan, A. Lundgren and D. Preda, A Quantum Adiabatic Evolution Algorithm Applied to Random Instances of NP-complete Problem, Science **292**, 472 (2001).

[2] T. Kadowaki, H. Nishimori, Quantum Annealing in the Tranverse Ising Model, Phys. Rev. E **58**, 5335 (1998).

[3] J. J. Hopfield, Neural Networks and Physical Systems with Emergent Collective Computational Properties, Proc. Nat. Acad. Sci. **79**, 2554 (1982).

[4] R. Neigoven, J. Neves, R. Sollacher and S. J. Glaser, Quantum Pattern Recognition with Liquid State NMR, Phys. Rev. A **79**, 042321 (2009).

[5] H. Nishimori and Y. Nonomura, Quantum Effects in Neural Networks, J. Phys. Soc. Jpn **65**, 3780 (1996); M. Scherbina and B. Tirozzi, Quantum Hopfield Model, arXiv:1201.5024 (2012).

Hybrid quantum repeater with encoding

Nadja K. Bernardes[1,2] **and Peter van Loock**[1,2]

[1]*Optical Quantum Information Theory Group, Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1/Bau 24, 91058 Erlangen, Germany*
[2]*Institute of Theoretical Physics I, Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany*

The main idea of this work is to apply quantum error correction (QEC) to a hybrid quantum repeater (HQR) aiming to improve the scheme against practical limitations such as imperfect generation of the entangled state, finite memory decoherence times, and imperfect two-qubit operations [1]. More specifically, the QEC codes under consideration here are the well-known qubit-repetition codes and Calderbank-Shor-Steane (CSS) codes. Due to their transversality property, entanglement connection and error correction can be performed with the same set of operations [2]. Our treatment is not restricted to analyze the in-principle performance of QEC codes for the hybrid quantum repeater, but it also shows how to actually implement an encoded HQR.

We analyze the scheme for a quantum repeater based on atomic qubit-entanglement distribution through optical coherent-state communication [3]. In particular we consider nonlocal distributions of two-qubit entangled memory pairs based on unambiguous state discrimination (USD) measurements of coherent states [4]. This scheme provides a clear relation between the probability of success P_0 of entanglement generation and the fidelity F of the entangled state:

$$P_0 = 1 - (2F - 1)^{\eta/(1-\eta)}. \tag{1}$$

Photon losses are considered to be the main source of error in the entanglement distribution and they will be described as a beam splitter with transmissivity η.

Our error models are defined as follows:

1. Imperfect generation of the entangled state. The initial conditionally prepared entangled state has the following form:

$$F|\phi^+\rangle\langle\phi^+| + (1 - F)|\phi^-\rangle\langle\phi^-|, \tag{2}$$

where $|\phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$.

2. Errors in the CNOT gates. Dissipation on quantum gates in our scheme will act in a two-qubit unitary operation U_{ij} as

$$U_{ij}\rho U_{ij}^\dagger \rightarrow U_{ij}\left[(1 - q_g)^2\rho + q_g(1 - q_g)\times \right. \tag{3}$$
$$\left. (Z_i\rho Z_i + X_j\rho X_j) + q_g^2 Z_i X_j \rho X_j Z_i\right]U_{ij}^\dagger.$$

3.Imperfect memories. The errors resulting from the imperfect memories are similarly described by a dephasing model, such that the qubit state ρ_A of memory A will be mapped, after a decaying time t, to

$$\Gamma_t^A(\rho_A) = (1 - q_m(t/2))\rho_A + q_m(t/2)Z\rho_A Z, \tag{4}$$

where $q_m(t) = (1 - e^{-t/\tau_c})/2$ and τ_c is the memory decoherence time.

We shall encode our entangled pair in a qubit-repetition code and in a CSS code. The advantage of these codes is that, due to their resemblance with classical codes, the logical operations can simply be understood as the corresponding operations applied upon each physical qubit individually. This permits doing the entanglement connection (swapping) between different repeater stations and the syndrome measurements (for error identification) at the same time, such that the swappings can be all executed simultaneously [2]. The correction operations will then be performed only on the initial and the final qubits of the whole protocol. The encoded quantum repeater protocol then operates much faster than the non-encoded scheme, and, as a result, still performs well even for rather short memory decoherence times.

Moreover, assuming sufficiently many initial resources, we calculate the entangled-pair distribution rate and we clearly identify a triple trade-off between the efficiency of the codes, the memory decoherence time, and the local gate errors. Finally, we show that in the presence of imperfections our system can achieve reasonable rates with high final fidelities, as an example, see Fig. 1.
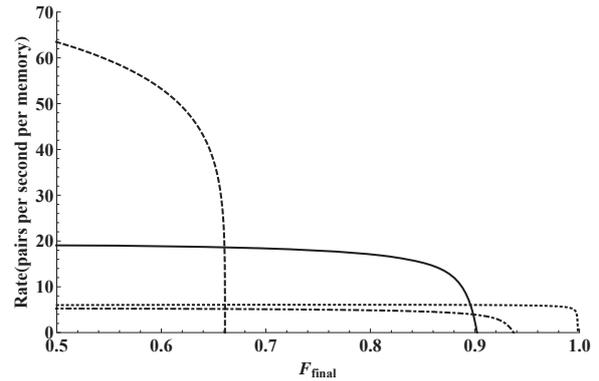
Figure 1: Rates for a HQR with encoding with two rounds of purification in the first nesting level with the parameters $L = 1280$ km, $L_0 = 20$ km, $\tau_c = 0.1$ s and $q_g = 0.1\%$. Dashed line is for the $[3, 1, 3]$ (repetition) code, solid line for $[7, 1, 3]$ (Steane), dashed line for the $[23, 1, 7]$ (Golay), and dot-dashed line for the $[25, 1, 5]$ (Bacon-Shor).

References

[1] N. K. Bernardes and P. van Loock, arXiv:1105.3566 (2011).

[2] L. Jiang *et al.*, Phys. Rev. A **79**, 032325 (2009).

[3] P. van Loock *et al.*, Phys. Rev. Lett. **96**, 240501 (2006).

[4] P. van Loock *et al.*, Phys. Rev. A **78**, 062319 (2008).

Adversarial entanglement verification without shared reference frames

Thomas Lawson[1], **Anna Pappa**[1], **Damian Markham**[1], **Iordanis Kerenidis**[2] and **Eleni Diamanti**[1]

[1]*LTCI, CNRS – Télécom ParisTech, Paris, France*
[2]*LIAFA, CNRS – Université Paris 7, Paris, France*

An interesting and important question in quantum information science is how best to verify entanglement. This is an essential process in many applications of quantum theory, as well as being of fundamental interest.

Typically, a verification protocol requires an established reference frame and cooperation between the verifiers, Alice and Bob. Here we address the problem of verifying entanglement in a misaligned reference frame. Such a situation may arise in quantum protocols requiring unacquainted parties to share entanglement, especially over large distances where alignment, which can only be perfectly achieved with infinite communication, is not feasible.

Furthermore, this invariance under rotation can be used to improve the security of a verification scheme, allowing Alice to guarantee entanglement even if she does not trust Bob, as in a steering inequality [1].

We propose a verification protocol that does not require a common reference frame and resides in the second level of the security hierarchy: *separability*; *steerability*; *nonlocality*; introduced in [2].

Consider the situation where Alice and Bob share no common frame of reference, as in [3, 4]. In this context Alice and Bob can verify entanglement by monitoring various quantities that are independent of local rotation. We will call these quantities *reference frame independent* (*rfi*), a term introduced in [5]. The protocol requires Alice and Bob to perform well defined (but arbitrarily rotated) operations. Several *rfi* expressions are found when Alice and Bob sample from the rotated orthogonal measurement triad (composed of the Pauli operators), $\sigma_{x'}, \sigma_{y'}, \sigma_{z'}$, where the *prime* signifies arbitrary rotation.

$$\langle\sigma_{x'}\sigma_{x'}\rangle^2 + \langle\sigma_{x'}\sigma_{y'}\rangle^2 + \langle\sigma_{x'}\sigma_{z'}\rangle^2, \quad (1)$$

$$\langle\sigma_{y'}\sigma_{x'}\rangle^2 + \langle\sigma_{y'}\sigma_{y'}\rangle^2 + \langle\sigma_{y'}\sigma_{z'}\rangle^2, \quad (2)$$

$$\langle\sigma_{z'}\sigma_{x'}\rangle^2 + \langle\sigma_{z'}\sigma_{y'}\rangle^2 + \langle\sigma_{z'}\sigma_{z'}\rangle^2. \quad (3)$$

When the measurements are made on a maximally entangled state each of the quantities above is equal to 1, independent of local rotation. However, for a separable state the sum of all *nine* terms is 1.

Note that the expressions (1), (2), (3) are just three of many *rfi* quantities *arising from such measurements*. We have developed a simple method for identifying the most obvious among those.

Furthermore, we have extended this analysis to more measurement bases – provided these bases are distributed appropriately – and multipartite systems.

Quantum steering has led to a model of entanglement verification when one party is untrusted, see [1] and references therein. In [2] a hierarchy is established: *separability*; *steerability*; *nonlocality*, according to the degree of trust required for one party to test entanglement.

We demonstrate an *rfi* entanglement verification protocol which falls into the *steerability* security category.

The building block of the scheme is the following *rfi* expression, based on the observations (1), (2), (3),

$$\begin{aligned} Q := &|1 - \left(\langle\sigma_{x'}\sigma_{x'}\rangle^2 + \langle\sigma_{x'}\sigma_{y'}\rangle^2 + \langle\sigma_{x'}\sigma_{z'}\rangle^2\right)| \\ &+|1 - \left(\langle\sigma_{y'}\sigma_{x'}\rangle^2 + \langle\sigma_{y'}\sigma_{y'}\rangle^2 + \langle\sigma_{y'}\sigma_{z'}\rangle^2\right)| \\ &+|1 - \left(\langle\sigma_{z'}\sigma_{x'}\rangle^2 + \langle\sigma_{z'}\sigma_{y'}\rangle^2 + \langle\sigma_{z'}\sigma_{z'}\rangle^2\right)|. \quad (4) \end{aligned}$$

This is equal to 0 for measurements on a maximally entangled state and 2 for a separable state. By monitoring several such quantities Alice can perform entanglement verification without trusting Bob.

Explicitly we show that Bob, who is in possession of the particle source, cannot fake entanglement by sending Alice single qubit states. As in all such tests, it is essential that Bob not be able to correlate his measurement bases with the source. To ensure this Alice specifies Bob's measurement (up to a global rotation which is chosen by him). Bob then replies with his measurement result. Alice can now check for entanglement by monitoring expressions such as (4).

In practice there exist cheating strategies for Bob whenever imperfect detection equipment is used. Existing steering protocols demand that Bob make measurements from an improved set of bases to overcome this. To a certain extent this is possible in our scheme. Bob chooses from several bases distributed to give reference frame independence. However, counter-intuitively, not all *rfi* bases are appropriate for this.

This protocol has obvious advantages whenever reference frame alignment is not available. Furthermore, it provides an additional level of security not found in previous verification protocols as Alice is never obliged to reveal her measurement bases.

References

[1] D. J. Saunders, S. J. Jones, H. M. Wiseman and G. J. Pryde, Nature Physics **7**, 918 (2011).

[2] H. M. Wiseman, S. J. Jones and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

[3] S. D. Bartlett, T. Rudolph and R. W. Spekkens, Rev. Mod. Phys. **79**, 555–609 (2007).

[4] P. Shadbolt, T. Vertesi, Y.-C. Liang, C. Branciard, N. Brunner and J. L. O'Brien *quant-ph/*1111.1853 (2011).

[5] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, Phys. Rev. A **82**, 012304 (2010).

Cat–state entanglement distribution with inefficient detectors

A. P. Lund[1], **T. C. Ralph**[1] **and H. Jeong**[2]

[1]*Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics,*
The University of Queensland, St Lucia, Queensland 4072 Australia.
[2]*Center for Macroscopic Quantum Control and Department of Physics and Astronomy,*
Seoul National University, Seoul 151-747, Korea

We present a scheme for generating cat–state entanglement whose output fidelity with an ideal entangled state is insensitive to loss in the detectors which perform the post-selection. We compare our scheme to a similar scheme [1] which has been previously demonstrated and show that it has superior performance for reasonable experimental conditions and sufficiently large coherent state encoding amplitude.

Here we define cat states to be superpositions of two coherent states, chosen to be of equal amplitude and opposite phase (i.e. (i.e. $|\alpha\rangle + |-\alpha\rangle$). It is possible to use these two coherent states as a qubit encoding basis [2, 3] giving an alternative encoding for optical quantum information. This basis can be used for fault tolerant quantum computing even if the two coherent states have an non-negligible overlap [5]. This choice has some advantages but it is experimentally challenging to perform some simple operations such as single qubit rotations. However, recent experiments have made significant advances in overcoming these difficulties [4].

Reference [1] proposes and implements a method for generating distributed entanglement in this encoding. The method starts with two parties generating equal superposition states both with an encoding amplitude α. Then each party uses a beam-splitter to tap off a small fraction of energy ϵ from their cat state and send it to a central location. There is a total loss of η between the two parties and it is assumed that this is distributed evenly between the central location and the two parties. At the central location the two low energy parts are received then interfered on a $50 : 50$ beam-splitter. Entanglement generation between the two parties is heralded by detection of a click at one of the outputs from the beam-splitter in the central locations. Local corrections are applied depending on the detection outcome.

As the energy distributed is small the chance of loosing a quanta of energy is also small. For each quanta of energy lost a sign flip error is introduced. However, the probability of getting the heralding click is, consequently, also small. This scheme also suffers from loss in the detector by the same mechanism. Detector losses can be a roadblock to implementing scaled-up protocols [6].

Our proposed scheme is resilient to loss within the detectors. The scheme utilises the result from [7]. Our scheme is still sensitive to loss in the channel. In our proposed scheme, the two parties generate superposition states as before but of different amplitude as the protocol is asymmetric between the two parties. One party is the sender and they generate a cat-state state of amplitude α and send a proportion ϵ along the lossy channel η to the receiving party. The receiving party then combines the small received amplitude with a cat-state state of amplitude $\sqrt{\rho}\alpha$ with $\rho = 1 - 2\epsilon + \epsilon\eta$ on a beam-splitter with reflectivity $\rho/(1 - \epsilon)$. The entanglement is heralded by taking one of the output modes of the beam-splitter

on the receiving end and mixing that with a coherent state of amplitude γ where $\gamma = 2\alpha/\sqrt{1/\rho + 1/(\eta(1 - \epsilon))}$. The entanglement is heralded by detecting two simultaneous clicks (of any number of photons) from the two outputs from this final beam-splitter with detector losses of l.

The fidelity of generation and probability of success for the two schemes is plotted in Figure 1 with reasonable assumptions about the loss rates. We find that within the proposed scheme there exists a region for larger α where the performance is superior to that of [1] even when taking account of the lower probability of success.
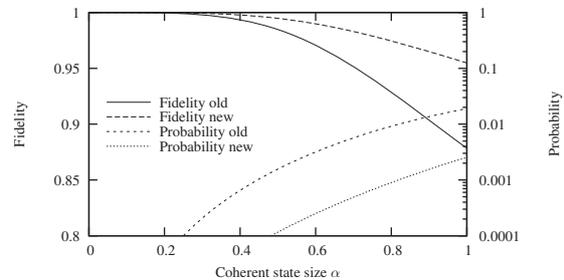
Figure 1: Fidelity (top curves, LHS axis) and probability of success (bottom curves, RHS axis) as a function of the encoding coherent state amplitude α. Assumed parameters are (see text) $\epsilon = 0.1$, $\eta = 0.5$, $l = 0.1$.

References

[1] A. Ourjoumtsev, F. Ferreyrol, R. Tualle-Brouri, and P. Grangier, *Nature Physics* **5** 189–192 (2009).

[2] H. Jeong and M. S. Kim, *Phys. Rev. A* **65** 042305 (2002).

[3] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, S. Glancy, *Phys. Rev. A* **68**, (2003).

[4] J. S. Neergaard-Nielsen, *et al.*, *Phys. Rev. Lett.* **105**, 053602 (2010).

[5] A. P. Lund, T. C. Ralph, H. L. Haselgrove, Phys. Rev. Lett. **100**, 030503 (2008).

[6] N. Sangouard, *et al.*, *J. Opt. Soc. Am. B* **27**, A137-A145 (2010).

[7] A. P. Lund, H. Jeong, T. C. Ralph, M. S. Kim, *Phys. Rev. A* **70**, 020101 (2004).

Noiseless amplification of information

Petr Marek[1] and Radim Filip[1]

[1]*Palacký University, Olomouc, Czech Republic*

Quantum physics has many peculiar properties which make lives of quantum physicists both harder and more interesting. Perhaps the most fundamental of these is observers' inability to extract all the information contained in a quantum state just from a single copy of it. This basic principle, which has strong relation to wave-particle duality, has many consequences. To name just few most important ones, there is quantum entanglement [1] necessary for many quantum information protocols, or the the no cloning theorem [2], which is responsible for security of quantum key distribution (QKD) [3].

Another consequence, closely related to the no cloning theorem, is our inability to do what is a standard part of classical communication channels - amplify signal in order to compensate for losses. Specifically we are speaking about coherent states of light, classical counterparts of wave amplitude of light. Even these semi-classical quantum states cannot be amplified without adding enough noise to render the process useless. Fortunately, this holds only for deterministic operations, as it was shown that in probabilistic regime it is possible to amplify the coherent states with varying levels of resource demands [4].

What remains to be seen, now that noiseless amplification has been shown feasible at some level, is how well are these amplifiers applicable to some realistic communication tasks. Some can be used to compensate losses [5], but that might not be enough in the most prevalent quantum communication protocol - QKD. We attempt to shed light on this issue by analyzing impact of the various kinds of noiseless amplifiers on mutual information shared by several communicating parties.

References

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[2] W.K. Wootters and W.H. Zurek, Nature **299**, 802 (1982).

[3] N. Gisin *et al.* Rev. Mod. Phys. 74, **145** (2002).

[4] G. Y. Xiang *et al.*, Nature Photonics **4**, 316 (2010); M. A. Usuga *et al.* Nature Physics **6**, 767 (2010); A. Zavatta *et al.*, Nature Photonics **5**, 52 (2011).

[5] T. C. Ralph, Phys. Rev. A **84**, 022339 (2011).

Self-similar visualization and sequence analysis of many-body wavefunctions

Javier Rodríguez-Laguna[1,2], Piotr Migdał[1], Miguel Ibáñez Berganza[3], Maciej Lewenstein[1,4] and Germán Sierra [3]

[1]ICFO–Institut de Ciències Fotòniques, 08860 Castelldefels (Barcelona), Spain
[2]Mathematics Department, Universidad Carlos III de Madrid, Spain
[3]Instituto de Física Teórica (IFT) UAM/CSIC, Cantoblanco (Madrid), Spain
[4]ICREA–Institució Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain

We present a pictorial representation of quantum many-body wavefunctions, in which a wavefunction characterizing a chain of n qudits is mapped to an image with $d^{n/2} \times d^{n/2}$ pixels. Such approach was introduced by Latorre [1] as a proof-of-principle tool to compress images using many-body wavefunctions. We [2] use this idea to analyze properties of ground states of commonly used Hamiltonians in condensed matter and cold atom physics, such as the Heisenberg or the Ising model in a transverse field (ITF).

The main property of the plotting scheme is the recursivity: increasing the number of qubits reflects in an increase in the image resolution, see Fig. 1 for an exemplary one. Thus, the plots are typically fractal-like, at least for translationally-invariant states, see Fig. 2. The two-dimensional structure is especially capable of capturing correlations between neighbouring particles. Many features of the wavefunction, such as magnetization, correlations and criticality, are represented by visual properties of the images. In particular, factorizability can be easily spotted: entanglement entropy turns out to be the deviation from the exact self-similarity, see Fig. 3.

Moreover, we investigate properties of the states using tools for sequence analysis - the Rényi fractal dimension and the information gain. The code for visualization is available on a dedicated website [3].

Figure 2: Examples for $n = 12$ qubit states. Color represent the sign. Left: ground state for the Heisenberg Hamiltonian with the periodic boundary conditions. Right: half-filled Dicke state.
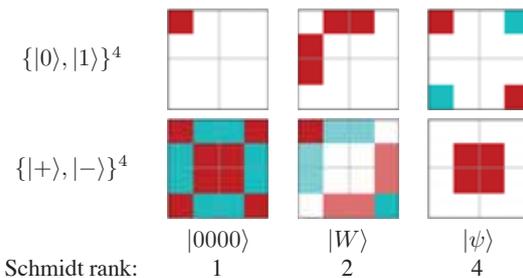
Figure 3: Entanglement estimation for 2–2 partition of four-qubit states. As examples we use a separable state $|0000\rangle$, W state and $|\psi\rangle = (|0000\rangle - |0101\rangle - |1010\rangle + |1111\rangle)/2$. They are presented in two different bases, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (-|0\rangle + |1\rangle)/\sqrt{2}$. Dividing in blocks is related to separating the first two particles from the last two. The Schmidt rank equals the number of linearly independent blocks, which can be counted by a naked eye.

[3] http://qubism.wikidot.com

Figure 1: A 2D plotting scheme of many-body wavefunctions. Left: each of the tensor basis states for 2 qubits: $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ is mapped into one of the four level-1 squares. Right: mapping of 4-qubit basis states into level-2 squares.

References

[1] Jose I. Latorre. Image compression and entanglement. (2005) Preprint: quant-ph/0510031.

[2] J. Rodríguez-Laguna, P. Migdał, M. Ibáñez Berganza, M. Lewenstein and G. Sierra (2011). Qubism: self-similar visualization of many-body wavefunctions. Preprint: 1112.3560.

Immunity of information encoded in singlet states against one particle loss

Piotr Migdał[1,2] and Konrad Banaszek[1]

[1]*Instytut Fizyki Teoretycznej, Wydział Fizyki, Uniwersytet Warszawski, Hoża 69, PL-00-681 Warszawa, Poland*

[2]*ICFO–Institut de Ciències Fotòniques, 08860 Castelldefels (Barcelona), Spain*

When an ensemble of elementary quantum systems decoheres through symmetric coupling with the environment, one can identify collective states that remain invariant in the course of evolution. These states span a so-called *decoherence-free subspace* (DFS) that is effectively decoupled from the interaction with the environment. More generally, it is possible to identify subspaces that can be formally decomposed into a tensor product of two subsystems, one of which "absorbs" decoherence, while the second one, named a *noiseless subsystem* or *a decoherence-free subsystem*, remains intact.

In this paper we consider the DFS for an ensemble of n qudits, i.e. elementary d-level systems, composed of states $|\Psi\rangle$ that are invariant with respect to all perfectly correlated $\mathrm{SU}(d)$ transformations:

$$U^{\otimes n}|\Psi\rangle = |\Psi\rangle, \qquad U \in \mathrm{SU}(d). \tag{1}$$

We prove [1] that this DFS features an additional degree of robustness, namely that the stored quantum information is immune to the loss of one of the qudits, regardless of the encoding.

This result, specialized to the polarization state of single photons for which $d = 2$, offers *combined* protection against two common optical decoherence mechanisms: photon loss due to scattering and residual absorption as well as collective depolarization that occurs inevitably in optical fibers used for long-haul transmission [2]. It is worth noting that another physical realization of the qubit case can be also an ensemble of spin-$\frac{1}{2}$ particles coupled identically to a varying magnetic field.

This provides a feasible scheme to protect quantum information encoded in the polarization state of a sequence of photons against both collective depolarization and one photon loss, which can be demonstrated with photon quadruplets (Fig.1) using currently available technology.

To generate a key, using so-called *trine codes*, the sender Alice could prepare photon quadruplets in one of randomly selected states $|\Xi_1\rangle$, $|\Xi_2\rangle$, or $|\Xi_3\rangle$. The ability to perform a projection onto any pair of orthogonal states $|\Xi_k\rangle$, $|\Xi_k^\perp\rangle$ (see Fig. 2) enables the receiving party Bob to tell, in the case when an outcome $|\Xi_k^\perp\rangle$ is obtained, which state has definitely not been prepared by Alice. Such correlations between Alice's preparations and Bob's outcomes can be distilled into a secure key [3].

Moreover, we analyze geometry of nonorthogonal bases for qubits that are made of products of two-particle singlet states and Dicke states. For singlet case [4] it is know in condensed matter physics as *valence bond basis*. Such approach makes is straightforward to identify which quantum correlations are intact after a particle loss or the collective decoherence and provides foundation for some key-distribution schemes as [5].
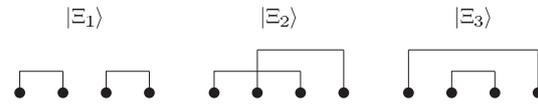
Figure 1: Diagrams depicting three non-equivalent products of two-qubit singlet states. They are nonorthogonal with the scalar product $\langle \Xi_i | \Xi_j \rangle = -1/2$ for $i \neq j$. In the Bloch representation of the two-dimensional DFS, they form a regular triangle inscribed into a great circle on the Bloch sphere.
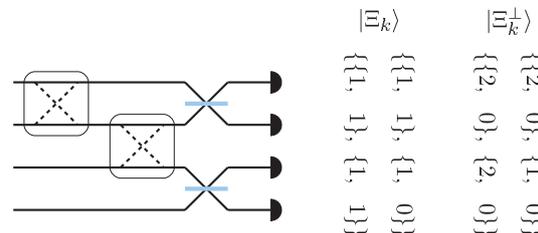
Figure 2: An experimental scheme for loss-tolerant detection of a logical qubit encoded in four photons. The projection basis $|\Xi_k\rangle$, $|\Xi_k^\perp\rangle$, where $k = 1, 2, 3$, is selected by a suitable rerouting of input photons. Pairs of photons are interfered on two balanced beam splitters and photon numbers are counted at their outputs. Combinations of outcomes for individual detectors that correspond to unambiguous identification of $|\Xi_k\rangle$ and $|\Xi_k^\perp\rangle$ are indicated with photon numbers in curly brackets. The ordering within both inner and outer brackets does not matter.

References

[1] P. Migdał and K. Banaszek, Immunity of information encoded in decoherence-free subspaces to particle loss. Phys. Rev. A **84**, 052318 (2011).

[2] M. Bourennane, M. Eibl, S. Gaertner, C. Kurtsiefer, A. Cabello, and H. Weinfurter, Decoherence-Free Quantum Information Processing with Four-Photon Entangled States. Phys. Rev. Lett. **92**, 107901 (2004).

[3] G. Tabia and B.-G. Englert, Efficient quantum key distribution with trines of reference-frame-free qubits. Phys. Lett. A, **375**, 817 (2011).

[4] D. W. Lyons and S. N. Walck, Multiparty quantum states stabilized by the diagonal subgroup of the local unitary group. Phys. Rev. A **78**, 042314, (2008).

[5] J. C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Robust polarization-based quantum key distribution over collective-noise channel. Phys. Rev. Lett. **92**, 017901 (2004).

Taming multipartite entanglement

Bastian Jungnitsch[1], **Tobias Moroder**[2,1], **Yaakov S. Weinstein**[3], **Martin Hofmann**[2], **Marcel Bergmann**[2] and **Otfried Gühne**[2,1]

[1]*Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Technikerstr. 21A, A-6020 Innsbruck, Austria*
[2]*Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Str. 3, D-57068 Siegen, Germany*
[3]*Quantum Information Science Group, MITRE, 260 Industrial Way West, Eatontown, NJ 07724, USA*

Entanglement is one of the most striking phenomena from the quantum realm. Apart from its manifestation in two particle scenarios there is currently an increased interest in its various multipartite forms. For quantum information multiparticle entanglement represents the key resource behind tasks like measurement-based quantum computation, high-precision metrology or secret sharing as a communication tasks. All these applications further sparked its interest and it is no wonder that current experiments strive to generate strong and robust entanglement between many particles. However, though there has been a lot of progress in recent years, the characterization of this kind of correlations is still very difficult. In particular genuine multipartite entanglement, its most strongest form, remains unruly and only scattered results concerning its characterization are known.

In this talk we present a general method to characterize genuine multipartite entanglement by considering a suitable relaxation on the level of quantum states [1]. Rather than trying to distinguish a given state from the set of all biseparable states, *i.e.*, the non-entangled states in this case, one only wants to ensure that it is not an element of a slightly larger set of states. This superset of states called PPT-mixtures can conveniently be described employing the Peres-Horodecki criterion of the bipartite case [2]. A schematic picture of this idea is shown in Fig. 1 for the exemplary case of three particles. Using this relaxation provides a more tractable problem which results in an operational entanglement criterion, which can indeed be considered as a generalization of the Peres-Horodecki criterion to the multipartite case.

The derived criterion can for instance be efficiently evaluated numerically by means of semidefinite programming, which we implemented in an easy-to-use software package [3]. This program works for example for generic states of up to 6-7 qubits. Apart from this numerical approach the whole problem can also be tackled analytically if one reformulates it within the context of entanglement witnesses. The resulting witnesses can be considered as the natural extension of decomposable witnesses [4] to the multipartite case. Besides mere detection this criterion can also be turned into a measure of genuine multipartite entanglement, which shows similar properties to the negativity of the bipartite case [5]. Its main advantage is again that it can be easily computed for general states such that even a rigorous quantitative analysis of genuine multipartite entanglement becomes possible.

We demonstrate the performance of our criterion by applying it to several prominent states. Moreover we present analytic construction methods for states that can be associated to the structure of a graph [6]. Via this method one obtains for example the statement that the largest ball of biseparable states around the totally mixed state vanishes for high particle
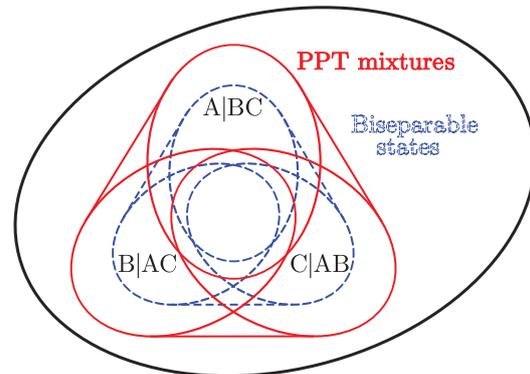
Figure 1: Idea of the criterion: Rather than characterizing the set of biseparable states (dashed region) built up by separable states for each possible bipartition, one considers the more tractable superset of PPT-mixtures (solid), formed by the convex combinations of states with a positive partial transpose for each splitting. Whenever a given state lies outside the set of PPT-mixtures, it is also outset the set of biseparable states and therefore genuine multipartite entangled.

numbers. Finally we show that the derived criterion is even sufficient for several interesting classes of states, including among others, permutationally invariant states of three qubits or graph-diagonal states of up to four qubits [7].

References

[1] B. Jungnitsch, T. Moroder and O. Gühne, Phys. Rev. Lett. **106**, 190502 (2011).

[2] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996); M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. A **223**, 1 (1996).

[3] PPTmixer, available from `mathworks.com`, FileID: 30968

[4] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).

[5] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).

[6] B. Jungnitsch, T. Moroder and O. Gühne, Phys. Rev. A **84**, 032310 (2011).

[7] O. Gühne, B. Jungnitsch, T. Moroder, Y. S. Weinstein, Phys. Rev. A **84**, 052319 (2011).

Experimental quantum measurement reversal using quantum error correction

Philipp Schindler[1], Julio T. Barreiro[1], Daniel Nigg[1], Matthias Brandl[1], Michael Chwalla[1,2], Thomas Monz[1], Markus Hennrich[1] and Rainer Blatt[1,2]

[1]*Institute for Experimental Physics, University of Innsbruck, A-6020 Innsbruck, Austria*
[2]*Institute for Quantum Optics and Quantum Information, A-6020 Innsbruck, Austria*

The measurement of a quantum state is a non-reversible process that projects the system onto the eigenstates of the measurement operator. Therefore, it is generally not possible to reconstruct the state prior to the measurement. However, the measurement projection can also be regarded as a qubit error which can be rectified by quantum error correction techniques. In particular, the projective measurement of a single qubit onto the two qubit states $|0\rangle$ and $|1\rangle$ can be interpreted as a complete phase damping process [1]. This projection can be reversed using a three qubit error correction algorithm protecting against phase flip errors.

Figure 1: a) The experimental sequence consists of the encoding and decoding steps to protect the qubit $|\psi\rangle$ from phase-flip errors, and the measurement projection by fluorescence detection on the first qubit. Hiding and unhiding sequences enclose the measurement to protect the ancilla qubits from being projected. b) The energy level scheme illustrates the (i) hiding and (ii) measurement projection sequences. c) A threshold method for the number of detected photons is used to distinguish between qubit state $|0\rangle$ and $|1\rangle$.

We report on the experimental realization of such quantum measurement reversal in a system of trapped Calcium ions. For the measurement reversal we adapt the algorithm presented in [2]. This 3-qubit quantum error correction code can fully correct for single qubit phase flips errors and is therefore ideally suited for the reversal of measurement projection

of one of the three qubits while being in the error-protected state. The measurement is performed by a laser induced fluorescence detection technique (electron shelving) which scatters photons from state $|1\rangle$ and remains dark for state $|0\rangle$ (see Figure 1). This measurement in the computational basis (σ_z) of a single qubit is described by a projection onto the z-axis of the Bloch sphere, but can also be interpreted as complete phase damping process where all the x-y information is lost. The three qubit error correction code can protect against such single qubit phase-flip errors, however the two ancilla qubits have to stay protected from the measurement. This is performed by hiding and unhiding pulses before and after the measurement (Figure 1). Furthermore, as measurements in ion trap quantum computers heat the motional state of the system it is necessary to re-cool the system before performing the correction step. This cooling has to be performed without affecting the quantum state of the qubits. We use a Raman cooling technique to re-cool the ion string within the sequence. Finally, we assess the fidelity of this measurement reversal using quantum process tomography.

Why is the measurement reversal possible? The quantum information $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is encoded in a logical qubit $\alpha|+++\rangle + \beta|---\rangle$ that is distributed over the three physical qubits. The measurement projection of a single physical qubit onto the basis states $|0\rangle$ and $|1\rangle$ does not reveal any information on the state of the logical qubit, but only destroys the phase of the first physical qubit. The decoding sequence can finally correct for the lost phase information.

References

[1] M.A. Nielsen, and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, (2010).

[2] P. Schindler, J.T. Barreiro, T. Monz, V. Nebendahl, D. Nigg, M. Chwalla, M. Hennrich, and R. Blatt, Experimental Repetitive Quantum Error Correction, Science, **332**, 1059 (2011).

Light pulse analysis with a multi-state atom interferometer

I. Herrera[1], **P. Lombardi**[1,2], **J. Petrovic**[1,3], **F. Schaefer**[1] **and F. S. Cataliotti**[1,4]

[1]*European Laboratory for Nonlinear Spectroscopy (LENS), Via Nello Carrara 1, 50019 Sesto F.no (FI), Italy*
[2]*Dipartimento di Fisica e Astronomia Università di Firenze via Sansone 1, 50019 Sesto F.no (FI), Italy*
[3]*Vinča Institute of Nuclear Sciences, PO Box 522, 11001 Belgrade, Serbia*
[4]*Dipartimento di Energetica "Sergio Stecco" Università di Firenze via S. Marta 3, 50139 Firenze, Italy*

We present a controllable multi-path cold-atom interferometer that is easy-to-use and fully merged with an atom chip.

The initial state is prepared by condensing ^{87}Rb atoms in a low-field seeking ground state, here $|F = 2, m_F = 2\rangle$. Coherent transfer of the atoms to other Zeeman sublevel of the same hyperfine state is realised by application of a resonant RF pulse. The interferometer is closed by remixing these states by the second RF pulse after a controllable time delay τ as in [1]. The second pulse maps the relative phases accumulated between different states during the delay into a population distribution at the output of the interferometer. The relative phases between the states are accumulated due to the presence of the trapping magnetic field **B**. In this field Zeeman states experience different potentials given by $V = m_F g_F \mu_0 |B|$ where m_F and g_F are the spin and Landè numbers, respectively, and μ_0 is the Bohr magneton. Therefore, their relative phases evolve with the frequencies equal to the multiples of the energy separation between the adjacent levels $\omega = g_F \mu_0 |\mathbf{B}|/\hbar$, yielding the output signals rich in harmonics. The harmonics cause the fringe narrowing with the number of states, which is the basic characteristic of a multi-path interferometer. If an external signal is applied during the delay between the pulses, it will contribute to the relative phases between the states causing a shift in the fringe positions at the output. Since the interferometric paths are not spatially separated, the interferometer is particularly suitable for measuring external fields whose interactions with atoms are state-sensitive. Finally, in order to determine the population of each output state, these states are spatially separated by application of the Stern-Gerlach method followed by the free-fall expansion and then imaged.

Applications of the proposed interferometer are based on different responses of the Zeeman states to an external field. Due to the simultaneous measurement of multiple state populations, the interferometer can be used in two basic measurement configurations: absolute measurement in which the signal is defined as a shift of fringes belonging to a chosen state, and differential measurement in which the signal is defined as the difference in shifts of fringes belonging to different states. Applications of the absolute measurements are in measuring the magnetic field amplitude which directly maps into the periodicity of the fringes and in measurements of parameters of light-atom interactions. An example of the latter is shown in Fig. 1 where a response of the $m_F = 2$ state to the far-off resonant light pulses with different circular polarizations is shown.

We wish to thank M. Schrambck (Atomisntitut, TU-Wien) at the ZMNS (TU-Wien) who realised the AtomChip we used. The chip was supplied through the CHIMONO collaboration. We acknowledge the financial support of the Fu-
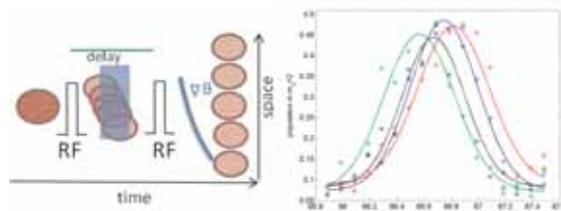
Figure 1: Here we demonstrate the sensitivity of the interferometer to a light pulse sent to the BEC during the time interval between the two Rabi pulses. The atoms were illuminated by the 40μs light pulse with the frequency stabilized to 6.568 GHz to the red of the $F = 2 \rightarrow F = 3$ Rb D$_2$ transition. The pulse was focused along the longer axis of the BEC and its beam waist at the condensate was 100μm. Due to the small diameter of the BEC (1μm) only a fraction of the pulse power was interacting with atoms. Black line shows the reference fringe without light, green line corresponds to $\sigma-$ light pulse with the power of 86nW, blue and red lines correspond to $\sigma+$ light pulses with powers 86nW and 176nW, respectively. All fringes are of the $m_F = 2$ state. Rabi frequency was set to give the pulse area of 1.35π. To facilitate the analyses we have plotted gaussian fits (full lines) of the experimental data (crosses). The polarisation of light determines the sign of the fringe shift, $\sigma-$ advances and $\sigma+$ delays the fringe pattern. The senstivities were estimated as shifts of the gaussians and were 0.13 rad/pJ for $\sigma-$ and 0.1 rad/pJ for $\sigma+$.

References

[1] Minardi, F., Fort, C., Maddaloni, P., Modugno, M. & Inguscio, M. Time-Domain Atom Interferometry across the Threshold for Bose-Einstein Condensation. *Phys. Rev. Lett.* **87**, 170401-4 (2001).

Control of Wannier orbitals for generating tunable Ising interactions of ultracold atoms in an optical lattice

K. Inaba[1,3], **Y. Tokunaga**[2,3], **K. Tamaki**[1,3], **K. Igeta**[1,3], **M. Yamashita**[1,3]

[1]*NTT Basic Research Labs., NTT Corporation, Atsugi, Kanagawa 243-0198, Japan*
[2]*NTT Secure Platform Labs., NTT Corporation, Musashino, Tokyo 180-8585, Japan*
[3]*CREST, JST, Chiyoda-ku, Tokyo 102-0075, Japan*

Ultracold atoms in an optical lattice are promising candidates with which we implement quantum computer and also quantum simulator [1]. High controllability and stability of atoms offers substantial advantages of this system for realizing the above two applications. Current experimental techniques demonstrate that single atoms at each site can be individually measured by addressing the lattice sites [2], which are great progress in both applications. A Feshbach resonance allows us to control the strength of the contact interaction between atoms [3]. However, the inter-site interactions, such as an Ising type spin-spin interaction, required for two-qubit gate in quantum computation are usually too weak to generate entanglement in a short time. This is because such magnetic interactions are basically induced by the perturbative processes. The entanglement generation utilizing the lattice potential modulations is one of the efficient ways to overcome this issue [4]. On the other hand, from the aspect of quantum simulator, the large inter-site interactions help us to realize the important magnetic phase transitions, such as the Néel transition, even under strong thermal fluctuations.

In this study, we propose a new method to create an tunable Ising interaction between atoms, and consider the two applications as mentioned below. The key to our idea is that we utilize higher Wannier orbitals as *controllable and accessible* environment, and then realize the Ising interaction between atoms in the lowest orbital at adjacent sites. Importantly, we can tune the strength of this interaction by controlling the coupling between atoms in the lowest orbital and the higher orbitals. Note that we treat Wannier orbitals in the *ab initio* manner in order to make this orbital control precise.

First, we apply the Ising interaction to multipartite entanglement generation of cluster states, and carefully investigate fidelity and scalability of our method [5]. Enhanced Ising interaction allows us to create the cluster state in a short time. We further propose to improve our method with the following two schemes. The fidelity can be enhanced by performing measurements on states of the environment followed by post-selection depending on the resulting outcomes. Substantial advantages as regards scalability can be obtained by our pair-wise entanglement generation scheme. Precise numerical simulations using an exact diagonalization confirm that the combination of the above schemes can generate very high-fidelity entanglement with current experimental technologies. Note that the present method is applicable to generating one, two, and three dimensional (1D, 2D, and 3D) cluster states, and thus is suitable for fault tolerant measurement based quantum computation schemes [6].

Secondly, we will further discuss the application of our tunable Ising interaction to quantum simulator of magnetism. We consider the following situation that the Ising interaction is effectively enhanced while the atoms are loaded into an optical lattice. Here, atoms during this loading process is well captured by the extended Hubbard Hamiltonian that includes the additional Ising interaction term with a large interaction strength. We will discuss the possibility of the efficient realization of Néel state using this effective model.

References

[1] I. Bloch, Nature (London) **453**, 1016 (2008).

[2] W. S. Bakr, A. Peng, M. E. Tai, R. Ma, J. Simon, J. I. Gillen, S. Fölling, L. Pollet, and M. Greiner, Science **329**, 547 (2010); C. Weitenberg, M. Endres, J. F. Sherson, M. Cheneau, P. Schausz, T. Fukuhara, I. Bloch, and S. Kuhr, Nature (London) **471**, 319 (2011); M. Endres, M. Cheneau, T. Fukuhara, C. Weitenberg, P. Schauß, C. Gross, L. Mazza, M. C. Bañuls, L. Pollet, I. Bloch and S. Kuhr, Science **334**, 200-203 (2011); J. Simon, W. S. Bakr, R. Ma, M. E. Tai, P. M. Preiss and M. Greiner, Nature (London) **472**, 307-312 (2011).

[3] H. Feshbach, Ann. Phys. (N.Y.) **5**, 357 (1958); C. A. Regal and D. S. Jin, Phys. Rev. Lett. **90**, 230404 (2003).

[4] O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hansch, and I. Bloch, Phys. Rev. Lett. **91**, 010407 (2003); O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hansch, and I. Bloch, Nature (London) **425**, 937 (2003); L.-M. Duan, E. Demler, and M. D. Lukin, Phys. Rev. Lett. **91**, 090402 (2003); B. Vaucher, A. Nunnenkamp, and D. Jaksch, New J. Phys. **10**, 023005 (2008); S. Trotzky, P. Cheinet, S. Folling, M. Feld, U. Schnorrberger, A. M. Rey, A. Polkovnikov, E. A. Demler, M. D. Lukin and I. Bloch, Science **319**, 295-299 (2008).

[5] K. Inaba, Y. Tokunaga, K. Tamaki, K. Igeta and M. Yamashita, arxiv:1202.6446.

[6] R. Raussendorf, J. Harrington, and K. Goyal, Ann. Phys. (NY) **321**, 2242 (2005); R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007); R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007); T. M. Stace, S. D. Barrett, and A. C. Doherty, Phys. Rev. Lett. **102**, 200501 (2009).

Excitation of a single atom with a temporally shaped light pulses

Syed Abdullah Aljunid[1], **Dao Hoang Lan**[1], **Yimin Wang**[1], <u>**Gleb Maslennikov**</u>[1], **Valerio Scarani**[1,2] and **Christian Kurtsiefer**[1,2]

[1]*Centre for Quantum Technologies, National University of Singapore, Singapore*
[2]*Department of Physics, National University of Singapore, Singapore*

We investigate the interaction between a single ^{87}Rb atom and optical pulses with a controlled temporal envelope. The excitation probability P_e of a single atom by a travelling light pulse in the abscense of optical resonator is governed by an overlap of atomic emission modes (both spatial and frequency) with the mode of the optical field [1, 2]. While in our experiment the spatial ovelap is fixed by high numerical aperture aspheric lens that focuses a Gaussian beam to an atom, the frequency/temporal overlap can be changed by shaping the temporal envelope of a coherent pulse. It is expected [1, 2] that for a light field in a Fock state, a rising exponential pulse would lead to higher P_e. Since it is technically challenging to prepare the field in a pure Fock state we mimic that state with a weak coherent pulse obtained from attenuated laser beam, and do the temporal shaping with fast modulators [3]. We are comparing P_e for two different pulse shapes: rising exponential and rectangular. The excitation probability is measured by detecting atomic fluorescence with high temporal resolution and normalizing the acquired rates by optical losses (Fig. 1).

Figure 2: Top: Maximal excitation probability of an atom versus the number of photons in a pulse. Bottom: Atomic population dynamics during the excitation pulse followed by exponential decay when the field is switched off (dashed line)

[1] M. Stobinska, et al., European Physics Letters **8**6, 14007 (2009)

[2] Y. Wang et. al., Phys. Rev. A. **83**, 063842 (2011)

[3] S.A. Aljunid et al., to be published

[4] I. Gerhardt et. al., Phys. Rev. A. **79**, 011402(R) (2009)

Figure 1: Experimental setup. The atomic fluorescence from temporarily shaped probe pulses is detected in a backward direction with APD1. The excitation probability is obtained by temporal binning of fluorescence counts in a timiestamp unit and normalized to excitation pulse power detected by APD2 in forward direction without an atom in a trap.

We have found that an atom is excited faster by using less photons in a driving pulse with a rising exponential shape (Fig. 2). Although a rectangular shape eventually leads to higher P_e, it takes more photons to bring it there. One also sees that the atomic transition is saturated for approximately 100 photons in a pulse. This suggests that one expects to see a nonlinear interaction between atom and light for such low photon number. Indeed, by increasing photon number to ≈ 1000 (Fig. 2) we observe Rabi oscillations with ≈ 100 MHz. This result show a possibility of optical switching for low photon numbers even without cavity assistance [4].

We want to note, that the observed effects should be more profound with optical Fock states and for a higher spatial overlap with atomic emission profile.

Simulating quantum effects of cosmological expansion using a static ion trap

Nicolas C. Menicucci[1,2], **S. Jay Olson**[3], and **Gerard J. Milburn**[3]

[1] *School of Physics, The University of Sydney, Sydney, NSW, 2006, Australia*
[2] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario, N2L 2Y5, Canada*
[3] *School of Mathematics and Physics, The University of Queensland, St Lucia, QLD, 4072, Australia*

We propose an experimental testbed using ions in the collective ground state of a static trap to study the analog of quantum-field effects in cosmological spacetimes [1]. To date, proposals for trapped-ion analog gravity experiments have simulated the effect of gravity on field modes by directly manipulating the ions' motion [2, 3]. In contrast, by associating laboratory time with *conformal time* in the simulated universe, we can encode the full effect of curvature in the modulation of the laser used to couple the ions' vibrational motion and electronic states. This modulated coupling serves as the analog of a field detector in an expanding spacetime.

Curved-spacetime quantum field theory (QFT) is essential to cosmology [4] and has given rise to fascinating results such as black-hole evaporation [5]. The difficulty in testing these effects directly has given rise to a number of proposals for testing *analog* curved-spacetime QFT effects [6], where spacetime is replaced by a laboratory system of coupled atoms (either individual atoms or a quasi-continuous fluid), and field modes are replaced by the collective modes of oscillation of the atoms—effectively a "phonon field." While the observable effects are conceptually the same (analogous), the parameters of the experiment may be adjusted to result in a much stronger and more easily observed effect. The key advantage of this proposal over other similar ones (e.g., for Bose-Einstein condensates [7]) is precise control of the detector coupling and efficient readout.

In the current proposal, the collective ground state of ions in a static linear trap serves as the analog of a scalar field in the conformal vacuum (i.e., the ordinary Minkowski vacuum with the ordinary time coordinate replaced by conformal time), and we encode the effects of spacetime curvature into a modulation of the analog detectors (i.e., the coupling of electronic and vibrational motion of a single ion), rather than in the motion of the atoms which comprise the analog spacetime. This amounts to making a shift in the analogy away from *laboratory time $\leftrightarrow$ detector proper time* (Figure 1) and towards *laboratory time $\leftrightarrow$ conformal time* (Figure 2). For many useful cases studied in cosmology, this identification encodes the entire effect of the spacetime curvature and therefore enables us to propose analog curved-spacetime QFT experiments in which the analog spacetime is fixed, thus making our proposals far more accessible experimentally. Further details may be found in Ref. [1].

Figure 1: Field picture. Expansion of the universe (left to right, below) causes the field modes to redshift, while the detector resonant frequency remains unchanged. This is simulated in the analog model by identifying laboratory time with detector proper time.
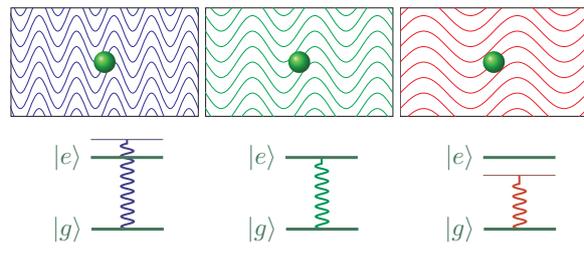
Figure 2: Detector picture. Expansion of the universe (left to right, below) causes the detector resonant frequency to blueshift, while the field modes remain unchanged. This is simulated in the analog model by identifying laboratory time with conformal time.

References

[1] N. C. Menicucci, S. J. Olson, and G. J. Milburn, "Simulating quantum effects of cosmological expansion using a static ion trap," New J. Phys. **12**, 095019 (2010).
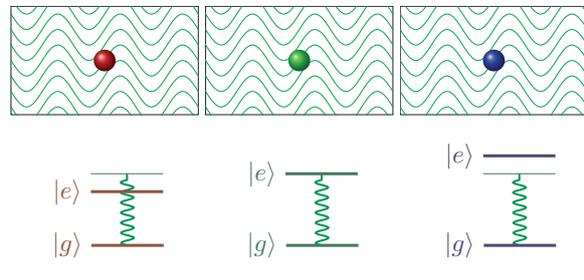
[2] P. M. Alsing, J. P. Dowling, and G. J. Milburn, "Ion Trap Simulations of Quantum Fields in an Expanding Universe," Phys. Rev. Lett. **94**, 220401 (2005).

[3] R. Schützhold *et al.*, "Analogue of Cosmological Particle Creation in an Ion Trap," Phys. Rev. Lett. **99**, 201301 (2007).

[4] S. Weinberg, *Cosmology* (Oxford, 2008).

[5] S. W. Hawking, "Particle creation by black holes," Comm. Math. Phys. **43**, 199 (1975).

[6] W. G. Unruh, "Experimental Black-Hole Evaporation?," Phys. Rev. Lett. **46**, 1351 (1981).

[7] P. O. Fedichev and U. R. Fischer, "Gibbons-Hawking Effect in the Sonic de Sitter Space-Time of an Expanding Bose-Einstein-Condensed Gas," Phys. Rev. Lett. **91**, 240407 (2003).

Single atom lensing

Sylvi Händel[1], **Andreas Jechow**[1], **Benjamin G. Norton**[1], **Erik W. Streed**[1] **and David Kielpinski**[1]

[1]*Centre for Quantum Dynamics, Griffith University, Brisbane QLD 4111, Australia*

Singly trapped ions can be utilised to explore the intriguing world of quantum optics, as they offer a high degree of control. In conjunction with their isolation from the environment they can be regarded as the most simple system for investigating microscopic optical behaviour. In particular fundamental optical devices such as a mirror [1] or a lens can be demonstrated by atom-light interactions.

Here we report on the unprecedented observation of lensing of light by a single atom. The phase shift of the scattered light with respect to the incident light is characteristic for lensing and in the case of a single atom localised to the atom's position.

Our system employs a ^{174}Yb$^+$ ion which is confined in a three dimensional radio frequency Paul trap formed by the electric quadrupole between two tungsten needles. Imaging of the ion is performed by focussing a resonant illumination field at $\lambda = 369.5$ nm to a spot size of $4.8\ \mu$m FWHM. When the illumination field is interacting with the atom scattering is induced. The scattered field as well as the illumination field are imaged with a large aperture phase fresnel (NA = 0.64) lens onto a CCD camera using a telescope of magnification x585. By using a phase fresnel lens which high numerical aperture we can demonstrate quantum-limited absorption imaging of a single atom [2, 3, 4].
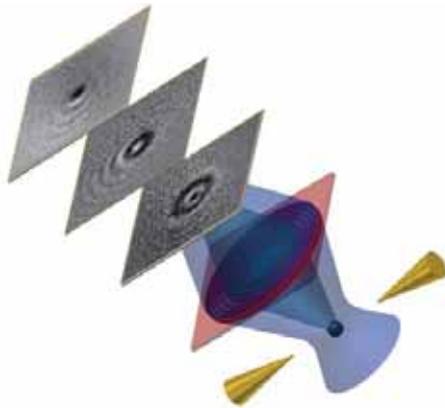
Figure 1: Configuration of the experimental apparatus. Images show example background-subtracted images of the light transmitted past the atom. The image size is 3.4 x 3.4 μm with a resolution of 370 nm. Shadow images of the atom showing lensing of the illumination field. The bright central spot in the middle image corresponds to the focus position.

An atom driven by a sufficiently weak illumination field can be modeled as a radiating electric dipole. On resonance, the re-radiated light presents a $\pi/2$ phase advance relative to the illumination field. When the illumination field and radiated field are reimaged along the same axis, the illumination field undergoes a relative phase delay of $\pi/2$, analogous to the Gouy phase shift for a Gaussian beam. The total phase shift of π results in destructive interference between the two light fields and the absorption of light by the atom, as investigated in our recent work [2]. Away from atomic resonance, the re-radiated light experiences a phase shift between 0 (for far red detuning) and π (for far blue detuning). This phase shift, localised to the position of the atom, induces a deviation of the light rays like that found in a lens. Figure 1 gives a conceptual illustration of the atom lensing effect.

Physical concepts of the single-atom lensing effect could possibly be used to construct novel nanophotonic devices from small numbers of atoms. An atomic scale waveguide can be constructed of a string of atoms, which is feasible in an optical lattice. The presented demonstration of a well isolated atom in free space could be realised instead in a solid-state host crystal. Recent progress in manufacturing three dimensional structures at the nanoscale have shown very impressive results with the manufacturing of metamaterials using electron beam lithography or focused ion beams.

References

[1] G. Hétet, L. Slodička, M. Hennrich and R. Blatt, Phys. Rev. Lett. **107**, 133002 (2011)

[2] E. W. Streed, A. Jechow, B. G. Norton and D. Kielpinski, http://arxiv.org/abs/1201.5280

[3] E. W. Streed, B. G. Norton, A. Jechow, T. J. Weinhold and D. Kielpinski, Phys. Rev. Lett. **106**, 010502 (2011)

[4] A. Jechow, E. W. Streed, B. G. Norton, M. Petrasiunas and D. Kielpinski, Opt. Lett. **36**, 1371 (2011)

Coherence and entanglement in a nano-mechanical cavity

L.-H. Sun[1,2]**, G.-X. Li**[1] **and Z. Ficek**[3]

[1]*Huazhong Normal University, Wuhan, P. R. China*
[2]*Yangtze University, Jingzhou, P. R. China*
[3]*KACST, Riyadh, Saudi Arabia*

There have recently been a great interest in theoretical and experimental studies of creation of quantum entanglement in optomechanical systems [1]. This interest stems from the possibility of the development of new practical techniques for engineering of entangled states of macroscopic systems through interactions with mechanical oscillators. With the recent progress in laser cooling techniques, fabrication of low-loss optical elements and high-Q mechanical resonators, it is now possible to prepare nanomechanical oscillators that can be controlled to a very hight precision and can even reach the quantum level of the oscillations. In these systems, the vibrations of mechanical oscillators are induced by radiation pressure that creates a strong nonlinear coupling of the vibrational mode to radiation modes.

In this presentation, we consider optomechanical effects on bosonic modes realized in one-dimensional optical lattice located inside a cavity with movable mirror, as illustrated in Fig. 1. We analyze entangled features indicative of the optomechanical effects. The overall approach adopted here is based on the use of the quantum Langevin equations and is an extension of the method proposed by Genes *et al.* [2] to the case of a multi-mode bosonic system.
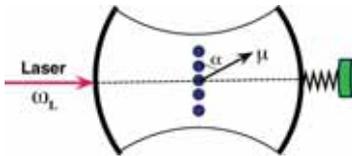
Figure 1: Schematic diagram of the optomechanical system. An optical lattice composed of regularly spaced atoms of the transition dipole moments $\vec{\mu}$ is located inside a single-mode cavity driven by a laser field of frequency ω_L. The cavity is composed of one fixed and one movable mirror that can undergo harmonic oscillations due to the radiation pressure induced by the laser field.

We present an analytical study of coherence and correlation effects produced in a single-mode nano-mechanical cavity containing an optical lattice of regularly trapped atoms. The system is modelled as a three-mode system, two orthogonal polariton modes representing the coupled optical lattice and the cavity mode, and one mechanical mode representing the oscillating mirror [3]. We show that the system is capable of generating a wide class of coherence and correlation effects, ranging from the first-order coherence, the anomalous autocorrelations and anomalous cross correlations between the modes. We explore the relationship between the generation of entanglement and the first-order coherence in the system.

Conditions for entanglement between two modes (A, B) of the system are determined in terms of the Cauchy-Schwartz inequality

$$\chi_{(A,B)} = \left[g_A^{(2)} g_B^{(2)} \right] / \left(g_{AB}^{(2)} \right)^2 > 1. \qquad (1)$$

Here, $\chi_{(A,B)}$ is the so-called Cauchy-Schwartz parameter in which

$$\begin{aligned} g_n^{(2)} &= 2 + \left| \eta_{(n,n)} \right|^2, \quad n = A, B, \\ g_{AB}^{(2)} &= 1 + \left| \gamma_{(A,B)} \right|^2 + \left| \eta_{(A,B)} \right|^2, \end{aligned} \qquad (2)$$

where $\left| \gamma_{(A,B)} \right|$ is the degree of the first-order coherence between the two modes, $\left| \eta_{(A,A)} \right|$ is the degree of the so-called "anomalous" autocorrelation inside the mode A, and $\left| \eta_{(A,B)} \right|$ is the degree of the anomalous cross correlation between the modes. Equation (1) shows that the Cauchy-Schwartz parameter depends on various correlations in the system, namely the anomalous autocorrelation, the first-order coherence and the anomalous cross correlation.

We examine separately the cases of two-mode and three-mode interactions which are distinguished by a suitable tuning of the mechanical mode to the polariton mode frequencies. We find that the generation of the first-order coherence between two modes of the system is equally effective in destroying entanglement between these modes. In other words, the creation of the first-order coherence among the polariton and mechanical modes is achieved at the expense of entanglement between them. The oscillating mirror makes the polaritons partly coherent. Thus, two independent thermal modes can be made by the oscillating mirror mutually coherent and the degree of coherence can, in principle, be as large as unity.

Further studies show that there is no entanglement between the independent polariton modes when both modes are simultaneously coupled to the mechanical mode by the parametric (squeezing-type) interaction. There is no entanglement between the polaritons even if the oscillating mirror is damped by a squeezed vacuum field. We establish that in order to effectively entangle two independent modes through an intermediate mode, one of the modes should be coupled to the intermediate mode by a parametric interaction but the other mode should be coupled by the linear-mixing (beamsplitter-type) interaction.

References

[1] M. Aspelmeyer, S. Gröblacher, K. Hammerer, and N. Kiesel, J. Opt. Soc. Am. B **27**, A189 (2010).

[2] C. Genes, A. Mari, P. Tombesi, and D. Vitali, Phys. Rev. A **78**, 032316 (2008).

[3] L. H. Sun, G. X. Li, and Z. Ficek, Phys. Rev. A **85**, 022327 (2012).

Fractional Quantum Hall Physics in Jaynes-Cummings-Hubbard Lattices

Andrew L. C. Hayward[1], **Andrew M. Martin**[1] and **Andrew D. Greentree**[1,2]

[1] *School of Physics, University of Melbourne, Australia*
[2] *School of Applied Sciences, RMIT University, Australia*

Jaynes-Cummings-Hubbard (JCH) arrays provide unique opportunities for quantum emulation. These systems promise unparalleled control and readout of the full quantum mechanical wavefunction, along with *in situ* tuning of the Hamiltonian. The JCH model is predicted to exhibit a number of solid state phenomena, including Mott/superfluid phases, semi-conductor physics, Josephson effect, metamaterials properties, and Bose-glass phases.

We show how to realise strongly correlated states of light in Jaynes-Cummings-Hubbard arrays under the introduction of an effective magnetic field. The effective field is realised by dynamic tuning of the cavity resonances [see Fig. 1]. We demonstrate the existence of Fractional Quantum Hall (FQH) states by computing topological invariants, phase transitions between topologically distinct states, and Laughlin wavefunction overlap. These states constitute new, strongly correlated states of light. Our system therefore provides a novel and powerful framework for investigating FQH physics.

A JCH lattice consists of an array of coupled photonic cavities, with each cavity mode coupled to a two-level atom [see Figs. 1(a) and (b)].

$$H^{JCH} = \sum_i^{\text{sites}} H_i^{JC} + \sum_j^{\text{N.N}} \kappa_{ij}(a_i a_j^\dagger + \text{h.c.}) \quad (1)$$

$$H^{JC} = \omega(a^\dagger a + \sigma_z) + \Delta\sigma^+\sigma^- + \beta(\sigma^+ a + \text{h.c.}). \quad (2)$$

$a(a^\dagger)$ and $\sigma^\pm$ are respectively the photonic and atomic raising and lowering operators. ω is the cavity frequecy, Δ the atomic detuning, β the dipole coupling strength, and κ_{ij} the inter-site tunneling rates. The Jaynes-Cummings Hamiltonian, H^{JC}, provides an onsite interaction which induces photon-photon correlations, necessary for the creation of FQH states.

A magnetic field induces a geometric phase from transport around a closed loop. In our model, this manifests as complex tunneling rates κ_{ij}. Since the photons do not couple to a magnetic field, the complex phases must be induced indirectly. To achieve this we propose a scheme based on phase offset photon assisted tunneling [see Fig. 3(c)]. Here, the presence fast oscillating fields breaks Time-Reversal symmetry (TRS), leading to an effective complex κ. This scheme allows the creation of arbitrarily large fields, providing access to the FQH regime.

We show for a number of small systems that, at filling factor $\nu = \frac{1}{2}$, our JCH model exhibits topological phases analogous to the FQH states seen in electronic media. This is demonstrated by: 1) the existence of a gapped groundstate 2) good overlap with a Laughlin Anzats, modified for the JCH model, and 3) by computing Chern numbers. The Chern number quantifies the topological nature of the many-body ground state, and corresponds directly to the quantized Hall conductance, thus providing explicit evidence of FQH
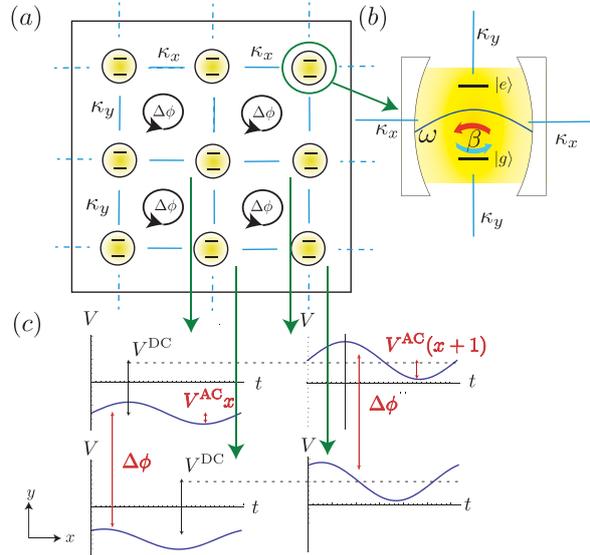
Figure 1: (a) Schematic of a square JCH lattice with a constant effective magnetic field. Photons moving around a plaquette acquire a phase $\Delta\phi$. (b) A single mode photonic cavity with frequency ω coupled to a two level atom with strength β. (c) Scheme for breaking TRS in photonic cavities: a potential $V = \left[V^{\text{DC}} + V^{\text{AC}}\sin\left(\omega^{\text{rf}}t + \Delta\phi y\right)\right] x$ (x and y in units of the lattice spacing) is applied to the cavities (indicated by green arrows) by dynamically tuning ω. The phase offset, $\Delta\phi$, along y results in the synthetic magnetic field seen in (a).

physics. These FQH states undergo a topological phase transition from highly correlated to uncorrelated as the photon-atom interaction is reduced.

We discuss experimental realization of our system. While our results are independent of the implementation, the most promising architecture for our system is in a circuit QED framework. Here, we show that our system is imminently realizable. We also present our most recent results, where we demonstrate the existence of more complex states, such as the Moore-Read Pfaffian state, in the JCH model. These states poses non-abelian excitations, which can be used for topologically protected quantum computing.

References

[1] A.L.C. Hayward, A.M. Martin and A.D. Greentree, Fractional Quantum Hall Physics in Jaynes-Cummings-Hubbard lattices, arXiv:1202.5067

Effect of excitation jitter on the indistinguishability of photons emitted from an InAs quantum dot

Harishankar Jayakumar[1], <u>Tobias Huber</u>[1], Thomas Kauten[1], Ana Predojević[1], Glenn Solomon[2], and Gregor Weihs[1]

[1]*Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, 6020 Innsbruck, Austria*
[2]*Joint Quantum Institute & National Institute of Standards and Technology, University of Maryland, Gaithersburg, USA*

Indistinguishable single photons on demand are essential for quantum computation with linear optics [1]. If two indistinguishable photons arrive at a beamsplitter at the same time, they coalesce and leave the beamsplitter through the same port. In past works a lot of effort has been made to understand the basic properties of indistinguishable photons. Theoretical studies of photons [2] and experimental realisations with photons created by atom-cavity systems [3] showed that apart from the spatial and polarisation overlap of the photon also the quality of the wavepackets plays an important role. Especially the dephasing and the jitter of the arrival time of the wavepackets is essential. Similar studies were performed on photons generated in consecutive pulses from a single quantum dot [4] and on photons originating from two different quantum dot devices [5]. Although these studies showed the negative influence of dephasing on the outcome of the experiment, due to the p-shell excitation used, they could not eliminate the jitter in the excitation process.

We performed resonant excitation of a quantum dot using a two-photon transition to the biexciton state. We measured Hong-Ou-Mandel interference with photons generated in successive pulses from a single quantum dot. For comparison we performed the same measurement with the same quantum dot excited above the bandgap, where phonon transitions are needed to relax to the biexciton state. The time uncertainty of this relaxation process introduces a jitter in the excitation process of the biexciton.

The experimental setup is depicted in Figure 1(c). Pulses created from a Ti:Sapphire laser get trimmed in frequency on a pulse shaper for the two-photon excitation. A pump interferometer with a time delay of $\tau = 3.2$ ns $+ \Delta$t creates two pulses per incoming laser pulse. These pulses excite a quantum dot embedded in a planar distributed Bragg reflector cavity, which allows the laser to be guided to the quantum dot. The quantum dot emission is coupled into a single mode fibre after a grating for spectral filtering. It is then directed through an analysing interferometer with a fixed time delay of $\tau_A = 3.2$ ns. Photons from the first excitation pulse, which travel the long path, and photons from the second excitation pulse, which travel the short path overlap at the beamsplitter and coalesce if they are indistinguishable.

Figure 1(a) shows the result of the Hong-Ou-Mandel interference experiment. The dip at zero time delay demonstrates the two-photon interference. The correlation function $g^{(2)}(\tau + \Delta t)$ is calculated from the two-photon time correlation data by dividing the area under the central peak by the mean of the side peak areas. The jitter from the non-resonant excitation process alters the wavepackets from two successive
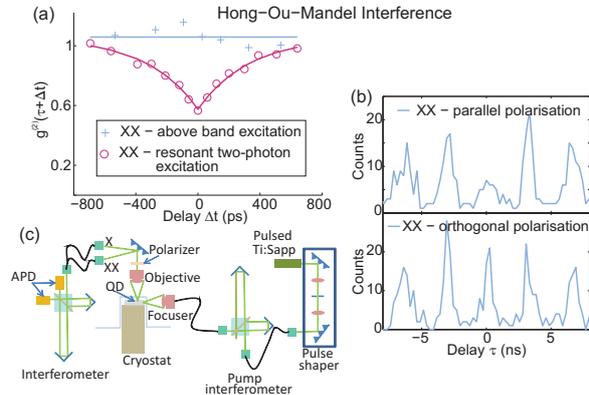
Figure 1: **a:** Results of the Hong-Ou-Mandel interference. The blue crosses are the results for above band excitation. The red circles are the results for resonant two-photon excitation. **b:** recorded data for resonant two-photon excitation for parallel and orthogonal polarisations. **c:** Schematics of the used setup.

pump pulses so that the two-photon interference vanishes. In addition, recharge events, which occur with above band excitation, could cause higher correlations. The above band excitation data is best fit by a constant $y = 1.06(5)$. The two-photon excitation process was fitted with a function of the form $y = a \cdot (1 - be^{-|x|/c})$, where a is a norming constant taking a non perfect beamsplitter into account, b is the dip depth and c is the width of the dip, corresponding to the lifetime of the excited state [4]. The fit gives $a = 1.04(6)$, $b = 0.45(3)$ and $c = 303 \pm 28$ ps.

This results show that not only the dephasing of the wavepackets but also the jitter in the excitation process can alter the quality of the indistinguishability of photons.

References

[1] E. Knill, R. Laflamme, and G. Milburn, Nature **409**, 46 (2001)

[2] T. Legero, T. Wilk, A. Kuhn, and G. Rempe, Appl. Phys. B **77**, 797 (2003)

[3] T. Legero, T. Wilk, M. Hennrich, G. Rempe, and A. Kuhn, PRL **93**, 070503 (2004)

[4] C. Santori, D. Fattal, J. Vučković, G. S. Solomon, and Y. Yamamoto, Nature **419**, 594 (2002)

[5] E. B. Flagg, A. Muller, S. V. Polyakov, A. Ling, A. Migdall, and G. S. Solomon, Proc. SPIE **7948**, 794818 (2011)

Coherent creation of a single photon cascade in a quantum dot to generate time-bin entangled photon pairs

Harishankar Jayakumar[1], **Ana Predojevic**[1], **Tobias Huber**[1], **Thomas Kauten**[1], **Glenn S. Solomon**[2] and **Gregor Weihs**[1]

[1]*Institute for Experimental Physics, University of Innsbruck, Technikerstrasse 25, 6020 Innsbruck, Austria*
[2]*Joint Quantum Institute , National Institute of Standards and Technology and University of Maryland, Gaithersburg, MD 20849, USA*

Time-bin entangled photons produced via parametric down conversion [1] have been used successfully to implement quantum information protocols. This type of entanglement in time can also be generated with the biexciton-exciton cascade in a quantum dot [2]. The main advantage with single emitters like quantum dots is that, multiple pair creation in an excitation pulse can be avoided. The critical aspect in the implementation is to coherently create a biexciton in a quantum dot such that no information about the creation is available to the quantum dot environment.

Here we present the successful demonstration of coherently creating a biexciton through resonant two-photon excitation [3] in an InAs quantum dot embedded in a planar microcavity. Orthogonal excitation-collection geometry, presence of a large biexciton binding energy and the microcavity result in the generation of deterministic, laser-scattering-free cascaded single photons that can be efficiently coupled into single mode optical fibers.
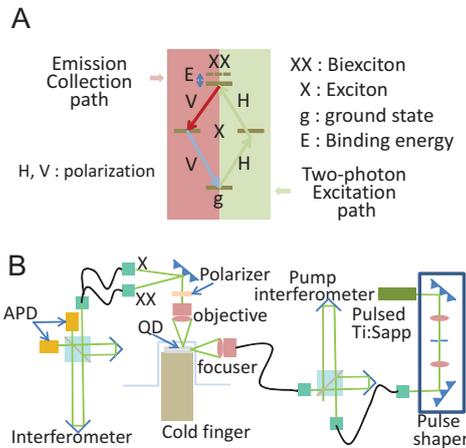
Figure 1: A: Excitation scheme. B: Experimental setup

Experimental setup

Self-assembled quanutm dots(SAQD) embedded in a DBR microcavity were cooled to 5K in a helium flow cryostat. picosecond pulsed laser tuned to be in degenerate two-photon resonance with the biexciton energy of the SAQD (Fig.1 A) was sent through a pulse shaper for spectral filtering. The filtered laser beam was focused on the cleaved edge of the sample to excite the SAQD through the wave guiding mode of the microcavity. Emitted photons were collected by a microscope objective from the sample surface in an orthogonal geometry. Exciton and biexciton photons were coupled into separate single mode fibers. The pump interferometer shown

in Fig.1 B creates two phase locked pulses and the second interferometer is used to analyze the time-bin entangled photons.
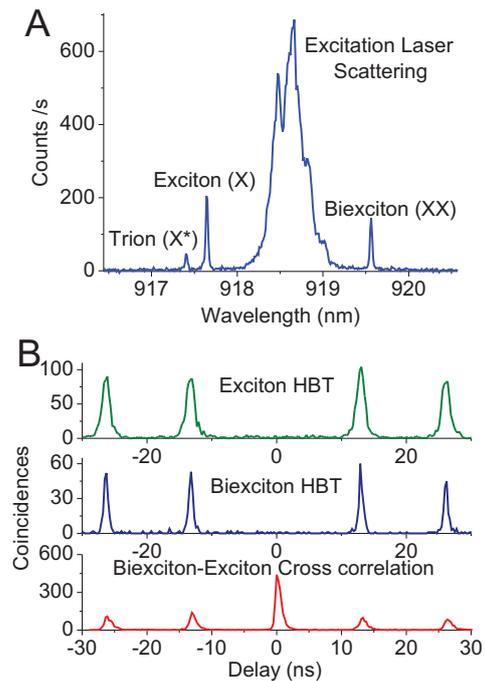
Figure 2: A: Photoluminescence spectrum. B: Correlation measurements

Results

Fig.2 A shows the photoluminescence from the quantum dot following a two-photon excitation. Hanbury Brown and Twiss measurements shown in Fig.2 B have complete two-photon suppression at zero delay. Cross-correlation between biexciton and exciton photons shows bunching at zero delay indicating a cascaded emission. Rabi oscillation of the biexciton state occupation was also observed.

Biexciton and exciton photons generated will be tested for time-bin entanglement in the analyzing interferometer by recording the coincidences at the output of the interferometer.

References

[1] J. Brendel et. al., Phys. Rev. Lett. 92, 227401 (2004).

[2] C. Simon et al., Phys. Rev. Lett. 94, 030502 (2005).

[3] T. Flissikowski et. al., Phys. Rev. Lett. 92, 227401 (2004).

Paramagnetic Kerr-type $\chi^{(3)}$ Nonlinearity in a Highly Pure Ultra-Low Loss Cryogenic Sapphire Microwave Whispering Gallery Mode Resonator

Daniel L. Creedon[1], Karim Benmessai[1], Warwick P. Bowen[2], Michael E. Tobar[1]

[1]*ARC Centre of Excellence for Engineered Quantum Systems, University of Western Australia, 35 Stirling Highway, Crawley WA 6009, Australia*
[2]*ARC Centre of Excellence for Engineered Quantum Systems, University of Queensland, St. Lucia QLD 4072, Australia*

Recent years have seen the development of a 3-level Whispering Gallery mode maser based on residual Fe^{3+} ions in the most pure samples of ultra-low loss HEMEX sapphire[1] [2]. We report that pumping with a single frequency ω_{12} between only the lower two energy levels in the maser scheme results in a hyperfine lattice interaction with relaxation times on the order of several seconds, and output signals consequently measured at $\omega_{12} - \Delta\omega$ and $\omega_{12} + \Delta\omega$ ($\Delta\omega = 7.667$ MHz). We show that the behaviour can be described as a degenerate four-wave mixing (FWM) process due to a third-order $\chi^{(3)}$ magnetic nonlinearity associated with the presence of order 10^{16} paramagnetic spins within the lattice[3] . We determine that the nonlinear coefficient of the system is extremely small, of order a few by 10^{-15} Hz/photon. The system is uniquely suited to a host of quantum measurement and control applications due to the ultra-low dielectric loss tangent of sapphire at low temperature [4], excellent microwave tunability, and a strong effect due to the nonlinearity from a mere 150 parts-per-billion concentration of paramagnetic ions.

Typically four-wave mixing is induced by the application of two source fields, one at ω_{12} and another at ω_{-}. In our experiments only a single pump frequency ω_{12} was actively applied, and the origin of the ω_{-} field was the indirect and inefficient excitation of a WG mode at a lower frequency through a slow cross-relaxation and hyperfine interaction. Further to these experiments, we implemented a classical four-wave mixing scheme with the injection of two pump frequencies, which resulted in the generation of a microwave comb with a repetition rate $\Delta\omega = 7.668$ MHz, due to each signal of the FWM acting as a source field for further mixing. When pumped at 12.037 GHz and 12.029 GHz, the resultant signal at 12.045 GHz had a dramatically increased output power indicating vastly improved quantum conversion efficiency. Figure 1 shows the output of a comb of four-wave mixing signals, whose power effectively maps the ESR bandwidth of the Fe^{3+} impurities. Of particular interest is the generation of four-wave mixing when pumped at 12.037 GHz and 12.045 GHz, noting that no WG mode or cavity resonance exists at the latter frequency. We anticipate that in this case, the difference frequency of $\Delta\omega$ is generated within the crystal, which then allows the generation of photons at 12.029 GHz which are resonantly enhanced by a WG mode, and efficient four-wave mixing can take place. This was tested, and excitation of the comb is possible by pumping at any one of the ω_{-}, ω_{12} or ω_{+} frequencies, in addition to the $\Delta\omega$ frequency at 7.668 MHz, albeit with much lower conversion efficiency. The frequency stability of the repetition rate of the comb was found to exceed that of a commercial Hydrogen maser. The instability relative to the excitation frequency was of order 2×10^{-15} at 100 seconds of integration.
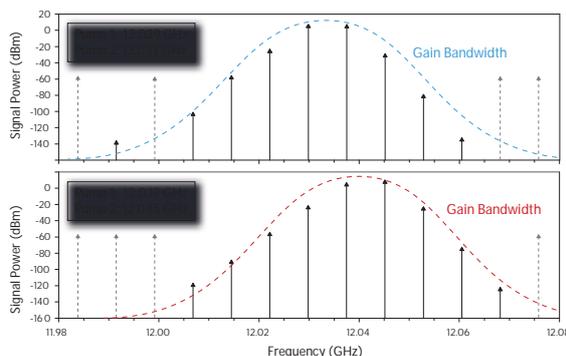
Figure 1: Measured spectrum of signals as a result of a classical doubly pumped four-wave mixing scheme.

Our recent investigations are focused on the milliKelvin properties of the Paramagnetic resonance in sapphire as well as its dependence on magnetic field. We observe a classical mode splitting that mimmics strong coupling due to gyrotropic paramagnetic susceptibility [5] that turns degenerate standing waves into non-degenerate travelling waves. An update of this work will be presented at the conference.

References

[1] Bourgeois, P. Y., Bazin, N., Kersalé, Y., et al., "Maser oscillation in a whispering-gallery-mode microwave resonator," *Applied Physics Letters* **87**, 224104 (2005).

[2] Benmessai, K., Creedon, D. L., Tobar, M. E., et al., "Measurement of the fundamental thermal noise limit in a cryogenic sapphire frequency standard using bi-modal maser oscillations," *Physical Review Letters* **100**, 233901 (2008).

[3] Creedon, D. L., Benmessai, K., Bowen, W., Tobar, M. E., "Four-Wave Mixing from Fe^{3+} Spins in Sapphire," *Physical Review Letters* **108**, 093902 (2012).

[4] Creedon, D. L., Reshitnyk, Y., Farr, W., Martinis, J. M., Duty, T. L., and Tobar, M. E., "High Q-factor sapphire whispering gallery mode microwave resonator at single photon energies and milli-Kelvin temperatures," *Applied Physics Letters* **98**(22), 222903 (2011).

[5] Benmessai, K., Tobar, M. E., Bazin, N., et al., "Creating traveling waves from standing waves from the gyrotropic paramagnetic properties of Fe^{3+} ions in a high-q whispering gallery mode sapphire resonator," *Physical Review B* **79**, 174432 (2009).

Showing the genuine tripartite energy-time entanglement of photon triplets produced by cascaded down-conversion

L. K. Shalm[1], D. R. Hamel[1], Z. Yan[1], C. Simon[2], K. J. Resch[1], and T. Jennewein[1]

[1]*Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, Canada*

[2]*Institute for Quantum Information Science and Department of Physics and Astronomy, University of Calgary, Canada*

Tripartite entanglement is interesting for fundamental tests of quantum mechanics, as well as for quantum information processing. Only recently has it been possible to produce photon triplets directly by cascaded spontaneous down-conversion (C-SPDC) [1]. A striking feature of these photon triplets is that they should be energy-time entangled, in what can be seen as a three particle extension of an EPR state.

Here, we show an experimental verification of the energy-time correlations of photon triplets produced by C-SPDC [2]. To do this, we construct a set of new entanglement criteria, inspired by uncertainty relations developed by van Loock and Furusawa [3]. While their uncertainty relations test whether a tripartite state is fully inseparable, our new criteria detect the presence of genuine tripartite entanglement. They consist of the following set of uncertainty relations:

$$[\Delta(t_2 - t_1) + \Delta(t_3 - t_1)] \Delta(\omega_1 + \omega_2 + \omega_3) \geq 1$$
$$[\Delta(t_2 - t_1) + \Delta(t_3 - t_2)] \Delta(\omega_1 + \omega_2 + \omega_3) \geq 1$$
$$[\Delta(t_3 - t_2) + \Delta(t_3 - t_1)] \Delta(\omega_1 + \omega_2 + \omega_3) \geq 1$$
$$[\Delta(t_2 - t_1) + \Delta(t_3 - t_1) + \Delta(t_3 - t_2)] \times$$
$$\Delta(\omega_1 + \omega_2 + \omega_3) \geq 2.$$

Violating any of these inequalities ensures that a system is genuinely tripartite entangled.
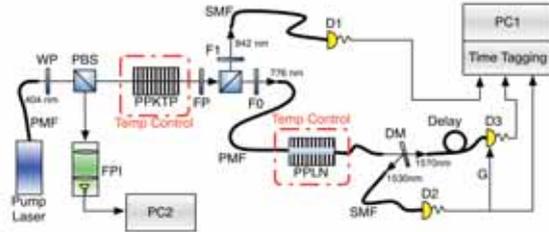
Figure 1: Experimental setup

The photon triplets are produced following the method developed by Hübel in al. [1], as shown in Fig. 1. A 404 nm grating stabilized diode laser, with a 5 MHz bandwidth, is used to pump a PPKTP crystal, producing photon pairs at 842 nm and 776 nm. The 776 nm photons are sent to a PPLN crystal, where they can be down-converted into photons at $\sim$1530 nm and $\sim$1570 nm. The 842 nm photons are detected using a standard silicon avalanche photodiode. The 1530 nm photons are detected using a free running negative feedback avalanche diode (NFAD) [4], the signal of which triggers a gated InGaAs detector to detects the 1570 nm photon.

The detection times are recorded as time tags, so that the time difference between any pair of photon detections can be calculated. This allows us to measure all of the $\Delta(t_i - t_j)$

terms of the inequalities. For the other term, which deals with the uncertainty in the sum of the frequencies, we take advantage of the fact that energy is conserved in SPDC. Therefore, we have that:

$$\Delta\omega_p = \Delta(\omega_1 + \omega_2 + \omega_3),$$

which is a quantity that can be measured. We do this by continuously monitoring the bandwidth of the pump laser during the entire experiment, using a scanning Fabry-Perot interferometer.
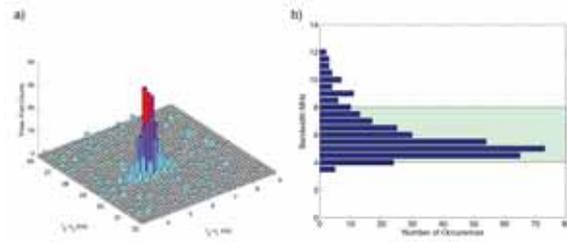
Figure 2: a: 2d histogram of photon detection time differences b: Histogram of laser bandwidths.

The results are shown in Fig. 2. Substituting the measured values for the different uncertainties in the inequalities gives:

$$[\Delta(t_2 - t_1) + \Delta(t_3 - t_1)] \Delta(\omega_1 + \omega_2 + \omega_3) = 0.03 \pm 0.01$$
$$[\Delta(t_2 - t_1) + \Delta(t_3 - t_2)] \Delta(\omega_1 + \omega_2 + \omega_3) = 0.02 \pm 0.01$$
$$[\Delta(t_3 - t_2) + \Delta(t_3 - t_1)] \Delta(\omega_1 + \omega_2 + \omega_3) = 0.018 \pm 0.005$$
$$[\Delta(t_2 - t_1) + \Delta(t_3 - t_1) + \Delta(t_3 - t_2)] \times$$
$$\Delta(\omega_1 + \omega_2 + \omega_3) = 0.03 \pm 0.01.$$

In all cases, we find that the uncertainty products are clearly much lower than the bounds, confirming that the C-SPDC process produces photon triplets that are genuinely tripartite entangled. This is the first demonstration of continuous variable entanglement of three individual photons, and leads to interesting directions for quantum information processing and for fundamental tests of quantum entanglement.

References

[1] H. Hübel et al., Nature, **466**, 601 (2010).

[2] L. K. Shalm et al., arXiv:1203.6315v1 (2012).

[3] P. van Loock and A. Furusawa, Phys. Rev. A **67**, 052315 (2003).

[4] Z. Yan et al., arXiv:1201.2433v2 (2012).

Deterministic linear-optics quantum computing based on a hybrid approach

Seung-Woo Lee and Hyunseok Jeong

Center for Macroscopic Quantum Control, Department of Physics and Astronomy, Seoul National University, Seoul, 151-742, Korea

We propose a novel scheme for all-optical quantum computation using hybrid qubits. It enables one to efficiently perform universal linear-optical gate operations in a simple and near-deterministic manner using hybrid entanglement as offline resources.

Our scheme combines advantages of two well known previous approaches. The linear optics quantum computation (LOQC) scheme [1] uses the horizontal and vertical polarization states, $|H\rangle$ and $|V\rangle$, as a qubit basis. A major difficulty in this approach is that two-qubit gates are nondeterministic, while single-qubit operations are straightforward. An alternatively approach, the coherent-state quantum computation (CSQC) [2, 3], employs two coherent states, $|\alpha\rangle$ and $|-\alpha\rangle$ with amplitudes $\pm\alpha$ as a qubit basis. Using this encoding scheme, the Bell-state measurement can be performed in a near-deterministic manner [4]. However, single qubit rotations produce cumbersome errors due to the nonorthogonality between $|\alpha\rangle$ and $|-\alpha\rangle$ [5]. It was found that the CSQC is relatively more resource-efficient than LOQC, but it suffers smaller fault-tolerance thresholds [5].

In our approach, the orthonormal basis to define optical hybrid qubits is $\{|0_L\rangle = |+\rangle|\alpha\rangle,\ |1_L\rangle = |-\rangle|-\alpha\rangle\}$, where $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$. The Z-basis measurement can be performed by a single measurement on either of the two physical modes. It can be done on the single-photon mode by a polarization measurement on the basis $|+\rangle$ and $|-\rangle$, or on the coherent-state mode using an ancillary coherent state [2].

In order to construct a universal set of gate operations, Pauli X, arbitrary Z (phase) rotation, Hadamard, and controlled-Z (CZ) gates suffice. The Pauli X operation can be performed by applying a bit flip operation on each of the two modes. The bit flip operation on the single-photon mode, $|+\rangle \leftrightarrow |-\rangle$, is implemented by a polarization rotator, and the operation on the coherent-state mode, $|\alpha\rangle \leftrightarrow |-\alpha\rangle$, by a π phase shifter. An arbitrary Z rotation ($\hat{Z}_\theta$) is performed by applying the phase shift operation only on the single-photon mode: $\{|+\rangle,\ |-\rangle\} \to \{|+\rangle,\ e^{i\theta}|-\rangle\}$, and no operation is required on the coherent-state mode. This is a significant advantage over CSQC in which Z rotations are highly nontrivial and cause a heavy increase of the circuit complexity [5].

A teleportation protocol is required to perform Hadamard and CZ operations. Using our approach, teleportation can be performed in a simple and near-deterministic manner. This is an extremely difficult task in the framework of LOQC [1]. It is also difficult in CSQC due to the difficulty in performing deterministic Z rotations, which is the cost of using a non-orthogonal qubit basis [5]. A maximally entangled state, $|\Psi_C\rangle \propto |0_L\rangle|0_L\rangle + |1_L\rangle|1_L\rangle$, in the hybrid basis can be used as a quantum channel for teleportation. As depicted in Fig. 1, the Bell measurement for an optical hybrid qubit can be performed using two smaller Bell measurement units, B_α and B_{II}. B_α discriminates between four Bell states in the coherent-state representation using a 50:50 beam split-

ter and two photon number parity measurements with success probability $\exp(-2|\alpha|^2)$ [4], while B_{II} identifies two of the Bell states in the single-photon encoding part using three polarization beam splitters and four on-off photodetectors with success probability 1/2 [6]. The whole teleportation process for a hybrid qubit is successful when at least one of B_α and B_{II} succeeds. This leads to the failure probability of $P_f = \exp(-2|\alpha|^2)/2$, which outperforms the previous schemes that require massive overheads with repetitive applications of teleporters [1, 5]. For example, 99% success rate of teleportation is achieved by encoding with $\alpha = 1.4$.

We have considered photon losses which are the major error source in optical quantum computation, and performed a numerical analysis for error thresholds using the 7-qubit STEANE code. Considering both the resource requirements and error thresholds, our scheme outperforms the previous ones when the amplitude is chosen to be $\alpha \approx 1$. The resource requirement is only $\sim 1/20$ times that of LOQC and the noise threshold ($\sim 6 \times 10^{-4}$) is also significantly improved over that of CSQC ($\sim 2 \times 10^{-4}$). Entangled states in the form of $|H\rangle|\alpha\rangle + |V\rangle|-\alpha\rangle$ are required as off-line resources for our scheme. Such entangled states can be generated either using weak nonlinearity or using photon addition and subtraction. Our scheme paves an efficient way to the realization of scalable optical quantum computation.
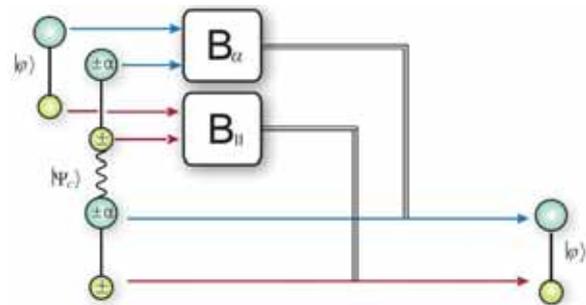
Figure 1: Schematic of teleportation protocol for an unknown hybrid qubit $|\varphi\rangle = a|+\rangle|\alpha\rangle + b|-\rangle|-\alpha\rangle$.

References

[1] E. Knill *et al.*, Nature **409**, 46 (2001).

[2] H. Jeong and M. S. Kim, Phys. Rev. A **65**, 042305 (2002).

[3] T. C. Ralph *et al.*, Phys. Rev. A **68**, 042319 (2003).

[4] H. Jeong *et al.*, Phys. Rev. A **64**, 052308 (2001).

[5] A. P. Lund *et al.*, Phys. Rev. Lett. **100**, 030503 (2008).

[6] J. Calsamiglia and N. Lütkenhaus, App. Phys. B **72**, 67 (2001).

Activation of Bound Entanglement in a Four-Qubit Smolin State

__Fumihiro Kaneda__[1], Ryosuke Shimizu[1,2], Satoshi Ishizaka[3], Yasuyoshi Mitsumori[1], Hideo Kosaka[1] and Keiichi Edamatsu[1]

[1]*Research Institute of Electrical Communication, Tohoku University, Sendai, Japan*
[2]*Center for Frontier Science and Engineering, University of Electro-Communications, Tokyo, Japan*
[3]*Graduate School of Integrated Arts and Sciences, Hiroshima University, Higashi-Hiroshima, Japan*

Entanglement, one of the most counterintuitive effects in quantum mechanics, is essential to quantum information processing (QIP). For efficient QIP, pure and strong entanglement has been thought to be indispensable. In contrast, there is a class of entanglement in mixed states, referred to as bound entanglement [1], which cannot be distilled into pure entanglement by means of local operations and classical communication (LOCC). In spite this "bound" property, it has been demonstrated that a certain class of bound entanglement can be distilled when two of the parties coming together ("unlocking") [2, 3]. Also, it was theoretically pointed out that two independent bound entangled states can cooperatively distill the entanglement. The process is called "superactivation" [4]. These interesting properties of the bound entangled states have attracted attention in QIP applications, e.g., remote information concentration [5]. Here, we experimentally demonstrate the "activation" [6] of the bound entanglement from the Smolin state encoded in photon polarizations.

In order to demonstrate the activation of the bound entanglement, we used the scheme shown in Fig. 1. In this scheme, the four qubits in the Smolin state ρ_s are shared by parties A, B, C, and D. In addition, B and C share another pair of qubits in the Bell state $|\psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$. When the qubits in B and C are projected onto one of the Bell states by the Bell state measurement (BSM), the qubits owned by A and D turn to be entangled with each other. Thus, the entanglement in the additional Bell state is transferred into the entanglement between A and D by LOCC. In other words, the bound entanglement between A and B that is undistillable by itself is activated with the help of the Bell state in other parties. This is strong contrast to the bound entanglement unlocking [2, 3] which requires non-local joint operations of qubits.

In the experiments of the activation of its bound entanglement, we need to simultaneously prepare the Smolin state and the Bell state, i.e., six-photon states. For the six-photon source, we used spontaneous parametric down conversion (SPDC) generated from three type-II β-barium borate (BBO) crystals pumped by the third harmonics (λ= 343 nm) of the mode-locked Yb laser [7]. The pump source has higher pulse energy ($\sim$ 50 nJ) than those of typical multi-photon generation systems based on the second harmonics of Ti-Sapphire lasers. Each BBO crystal produces a photon-pair in the Bell state at 686 nm, where the quantum efficiencies of our single-photon detectors are around the maximum ($\sim$65%). In our experimental setup, the four- and six-photon counting rate was 200 /sec and 0.9 /sec. The Smolin state was prepared by the synchronous modulation of a pair of $|\psi^+\rangle$ states using four liquid crystal variable retarders [3]. The density matrices of the generated Smolin state ρ_s^{exp} and the two-qubit state after the activation process ρ_{AD} were reconstructed by the state tomography.
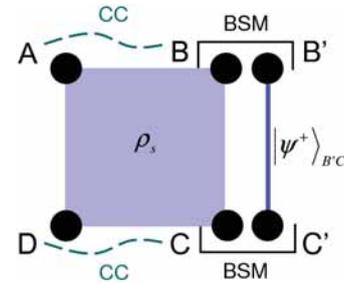
Figure 1: The scheme of the activation of the bound entanglement in the Smolin state ρ_s. BSM; the Bell state measurement, CC; Classical Channel.

We first characterized the obtained density matrix of the Smolin state ρ_s^{exp}. The fidelity of ρ_s^{exp} to that of the ideal Smolin state ρ_s was calculated to be 0.82. We then evaluated the separability of the generated state across the two-two bipartite cuts in terms of the relative entropy of entanglement (REE) [8] which quantifies the upper bound of the distillable entanglement. The values of the REE at the bipartite cuts AB|CD, AC|BD, and AD|BC were calculated to be 0.03, 0.08, and 0.07, respectively. This indicates that ρ_s^{exp} has almost no distillable entanglement as we expect for the Smolin state whose REE values are zero for any two-two bipartite cuts. Then, we have experimentally confirmed the activation of the bound entanglement making a comparison between the distillable entanglement of the state before (ρ_s^{exp}) and after (ρ_{AD}) the activation process.

References

[1] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. Lett. **80** , 5329 (1998).

[2] J. A. Smolin, Phys. Rev. A **63**, 032306 (2001).

[3] E. Amselem, M. Bourennane, Nature Physics. **5**, 748 (2009), J. Lavoie, R. Kaltenbaek, M. Piani, K. J. Resch, Phys. Rev. Lett. **105**, 130501 (2010).

[4] P. Shor, J. Smolin, A. Thapliyal, Phys. Rev. Lett. **90**, 107901 (2003).

[5] M. Murao, V. Vedral, Phys. Rev. Lett. **86**, 352 (2001) .

[6] P. Horodecki, M. Horodecki, R. Horodecki, Phys. Rev. Lett. **82** 1056 (1999).

[7] F. Kaneda, R. Shimizu, Y. Mitsumori, H. Kosaka, K. Edamatsu, Progress in Informatics **8**, 27 (2011).

[8] L Henderson and V Vedral, Phys. Rev. Lett. **84**, 2263 (2000).

Heralded noiseless amplification of a polarization-encoded qubit

Sacha Kocsis[1], **Guoyong Xiang**[1,2], **Tim C. Ralph**[3] and **Geoff J. Pryde**[1]

[1]*Centre for Quantum Computation and Communication Technology, Centre for Quantum Dynamics, Griffith University, Brisbane 4111, Australia*
[2]*Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, China*
[3]*Centre for Quantum Computation and Communication Technology, Department of Physics, University of Queensland, Brisbane 4072, Australia*

Photons are the best long-range carriers of quantum information, but the unavoidable absorption and scattering of photons in a transmission channel places a serious limitation on the distance over which quantum communication protocols are viable. Signal amplification will therefore be an essential feature of quantum technologies. But the well known no-cloning theorem [1], and the minimum noise cost for deterministic amplification of a quantum state [2], imply that there are unique challenges to amplifying a quantum signal.

Nondeterministic noiseless amplification of a small coherent state has previously been achieved using various approaches [3, 4, 5, 6]. These results demonstrated the noiseless linear amplification of a single mode quantum state, with a potential application to entanglement distillation in quantum repeaters, for example.

Here, we construct a two mode amplifer, to demonstrate the first heralded noiseless linear amplification of a qubit encoded in the polarization state of a single photon. This promises to extend the range of quantum communication protocols to which the amplification of a quantum signal can be applied. Since the recent successful hacking of prototype QKD systems [7], device independent QKD (DIQKD) has generated enormous interest, as it promises to close QKD's first proven security breach. Recently, it has been theoretically shown that a qubit amplifier can enable DIQKD over appreciable distances [8].

The qubit amplifier consists of two mode amplifiers in series (Fig. 1), which are themselves based on the generalized quantum scissors [9]. We double pass 100 mW of 390 nm light through a 2 mm BBO crystal, to obtain two pairs of degenerate unentangled photons from spontaneous parametric down-conversion (SPDC). Three of the single photons are used directly in the circuit, and the last photon is used as an external trigger. The variable reflectivity η of a beam splitter in an amplifier stage (we use a half-wave plate and polarizing beam splitter to create a variable reflectivity beamsplitter) determines the amplitude gain g at the output. One single photon (the "input") passes through an initial beam splitter with high reflectivity, to simulate a very lossy channel. The resulting mixed state ρ_{in} consists of a large vacuum component and a small single photon component ($\gamma_0 > \gamma_1$):

$$\rho_{in} = \gamma_0|0\rangle\langle0| + \gamma_1|\psi_1\rangle\langle\psi_1| \qquad (1)$$

The polarization qubit $|\psi_1\rangle$ exists in the single photon subspace:

$$|\psi_1\rangle = \alpha|1_H\rangle + \beta|1_V\rangle \equiv \alpha|H\rangle + \beta|V\rangle \qquad (2)$$

The V and H polarizations are amplified separately, conditional on detection of one photon in either $D1$ or $D2$ (but not
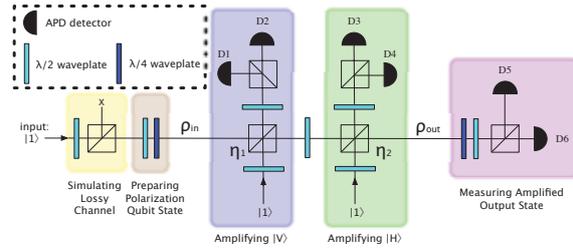
Figure 1: Two single-mode amplifier stages arranged in series to make a qubit amplifier. Half-wave plates and polarizing beam splitters set variable reflectivities η_1 and η_2, which determine the gains from the two amplifier stages. The total gain g is taken to be the average of the two individual gain factors.

both) for V, and in either $D3$ or $D4$ for H. At the end, the two polarizations are coherently recombined to recover the qubit. The expected output, ρ_{out}, is a mixed state with a relatively smaller vacuum component, as a result of the amplification:

$$\rho_{out} = \gamma_0'|0\rangle\langle0| + g^2\gamma_1|\psi_1\rangle\langle\psi_1| \qquad (3)$$

The gain factor $g^2 = (1 - \eta)/\eta > 1$, with $\eta_1 = \eta_2 = \eta$.

We collected preliminary data for a state size $\gamma_1 = 0.12$. For a state of this size, saturation of the gain will be observed, which arises from the imperfect delivery of ancilla photons to the circuit. For a nominal gain of $g^2 = 4$, we therefore measure an actual gain of $g_m^2 \simeq 2.6$. For these parameters, the average fidelity between the amplified output qubit and the ideal qubit was measured to be 88%. We believe that the small amount of mixture in the qubit subspace of the output state is due to higher order effects in our single photon source, and imperfect quantum interference in the second amplifier stage.

The fidelity between the original state, ρ_{in}, and the ideal qubit state, $|\psi_1\rangle$, was compared to the fidelity between the measured output state ρ_{out}' and $|\psi_1\rangle$. This fidelity increased from $\langle\psi_1|\rho_{in}|\psi_1\rangle = 0.12$ to $\langle\psi_1|\rho_{out}'|\psi_1\rangle \simeq 0.23$, where both fidelities are averaged over the canonical basis states. This demonstrates that the qubit amplifier has significantly improved the signal to noise ratio in a lossy channel. As increasingly efficient single photon generation and delivery techniques are developed, it will become possible to achieve much larger coefficients $g_m^2\gamma_1$, resulting in very pure single photons in future realizations based on this protocol.

References

[1] Wootters, W. K. & Zurek, W. H., *Nature* **299**, 802-803 (1982).
[2] Caves, C. M., *Phys. Rev. D* **23**, 1693-1708 (1981).
[3] Xiang, G. Y. *et al.*, *Nature Photon.* **4**, 316-319 (2010).
[4] Ferreyrol, F. *et al.*, *Phys. Rev. Lett.* **104**, 123603 (2010).
[5] Zavatta, A., Fiurasek, J., & Bellini, M., *Nature Photon.* **5**, 52-56 (2010).
[6] Usuga, M. A. *et al.*, *Nature Phys.* **6**, 767-771 (2010).
[7] Lydersen, L. *et al.*, *Nature Photon.* **4**, 686-689 (2010).
[8] Gisin, N., Pironion, S. & Sangouard, N., *Phys. Rev. Lett.* **105**, 070501 (2010).
[9] Pegg, D. T., Phillips, L. S., & Barnett, S. M., *Phys. Rev. Lett.* **81**, 1604-1606 (1998).

Quantum Interference of Independently Generated Telecom-band Single Photons

Monika Patel,[1] **Joseph B. Altepeter,**[2] **Yu-Ping Huang,**[2] **Neal N. Oza,**[2] **and Prem Kumar**[1,2]
Center for Photonic Communication and Computing,
[1]*Department of Physics and Astronomy,* [2]*Department of Electrical Engineering and Computer Science,*
Northwestern University, 2145 Sheridan Road, Evanston, IL 60208-3118, USA

We report on heralded generation of pure single photons in the 1310-nm telecom O-band using standard single-mode fibers. High spectral purity is demonstrated via measurement of Hong-Ou-Mandel (HOM) interference between such photons produced in two pieces of spatially-separated fibers that are pumped by laser pulses with no mutual phase coherence. The experimental data are shown to agree well with the results of simulations using a quantum multimode theory that takes into account noises due to multi-pair generation and Raman scattering, without the need for any fitting parameter.

The experimental setup is sketched in Fig. 1. The pump is generated in a 10-GHz hybrid mode-locked laser (U2T, model TMLL1310) whose output is pulse-picked at 50-MHz rate using an amplitude modulator. After power boost in a fiber amplifier, the pump pulses are split at a 50:50 fiber splitter and sent to two separate fiber paths. By inserting an extra piece of fiber in one path, a relative time delay between the split pulses is introduced. These pulses then separately generate signal-idler photon pairs via spontaneous four-wave mixing in two different standard single-mode fiber spools [1]. The generated signal photons from the two spools separately pass through a fiber polarization controller (FPC) and a filter, before being combined at a 50:50 fiber coupler. Using the FPCs and by careful path matching, the signal photons from the two spools are aligned to be identical with each other in all degrees of freedom: polarization, spectral, and temporal. The 50:50-coupler outputs are then detected by two InGaAs single-photon detectors (NuCrypt LLC, model CPDS-4). Two additional such detectors are used to detect the idler photons emerging directly from the filters. A variable delay stage is used to change the temporal overlap of the signal photons, while fourfold coincidence counts are recorded to form a HOM interference pattern between the signal photons heralded by the idler photons.
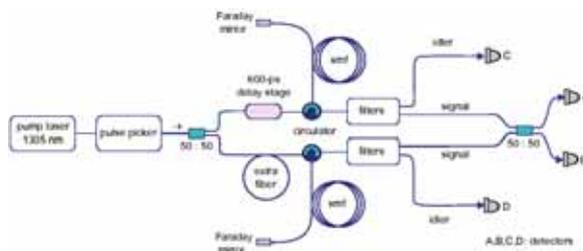
Figure 1: Experimental layout for measuring quantum interference between heralded single photons produced from mutually incoherent pump pulses in separate fiber spools.

To ensure that the single photons are created from independent pump pulses, we measure the phase coherence of the pump pulse train via classical interference in an asymmetric Mach-Zehnder fiber interferometer, with the visibility-versus-delay result shown in Fig. 2. As seen, the phase coherence starts to decay almost immediately with the visibility dropping to 50% at a time delay of 17 pulse periods. It approaches zero at a delay of about 90 pulse periods, where independent generation of single photons in the two fiber spools is achieved. In our experiment, we recorded fourfold coincidence counts for various time delays between the signal photons, ranging from zero to 1000 pulse periods (100 ns), from which the HOM visibility is determined (see Fig. 2 inset for a typical interference pattern). As shown in Fig. 2, the measured HOM visibility ($76.4\% \pm 4.2\%$) remains unchanged within error limits for all time delays. These results confirm that (a) highly pure single photons are produced in our experiment (HOM visibility much greater than 50%) and (b) the single photons produced from distinct pump pulses with no mutual phase coherence interfere with as high a visibility as those produced from the same pump pulse (case with 0 time delay). We note that the experimental results are in good agreement with those predicted by our theory using no fitting parameters [2].
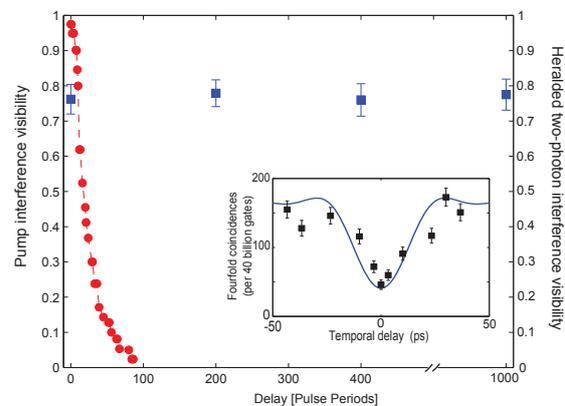
Figure 2: Pump interference visibility and heralded two-photon-interference visibility plotted as a function of pump pulse delay. Inset: a typical HOM interference pattern, shown for measured (scatters) and predicted (curve) results.

In conclusion, we have observed high-visibility quantum interference between single photons produced independently in spatially separate fiber-based sources at a telecom-band wavelength. Future experiments will involve using separate lasers to pump the two fiber spools.

References

[1] M. A. Hall, et al., Opt. Exp. **17**, 14558 (2009).

[2] Y. -P. Huang, et al., Phys. Rev. A. **82**, 043826 (2010).

Direct fidelity estimation by post-selected C-SWAPs for three photons

Sang Min Lee[1], **Sang-Kyung Choi**[1] and **Hee Su Park**[1]

[1]*Korea Research Institute of Standards and Science, Daejeon 305-340, Republic of Korea*

Controlled-swap (C-SWAP) operations enable a direct estimation of the fidelity of input states from the visibility of an interference pattern. We demonstrate C-SWAPs with linear optics and post-selection of coincidence counting for three input photons generated from double-pass spontaneous parametric down-conversion (SPDC).

A previous theoretical work [1] has shown that nonlinear functions of density matrices can be directly estimated by means of C-SWAPs. In particular, the fidelity $\text{Tr}[\rho_1 \rho_2 \cdots \rho_m]$ of density matrices $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_m$ can be evaluated by measuring the visibility of the interference pattern produced by C-SWAPs and phase shifting of the control qubit.
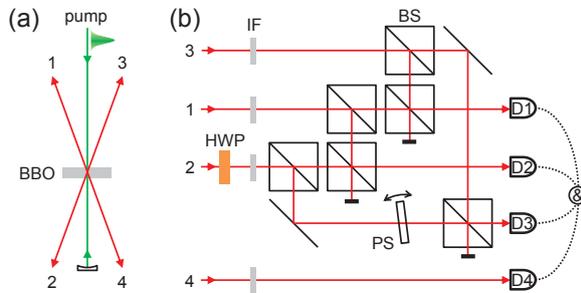
Figure 1: (a) Four photons generated by double-pass SPDC, (b) Scheme of post-selected C-SWAP operation for three input photons. HWP: half-wave plate, IF: interference filter (5 nm), BS: balanced beam splitter, PS: phase shifter (1mm-thick glass plate), D1~D4: single-mode-fiber-coupled single-photon detectors (PerkinElmer SPCM-AQ4C)

Figure 1 shows our experiment with four input single photons generated by double-pass SPDC. The states of photon 1, 2 and 3 are the input states for C-SWAP, and photon 4 is the trigger. Each input photon is horizontally polarized (the slow axis of the half-wave plate (HWP) is initially horizontal), and passes through an interference filter (IF) with a 5-nm bandwidth followed by a 50:50 beam splitter (BS). A secondary BS combines the transmitting output path from the primary BS for each photon with a reflecting output path from the primary BS for another photon. The post-selected C-SWAP is completed by four-fold coincidence counting with single-photon detectors, where D1~D3 are respectively located at the output paths from the secondary BSs and D4 detects the trigger photon. A successful post-selection corresponds to only two cases, Case T and Case R, where Case T(R) corresponds to all input photons being transmitted(reflected) at the primary BSs. Which case occurs determines whether the successfully detected photons are all shifted to the next detector (Case R) or not (Case T). This operation corresponds to the controlled-shift (C-SHIFT) operation ($m > 2$), which is the generalized version of C-SWAP ($m = 2$) [1].
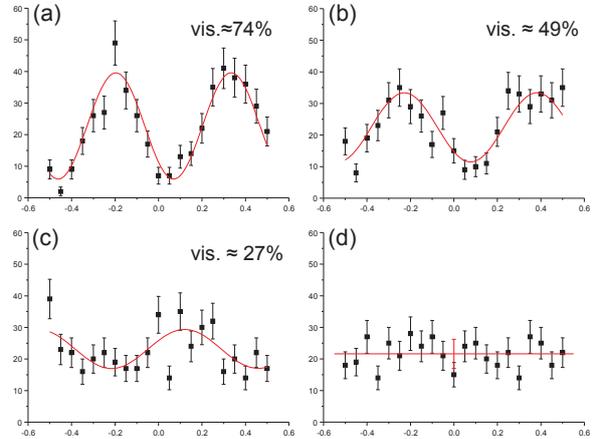
Figure 2: Polarization of input photon 2: (a) Horizontal, (b) 30 deg., (c) 60 deg., (d) Vertical. Y-axis denotes four-fold coincidence counts (/500 s), X-axis denotes displacement of PS (mm).

The fidelity among the input states is equivalent to the visibility of the interference pattern of four-fold coincidence counts generated by varying the phase shifter (PS) located, as shown in Fig. 1 (b), in the lower path for photon 2. The results for four different polarizations of input photon 2 obtained by varying an HWP are shown in Fig. 2. Here, each data point in Fig. 2 represents four-fold coincidence counts in 500 s, and the solid lines are sinusoidal fits to the data. Figure 2 clearly shows the fidelity decreasing with increasing difference of polarization between photon 2 and the other photons. The visibility of less than 1 for Fig. 2 (a) is presumably caused by nonuniform IFs, optical misalignment in the experimental setup, and the mixedness of each input photon state.

The scheme of post-selected C-SWAP shown in Fig. 1 (b) can be extended to an arbitrary number of input photons, provided more BSs and multifold coincidence counting. However, a larger number of input photons leads to lower counting rates because of the lower success probability for post-selection.

References

[1] Artur K. Ekert, Carolina Moura Alves, Daniel K. L. Oi, Michał Horodecki, Paweł Horodecki, and L. C. Kwek, Phys. Rev. Lett., **88**, 217901 (2002).

Experimental realisation of Shor's quantum factoring algorithm using qubit recycling

Enrique Martin-Lopez, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou and Jeremy O'Brien

Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK

Quantum algorithms are computational routines that exploit quantum mechanics to solve problems exponentially faster than the best classical algorithms [1, 2, 3]. Shor's quantum algorithm [4] for fast factoring of composite numbers is a key example and the prime motivator in the international effort to realise a quantum computer. However, due to the large number of resources required, to date, there have been only four small scale demonstrations [5, 6, 7, 8]. Here we address this resource demand and demonstrate a scalable version of Shor's algorithm in which the n qubit control register is replaced by a single qubit that is recycled n times: the total number of qubits is one third of that required in the standard protocol [9]. Encoding the work register in higher-dimensional states, we implement a two-photon compiled algorithm to factor $N = 21$. Significantly, the algorithmic output exhibits structure that is distinguishable from noise, in contrast to previous demonstrations.

The correct algorithmic output from the quantum order finding circuit for factoring $N = 21$ is confirmed by the experimental results with a fidelity of $99 \pm 4\%$ with the ideal probability distribution. The experimental output has a critical dependence on decoherence: phase instability drives the output toward a uniform probability distribution, in contrast with previous experimental demonstrations of Shor's algorithm, all of them for $N = 15$, in which a uniform probability distribution is the expected outcome. We confirmed this analysis experimentally

These results point to larger-scale implementations of Shor's algorithm by harnessing substantial but scalable resource reductions applicable to all physical architectures.

References

[1] R. P. Feynman, Int. J. Thy. Phys. **21**, 467 (1982).

[2] D. Deutsch, Proc. R. Soc. Lond. A **400**, 97 (1985).

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[4] P. W. Shor, Proc. 35th Annu. Symp. Foundations of Computer Science and IEEE Computer Society and Los Alamitos and CA pp. 124-134 (1994), ed. S. Goldwasser.

[5] L. M. K Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature **414**, 883 (2001).

[6] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **99**, 250504 (2007).

[7] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, Phys. Rev. Lett. **99**, 250505 (2007).

[8] A. Politi, J. C. F. Matthews, and J. L. O'Brien, Science **325**, 1221 (2009).

[9] S. Parker and M. B. Plenio, Phys. Rev. Lett **85**, 3049 (2000).

Generation and characterization of EPR beams with a photonic chip

__Genta Masada__[1,2], __Kazunori Miyata__[1], __Alberto Politi__[3], __Jeremy L. O'Brien__[3], __Hiroshi Takahashi__[4] and __Akira Furusawa__[1]

[1]_Department of Applied Physics, School of Engineering, The University of Tokyo, Tokyo, Japan_
[2]_Tamagawa University, Tokyo, Japan_
[3]_University of Bristol, Bristol, U.K._
[4]_NTT Photonics Laboratories, Kanagawa, Japan_

The Einstein-Podolsky-Rosen (EPR)[1] beams, i.e. two mode squeezed vacuum, are essential resources for continuous-variable (CV) quantum teleportation[2] which is one of the most important protocol in CV quantum information processing. An experimental setup of CV quantum teleportation is a complicated optical circuit consisting of a number of mirrors, lenses and beam splitters. The integration of all these optical elements in a single photonic chip is required for both scalability and miniaturization. Here we report the first step toward a fully integrated CV experiment, demonstrating the generation and characterization of EPR beams in a photonic chip where waveguide interferometers are integrated.
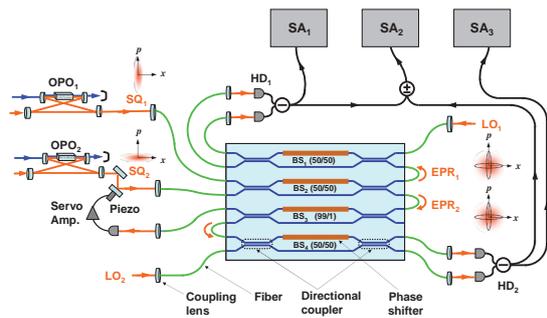
Figure 1: Experimental setup with four waveguide interferometers.

The EPR beams can be generated by combining two squeezed light (SQ) beams by a half beam splitter and characterized by balanced homodyne measurements with local oscillator (LO) beams. Fig.1 shows experimental setup with a chip where waveguide Mach-Zehnder interferometers are integrated[3]. Each interferometer consists of a pair of directional couplers and a phase shifter. The waveguide interferometer can be regarded as a beam splitter (BS) with variable transmission by tuning a relative phase between two arms[4]. BS_1, BS_2, and BS_4 are adjusted as half beam splitters. Two SQ beams at 860nm (SQ_1 and SQ_2) are generated by sub-threshold optical parametric oscillators (OPOs) and combined by BS_2 to generate entangled EPR_1 and EPR_2 beams. BS_1(BS_4) combines EPR_1(EPR_2) and LO_1(LO_2) and is used for balanced homodyne (HD) measurement. In our experiment weak coherent beams are introduced into OPO_1 and OPO_2. 1% of the weak coherent beams is picked up by BS_3 adjusted as 99 to 1 branching ratio and used for phase locking between SQ_1 and SQ_2 at 90 degrees.

Fig.2 (a) and (b) are showing noise levels of both quadra-
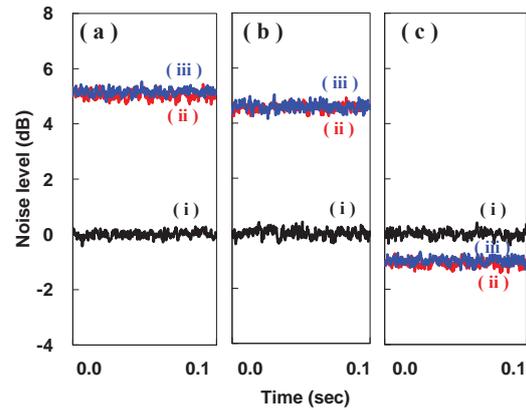
Figure 2: Noise measurement results. (a) and (b) are results on EPR_1 and EPR_2 respectively. (i), (ii) and (iii) represent the vacuum noise level normalized to 0 dB, $\langle\Delta\hat{x}^2\rangle$ and $\langle\Delta\hat{p}^2\rangle$ at each figures. (c) is reslut on the inseparability criterion. (i), (ii) and (iii) represent the noise level without quantum correlation, $\langle[\Delta(\hat{x}_1-\hat{x}_2)]^2\rangle$ and $\langle[\Delta(\hat{p}_1+\hat{p}_2)]^2\rangle$ respectively. Measurement frequency is 1.5 MHz. Resolution bandwidth is 30kHz and video bandwidth is 300Hz. All traces are averaged 20 times.

ture phase amplitudes $\hat{x}$ (ii) and $\hat{p}$ (iii) of EPR_1 and EPR_2 respectively. Fig.2 (c) shows $\langle[\Delta(\hat{x}_1-\hat{x}_2)]^2\rangle$ (ii) and $\langle[\Delta(\hat{p}_1+\hat{p}_2)]^2\rangle$ (iii) which are taken by using a hybrid junction. The results satisfies the inseparability criterion[5][6] of

$$\Delta_{1,2}^2 = \langle[\Delta(\hat{x}_1-\hat{x}_2)]^2\rangle + \langle[\Delta(\hat{p}_1+\hat{p}_2)]^2\rangle = 0.79 < 1. \quad (1)$$

In conclusion we succeeded in generating and characterizing the quantum entanglement by using waveguide interferometers integrated in a chip.

References

[1] A. Einstein _et al._, Phys. Rev. __47__, 777 (1935).

[2] A. Furusawa _et al._, Science, __282__, 706 (1998).

[3] A. Politi _et al._, Science, __320__, 646 (2008).

[4] J.C.M. Matthews _et al._, Nature Photonics __3__, 346 (2009).

[5] L.-M. Duan _et al._, Phys. Rev. Lett., __84__, 2722 (2000).

[6] R. Simon, Phys. Rev. Lett. __84__, 2726 (2000).

Quantum computation with non-Abelian continuous-variable anyons

Darran Milne[1], Natalia Korolkova[1] and Peter van Loock[2]

[1]*School of Physics and Astronomy, University of St.Andrews, North Haugh, St. Andrews, Fife, KY16 9SS, Scotland,*
[2]*Optical Quantum Information Theory Group, Max-Planck Institute for the Science of Light, Günther-Scharowsky-Str.1/Bau 26 and Institute of Theoretical Physics, Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany*

Topological quantum computation has become a highly important area of study in recent years for its potential to store and manipulate quantum information within protected topological degrees of freedom [1, 2]. One of the most important classes of topological models are the lattice models proposed by Kitaev [3]. In these models, quantum systems (e.g. qubits) form a two-dimensional lattice that define a topological surface code with the states of the qubits representing the vacuum or *anyonic* [4] populations. These anyons can be manipulated through braiding and fusion to act on an underlying computational space and hence enact topologically protected quantum gate operations.

Only recently have these ideas been extended to the continuous-variable (CV) regime [5]. In these systems, the Kitaev spin lattices are replaced by lattices composed of CV qumodes. As in the qubit Kitaev code, there are two types of excitations. These are generated on the surface of such a lattice by phase-space displacements and the particles are characterized by a continuous parameter, dependent on the magnitude of the displacement. These have been shown to be a CV analogue of Abelian anyons since braiding of the anyons evolves the state by a phase factor. Unlike the original Kitaev code, the phase changes are not restricted to ± 1. In the CV case we can choose an arbitrary phase. Further work has been carried out to investigate the potential for such Abelian anyons in a CV computational context [6], but here we show how to extend this simple model to include non-Abelian anyons.

The defining property of non-Abelian anyons is that under fusion they produce multiple possible outcomes. To achieve this in our CV scheme, we take combinations of the two different types CV Abelian anyons. Under fusion, these combined states produces the multiple fusion outcomes we require [7, 8]. We find fusion and braid matrices to describe this new anyon model and show that is indeed non-Abelian, but it is not immediately obvious how to construct a useful computational basis within the fusion spaces of the CV anyons. In order to simplify the system, we restrict the allowed states by only allowing the initial anyons to be generated from identical phase-space displacements. This reduced space of states has much simpler fusion and braiding rules that share many properties with another important topological model, the Ising model [9, 10]. Quantum computation using Ising anyons has been shown to be non-universal due to the restrictions on the allowed phase under braiding. The main advantage our scheme has over the standard Ising model is that the CV anyons retain the ability to yield arbitrary phase changes that merely depend on the initial phase-space displacements we apply to the ground state.

Following from this, we construct a computational basis within the fusion spaces of the CV non-Abelian anyons. The fusions matrices have a two-dimensional structure so this system ideally lends itself to the storage of qubits as the unit of quantum information. The fusion space is a non-local property of the system and hence the qubits are protected from local sources of error. We then show how one- and two-qubit gates can be performed and find that these gates form a computationally universal set. Finally, we discuss the fault tolerance of the system against amplitude damping and finite squeezing of the initial resource state.

References

[1] M. Freedman, A. Kitaev, M. Larsen, and Z. Wang, Bull. Am. Mat. Soc. **40**, 31 (2002).

[2] C. Nayak, S. Simon, A. Stern, M. Freedman, and S. Das Sarma, Rev. Mod. Phys. **80**, 1083 (2008).

[3] A. Kitaev, Ann, Phys. (N.Y.) **303**, 2 (2003).

[4] F. Wilczek, Phys. Rev. Lett. **48**, 1144 (1982).

[5] J. Zhang, C. Xie, K. Peng, and P. van Loock, Phys. Rev. A **78**, 052121 (2008).

[6] D. F. Milne, N. V. Korolkova, P. van Loock, arXiv:1112.5385v1 (2011).

[7] J. R. Wootton, V. Lahtinen, Z. Wang, and J. K. Pachos, Phys. Rev. B **78**, 161102 (2008).

[8] J. R. Wootton, V. Lahtinen, B. Doucot and J. K. Pachos, arXiv:0908.0708v2 [quant-ph], (2009).

[9] V. Lahtinen. G. Kells, A. Carollo, T. Stitt, J. Vala, J. K. Pachos, Ann, Phys, **323**, 9, (2008).

[10] L .S. Georgiev, Nucl. Phys. B **651**, 331-360 (2003)

A source of high-purity heralded single-photons
and a novel witness for single-photon entanglement

Olivier Morin, Claude Fabre, and Julien Laurat
*Laboratoire Kastler Brossel, Université Pierre et Marie Curie, Ecole Normale Supérieure, CNRS,
Case 74, 4 place Jussieu, 75005 Paris, France*

Jean-Daniel Bancal, Pavel Sekatski, Melvyn Ho, Nicolas Gisin, and Nicolas Sangouard
Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

A driving component for the development of diverse quantum information applications is the ability to efficiently engineer non-classical states of light. In particular, a great number of communication or computing protocols require single-photon states [1]. We present here the conditional preparation of high-purity single-photon Fock state based on a continuous-wave type-II optical parametric oscillator (OPO). We will then detail the preliminary results of the implementation of a witness uniquely suited for single-photon entanglement, a widely used resource in the context of long-distance quantum communication [2]. This operational witness is inspired by a Bell-type scenario which requires only local homodyne measurements.

Heralded single-photon preparation

A continuous-wave type-II OPO [3] pumped at 532 nm is used to generate a two-mode squeezed state. From this resource, a single-photon Fock state can be heralded by conditional measurement on one of the mode. For this purpose, we use a superconducting single-photon detector (SSPD). The resulting state is then characterized by quantum state tomography via homodyne detection. The experimental results are given on Figure 1. The density matrix of the generated state shows a single-photon component above 75% (86% if corrected from detection losses). The preparation rate is around 70 kHz, for a bandwidth of 30 MHz.
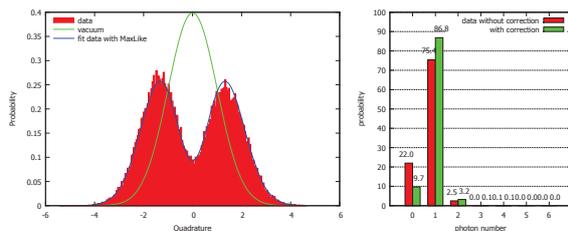
Figure 1: Single-photon Fock state generated by conditional measurements operated on the output of a type-II OPO. The left figure gives the measured marginal distribution, while the right one provides the photon-number distribution of the reconstructed state.

This well-known preparation technique is applied here for the first time with a type-II OPO. The resulting single-photon state is particularly suited for quantum information protocols that require high-visibility interference. In addition to high-purity and high brightness, the state has indeed a very well-defined spatial mode due to the OPO cavity.

Witnessing Single-photon entanglement

We now describe a novel hybrid witness for single-photon entanglement. Two distant observers, Alice & Bob, share a quantum state. To check whether it is entangled, each of them randomly chooses a measurement among two quadratures, $\{\bar{X}, \bar{P}\}$ for Alice and $\{\bar{X} + \bar{P}, \bar{X} - \bar{P}\}$ for Bob. At each run, they obtain a real number. They then process the results to get binary outcomes using a sign binning, i.e. they attribute the result -1 if the result is negative and +1 otherwise (Fig. 2). By repeating the experiment several times, Alice & Bob can compute the correlation for each couple of basis and the obtain the CHSH polynomial

$$S = E_{\bar{X}, \bar{X}+\bar{P}} + E_{\bar{X}, \bar{X}-\bar{P}} + E_{\bar{P}, \bar{X}+\bar{P}} - E_{\bar{P}, \bar{X}-\bar{P}}.$$
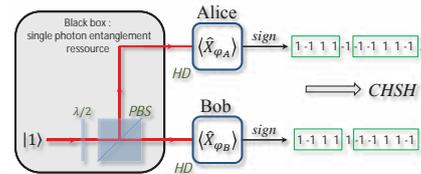
Figure 2: Experimentally witnessing single-photon entanglement with local homodyne measurements.

With only the local measurement of photon-number probabilities, without thus full tomography, one can calculate the separability bound S_{sep}. As a consequence if the measured polynomial CHSH is above $S > S_{\text{sep}}$, Alice & Bob can conclude that the state they share is entangled.

We are testing this witness by using the single-photon resource presented previously. The single-photon entanglement obtained by splitting it on a beam-splitter,

$$\frac{1}{\sqrt{2}}(|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B),$$

should lead to a clear violation of the separability bound. We will provide first results in this direction.

References

[1] J.L. O'Brien *et al.*, Nature Photon. **3**, 687 (2009).

[2] N. Sangouard *et al.*, Rev. Mod. Phys. **83**, 33 (2011).

[3] J. Laurat *et al.*, Type-II OPO: a versatile source of correlations and entanglement, in "Quantum information with continuous-variables of atoms and light", Ed. N. Cerf and E. Polzik, Imperial College Press (2007).

Quantum tele-amplification with a continuous variable superposition state

Jonas S. Neergaard-Nielsen[1,2]**, Yujiro Eto**[1]**, Chang-Woo Lee**[3,4]**, Hyunseok Jeong**[3] **and Masahide Sasaki**[1]

[1]*National Institute of Information and Communications Technology, Tokyo, Japan*
[2]*Technical University of Denmark, Kongens Lyngby, Denmark*
[3]*Seoul National University, Seoul, Korea*
[4]*Texas A&M University, Doha, Qatar*

In standard linear optical quantum computing (LOQC), qubits are encoded in the states of single photons. As an alternative, coherent states can be used for the qubit basis. This scheme, known as coherent state quantum computation (CSQC) [1], requires the availability of resource states in the form of coherent state superpositions (CSS) and gates based on quantum teleportation. True superpositions of coherent states are exceedingly hard to come by, but, for small amplitudes, good approximations to the states $|\psi\rangle = \mu|\alpha\rangle + \nu|-\alpha\rangle$ can be made by subtracting photons from a squeezed vacuum state, as demonstrated in several experiments recently [2]. In particular, a squeezed photon (the simplest state obtained by this method) approximates well the odd CSS state $|-\rangle \propto |\alpha\rangle - |-\alpha\rangle$. To teleport the qubit states $|\psi\rangle$, suitable entanglement resources are $|-\rangle$ or the squeezed photon after being split into two modes, Alice and Bob, on a beamsplitter [3, 4, 5]. After Alice mixes the unknown input state with her share of the entangled state and does a photon number detection, the state is teleported to Bob. Ideally, the success probability will be between 0.5 and 1, as opposed to standard LOQC, where it is limited to 0.5.

We implemented a simplified version of this teleportation scheme, using a squeezed photon as the resource (Figure 1a). In spite of experimental imperfections, such as losses and the use of an on/off detector instead of a photon number-resolving detector, we were able to teleport coherent states with high fidelities as verified by full homodyne tomography. This constitutes one of the first practical applications of photon-subtracted squeezed vacuum states.

An interesting aspect of CSQC is that an additional external degree of freedom of the qubits is available in the form of the amplitude α of the constituent coherent states. One could imagine situations where it would be advantageous to alter the amplitude. This becomes possible with the teleportation protocol: By adjusting the squeezing level and the beamsplitter ratios, we can convert an input qubit state $\mu|\alpha\rangle + \nu|-\alpha\rangle$ into an amplified state $\mu|g\alpha\rangle + \nu|-g\alpha\rangle$ that preserves the superposition. We demonstrated this for a range of different input amplitudes and gains. Figure 1b presents examples of two states teleported with unity gain and with $g = 2.2$, respectively. Because of limited experimental resources, we could only perform the teleportation and tele-amplification of coherent states, but in principle the protocol will work for arbitrary input qubit states – albeit in general with lower fidelities than for the coherent states.

Finally, we show that in the special case of coherent state inputs, the state transfer is resistant to even heavy losses in the channel between Bob and Alice, through a compensation on Alice's beamsplitter. This could have applications to coherent state quantum key distribution.
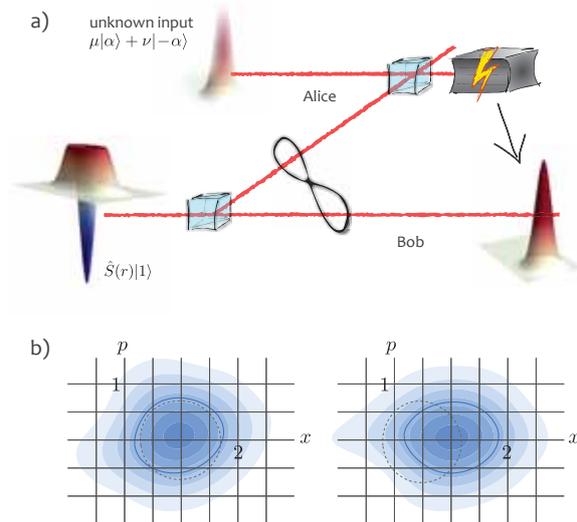
Figure 1: a) The teleportation scheme: An (in principle) unknown coherent state qubit is mixed with Alice's part of a dual-mode squeezed photon; upon a photon detection, Bob's part of the squeezed photon is transformed into the state of the input qubit. b) Experimentally reconstructed Wigner functions of the output states after teleportation with gains $g = 1$ and $g = 2.2$ of input coherent states with amplitudes $\alpha = 0.7$ and $\alpha = 0.35$, respectively. The dashed circles are the input state contours.

References

[1] H. Jeong and T. C. Ralph, in Quantum Information with Continuous Variables of Atoms and Light, edited by N. J. Cerf, G. Leuchs, and E. S. Polzik (Imperial College Press, 2007).

[2] J. S. Neergaard-Nielsen, M. Takeuchi, K. Wakui, H. Takahashi, K. Hayasaka, M. Takeoka and M. Sasaki, Progress in Informatics, **8**, 5 (2011).

[3] S. van Enk and O. Hirota, Phys. Rev. A, **64**, 022313 (2001).

[4] H. Jeong, M. S. Kim and Jinhyoung Lee, Phys. Rev. A, **64**, 052308 (2001).

[5] A. Brańczyk and T. Ralph, Phys. Rev. A, **78**, 052304 (2008).

A pseudo-deterministic single-photon source based on temporally multiplexed spontaneous parametric down-conversion

Hee Su Park[1,2], **Kevin T. McCusker**[1] **and Paul G. Kwiat**[1]

[1] *University of Illinois at Urbana-Champaign, Urbana, United States*
[2] *Korea Research Institute of Standards and Science, Daejeon, South Korea*

Deterministic single-photon sources are key components for practical photonic quantum information processing [1]. While single atom emitters such as quantum dots and NV-centers *do* produce single photons, collecting them efficiently remains challenging. Spontaneous parametric down-conversion (SPDC) as a photon source has shown an advantage of a greater collection efficiency: A photon in the output port can be heralded with a high probability by detection and collection of its twin photon. However, the output time is still probabilistic, and one cannot indefinitely increase the photon generation probability because it also increases the probability of unwanted multi-photon generation. To realize a near-deterministic single photon source, this work combines SPDC pumped by multiple pulses and an optical storage cavity that stores a photon and emits at a predetermined time [2]. A similar approach based on spatial multiplexing of SPDC has also been proposed [3].

The schematic of our experimental setup is shown in Fig. 1(a). A BBO crystal is pumped by a pulse train from a mode-locked laser (wavelength 355 nm) for non-collinear type-I SPDC. Both SPDC photons are coupled to single-mode fibers (SMFs). One photon is detected by a single-photon counter (SPC), and the other photon enters a cavity after passing through an optical delay line. Detection of a photon by the SPC triggers the Pockels cell (PC) in the cavity such that the PC rotates the polarization of the photon by 90° during the first round trip. Then the photon is stored in the cavity until it is released by the second switching of the PC (see Fig. 1(b)). The single-photon generation probability increases according to the number of pulses N_{total} used for one output time window. In contrast, the multi-photon generation can be suppressed by keeping the photon generation probability by a single pulse sufficiently small.

The performance of the setup is characterized by the single photon generation probability p_1 and the second-order correlation $g^{(2)}$, measured with coincidence of two counters at the output. Since the cavity has a finite loss due to optical components, p_1 peaks at a specific value of N_{total} [4]. This maximum p_1 depends on the photon generation probability by SPDC, the cavity loss (or finesse), and the coupling loss. $g^{(2)}$ strongly depends on the heralding efficiency between twin photons, which is determined by imaging optics for SPDC and spectral filters for photons.

The current experimental setup uses an SPDC photon-pair source that has a heralding efficiency above 50% and a sufficient photon pair generation rate. The cavity loss is below 4%. These lead to an expected $p_1 \geq 50\%$ and $g^{(2)} \sim 0.4$. Current experimental progress will be presented.
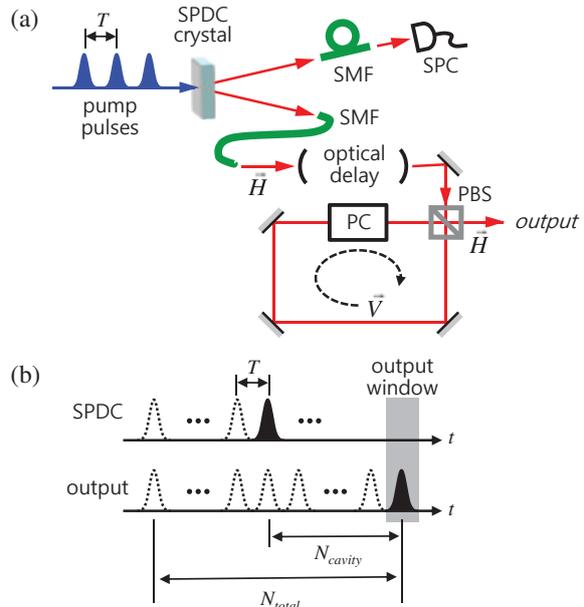
Figure 1: Schematic of the single photon source. (a) Experimental setup. (b) Output timing of photons. SMF: single-mode fiber, SPC: single-photon counter, PC: Pockels cell, PBS: polarizing beam splitter, N_{total}: the total number of input pulses for one output, N_{cavity}: the number of round trip inside the cavity.

References

[1] J. Cheung, A. Migdall and M.-L. Rastello, J. Mod. Opt., **56**, 139 (2009).

[2] T. B. Pittman, B. C. Jacobs and J. D. Franson, Phys. Rev. A, **66**, 042303 (2002).

[3] A. L. Migdall, D. Branning and S. Castelletto, Phys. Rev. A, **66**, 053805 (2002).

[4] E. Jeffrey, N. A. Peters and P. G. Kwiat, New J. Phys., **6**, 100 (2004).

Multi-particle Quantum Walks on Integrated Waveguide Arrays

K. Poulios[1], **D. Fry**[1], **J. D. A. Meinecke**[1], **M. Lobino**[1], **J. C. F. Matthews**[1], **A. Peruzzo**[1], **X. Zhou**[1], **A. Politi**[1,2], **N. Matsuda**[3], **N. Ismail**[4], **K. Wörhoff**[4], **R. Keil**[5], **A. Szameit**[5], **M. G. Thompson**[1] and **J. L. O'Brien**[1]

[1]*Centre for Quantum Photonics, University of Bristol, Bristol, UK*
[2]*Now at: Center for Spintronics and Quantum Computation, University of California Santa Barbara, USA*
[3]*NTT Basic Research Laboratories, NTT Corporation, Atsugi, Japan*
[4]*Integrated Optical Microsystems Group, MESA+ Institute for Nanotechnology, University of Twente, Enschede, The Netherlands*
[5]*Institute of Applied Physics, Friedrich-Schiller-Universität, Jena, Germany*

Multi-photon quantum walks on integrated circuits are demonstrated, showing non-classical correlations, in one and two dimensional networks. Time evolution of quantum walks and a scheme for simulating fermionic quantum walks using entanglement are also demonstrated.

Continuous-time quantum walks (CTQW) have been realized in different platforms, with single and multiple quantum particles. Single particle CTQW can be described in the context of classical wave theory. Conversely, multi-particle CTQW[1] exhibit truly non-classical behaviour and pave the way to new applications in quantum information science.

Integrated circuits provide the ideal platform for implementing large networks of CTQW, due to their inherent interferometric stability and small size. Non-classical interference of single photons has been demonstrated on integrated platforms[2] and is at the heart of emerging quantum technologies.

Lithographic fabrication of waveguides is restricted to one dimensional waveguide arrays. The direct-write laser technique for inscribing waveguides in a substrate[3] allows the creation of structures in three dimensions; hence more complex networks can be fabricated.

The one-dimensional CTQW network consists of an array of 21 evanescently coupled silicon-oxynitride (SiO_xN_y) waveguides. The measured correlation matrices (depicting the probability of detecting one photon in waveguide i coincident with the other photon detected in waveguide j) show distinct differences between distinguishable and indistinguishable input photons, that strongly depend on the input state, demonstrating the non-classical correlations between indistinguishable photons. A generalised Hong-Ou-Mandel type interference over a large network of 21 modes is demonstrated. The true quantum-mechanical nature of the correlations observed is corroborated by violations of an inequality that sets a limit to the visibility of quantum features that can be observed when using classical light.

Since the length of the coupling region in the devices measured directly relates to the time of the evolution of the CTQW, by measuring the correlations between indistinguishable photons for different coupling lengths, the coherent evolution of CTQW can be investigated. We experimentally measure three different time steps and confirm the coherent evolution of the input state. The network here has a finite number of waveguides, allowing us to study boundary conditions when photons reach the outermost waveguides.

We also show that by using bipartite, two-level entanglement for photon pairs injected in two identical CTQW networks (defined here by the TE and TM modes of the waveguides) and detecting the two-fold coincidences between these
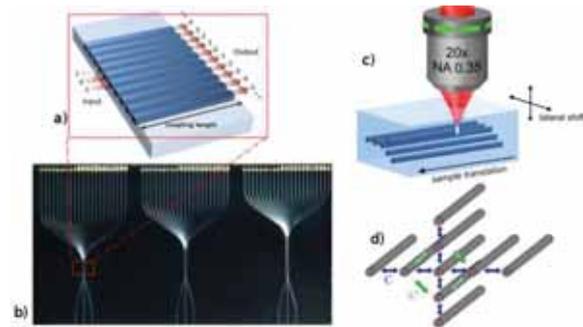
Figure 1: a)Schematic of coupling region of a 1D evanescently coupled waveguide array. b)Picture of chip, with three different coupling lengths of the 1D quantum walk network, corresponding to the three time steps. c)Schematic of the direct write laser technique to inscribe waveguides in a substrate. d)Schematic of the 2D quantum walk network, where C nearest neighbouring coupling and C' second order coupling.

two networks, we can simulate the statistics of two non-interacting fermions undergoing a CTQW using photons. Pauli's exclusion principle is observed across many modes, depicted by the vanishing of the diagonal elements of the correlation matrix (both photons detected on the same waveguide).

We finally report experimental demonstration of the first two-dimensional CTQW of correlated photons and observe correlations beyond the classical limit. Non-classical interference of photons propagating in orthogonal planes is present, with the output statistics depending on the input state of the photons. Violations are observed across the network showing behaviour that cannot be simulated with classical light across a two-dimensional lattice.

References

[1] A. Peruzzo, M. Lobino, J. C. F. Matthews, N. Matsuda, A. Politi, K. Poulios, X. Zhou, Y. Lahini, N. Ismail, K. Wörhoff, Y. Bromberg, Y. Silberberg, M. G. Thompson and J. L. O'Brien, Science, **329**, 1500 (2010).

[2] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu and J. L. OBrien, Science, **320**, 646 (2008).

[3] A. Szameit and S. Nolte, J. Phys. B: At. Mol. Opt. Phys., **43**, 163001 (2010).

Loss-tolerant EPR-steering over 1 km of optical fibre

A. J. Bennet[1,2], D. A. Evans[1,2], D. J. Saunders[1,2], C. Branciard[3], E. G. Cavalcanti[2], H. M. Wiseman[1,2] and G. J. Pryde[1,2]

[1]*Centre for Quantum Computation and Communication Technology (Australian Research Council)*
[2]*Centre for Quantum Dynamics, Griffith University, Brisbane, Queensland 4111, Australia*
[3]*School of Mathematics and Physics, University of Queensland, Brisbane, Queensland 4072, Australia*

Whether for quantum cryptography or for testing fundamental properties of the universe, it will be essential to demonstrate nonclassical effects over longer and longer distances. The barrier to doing so is loss of photons during propagation, because considering only those cases where a photon is detected opens a detection loophole in the security of any quantum information task in which parties or devices are untrusted. EPR-steering [1] is a nonclassical effect which allows one party (who trusts his own apparatus) to verify that he shares entanglement with another party, even though he doesn't trust her. Using new, arbitrarily loss-tolerant tests, we perform a detection-loophole-free demonstration of EPR-steering with entangled photon pairs over a high-loss channel.

The detection loophole in EPR-steering is in exact analogy to that for Bell inequalities. The latter are similar to EPR-steering inequalities except that neither Alice nor Bob, nor their apparatus, are trusted. Violating an EPR-steering inequality is easier than violating a Bell-inequality, but harder than witnessing entanglement (with trusted parties). This hierarchy has previously been demonstrated experimentally both in terms of how noise-tolerant these tests are [1] and in terms of how simple they can be made (minimizing the number of distinct outcomes) [2]. We note however that both of these experiments also used the fair sampling assumption.

Nonclassical effects such as Bell nonlocality and EPR-steering illuminate fundamental issues in quantum mechanics and have direct applications in quantum technology. For instance, the violation of a Bell inequality allows for device-independent (DI) secure QKD: the two parties can establish a secret key even if they bought their equipment from an adversary [3]. Bob's ability to verify entanglement via EPR-steering with no detection loophole [4, 5] likewise provides a resource for quantum communications, and a related one-sided DI secure QKD protocol — appropriate for Bob, at home base, to communicate with a roaming Alice — has been proposed [6].

In EPR-steering, Bob trusts his own apparatus, so he can safely discard those experimental runs where he fails to detect a photon. However, Bob cannot trust any claims Alice makes about the propagation losses or the efficiency of her detectors. Our key theoretical result is that Bob can close the EPR-steering detection loophole, even in the presence of arbitrarily high loss, by calculating new bounds for EPR-steering inequalities which depend on the number of measurement settings used in the protocol and Alice's heralding efficiency.

We experimentally demonstrated detection-loophole free EPR-steering using photonic Bell states generated from an efficient Sagnac spontaneous parametric down-conversion source [4], Fig. 1. We implemented the relevant n-setting measurement schemes for $n = 3, 4, 6, 10$ and 16, and our experiments yielded near-maximal steering correlations in each
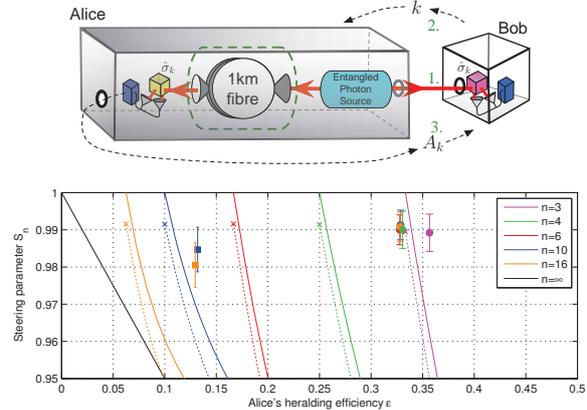
Figure 1: (Top) Conceptual representation of the EPR-steering task. Bob must assume that Alice controls the source, her line, and her detectors. Bob implements the measurement σ_k and monitors the measurement outcome. Alice measures in the same direction as Bob using an identical apparatus. (Bottom) Experimental demonstration. Circles represent experimental data straight from the entangled source (no fibre). Squares ($n = 10$ and 16 only) represent data with the fibre installed, demonstrating loss-tolerant EPR-steering with a transmission distance of 1 km. Solid curves are steering bounds and dotted curves are derived from experimental near-optimal attempted cheating attacks by a hypothetical dishonest Alice.

case. Our source and detector configuration achieved a maximum heralding efficiency of 0.354 ± 0.001, far above the minimum requirement of 0.02 set by the quality of our correlations. In this regime, we easily violated EPR-steering inequalities for $n = 3$ and greater, with no detection loophole.

To test the robustness of our protocol we inserted 1 km of single-mode fibre between the Alice-side output of the Sagnac interferometer and Alice's measurement apparatus. This increased the total loss to 8.9 dB, leading to a heralding efficiency of 0.131 ± 0.002. We successfully demonstrated EPR-steering with this setup, observing $n = 10$ and $n = 16$ steering parameters (correlation functions) of $S_{10} = 0.985 \pm 0.006$ and $S_{16} = 0.981 \pm 0.006$; 2.6 and 5.3 standard deviations above the respective bounds. Thus an honest Alice can convince Bob that they share entanglement, even in the presence of very significant photon losses.

References

[1] D. J. Saunders *et al.*, Nat. Phys. **76**, 845 (2010).
[2] D. J. Saunders *et al.*, arXiv:1103.0306
[3] A. Acin *et al.*, Phys. Rev. Lett. **98**, 230501 (2007).
[4] A. J. Bennet *et al.*, arXiv:1111.0739
[5] D. H. Smith *et al.*, Nat. Comms **3**, 625 (2012);
    B. Wittmann *et al.*, arXiv:1111.0760
[6] C. Branciard *et al.*, Phys. Rev. A **85**, 010301 (2012)

Towards implementing coherent photon conversion (CPC) for scalable optical quantum information processing

Sven Ramelow[1,2], **Nathan K. Langford**[1,2,†], **Robert Prevedel**[1,2,⋆], **William J. Munro**[3], **Gerard J. Milburn**[1,4], **Anton Zeilinger** [1,2]

[1]*Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria*
[2]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria*
[3]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[4]*Centre for Engineered Quantum Systems, University of Queensland, St Lucia, 4072 Queensland, Australia*

Coherently converting photons between different states offers intriguing new possibilities and applications in quantum optical experiments.

While single photons offer many advantages for quantum information technologies, key unresolved challenges are scalable on-demand single photon sources; deterministic two-photon interactions; and near 100%-efficient detection. All these can be solved with a single versatile process – a novel four-wave mixing process that we introduce here as a special case of the more general scheme of *coherent photon conversion* (CPC) [1]. It can provide valuable photonic quantum processing tools, from the scalable creation of single- and multi-photon states to implementing deterministic entangling gates using a novel type of photon-photon interaction and high-efficiency detection. Notably, this would enable scalable photonic quantum computing. Using photonic crystal fibres, we experimentally demonstrated a nonlinear process suited for coherent photon conversion. We observed correlated photon-pair production at the predicted wavelengths and experimentally characterised the enhancement of the interaction strength by varying the pump power. We further analyse now how current technology can provide a feasible path towards deterministic operation. In particular several material systems based on integrated photonics are analysed.

Interestingly, the general scheme of CPC could also be implemented in opto-mechanical or superconducting systems which can as well exhibit very strong nonlinearities for bosonic excitations.

Figure 1: **Left top and middle:** Scalable element for deterministic photon doubling. A '$\pi/2$'-CPC interaction ($\Gamma t = \pi/2$) can be used both to convert any single-photon source into a good source of multiphoton states and to perform high-efficiency, low-noise detection using standard single photon detectors. **Left bottom:** Deterministic controlled-phase gate. A $\pi/2$-CPC interaction ($\Gamma t = \pi$) is an effective photon-photon interaction that implements an entangling controlled-Z gate between two logical states (for example polarization or spatial encoding) of photons with different frequencies. **Right top:** The one-photon Fock-state preparation using cascaded two-photon-filtering. Combined with a single photon-doubling step and given a weak coherent input state with $|\alpha|^2 = 1.5$, in five steps this scheme gives heralded single photons with high efficiency ($\sim 56\%$) and minimal higher-order terms ($< 0.3\%$). **Right bottom:** Summary of the different CPC-based processes that can be implemented with a single device using different input states and interaction strengths.

References

[1] N. K. Langford, S. Ramelow, R. Prevedel, W. J. Munro, G. J. Milburn, A. Zeilinger, Nature, **478**, 360 (2011).

† Current address: Department of Physics, Royal Holloway, University of London, Egham TW20 0EX, United Kingdom

⋆ Current address: Research Institute for Molecular Pathology (IMP), Dr.-Bohr-Gasse 7-9, 1030 Vienna, Austria

Towards a Hybrid Quantum System: Ultracolold atoms meet a superconducting surface

Stefan Minniberger[1], Fritz Randulf Diorico[1], Stephan Schneider[1] and Jörg Schmiedmayer[1]

[1]Vienna Center for Quantum Science and Technology, Vienna University of Technology, Vienna, Austria

Hybrid quantum systems attract more and more attention in the quantum information community. While superconducting Qubits allow fast processing, their short coherence times require an efficient quantum memory. Ultracold atoms however show coherence times on the order of seconds. The collective coupling strength of 10^6 atoms near ($1\mu m$) a high-Q superconducting waveguide resonator ($Q \sim 10^6$) reaches 40kHz. The combination of ultracold atoms and a cryogenic environment however poses a significant experimental challenge, since a traditional MOT setup not only requires strong laser light from six directions, but also a high-power ($\sim$50W) alkali-metal dispenser. The heat dissipation of a MOT is well above the cooling power of common cryostats and direct laser-light is detrimental to any superconducting surface.

We are planning to realize such a hybrid quantum system by using a magnetic transport scheme for ^{87}Rb atoms. The experiment consists of two connected vacuum chambers. The lower chamber is at room temperature. A standard magneto-optical trap traps and precools around $5 \cdot 10^8$ atoms to $100\mu K$. With a series of overlapping coil pairs, those atoms are transported horizontally along a distance of 200mm. This horizontal magnetic conveyor-belt is followed by a novel on-axis magnetic transport. It consists of nine coils which transport the atoms vertically by another $\sim$200mm through a hole into the upper vacuum chamber. This chamber is cooled to around 5 Kelvin by a closed cycle cryostat. The last four transport coils are situated in the cryochamber and made of superconducting wire. This transport scheme allows us to transfer $5 \cdot 10^7$ atoms from the lower MOT-chamber to the cryo chamber within a few seconds. Once in the cryo, the original quadrupole-trap is converted to an Ioffe-Pritchard type trap with a non-zero trap bottom to avoid spin-flip losses.

In this trap, the atoms reach lifetimes of up to 300s. Our coil setup includes bias coils for all directions, which enables us to precisely control the magnetic fields. A superconducting atom chip made of Niobium is mounted on a quartz crystal two millimetres above the magnetic trap. After precooling the atoms with RF radiation to 10 μK, they will be transferred to the chip-trap, where the higher trapping frequencies will allow us to cool down to degeneracy. Future chips will contain micowave transmission-line resonators. With a cold atomic ensemble very close to that resonator, we expect to observe coupling between those two systems.

Furthermore, the atoms could be used to map out current distributions and vortices in superconducting surfaces. Another important feature of our apparatus is the very short turnaround time for experimental modifications. Changing the atom chip can be done in a matter of one week, since our cryo chamber does not require bake-out to reach the desired pressure level.
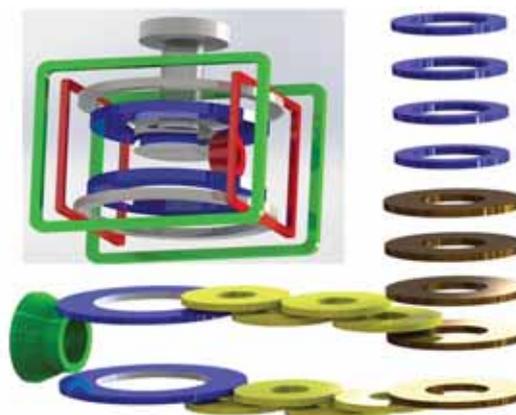
Figure 1: Magnetic conveyor belt. The inset shows the last two transport coils plus the Ioffe- and Bias coils and the superconducting chip in the cryostat.

References

[1] Stefan Haslinger, PhD Thesis, TU Wien, 2011

[2] J. Verdu, H. Zoubi, Ch. Koller, H. Ritsch and J. Schmiedmayer, Phys. Ref. Lett., **103**, 043603 (2009).

State preparation of cold cesium atoms in a nanofiber-based two-color dipole trap

Rudolf Mitsch, Daniel Reitz, Philipp Schneeweiss and Arno Rauschenbeutel

Vienna Center for Quantum Science and Technology, Atominstitut, TU Wien, Stadionallee 2, 1020 Vienna, Austria

We have recently demonstrated a new experimental platform for trapping and optically interfacing laser-cooled cesium atoms [1, 2]. The scheme uses a two-color evanescent field surrounding an optical nanofiber to localize the atoms in a one-dimensional optical lattice 200 nm above the nanofiber surface (see Fig. 1). In order to use this fiber-coupled ensemble of trapped atoms for applications in the context of quantum communication and quantum information processing, an initialization of the atoms in a well defined quantum state has to be realized. In free-beam dipole traps, such a state preparation is usually achieved by means of optical pumping. However, the nanofiber guided fields exhibit a complex polarization pattern which hampers the implementation of standard optical pumping schemes based on, e.g., the interaction of the atoms with circularly polarized light. Here, we show that optical pumping of the atoms using fiber guided light fields is possible in spite of this fact.

Our system opens the route towards the direct integration of laser-cooled atomic ensembles within fiber networks, an important prerequisite for large scale quantum communication. Moreover, our nanofiber trap is ideally suited to the realization of hybrid quantum systems that combine atoms with solid state quantum devices. Financial support by the Volkswagen Foundation, the ESF and the FWF (CoQuS graduate school) is gratefully acknowledged.
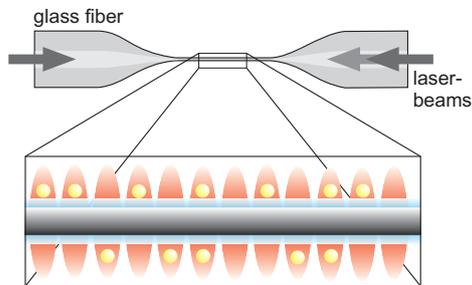
Figure 1: Experimental setup of the fiber-based atom trap. The blue-detuned running wave in combination with the red-detuned standing wave create the trapping potential.

References

[1] E. Vetsch, D. Reitz, G. Sagué, R. Schmidt, S. T. Dawkins, and A. Rauschenbeutel, Phys. Rev. Lett. **104**, 203603 (2010).

[2] S. T. Dawkins, R. Mitsch, D. Reitz, E. Vetsch, and A. Rauschenbeutel, Phys. Rev. Lett. **107**, 243601 (2011).

Nano-Structured Optical Nanofiber: A Novel Workbench For Cavity-QED

K. P. Nayak[1], Y. Kawai[1], Fam Le Kien[1], K. Nakajima[2], H. T. Miyazaki[2], Y. Sugimoto[2], and K. Hakuta[1]

[1]Center for Photonic Innovations, University of Electro-Communications, Tokyo, Japan
[2]Nanotechnology Innovation Center, National Institute for Material Science, Tsukuba, Japan

Abstract: We discuss the characteristics of optical nanofiber cavity fabricated by drilling periodic nano-grooves on a sub-wavelength diameter silica fiber using focused ion beam milling. Due to both transverse and longitudinal confinement of the field, such a nanofiber cavity can become a promising workbench for cavity-QED.

Introduction: Various designs of high-Q micro/nanostructured resonators are proposed to control the quantum states of light and matter. The key point is to realize strong confinement of the field in these structures to explore the exciting physics of cavity quantum electrodynamics (cavity-QED). Sub-wavelength diameter silica fiber, known as optical nanofiber, is becoming a promising candidate for manipulating single atoms/photons [1]. Due to the strong confinement of the field in the guided mode the spontaneous emission of atoms can be modified around the nanofiber and a significant fraction ($\sim$22%) of atomic emission can be coupled to the guided mode. The coupling between the atom and the nanofiber guided modes can be substantially improved by introducing an inline fiber cavity. It is theoretically estimated that when the diameter of the nanofiber is 400 nm, even with a low-finesse cavity with finesse of 30, almost $\sim$94% of the total emission can be channeled into the guided modes [2].

In this paper we present the fabrication and characteristics of such an optical nanofiber cavity. We drill periodic nano-grooves on the nanofiber using focused ion beam (FIB) milling technique. Such periodic nano-structures on the nanofiber induce strong modulation of refractive index for the field propagating in the guided modes and act as fiber Bragg gratings. Using such nanofiber Bragg grating (NFBG) structures we have realized nanofiber cavity.

Experiments: A schematic diagram of the nanofiber cavity is shown in Fig. 1(a). The diameter of the nanofiber is $\sim$400 $-$ 600 nm and it is located at the waist of a tapered optical fiber. A 30 keV beam of Ga^+-ions was focused on to the nanofiber with a beam spot size of $\sim$14 nm. The beam current was $\sim$10 pA and the exposure time for milling each groove was 1 s. The inset shows the FIB image of a NFBG structure. The fiber diameter is $\sim$520 nm, each groove has a depth of $\sim$50 nm and width of $\sim$150 nm. The separation between the grooves (Λ_G) is estimated using coupled mode theory.

Results and Discussion: The transmission spectrum of a 50 μm nanofiber cavity is shown in Fig. 1(b). The cavity is made of two NFBGs and each NFBG consists of 180 periods. This cavity is designed for resonance at a wavelength of $\sim$800 nm and the Λ_G value is 345 nm. The green and blue curves show the cavity modes for input polarization perpendicular (X-polarization) and parallel (Y-polarization) to the plane of the grooves respectively. The central broad dip corresponds to the Bragg resonance of the NFBG and the peaks
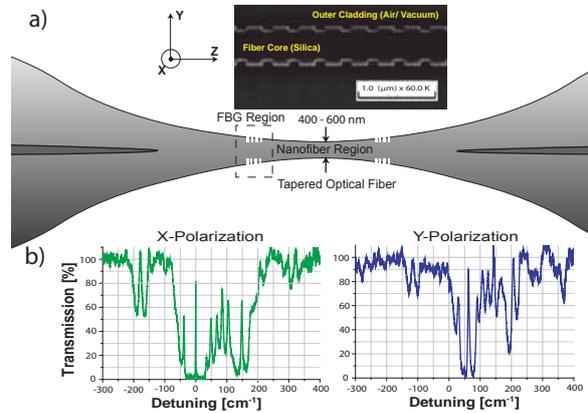
Figure 1: a) Schematic diagram of the nanofiber cavity. The inset shows the FIB image of the NFBG structures on the nanofiber. b) The transmission spectra of a nanofiber cavity. The green and blue curves show the cavity modes for two orthogonal input polarizations.

appearing within it correspond to the cavity modes. The observed spectra for the two orthogonal input polarizations are quite different from each other. The observed blue shift in the spectrum for the Y-polarization may be understood from the ellipticity induced by the grooves. In the spectrum for X-polarization, the cavity mode appearing around the detuning of 0 cm^{-1} (corresponding to frequency $\sim$12468 cm^{-1} and wavelength $\sim$802 nm) have a finesse of $F\sim$35 and the on resonance transmission is $\sim$80%. Unlike to common believe such NFBG structures do not induce any major scattering loss, which results in such low-loss nanofiber cavity.

Conclusion: In conclusion we have introduced the fabrication of low-loss optical nanofiber cavity using focused ion beam milling. Due to the confinement of the field in the guided mode of the nanofiber, even with such low-finesse nanofiber cavity strong enhancement of the spontaneous emission of atoms can be realized. Such atom + nanofiber cavity system can become a promising workbench for cavity QED and quantum nonlinear optics and will find various applications in quantum information technology. Apart from atoms, solid-state quantum emitters like quantum dots or diamond nano-crystals can also be implemented.

References

[1] K. P. Nayak and K. Hakuta, New J. Phys., **10**, 053003 (2008).

[2] Fam Le Kien and K. Hakuta, Phys. Rev. A, **80**, 053826 (2009).

High-fidelity frequency down-conversion of visible entangled photon pairs with superconducting single-photon detectors

Rikizo Ikuta[1], **Hiroshi Kato**[1], **Yoshiaki Kusaka**[1], **Shigehito Miki**[2], **Taro Yamashita**[2], **Hirotaka Terai**[2], **Mikio Fujiwara**[2], **Takashi Yamamoto**[1], **Masato Koashi**[3], **Masahide Sasaki**[2], **Zhen Wang**[2] and **Nobuyuki Imoto**[1]

[1] *Graduate School of Engineering Science, Osaka University, Japan*
[2] *Advanced ICT Research Institute, National Institute of Information and Communications Technology (NICT), Japan*
[3] *Photon Science Center, The University of Tokyo, Japan*

Near-infrared photons in telecommunication bands are necessary for transmitting quantum information over long distance, while visible photons are generated from many of quantum memories and processors using atoms, trapped ions and solid states. Thus a quantum interface for optical frequency down-conversion of photons from visible to the telecommunication bands while preserving their quantum information is required for filling the wavelength gap and achieving efficient quantum communication [1]. Recently we have demonstrated a quantum interface for such a frequency down-conversion by using difference frequency generation via a second-order nonlinearity of a periodically-poled lithium niobate (PPLN) crystal [2]. The solid-state-based quantum interface is applicable to converting a wide range of wavelengths to the telecommunication bands, and it has a possibility to have wide acceptance bandwidths. In the experiments in Ref. [2], we performed the frequency down-conversion of one half of a pico-second entangled photon pair at 780 nm to a telecommunication wavelength at 1522 nm. The observed fidelity of the two-photon state after the frequency conversion to a maximally entangled state was 0.75 ± 0.06.

The degradation of the fidelity is considered to be mainly caused by an optical noise of the anti-Stokes Raman scattering of the strong cw pump light used for the difference frequency generation. Because the noise photons from the Raman scattering are continuously generated and have a broader spectrum than that of the pico-second signal photons, photon detection with a faster time resolution and a tighter spectral filtering are effective methods for achieving a high-fidelity frequency conversion. In the previous experiment, we used commercial photon detectors; an InGaAs/InP avalanche photodiode (APD) for the telecommunication wavelength and a silicon APD for the visible wavelength. Their typical time resolutions were several hundreds of pico seconds which is much longer than the pulse duration of the signal photons. In addition, the Raman scattering linearly increases with the pump power, whereas the efficiency of the frequency conversion of signal photons by the PPLN crystal is proportional to $\sin^2(\sqrt{\eta P})$, where P is the pump power and η is a constant. Thus the decrease of the pump power will increase the signal-to-noise ratio. This is only true until the power of the converted photons is high enough in comparison to the dark counts of the photon detector. As a result, there is an optimal pump power for the best signal-to-noise ratio. The dark count rate of the InGaAs/InP APD we used was typically $\sim 10^{-4}/\text{ns}$ during a gate window of 100 ns.

In this study, we suppress the effect of the optical noise from the Raman scattering by using superconducting single-photon detectors (SSPDs) [3, 4, 5] for the photon detection instead of the APDs used in the previous experiment [2], and we demonstrate a high-fidelity performance of our quantum interface. The SSPDs typically have time resolutions of $\sim$ 100 ps and dark count rates of $\sim$ 100 Hz, and these values surpass those of the APDs. The resulting enhancement of the signal-to-noise ratio enables us to achieve a higher fidelity of 0.93 ± 0.04 after the frequency down-conversion.

Figure 1: Our experimental setup for frequency down-conversion of one half of a visible entangled photon pair.

References

[1] P. Kumar, Opt. Lett. **15**, 1476 (1990).

[2] R. Ikuta *et al.*, *Nature Commun.* **2**, 537 (2011).

[3] S. Miki, M. Takeda, M. Fujiwara, M. Sasaki, and Z.Wang, Opt. Express **17**, 23557 (2009).

[4] S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, and Z. Wang, Opt. Lett. **35**, 2133 (2010).

[5] S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, and Z. Wang, IEEE Trans. Appl. Supercond. **21**, 332 (2011).

Quantum Storage of Polarization Qubits in a Doped Solid

Mustafa Gündoğan[1], **Patrick M. Ledingham**[1], **Attaallah Almasi**[1], **Matteo Cristiani**[1] and **Hugues de Riedmatten**[1,2]

[1]*ICFO - Institut de Ciencies Fotoniques, Av. Carl Friedrich Gauss, 3, 08860 Castelldefels, Barcelona, Spain*

[2]*ICREA - Instituci Catalana de Recerca i Estudis Avançats, 08015 Barcelona, Spain*

Efficient, coherent and reversible mapping between quantum light and matter is necessary technology for quantum information science. Such technology would allow for an efficient quantum memory for light (QM), an essential component for long distance quantum communication and repeater applications [1].

Demonstrations of QMs include hot and cold atomic gases [1], single atoms in a cavity [2] and rare earth ion doped solids (REIDS) [3, 4, 5, 6, 7]. Cryogenically cooled REIDS are an attractive candidate for a QM as they offer an atomic ensemble trapped naturally within a host crystal allowing for long optical and spin coherence times. Moreover, there is a large static inhomogeneous broadening of the optical transition due to the crystal environment providing a large optical bandwidth. Furthermore, the inhomogeneously broadened line can be shaped at will using spectral hole-burning techniques, allowing for the creation of complex spectral features required for QM protocols such as the atomic frequency comb protocol (AFC) [4, 5].

Previous realizations of REIDS as QMs have been limited to multimode storage in the time degree of freedom, for example, time bin or energy-time qubits. However, quantum information is often encoded into the polarization state of photons, which provide an easy way to manipulate and analyze the qubits. Thus, extending the storage capability of a solid state QM to polarization encoded qubits would bring more flexibility to this kind of interface. The limitation is that REIDS are in general birefringent, anisotropically absorbing materials. Thus, when used as a QM, the efficiency of storage and retrieval is strongly dependent on the polarization of the input light which would result in a severely degraded fidelity for the retrieved polarization qubit.

In this experimental work we demonstrate quantum storage and retrieval of polarization qubits using a solid state device [8]. Our memory is based on AFC in Pr^{3+}: Y_2SiO_5 with resonant transition at 606 nm [5]. We used the burn-back method described in [9] to create the AFC. The AFC consists of four absorbing peaks separated by 2 MHz resulting in a storage time of 500 ns. The qubits are encoded in weak coherent pulses and detected with a single photon detector (SPD).

To address the problem of anisotropic absorption, a beam displacer (BD) is used before the memory, spatially separating the vertical and horizontal polarization components of the input polarization qubit by 2.7 mm. Then, the horizontal component is rotated to vertical polarization via a half wave plate, such that now the two beams co-propagate the absorbing medium with the same polarization. Finally, the polarization is rotated back to horizontal and combined onto another BD. Testing the BD-AFC memory with a complete set of input polarizations, the average storage and retrieval efficiency is $10.6 \pm 2.3\%$.

We characterize the quantum nature of the memory by preparing input polarization qubits in the bases $|V\rangle, |D\rangle, |R\rangle$
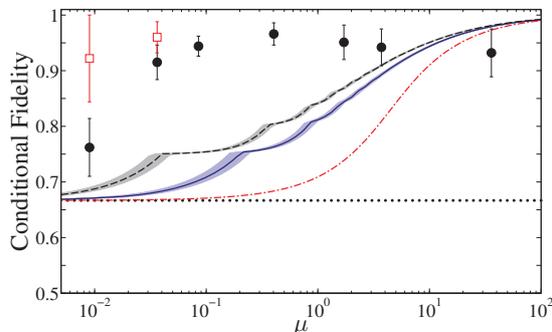
Figure 1: Average conditional fidelity measured as a function of the mean number of photons per pulse μ. Solid dots represent raw measured data, empty squares with dark counts subtracted. The dotted line is $2/3$, the classical bound for a Fock state. The dashed-dotted (solid) line is the bound for a 100% (10%) memory efficiency. The dashed line takes into account the detection probability of the SPD and transmission loss between the memory and the SPD (2%). Shaded areas represent an error of $\pm 2\%$.

and measuring the conditional fidelity of the retrieved qubit using quantum state tomography for different mean photon numbers μ ranging from $\mu = 0.01$ up to 35. For $\mu = 0.4$, the average conditional fidelity is $96 \pm 2\%$. The average measured conditional fidelity is around 95% for all input numbers tested. For $\mu \leq 3.5$, the conditional fidelity is significantly higher than the maximum achievable fidelity using a classical measure and prepare strategy taking into account the Poissonian statistics of the input pulse, the finite efficiency of the memory and the efficiency of detection including transmission loss between the memory and the SPD [2, 8] (see Figure 1). We thus demonstrate quantum storage and retrieval of polarization qubits implemented with weak coherent pulses at the single photon level, in a solid state device.

References

[1] K. Hammerer et al., Rev. Mod. Phys. **82**, 1041 (2010).

[2] H. P. Specht et al., Nature **473**, 190 (2011).

[3] M. P. Hedges et al., Nature **465**, 1052 (2010).

[4] H. de Riedmatten et al., Nature **456**, 773 (2008).

[5] M. Afzelius et al., Phys. Rev. A **79**, 052329 (2009).

[6] E. Saglamyurek et al., Nature **469**, 512 (2011).

[7] C. Clausen et al., Nature **469**, 508 (2011).

[8] M. Gündoğan et al., arXiv:1201.4149 (2012).

[9] M. Nilsson et al., Phys. Rev. B **70**, 214116 (2004).

Storage of Multiple Images using a Gradient Echo Memory in a Vapor Cell

Alberto M. Marino, Quentin Glorieux, Jeremy B. Clark, and Paul D. Lett

Joint Quantum Institute, National Institute of Standards and Technology and the University of Maryland, Gaithersburg, MD 20899 USA

Introduction

The development of a quantum memory that can store quantum states of light without a significant degradation is an active field of research. Quantum memories play a fundamental role in the development of quantum information science and are an essential requirement for the implementation of a quantum network [1]. A number of different techniques have been developed for their implementation. In particular, the gradient echo memory (GEM) [2] offers a promising technique with high recovery efficiencies [3] and the ability of temporal multiplexing [4]. We show that it is possible to use GEM for the simultaneous storage of multiple images, thus extending the multiplexing properties of this memory technique to the spatial domain.

Gradient Echo Memory

The GEM technique is based on the reversible dephasing of the macroscopic coherence of an atomic ensemble. In such a memory, the state of a light field is transferred to the long lived coherence of the hyperfine atomic ground states by combing it with a strong control field in a Λ configuration. A spatially dependent Zeeman shift is obtained with a linearly varying magnetic field along the propagation direction of the fields. After storage in the ground state coherence, the magnetic field gradient will cause the atomic dipoles to dephase. It is possible, however, to recover the information stored in the dipoles by flipping the direction of the magnetic field gradient. This inverts the precession direction of the dipoles and leads to their rephasing. Once the rephasing occurs, the stored state is retrieved if the control field is present.

In order to implement the GEM we use a 7cm-long ^{85}Rb vapor cell with Ne buffer gas at a pressure of 5 Torr and a linearly varying magnetic field of 15 μT/cm along the cell. In addition to allowing us to study the storage of classical images, this setup will allow us in the future to extend the study to the quantum regime, as it is compatible with the entangled images generated in recent experiments [5].

Simultaneous Storage of Multiple Images

We use this configuration for the simultaneous storage of two different images with a temporal delay between them and show that it is possible to temporally distinguish them after the retrieval process. In order to generate the images to be stored, the input pulses go through amplitude masks which are then imaged into the Rb cell. As a result of the storage process the transverse profile of the images is transferred to the transverse distribution of the atomic coherence, making it possible to store spatial information. After the cell a portion of the beam is picked-up to measure the intensity profile and the rest is sent to an intensified CCD camera to measure the temporal evolution of the spatial distribution of the retrieved images.

Figure 1 shows the storage and retrieval of images using
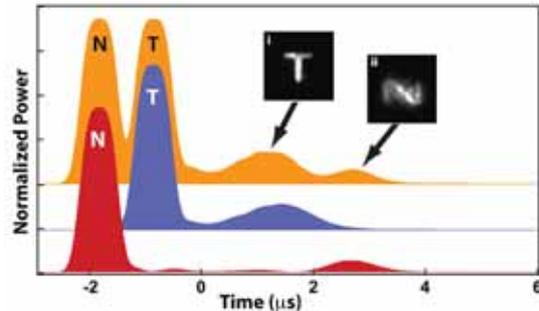
Figure 1: Simultaneous storage and retrieval of images. Spatially-integrated intensity of the storage/retrival process for a single image, "N" (red, lower) or "T" (blue, middle), and two images simultaneously (orange, top). The magnetic gradient is flipped at time zero, such that the input pulse is at negative times and the retrieved pulse is at the symmetric positive time. The insets show the retrieved images at 0.3 μs and 2.7 μs after the magnetic gradient flip.

the configuration described above. We start by studying the storage of an individual image with a "T" (blue middle trace) or an "N" (red lower trace) shape. For these images we have observed a retrieval efficiency of up to 8% and storage times over 4 μs. To store both images simultaneously in the atomic memory, we combine the two different spatial patterns on a beam splitter with a delay of 1 μs between them (orange top trace). Insets i and ii in Fig. 1 show the retrieved field after a storage time of 0.5 μs and 4.5 μs, respectively. As can be seen form these images, the shape of the output can clearly be distinguished between the "T" and "N" shapes. Note that even though the "N" was stored first, it comes out last. This is a result of the GEM which in its basic configuration operates as a first-in-last-out memory [4].

To study the limitations on the spatial fidelity of the recovered images we use a resolution chart to quantify the effect of atomic diffusion at a given buffer gas partial pressure. We find that the atomic diffusion will ultimately limit the spatial resolution of the retrieved images from the memory.

References

[1] H. J. Kimble, Nature **453**, 1023 (2008).

[2] G. Hétet *et al.*, Opt. Lett. **33**, 2323 (2008).

[3] M. Hosseini *et al.*, Nature Comm. **2**, 174 (2011).

[4] M. Hosseini *et al.*, Nature **461**, 241 (2009).

[5] V. Boyer, A.M. Marino, R.C. Pooser, and P.D. Lett, Science **321**, 544 (2008).

Demonstration of non-classical interference between heralded single photons from PCF and PPLN-based sources

A. R. McMillan[1,3], **A. S. Clark**[1], **L. Labonté**[2], **B. Bell**[1], **O. Alibart**[2], **A. Martin**[2], **S. Tanzilli**[2], **W. J. Wadsworth**[3] and **J. G. Rarity**[1]

[1]*Centre for Quantum Photonics, University of Bristol, UK*
[2]*Le Laboratoire de Physique de la Matière Condensée , Université de Nice-Sophia Anipolis, France*
[3]*Centre for Photonics and Photonic Materials, University of Bath, UK*

Non-classical Hong-Ou-Mandel (HOM) interference [1], which occurs when two indistinguishable photons arrive simultaneously at a beam-splitter, is critical for the implementation of many important protocols in quantum information. High visibility HOM interference has previously been demonstrated between heralded single photons from two separate fibre-based photon sources [2], and between the photons output from independent crystal-based sources [3]. Here we demonstrate interference between indistinguishable photons generated through two different mechanisms, one through the $\chi^{(3)}$ process of four-wave mixing in a photonic crystal fibre, and the other by $\chi^{(2)}$ parametric down-conversion in a periodically poled lithium niobate (PPLN) waveguide on a chip.

The two sources were designed to achieve phase-matching for an idler wavelength of 1550 nm, suitable for communications applications. To achieve this idler wavelength, a bulk LBO crystal was used to frequency double the pump light before the PPLN waveguide, allowing both sources to be pumped using synchronised picosecond pulses from the same 1064 nm fibre laser. Matching narrowband, tuneable, fibre-based filtering was applied to the idler photons from both sources in order to ensure spectral indistinguishability and purity of the interfering photons [4]. Spatial indistinguishability of the idler photons was guaranteed by performing the interference in a single-mode fused-fibre coupler, while the polarisation state of the photons at the coupler was matched through use of fibre polarisation controllers (FPC).
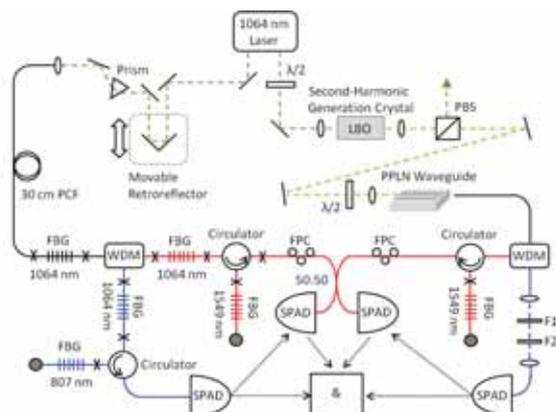
Figure 1: Setup used to measure the HOM interference visibility, showing the PCF-based photon source (left side of diagram) and PPLN-based source (right side of diagram). Idler photons from the two sources interfere at a 50:50 coupler.

At the two output ports of the fibre coupler, InGaAs based single photon avalanche diodes (SPAD) were used to detect idler photons arriving from both sources. Each of these detectors was triggered by the detection of signal photons from one of the sources, measured using silicon-based SPADs. Bunching of idler photons due to the HOM effect was observed by a dip in the rate of four-fold coincidence counts between all of the detectors as the relative arrival time of the photons at the coupler was varied using a movable retroreflector.
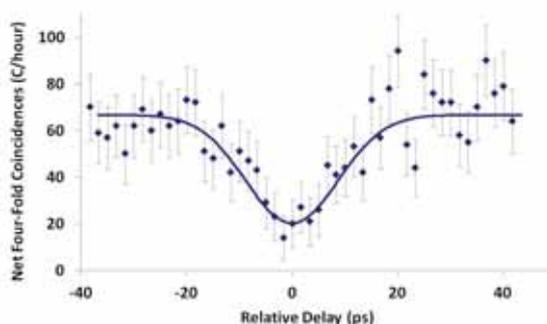
Figure 2: Net coincident four-fold detection events for different positions of the movable retroreflector.

After accounting for the background four-fold count rate due to multiple photon pair generation events in each source individually, a HOM dip with a net visibility of 70% was obtained. The visibility at present is limited primarily by temporal distinguishability caused by pulse walk-off, due to group velocity dispersion in the PPLN waveguide. We anticipate that an interference visibility of 80% can be achieved with the present setup by further optimising the spectral filtering and by reducing the PCF length to minimise effect of pulse walk-off in the fibre-based source. This demonstration of compatibility between photons from disparate sources represents a first step towards realising applications in future quantum networks encompassing multiple types of photon sources, such as quantum relays based on entanglement swapping operations [5].

References

[1] C. K. Hong et al., Phys. Rev. Lett. **59**, 2044 (1987).

[2] J. Fulconis et al., New J. Phys. **9**, 276 (2007).

[3] P. Aboussouan et al., Phys. Rev. A **81**, 021801(R) (2010).

[4] A. R. McMillan et al., Opt. Express **17**, 6156 (2009).

[5] M. Halder et al., Nature Phys. **3**, 692 (2007).

Bi-photon generation with optimized wavefront by means of Adaptive Optics

__Mattia Minozzi__[1], Stefano Bonora[3], Alexander V. Sergienko[2], Giuseppe Vallone[1] and Paolo Villoresi[1]

[1]*Department of Information Engineering, University of Padova, Padova, Italy*
[2]*Department of Electrical & Computer Engineering, Department of Physics, University of Boston, Boston, U.S.A.*
[3]*Institute for Photonics and Nanotechnology, Nat. Res. Council, Padova, Italy*

The importance of pump wavefront on the generation of entangled photons in SPDC process have been envisaged in the nineties [1, 2]. In this work we address experimentally this issue, by realizing an experiment in which we shape and control the pump wavefront so as to optimize the collection of correlated pairs into single-mode fibers. In order to achieve this target, the deformable mirror becomes the key device to have full control of the pump beam.

The modulation of the $404nm$ pump wavefront is achieved by the setup illustrated in Fig. 1.
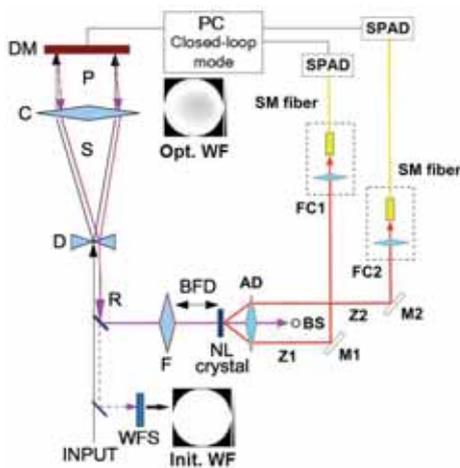
Figure 1: Experimental setup.

The use of a deformable mirror (DM) allows to shape the pump wavefront before interacting with a nonlinear BBO type-I crystal (NL crystal). Then, the degenerate SPDC photons at $808nm$ are selected and measured by high-efficiency SPADs. Since down-converted light retains memory of the pump wavefront, the effect of the deformable mirror is significant for fiber coupling optimization. Therefore, slight changes in pump wavefront result in substantial alterations of coincidence counting rate. Consequently, the search for a suitable wavefront, which can correct aberrations and optimize coincidences, is of great interest. Such a task can be solved by the use of an evolutionary algorithm, which puts in feedback the action of the mirror with coincidence counting rate. Thus, *Ant colony optimisation* [3] was employed to improve coincidences and optimize the collection efficiency of SPDC light.

In the beginning the fiber coupling is maximized manually with a plane wavefront, which is imposed by the deformable mirror before F lens. Such a setup is usually adopted to produce SPDC light. In this experiment we continue with a special adaptive algorithm in order to improve and maximize co-

incidence counting rate. Several runs of the algorithm showed an increase in coincidences by over 20%, as it is illustrated in Fig. 2(a).
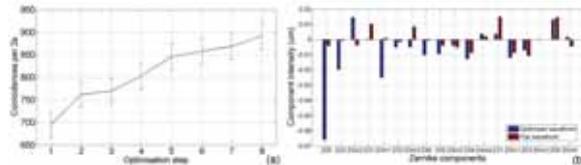
Figure 2: Algorithm steps showing an effective improvement (a). Optimized wavefront compared to initial flat one (b).

By comparing coincidence signal with single channel counts, a growth in coincidences results in a rise in two-photon coupling efficiency: the ratio between coincidences and single channel counts. Thus, efficiency increased by 20% at the end of the run, since single counts remained stable. A futher point of interest is that the wavefront at F lens is no more flat at the end of the algorithm run, as it can be seen from the interferograms illustrated in Fig. 1. As a result, several Zernike components are present, the most significant of which is defocus. However, second, third and fourth order aberrations appear, as it is shown in Fig. 2(b), to optimize the generated wavefront of the two-photon wavefunction.

In conclusion, the pump wavefront manipulation was realized by means of the use of a deformable membrane mirror with the target of optimizing the entangled photons coupling efficiency. The optimization was realized with an evolutionary algorithm to drive the deformable mirror itself. Finally, we measured that the optimized wavefront is no more flat, but contains several aberrations.

Acknowledgments

References

[1] A. V. Belinskii, D. N. Klyshko, Zh. Eksp. Teor. Fiz. 105, 487-493 (1994)

[2] T. B. Pittman, D. V. Strekalov, D. N. Klyshko, M. H. Rubin, A. V. Sergienko, Y. H. Shih, Phys. Rev. A, 53, 4 (1996).

[3] E. Bonabeau, M. Dorigo, G. Theraulaz, Nature, Vol. 406 (6 July 2000).

Quantum storage of orbital angular momentum at the single photon level in cold Cs atoms

Adrien Nicolas[1], **Lambert Giner**[1], **Lucile Veissier**[1], **Alexandra Sheremet**[1], **Michael Scherman**[1], **Jose W.R. Tabosa**[2], **Elisabeth Giacobino**[1] and **Julien Laurat**[1]

[1] *Laboratoire Kastler Brossel, Université Pierre et Marie Curie, Ecole Normale Supérieure, CNRS, 4 place Jussieu, 75005 Paris, France*
[2] *Departamento de Fisica, Universidade Federal de Pernambuco 50670-901 Recife, PE, Brazil*

Storage and read-out of non classical states of light is a critical element for quantum information networks. Laguerre-Gaussian beams, i.e. beams of light carrying orbital angular momentum, are intrinsically high dimensional quantum systems. They have been identified as interesting candidates for the implementation of various quantum information protocols [1] [2]. In the past few years storage of light carrying orbital angular momentum has been demonstrated [3, 4]. Here, we report on the storage of photonic qubits that are superpositions of Laguerre-Gaussian modes of opposite helicities in an ensemble of cold Caesium atoms.

Laguerre-Gaussian beams constitute a complete basis of solutions for the paraxial approximation denoted as $|LG_p^l\rangle$, where l and p are integer indices describing respectively the azimuthal phase, i.e. the orbital angular momentum (OAM) of the beam, and the number of radial nodes of the amplitude. In our experiment, we use the lowest order modes with indices $p = 0$ and $l = 1$ to form a qubit basis. The phase structure of such a mode is shown in Fig. 1. A superposition of these modes is a Hermite-Gaussian mode. In our experiment, the OAM is imprinted on very faint coherent pulses (with less than one photon per pulse) using reflection on a spatial light modulator (SLM).

tion propagate across the atomic medium. The control beam is generated by a stabilized laser diode whereas the signal field is generated by a Ti:Sa laser locked at resonance using saturated absorption spectroscopy. The two lasers are locked in phase and in frequency. The experimental set-up is shown in Fig. 2.

An orbital angular momentum is imprinted on the signal beam as explained above and the photonic signal to be stored is transferred to a hyperfine atomic coherence via dynamic EIT. For this the control beam intensity is turned off once the signal pulse has entered the cold atomic medium. After a few μs storage time, the control field is turned on again and the light emerging out of the memory is analyzed with mode selectors made of phase holograms that perform orbital angular momentum subtraction and single mode optical fibers serving as spatial filters [5]. The fibers are then directed to two APDs that allow to measure the $l = +1$ and $l = -1$ components of the beam.

Using temporal pulse shaping of the signal field, we recover the photonic signal carrying OAM with efficiencies above 23% for both modes. We have thus demonstrated storage of orbital angular momentum at the level of a single photon.

Figure 1: Interference pattern showing the phase structure of a Laguerre-Gaussian beam
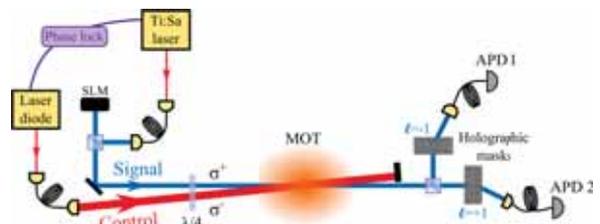
Figure 2: Optical setup of the experiment

The quantum memory device is an ensemble of cold Caesium atoms in a magneto-optical trap (MOT), with an optical depth above 20. The experiment is performed in sequences. A sequence starts with a build-up period of the MOT of about 20 ms, then the magnetic field and the trapping beams are turned off for the memory operation. A memory phase lasts for a few ms, during which the photonic signal is stored and retrieved and it is repeated 100 times per sequence. The full sequence is in turn repeated 40 times per second and the results are accumulated.

The storage period involves a classical control pulse resonant with the $|6S_{1/2}F = 3>$ to $|6P_{3/2}F = 4>$ transition. It opens a transparency window which lets the 1 μs long signal pulse close to the $|6S_{1/2}F = 4>$ to $|6P_{3/2}F = 4>$ transi-

References

[1] G. Gibson, J. Courtial, M. Padgett, M. Vasnetsov, V. Pas'ko, S. M. Barnett, S. Franke-Arnold, Opt. Ex. **12** 5448 (2004)

[2] S. Groeblacher, T. Jannewein, A. Vaziri, G. Weihs, A. Zeilinger, N. J. Phys. **8**, 75 (2006)

[3] R. Pugatch, M. Shuker, O. Firstenberg, A. Ron, N. Davidson, Phys. Rev. Lett. **98**, 203601 ((2007)

[4] D. Moretti, D. Felinto, J.W.R. Tabosa, Phys. Rev. A **79**, 023825 (2009)

[5] A. Mair, A. Vaziri, G. Weihs, A. Zeilinger, Nature **412**, 131 (2001)

Superradiance from entangled atoms

R. Wiegner[1], J. von Zanthier[1,2] and G. S. Agarwal[2,3]

[1] *Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, 91054 Erlangen, Germany*
[2] *Erlangen Graduate School in Advanced Optical Technologies (SAOT), Universität Erlangen-Nürnberg, 91052 Erlangen, Germany*
[3] *Department of Physics, Oklahoma State University, Stillwater, OK 74074, USA*

The phenomenal progress in the preparation of entangled states of atoms, particularly in chains of trapped ions [1], has enabled one to demonstrate many basic tasks in quantum computation and quantum metrology. However it has been much less conceived that entangled states endow us with new means for doing optical physics [2] what traditionally is accomplished using independent atoms, though with exceptions [3, 4, 5]. Since one has succeeded in preparing well characterized entangled states albeit for a small number of qubits, it is pertinent to ask how the radiative properties of atoms in well characterized entangled states differ from those of atoms prepared in separable states.

Here, we consider a system of N atoms prepared in well characterized entangled states like W-states where the inter-atomic distance is much larger than the emission wavelength and discuss the far-field radiation pattern created by this atomic ensemble [6]. We note that the investigated scheme differs from common experiments on superradiance [7] where a gas of atoms is initially prepared in the fully excited state, i.e., the Dicke state $|N/2, N/2\rangle$, and the variation of the systems' radiation over long time scales is explored as the state evolves to the ground state. In contrast, we are discussing the short time behavior of the radiation emitted by entangled atoms in generalized symmetric W-states, i.e., for W-states with an arbitrary number n_e of excited atoms. We show how the nature of the initial W-state dictates its radiative characteristics and find enhanced spontaneous emission. We trace this enhancement of spontaneous emission back to interferences of multiple photon quantum path ways and introduce a framework which enables to precisely identify each specific quantum path leading to the enhanced radiation. This framework is especially relevant as separable initially excited states obviously do not give rise to interferences at the level of the mean radiated intensity as their dipole moment is zero. We emphasize that the considered entangled states have also zero dipole moment. However, since our quantum path framework is not based on the dipole moment, it can physically explain the enhanced radiation where a classical antenna interpretation is not applicable.

Besides studying the maximal enhancement of radiation we also investigate the angular dependence of the scattered intensity to better characterize the radiation emitted by those states. A strong focussing of the radiation created by initial W-states is shown. We extend our investigation also to non-symmetric generalized W-states and give examples which support the interpretation of super- and subradiance in terms of quantum path interference even for a broader class of states.

References

[1] R. Blatt and D. Wineland, Nature **453**, 1008 (2008).

[2] G. S. Agarwal, Phys. Rev. A **83**, 023802 (2011).

[3] R. H. Dicke, Phys. Rev. **93**, 99 (1954).

[4] M. O. Scully and A. A. Svidzinsky, Science **325**, 1510 (2009).

[5] M. O. Scully, Phys. Rev. Lett. **102**, 143601 (2009).

[6] R. Wiegner, J. von Zanthier, G. S. Agarwal, Phys. Rev. A 84, 023805 (2011).

[7] L. Allen and J. H. Eberly, *Optical Resonance and Two-Level Atoms*, (Wiley, New York, 1975).

New free-running, low noise 1550nm single photon detector for commercial applications

Gerhard Humer[1], Andreas Poppe[1], Momtchil Peev[1], Martin Stierle[1],
Sven Ramelow[2], Christoph Schäff[2], Anton Zeilinger[2], Rupert Ursin[2]

[1]AIT Austrian Institute of Technology, Donau-City-Strasse 1, 1220 Vienna, Austria
[2]Institute for Quantum Optics and Quantum Information (IQOQI) Vienna, Austrian Academy of Sciences (ÖAW), Boltzmanngasse 3, 1090 Vienna, Austria

In the last several years AIT developed a single photon detector in the 1500nm range. The target was to achieve very low dark count rates and low afterpulsing probabilities in a free-running regime. For this a very fast active quenching circuit is implemented to reduce the negative effects of the arising avalanche. High frequency reflections and losses had to be taken into account to realize a broad band matching of the transmission lines and input/output impedances using a broadband vector channel analyzer. This results in an output signal with very low jitter and high signal to noise ratio. Moreover, an efficient thermoelectric cooling setup provides temperatures beyond -60°C necessary for the low dark count rates. The module can be adjusted to operate with detection probabilities between around 0,3% and 10%. The dead-time is around 5us resulting in a high peak count rate. Standard SMA connectors provide the corresponding output pulses with a timing resolution better than 350ps at 10% efficiency. An USB interface connects the device to a controlling PC with a Graphical User Interface. A standard FC/PC connector with a single mode fiber is provided as optical input. The single photon detector provides a cost-effective solution for applications where low noise and free-running operation is required.

Figure 1: Evaluation of 8 single photon detectors

In this contribution we describe the functionality of the detector components and a comprehensive characterization of the performance of the device. This includes depicting the functional relations with block diagrams. The most important challenge of the design is the high frequency part concerning the dimension and parasitic capacity of the used single photon avalanche diode. For this reason the two-terminal-pair parameters (S-parameter) were measured. These S-parameters build the basis for the simulation supported design of the optimized electronic matching circuit. The need of a very accurate adjustable bias voltage is explained and the design solution is depicted. The automatic control and regulation of the cooling system is also discussed. Finally the USB interface and control unit are presented.

Measurement

A novel method for afterpulsing characterization is presented, which uses the probability density function of the timing distances between the measured events. Based on the theoretical density function for a perfect detector the imperfectness can be separated in a very comfortable way. This method allows detector characterization even using the intrinsic dark counts. After presenting the theoretical background the measurement results are presented und discussed. These include the dark count rate, the afterpulsing probability and the timing jitter as a function of the quantum efficiency.
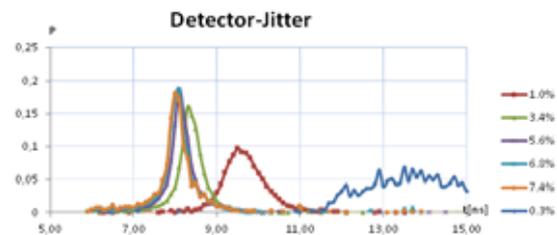
Figure 2: Detector jitter for different quantum efficiency settings. The measurement is done with a source of correlated pairs of photons and a time tag unit plotting the histogram of the time differences.

Further interesting results are the dark count rates and afterpulsing probabilities as a function of temperature and efficiency. Moreover the plots depicting efficiency against temperature and efficiency versus SPAD bias voltage allow us to identify the required specifications for the accuracy of the voltage and temperature regulation. Finally, we characterize the peak count rate and determine the correction factor as a function of the measured count rate.

Integrated quantum photonics for polarization encoded qubits

F. Sciarrino[1,2], **L. Sansoni**[1], **P. Mataloni**[1,2], **A. Crespi**[3,4], **R. Ramponi**[3,5] and **R. Osellame**[3,4],

[1]*Dipartimento di Fisica, Sapienza Università di Roma, Piazzale Aldo Moro, 5, I-00185 Roma, Italy*
[2]*Istituto Nazionale di Ottica, Consiglio Nazionale delle Ricerche (INO-CNR), Largo Enrico Fermi, 6, I-50125 Firenze, Italy*
[3]*Istituto di Fotonica e Nanotecnologie, Consiglio Nazionale delle Ricerche (IFN-CNR), Piazza L. da Vinci, 32, I-20133 Milano, Italy*
[4]*Dipartimento di Fisica, Politecnico di Milano, Piazza Leonardo da Vinci, 32, I-20133 Milano, Italy*

The ability to manipulate quantum states of light by integrated devices may open new perspectives both for fundamental tests of quantum mechanics and for novel technological applications. The technology for handling polarization-encoded qubits, the most commonly adopted approach, was still missing in quantum optical circuits until the ultrafast laser writing (ULW) technique was adopted for the first time to realize integrated devices able to support and manipulate polarization encoded qubits [1]. In the ULW technique a femtosecond laser is focused on a glass substrate inducing a variation of the glass refractive index in the region around the focus: by translating the substrate with respect to the laser beam it is possible to directly write wave-guides inside the chip (see Fig. 1(a)).

Thanks to this method, polarization dependent and independent devices can be realized. In particular the maintenance of polarization entanglement was demonstrated in a balanced polarization independent integrated beam splitter [1] and an integrated CNOT gate for polarization qubits was realized and carachterized [2]. This second result has been enabled by the integration, based on femtosecond laser waveguide writing, of partially polarizing beam splitters on a glass chip. We characterize the logical truth table of the quantum gate demonstrating its high fidelity to the expected one and show the ability of this gate to transform separable states into entangled ones and vice versa. We also exploited integrated optics for quantum simulation tasks: by adopting the ULW technique an integrated quantum walk circuit was realized [3]. We reported the experimental demonstration on how the particle statistics, either bosonic or fermionic, influences a two-particle quantum walk (QW) [3], i.e. the implementation of a discrete quantum walk for entangled particles. By changing the symmetry of entanglement we can simulate the quantum dynamics of the walks of two particles with bosonic or fermionic statistics. These results are made possible by the adoption of novel three-dimensional geometries in integrated optical circuits fabricated by femtosecond laser pulses, which preserve the indistinguishability of the two polarizations as well as provide high phase accuracy and stability. With such a circuit, for the first time, we investigate how the particle statistics, either bosonic or fermionic, influences a two-particle discrete quantum walk. Such experiment has been realized by adopting two-photon entangled states and an array of integrated symmetric directional couplers (see Fig. 1(b)). The polarization entanglement was exploited to simulate the bunching-antibunching feature of non interacting bosons and fermions. In Fig. 1(c-d) the measured probability distributions for bosonic and fermionic two particle QWs are shown. We compared the experimental distributions with the expected ones through the similarity, a quantum gen-

eralization of the classical fidelity between two distributions, obtaining $S_{bos} = 0.982 \pm 0.002$ and $S_{fer} = 0.973 \pm 0.002$ for the bosonic and fermionic quantum walk, respectively, in good agreement with the expected ones. The insensitivity to photon polarization, high-accuracy in the phase control and intrinsic scalability of the integrated multi-DC network presented in this work, pave the way to further advanced investigations on complexity physics phenomena. For instance, by introducing suitable static and dynamic disorder in the walk it would be possible to simulate the interruption of diffusion in a periodic lattice, like Anderson localization [4], and the noise-assisted quantum transport effect [5, 6].
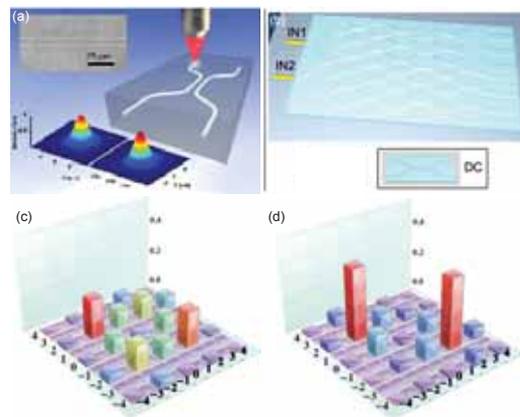
Figure 1: (a) Directional coupler realized with ULW, (b) QW circuit, (c-d) measured probability distributions of bosonic and fermionic two-particle QW.

References

[1] L. Sansoni *et al.*, Physical Review Letters **105**, 200503 (2010).

[2] A. Crespi *et al.*, Nature Communications **2**, 566 (2011).

[3] L. Sansoni *et al.*, Physical Review Letters **108**, 010502 (2012).

[4] P. Anderson, Physical Review **109**, 1492 (1958).

[5] M. Mohseni, P. Rebentrost, S. Lloyd, and A. Aspuru-Guzik, The Journal of Chemical Physics **129**, 174106 (2008).

[6] F. Caruso, N. Spagnolo, C. Vitelli, F. Sciarrino, and M. B. Plenio, Physical Review A **83**, 013811 (2011).

Poster session 3 Thursday abstracts

Experimental test of measurement-disturbance relations in generalized photon-polarization measurements

So-Young Baek[1], **Fumihiro Kaneda**[1], **Masanao Ozawa**[2], **and Keiichi Edamatsu**[1]

[1]*Research Institute of Electrical Communication, Tohoku University, Sendai, Japan*
[2]*Graduate School of Information Science, Nagoya University, Nagoya, Japan*

The Heisenberg uncertainty principle, originally formulated in 1927, describes the trade-off relation between the error of a measurement of one observable $\epsilon(A)$ and the disturbance caused on another complementary observable $\eta(B)$ such that their product should be no less than the limit set by Planck's constant [1]. The generalized form of the Heisenberg relation

$$\epsilon(A)\eta(B) \geq \frac{1}{2}|\langle[A,B]\rangle| \qquad (1)$$

has been taken as a fundamental limitation on our ability to make physical observations. However, Ozawa in 1988 showed a model of position measurement that breaks Heisenberg's relation [2] and in 2003 revealed an alternative relation for error and disturbance to be proven universally valid [3]: Any measurement of an observable A in a state ψ with the error $\epsilon(A)$ causes the disturbance $\eta(B)$ on another observable B satisfying

$$\epsilon(A)\eta(B) + \epsilon(A)\sigma(B) + \sigma(A)\eta(B) \geq \frac{1}{2}|\langle[A,B]\rangle|, \quad (2)$$

where $\sigma(A)$ and $\sigma(B)$ stand for the standard deviations in the state ψ. Ozawa's relation has two additional correlation terms. It turns out that they are redundant, or Heisenberg's relation holds, when the mean error and the mean disturbance are independent of the input state ψ [4]. However, the presence of those terms allows the error-disturbance product $\epsilon(A)\eta(B)$ to be much below the lower bound of Eq. (1).

Recently, Erhart *et al.* have experimentally demonstrated Ozawa's relation in neutron spin measurements [5], using the "three-state method" for measuring error and disturbance proposed in Ref. [4]. In this paper, we report an experimental test of Ozawa's relation using the "three-state method" for a single-photon polarization qubit. The test is carried out by linear optical devices [6] and realizes an indirect measurement model that validates Ozawa's relation and breaks Heisenberg's relation for various values of an experimental parameter, the "measurement strength". In the previous attempt [5], the projective measurement of a spin component is implemented by a pair of projective operations, each of which is carried out in an independent experimental set-up by a spin-analyzer, which passes only one fixed outcome ($+1$ or -1) of measurement. This is unlike any indirect measurement model, in which the apparatus probabilistically passes two possible outcomes ($+1$ and -1) in a single experimental set-up. Moreover, our measurements are of a more general class of quantum measurements than the class of projective measurements, which were tested previously [5].

We define X, Y, and Z be the Pauli matrices and take the signal observable to be measured as $A = Z$ and consider the disturbance in the signal observable $B = X$. To compare Ozawa's relation with Heisenberg's relation, we choose the input signal state as an eigenstate of Y since it gives the maximum value of $C(Z,X) \equiv |\langle\psi|[Z,X]|\psi\rangle|/2 = |\langle\psi|Y|\psi\rangle| = 1$, and is thus the most stringent test for these relations.

From the experimentally measured error and disturbance, we evaluate Ozawa's quantity (solid circles) and Heisenberg's quantity (solid squares) in Fig. 1. The upper and lower solid lines are the corresponding theoretical plots as functions of measurement strength after the non-ideal PBS extinction ratio of the measurement setup is taken into account. The dashed and dotted lines are theoretical plots for an ideal PBS. As shown in Eq. (1) and Eq. (2), both uncertainty relations have the same lower bound $C(Z,X) = 1$ (middle solid line). The data clearly demonstrate that Ozawa's relation is always valid, whereas Heisenberg's relation is false for all measurement strengths.

A correct understanding and experimental confirmation of the error-disturbance relation will not only foster insight into fundamental limitations of measurements but also advance the precision measurement technology in quantum information processing.
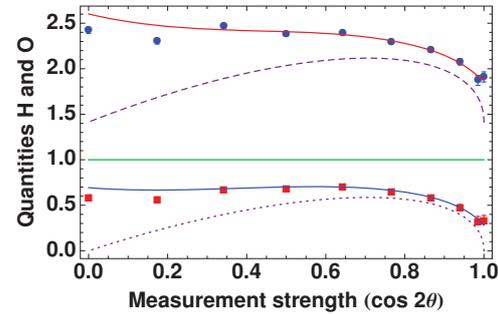
Figure 1: Experimentally measured quantities $H \equiv \epsilon(Z)\eta(X)$ (solid squares) and $O \equiv \epsilon(Z)\eta(X) + \epsilon(Z)\sigma(X) + \sigma(Z)\eta(X)$ (solid circles) appearing in Eq.(1) and Eq.(2), respectively.

References

[1] W. Heisenberg, Z. Phys. **43**, 172 (1927).

[2] M. Ozawa, Phys. Rev. Lett. **60**, 385 (1988).

[3] M. Ozawa, Phys. Rev. A **67**, 042105 (2003).

[4] M. Ozawa, Ann. Phys. (N.Y.) **311**, 350 (2004).

[5] J. Erhart, S. Sponar, G. Sulyok, G. Badurek, M. Ozawa, and Y. Hasegawa, Nature Phys. **8**, 185 (2012)

[6] S.-Y. Baek, Y,-W. Cheong, and Y.-H. Kim, Phys. Rev. A **77**, 060308(R) (2008).

Multi-settings Greenberger-Horne-Zeilinger nonlocality for N-partite qu$D$its

Junghee Ryu[1,2], **Changhyoup Lee**[1,2] **and Jinhyoung Lee**[2]

[1]*Research Institute for Natural Sciences, Seoul, Hanyang University*
[2]*Department of Physics, Seoul, Hanyang University*

Abstract.—We generalize Greenberger-Horne-Zeilinger (GHZ) nonlocality of three qubits to N-partite and D-dimensional systems, particularly involving *more than two* alternative measurements for each party. For the purpose, we employ the concurrent observables that have a common eigenstate even though they are mutually incompatible. To construct these observables, we apply the appropriate phase shifter to a given reference observable, which gives rise to the genuinely many measurement settings. We suggest a systematic method in which the divisors of the number of dimension are significant to construct the GHZ nonlocality. As a result, we show the GHZ nonlocality for arbitrary multipartite high-dimensional systems with many measurement settings. Our results reproduce the previous works [1, 2, 3].

Introduction.—Ever since the appearance of entanglement, it has been regarded that quantum entanglement plays an important resource for quantum information processing (QIP), such as quantum teleportation, computing and cryptography. Nonlocality is also one of the most distinct features against classical physics. Bell showed that nonlocality exhibits by the constraint, so-called Bell's inequality, that local realism imposes on the correlations obtained from the measurements between two separated systems [4]. Even though nonlocality has been studied by using statistical inequalities, it was shown *without any statistical inequalities* for a tripartite system [5]. It is also widely regarded that nonlocality is one of the important ingredients in QIP. A link between the security of quantum communication and the violation of Bell inequalities was studied. The GHZ nonlocality was connected to quantum error-correcting codes and also with stabilizing code of graph state. The GHZ state, a quantum state which exhibits the GHZ nonlocality, has been utilized at the heart of quantum secret sharing and quantum key distribution [2, 6].

Since the discovery of the Bell's theorem [4], the research of nonlocality test for more arbitrary complex systems has been considered as one of the significant challenges in foundation of quantum theory and QIP. For the sake of simplicity, we denote a complex system by (N, M, D): N parties, M measurement settings for each party, and D distinct outcomes for each measurement. Żukowski and Kaszlikowski showed the GHZ nonlocality for a $(D+1, 2, D)$ system [1]. They also generalized to arbitrary D-partite D-dimensional system [7]. The GHZ nonlocality for $(N > D, 2, \text{even } D)$ system was examined by Cerf *et al.*, which is based on operator relations [2]. They also proposed the criteria about genuinely N-partite and D-dimensional GHZ nonlocality. On the contrary to the previous works, J. Lee *et al.* employed an observables that are incompatible but still have a common eigenstate [3]. As a result, they showed the contradictions for arbitrary genuinely (odd N, 2, even D) systems. Although many studies for generalization of the GHZ nonlocality have been reported, there is no answer yet to arbitrary *odd*-dimensional *multipar-*

tite systems. Also, so far the analysis of the GHZ nonlocality was considered for the systems that only *two* measurement settings are implemented by each party.

Main.—The concurrent observable is that its common eigenstate is equal to a given quantum state [3]. As long as the quantum system is prepared in its common eigenstate, the measurement results of these observables can simultaneously be identified. To construct the composite observables for GHZ nonlocality, we employ the concurrent observables that are incompatible and nevertheless have a common eigenstate. In general, while it is difficult to find all concurrent observables, Lee *et al.* suggested a method by which we can easily find a particular set of them by using the symmetries of a given quantum state [3]. For the purpose, we consider an unitary operator $\hat{U} = \bigotimes_{j=1}^{N} \hat{P}_j$ for a N-partite system, where the local phase shifter is given by $\hat{P}_j = \sum_{n=0}^{D-1} \omega^{f_j(n)} |n\rangle \langle n|$. Here $\omega = \exp(2\pi i/D)$ is a primitive Dth root of unity over the complex field.

In this work, we obtain an invariant condition, which leaves the generalized GHZ state invariant by the unitary operator $\hat{U}$, based on the phase value $\omega^{f_j(n)}$. It is an essential for constructing the concurrent observables and the genuinely many observables. We suggest a systematic method to construct the GHZ nonlocality, by which the divisor of the number of dimension determine the number of observer. As a result, we show multi-settings GHZ nonlocality for N-partite qu$D$its systems. Our result is also genuinely (N, M, D) GHZ nonlocality according to the Ref. [2].

References

[1] M. Żukowski and D. Kaszlikowski, Phys. Rev. A **59**, 3200 (1999).

[2] N. J. Cerf, S. Massar, and S. Pironio, Phys. Rev. Lett. **89**, 080402 (2002).

[3] J. Lee, S.-W. Lee, and M. S. Kim, Phys. Rev. A **73**, 032316 (2006).

[4] J. S. Bell, Physics **1**, 195 (1964).

[5] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bells Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989).

[6] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001); A. Cabello and P. Moreno, Phys. Rev. A **81**, 042110 (2010); M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999); J. Kempe, Phys. Rev. A **60**, 910 (1999).

[7] D. Kaszlikowski and M. Żukowski, Phys. Rev. A **66**, 042107 (2002).

Conservation of operator current in open quantum systems and application to Cooper pair pumping

Juha Salmilehto[1], **Paolo Solinas**[1,2], **Mikko Möttönen**[1,2] and **Jukka P. Pekola**[2]

[1]*Department of Applied Physics/COMP, Aalto University, P.O. Box 13500, FI-00076 AALTO, Finland*
[2]*Low Temperature Laboratory, Aalto University, P.O. Box 13500, FI-00076 AALTO, Finland*

Even though master equations are amongst the standard tools for describing dissipative systems, their use is reminiscent of walking a tightrope: one is forced to apply a series of approximations hoping that fundamental physical properties are not lost in the process. To postulate an axiom for one such important property, we present a time-local conservation law ensuring that any current flowing into the reduced system equals the current obtained by it. More spesifically, the law guarantees that the temporal change of any system observable given by a master equation equals the temporal integral of the related current operator [1].

The conservation law reduces to a comparison of dissipative currents, that is, currents induced directly by the interaction with the environment and takes the form

$$-\frac{i}{\hbar}\text{Tr}\{\hat{\rho}[\hat{G}, \hat{H}_I]\} = \text{Tr}_S\{\hat{D}\hat{G}\}, \qquad (1)$$

where $\hat{G}$ is an arbitrary system observable, $\hat{H}_I$ is the interaction Hamiltonian and $\hat{D}$ is a generalized dissipator describing the full effect of the interaction. If a set of approximations is applied in the process of deriving a spesific description of the reduced dynamics, the condition in Eq. (1) can be used to study the resulting master equation: if the condition is not obeyed naturally, an artificial effective Hamiltonian emerges in the complete desription of the dynamics destroying conservation. This provides an explanation for the charge nonconservation observed, for example, in Ref. [2] in connection with the secular approximation. Additionally, we present a few typical examples of master equations in the Lindblad form and rigorously show that the secular approximation causes nonconservation in the case vanishing dissipative current. Hence, Lindblad-type master equations are not intrinsically safe from exhibiting this type of nonphysical behavior.

To establish the pysical relevance of our theory, we study the transport of Cooper pairs through a superconducting charge pump using a recently developed master equation approach for steered systems [3]. The operation of the device is based on controlled manipulation of external voltages and magnetic fluxes in an adiabatic manner. The device is of fundamental interest since the charge pumped through it during the operation has been shown to relate to the Berry phase both theoretically and experimentally [4]. The conservation law indicates that if one studies the charge transferred through the device, dissipative current must be accounted for if the system is interacting with a flux noise environment causing phase bias fluctuations [5]. In case of charge noise, the master equation properly indicates vanishing dissipative current.

Using a scheme to engineer the noise environment, we present the response of the spectral density of the phase bias noise to external manipulation and describe the main dissipative transport characteristics. Especially, we show that the strength of the system-environment interaction can be significantly reduced to effectively decouple the system from the noise source. The dissipative currents turn out to be relatively
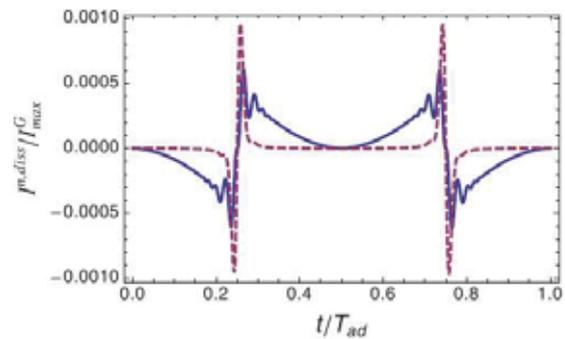
Figure 1: Dynamic dissipative current $I^{D,\text{diss}}$ (solid line) and geometric dissipative current $I^{G,\text{diss}}$ (dashed line) normalized by the maximum geometric current I_{max}^G during the driving cycle.

small in comparison especially in the steady state since they are not selective to the pumping direction. Nevertheless, the effect of tuning the coupling strength artificially should be visible in the total pumped charge.

References

[1] J. Salmilehto, P. Solinas and M. Möttönen, Phys. Rev. A, **85**, 032110 (2012).

[2] J. Prachař and T. Novotný, Physica E, **42**, 565 (2010).

[3] J. P. Pekola, V. Brosco, M. Möttönen, P. Solinas and A. Shnirman, Phys. Rev. Lett, **105**, 030401 (2010); P. Solinas, M. Möttönen, J. Salmilehto and J. P. Pekola, Phys. Rev. B, **82**, 134517 (2010).

[4] M. Möttönen, J. P. Pekola, J. J. Vartiainen, V. Brosco and F. W. J. Hekking, Phys. Rev. B **73**, 214523 (2006); M. Möttönen, J. J. Vartiainen and J. P. Pekola, Phys. Rev. Lett. **100**, 177201 (2008).

[5] P. Solinas, M. Möttönen, J. Salmilehto and J. P. Pekola, Phys. Rev. B **85**, 024527 (2012).

Informationally complete phase space observables

Jukka Kiukas[1], **Pekka Lahti**[2], **Jussi Schultz**[2] and **Reinhard F. Werner**[1]

[1] *Institute for Theoretical Physics, University of Hannover, Hannover, Germany*
[2] *Turku Centre for Quantum Physics, Department of Physics and Astronomy, University of Turku, Turku, Finland*

Informationally complete covariant phase space observables are of utmost importance from both foundational and practical aspects of quantum mechanics. Indeed, the wide variety of applications includes such issues as approximate joint measurements of position and momentum, quantization, and continuous variable quantum tomography. Here we present a simple proof for the characterization of informational completeness for these observables.

Each covariant phase space observable G^T is generated by a unique positive trace one operator T, and a necessary and sufficient condition for informational completeness can be expressed in terms of the zero set $Z(T)$ of the Weyl transform of T, the relevant condition being that $Z(T)$ has dense complement. We then consider this condition and two other possible ways to characterize the smallness of $Z(T)$, namely, that $Z(T)$ is empty, or $Z(T)$ is of Lebesgue measure zero. In particular, we present counterexamples showing that, in contrast to some previous claims, neither of these conditions is necessary for informational completeness. We discuss the meaning of these three conditions and their connection to the classical problem of characterizing the functions $f \in L^1 \cap L^p$, $1 \le p \le \infty$, having the property that the linear combinations of translates of f are dense in L^p.

We also consider the possibility of deducing the informational completeness of G^T from the state distinction properties of the unsharp position and momentum observables arising as the Cartesian margins of G^T. We show that there exist informationally incomplete phase space observables such that the margins are informationally equivalent with sharp position and momentum. This means that it is possible to reconstruct the position and momentum distributions from the statistics of a single measurement even though the state is not uniquely determined by the statistics.

Observing the Average Trajectories of Single Photons in a Two-Slit Interferometer

L. Krister Shalm[1,5], **Sacha Kocsis,**[1,2*] **Boris Braverman,**[1*] **Sylvain Ravets,**[3*] **Martin J. Stevens,**[4] **Richard P. Mirin,**[4] **and Aephraim M. Steinberg**[1†]

[1]*Centre for Quantum Information and Quantum Control and Institute for Optical Sciences, University of Toronto, Canada*
[2]*Centre for Quantum Dynamics, Griffith University, Brisbane, Australia*
[3]*Laboratoire Charles Fabry, Institut d'Optique, CNRS,Univ Paris-Sud, France*
[4]*National Institute of Standards and Technology, USA*
[5]*Institute for Quantum Computing, University of Waterloo, Canada*

In classical physics the dynamics of a particle's evolution are governed by its position and velocity; to simultaneously know the particle's position and velocity is to know its past, present, and future. The Heisenberg uncertainty principle in quantum mechanics, however, forbids simultaneous knowledge of the precise position and velocity of a particle. This makes it impossible to determine the trajectory of a single quantum particle in the same way as one would that of a classical particle—any information gained about the quantum particle's position irrevocably alters its momentum (and vice-versa) in a way that is fundamentally uncertain. It is possible, however, to "weakly" measure a system, gaining some information about one property without appreciably disturbing the future evolution [1]; while the information obtained from any individual measurement is limited, averaging over many trials determines an accurate mean value for the observable of interest, even for subensembles defined by some subsequent selection. It was recently pointed out that this procedure - weak measurement followed by post-selection - provides a natural way of operationally defining a set of average trajectories for a particle [2]. We utilize this approach to reconstruct weak-valued trajectories for single photons as they pass through a double-slit experiment [3].

In our experiment we send an ensemble of single photons, emitted one-by-one from an InGaAs quantum dot, through a two-slit interferometer and perform a weak measurement on each photon to gain a small amount of information about its momentum, followed by a strong measurement that post-selects the subensemble of photons arriving at a particular position. We use the polarization degree of freedom of the photons as a "pointer" that weakly couples to and measures the momentum of the photons. This weak momentum measurement does not appreciably disturb the system and interference is still observed. The two measurements must be repeated on a large ensemble of particles in order to extract a useful amount of information about the system. From this set of measurements, we can determine the average momentum of the photons reaching any particular position in the image plane, and by repeating this procedure in a series of planes, we can reconstruct trajectories over that range (see Fig. 1).

These experimentally reconstructed trajectories represent the average behaviour of subensembles of photons. The trajectories resemble a hydrodynamic flow with a clearly visible central line of symmetry; trajectories originating from one slit do not cross into the opposite side of the interference pattern. Furthermore, trajectories at the edges of bright fringes tend to cross over to join more central bright fringes, thus generating the observed intensity distribution due to interference. In this sense, weak measurement finally allows us to speak about
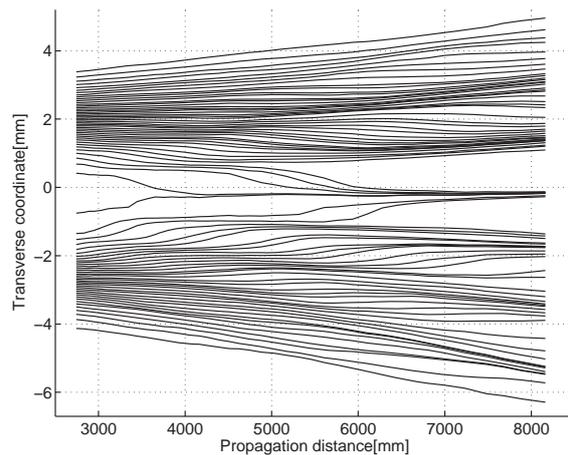
Figure 1: Reconstructed average trajectories of an ensemble of single photons in the double-slit interferometer using data from 41 imaging planes.

what "happens" to an ensemble of particles inside an interferometer. Using weak measurements we are able to provide a new perspective on the double-slit experiment, which Feynman famously considered to have in it "the heart of quantum mechanics" [4].

References

[1] Y. Aharonov, D. Z. Albert, L. Vaidman, How the Result of a Measurement of a Component of the Spin of a Spin-1/2 Particle Can Turn Out To Be 100, Phys. Rev. Lett. 60, 1351 (1988).

[2] H. M. Wiseman, Grounding Bohmian Mechanics in Weak Values and Bayesianism, New J. Phys. 9, 165 (2007).

[3] S. Kocsis et al., Observing the Average Trajectories of Single Photons in a Two-Slit Interferometer, accepted for publication in Science.

[4] R. P. Feynman, R. B. Leighton, M. L. Sands, The Feynman Lectures on Physics (Addison-Wesley, Boston, 1989).

Three qubit correlations in Four qubit States

S. Shelly Sharma[1] **and N. K. Sharma**[2]

[1]*Departamento de Fisica, Universidade Estadual de Londrina, Londrina 86051-990, PR Brazil*

[2]*Departamento de Matematica, Universidade Estadual de Londrina, Londrina 86051-990, PR Brazil*

Two multipartite pure states are equivalent under stochastic local operations and classical communication (SLOCC) [1, 2] if one can be obtained from the other with some probability using only local operations and classical communication among different parties. Attempts [3, 4] to classify four-qubit entangled pure states under SLOCC, have revealed that several entanglement classes contain a continuous range of strictly nonequivalent states, although with similar structure. In view of this, we have proposed classification criteria [5] based on nature of multiqubit correlations in N-qubit pure states. An entanglement class is characterized by the combination of $K-$way $(2 < K < N)$ partially transposed operators in the expansion of global partial transpose of canonical state. In this article, we examine the three qubit invariants of four qubit states in principle classes and derive higher degree invariants to quantify four-way and three way correlations.

For a two qubit state that is in $C^2 \otimes C^2$ space, negative eigenvalue of partial transpose is the relevant invariant to distinguish between the separable and entangled states. In three qubit state space $C^2 \otimes C^2 \otimes C^2$ two qubit subspace (for a selected pair of qubits) is characterized by a pair of two qubit invariants, while new two qubit invariants arise due to three body correlations in the composite space. The most important three qubit polynomial invariant is a degree four combination of two qubit invariants. The entanglement monotone constructed from this coincides with Wootter's three tangle. When three qubit invariant is zero, the invariants of the system involve only two-way invariants. Four qubit states sit in the space $C^2 \otimes C^2 \otimes C^2 \otimes C^2$ with three qubit subspaces for each set of three qubits. If there were no four body correlations, combinations of three tangles should determine the entanglement of four qubit state. And in the absence of three qubit correlations, the invariants depend only on two qubit invariants. When four body correlations are present, additional three qubit invariants that depend on four way negativity fonts exist. For a given set of three qubits, three qubit invariants constitute a five dimensional space and are easily found by action of a local unitary on the fourth qubit. The transformation equations for three qubit invariants yield four qubit invariants. One can continue the process to higher number of qubits. It is well known that the number of invariants increases with increase in the number of qubits. The advantage of our technique is that we obtain invariants that are easily related to invariants in sub spaces, as such to the structure of the quantum state at hand. An important point, which is relevant to classification of states is construction of polynomial invariants for states other than the most general state. Our method can be easily applied to such states.

Transformation equations under local unitary on fourth qubit are written for three qubit invariants $\left(I_4^{A_1 A_2 A_3 A_4}\right)_{A_4}$ and $\left(I_3^{A_1 A_2 A_3}\right)_{(A_4)_0}$ expressed in terms of negativity fonts [6]. From the resulting polynomial the four qubit invariant is found to be

$$
\begin{aligned}
&\left(I_4^{A_1 A_2 A_3 A_4}\right)_{A_4} \\
=\ &\left(I_3^{A_1 A_2 A_3}\right)_{(A_4)_0} \left(I_3^{A_1 A_2 A_3}\right)_{(A_4)_1} \\
&+ 3\left(T_{A_4}^{A_1 A_2 A_3}\right)^2 - 4 P_{(A_4)_0}^{A_1 A_2 A_3} P_{(A_4)_1}^{A_1 A_2 A_3}.
\end{aligned}
$$

It is a four qubit invariant of degree eight expressed in terms of three qubit invariants for $A_1 A_2 A_3$. Here $T_{A_4}^{A_1 A_2 A_3}$, $P_{(A_4)_0}^{A_1 A_2 A_3}$ and $P_{(A_4)_1}^{A_1 A_2 A_3}$ are three qubit invariants in 16 dimensional space of four qubit state. This invariant quantifies 4-way correlations in a manner similar to that of three tangle for three qubit ystem. In the absence of four-way three tangles, the transformation equations acquire a simpler form and easily yield relevant four qubit invariants composed of three-way tangles. Invariant to quantify entanglement of a four qubit state having purely two qubit correlations is also presented. What is the utility of these polynomial invariants? Quantum entanglement distributed between distant parties is an essential resource for practical quantum information processing hence the necessity to quantify entanglement. A polynomial invariant may be used to construct an entanglement monotone, a real-valued function of quantum state which decreases monotonically under local operations with classical communication.

References

[1] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A 62, 062314 (2000).

[2] F. Verstraete, J. Dehaene, B. DeMoor, and H. Verschelde, Phys. Rev. A 65, 052112 (2002).

[3] L. Lamata, J. Leon, D. Salgado and E. Solano, Phys. Rev. A75, 022318 (2007).

[4] D. Li, X. Li, H. Huang, and X. Li, Quant. Inf. Comp. 9, 0778 (2009).

[5] S. S. Sharma and N. K. Sharma, Phys. Rev. A 85, 042315 (2012).

[6] S. S. Sharma and N. K. Sharma, Phys. Rev. A 82, 052340 (2010).

Implementing the Aharon-Vaidman quantum game with a Young type photonic qutrit

Piotr Kolenderski[1,2], **Urbasi Sinha**[1], **Li Youning**[3], **Tong Zhao**[1], **Matthew Volpini**[1], **Adán Cabello**[4,5], **Raymond Laflamme**[1] **and Thomas Jennewein**[1]

[1] *Institute for Quantum Computing, University of Waterloo, 200 University Ave. West, Waterloo, Ontario, CA*

[2] *Institute of Physics, Nicolaus Copernicus University, Grudziadzka 5, 87-100 Toruń, Poland*

[3] *Department of Physics, Tsinghua University, Beijing 100084, P. R. China*

[4] *Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*

[5] *Department of Physics, Stockholm University, S-10691 Stockholm, Sweden*

The Aharon-Vaidman (AV) [1] game exemplifies the advantage of using simple quantum systems to outperform classical strategies. We present an experimental test [2] of this quantum advantage by using a three-state quantum system (qutrit) encoded in a spatial mode of a single photon passing through a system of three slits. The preparation of a particular state is controlled as the photon propagates through the slits by varying the number of open slits and their respective phases. The measurements are achieved by placing detectors in the specific positions in the near and far-field after the slits. This set of tools allowed us to perform tomographic reconstructions of generalized qutrit states, and implement the quantum version of the AV game with compelling evidence of the quantum advantage.
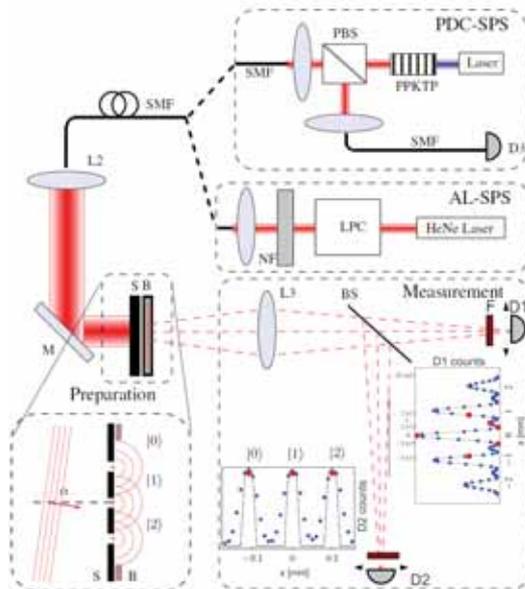
Figure 1: Thr experimental setup.

In the classical analogue of the game, Alice puts a particle in one of three boxes such that when Bob, who in next turn is allowed to check only two of them, is most likely to find it. Alice wins whenever Bob discovers the particle. Hence, it is obvious that Alice will not use the box that Bob does not have access to and therefore her chance to win is 50%. On the other hand, when she uses quantum particles her chance rises above this limit and ideally reaches 100%.

This can happen when she chooses her particle to be in the state $|\psi_A\rangle = \frac{1}{\sqrt{3}} (|0\rangle + |1\rangle + |2\rangle)$ in the first turn of the game and in the third turn she makes a projective measurement on $|\psi_{Am}\rangle = \frac{1}{\sqrt{3}} (|0\rangle - |1\rangle + |2\rangle)$. If Alice detects a particle, she accepts the game trial, and if she does not, she cancels it.

The Experimental setup is depicted in Figure 1. The AL-SPS comprises of HeNe laser, laser power controller (LPC) and neutral filter (NF). The PDC-SPS is based on PPKTP crystal pumped by blue continuous wave laser. Heralding photon is detected by detector D3. The single photons from both sources are coupled to single mode fibers (SMF). A qutrit is prepared using the blocking mask and three slits. Next the measurement part of the setup comprises of a lens (L3), a pellicle beamsplitter (BS), colour filters (F) and two detection systems (D1, D2), each comprised of multimode fiber mounted on a precise motorized stage (Thorlabs ZST13) and a Perkin Elemer avalanche photodiode.
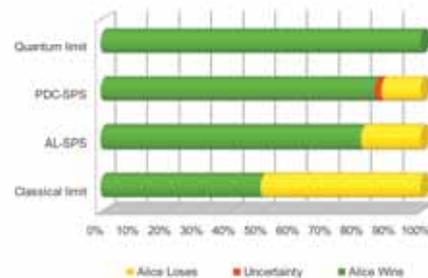
Figure 2: Experimental and theoretical, best classical and best quantum winning trials in the quantum game.

For the quantum game the qutrit was prepared in $|\psi_A\rangle$. We simulated all possible scenarios of Bob's measurement using PDC-SPS and AL-SPS. Despite the practical limitations of our experimental setup, Alice had a 87% chance to win using PDC-SPS and 82% using AL-SPS, see Figure 2. This is much better than classical strategy and close to the ideal quantum limit.

References

[1] N. Aharon and L. Vaidman, Phys. Rev. A **77**, 052310 (2008).

[2] P. Kolenderski, U. Sinha, Li Youning, T. Zhao, M. Volpini, A. Cabello, R. Laflamme, T. Jennewein, arXiv:1107.5828

Entanglement detection via mutually unbiased bases

Christoph Spengler[1], **Marcus Huber**[2], **Stephen Brierley**[2], **Theodor Adaktylos**[1] and **Beatrix C. Hiesmayr**[1,3]

[1]*University of Vienna, Faculty of Physics, Boltzmanngasse 5, 1090 Vienna, Austria*
[2]*University of Bristol, Department of Mathematics, Bristol BS8 1TW, U.K.*
[3]*Masaryk University, Institute of Theoretical Physics and Astrophysics, Kotlářská 2, 61137 Brno, Czech Republic*

We investigate correlations among complementary observables. In particular, we show how to take advantage of mutually unbiased bases (MUBs) for the detection of entanglement in arbitrarily high-dimensional quantum systems. It is shown that their properties can be exploited to construct entanglement criteria which are experimentally implementable with few local measurement settings. The introduced concepts are not restricted to bipartite finite-dimensional systems, but are also applicable to continuous variables and multipartite systems. This is demonstrated by two examples – the two-mode squeezed state and the Aharonov state. In addition, and more importantly from a theoretical point of view, we find a link between the separability problem and the maximum number of mutually unbiased bases.

Entanglement and complementarity are two key features of quantum theory. Both play a central role in numerous algorithms of quantum information processing. Although entanglement and complementarity have been extensively studied within the last decades, there still remain several open problems related to them. Regarding entanglement, one important problem concerns the reliable and efficient detection in experiments. While for bipartite two-level systems it is possible to experimentally verify the presence of entanglement by making a few joint local measurements, the number of measurements needed for entanglement detection generally scales problematically with the size of the system. Here, the main challenge for high-dimensional multiparticle systems is not only to develop mathematical tools for entanglement detection, but to find schemes whose experimental implementation requires minimal effort. In other words, the aim is to verify entanglement with as few measurement settings as possible, specifically without resorting to full state tomography.

Also complementarity still raises many unanswered questions. One of these concerns the maximum number of complementary observables for a given system. In the mathematical formalism, complementarity expresses itself through the fact that there are pairs of observables for which no common eigenbasis can be found. The extreme case of complementarity is when the eigenbases of two observables form a pair of mutually unbiased bases (MUBs). This is when all (normalized) eigenvectors of one observable have the same overlap with all eigenvectors of the other observable. The question of how many MUBs exist for a given Hilbert space has been a lively topic of research. An answer to this question is currently only known for systems of prime-power dimension. For such systems one can explicitly construct a complete set of $d + 1$ MUBs. For all other dimensions the exact number of MUBs is unknown, and it is suggested that in some cases it is impossible to obtain $d + 1$ MUBs. At the moment, it is unclear if the (non-)existence of a complete set of MUBs in non-prime-power dimensions has fundamental reasons or crucial consequences for applications. In order to shed light on these issues, we must (a) find additional applications of MUBs besides quantum state tomography and the mean king problem, and (b) develop new techniques to bound the number of MUBs.

In this poster we approach these problems in the following way (for mathematical details see Ref. [1]): We link the concept of MUBs with the separability problem. We show that one can exploit the properties of MUBs to derive powerful entanglement detection criteria for arbitrarily high-dimensional systems. These criteria are well suited for the experimental verification of entanglement as they are experimentally accessible through measuring correlations between only a few local observables. In contrast to a full state tomography where the experimental effort can grow exponentially with the system size, our approach enables optimal entanglement detection using a number of measurement settings which scales only linearly with the dimensionality of the local systems. In fact, we also show that even two local MUB settings in general are enough for a comparably robust entanglement test. Furthermore, by considering the noise thresholds of our criteria we find an interesting theoretical connection between the separability of density matrices and the maximum number of MUBs. Specifically, we provide a novel proof of the upper bound of $d + 1$ MUBs in any dimension and discuss its tightness. We also consider extensions of our methodology for continuous variables and multipartite systems. These are discussed by the example of the two-mode squeezed state and the Aharonov state.
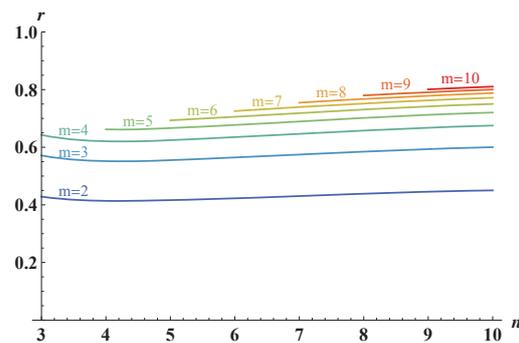
Figure 1: The noise robustness r of our criteria for the n-partite Aharonov state in the presence of white noise, i.e. $\rho_{\text{aw}} = \alpha \, |\mathcal{S}_n\rangle \langle \mathcal{S}_n| + \frac{1-\alpha}{n^n} \mathbb{1}$. For $1 - \alpha < r$ the state ρ_{aw} is detected to be genuine multipartite entangled. The detection strength increases with the number m of used MUBs.

References

[1] C. Spengler *et al.*, arXiv:1202.5058 (2012).

Tests of alternative Quantum Theories with Neutrons

S. Sponar[1], **J. Klepp**[2], **R. Loidl**[1], **C. Schmitzer**[3], **H. Bartosik**[3], **K. Durstberger-Rennhofer**[1], **H. Rauch**[1] **and Y. Hasegawa**[1]

[1]*Atominstitut, Vienna University of Technology, Austria;* [2] *Faculty of Physics, University of Vienna, Austria;* [3] *CERN, Geneve, Switzerland*

Neutron interferometry, where an interference effects of matter waves passing through a perfect silicon-crystal interferometer (see Fig. 1), is observed, and neutron polarimetry, also referred to as spin-interferometry, have established as a powerful tool for investigation of fundamental quantum mechanical concepts with massive particles. Utilizing these techniques topics such as topological effects on the wavefunction, entanglement detection and test of realistic models have been investigated in detail. Using neutron interferometry the 4π spinor symmetry of fermions, the spin-superposition law and various gravitational effects have been demonstrated [1]. Entanglement between different degrees of freedom (the neutron's spin and path) has been verified by violation of a Bell inequality [2]. Later on, influence of geometric phases on Bell measurements has been investigated in detail, demonstrating the effect of geometric phase can be balanced by a change in Bell angles [3]. In addition, preparation of Greenberger-Horne-Zeilinger entanglement [4] consisting of spin, path and total energy degree of freedom, in a single neutron system, has been performed successfully. A final value was obtained, violating a Mermin-like inequality, which clearly contradicts the noncontextual (realistic) assumption and confirms quantum contextuality.
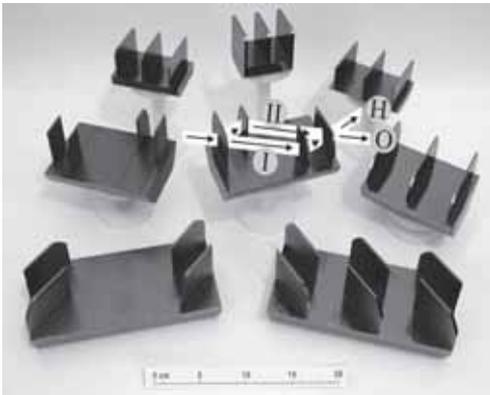
Figure 1: various neutron interferometers of triple-plate, skew-symmetric and double-loop type.

Tests of contextual realist models require a significantly higher contrast and are therefore not feasible with neutron interferometry. The advantage of neutron polarimetry compared to perfect crystal interferometry lies in high contrast and phase stability, due to its insensitive to ambient mechanical and thermal disturbances. Neutron polarimetry has been used to demonstrate fundamental quantum mechanical properties, such as noncommutation of the Pauli spin operator and a number of geometric phase measurements - for example observation of the nonadditivity of the mixed-state phase for purely geometric, purely dynamical, and combined phases [5]. Falsification of a contextual realistic model, analogous to Leggett's non-local realistic model for entangled pairs of particles [6], has been achieved using neutron polarimetry [7]. The polarimetric setup is depicted in Fig. 2, (a). Correlation measurements of the spin-energy entangled single-particle system show violation of a Leggett-type inequality by more than 7.6 standard deviations (see Fig. 2, (b)). Our experimental data rule out a class of contextual realistic theories and are fully in favor of quantum mechanics.
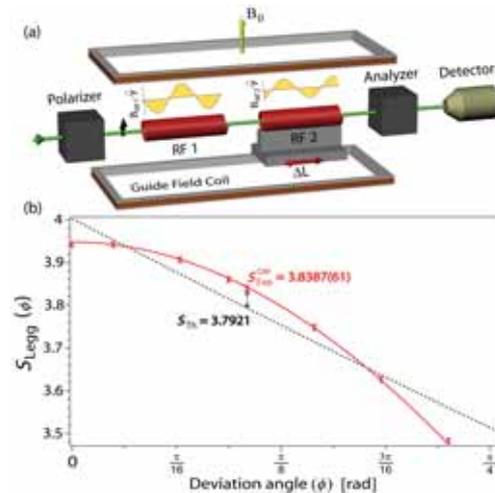
Figure 2: (a): Experimental setup of the neutron polarimetric test of Leggett's contextual realistic model. (b): Experimental results confirming the predictions of quantum mechanics.

References

[1] H. Rauch and S. A. Werner, *Neutron Interferometry*, Clarendon Press, Oxford (2000).

[2] Y. Hasegawa, R. Loidl, G. Badurek, M. Baron and H. Rauch, Nature **425**, 45 (2003).

[3] S. Sponar, J. Klepp, R. Loidl, S. Filipp, K. Durstberger-Rennhofer, R. A. Bertlmann, G. Badurek, H. Rauch and Y. Hasegawa, Phys. Rev. A **81**, 042113 (2010).

[4] Y. Hasegawa, R. Loidl, G. Badurek, K. Durstberger-Rennhofer, S. Sponar and H. Rauch, Phys. Rev. A **81**, 032121 (2010).

[5] J. Klepp, S. Sponar, S. Filipp, M. Lettner, G. Badurek and Y. Hasegawa, Phys. Rev. Lett. **101**, 150404 (2008).

[6] A. J. Leggett, Found. Phys. **33**, 1496 (2003).

[7] Y. Hasegawa, C. Schmitzer, H. Bartosik, J. Klepp, S. Sponar, K. Durstberger-Rennhofer and G. Badurek, New J. Phys **14**, 023039 (2012).

Experimental demonstration of Legett-Garg inequality violations by measurements with high resolution and back-action

Yutaro Suzuki[1], **Masataka Iinuma**[1] **and Holger F. Hofmann**[1,2]

[1]*Graduate school of Advanced Sciences of Matter, Hiroshima University, 1-3-1 Kagamiyama, Higashi-Hiroshima 739-8530, Japan*

[2]*JST, Crest, Sanbancho 5, Chiyoda-ku, Tokyo 102-0075, Japan*

The uncertainty principle limits the precision for joint measurement of non-commuting observables. In a sequential measurement, the initial measurement causes an unavoidable back-action on the system, so that the result of the final measurement cannot provide precise information about the original value of the corresponding observable. However, a realist model of measurement uncertainties could explain the measurement probabilities of sequential measurements in terms of an intrinsic joint probability represented by the initial quantum state.

The Leggett-Garg inequalties (LGI) were introduced to show that quantum statistics seems to contradict the assumptions of an intrinsic joint probability [1]. Originally, Legett and Garg argued that the spin correlations observed in separate measurements indicated a violation of their inequality, demonstrating that quantum mechanics was inconsistent with a realist model of the corresponding spins. A direct test by sequential measurements is difficult, because the initial measurement changes the output statistics of the final measurement in such a way, that the experimentally observed correlation between the input spin component and the final spin measurement does not violate the LGI anymore. Since the first measurement changes the quantum state, this could be interpreted as an effect of the measurement back-action. It might then be possible to analyze the intrinsic statistics by using an appropriate model of the statistical errors induced by the back-action.

Recently, weak measurements have been used to circumvent some of the limitations of measurement uncertainties. Weak measurements are sequential measurement where the effect of the measurement back-action in the initial measurement is minimized, so that the final measurement can be interpreted as a precise measurement of the input. Although the weak measurement result has a very low signal-to-noise ratio, average results can still be extracted from a sufficiently large number of measurements. Interestingly, weak measurements can be interpreted directly in terms of joint probabilities for the observables measured in the initial and the final measurement. The LGI violation then corresponds to a negative joint probability, and this result has indeed been observed in a number of recent experiments.

The demonstrations of LGI violations by weak measurements all depend on the assumption that the measurement uncertainty of the initial measurement merely results in a linear reduction of the observed spin expectation value. They are therefore based on a very simple error model that could also be applied to the measurement back-action. In this presentation, we analyze experimental data from a sequential measurement with variable measurement strength and show that the same intrinsic joint probability can be obtained for any combination of measurement resolution and back-action.

The experiment was realized using an interferometric setup previous introduced by us [2]. In this setup, the diagonal polarizations P and M of a single photon are distinguished by path interference. The visibility of this interference is controlled by polarization rotations that also induce the measurement back-action. The strength of the PM measurement is therefore controlled by a simple rotation of the half wave plates in the paths of the interferometer. To obtain an LGI violation, the initial state is polarized at $22.5°$, halfway between vertical V polarization and P polarization. This defines spin s_1 of the LGI inequalities. The variable strength measurement realized by our interferometric setup partially resolves the diagonal polarizations, corresponding to a second spin direction s_2. The final measurement is performed in the output ports of the interferometer and distinguishes the horizontal H and the vertical V polarization, corresponding to a third spin direction s_3.

From the photon detection rates in the output, we obtain an experimental joint probability of s_2 and s_3 for an initial state with $s_1 = +1$. These joint probabilities include resolution errors in the value of s_2 and back-action errors in the value of s_3. Since the spins and their measurement results can only take values of ± 1, each of these errors can be described by a single spin-flip probability. These spin flip probabilities can be obtained independently by characterizing the resolution and the back-action of the experimental setup. We can then reconstruct the intrinsic joint probability of the quantum state for any measurement strength by using the appropriate spin flip rates for the experimentally determined measurement resolution and back-action.

Although the experimentally observed joint probabilities depend strongly on measurement strength, the reconstructed intrinsic joint probabilities always reproduce the same theoretically predicted values, including the negative probability responsible for the LGI violation. We thus find that the LGI violation is an intrinsic property of the quantum state that does not depend on the measurement interaction used to confirm it. Moreover, our analysis demonstrates that non-classical statistics can be obtained at intermediate measurement strengths if the statistical effects of all measurement uncertainties are taken into account. Since the signal-to-noise ratio of such intermediate strength measurements is much better than that of the weak measurement limit, this possibility provides a promising alternative in the experimental investigation of quantum paradoxes and other characteristic features of quantum statistics.

References

[1] A. J Leggett and A. Garg, Phys. Rev. Lett. **54**, 857 (1985)

[2] M. Iinuma, Y. Suzuki, G. Taguchi, Y. Kadoya and H. F. Hofmann, New J. Phys. **13**, 033041 (2011)

Chain Rule Implies Tsirelson's Bound

Eyuri Wakakuwa[1] **and Mio Murao**[1,2]

[1]*Department of Physics, Graduate school of Science, The University of Tokyo*
[2]*Institute for Nano Quantum Information Electronics, The University of Tokyo*

We generalize the quantum mutual information between a classical system and a quantum system to the mutual information between a classical system and a general probabilistic system. The generalization is based on the consideration of the classical information capacity of a general probabilistic system. We then consider a bipartite nonlocality-assisted classical communication task, and investigate the receiver's information gain by using this generalized mutual information. We show that the chain rule of our generalized mutual information is more essential than information causality in the information theoretical derivation of Tsirelson's bound.

Background: Recently, *information causality* has been proposed as an information theoretical principle at the foundation of quantum mechanics [1]. Suppose that Alice wants to send to distant Bob information about N independent bits $X_1, \cdots, X_N =: \vec{X}$, under the condition that they can only use a m bit classical communication $\vec{M}$ from Alice to Bob and a supplementary no-signalling resource preshared between them (see Figure). Information causality states that, in this situation, Bob's information gain about $\vec{X}$ cannot be greater than m.

In [1], a function J to evaluate Bob's information gain is defined by

$$J := \sum_{k=1}^{N} I(X_k : G_k, \vec{M}) , \qquad (1)$$

where G_k is the outcome of Bob's measurement on his part of the preshared resource (denoted by B in the Figure), performed to obtain information about X_k after the communication. Then information causality is formulated as

$$J \leq m . \qquad (2)$$

Tsirelson's bound can be derived from this purely information theoretical constraint. Note that the function J is introduced to avoid the difficulty in consistently defining $I(\vec{X} : \vec{M}, B)$ in general probabilistic theories, which would quantify information about $\vec{X}$ contained in all that Bob has after the communication.

However, there is an issue that the choice of the function J is rather artificial, since the sum of mutual information defined over the outcomes of possibly incompatible measurements is not operationally meaningful. Interpreting J as the amount of information potentially accessible to Bob does not eliminate such artificiality.

Definition: The quantum mutual information $I(X : S_Q)$ between a classical system X and a quantum mechanical system S_Q is identified with the least upper bound on the information transmission rate by the Holevo-Schumacher-Westmoreland theorem. By way of analogy, we define a generalized mutual information $I(X : S_G)$ between a classical system X and a general probabilistic system S_G as the function that satisfies the following two properties:
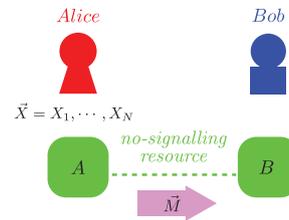
1. If $R < I(X : S_G)$, then rate R is achievable,
2. If rate R is achievable, then $R \leq I(X : S_G)$.

This generalized mutual information is always nonnegative and satisfies the data processing inequality, but does not necessarily satisfy the chain rule.

Results: Using this generalized mutual information, we evaluate Bob's information gain by $I(\vec{X} : \vec{M}, B)$ instead of J. Thus information causality is formulated as $I(\vec{X} : \vec{M}, B) \leq m$. We obtain two results. First, information causality in this formulation always holds in any general probabilistic theory. Thus comparing Bob's information gain and the amount of classical communication is not essential for the derivation of Tsirelson's bound. Second, the violation of (2) implies the violation of the chain rule $I(X, Y : S) = I(X : S) + I(Y : S, X) - I(X : Y)$. Conversely, it means that the chain rule implies (2), and consequently Tsirelson's bound. Thus we can consider the inequality (2) as one criteria for the violation of the chain rule. These two results indicate that it is not information causality but the chain rule of our generalized mutual information that implies Tsirelson's bound information theoretically.

Example: A gbit is the general probabilistic counterpart of a qubit [2]. Assuming that the classical information capacity of one gbit is not more than one bit, we derive a nontrivial restriction on the state space of a gbit from the chain rule. This is an example showing that our chain-rule-based method is applicable not only to the situation of two-party communication like information causality, but also to more general situations.

Advantage: Our method has advantages over the previous entropic approaches to the analysis of information causality in that our generalized mutual information has a highly operational meaning as the information transmission rate, and that it reveals the importance of the chain rule.

References
[1] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter and M. Zukowski, Nature 461, 1101 (2009)
[2] J. Barret, Phys. Rev. A 75, 032304 (2007)

Nonlocality of Symmetric States

Zizhu Wang and Damian Markham

CNRS LTCI, Telecom ParisTech, Département INFRES, 23 Avenue d'Italie, 75214 Paris, France

Nonlocality is a foundational feature of quantum mechanics and is increasingly becoming recognised as a key resource for quantum information theory. In this work we study the nonlocal properties of permutation symmetric states of n-qubits. We show that all these states are nonlocal, via an extended version of the Hardy paradox and associated inequalities. Natural extensions of both the paradoxes and the inequalities are developed which relate different entanglement classes to different nonlocal features. Belonging to a given entanglement class will guarantee the violation of associated Bell inequalities which see the persistence of correlations to subsets of players, whereas there are states outside that class which do not violate.

The original Hardy paradox was proposed by Hardy in the early 1990s to give an "almost probability-free" test of nonlocality for almost all bipartite entangled states [2] [3]. Instead of relying on expectation values of correlated observables, the paradox relies on a set of four conditions about probabilities of different combinations of measurement outcomes given different combinations of measurement settings. In a 2-setting/2-outcome experiment, the statements are (the binary string before the vertical line denotes outcomes, the binary string after the vertical line denotes measurement settings):

$$P(00|00) > 0 \tag{1}$$
$$P(00|01) = 0 \tag{2}$$
$$P(00|10) = 0 \tag{3}$$
$$P(11|11) = 0. \tag{4}$$

It can be shown that the first three conditions lead to the conclusion $P(11|11) = 1$, contradicting the last condition. However, Hardy showed how to find measurement settings for almost all bipartite entangled states such that all fours of these statements are satisfied. Not only that, Hardy also pointed out that these four statements can be easily put into a Bell's inequality, where if one assumes local hidden variable theory,

$$\mathcal{P}^2 = P(00|00) - P(00|01) - P(00|10) - P(11|11) \leq 0. \tag{5}$$

The extension of this paradox and inequality to n party is relatively straight forward. Each party can still only measure one of two settings, obtaining one of two outcomes. Instead of having only four conditions, we now have $n + 2$:

$$P(0\ldots0|0\ldots0) > 0 \tag{6}$$
$$P(0\ldots0|\pi(0\ldots1)) = 0 \tag{7}$$
$$P(1\ldots1|1\ldots1) = 0, \tag{8}$$

where $\pi(0\ldots1)$ denotes the permutation of the string containing $n - 1$ zeros and a single one, so the middle condition is actually n conditions. The logical contradiction arises in a similar way as the original paradox. Similarly, the inequality now becomes

$$\mathcal{P}^n = P(0\ldots0|0\ldots0) - \sum P(0\ldots0|\pi(0\ldots1))$$
$$- P(1\ldots1|1\ldots1) \leq 0. \tag{9}$$

Using the Majorana representation [4], we can find measurement settings which satisfy conditions (6) to (8) for almost all permutation symmetric states, thus also violating the inequality (9).

By an extension of the inequality (9), we can also distinguish "representative" states from different SLOCC classes by exploiting the degeneracy of their Majorana points (the qubits used in Majorana representation to represent permutation symmetric states) [1]. By noting

$$\mathcal{Q}_d^n = \mathcal{P}_n - P(\underbrace{1\ldots1}_{n-1}|\underbrace{1\ldots1}_{n-1}) - \ldots - P(\underbrace{1\ldots1}_{n-d+1}|\underbrace{1\ldots1}_{n-d+1}), \tag{10}$$

we can show that a state with degeneracy d still violates $\mathcal{Q}_n^d$ while a "representative" state with lower degeneracy does not, as shown by the example below.

(a) $\mathcal{Q}_3^4 \leq -0.0609$ (b) $\mathcal{Q}_3^4 \geq 0.0141$
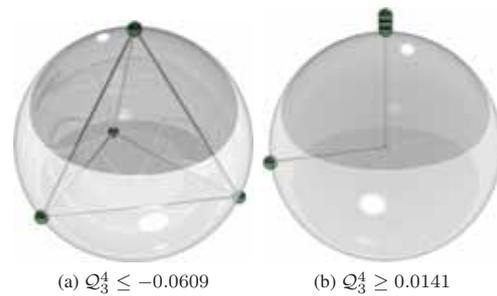
Figure 1: The state a) $|T\rangle = \sqrt{\frac{1}{3}}|0000\rangle + \sqrt{\frac{2}{3}}|S(4,3)\rangle$ does not violate $\mathcal{Q}_3^4$ while all states with degeneracy $d = 3$ do, such as the state b) $|D_3\rangle = K \sum_{perm} |000+\rangle$.

References

[1] T. Bastin, S. Krins, P. Mathonet, et al. Operational families of entanglement classes for symmetric n-qubit states. *Phys. Rev. Lett.*, 103(7):070503, Aug 2009.

[2] Lucien Hardy. Nonlocality for two particles without inequalities for almost all entangled states. *Phys. Rev. Lett.*, 71(11):1665–1668, Sep 1993.

[3] Lucien Hardy. Nonlocality of a single photon revisited. *Phys. Rev. Lett.*, 73(17):2279–2283, Oct 1994.

[4] E. Majorana. Atomi orientati in campo magnetico variabile. *Il Nuovo Cimento*, 9(2):43–50, 1932.

Loophole-free Einstein-Podolsky-Rosen Experiment via quantum steering

<u>Bernhard Wittmann</u>[1,2], Sven Ramelow[1,2], Fabian Steinlechner[2], Nathan K. Langford[2], Nicolas Brunner[3], Howard M. Wiseman[4], Rupert Ursin[2] and Anton Zeilinger[1,2]

[1]*Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, Vienna, Austria*

[2]*Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Vienna, Austria*

[3]*H.H. Wills Physics Laboratory, University of Bristol, Bristol, Australia*

[4]*Centre for Quantum Computation and Communication Technology, Centre for Quantum Dynamics, Griffith University, Brisbane, Australia*

The term steering was introduced by Schrdinger in 1935[1, 2] as a reply to the famous EPR paper[3] to describe the fact that entanglement would seem to allow an experimenter to remotely steer the state of a distant system. EPR concluded that quantum mechanics seems to be not complete and Einstein called this spooky action at a distance. Experiments testing quantum mechanics have provided increasing evidence against local realistic theories. However, a conclusive test that simultaneously closes all major loopholes (the locality, freedom-of-choice, and detection loopholes) remains an open challenge. Therefore it is still possible to explain the outcome of all up to date experiments in the framework of local realism (classical theory). Here, we present the first loophole-free demonstration of the EPR-experiment via quantum steering. We demonstrates this effect while simultaneously closing all loopholes: both the locality loophole and a specific form of the freedom-of-choice loophole are closed by having a large separation of the parties and using fast quantum random number generators and the fair-sampling loophole is closed by having high overall detection efficiency. Thereby, we exclude for the first time loophole-free an important class of local realistic theories. Beside its foundational importance loophole-free steering is relevant for device-independent certification of quantum entanglement.

to predict his result (+1, -1). Provided the correlation between her prediction and his result is above the steering bound, Bob is forced to conclude Alice indeed remotely steered his state (spooky action at a distance), or give up his assumption of a local quantum state. **Bottom:** Using entangled pairs of photons produced by an EPR source Alice can demonstrate steering. She measures her photon with the same setting Bob announced. Entanglement ensures (anti)-correlations between Alices and Bobs outcomes for all measurement choices and allows to violate the steering bound. To close the fair sampling loophole one must also account for Alices inconclusive (0) results when she detects no photon and include these results when calculating the steering value.

References

[1] E. Schrödinger, Discussion of probability relations between separated systems, Proc. Camb. Phil. Soc. **31**, 553 (1935).

[2] H. M. Wiseman, S. J. Jones. A. C. Doherty, Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox, Phys. Rev. Lett. **98**, 140402 (2007).

[3] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777-780 (1935).
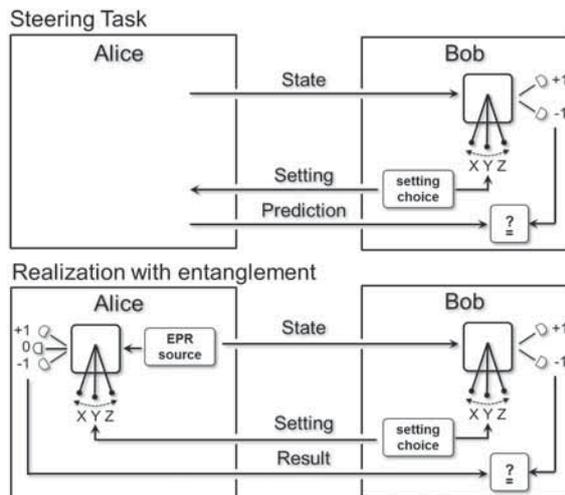
Figure 1: **Top:** In a steering experiment, Alice sends a system to Bob that he assumes to be an unknown local quantum state[2]. Next Bob chooses freely in which setting (X, Y or Z) to measure. Then he sends his choice of setting to Alice and records secretly his measurement result. Bob now challenges Alice, who claims that she can steer his state from a distance,

Quantum interferometric visibility as a witness of general relativistic proper time

Magdalena Zych[1]**, Fabio Costa**[1]**, Igor Pikovski**[1]**, and Časlav Brukner**[1] [2]

[1]*Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria*
[2]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, Vienna, Austria*

Current attempts to probe general relativistic effects in quantum mechanics focus on precision measurements of phase shifts in matter-wave interferometry. Yet, phase shifts can always be explained as arising due to an Aharonov-Bohm effect, where a particle in a flat space-time is subject to an effective potential. Here we propose a novel quantum effect that cannot be explained without the general relativistic notion of proper time. We consider interference of a "clock" - a particle with evolving internal degrees of freedom - that will not only display a phase shift, but also reduce the visibility of the interference pattern. According to general relativity proper time flows at different rates in different regions of space-time. Therefore, due to quantum complementarity the visibility will drop to the extent to which the path information becomes available from the "clock". Such a gravitationally induced decoherence would provide the first test of a genuine general relativistic notion of proper time in quantum mechanics.

Figure 1: According to general relativity, time flows differently at different positions due to the distortion of space-time by a nearby massive object. A single clock being in a superposition of two locations allows probing quantum interference effects in combination with general relativity [**?**]. Image credits: Quantum Optics, Quantum Nanophysics, Quantum Information; University of Vienna.

general relativistic proper time. *Nat. Commun.* **2**, doi:10.1038/ncomms1498 (2011).

References

[1] Zych, M., Costa, F., Pikovski, I. & Brukner, Č. Quantum interferometric visibility as a witness of

Quantum metrology with a scanning probe atom interferometer

Caspar F. Ockeloen, Max F. Riedel, Roman Schmied, and Philipp Treutlein

Department of Physics, University of Basel, Switzerland

Spin squeezing is a form of entanglement with immediate practical applications in quantum metrology [1, 2]: entanglement between N particles can reduce the uncertainty of an interferometric measurement from the standard quantum limit (SQL) $\Delta\varphi \geq 1/\sqrt{N}$ towards the ultimate Heisenberg limit $\Delta\varphi \geq 1/N$. In situations where the particle number N cannot easily be increased, spin squeezing can lead to a significant improvement of the measurement precision [3].

We have previously spin-squeezed the collective hyperfine pseudo-spin of a ^{87}Rb Bose–Einstein condensate by -2.5 dB [4] and analyzed the resulting states by quantum tomography [5]. We now make practical use of these spin-squeezed states by experimentally realizing a Ramsey interferometer operating beyond the SQL [6]. Our interferometer outperforms an ideal classical interferometer with the same number of particles (~ 1300) by -4 dB for interrogation times up to 20 ms.

We first produce spin-squeezed states by controlled collisional interactions between the atoms using a state-dependent microwave near-field potential generated on an atom chip [4]. We observe spin noise reduction by up to 4.5 dB below the SQL with a spin coherence of more than 98%, which is a witness for a depth of entanglement of at least 40 particles [2]. These states are then used as input in a Ramsey interferometer sequence. We use our interferometer to perform sub-shot-noise measurements of the microwave field from an integrated waveguide on the atom chip. In order to perform spatially resolved measurements, the spin-squeezed Bose–Einstein condensate is scanned over tens of micrometers without loss of entanglement.

Our experiments are performed on a micro-fabricated atom chip providing small and well-localized trapped atomic ensembles. This makes our technique promising for high-precision measurements with micrometer spatial resolution, *e.g.* probing electromagnetic fields close to the chip surface.

Figure 1: Tomographically reconstructed Wigner function of the spin-squeezed input state to our sub-SQL interferometer [5].

References

[1] D. J. Wineland, J. J. Bollinger, W. M. Itano, and D. J. Heinzen. Squeezed atomic states and projection noise in spectroscopy. *Phys. Rev. A*, 50(1):67–88, 1994.

[2] A. S. Sørensen and K. Mølmer. Entanglement and extreme spin squeezing. *Phys. Rev. Lett.*, 86(20):4431–4434, 2001.

[3] The LIGO Scientific Collaboration. A gravitational wave observatory operating beyond the quantum shot-noise limit. *Nature Physics*, 7:962–965, 2011.

[4] M. F. Riedel, P. Böhi, Y. Li, T. W. Hänsch, A. Sinatra, and P. Treutlein. Atom-chip-based generation of entanglement for quantum metrology. *Nature*, 464:1170–1173, 2010.

[5] R. Schmied and P. Treutlein. Tomographic reconstruction of the Wigner function on the Bloch sphere. *New J. Phys.*, 13:065019, 2011.

[6] C. F. Ockeloen, M. F. Riedel, R. Schmied, and P. Treutlein. Quantum metrology with a scanning probe atom interferometer. *Manuscript in preparation*, 2012.

Towards a nuclear clock with Thorium-229

Matthias Schreitl[1], **Georg Winkler**[1], **Georgy Kazakov**[1,2], **Georg Steinhauser**[1] and **Thorsten Schumm**[1]

[1] *Vienna University of Technology, Vienna, Austria*
[2] *St-Petersburg State Polytechnic University, St-Petersburg, Russia*

The current time standard uses a hyperfine transition of the electronic ground state of Cesium. An improvement of the clock's Q-factor by some orders of magnitude could be achieved by exploiting transitions with higher energy differences, e.g. in the optical range. However, challenges like Doppler-broadening due to the thermal movement of the atoms and finding a sufficiently long-living state which provides a narrow line width have to be mastered. Promising approaches are Sr lattice clocks [1] and Hg^+-ion clocks [2].

Nuclear transitions can be much more stable against external perturbations due to the shielding of the electrons and offer a huge range of possible lifetimes. Usually the energy of nuclear states are in the range of keV or even MeV which reflects in entirely different tools and methods compared to atomic physics: particle accelerators instead of lasers for state manipulation.

The isotope Thorium-229 however is predicted to provide a unique low-energy excited state which is separated by only $7.6 \pm 0.5\ eV$ [3] from the ground state and thereby in the range of UV lasers which would make coherent manipulation of these nuclei possible. An expected lifetime of several hours [3] makes this transition an excellent candidate for a new time standard, with a potential to outperform existing clocks by orders of magnitudes. Our experimental approach consists in embedding $^{229}Th^{4+}$ in the UV-transparent crystal structure of Calcium fluoride (CaF_2). This provides the advantages of having a room-temperature solid-state sample with a great number of nuclei (crystals with up to 10^{18} nuclei/cm^3 of the chemically identical ^{232}Th are already available). Furthermore this method does not require a complex experimental setup like in atom or ion traps and the small crystal which hosts the nuclei of interest can easily be combined with high flux excitation sources like UV lamps and synchrotrons. Since the Th^{4+}-ions in the crystal lattice are expected to be confined in the Lamb-Dicke regime, the nuclei experience no sensitivity to recoil or first-order Doppler effects.

The next steps in our experiment include the characterization of the crystals doped with ^{232}Th in order to ensure the transparency in the relevant wavelength region, the reliable substitution of the Thorium ions in the crystal lattice and the role of defects. A broadband UV-lamp will subsequently be used to try to excite the predicted nuclear transition and detect fluorescence in a crystal doped with ^{229}Th. A frequency comb is currently set up which will be transferred to the 160 nm region by a high-harmonic generation build-up cavity and will be used as a precision measurement tool for comparison of the nuclear transition to other frequency standards.

Current theories that attempt to unify gravity with the other fundamental forces can lead to spatial and temporal variation of fundamental constants [4]. Nuclear energy states are mainly affected by the strong interaction and Coulomb repulsion. A precise measurement of the uniquely low nuclear transition frequency in ^{229}Th will therefore allow to measure possible variations of the fine-structure constant with increased precision [5, 6] since the variations in a nucleus are enhanced compared to atomic transitions.

References

[1] A. D. Ludlow et al., Science **319**, 1805 (2008).

[2] T. Rosenband et al., Science **319**, 1808 (2008).

[3] B. R. Beck, J. A. Becker, P. Beiersdorfer, G. V. Brown, K. J. Moody, J. B. Wilhelmy, F. S. Porter, C. A. Kilbourne, and R. L. Kelley, Phys. Rev. Lett., **98**, 142501 (2007).

[4] K.A. Olive and Y. Z. Qian, Phys. Today 57, **10**, 40 (2004).

[5] V. V. Flambaum, Phys. Rev. Lett., **97**, 092502 (2006).

[6] X.-T. He, and Z.-Z. Ren, Nucl. Phys. A **806**, 117 (2008).

High-resolution Quantum Interferometry Meets Telecom Industry Needs

A. V. Sergienko[1,3], **A.M. Fraine**[1], **O.V. Minaeva**[1,2], **R. Egorov**[1], **D. S. Simon**[1,4]

[1]*Dept. of Electrical & Computer Engineering, Boston University, Boston, Massachusetts 02215*
[2]*Dept. of Biomedical Engineering, Boston University, Boston, Massachusetts 02215*
[3]*Dept. of Physics, Boston University, Boston, Massachusetts 02215*
[4]*Dept. of Physics and Astronomy, Stonehill College, 320 Washington Street, Easton, MA 02357*

A quantum interferometric measurement of polarization mode dispersion (PMD) of commercial telecommunication wavelength selective switch (WSS) demonstrates advantages of quantum optical technology over conventional measurement. It provides greater precision than that of currently available commercial PMD characterization devices thus saving a great deal of networking hardware resources that must be allocated for PMD compensation in metropolitan networks.

Quantum information, quantum computing, and quantum communication have been at the focus of research activities all over the world. A great number of exciting theoretical concepts have been developed and published in the best research journals, and many of those concepts have been realized experimentally. Currently, the biggest concern is whether any of those exciting quantum principles and technological approaches will be useful for solving real-world technical challenges. This highlights an importance of demonstrating how practical technologies benefiting from the higher dimensionality of entangled states can beat the best classical optical measurement approaches.

The need for high-resolution dispersion measurements is increasing with current trends in high-speed fiber optic networks. The highest information transmission load per fiber is currently in metropolitan settings, where the requested traffic rate is extremely high but fiber resources are not as huge as in trunk lines. Until the widespread deployment of ROADM (reconfigurable optical add-drop module) systems, only the optical fiber was considered to be the major contributor to the overall system PMD. With an increase in the number of discrete network components, the aggregate effect of component PMD is becoming comparable to the PMD introduced by the fiber. The evaluation of dispersion parameters from each discrete component such as optical switch, router, or amplifier is becoming critical for the overall system performance because of high (and variable) number of such elements engaged in each connection. In particular, it is desirable to measure extremely small values of polarization mode dispersion (PMD) ($< 10 fs$) to avoid over-budgeting PMD compensation resources in metropolitan networks due to misinterpretation from conventional measurement devices with resolution on the order of 100 fs.

We report on the first realization of practical quantum measurement technology: high-resolution evaluation of polarization mode dispersion (PMD) in switching and routing elements of modern telecommunication networks using quantum interferometry with polarization entangled photons. This current result is based on several earlier theoretical and experimental findings [1, 2, 3] During the initial demonstration of underlying physical principles in the laboratory (see
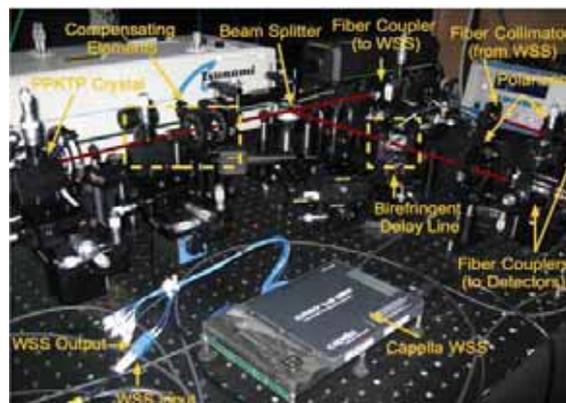
Figure 1: Optical layout for PMD measurement in MEMS-based WSS.

Fig. 1) we demonstrated its practical usefulness for the the company that manufactures modern telecom devices such as wavelength selective switches (WSS) [4]. The demonstrated high resolution in evaluating specific values of PMD for each channel of purely optical networking switch will allow industrial telecom system integrators (such as Ciena, Cisco, Alcatel, Infinera, etc..) to save significant resources (hardware, energy, and labor cost) by avoiding the need to budget for excessive PMD compensation circuits that is dictated by the lower resolution of best traditional technologies.

The approach used to achieve this goal actively uses polarization entangled states of light, which are responsible for such non-classical effects as dispersion cancellation and simultaneous measurement of group and phase velocity in a single interferometric measurement. The value of this new technology will be growing in the future because the constantly increasing speed of telecommunication signal transfer in metropolitan network will require greater resolution for evaluation and handling PMD.

References

[1] A.V. Sergienko, Y.H. Shih, M.H. Rubin, J. Opt. Soc. of Am. B, **12**, 859 (1995).

[2] D. Branning, A.L. Migdall, A.V. Sergienko, Phys. Rev. A, **62**, 063808 (2000).

[3] A. Fraine, D.S. Simon, O. Minaeva, R. Egorov, A.V. Sergienko, Opt. Exp., **19**, 22820 (2011).

[4] A. Fraine, O. Minaeva, D.S. Simon, R. Egorov, and A.V. Sergienko, Optics Express, v. **20**, pp. 2025-2033 (2012).

On Signal Amplification via Weak Measurement

Yutaka Shikano

Institute for Molecular Science, Japan
Chapman University, California, United States

The weak measurement proposed by Aharonov and his colleagues [1] extracts information of a physical quantity of the system by post-selection as the shifts of the argument of the probe wavefunction. The shift is called the weak value and is larger for the post-selected state more orthogonal to the initial state. Usually, the weak value is a useful tool to understand the foundations of quantum mechanics, for more details see the review paper [2]. Recently, the signal amplification by the weak measurement has been extensively studied. In the case that the weak value ——— with the pre-selected state and the post-selected state and the coupling constant between the system and the probe in the von Neumann interaction are given, the optimal probe wavefunction in the momentum space is obtained as

$$\underline{\hspace{2cm}} \qquad \underline{\hspace{2cm}}$$
$$\underline{\hspace{2cm}} \underline{\hspace{3cm}}$$

when , , and the support of the function is [3]. The optimal probe wavefunction gives and the maximum shift of the expectation value of the probe position as

$$\underline{\hspace{2cm}}$$

We emphasize that the maximum shift is given only by the weak value and has no upper bound as becomes large. On the other hand, the shifts given by the Gaussian probe wavefunction has the upper bound because of the back action as explained before. The back action factor is canceled out in the expression for optimal probe wavefunction, and therefore we have understood the reason for the amplification to have no upper bound. In this presentation, I shall explicitly obtain the optimal probe wavefunction and the amplification factor for a given weak value, which can be calculated from experimental setup. It is shown that the amplification factor has no upper bound in contrast to the Gaussian probe wavefunction and that the signal is sharp. Also, I will discuss the optimality for the shot-noise ratio in the same setup.

References

[1] Y. Aharonov, D. Z. Albert, and L. Vaidman, Phys. Rev. Lett. **60**, 1351 (1988).

[2] Y. Shikano, in "Measurements in Quantum Mechanics", edited by M. R. Pahlavani (InTech, 2012) p. 75.

[3] Y. Susa, Y. Shikano, and A. Hosoya, arXiv:1203.0827.

Reconstruction of single photon's transverse spatial wave function

Piotr Kolenderski[(1,2)], **Artur Czerwinski**[(2)] **Carmelo Scarcella**[(3)], **Simone Bellisai**[(3)], **Alberto Tosi**[(3)], **and Thomas Jennewein**[(1)]

[(1)] *Institute for Quantum Computing, University of Waterloo, 200 University Ave. West, Waterloo, Ontario, Canada*
[(2)] *Institute of Physics, Nicolaus Copernicus University, Grudziadzka 5, 87-100 Toruń, Poland*
[(3)] *Politecnico di Milano, Dipartimento di Elettronica e Informazione Piazza Leonardo da Vinci 32, I-20133 Milano, Italy*

In 1933 Pauli was pondering if a wave function of a particle was uniquely determined by probability distributions of its position and momentum [1]. The problem of reconstruction the complex wave from measurable intensity distributions appears in many branches of physics, e.g. coherence theory, electron microscopy and so forth, so there have been many approaches to solve it. We are using Paulis ideas in quantum optics in conjunction with a phase retrieval algorithm [2], which is a tool to compute a wave function from the two intensity measurements.
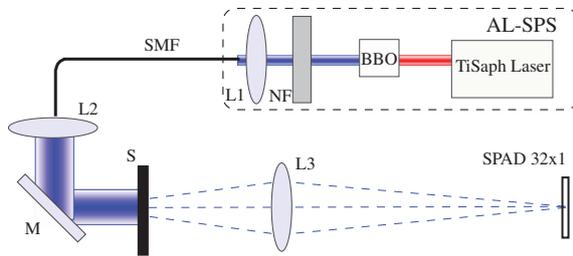
Figure 1: Experimental setup.

The experimental setup depicted in Figure 1 consists of attenuated laser source (AL-SPS) comprised of TiSaph pulsed laser pumping 2 mm thick BBO crystal used to generate second harmonic at $\lambda = 396$ nm. The light is attenuated and coupled into single mode fiber (SMF) using lens L1. Next, the photon is prepared in gaussian mode of a diameter ≈ 3 mm in diameter FWHM. This allows to justify the assumption that it is a plane wave at the slits (S) of the characteristic with $30\mu m$ and the distance between each two $100\mu m$. Next, the photon propagates through the lens ($f = 150$mm) (L3). The flip mirrors are set such that the array of 32 by 1 single photon avalanche diodes (SPAD) [3] can measure either an image $\psi(x)$ or an interference pattern $\tilde{\psi}(k_x)$, where $k_x = 2\pi x/f\lambda$.

The procedure is based on Gerchberg and Saxton work [2]. The input data to the algorithm is: the probability distributional of position $|\psi(x)|^2$ and momentum $|\tilde{\psi}(k_x)|^2$. The result is the phase $\psi(x)$. The iterative steps can are as follows:

1. Take random initial phase $\phi_0(x)$.

2. Evaluate inverse fourier transform of $|\tilde{\psi}(x)|\exp(i\phi_m(x))$. Here $\phi_m(x)$ is the phase retrieved at the mth iteration of the algorithm.

3. Evaluate fourier transform of $|\tilde{\psi}(x)|\exp(i\tilde{\phi}_m(x))$, where $\tilde{\phi}_m(x)$ is a phase of the inverse fourier transform from the previous step.

4. Take the phase of the result and start again at step 2.
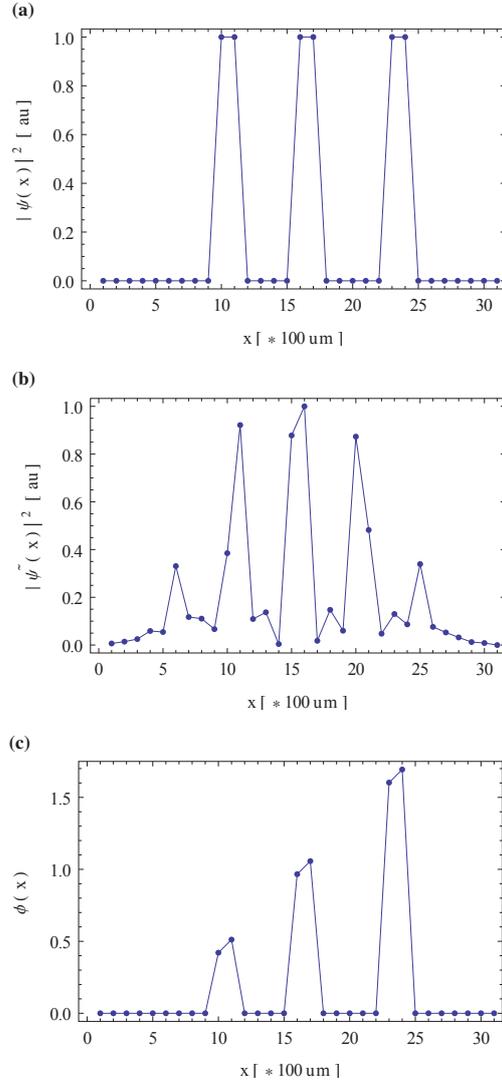
Figure 2: Numerically simulated (a) $|\psi(x)|^2$ and (b) $|\tilde{\psi}(x)|^2$. (c) The result of the phase retrieval algorithm $\phi(x)$.

The simulation results in one dimension are depicted in Figure 2.

References

[1] J. R. Fienup, Appl. Opt., **21**, 2758, (1982).

[2] R. Gerchberg and W. O. Saxton, Optik,**35**, 237, (1971).

[3] F. Guerrieri *et. al.* , IEEE Phot. Journal, **2**, 759 (2010).

Phase estimation for noisy detectors via parametric amplification

Nicolò Spagnolo[1]**, Chiara Vitelli**[1]**, Vittorio Giovannetti**[2]**, Lorenzo Maccone**[3] **and Fabio Sciarrino**[1,4]

[1]*Dipartimento di Fisica, Sapienza Università di Roma, Rome, Italy*
[2]*NEST, Scuola Normale Superiore and Istituto Nanoscienze-CNR, Pisa, Italy*
[3]*Dipartimento di Fisica, Università di Pavia, Pavia, Italy*
[4]*Istituto Nazionale di Ottica (INO-CNR), Firenze, Italy*

From the investigation of fragile biological samples, such as tissues or blood proteins in aqueous buffer solution, to gravitational wave measurements, the estimation of an optical phase ϕ [1] through interferometric experiments is an ubiquitous technique. For each input state of the probe, the maximum accuracy of the process, optimized over all possible measurement strategies, is provided by the quantum Fisher information I_ϕ^q through the quantum Cramér-Rao (QCR) bound [1]. In the absence of noise and when no quantum effects (like entanglement or squeezing) are exploited in the probe preparation, the QCR bound scales as the inverse of the mean photon number, the Standard Quantum Limit (SQL). Better performances are known to be achievable when using entangled input signals. However, the sensitivity in optical phase estimation experiments is strongly affected by losses during the signal propagation or at the detection stage. The optimal quantum states of the probing signals in the presence of loss were recently found. However, in many cases of practical interest, their associated accuracy is worse than the one obtainable without employing quantum resources but neglecting the detector's loss. Additionally, in the presence of loss, the SQL can be asymptotically beaten only by a constant factor, so that sophisticated sub-SQL strategies (implemented up to now only for few photons) may not be worth the effort. An alternative approach, exploited in gravitational wave interferometry, relies on combining an intense coherent beam with squeezed light on a beam-splitter, obtaining an enhancement in the sensitivity of a constant factor proportional to the squeezing factor.

We report an experimentally feasible strategy that leads to significantly improved performances in presence of a lossy environment. Our scheme employs a conventional interferometric phase sensing stage, and exploits an optical parametric amplifier (OPA) carrying the phase after the interaction with the sample, but before the lossy detectors [see Fig. 1]. The OPA (an optimal phase-covariant quantum cloning machine) transfers the properties of the injected state into a field with a larger number of particles, robust under losses and decoherence [2], thus allowing us to protect the information on the phase ϕ encoded in the probe state.

We discuss the experimental implementation of the amplifier-based strategy with different classes of probe states. A first quantum interferometric experiment has been performed with single-photon probes [3], showing that a significant enhancement in the phase sensitivity can be reached in the high losses regime with the present method. We then demonstrated both theoretically and experimentally the performances of this scheme when coherent-states probes are adopted. A detailed analysis of the quantum Fisher information [1] show that, by adopting the amplification-based strat-
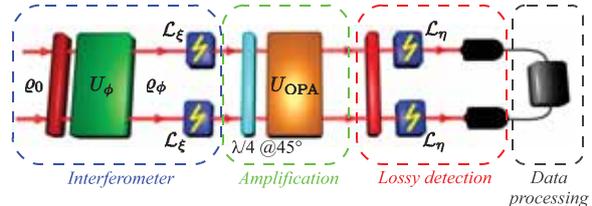
Figure 1: Scheme of the amplifier based strategy. The probe state undergoes an optical parametric amplification process before lossy detection but after the interaction with the sample.

egy, the extracted information on the phase ϕ can achieve the quantum Cramér-Rao bound associated to the coherent probe state measured with a perfect detection apparatus. We then describe the experimental implementation with coherent-states probe in high lossy conditions, showing that we can achieve a significative phase-sensitivity enhancement with respect to the coherent probe based strategy, and that the optimal performances of the scheme can be achieved with a suitable data-processing. Furthermore, no post-selection is employed to filter the output signal.

The present strategy can find application in all contexts where the sample under investigation is fragile with respect to the intensity of the impinging field, such as optical microscopy or the analysis of biological systems, since the amplification process is performed after the probe-sample interaction. As a further perspective, we discuss how the present strategy can be exploited in phase estimation protocols with noisy detectors involving quantum probe states, such as squeezed light. The adoption of the amplifier based strategy can lead to an extension of the parameter's region where the adoption of quantum resources can effectively lead to sub-SQL performances in phase estimation tasks.

References

[1] V. Giovannetti, S. Lloyd, and L. Maccone, Nature Phot. **5**, 222 (2011).

[2] N. Spagnolo, C. Vitelli, T. De Angelis, F. Sciarrino, and F. De Martini, Phys. Rev. A **80**, 032318 (2009).

[3] C. Vitelli, N. Spagnolo, L. Toffoli, F. Sciarrino, and F. De Martini, Phys. Rev. Lett. **105**, 113602 (2010).

[4] N. Spagnolo, C. Vitelli, V. G. Lucivero, V. Giovannetti, L. Maccone and F. Sciarrino, e-print arXiv:1107. (2011).

Understanding boundary effects in quantum state tomography – one qubit case

Takanori Sugiyama[1]**, Peter S. Turner**[1] **and Mio Murao**[1]

[1]*The University of Tokyo, Tokyo, Japan.*

For parameter estimation with finite data sets, the expected infidelity can deviate significantly from its asymptotic (large data set) behavior. A major reason for this is the existence of a boundary in the parameter space imposed by constraints, such as the positive semidefiniteness of density matrices. Applying ideas from classical statistical estimation theory, we show that, at least in the case of one qubit state estimation, this nonasymptotic behaviour can be predicted with high precision.

Quantum estimation: For successful experimental implementation of any quantum information protocol, the quantum states involved must be confirmed to be sufficiently closed to their theoretical targets. One way to obtain such a confirmation is to perform another experiment and from the obtained data make an estimate of the density matrix involved. Statistically, this is a constrained multi-parameter estimation problem – the quantum estimation problem – where we assume we are given a finite number of identical copies of a quantum state, N, we perform measurements whose mathematical description is assumed to be known, and from the outcome statistics we make our estimate. Due to the probabilistic behavior of the measurement outcomes and the finiteness of the number of measurement trials, there always exist statistical errors in any quantum estimate. The size of the error depends on the choice of the measurements and the estimation procedure. In statistics, the former is called an experimental design, while the latter is called an estimator. It is, therefore, important to evaluate the size of the error for a given combination of experimental design and estimator for a given finite N.

Asymptotic theory: A standard combination in quantum information experiments is that of quantum tomography and maximum likelihood estimator. Although the term "quantum tomography" can be used in several different contexts, we use it to mean an experimental design in which an independently and identically prepared set of measurements are used throughout the entire experiment [1]. The expected infidelity, $\bar{\Delta}_N$, is the statistical expectation value of the infidelity between the true and the estimated density matrices, and is used as a measure for evaluating the effect of the statistical errors on the estimated density matrix. The asymptotic behavior of the expected infidelity for this combination has been studied very well [2]. Using the asymptotic theory for parameter estimation, we can show that for sufficiently large N,

$$\bar{\Delta}_N \sim \frac{\text{tr}[HF^{-1}]}{N}, \qquad (1)$$

where H is the Hesse matrix of the infidelity and F is the Fisher matrix.

Nonasymptotic results: We consider the standard experimental design given by repeated XYZ projective measurements, and a maximum likelihood estimator. Figure 1 shows numerical results for the expected infidelity for the following three true states: the totally mixed state with Bloch vector $(r, \theta, \phi) = (0, 0, 0)$ (solid line), the nearly pure 'aligned' state
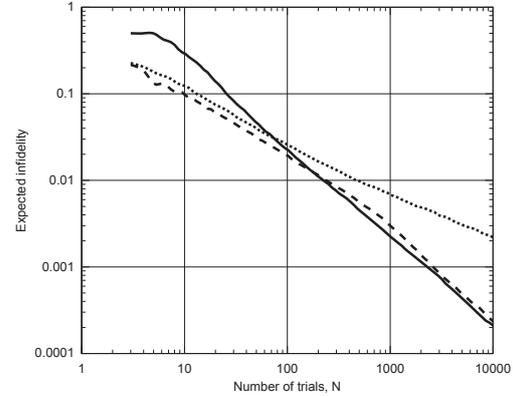
Figure 1: Behaviour of the expected infidelity for estimation of three different true states, see text for details.

$(0.99, 0, 0)$ (dashed line), and the nearly pure 'misaligned' state $(0.99, \pi/4, \pi/4)$ (dotted line). We see for all $N > 10$, the mixed state behaves roughly as $O(1/N)$, while the misaligned converges more slowly. The aligned state is interesting, as it switches between these two behaviours at around $N = 1000$, an experimentally realistic value, also reported in [3, 4]. This shows that there are regions of applicability of Eq. (1), defining nonasymptotic and asymptotic values of N, which depend strongly on the true density matrix. One of the main reasons for this deviation from asymptotic behaviour is the existence of a boundary in the parameter space, imposed by the condition that density matrices be positive semidefinite. Applying ideas from classical statistical estimation theory, we derive a simple function that reproduces the plots in Figure 1 with high precision. This makes it possible to predict the point at which the behavior of the expected infidelity switches to $O(1/N)$, which can be useful for adaptive estimation schemes.

References

[1] M. Paris and J. Řeháček, *Quantum State Estimation*, Lecture Notes in Physics (Springer, Berlin, 2004).

[2] R. D. Gill and S. Massar, Phys. Rev. A **61**, 042312 (2000).

[3] M. D. de Burgh, N. K. Langford, A. C. Doherty, and Alexei Gilchrist, Phys. Rev. A **78**, 052122 (2008).

[4] T. Sugiyama, P. S. Turner, and Mio Murao, quant-ph/1203.3391v1.

Measurement of two-mode squeezing with photon number resolving multi- pixel detectors

Dmitry A. Kalashnikov[1], **Si-Hui Tan**[1], **Timur Sh. Iskhakov** [2], **Maria V. Chekhova**[2] and **Leonid A. Krivitsky**[1]

[1]*Data Storage Institute, Agency for Science, Technology and Research, Singapore*
[2]*Max Planck Institute for the Science of Light, Erlangen, Germany*

The development of photon number resolving detectors, such as single photon avalanche detectors (SPADs) and transition edge sensors (TESs), enables the characterization of multiphoton entangled states which are promising resources for quantum communication, measurement and computation. In this work, the measurement of a two-mode squeezed vacuum (SV) state generated in an optical parametric amplifier (OPA) was performed with photon number resolving multi-pixel counters (MPPCs). Although the MPPC has already been used to study SV states [1], these studies were restricted to the regime of much less than one photon per pulse. We expand the application of the MPPC to the study of relatively bright SV states with up to 5 photons per pulse.

Strong correlation between the photon numbers in the signal and idler modes of the SV state results in the suppression of the variance of their difference below the shot-noise limit and quantified by the noise reduction factor (NRF),

$$\text{NRF} = \frac{\text{Var}(\widehat{N}_s - \widehat{N}_i)}{\langle \widehat{N}_s + \widehat{N}_i \rangle}, \qquad (1)$$

where $\widehat{N}_s$ and $\widehat{N}_i$ are the photocount operators of the detectors in the signal and idler modes respectively. The MPPC is prone to crosstalk, which contributes spurious counts almost simultaneously with the detection of real photons. At 5 photons per pulse, the MPPC also exhibits saturation. The loss, crosstalk and saturation in the MPPC were modeled by a positive-operator value measure (POVM) of [2], where loss and crosstalk are considered as Bayesian processes. Saturation limits the photon number resolution to $N_{\max}$ photons. Let us denote $\langle \hat{n} \rangle$ as the mean photon number impinging on the detector, P as the crosstalk probability, and η as the q.e. of the detector, which also accounts for the losses in the optical system.

Using the POVM, we show that as $\langle \hat{n} \rangle \to 0$, $\text{NRF} = \frac{1+3P}{1+P}$ for the coherent state which is greater than unity–the value expected for a lossy PNRD without the crosstalk. Thus, the effect of the crosstalk is to increase the NRF. Also, as $\langle \hat{n} \rangle \to 0$ for the SV state the model yields $\text{NRF} = \frac{1+3P}{1+P} - (1 + P)\eta$. Thus the difference in NRF values for the two states is equal to the effective q.e. of the detectors $\eta_E \equiv (1 + P)\eta$, differing from the absolute q.e. due to the presence of crosstalk. Numerical calculations show that the effect of saturation is to decrease the NRF with increasing $\langle \hat{n} \rangle$. Fig. 1 shows the experimental data and theoretical fits of NRF versus $\langle \hat{n} \rangle$ for the (two-mode) coherent and SV states. The theory agrees with the experiment up to $\langle \hat{n} \rangle = 5$. Beyond this limit, the MPPC stops discriminating photon numbers reliably and could be the cause of the deviation of experiment from theory.

In conclusion, we have performed an experiment in which the NRFs of coherent and SV states have been measured with
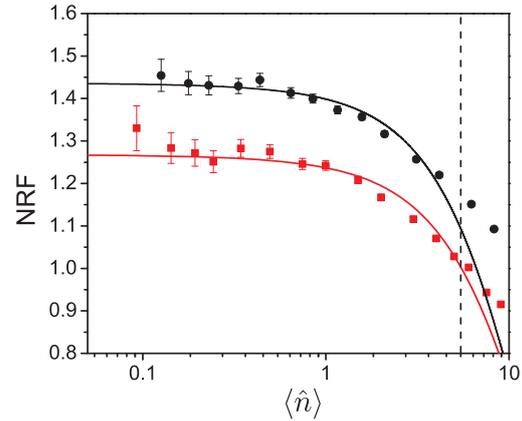
Figure 1: Dependence of the NRF on the mean number of photons measured for the coherent state (circles) and the SV state (squares). The theoretical fits for the NRF are done for the range of average photon numbers up to 5 photons (vertical dashed line), which marks the range of reliable photon-number resolution. The solid lines are fits to the theoretical model with effective q.e. values of $\eta_E = 0.208$ with $R^2 = 0.9999$ for the coherent state (532 nm), and $\eta_E = 0.188$ with $R^2 = 0.9994$ for the SV state (568 nm), respectively. These values agree with those used for the calibration of the MPPC.

commercially available MPPC modules at relatively high photon numbers (up to 5). The main conclusions we can make are: (1) the crosstalk in the MPPC leads to an increase in the NRF for both coherent and SV states, (2) saturation of the MPPC leads to the decrease of NRF with increasing photon numbers. The experimental data agrees with the theoretical model which takes into account the saturation and the crosstalk although the fits deviate at higher mean photon numbers, where the photon number resolution of the detectors is limited. These results extend the use of MPPCs for the characterization of quantum light in a significantly broader range than that of conventional SPADs.

References

[1] D.A. Kalashnikov, S.-H. Tan, M.V. Chekhova, L.A. Krivitsky, Opt. Express **19**, 9352 (2011).

[2] I. Afek, A. Natan, O. Ambar, Y. Silberberg, Phys. Rev. A **79**, 043830 (2009).

[3] A. Agliati, M. Bondani, A. Andreoni, G. D. Cillis, M. G. A Paris, J. Opt. B: Quantum Semiclass. Opt. **7**, S652 (2005).

Tailoring two-photon interference from independent sources

Douglas Vitoreti[1], Thiago Ferreira da Silva[1,2], Guilherme P. Temporão[1], and Jean Pierre von der Weid[1]

[1] Pontifical Catholic University of Rio de Janeiro, Rio de Janeiro, Brazil
[2] National Institute of Metrology, Quality and Technology, Duque de Caxias, Brazil

Fiber-optical quantum communication over long distances has many technological challenges, such as overcoming the losses introduced by the optical fibers. Even with fiber attenuations as low as 0.2 dB/km, direct transmission of qubits is limited to a few hundreds of kilometers. Quantum repeaters [1] have been proposed as a solution to this problem. Especially concerning the two-photon protocols, which rely on a Bell state measurement for the entanglement swapping step, quantum repeaters require the remote interference between single photons stable within their coherence length. We present an analysis of the interference between photons generated by two independent optical sources observed through coincidence counts between two single-photon detectors (SPDs) after a beamsplitter (BS). The interference between photons from different attenuated continuous-wave lasers was measured with the setup shown in Fig. 1, where Alice and Bob send photons to a mid-way station Charlie.
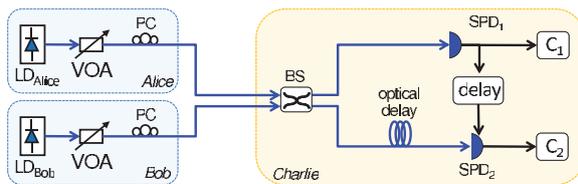
Figure 1: Setup for measuring interference between independent faint laser sources. VOA: variable optical attenuator; PC: polarization controller; Cx: pulse counter.

Two independent laser diodes (LD), with 800 kHz and 6 MHz long-term linewidths respectively, were attenuated at Alice and Bob to reach the single-photon level. The polarization states of the lasers are adjusted to overlap and are sent over an optical fiber spool to reach the 50% BS at Charlie's station. SPD_1 and SPD_2 are placed at each output port of the BS, with an additional hundred meters-long optical delay line at one branch. Given that a counting event is recorded at SPD_1, it triggers a 2.5 ns wide gate on SPD_2 after a controlled delay which allows for relative gates scan. The conditional count rate at SPD_2 summed over a time interval gives the coincidence count rate. A tap from the laser sources is combined in a fast photodiode for monitoring the frequency difference through the electric beat note. This difference was adjusted by tuning the laser cavities relative to each other. The linewidth of one laser was further broadened by FM modulation. The coincidence ratio between the SPDs was measured as a function of the gate delay between them, resulting in the interference patterns shown in Fig. 2.

The photon bunching effect can be visualized as a reduction of coincidence counts when the relative delay between the detectors is close to zero. The maximum visibility is limited to 0.5 due to multi-photon emission per time interval [2].
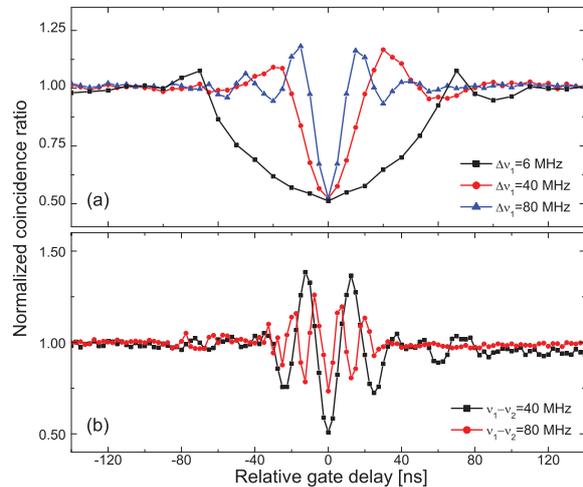
Figure 2: Coincidence ratio measured with (a) overlapping and (b) displaced laser central frequencies.

Increasing the relative gate delay, the photons become distinguishable by their coherence lengths and the interference visibility vanishes, while the coincidence ratio increases. The increase in the linewidth of the 6 MHz-wide laser source ($\Delta\nu_1$) to 40 and 80 MHz makes the Hong-Ou-Mandel dip narrower from 94.6 ns to 24.9 ns and 12.4 ns, respectively, at the same time exhibiting an oscillatory behavior. When a frequency mismatch is introduced between the laser sources ($\nu_1 - \nu_2$), the oscillations are clearer, as seen in Fig. 2b, corresponding to the beat frequency of the laser lines [3], which lasts within the photons coherence lengths. As soon as the Fourier conjugate of the frequency mismatch approaches the gate duration of 2.5 ns, the visibility of the interference curve decreases, which can clearly be observed for a mismatch of 80 MHz.

It is thus possible, by carefully adjusting the relative gate delay of the detectors according to the frequency mismatch of the laser sources, to obtain anti-bunching effects, where two photons impinging on the BS have a greater probability to exit from opposite (random) outputs. This tailoring of bunching/anti-bunching effects might be proven useful not only for quantum repeaters based on two-photon interference but also for other quantum communication applications.

References

[1] N. Sangouard et al, Rev. Mod. Phys., **83**, 33 (2011).

[2] J. G. Rarity et al, J. Opt. B: Quantum Semiclass. Opt., **7**, S171 (2005).

[3] T. Legero et al, Phys. Rev. Lett., **93**, 070503 (2004).

Extremely high Q-factor mechanical modes in quartz Bulk Acoustic Resonators at millikelvin temperature

Maxim Goryachev[1,2], Daniel L. Creedon[1], Eugene N. Ivanov[1], Serge Galliou[2], Roger Bourquin[2] and Michael E. Tobar[1]

[1]ARC Centre of Excellence for Engineered Quantum Systems, University of Western Australia, 35 Stirling Highway, Crawley WA 6009, Australia
[2]Department of Time and Frequency, FEMTO-ST Institute, ENSMM, 26 Chemin de l'Épitaphe, 25000, Besançon, France

Low-loss, high frequency acoustic resonators cooled to millikelvin temperatures are a topic of great interest for application to hybrid quantum systems. When cooled to 20 mK, we show that resonant acoustic phonon modes in a Bulk Acoustic Wave (BAW) quartz resonator demonstrate exceptionally low loss (with Q-factors of order billions) at frequencies of 15.6 and 65.4 MHz, with a maximum $f.Q$ product of 7.8×10^{16} Hz [1]. Given this result, we show that the Q-factor in such devices near the quantum ground state can be four orders of magnitude better than previously attained. Such resonators possess the low losses crucial for electromagnetic cooling to the phonon ground state, and the possibility of long coherence and interaction times of a few seconds, allowing multiple quantum gate operations.

To achieve the operation of hybrid mechanical systems in their quantum ground state, it is vital to develop acoustic resonators with very low losses at temperatures approaching absolute zero. The frequencies accessible using mechanical systems are low, and thus a lower temperature is required (governed by $\hbar\omega > k_B T$) to reach the equilibrium ground state. The average number of thermal phonons should follow the Bose-Einstein distribution

$$n_{TH} \sim \frac{1}{e^{\frac{\hbar\omega}{k_B T}} - 1} \qquad (1)$$

where $\hbar$ is the reduced Planck constant, and T and k_B are the temperature and Boltzmann's constant respectively. For example, at 10 mK a frequency of greater than 144 MHz is required to have $n_{TH} < 1$, which increases proportionally with temperature. Aside from conventional thermodynamic cooling, the ground state or Standard Quantum Limit could potentially be reached by exploiting an extremely low loss resonance, where the mode can be cold damped through feedback or a parametric processes. In the ideal case the ratio Q/T remains constant, where the acoustic Q-factor is reduced as the mode amplitude is then damped and electromagnetically cooled to a lower temperature. Alternatively, if the change in state of the resonance can be measured at a rate faster than the dissipation rate γ, the bath noise is filtered by the high-Q resonance, which is no longer in equilibrium with the bath. In such a case, the effective noise temperature is reduced so that a change in state of order one acoustic phonon could be measureable. The effective temperature, T_{eff}, is then related to the physical temperature, T, by $T_{eff} = T\tau\gamma/2$, where τ is the measurement time. With these techniques in mind, the development of cold, high frequency, ultra-low-loss acoustic resonators represents a crucial step in overcoming the challenge of maintaining long coherence times in systems occupying their quantum ground state.

In this work, we measure a quartz BAW resonator designed with non-contacting electrodes down to 18 mK, and show that the Q-factor continues to increase beyond 10^9, albeit with a smaller power law exponent. To allow the acoustic modes to be trapped between the electrodes at the centre of the resonator, isolating the mode from mechanical losses due to coupling to the support ring, the resonator is manufactured with a planoconvex shape. The longitudinal overtones are the most strongly trapped and thus exhibit particularly high quality factors. Here, we present measurements characterising the 5th and 21st overtones with effective mode masses of order 5 and 0.7 milligram respectively (total resonator mass of 220 mg) at frequencies 15.6 and 65.4 MHz respectively, which exhibit Q-factors exceeding 10^9 corresponding to decay times of order tens of seconds. The Q-factor increases almost exponentially with applied power although resonance line shape remains undeformed.
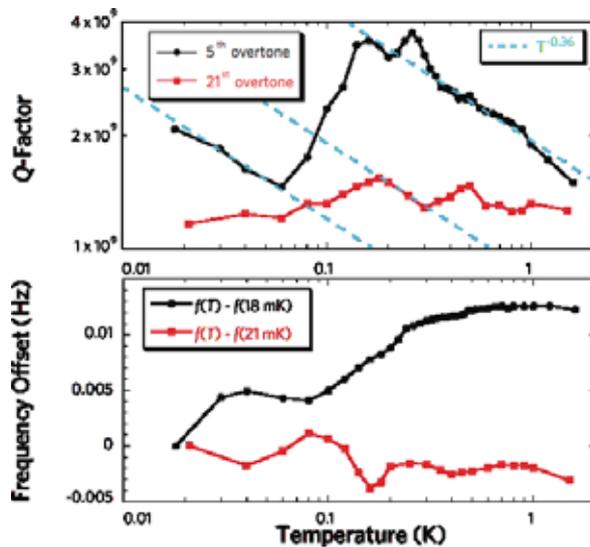
Figure 1: Q-factor and frequency offset versus temperature, $f(T)$, for the 5th and 21st overtones with respect to the frequency at 18 and 21 mK respectively, at -52.5 dBm input power. Dashed lines show a $T^{-0.36}$ dependence for both overtones in various temperature regions.

References

[1] M. Goryachev, D. L. Creedon, E. N. Ivanov, S. Galliou, R. Bourquin, M. E. Tobar, arXiv:1202.4556 (2012).

QCMC 2012
Vienna, Austria

Beating the classical resolution limit via multi-photon interferences of independent light sources

S. Oppel[1,2], **Th. Büttner**[1], **P. Kok**[3], **J. von Zanthier**[1,2]

[1]*Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, 91054 Erlangen, Germany*
[2]*Erlangen Graduate School in Advanced Optical Technologies (SAOT), Universität Erlangen-Nürnberg, 91052 Erlangen, Germany*
[3]*Department of Physics and Astronomy, University of Sheffield, Sheffield S3 7RH, United Kingdom*

Multi-photon interferences with indistinguishable photons from independent light sources are at the focus of current research due to their potential in quantum metrology, optical quantum computing, and entanglement of remote particles [1, 2, 3]. The paradigmatic states for multi-photon interference are the highly entangled NOON states which can be used to achieve enhanced resolution in interferometry and lithography [4, 7, 6, 5]. However, multi-photon interferences from independent, uncorrelated emitters can also lead to enhanced resolution [8]. So far, such quantum interferences have been observed with maximally two independent emitters [7, 9, 10, 11, 12, 13, 14, 15, 16].

Here we report the measurement of quantum interferences of photons emitted by up to five independent emitters [17]. We observe the multi-photon interference patterns using thermal light sources (TLS) and compare the corresponding multi-photon signals to those obtained with single photon emitters (SPE). It is shown that for equal numbers of emitters and detectors at particular *magic positions* $\mathbf{r}_2, \ldots, \mathbf{r}_N$ the normalized Nth order spatial intensity correlation function $g^{(N)}(\mathbf{r}_1, \ldots, \mathbf{r}_N)$ as function of $\mathbf{r}_1$ displays a purely sinusoidal interference pattern of the form $g^N(\mathbf{r}_1) \propto 1 + V_0^{(N)} \cos[(N-1)\delta(\mathbf{r}_1)]$, where $\delta(\mathbf{r}_1)$ and $V_0^{(N)}$ are the relative phase accumulated by photons from adjacent emitters towards the detector at $\mathbf{r}_1$ and the visibility of the correlation signal, respectively. This modulations exhibits a fringe spacing equivalent to those of NOON states with $N-1$ photons.

A detailed quantum field theoretical description allows to identify each quantum path contributing to the N-photon signal. It shows that for N TLS the same interference terms contribute to the multi-photon signal as those obtained from N SPE; however, for TLS the visibility is less than 100%. In particular, for both, TLS and SPE, the multitude of N-photon quantum paths for the particular detector positions always lead to a NOON-like modulation oscillating at the highest possible frequency of the spatial structure of the light source, all other terms cancelling out by destructive interference or adding to the background of the signal. In this way, for $N > 2$, it is not only possible to isolate for $g^N(\mathbf{r}_1)$ the highest possible spatial frequency of the structure but also to observe a gain in resolution which overcomes the canonical classical resolution limit.

The measurement can be considered an extension of the landmark experiment by Hanbury Brown and Twiss who investigated intensity correlations up to second order [18]. Here we go beyond this level by measuring spatial intensity correlations up to fifth order.

References

[1] E. Knill, R. Laflamme, G. J. Milburn, *Nature* **409**, 46 (2001).

[2] D. L. Moehring *et al.*, *Nature* **449**, 68 (2007).

[3] P. Kok, B. W. Lovett, Introduction to Optical Quantum Information Processing (Cambridge University Press, Cambridge, 2010).

[4] A. N. Boto, *et al.*, *Phys. Rev. Lett.* **85**, 2733 (2000).

[5] P. Walther *et al.*, *Nature* **429**, 158 (2004).

[6] M. W. Mitchell, J. S. Lundeen, A. M. Steinberg, *Nature* **429**, 161 (2004).

[7] M. D'Angelo, M. V. Chekhova, Y. Shih, *Phys. Rev. Lett.* **87**, 013602 (2001).

[8] C. Thiel *et al.*, *Phys. Rev. Lett.* **99**, 133603 (2007).

[9] R. Kaltenbaek, B. Blauensteiner, M. Żukowski, M. Aspelmeyer, A. Zeilinger, *Phys. Rev. Lett.* **96**, 240502 (2006).

[10] J. Beugnon *et al.*, *Nature* **440**, 779 (2006).

[11] P. Maunz *et al.*, *Nature Phys.* **3**, 538 (2007).

[12] I. N. Agafonov, M. V. Chekhova, T. Sh. Iskhakov, A. N. Penin, *Phys. Rev. A* **77**, 053801 (2008).

[13] K. Sanaka, A. Pawlis, T. D. Ladd, K. Lischka, Y. Yamamoto, *Phys. Rev. Lett.* **103**, 053601 (2009).

[14] I. N. Agafonov, M. V. Chekhova, T. Sh. Iskhakov, L.-A. Wu, *J. Mod. Opt.* **56**, 422 (2009).

[15] R. Lettow *et al.*, *Phys. Rev. Lett.* **104**, 123605 (2010).

[16] Y. Zhou, J. Simon, J. Liu, Y. Shih, *Phys. Rev. A* **81**, 043831 (2010).

[17] S. Oppel, Th. Büttner, P. Kok, J. von Zanthier, ArXiv: quant-ph/1202.2294.

[18] R. Hanbury Brown, R. Q. Twiss, *Nature* **177**, 27 (1956).

Experimental Implementations of Quantum Illumination

Maria Tengner, Sara L. Mouradian, Tian Zhong, P. Ben Dixon, Zhesen Zhang, Franco N. C. Wong, and Jeffrey H. Shapiro

Massachusetts Institute of Technology, Cambridge, United States

Entanglement is arguably the key resource for quantum information applications; however it is fragile. Usually this fragility limits its use to low-noise, low-loss experimental regimes. Quantum illumination (QI), however, is an entanglement-based paradigm that is not subject to these limitations [1]-[4]. Here we present two experimental implementations of QI, one for target detection and the other for communication that is secure against passive eavesdropping.

The QI paradigm is as follows: entangled signal and ancilla beams are created at a source. The signal beam is sent through a noisy, lossy channel to a target region, while the ancilla beam is retained in a noiseless, lossless environment. The receiver makes a joint measurement on light returned from the target region, together with the retained ancilla, to determine relevant properties of the target region. For target detection, the relevant property is the absence or presence of a reflector in the target region. For secure communication, the relevant property is message modulation imposed in the target region. Noise and loss in the signal's roundtrip propagation to and from the target region are entanglement breaking, viz., the returned light is *not* entangled with the retained ancilla. Yet theory has shown that QI offers significant performance advantages—in both target detection and communication—over a system that uses a coherent-state transmitter of the same average photon flux [2]-[4].
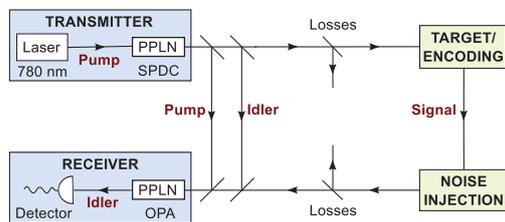
Figure 1: Conceptual setups for QI experiments.

Figure 1 shows the conceptual setups for our QI implementations. In both applications our source consists of a periodically poled lithium niobate (PPLN) crystal creating quadrature entangled signal and idler beams through spontaneous parametric down-conversion (SPDC). The idler beam is retained while the signal is sent over a lossy channel. For target detection, the signal beam may or may not encounter a mirror in the target region, but in either case noise is injected into the return light path. For secure communication, Alice sends the unmodulated signal beam to Bob—who is in the target region—on which he encodes his message with binary phase-shift keying (BPSK). Bob then amplifies the modulated signal beam—adding noise—and returns it to Alice through a lossy channel. In both cases the receiver consists of a low-gain PPLN optical parametric amplifier (OPA) whose output undergoes direct detection [3].

We have preliminary results verifying the QI concept. The detected power spectral densities for our QI target detection apparatus are shown in Fig. 2. The signal power is more than 40 dB above the noise floor in these data. Measurements of a 180 kbit/s BPSK message are shown in Fig. 3.

It is expected that further experimental results will clearly show the target-detection benefit of QI over coherent-state illumination, and the immunity of QI communication to passive eavesdropping.
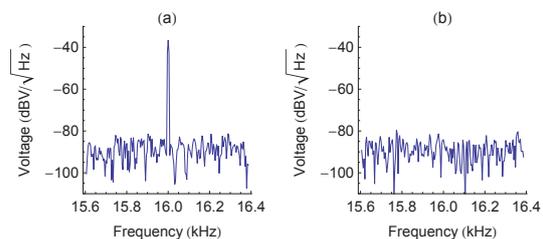
Figure 2: Detected power spectral densities from QI target detection: (a) target present and (b) target absent.
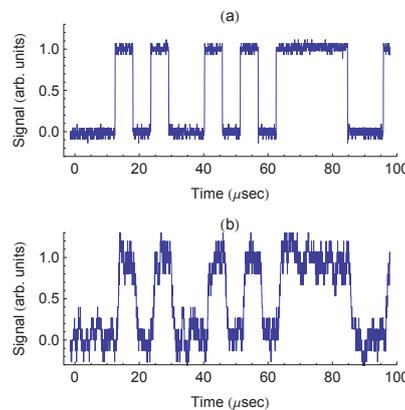
Figure 3: QI communication: (a) transmitted message and (b) received message.

References

[1] S. Lloyd, Science **321,** 1463 (2008).

[2] S. H. Tan, et al., Phys. Rev. Lett. **101,** 253601 (2008).

[3] S. Guha and B. I. Erkmen, Phys. Rev. A **80,** 052310 (2009).

[4] J. H. Shapiro, Phys. Rev. A **80,** 022320 (2009).

Quantum M-ary Phase Discrimination

Ranjith Nair[1], **Brent J. Yen**[1], **Saikat Guha**[2], **Jeffrey H. Shapiro**[3], and **Stefano Pirandola**[4]

[1]*National University of Singapore, Singapore*
[2]*Raytheon BBN Technologies, Cambridge, MA, United States*
[3]*Massachusetts Institute of Technology, Cambridge, MA, United States*
[4]*University of York, York, United Kingdom*

We present a study of quantum M-ary phase discrimination in which a quantum-optical probe state is modulated by one of M uniformly-spaced phase shifts. We assume ideal loss-less transmission and allow full freedom in choosing probe states with any number of signal and ancilla modes with an energy (photon number) constraint in either the signal modes alone or in the signal and ancilla modes together. For lossless operation and unrestricted positive operator-valued measurements (POVMs) at the receiver, we find the explicit form of the probe state that minimizes the average error probability under an energy constraint of N photons. We also consider an implementation of the binary $M = 2$ case.

One application of these results is to the problem of quantum reading [1] of a classical digital memory. The phase encoded version of a digital memory is a specific instance of the problem considered here. The phase discrimination problem may also be viewed within a communication theory context as M-ary phase shift keying (M-ary PSK) modulation [2]. Finally, we note that minimum-error phase discrimination may be considered as the discrete version of MMSE phase estimation which is an active area of research, see e.g., [3].

Consider the set $\{2\pi m/M\}_{m=0}^{M-1}$ of phase shifts on the unit circle. In Fig. 1, a probe state $|\psi\rangle_{AS}$ of signal and ancilla modes is prepared at the transmitter. The action of the mth phase shift to each of $J \geq 1$ optical field modes is represented by the unitary operator $\hat{U}_m = \bigotimes_{j=1}^{J} e^{im(2\pi/M)\hat{N}_S^{(j)}}$, where $\hat{N}_S^{(j)} = \hat{a}_S^{(j)\dagger}\hat{a}_S^{(j)}$ is the number operator for the jth signal mode. In addition to these J signal modes, we allow any number $J' \geq 0$ of ancilla modes which do not acquire the m-dependent phase shift. We assume the return and ancilla modes are measured using a minimum-error-probability POVM. We are interested in choosing a probe state that minimizes the error probability under a given energy constraint when the unknown phase shift m is chosen at random.
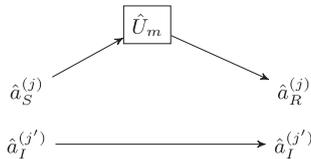
Figure 1: A pure transmitter state $|\psi\rangle_{AS}$ of J signal modes and J' ancilla modes is prepared to probe an unknown random phase shift. A joint quantum measurement is performed on the return and ancilla modes.

For an average total energy constraint in the signal modes, $\langle \sum_{j=1}^{J} \hat{N}_S^{(j)} \rangle \leq N_S$, we derive the optimal probe state. When m is chosen with a uniform prior distribution, the output states form a symmetric set, and it is known [4] that the

square-root measurement is the minimum-error-probability POVM. In the case $N_S \geq (M-1)/2$, the uniform superposition state $|\psi\rangle_S = \frac{1}{\sqrt{M}}(|0\rangle_S + \cdots + |M-1\rangle_S)$ achieves zero error probability. Among all transmitter states satisfying $\langle \sum_{j=1}^{M-1} \hat{N}_S^{(j)} \rangle \leq N_S < (M-1)/2$, the minimum error probability is achieved by a single-mode state of the form

$$|\psi\rangle_S = \sum_{n=0}^{M-1} \sqrt{p_n^{\text{opt}}}|n\rangle_S \qquad (1)$$

with p^{opt} given by $p_n^{\text{opt}} = \frac{1}{(A+nB)^2}, \forall n$, where A, B are positive constants chosen to satisfy the constraints $\sum_{n=0}^{M-1} p_n = 1$ and $\sum_{n=0}^{M-1} np_n = N_S$. It is remarkable that neither multiple signal modes nor ancillary entanglement is necessary for optimum performance. This result also shows that any transmitter state achieving zero-error must have signal energy at least $(M-1)/2$. We compare the performance of the optimal state to several standard states in quantum optics, including coherent states.

We also consider the design of an optimal probe state under a total (signal plus ancilla) average energy constraint. Under this constraint, which is a measure of the entire resources in state preparation, the state (1) achieves the minimum error probability. Finally, we extend these results to show that among all mixed-state transmitters, state (1) is optimal under either energy constraint.

For binary $M = 2$ phase discrimination, we show that optimum performance $P_e = 1/2 - \sqrt{N_S(1 - N_S)}$ is readily demonstrable with current technology using single-photon sources and linear optics. Conditional on no erasures in a system with transmission loss and nonideal detector efficiency, the error rate remains the same as the optimal lossless error rate.

References

[1] S. Pirandola, Phys. Rev. Lett., **106**, 090504, (2011); O. Hirota, e-print arXiv:1108.4163, (2011).

[2] K. Kato, M. Osaki, M. Sasaki, and O. Hirota, IEEE Trans. Comm., **47**, 248, (1999).

[3] R. Demkowicz-Dobrzański, Phys. Rev. A, **83**, 061802R, (2011); A. Datta, L. Zhang, N. Thomas-Peter, U. Dorner, B. J. Smith, and I. A. Walmsley, Phys. Rev. A, **83**, 063836, (2011).

[4] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. of Theor. Phys., **36**, 1269, (1997).

Franson interferometry with 99.6% visibility via fiberoptic dispersion engineering

Tian Zhong and Franco N. C. Wong

Massachusetts Institute of Technology, Cambridge, United States

Time-energy entanglement is of fundamental importance in both quantum physics [1] and quantum information technology. Franson quantum interferometry [1] is used to measure Bell's Inequality for time-energy entanglement and is essential as a security test in fiber-optic quantum key distribution (QKD) based on time-bin entanglement. However, unlike polarization entanglement for which >99% quantum-interference visibility has been routinely reported [2], equally high quality time-energy entanglement with >97% visibility (with proper background subtraction) has not been reported, to the best of our knowledge. The problem lies in the dispersion mismatch between the long and short paths of each unbalanced arm of the Franson interferometer. Here we confirm dispersion limitation of Franson interferometry using a narrowband filter and report, for the first time, Franson quantum-interference of time-energy entangled photons with 99.6% visibility using fiber-based dispersion compensation with no filtering and without background subtraction.
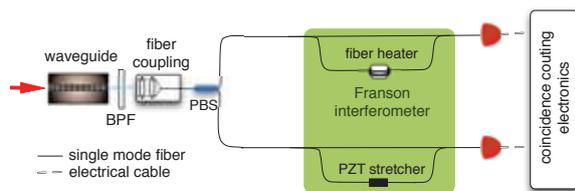
Figure 1: Setup of Franson quantum intefereometry.

Fig. 1 shows our experimental setup. Time-energy entangled photons at degenerate 1560 nm were efficiently generated via spontaneous parametric downconversion in a type-II PPKTP waveguide source [3]. With a countinous-wave pump, the two-photon phase matching bandwidth was 2 nm. After coupling into a polarization maintaining fiber, the signal and idler photons were separated using a fiber polarizing beam splitter, and sent to two arms of the Franson interferometer. We measured their coincidences using two 20% efficient self-differencing InGaAs single-photon avalanche photodiodes with 628.5-MHz repetition rate sinusoidal gating [3].

A phase-stable fiber Franson interferometer was implemented. A configuration using only standard single-mode fiber (SMF: GVD=17ps/nm/km), as shown in Fig. 2(a), yields a dispersion mismatch that degrades the two-photon spectral and temporal correlation. The resulting Franson visibility was limited to 98.2%, as confirmed experimentally in Fig. 3 (solid squares) and in line with our theoretical estimate. Such dispersion mismatch can be reduced by narrow-band spectral filtering, as indicated in Fig. 2(b), but at the expense of decreased photon-pair flux. We obtained a Franson quantum-interference of 99.4% (Fig. 3, solid diamonds) without subtraction of background counts. Also, we estimate that at the lowest mean pair generation rate of 0.2% per co-

incidence window, double-pair events contribute 0.2% of the visibility reduction. The use of narrowband filtering confirms dispersion is responsible for Franson visibility degradation.
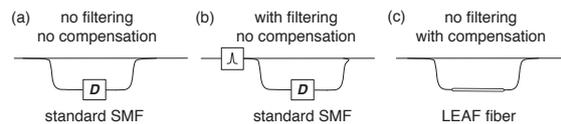
Figure 2: Three configurations of Franson interferometer.

In Fig. 2(c), we implemented a dispersion-compensated interferometer by replacing a portion of the long-path SMF with low dispersion LEAF fiber (GVD=4ps/nm/km) such that the net dispersion in both short and long paths are matched. The dispersion compensation restores the spectral and temporal overlap of the two photons, therefore recovering the high fidelity of the entangled states and without any loss of flux. As shown in Fig. 3 (solid triangles), the measured Franson quantum-interference visibility reaches 99.6%, surpassing even the narrowband filtering case with no loss of flux. Our new results without subtraction of accidentals match those of polarization entangled photons and indicate the importance of dispersion compensation in Franson interferometric measurements and in QKD based on time-bin entanglement.
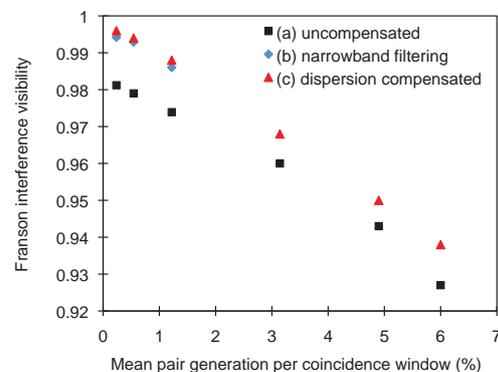
Figure 3: Measured Franson quantum-interference visibilities without subtraction of accidentals.

References

[1] J. D. Franson, Phys. Rev. Lett., **62**, 2205 (1989).

[2] F. N. C. Wong, J. H. Shapiro, and T. Kim, Laser Phys. 1**6**, 1517 (2006).

[3] T. Zhong *et al.*, "Efficient single-spatial-mode PPKTP waveguide source for high dimensional entanglement-based QKD," CLEO/QELS, paper JTh1K3 (2012).

Coherent manipulation of an NV center and an carbon nuclear spin

Burkhard Scharfenberger[1], **William J. Munro**[2] and **Kae Nemoto**[1]

[1]*National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*
[2]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

Summary. — Nitrogen vacancy centers (NV) in diamond are a promising system for the realization of a solid state qubit and thus its properties as well as applications in quantum computation have been been studied intensely on both a theoretical and experimental level in the past decade. We study a 3 qubit system formed by the NV center's electronic and nuclear spin plus an adjacent spin 1/2 carbon ^{13}C. Specifically, we propose a manipulation scheme utilizing the hyperfine coupling of the effective S=1 degree of freedom of the vacancy electrons to the two adjacent nuclear spins to achieve accurate coherent control of all three qubits.

Background. — NV- centers in diamond have been the focus of intense study for use as qubit in quantum computation as it offers both long coherence times when compared to other solid state systems and is comparativily easy to adress using optics and rf pulses. The electronic S=1 degree of freedom of the charged vacancy lives in an environment of nuclear spins that couple to it via hyperfine interaction: there is at least the one of the nitrogen, but often one or more spin $S = 1/2$ ^{13}C carbon atoms are also present. Because of their very long coherence times due to their weak coupling to the environment, it was proposed early on to use these nuclear spins as a quantum memory, while fast operations could be performed on the electron. To date, there have among others been experimental demonstrations of the use of NVC as quantum registers: state transfer between the vacancy and an ensemble of several adjacent carbon ^{13}C spins [1], multi-partite entanglement of spins [2] and recently also single-shot readout of the vacancy and nuclear spin states [3]. Apart from helping to improve experimental techniques, these experiments serve as beautiful and necessary proofs-of principle for the idea of joint operations on the electrons and nuclear spins . What is still lacking however is complete scheme of how to coherently address individual nuclear spins and perform all necessary operations of universal quantum computation.

Our work. — In a recent numerical simulation study of a basic NV center, Everitt et al. are able to show that magnetic field and rf-driving provide enough control for coherent manipulation [6]. In this work, we identify a control scheme for a system consisting of the basic NV center (the nitrogen is assumed to be the $S = 1/2$ ^{15}N) and one additional carbon ^{13}C. The dynamics of this NVC system are dominated by the strong hyperfine coupling of the vacancy electron spin to the carbon. We consider several possible lattice positions for the carbon ^{13}C atom, for all of which we assume the hyperfine tensor to be axial, which is an approximation well justified by both recent DFT studies of hyperfine coupling constants for the ground state of the vacancy center [4] as well as experimental observations [5]. For the nitrogen spin, the hyperfine axis is aligned with the NV axis. However this is not the case for the ^{13}C, and this misalignment gives rise to unusual counter-rotating and spin-flip terms in the effective hamilto-

nian needed to desribe the combined NVC system.
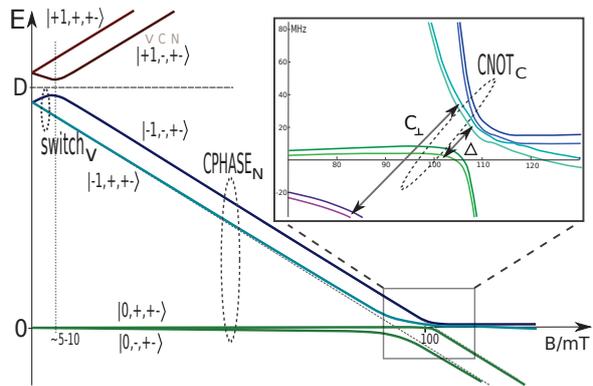
Figure 1: Level structure of the NVC complex with magnetic field settings and approximate states used in coherent manipulation

Tuning the magnetic field to values in the vicinity of the $|m_S = 0\rangle$, $|m_S = -1\rangle$ level crossing, this allows implementation of controlled spin flips of the carbon nuclear spin, i.e. a CNOT operation. Similar to the scheme of [6] the nitrogen is controlled via the parallel hyperfine interaction, yielding a unitary evolution equivalent to a CPHASE gate. Single qubit operations on the carbon and nitrogen would be done by swapping states with the vacancy spin. Since the hyperfine interaction cannot be turned off, both nuclear spins will accumulate an vacancy spin dependant phase due to the parallel hyperfine interaction during operations on the vacancy. This unwelcome entangling phase can be eliminated, at least to first order, by periodically switching the computational qubit space of the electron from $\{|m_S = 0\rangle, |m_S = -1\rangle\}$ to $\{|m_S = 0\rangle, |m_S = +1\rangle\}$. This could be done using crystal strain, which is always present in real NV centers, since it acts like a spin-flip term in the $\{|m_S = -1\rangle, |m_S = +1\rangle\}$ space. Gate times would be on the order of 6-7ns in case of the CNOT$_C$ and 310-330ns for the CPHASE$_N$.

References

[1] M. V. Gurudev Dutt et al., Science **316**, 1312 (2007).

[2] P. Neumann et al., Science **320**, 1326 (2008).

[3] L. Robledo et al., Nature **477**, 574 (2011).

[4] A. Gali, M. Fyta and E. Kaxiras, Phys. Rev. B **77**, 155206 (2008).

[5] S. Felton et al., Phys. Rev. B **79**, 075203 (2009).

[6] M. E. Everitt et al., unpublished

Evading quantum mechanics

Mankei Tsang[1,2] **and Carlton M. Caves**[3]

[1] *Department of Electrical and Computer Engineering, National University of Singapore, 4 Engineering Drive 3, Singapore 117583*
[2] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117551*
[3] *Center for Quantum Information and Control, University of New Mexico, MSC074220, Albuquerque, New Mexico 87131-0001, USA*

Quantum mechanics is potentially advantageous for certain information-processing tasks, but its probabilistic nature and requirement of measurement back action often limit the precision of conventional classical information-processing devices, such as sensors and atomic clocks. Here we show that by engineering the dynamics of coupled quantum systems, it is possible to construct a subsystem that evades the laws of quantum mechanics, at all times of interest, and obeys any classical dynamics, linear or nonlinear, that we choose.

To do so, let us revisit the concept of quantum nondemolition (QND) [1]. A QND observable is represented by a Heisenberg-picture operator $O(t)$ that commutes with itself at times t and t' when the observable is measured:

$$[O(t), O(t')] = 0 . \tag{1}$$

The most well-known QND observables are ones that remain *static* in the absence of classical signals, viz.,

$$O(t) = O(t') . \tag{2}$$

Nowadays it is often assumed that Eqs. (1) and (2) are interchangeable as the QND condition [2, 3].

To show that there exists a much wider class of QND observables, we generalize the concept of a QND observable to that of a *quantum-mechanics-free subsystem* (QMFS), which is a set of observables $\mathcal{O} = \{O_1, O_2, \ldots, O_N\}$ that obey, in the Heisenberg picture,

$$[O_j(t), O_k(t')] = 0 \text{ for all } j \text{ and } k, \tag{3}$$

at all times t and t' when the observables are measured. The operators can then be mapped to a classical stochastic processes by virtue of the spectral theorem [4] and become immune to the laws of quantum mechanics, including the Heisenberg principle and measurement invasiveness.

To construct a QMFS, consider two sets of canonical positions and momenta, $\{Q, P\} = \{Q_1, Q_2, \ldots, Q_M, P_1, P_2, \ldots, P_M\}$ and $\{\Phi, \Pi\} = \{\Phi_1, \Phi_2, \ldots, \Phi_M, \Pi_1, \Pi_2, \ldots, \Pi_M\}$, which obey the usual canonical commutation relations. Suppose the Hamiltonian has the form $H = \frac{1}{2}\sum_{j=1}^{M}(P_j f_j + f_j P_j + \Phi_j g_j + g_j \Phi_j) + h$, where $f_j = f_j(Q, \Pi, t)$, $g_j = g_j(Q, \Pi, t)$, and $h = h(Q, \Pi, t)$ are arbitrary, Hermitian-valued functions. The equations of motion for $Q_j(t)$ and $\Pi_j(t)$ become

$$\dot{Q}_j = f_j(Q(t), \Pi(t), t) , \quad \dot{\Pi}_j = -g_j(Q(t), \Pi(t), t) . \tag{4}$$

The Q and Π variables are dynamically coupled to each other, but not to the incompatible set $\{\Phi, P\}$, and thus obey Eq. (3) and form a QMFS, as depicted in Fig. 1. A prime example arises when one measures the collective position of a pair of quantum harmonic oscillators $\{q, p\}$ and $\{q', p'\}$, one with positive mass and one with negative mass, with $Q = q + q'$ and $\Pi = (p - p')/2$. This QMFS, behaving as a classical harmonic oscillator, has been experimentally demonstrated with atomic spin ensembles [5] and also proposed to remove back-action noise in optomechanics [6]. See Ref. [7] for a more in-depth discussion.
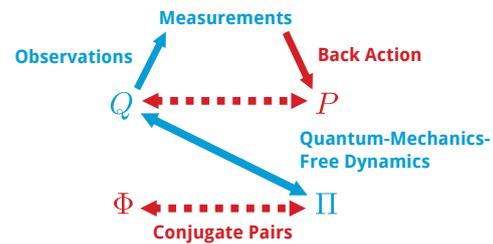
Figure 1: A quantum-mechanics-free subsystem.

It is possible to construct discrete-variable QMFSs as well. Consider a three-qubit quantum Toffoli gate [8], which transforms the Heisenberg-picture Pauli Z operators according to $Z'_1 = Z_1, Z'_2 = Z_2, Z'_3 = (I - (I - Z_1)(I - Z_2)/2)Z_3$, where I is the identity operator. The input and output Z operators all commute, so the Z operators can be mapped to classical bits that undergo classical information processing, and one can use a circuit of Toffoli gates as a universal classical computer to implement arbitrary classical discrete-variable dynamics in discrete time.

References

[1] C. M. Caves *et al.*, Rev. Mod. Phys. **52**, 341 (1980).

[2] H. M. Wiseman and G. J. Milburn, *Quantum Measurement and Control* (Cambridge University Press, Cambridge, 2010).

[3] C. Monroe, Phys. Today **64**(1), 8 (2011).

[4] M. Reed, and B. Simon, *Methods of Modern Mathematical Physics. I: Functional Analysis* (Academic Press, San Diego, 1980).

[5] B. Julsgaard, A. Kozhekin, and E. S. Polzik, Nature (London) **413**, 400 (2001).

[6] M. Tsang and C. M. Caves, Phys. Rev. Lett. **105**, 123601 (2010).

[7] M. Tsang and C. M. Caves, e-print arXiv:1203.2317.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

Quantum feedback control of atomic coherent states

Thomas Vanderbruggen[1], **Ralf Kohlhaas**[1], **Andrea Bertoldi**[1], **Simon Bernon**[1], **Alain Aspect**[1], **Arnaud Landragin**[2], **and Philippe Bouyer**[1,3]

[1]*Laboratoire Charles Fabry, Institut d'Optique, CNRS, Université Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau cedex, France*
[2]*LNE-SYRTE, Observatoire de Paris, CNRS and UPMC, 61 avenue de l'Observatoire, F-75014 Paris, France*
[3]*Laboratoire Photonique, Numérique et Nanosciences - LP2N Université Bordeaux - IOGS - CNRS : UMR 5298 - Bât. A30, 351 cours de la liberation, Talence, France*

The success of technologies depends on the stability they reach in their environment. For quantum systems, this condition has until now hindered many technologies to enter real world applications. The reason is that when a quantum system interacts with the environment it loses its quantum features through a process called decoherence. To stabilize the system against the random perturbations from the environment, a feedback loop may be used. It consists in monitoring the perturbation before correcting it. Implementing this method for a quantum system is challenging since a measurement backaction occurs during the state monitoring. To overcome this effect, weak nondestructive measurements can be used, which allow a partial recovery of information while inducing a negligible disturbance.

We demonstrate the stabilization of an atomic coherent spin states (CSS) where all the atoms of the sample are in a coherent superposition of two internal atomic states. This state $|\pi/2\rangle$ is prepared using a $\pi/2$ microwave pulse. We protect this state against an iterated sequence of random collective flips (RCFs). A RCF is a simple decoherence model that consists in a rotation $\pm\alpha$ of the collective spin around the X axis of the Bloch sphere, where the rotation sign is random. After a RCF, the initially pure state $|\pi/2\rangle$ is in a statistical mixture of the states $|\pi/2 - \alpha\rangle$ and $|\pi/2 + \alpha\rangle$ with equal probability. Using a weak nondestructive probe that induces a negligible disturbance, we determine which flip the system has undergone and correct it by applying the opposite rotation.

The nondestructive detection measures the observable J_z that is the population difference between the two atomic levels. The detection is based on the frequency modulation spectroscopy technique [1] that measures the phase-shift induced by the atomic sample on a far off-resonance probe. From the sign of J_z, we determine in which hemisphere the collective spin lies after the RCF.

The experimental sequence starts with the loading of the dipole trap, followed by a state preparation to polarize the atomic sample before generating the $|\pi/2\rangle$ state. The RCF is then applied, consisting in a $\pi/4$ microwave pulse with a sign randomly set by a quantum random number generator. After the RCF, a detection pulse is sent and the result is treated in real-time with a micro-controller that sets the rotation sign of the correction by adjusting the phase of the microwave.

In a single feedback cycle, composed of a sequence RCF-measurement-correction, an optimum number of photons per probe pulse is determined as a compromise between a the precision of the measurement and the amount of extra-decoherence induced by the probe (mainly due to sponta-

neous emission). After the sequence, 97.5 % of the inital coherence is recovered, which is higher than the residual coherence of 71 % of the statiscal mixture obtained after the RCF. This proves the efficiency of the feedback scheme since it is able to protect, at least partially, the state against decoherence.

The scheme is then used for the real-time feedback stabilization of the CSS against the iterated application of the RCF noise. Our feedback procedure increases the coherence lifetime of the quantum state by more than one order of magnitude.

References

[1] S. Bernon, T. Vanderbruggen, R. Kohlhaas, A. Bertoldi, A. Landragin, and P. Bouyer, New J. Phys. **13**, 065021 (2011).

[2] T. Vanderbruggen, S. Bernon, A. Bertoldi, A. Landragin, and P. Bouyer, Phys. Rev. A **83**, 013821 (2011).

Timing synchronization with photon pairs for quantum communications

Thomas Lorünser[1], **Andreas Happe**[1], **Momtchil Peev**[1], **Florian Hipp**[1], **Damian Melniczuk**[1,2], **Pattama Cummon**[3], **Pituk Panthong**[3], **Paramin Sangwongngam**[3] and **Andreas Poppe**[1]

[1]*AIT Austrian Institute of Technology, Donau-City-Strasse 1, 1220 Vienna, Austria*
[2]*Wrocaw University of Technology, Institute of Physics, 50-370 Wrocaw, Poland*
[3]*NECTEC, 112 Phatonyothin road, 12120 Pthumthani, Thailand*

For quantum communication experiments with entangled photon pairs far-distant measurement results are correlated. Thereby the timing of the coincidence window and its width are critical. In contrast to lab experiments, where accurate timing could be adjusted easily by e.g. matched cable length, in distributed experiments a common clock more accurate than the coincidence time is requested by means of time stable synchronization channels or atom clocks synchronized by GPS. Synchronization of distant clocks is far from trivial and minor offsets may be crucial for the outcome of an experiment e.g. very recently 60ns had been sufficient to simulate an experimental contradiction with relativity theory [1]. Moreover, entangled photon pair sources are suitable for the operation of switched star shaped networks, allowing on demand connectivity of a high number of potential users. Efficient synchronization mechanisms will be crucial key to enable such architectures.

In this contribution we demonstrate distant synchronization without additional time stable signals parallel to the quantum channel. Instead we developed an universal software solution exploiting timing information of SPDC-pair photon arrivals.
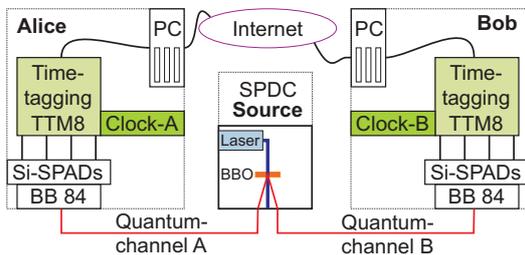
Figure 1: Schematic of the setup. The only direct connection between the peers Alice and Bob is the internet. They are connected to the source only over the quantum channel.

The overall setup is illustrated in Fig. 1. A typical type-II BBO-source pumped by a CW-laser generates entangled photons, which are sent to Alice and Bob over quantum channels A and B, respectively. In the BB84-modules the photons are analysed in the four polarization orientations (H, V, D and A) typical for the BB84 protocol and detected by Si-SPADs. The arrival is registered by the time-tagging module TTM8 and a 64-bit time-tag is generated with an accuracy of 100ps.

For coincidence detection, Bob sends his time-tags to Alice, where our software calculates the time and frequency offset between the respective TTM8 clocks. To be fully independent of time stable channels, the software must continuously compensate for the drift between the two free running clocks at Alice and Bob and follow the drift fluctuations in short- and long-term. Typical measurements of clock stability between two TTM8 during two 24-hours test runs are shown in Fig. 2.
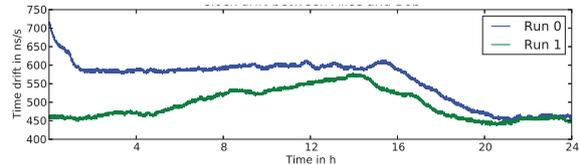
Figure 2: Drift between TTM8 clocks of Alice and Bob.

This drift and its variation over time is by far larger as the coincidence window, but still an appropriate starting point for our coincidence-detection software. A dedicated correlation algorithm is capable of synchronizing the two peers down to the sub-ns level and therefore enables efficient identification of coinciding pair events. The systems find the correct phase and frequency offset between the two clocks in real-time and furthermore find optimal time window sizes dependent on the signal to noise ratio. However, a coarse offset estimation in the order of 1 ms has to be known. This is done by synchronizing the PC-clocks with available synchronization software (e.g. ptp) over their network connections.

Measurement results are shown in Fig. 3. The left graph is the error of the estimated offset for the processed data which is a quality measure for the applied data evaluation. Less than 40 out of more than 15.000 values show a deviation larger than the timing jitter of the Si-APDs. The right graph shows the distribution of the measured correlation events. A deviation from the Gaussian distribution as a long tail towards the origin would indicate performance degradation of the algorithms, which is not the case. The current software implementation is capable of processing rates of up to 1 MEvents/s per peer in real-time compatible with the AIT QKD postprocessing stack for subsequent quantum key generation.
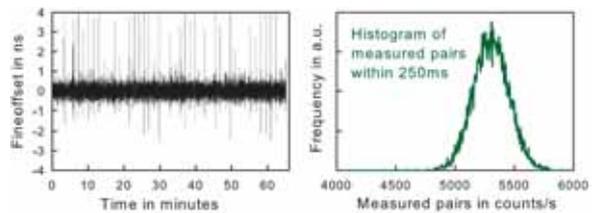
Figure 3: left: Phase estimation of the control loop. right: Stability of the correlation finding algorithm.

Conclusions: The presented mechanism allow to extend entanglement based QKD from typical QKD-link system to a full QKD-network with a SPDC-source in a central position.

References

[1] T. Adam et al. arXiv:1109.4897, November 2011.

Practical schemes for measurement-device-independent quantum key distribution

Xiongfeng Ma[1,2] and <u>Mohsen Razavi</u>[1]

[1] *School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK*
[2] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China*

Quantum key distribution (QKD) enables two remote parties to securely exchange secret keys. Various device imperfections must, however, be examined before security proofs can be applied to practical scenarios. That has stimulated research on device-independent QKD schemes. Such schemes, however, mostly impose impractical constraints on system components. Noting that the majority of hacking strategies exploit *detection* loopholes [1, 2], several measurement-device-independent QKD (MDI-QKD) schemes have recently been proposed [3, 4]. In MDI-QKD, while the sources are trustful, measurement tasks can be left to untrusted parties, who perform entanglement swapping operations. The originally proposed MDI-QKD scheme uses polarization encoding for its operation [3], followed by two phase-encoding schemes [4]. Here, we build on recent progress on MDI-QKD to propose alternative practical schemes resilient to detection loopholes.

Our MDI-QKD schemes rely on phase encoding as well, but considerably reduce the complexity, hence the cost of the measurement modules. Figure 1(a) schematically shows our path-phase-encoding MDI-QKD scheme. Here, Alice and Bob each encode their single photons by introducing a relative phase shift between their reference and signal beams. The phase shifts are applied to the signal modes using phase modulators (PMs), and are chosen from the set $\{0, \pi/2, \pi, 3\pi/2\}$. A partial Bell-state measurement (BSM), performed by Eve or Charlie, on the two reference and the two signal modes would establish correlations between the raw key bits of Alice and Bob. Provided that they use the same phase basis, a joint click on detectors r_0 and s_0 implies identical bits for Alice and Bob, so does a joint click on r_1 and s_1. A joint click on r_0 and s_1, or, r_1 and s_0 would imply complement bits. In Fig. 1(a), it is required that the relative phase between the reference and signal beams is maintained. In practice, this can be achieved by using the setup of Fig. 1(b), which uses time-phase encoding. Moreover, we can show that such a setup can work with only two single-photon detectors, as compared to the schemes proposed in [4], which require optical switches and typically four detectors.

We can extend our schemes to use decoy-state, with weak laser pulses rather than ideal single photons, protocols. It turns out, however, that a mutual phase reference is required in this case. Moreover, the quantum bit error rate (QBER) can be relatively high if one uses a standard decoy-state protocol [5]. To reduce the QBER, we use a post-selection technique, in which Alice and Bob divide $[0, 2\pi]$ into N segments, randomly choose one of these segments for phase randomization, and inform each other of the chosen segment at the sifting stage. We can show that by sending as few as 2-3 bits of information, the QBER is reduced to reasonable values.

Figure 2 shows lower bounds on secret key generation rates for our scheme in Fig. 1(a) with single photons and decoy states as compared to that of [3]. As can be seen, all
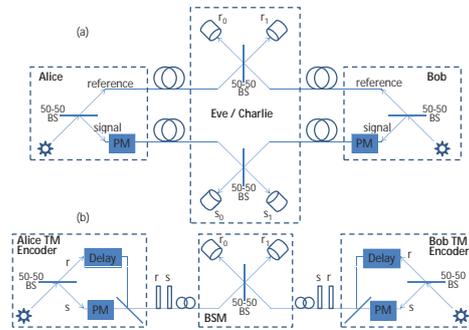
Figure 1: Schematic diagrams for (a) path-phase-encoding and (b) time-phase-encoding MDI-QKD schemes.

schemes can operate over long distances with path loss exceeding 30 dB. If single-photon sources are available, our scheme offers simple detection setups at improved secret key generation rates. This work was in part supported by the European Community's Framework programme under Grant Agreement 277110.
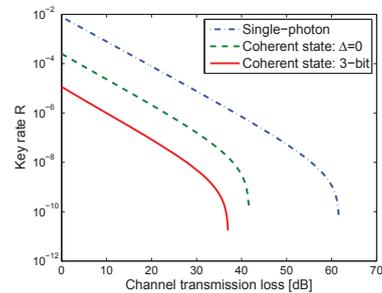
Figure 2: Key rate comparison for single-photon and decoy-state MDI-QKD schemes. The solid line indicates the key rate for our scheme with decoy states using 8 segments for phase selection. The dashed line shows the performance of the original MDI-QKD in [3]. In all graphs, quantum efficiency is 14.5%, dark count rate is 3×10^{-6}/pulse, error correction inefficiency is 1.16, and misalignment error is 1.5%.

References

[1] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74,** 022313 (2006).

[2] C. Wiechers *et al.*, New J. Phys. **13,** 013043 (2011).

[3] H.-K. Lo, M. Curty, and B. Qi, quant-ph: 1109.1473.

[4] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, quant-ph: 1111.3413.

[5] H.-K. Lo *et al.*, Phys. Rev. Lett. **94,** 230504 (2005).

Middle-term operation performance of long-distance quantum key distribution over a field-installed 90-km fiber-optic loop

K.Shimizu[1]**,T.Honjo**[2]**,M.Fujiwara**[3]**,S.Miki**[3]**,T.Yamashita**[3]**,H.Terai**[3]**, Z.Wang**[3]**, and M.Sasaki**[3]

[1]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[2]*NTT Information Sharing Platform Laboratories, NTT Corporation, 3-9-11 Midoricho, Musashino, Tokyo 180-8585, Japan*
[3]*National Institute of Information and Communication Technology (NICT), Japan*

I. Introduction: This paper reports on the middle-term operation performance of the differential phase shift quantum key distribution (DPS-QKD) system which is incorporated with the test-bed fiber-optic network installed over Tokyo metropolitan area[1]. Completely free-run operation over 10 days was demonstrated for long-distance quantum key distribution over a field- installed 90-km fiber-optic loop with a loss of 31 dB. With a use of superconducting single photon detectors (SSPDs), secure key generation rate of about 400 bps was achieved after error correction and privacy amplification processing. Automatic stabilization is introduced for the free-run operation.

II. Configuration of the system and experiment: The transmitter, Alice, and receiver, Bob, of the DPS-QKD system are placed at the same laboratory in Koganei terminal, which is 45-Km distant from the central junction, Otemachi, of the test-bed fiber-optic network. Except for the regions near the termination points, optical cable is installed underground. Optical loss between Alice and Bob is 31 dB for the 90(=45x2)-km loop-back quantum channel. Alice and Bob are synchronized with the clock signal which is transmitted over another 90-km loop-back optical fiber. Figure 1 outlines the experimental setup. Light wavelength is 1551 nm. The light pulse with a 100-ps width is generated by the intensity modulator with the period of 1-ns. The pulse undergoes 0 or π phase shift such that the pulse sequence carries a pseudo random number. Then the pulse is attenuated such that each pulse contains 0.2 photons in average. In Bob side, the pulse sequence is launched into the delayed Machzehnder interferometer (MZI), where photon is routed to the different output ports 1 and 2 dependent of phase difference, 0 or π, of adjacent two pulses.

The phase difference is robust against temporal disturbance in the propagation. Then output from each port is directed to an SSPD after optimization of the polarization state. Insertion of the MZI and the polarization controller imposes extra 2 dB loss. SSPDs are operated at 2.5 K. Quantum efficiency η and dark count rate Dc are as follows. SSPD1:(η,Dc)= (0.1,50cps) and SSPD2: (η,Dc)=(0.05,100cps).

III. Preliminary results: Free-run operation performance was evaluated over 264 hours in the end of January 2012. Temperature of the MZI circuit was under feedback control such that quantum bit error rate (QBER) dose not exceed 4%, which was the threshold for the secure key distillation. Figure 2(a) shows the 1-hour average of the QBER(%) and the MZI temperature(deg.), where bar indicates the maximal and minimal values. Figure 2(b) shows the sifted key rate (bps) and the secure key generation rate (bps) for every one hour. In spite of 30-dB loss, achieved secure key generation rate is about 400 bps, which is half of the result in the field exper-

iment for the plug and play QKD over 15-km[2]. Although large fluctuation in the QBER degrades the secure key generation rate, automatic recovery was confirmed.
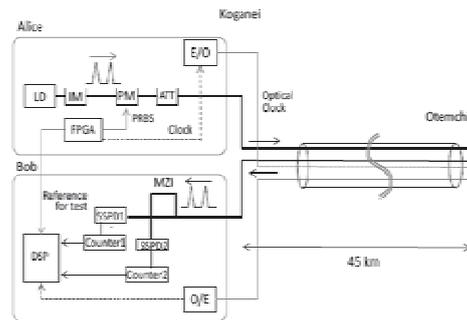
Figure 1: Experimental setup.
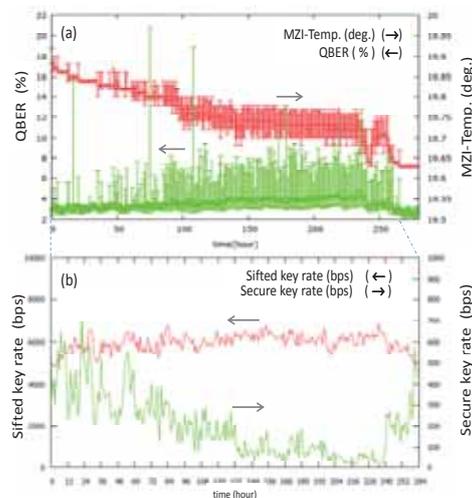
Figure 2: QBER, MZI-temp., Sifted and Secure key rate.

References

[1] M.Sasaki et.al., Opt.Express 19,10387 (2011).

[2] D.Stucki et.al., New J.Phys.13,123001 (2011).

Cheat-sensitive commitment of a classical bit coded in a block of mxn round-trip qubits

Kaoru Shimizu[1], Kiyoshi Tamaki[1] and Nobuyuki Imoto[2]

[1]*NTT Basic Research Laboratories, NTT Corporation,Atsugi,Kanagawa 243-0198, Japan*
[2]*Graduate School of Engineering Science, Osaka University, Osaka 560-8531, Japan*

I.Introduction: We propose here a quantum protocol for a cheat-sensitive commitment of a classical bit Z. As same as bit commitment(BC), Alice, the receiver of Z, can examine dishonest Bob, who changes or postpones his choice of Z. In contrast to BC, cheat-sensitive BC(CSBC) abandons guaranteed concealment for Z. Nevertheless, CSBC enables Bob, the sender of Z, to examine dishonest Alice, who violates concealment. Since the no-go theorem of quantum BC [1] tells us nothing about CSBC, it has been an open question as to whether or not quantum mechanics provides us with a security solution to CSBC tasks. Our CSBC framework is based on an appropriate quantum bit escrow protocol with a round-trip of a qubit particle. If Z is coded in a block of mxn round-trip qubits, impartial examinations and probabilistic security criteria can be achieved [2].

II.Bit escrow protocol with a round-trip qubit: Here we assume Alice and Bob are honest. $X=|X+\rangle,|X-\rangle$ and $Y=|Y+\rangle,|Y-\rangle$ indicate a pair of conjugate bases. Basis X and Y correspond 0 and 1, respectively. [Commitment phase] Alice chooses the sending basis S=X or S=Y and the spin state $|AS\rangle=|S+\rangle$ or $|As\rangle=|-\rangle$ in a random way. Then she records $|As\rangle$ and send the qubit to Bob. Next, Bob decides basis C=X or C=Y to perform a projection measurement for the qubit. Bob records his outcome spin state $|BC\rangle=|C+\rangle$ or $|BC\rangle=|C-\rangle$ and then returns the qubit to Alice. Alice then performs a projection measurement with the other basis R which is conjugate with S. She records her obtained outcome spin state $|AR\rangle=|R+\rangle$ or $|AR\rangle=|R-\rangle$.

[Opening phase] There are two exclusive cases in the opening phase. If Alice examines Bob, she requests him to open his coding basis C and the spin state $|BC\rangle$. For C=S, she confirms $|BC\rangle=|AS\rangle$. For C=R, she confirms $|BC\rangle=|AR\rangle$. Honest Bob can always pass the examination. Once she is notified of C, she can always assert $|BC\rangle$ with regardless of C. Hence, dishonest Bob, who answers the wrong basis and fakes the spin state, is detected by Alice with a 1/2 probability. If Bob examines Alice, he requests her to open her recorded spin states $|AS\rangle,|AR\rangle$. For C=S, he confirms $|AS\rangle=|BC\rangle$. For C=R, he confirms $|AR\rangle=|BC\rangle$. Honest Alice can always pass the examination whereas her legitimate bases arrangement afforded no information on C in the commitment phase. If dishonest Alice employs the illegitimate bases arrangement R=S, she can find that C is not identical to R=S when she obtains $|AS\rangle\neq|AR\rangle$ with a 1/4 probability. However, her measurement destroys the spin state $|C+-\rangle$ and she fails to pass the examination with a 1/2 probability.

III.Minimal CSBC protocol: Although the two different examination cases are exclusive in the case of one round-trip, mxn repetitions of the round-trip can provide impartiality between Alice and Bob.

[Commitment phase] Step1: Alice prepares a set of mxn qubit particles b^{ij}(i=1∼m,j=1∼n). Address i specifies the sequence of n particles and address j locates the particle in a sequence. For each particles, she chooses the basis S^{ij} and $|AS\rangle^{ij}$ in a random way. Then she sends all particles to Bob. Step2: Bob chooses m different subordinates bits u^i=0 or u^i=1 such that their parity represents his commitment bit Z. He repeats the following sub-steps from i=1 to i=m.(i) Assign the same basis C^i for all j particles belonging to the i-th sequence. (ii) Perform the measurement with C^i and obtains the outcomes $|BC\rangle^{ij}$(j=1∼n). (iii) Return the particles. Step3: For each particle, Alice obtains the outcome spin states $|AR\rangle^{ij}$(j=1∼n) with the measurement basis $R^{ij}\neq S^{ij}$.

[Opening phase] Step4: Bob opens Z and u^i(i=1∼m) which means C^i. Step5: Alice deduces $|AC\rangle^{ij}$ to be identical to $|AS\rangle^{ij}$ if $C^i=S^{ij}$, or to be identical to $|AR\rangle^{ij}$ if $C^i=R^{ij}$. For each sequence: Step6: Bob samples an arbitrary set of kn (k_i1/3) particles at random and notifies Alice of the locations for test. Step7: Alice answers him with her deduced state $|AC\rangle^{ij}$ for kn test particles. Step8: In total, Bob examines $|AC\rangle^{ij}=|BC\rangle^{ij}$ for mx(kn) particles. Unless he finds anti-coincidence, he regards Alice as honest. Otherwise he rejects Alice. For each sequence: Step9: Bob opens $|BC\rangle^{ij}$ for all (1-k)n particles. Step10: Alice examines the coincidence $|BC\rangle^{ij}=|AC\rangle^{ij}$ for those particles, which she employs as test particles. If she detects no errors, she accepts Z. Otherwise she rejects Z. After some detailed analysis, we can estimate the probabilities of detection as PB=1-$(1/2)^{2km}$ for dishonest Alice and PA=1-$(1/2)^{(1-2k)n}$ for dishonest Bob.

References

[1] H.K.Lo and H.F.Chau, Phys.Rev.Lett.78,3410(1997).

[2] K.Shimizu, H.Fukasaka, K.Tamaki and N.Imoto, Phys.Rev.A84,022308(2011).

Implmentation of Semi-device-independent Quantum Key Distribution

Devin H. Smith[1,2], **Geoff Gillett**[1,2], **Cyril Branciard**[2], **Marcelo de Almeida**[1,2], **Alessandro Fedrizzi**[1,2], **Brice Calkins**[3], **Thomas Gerrits**[3], **Adriana Lita**[3], **Antia Lamas-Linares**[3], **Sae Woo Nam**[3] and **Andrew G. White**[1,2]

[1]*Centre for Engineered Quantum Systems and Centre for Quantum Computation and Communication Technology (Australian Research Council), University of Queensland, Brisbane, Australia.*
[2]*School of Mathematics and Physics, University of Queensland, Brisbane, Australia*
[3]*National Institute of Standards and Technology, Boulder, Colorado, USA*

Quantum Key Distribution (QKD) relies upon several fundamental for its security, the most obvious being the correctness of quantum mechanics. Another critical assumption is that the apparatus of the two parties is well understood: to increase security, many attempts have been made to relax this assumption[1].

The primary trade-off made in relaxing QKD assumptions is between restrictive assumptions and restrictive requirements on implementation, primarily in the amount of loss tolerable before the secret key rate drops to zero. This is measured with the heralding ratio: given that one party receives an event, the fraction of times that the other does as well. Allowing both apparatus to be treated as an untrusted black box— the device independent case—sets the bound on the heralding rate to 91%, infeasible with current technology.

Recently QKD protocols have been described where only one party's apparatus is untrustworthy[2, 3]: in this case the heralding rate must exceed only 65.9%. Such a model can be realised for communication between a central authority and a remote observer whose apparatus may have been tampered with: a bank and a customer, for instance. In the protocol presented in ref [2], the relaxed bounds arise from steering inequalities, just as the *fully* device independent bound arises from Bell inequalities.

Here, we implement this protocol experimentally, building on our previous work on violating steering inequalities[4]: prior to this work, reaching the heralding rate required was infeasible. Transition edge sensors, are about twice as efficient as avalanche photodiodes [5], making these experiments possible. We generate entangled photon pairs in a periodically poled potassium titanyl phosphate (ppKTP) crystal in a polarising Sagnac interferometer, pumped with a 410nm laser diode. The untrusted black box apparatus is immediately adjacent to the source to minimise loss, and consists of a electro-optic modulator (EOM), a polarising beamsplitter and two superconducting transition edge sensors (TES) [5] with near-unit efficiency, see figure. The trusted apparatus is separated from the photon source via a fibre channel, and in contrast to the untrusted apparatus equipped with an additional 2 nm bandwidth filter to optimise the heralding efficiency.

This allows us to demonstrate the protocol in the lab, for the first time demonstrating device independence in QKD.

References

[1] Acin, A., *et al.* Device-independent security of quantum cryptography against colective attacks. Phys. Rev. Lett. 98, 230501 (2007)

[2] Branciard, C., *et al.* One-sided device-independent quantum key distribution: security, feasibility and the connection with steering. Phys. Rev. A 85, 010301 (2012).

[3] Ma, X. & Lütkenhaus, N. Improved data post-processing in quantum key distribution and application to loss thresholds in device independent QKD. Preprint at `http://arXiv.org/abs/1109.1203` (2011).

[4] Smith, D.H., Gillet, G., *et al.*. Conclusive quantum steering with superconducting transition-edge sensors. Nature Commun. 3, 625 (2012).

[5] Lita, A. E., Miller, A. J. & Nam, S. W. Counting near-infrared single-photons with 95% efficiency. Opt. Express 16, 30323040 (2008).

Coherent pulse position modulation quantum cipher

Masaki Sohma[1] and Osamu Hirota[1]

[1] *Quantum Information Science Research Center, Tamagawa University*

The coherent pulse position modulation (CPPM) cryptosystem has been proposed as a quantum cipher with multi mode quantum signal states[1]. It is a generalization of Y00 (or $\alpha\eta$) cryptosystem and has desirable characteristics. In the CPPM cryptosystem Alice encodes her classical messages by the block encoding where n-bit block j ($j = 1, ..., N = 2^n$) corresponds to the pulse position modulation (PPM) quantum signals with N slots, $|\Phi_j\rangle = |0\rangle_1 \otimes \cdots \otimes |\alpha_0\rangle_j \otimes \cdots \otimes |0\rangle_N$. In addition, Alice apply the unitary operator U_{K_i} to PPM quantum signals $|\Phi_j\rangle$, where the unitary operator U_{K_i} is randomly chosen via running key K_i generated by using PRNG on a secret key K_s. Thus, Alice gets the N-arry quantum signal states, $|\Psi_j(K_i)\rangle = U_{K_i}|\Phi_j\rangle$ which are sent to Bob. Let us assume an ideal channel. Since the secret key K_s, PRNG and the map $K_i \to U_{K_i}$ are shared by Alice and Bob, Bob can apply the unitary operator $U_{K_i}^\dagger$ to the received the quantum signal $|\Psi_j(K_i)\rangle$ and obtain the PPM quantum signal $|\Phi_j\rangle$. Bob decodes the message by the direct detection for $|\Phi_j\rangle$, which is known to be a suboptimal detection for PPM signals. Then Bob's block error rate is given by $P_e^{dir} = (1 - 1/N)e^{-|\alpha_0|^2} < e^{-|\alpha_0|^2}$. Here $e^{-|\alpha_0|^2} \approx 0$ holds for enough large signal energy $S = |\alpha_0|^2$.

Let us consider the unitary operator U of the form $|\alpha_1\rangle \otimes \cdots \otimes |\alpha_N\rangle \to |\alpha_1'\rangle \otimes \cdots \otimes |\alpha_N'\rangle$. We assume that the unitary operator U has the symplectic transformation $\mathcal{L}$, which is given through the charasteristic function. Then the unitary operator U can be determined uniquely by the unitary matrix $\mathcal{L}_C : (\alpha_1, ..., \alpha_N)^T \to (\alpha_1', ..., \alpha_N')^T$.

We give a foundation for discussing security of CPPM cryptosystem. Without knowing the secret key K_s Eve cannot apply the appropriate unitary operator to encrypted quantum signals $|\Psi_j(K_i)\rangle$, and hence she has to receive directly them. Since the quantum optimum receiver is unknown for such signals, we apply the heterodyne receiver, which is suboptimum and appropriate to discuss the performance of error. This scheme is called heterodyne attack. Our target is to study the heterodyne attack on $U|\phi\rangle$, where $|\phi\rangle$ is a general N-ary coherent state $|\alpha_1\rangle \otimes \cdots \otimes |\alpha_N\rangle$. Heterodyne detection is characterized by a family of operators with a parameter $\beta \in \mathbb{C}$, $X(\beta) = |\beta\rangle\langle\beta|/\pi$. The outcomes β of the heterodyne detection for a coherent state $|\alpha\rangle$ appears with the probability density function $\text{Tr}|\alpha\rangle\langle\alpha|X(\beta)$, which represents the normal distribution with the correlation matrix $(1/2)I_2$. The outcomes $\vec{\beta} = (\beta_1, ..., \beta_N)^T$ of the indivisual heterodyne detection for $U|\phi\rangle$ obeys the probability density function, $P_{U|\phi\rangle}(\vec{\beta}) = \text{Tr}|\phi\rangle\langle\phi|U^\dagger|\psi\rangle\langle\psi|U/\pi^N$, with $|\psi\rangle = |\beta_1\rangle \otimes \cdots \otimes |\beta_N\rangle$. Here, putting $\vec{\beta}' = (\beta_1', ..., \beta_N')^T = \mathcal{L}_C^*\vec{\beta}$, we get $U^\dagger|\psi\rangle\langle\psi|U/\pi^N = \otimes_{j=1}^N X(\beta_j')$. Then we obtain

$$P_{U|\phi\rangle}(\vec{\beta}) = P_{|\phi\rangle}(\vec{\beta}'), \qquad (1)$$

where $P_{|\phi\rangle}$ is the probability density function with which the outcomes of heterodyne detection for the state $|\phi\rangle$ appears.

Eq. (1) shows that the vectors $\vec{\beta}'$ given by applying the unitary matrix $\mathcal{L}_C^*$ to the outcomes $\vec{\beta}$ obeys the probability density function $P_{|\phi\rangle}$.

Yuen claimed that the CPPM cryptosystem has the following noteworthy property[1]. We allow Eve to get the secret key K_s after her heterodyne measurement for the encrypted quantum signals $|\Psi_j(K_i)\rangle$ and hence to know the unitary operator U_{K_i}. Then Eve can apply the unitary matrix $\mathcal{L}_{C,K_i}^*$ to obtain the vector $\vec{\beta}'$, which obeys to the probability density function $P_{|\Phi_j\rangle}$. This fact enables us to apply the decoding process for PPM signals. That is, Eve may use maximum-likelihood decoding for $\vec{\beta}'$, whose rule is to pick the j for which β_j' is largest, and her error probability is lower bounded as: $P_e^{het}(key) \geq Q_N(z)\Phi(z - \sqrt{2S})$, where the parameter z can take any real number value and $\Phi(z) = 1 - ((1/\sqrt{2\pi})\int_{-\infty}^y \exp(-v^2/2)dv)^{N-1}$. Putting $z = \sqrt{fn}$ and $n = \log_2 N$ in this inequality, we obtain

$$P_e^{het}(key) \geq Q_{2^n}(\sqrt{fn})\Phi(\sqrt{fn} - \sqrt{2S}) \to 1, n \to \infty.$$

Thus, in the CPPM scheme, Eve cannot pin down the information bit even if she gets the true secret key K_s and PRNG after her measurement.

In the CPPM system, the unitary operator U_{K_i} can be realized by combination of beam splitters and phase shifts. However such system becomes too complicated to implement when the number of slots, 2^n, is large. On the other hand, we can take another approach to implementing the unitary operator U_{K_i} by taking a state expression different from $|\Phi_j\rangle$. We use the model of Gaussian waveform channel [2], where we consider the periodic operator valued fanction $X(t) = \sum_j \sqrt{2\pi\hbar\omega_j/T}(a_j e^{-i\omega_j t} + a_j^\dagger e^{i\omega_j t})$, which corresponds to electric field in a planar wave with periodic boundary condition on finite interval. Then we can describe the quantum PPM signal as the quantum state $S = \otimes_j |\gamma_j\rangle\langle\gamma_j|$ such that $\gamma(t) = \text{Tr}SX(t)$ gives a classical PPM signal. We employ the unitary transformation of the form $\otimes_j |\gamma_j\rangle\langle\gamma_j| \to \otimes_j |\gamma_j'\rangle\langle\gamma_j'|$. Among such unitary operaotrs, the spectral-phase encryption (phase mask) can be implemented by the acousto-optic modulator[3]. We can estimate the security of such system in a similar mannar as in the case of CPPM system. Detailed analysis will be given in the presentation at the conference.

References

[1] H.P. Yuen, J. Selected topics in Quantum Electronics, **15**,6,1630-1645 (2009).

[2] A. S. Holevo, Tamagawa University Research Review, **4**, 1 (1998).

[3] S. Ozharar et. al. Journal of lightwave technology, **29** 14 (2011).

Novel QKD experiments performed at INRIM

Alessio Avella[1], **Giorgio Brida**[1], **Dino Carpentras**[1], **Andrea Cavanna**[1], **Ivo Pietro Degiovanni**[1], **Marco Genovese**[1], **Marco Gramegna**[1], **and Paolo Traina**[1]

[1]*INRIM - Istituto Nazionale di Ricerca Metrologica, Turin, Italy*

In recent years Quantum Key Distribution (QKD) has emerged as the most paradigmatic example of Quantum technology allowing the realization of intrinsically secure communication links over hundreds of kilometers. Beyond its commercial interest QKD also has high conceptual relevance in the study of quantum information theory and the foundations of quantum mechanics. In particular, the discussion on the minimal resources needed in order to obtain absolutely secure quantum communication is yet to be concluded.

Here we present our last experimental results concerning two novel quantum cryptographic schemes which do not require some of the most widely accepted conditions for realizing QKD.

The first is Goldenberg-Vaidman protocol [1], in which even if only orthogonal states (that in general can be cloned without altering the state) are used, any eavesdropping attempt is detectable.

The second is Noh09 protocol [2] which, being based on the quantum counterfactual effect, does not even require any actual photon transmission in the quantum channel between the parties for the communication.

References

[1] L. Goldenberg and L. Vaidman, Phys. Rev. Lett., **75**, 1239 (1995).

[2] T.-G. Noh, Phys. Rev. Lett., **103**, 230501 (2009).

Turbulent single-photon propagation in the Canary optical link

Ivan Capraro[a], Andrea Tomaello[a], Thomas Herbst[b], Rupert Ursin[c], Giuseppe Vallone[a] and Paolo Villoresi[a]

[a] Department of Information Engineering, University of Padova, Padova, Italy
[b] Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, Vienna, Austria
[c] IQOQI - Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Vienna, Austria

The long free-space links on ground are excellent tools for investigating quantum phenomena over long distances[1] as well as the most convenient test bench for the quantum communication to the Space and between spacecrafts. The Canary archipelago provides a remarkable environment, and in particular the sites of the Optical Ground Station (OGS) of the European Space Agency (ESA), in Tenerife and the Jakobus Kapteyn Telescope (JKT) in La Palma, separated by 144 km, both at the altitude of about 2400 m above the Atlantic Ocean.

In this work we have tested the link using a novel transmitter, using a singlet aspheric lens of 23 cm diameter and 220 cm focal length. The choice of the lens aims to minimize the spot size at OGS compared to the telescope primary mirror according to our observations and consequently a greater power transfer between the two sites. A near infrared (808 nm) laser coupled into single mode fiber and suitably attenuated was used as source. The transmitter setup is shown in

Figure 1: Transmitter setup at the JKT in La Palma.

Fig. 1. The receiver was the OGS telescope, of 1 meter of diameter. In the Coudé focalplane we collected the stream of attenuated coherent beam with a single photon detector (SPAD) and a multiscaler. The fluctuation of the received
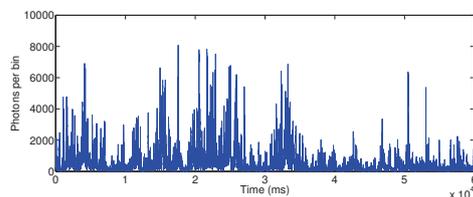
Figure 2: Photons collected in 1 minute with bins of 1 ms.

signal has been calculated from suitably binned single photon counts, in order to analyze the intensity fluctuation of the gathered beam. An example of 1 minute acquisition is shown in Fig. 2. In agreement with Ref. [2], the statistics of the

photon collection varies from the poissonian at the transmitter to lognormal at the receiver, as it is demonstrated in the fit reported in Fig. 3. The fraction above a given number of pho-
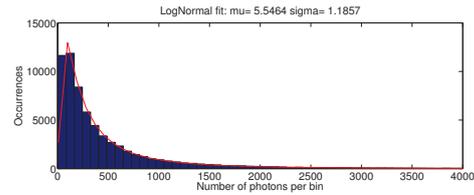
Figure 3: Fit of the photon counts with a lognormal.

ton per bin, that is related to the intensity, may be calculated using Eq. 1, and in the case shown is predicted to be of 7%, confirmed by the observations.

$$p(q > q_0) = \frac{1}{2}(1 - \mathrm{erf}[\frac{\ln \frac{q_0}{\langle q \rangle} + \frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}}]) \qquad (1)$$

However, the analysis of the temporal distribution of this high intensity fraction have shown that such fraction is collected in a series of fairly long consecutive pulses, that spans a few tens of ms, as shown in Fig. 4 in the case of a value of collection at least twice of the average value, that results of 6.4%. Such
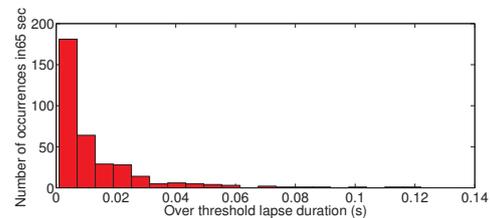
Figure 4: Duration of the consecutive lapses.

bright period corresponds to about a million laser pulses in the quantum communication implementation[1]. Therefore, the effect of turbulence is here found to provide a noticeable fraction of the link time with a significant lower-than-average optical losses.

References

[1] Ursin, R. et al., "Entanglement-based quantum communication over 144 km," *Nat. Phys.* **3**, 481 (2007).

[2] Milonni, P. W. et al., "Effects of propagation through atmospheric turbulence on photon statistics," *J. of Opt. B* **6**, S742–S745 (2004).

Security of Continuous Variable Quantum Cryptography with Post-selection

Nathan Walk[1], Thomas Symul[2], Ping Koy Lam[2] and Timothy C. Ralph[1]

[1] Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland
[2] Centre for Quantum Computation and Communication Technology, Department of Quantum Science, Australian National University

Quantum key distribution (QKD) is a quantum communications protocol in which a random key is distributed between two distant parties with security guaranteed by fundamental limits to quantum measurement[1]. It has been studied and implemented in both discrete and continuous variables of the optical field with the latter offering very high raw bit rates and an attractive synergy with existing communications infrastructure although efficiently reconciling the continuously valued measurements has proved challenging.

A promising avenue is the use of classical post-selection techniques [2] but these have faced a significant theoretical hurdle in that is has only been possible to prove their security under the assumption of a Gaussian eavesdropping attack[3]. We remove this restriction and provide a security proof without such an assumption by providing an entanglement based version of the post-selection protocol. Based on the proof method we also propose a different form of post-selection to provide a protocol for which the lower bounds on the achievable secret key rate will be tighter.

We now sketch the proof. At the end of the protocol the legitimate parties have access to the second order moments of the quadratures of the ensemble before and after the post-selection process. We may safely assume that the final ensemble is Gaussian as this would maximise the eavesdropper's information. In the event that a non-Gaussian post-selection is employed this is equivalent to assuming the the eavesdropper implemented exactly the correct non-Gaussian attack such that the two operations combine to give a Gaussian ensemble overall. Another way to calculate this lower bound to the secret key rate is to identify a combination of a Gaussian attack and Gaussian post-selection that result in the same statistics for both the original and post-selected ensemble.

In general any post-selection will result in an ensemble that looks like it has undergone some or all of a) entanglement distillation/noiseless amplification[4], b) classical amplification, c) additional noise. Gaussian operations achieving these respectively are (Fig.1) a noiseless linear amplifier (NLA), two-mode squeezing(TMS), and interaction with one arm of an EPR state at a beamsplitter. Using only the covariance matrices before and after post-selection the parameters of the equivalent Gaussian post-selection and channel can be uniquely determined.

Note that a completely general post-selection, especially one that explicitly breaks phase symmetry, may require a more complicated representation than Fig.1 and this the case for the kind of post-selection originally proposed.

Motivated by this and the fact that non-Gaussian operations tend to appear as further excess noise at the level of the covariance matrix we propose a 'Gaussian' kind of post-selection. Whereas original proposals kept or rejected data based simply upon the absolute value relative to some cut-
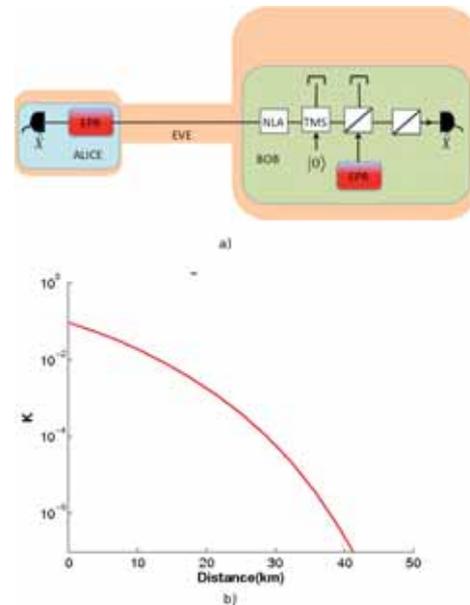
Figure 1: a) Entanglement based version of post-selection protocol. b) Secret key rate as a function of distance which is related to transmission via $T = \eta 10^{-.02 dist}$ where $\eta = 0.6$.

off we introduce a different filtering where data is kept probabilistically with a view to transforming the original distribution in to a Gaussian of a larger variance. Of course this operation cannot be perfectly implemented but the non-Gaussianity involved is considerably less and thus this new protocol is much more suited to our new proof. As a simple application of our proof we calculate the secret key rate of a direct reconciliation protocol including 'Gaussian' post-selection and find that key is achieved well beyond the range possible without post-selection demonstrating that the bounds achieved under this method are not prohibitively pessimistic.

References

[1] V. Scarani, et. al., Rev. Mod. Phys, **81**, 1301 (2009).

[2] Ch. Silberhorn, T. C. Ralph, N. Lutkenhaus and G. Leuchs, Phys. Rev. Lett, **89**, 167901, (2002).

[3] M. Heid and N. Lutkenhaus, Phys. Rev. A, **76**, 022313 (2007).

[4] T. C. Ralph and A. P. Lund, *Quantum Communication Measurement and Computing Proceedings of 9th International Conference*, (AIP, New York, 2009).

Gigahertz quantum key distribution over 260 km of standard telecom fiber

Shuang Wang,[1] Zhen-Qiang Yin,[1] Wei Chen,[1] Jun-Fu Guo,[2] Hong-Wei Li,[1] Guang-Can Guo,[1] and Zheng-Fu Han[1]
[1]*Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, China*
[2]*Anhui Asky Quantum Technology Co.,Ltd., Wuhu 241002, China*

With the dispersion-shifted fiber, Takesue et al. realized the first QKD experiment over 42.1 dB channel loss and 200 km of distance [1]. Then, with the ultra low loss fiber, Stucki et al. implemented the first QKD experiment over 250 km of distance, but the channel loss is still 42.6 dB [2]. In this paper, focused on the transmission over the widely used standard (ITU-T G.652) telecom fiber, of which loss coefficient is about 0.2 dB/km and dispersion is about 17 ps/(km · nm) at 1550 nm region, we report a QKD experiment over 260 km of this standard telecom fiber with 52.9 dB channel loss [3]. This is the first QKD experiment exceeding 50 dB in channel loss and 250 km in length.

We chose the differential phase shift QKD (DPS-QKD) protocol to be implemented with 2 GHz rate [3]. The experimental setup is outlined in Fig. 1.
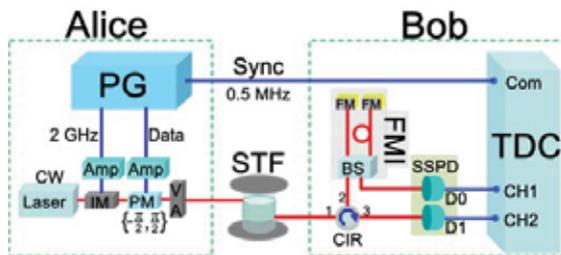
FIG. 1: Schematic of the DPS-QKD setup [3].

Based on specific experimental parameters, the secure key rate under individual attacks could be maximized by choosing optimal μ for each fiber length, and the attainable maximum distance is 281 km in principle. With standard telecom fiber, the sifted key rates and QBERs were measured at seven different fiber lengths.

The dark count rate of detectors is a major limiting factor for long-distance QKD . Therefore the ultra low-noise SSPD was used in our DPS-QKD system. We first set the EDE and DCR of SSPD at 2.5% and 1 Hz respectively. Through careful optimization of the 1-bit delayed interferometer, we achieved the values of QBER below 2% for the first six lengths, and of 3.45% for the 260 km length fiber with 52.9 dB loss. At 205 km with 41.6 dB transmission loss, 99.2 bits/s secure key rate was ob-

tained, this rate value was more than eight times of that achieved in 10-GHz DPS-QKD experiment at 200 km with 42.1 dB loss [1]. Although the channel loss of 260 km was one order of magnitude larger than the loss 42.6 dB in previous 250 km QKD experiment [2], in which the ultra low loss fiber with 0.164 dB/km loss coefficient
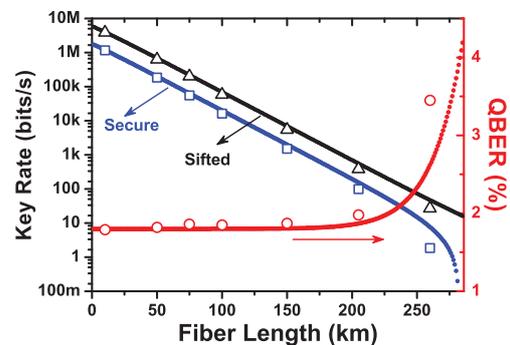
FIG. 2: Experimental results of DPS-QKD [3].

was used, secure keys with 1.85 bits/s rate could still be shared between Alice and Bob.

When the transmission fiber length was short, the signal contribution was much larger than the dark count contribution. In order to get higher key rate, we improved the quantum efficiency of SSPD by increasing the bias current, though the dark count rate increased faster as the current increased. In the 50 km fiber length experiment, another $\eta_D = 11.2\%$ value was tested, QBER was 1.89%, and the corresponding secure key rate got up to 0.81 Mbits/s, which was close to Dixon's BB84 experiment [4].

In summary, we have experimentally demonstrated that quantum key distribution is possible over 260 km standard telecom fiber with 52.9 dB loss. Using the ultra low loss fiber with 0.164 dB/km loss coefficient [2], the quantum key exchange over 340 km distance is in sight.

[1] H. Takesue et al. Nature Photonics **1**, 343 (2007).
[2] D. Stucki et al. New J. Phys. **11**, 075003 (2009).
[3] S. Wang et al. Opt. Lett. **37**, 1008 (2012).
[4] A. R. Dixon et al. Appl. Phys. Lett. **96**, 161102 (2010).

WDM quantum key distribution system using dual-mode single photon detectors

__K. Yoshino__[1], M. Fujiwara[2], A. Tanaka[1]*, S. Takahashi[1], Y. Nambu[1], A. Tomita[3], S. Miki[2], T. Yamashita[2], Z. Wang[2], M. Sasaki[2] and A. Tajima[1]

[1]*NEC Corporation, Kasawaki, Japan*
[2]*National Institute of Information and Communications Technology, Tokyo, Japan*
[3]*Hokkaido University, Sapporo, Japan*

Quantum key distribution (QKD), which enables us to share secret random numbers between distant parties, can realize information-theoretically secure communication. Recently video data encryption using QKD has been performed in installed optical fiber networks [1]. As single photon detection (SPD) devices, avalanche photodiodes (APDs) and superconducting single photon detectors (SSPDs) have been mainly used. Thermo-electric cooled APD is suitable for downsizing and low-cost manufacturing. Although SSPD needs a special cooling system ($\sim$2 K), their noises are extremely small. Therefore SSPD is suited for a long-distance transmission, where QKD performance is very sensitive to the noises. We should use appropriate detectors in each situation.

To realize flexible QKD, we developed 'dual-mode' SPD circuits applicable to APD and SSPD. We incorporated them into our wavelength-division multiplexing (WDM) QKD system and performed a field test through a 45-km fiber [2].

The block diagrams of a SPD circuit with an APD and a SSPD are shown in fig.1 (a) and (b). For the APD, a field programmable gate array (FPGA) on the SPD circuit generates sine-wave gate pulses and DC bias voltage, which is applied to the APD. After passing through the APD, gate pulses are removed by a band eliminate filter (BEF). Remaining photon detection signals enter into an analog-to-digital converter (ADC). Then the FPGA retrieves the voltage data from the ADC. Meanwhile, the SSPD is driven by a current source. Output signals from the SSPD are sampled by the ADC.

Different discrimination processes are applied by the FPGA to sampled voltage data from each device because of the differences in output signal property. For the APD, ampli-

Table 1: Key generation performances over 12 hours.

Wavelength [nm]	Detector	QBER [%]	Sifted key rate [kbps]	Secure key rate [kbps]
λ1: 1549.32	APD	3.03	381.22	91.11
λ2: 1550.12	SSPD	3.02	160.31	40.56
λ3: 1550.92	SSPD	2.32	301.10	76.18

tudes of detection signals fluctuate widely. It is desirable to set the threshold as low as possible to improve the detection efficiency. However, residual gate pulses derived from the imperfection of the BEF prevent to lower the threshold. To avoid this, we implemented gate pulse subtraction method, which extracts waveforms of residual gates and subtracts them from original ones (fig.1 (c)). It leads to lower threshold level.

For the SSPD, although the amplitudes of output signals are nearly uniform, multiple data exceed the threshold due to the wide signals. Additionally, non-gate operation causes unwanted satellite pulse detection (fig.1 (e)). It appears before and after the primary pulse by the delay of interferometers (400 ps in our system). To remove the satellite detection, we implemented mask processing and odd-even data selection (fig.1 (d)). First, to validate only first data point among multiple data exceeding the threshold in single detection event, subsequent data are masked. Then odd or even number data ('o' or 'x' in fig.1 (d)) are selected. Because sampling interval of our system is about 400 ps and satellite pulse appears 400 ps apart from primary pulse, odd or even data correspond to primary or satellite pulses. Thus, we can extract correct detection events (corresponding to 'o') by odd-even selection.

Our dual-mode SPD circuit can be effectively used for both APD and SSPD only by rewriting the FPGA program.

We demonstrated our 3-channel WDM QKD system. The block diagram of single channel is shown in fig.1 (e). We tested the system through a 45-km installed single-mode fiber, whose total loss is 14.5 dB. In the receiver, one APD system and two SSPD systems were used. Key generation performances are summarized in Table 1. Secure key generation at a rate of 208 kbps in total during 12 hours was achieved, which is the highest level in the world.

We have developed dual-mode SPD circuits applicable to APD and SSPD. Using the circuits with APD and SSPD, our three-channel WDM QKD system could generate secure keys of 208 kbps in total through a 45-km installed fiber.

* A. Tanaka is currently with NEC Laboratories America.
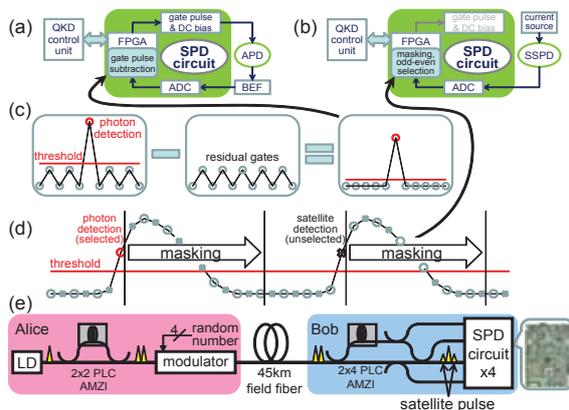
Figure 1: (a) SPD circuit with APD and (b) SSPD. (c) Gate pulse subtraction for APD. Frequencies of gate pulse and sampling are 1.24 and 2.48 GHz. (d) Masking and odd-even selection for SSPD. (e) Single-channel QKD. Three channels were used in the field test.

References

[1] M. Sasaki, et. al., Opt. Express __19__, 10387 (2011).

[2] K. Yoshino, et. al., Opt. Lett. __37__, 223 (2012).

Measurement-based quantum repeaters

Michael Zwerger[1], **Wolfgang Dür**[1] **and Hans J. Briegel**[1,2]

[1]*Institut für Theoretische Physik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria*
[2]*Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften, Innsbruck, Austria*

We introduce measurement-based quantum repeaters, where small-scale measurement-based quantum processors are used to perform entanglement purification and entanglement swapping in a long-range quantum communication protocol. In the scheme, pre-prepared entangled states stored at intermediate repeater stations are coupled with incoming photons by simple Bell-measurements, without the need of performing additional quantum gates. We show how to construct the required resource states, and how to minimize their size. We analyze the performance of the scheme under noise and imperfections, with focus on small-scale implementations involving entangled states of few qubits. We find measurement-based purification protocols with significantly improved noise thresholds. Furthermore we show that already resource states of small size suffice to significantly increase the maximal communication distance. We also discuss possible advantages of our scheme for different set-ups.

References

[1] M. Zwerger, W. Dür, and H.J. Briegel, arXiv:1204.2178

Implementing controlled-unitary operations over the butterfly network

Akihito Soeda[1], **Yoshiyuki Kinjo**[1], **Peter S. Turner**[1], and <u>**Mio Murao**</u>[1]

[1]*The University of Tokyo, Tokyo, Japan*

In order to investigate distributed quantum computation under restricted network resources, we introduce a quantum computation task over the butterfly network where *both* quantum and classical communications are limited. We consider deterministically performing a two-qubit global unitary operation on two unknown inputs given at different nodes, with outputs at two distinct nodes. By using a particular resource setting introduced by Hayashi [1], we show that unitary operations can be performed *without adding any entanglement resource*, if and only if the unitary operations are locally unitary equivalent to controlled-unitary operations. Our protocol is optimal in the sense that the unitary operations cannot be implemented if we relax the specifications of any of the channels.

Communication over the butterfly network: In large networks, it often happens that communication traffic is concentrated in some of the channels. This leads to a bottleneck problem and it restricts the total communication performance. In network information theory, this problem has been extensively studied for the last decade as network source coding. Although solving general network problems is difficult, a solution of the 2-pair communication (communications between two disjoint sender-receiver pairs) bottleneck problem is known for a simple directed network called the *butterfly network* [2] in the classical case. In the quantum case, where the no-cloning theorem holds, the method used in the classical case cannot be applied directly, since it involves cloning inputs. Nevertheless, in [3], it is shown that efficient network source coding on the quantum butterfly network, where edges represent 1-qubit quantum channels, is possible for transmitting approximated states. In [1], it is shown that perfect quantum 2-pair communication over the butterfly network is possible if we add two maximally entangled qubits between the inputs and allow each channel to use either 1 qubit of communication or 2 bits of communication.

Computation over the butterfly network: The task we consider is to deterministically implement a global unitary operation on two inputs at distant nodes and obtain two outputs at distinct nodes on a network by combining both quantum computation, namely, performing a gate operation on inputs, and network communication, namely, sending outputs, in a *single task*. We say that a two qubit unitary operation U is implementable over a network, if we can obtain a joint output state $U|\psi_1\rangle|\psi_2\rangle$ of qubits at the nodes B_1 and B_2, for any input state $|\psi_1\rangle|\psi_2\rangle$ of two qubits, one at node A_1 and the other at node A_2, by performing general operations including measurements at each node and communicating qubit and bit information through channels specified by edges.

Implementation of controlled-unitary operations A controlled-unitary operation is given by $C_u = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes u$ where u is a single qubit unitary operation. Since any controlled-unitary operation is locally unitarily equivalent to a controlled-phase operation, we only need to consider the implementation of the corresponding controlled-phase

operation C_{u_θ} where $u_\theta = |0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|$. Additional local unitary operations can be performed at the input and output nodes. The protocol to implement C_{u_θ} over the particular butterfly network introduced by Hayashi [1] is given by the quantum circuit shown in Figure 1a. Quantum/classical information is transmitted between the nodes using the quantum/classical communication specified by the edges shown in Figure 1b. By analyzing this protocol, we also show that global unitary operations are implementable over this butterfly network without adding any extra resources *only if* they are locally unitarily equivalent to controlled-unitary operations [4].
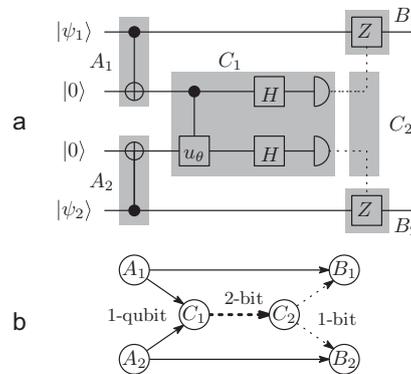
Figure 1: a: The quantum circuit for implementing a controlled-phase operation on the first qubit and the fourth qubit. Each shaded block indicates operations at a node. H denotes a Hadamard operation, and detectors denote the Z-measurements. The dotted line represents a controlled operation depending on the measurement outcome. b: The butterfly network corresponding to the quantum circuit above. The solid line, thick dotted line and the thin dotted line denote a single qubit channel, a two bit channel, and a single bit channel, respectively.

References

[1] M. Hayashi, Phys. Rev. A **76**, 040301(R) (2007).

[2] R. Ahlswede *et al.*, IEEE Trans. Inf. Th. **46**, 1204 (2000).

[3] M. Hayashi *et. al.*, quant-ph/0601088v2 (2006), D. Leung and J. Oppenheim and A. Winter, quant-ph/0608223v4 (2007).

[4] A. Soeda, Y. Kinjo, P. S. Turner and M. Murao, Phys. Rev. A 84, 012333 (2011).

Universal construction of controlled-unitary gates using the dynamical decoupling and the quantum Zeno effect

Shojun Nakayama[1], Akihito Soeda[2] and Mio Murao[1]

[1]*University of Tokyo, Tokyo, Japan*
[2]*National University of Singapore, Singarpore, Singapore*

We present two new algorithms that *universally* construct a quantum circuit approximating a controlled-$U(t)$ gate up to the global phase factor of $U(t)$, where $U(t) = e^{-iHt}$ is the unitary evolution operator a system's *unknown* Hamiltonian H of a system, and is given as a black box with tunable parameter t. We show that it is possible to construct controlled-$U(t)$ with arbitrarily high accuracy. This algorithm is based on the *dynamical decoupling [6]*. If another black box consisting of a time-inverted version of $U(t)$, namely $U(-t) = U^\dagger(t)$, is also available in addition to the black box consisting of $U(t)$, we can implement controlled-$U(t)$ *exactly* with arbitrarily high success probability. This algorithm is based on *the quantum Zeno effect.*

Controllization of unitary operations: Controlled-unitary operations play important roles in quantum algorithms. Examples include Kitaev's phase estimation algorithm [1], Shor's period-finding and factorization algorithm [2], precision length metrology [3], and thermalization algorithms for Hamiltonian systems using the Metropolis method [4]. Several methods for constructing controlled unitary operations are known. However, these methods require specific input states [3], knowledge of the given Hamiltonian [4] or take advantage of a specific feature of the system's Hilbert space [5].

The algorithm based on the dynamical decoupling: The first controllization algorithm is given by N iterations of the operation represented by the quantum circuit shown in Figure.1.
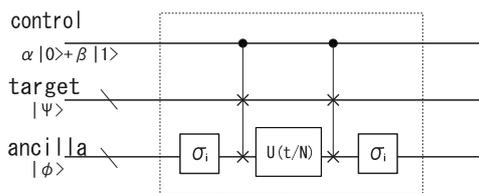
Figure 1: σ_i is randomly chosen from the set of generalized Pauli operations for each iteration. The dimension of the ancilla system is the same as that of the target system.

When the control qubit is $|1\rangle$, the target state picks up the unitary $U(t/N)$ but the ancilla state does not change. On the other hand, when the control bit is $|0\rangle$, the ancilla state is affected by the unitary $\sigma_i U(t/N)\sigma_i$. The change of the ancilla state depends on the state of the control qubit, but if we chose σ_i randomly, the effect of the accumulation of the unitary operations is almost an identity operation with the error order of $1/N$. This property is the dynamical decoupling [6].

Moreover, we show that if the system consists of spins ar-

rayed on a square lattice and only nearest neighbor interactions exist, by choosing an appropriate order of Pauli operations instead of random choices, a controlled-unitary with $1/N^2$ order of error can be implemented.

The algorithm based on the quantum Zeno effect: If $U^\dagger(t)$ is also possible, we can implement a controlled unitary exactly. Consider the following unitary on $(|0\rangle + |1\rangle)|\psi\rangle|\phi\rangle$

$$U_{cs}\left(\mathbf{I}_{cnt} \otimes U(t/N) \otimes U^\dagger(t/2N)\right) U_{cs}(|0\rangle + |1\rangle)|\psi\rangle|\phi\rangle$$
$$= |0\rangle|\psi\rangle U(t/2N)|\phi\rangle + |1\rangle U(t)|\psi\rangle U^\dagger(t/2N)|\phi\rangle \quad (1)$$

where U_{cs} denotes a controlled-swap operation between the target and ancilla systems. Then perform a projective measurement including $|\phi\rangle\langle\phi|$. If we obtain the outcome $|\phi\rangle$, the state of the remaining systems is given by

$$|0\rangle|\psi\rangle + e^{i\theta(H,t,N)}|1\rangle U(t/N)|\psi\rangle \quad (2)$$

where

$$e^{i\theta(H,t,N)} = \frac{\langle\phi|U^\dagger(t/2N)|\phi\rangle}{\langle\phi|U(t/2N)|\phi\rangle}. \quad (3)$$

This is the controlled unitary up to the irrelevant global phase of $U(t/N)$.

Notice that the probability for obtaining the measurement outcomes other than $|\phi\rangle$ is $1/N^2$ for $U(t/N)$. This effect of frequent measurement to stabilize a state is referred to as the quantum Zeno effect. If we iterate this process N times with the ancilla state being reset in $|\phi\rangle$ after each measurement, the total error probability is of the order of $1/N$. Therefore, by iterating this operation N times, we obtain the controlled-$U(t)$ gate up to the global phase factor of $U(t)$ with arbitrary high success probability.

References

[1] A. Y. Kitaev, *Electr. Coll. Comput. Complex* **3**, 3 (1996)

[2] P. W. Shor, *arXiv* :9508027 (1996)

[3] B. L. Higgins, D. W. Berry, S. D. Bartlett, H. M. Wiseman and G. J. Pryde, *Nature* **450**, 393–396 (2007)

[4] K. Temme, T.J. Osborne, K.G. Vollbrecht, D. Poulin, F. Verstraete, *arXiv*:0911.3635 (2010)

[5] X-Q Zhou, T. C. Ralph, P. Kalasuwan, M. Zhang, A. Peruzzo, B. P. Lanyon and J. L. O'Brien, *Nature Communications* **413** (2011)

[6] L. Viola, E. Knill and S. Lloyd, Phys. Rev. Lett. 82, 2417–2421 (1999).

Robustness of Device Independent Dimension Witnesses

Michele Dall'Arno[1], **Rodrigo Gallego**[1], <u>**Elsa Passaro**</u>[1]**, and Antonio Acín**[1,2]

[1]*ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*
[2]*ICREA-Institució Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain*

Device independent dimension witnesses (**DIDWs**) [1, 2, 3] provide a lower bound on the dimensionality of classical and quantum systems, where no assumptions are made about the way the devices work or on what system they operate, but only the correlations among preparations, measurements and outcomes are considered.

In [4], we characterize the sets of classical and quantum correlations achievable with local and shared randomness, and provide analytical and numerical tools for the optimization of DIDWs. In particular, we consider the sets of correlation matrices $\mathcal{M}^C$ ($\mathcal{M}^Q$), $\mathcal{M}_{LR}^C$ ($\mathcal{M}_{LR}^Q$) and $\mathcal{M}_{SR}^C$ ($\mathcal{M}_{SR}^Q$) given by classical (quantum) ensembles, when no randomness, local randomness and shared randomness is allowed, respectively. We show that

$$\mathcal{M}^C \subset \mathcal{M}_{LR}^C \subset \mathcal{M}^Q = \mathcal{M}_{LR}^Q, \quad (1)$$

$$\mathcal{P}(\mathcal{M}^Q) = \mathcal{P}(\mathcal{M}_{LR}^C) = \mathcal{P}(\mathcal{M}^C) = \mathcal{M}_{SR}^C. \quad (2)$$

where we denote with $\mathcal{P}(\mathcal{M})$ the polytope corresponding to the convex closure of $\mathcal{M}$.

The general setup for performing device independent dimension witnessing is given by a preparing device (on Alice's side) and a measuring device (on Bob's side) with shared randomness. Alice chooses the value of index $i = 1, \ldots M$ and sends to Bob the state $\rho_{i,\lambda} \in \mathcal{L}(\mathcal{H})$, where $\mathcal{L}(\mathcal{H})$ is the space of linear operators on the Hilbert space $\mathcal{H}$. Bob chooses the value of index $k = 1, \ldots K$ and performs the POVM $\Pi_{k,\lambda}$ on the received state, obtaining the outcome $j = 1, \ldots N$.
Finally they collect the statistics over indexes i, j, and k, getting the conditional probabilities $p_{j|i,k}$. Their task is to provide a lower bound on the dimension d of $\mathcal{H}$ or, when d is known, to say if the state ρ_i may be classical. To this aim they apply a dimension witness.

Definition. *A device independent dimension witness $W(p_{i|j,k})$ is a function of the conditional probabilities $p_{i|j,k}$ such that*

$$W(p_{i|j,k}) \geq L_d \Rightarrow \dim(\mathcal{H}) \geq d, \quad (3)$$

for some L_d which depends on W.
We show that the maximum of any linear DIDW is achieved by an ensemble of pure states and without shared randomness, and we give an algorithm to optimize any linear DIDW.

The problem of the **robustness of DIDWs to noise and loss** unavoidably affects any implementation such as semidevice independent quantum key distribution [5], random access code and randomness generation [6]. To address this problem we consider an ideal preparing device followed by a measurement device with non-ideal detection efficiency, namely where each POVM $\Pi = \{\Pi^j\}$ is replaced by a lossy POVM

$$\Pi^{(\eta)} := \{\eta\Pi, (1-\eta)\mathbb{1}\}. \quad (4)$$

The lossy POVM has an outcome more than the ideal one, that we associate to the no-click event. We generalize the tools used for the optimization of DIDWs to the noisy and lossy case, considering the simplest non-trivial scenario with $M = 3$ preparations and $K = 2$ POVMs each with $N = 3$ outcomes, one of which being proportional to the identity.

The DIDW given by $W(R, P) = \sum_{ijk} c_{ijk} \text{Tr}[\rho_i \Pi_k^j]$, with

$$c_{ijk} = \begin{cases} \delta_{j1} & \text{if } i + k \leq M \\ -\delta_{j1} & \text{otherwise} \end{cases},$$

which is the only nontrivial DIDW for $M = 3$, $K = 2$, and $N = 2$ [1], is verified to be a tight DIDW even with $N = 3$, and in this case, to be the most robust to noise. In [1] it is conjectured that its generalization to higher dimensions, with $M = d + 1$, $K = d$ and $N = 2$ is a tight DIDW for dimension d, and in [4] we conjecture that it is also the most robust to noise.

Finally, we provide an upper and lower bound for the maximum of this DIDW as a function of the dimension d. The figure below plots the maximal value (middle line) of the parameter η^C characterizing non-ideal detection efficiency for different values of the dimension d of the Hilbert space $\mathcal{H}$.
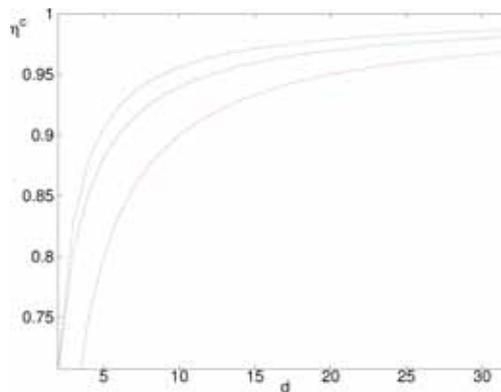
References

[1] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. **105**, 230501 (2010).

[2] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, arXiv:quant-ph/1111.1208.

[3] H. Ahrens, P. Badziąg, A. Cabello, and M. Bourennane, arXiv:quant-ph/1111.1277.

[4] M. Dall'Arno, R. Gallego, E. Passaro, and A. Acín (to be submitted).

[5] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302 (2011).

[6] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, arxiv:quant-ph/1109.5259.

Dissipative Quantum Computing with Open Quantum Walks

Ilya Sinayskiy[1] and Francesco Petruccione[1]

[1] *NITheP and School of Chemistry and Physics, University of KwaZulu-Natal, Durban, South Africa*

The description of any quantum system includes the unavoidable effect of the interaction with the environment [1]. Such open quantum systems are characterized by the presence of decoherence and dissipation. Typically, the influence of the interaction with the environment on the reduced systems needs to be eliminated or minimized. However, it was shown recently that the interaction with the environment not only can create complex entangled states [2], but also allows for universal quantum computation [3].

One of the well established approaches to formulate quantum computing algorithms is the language of quantum walks [4]. Both, continuous and discrete-time quantum walks can perform universal quantum computation [5]. Typically, taking into account the decoherence and dissipation in a quantum walk reduces its applicability for quantum computation [7].

Recently, a framework for discrete time open quantum walks on graphs was proposed [8], which is based upon an exclusively dissipative dynamics. The flexibility and the strength of the open quantum walk formalism [8] will be used to implement quantum algorithms for dissipative quantum computing. With the example of the Toffoli gate and the Quantum Fourier Transform with 3 and 4 qubits we will show that the open quantum walk implementation of the corresponding algorithms outperforms the original dissipative quantum computing model [3]. In Fig 1 the efficiency of OQW implementation of 3-qubit QFT is presented. Curves (1)-(4) in Fig. 1a correspond to different values of the parameter $\omega = 0.5, 0.6, 0.8, 0.9$, respectively. The curve (1) corresponds to the case $\omega = 0.5$ which is the conventional dissipative quantum computing model.

Figure 1: Open quantum walk efficiency of the 3-qubit QFT. Fig. 1a shows the dynamics of the detection probability in the final node 9 as function of the number of steps of the OQW. Curves (a1) to (a4) correspond to different values of the parameter $\omega = 0.5, 0.6, 0.8, 0.9$, respectively. Fig. 1b shows the number of steps needed to reach the steady state (squares) and the probability of detection of the successful implementation of the quantum algorithm (circles) as function of the parameter ω. The number of steps to reach a steady states is simulated with 10^{-7} accuracy.

References

[1] Breuer H.-P. and Petruccione F.: The Theory of Open Quantum Systems, 613p, Oxford University Press, Oxford, (2002)

[2] Diehl S *et al*, Nature Phys. 4, 878-883 (2008); Vacanti G. and Beige A., New J. Phys. 11, 083008, (2009); Kraus B.*et al*, Phys. Rev. A**78**, 042307 (2008); Kastoryano M.J., Reiter F., and Sørensen A. S., Phys. Rev. Lett. **106**, 090502 (2011); Sinaysky I., Petruccione F. and Burgarth D., Phys. Rev. A 78, 062301 (2008); Pumulo N., Sinayskiy I. and Petruccione F., Phys. Lett A, V375, Issue 36, 3157-3166 (2011).

[3] Verstraete F., Wolf M.M. , and Cirac J. I., Nature Phys. 5, 633 (2009)

[4] Aharonov Y., Davidovich L. and Zagury N., Phys. Rev. A**48**, 16871690 (1993); Kempe J., Contemporary Physics, V44, 4, pp307-327 (2003).

[5] Childs A.M.: Universal Computation by Quantum Walk, Phys. Rev. Lett. **102**, 180501 (2009).

[6] Lovett N.B., Cooper S., Everitt M., Trevers M. and Kendon V.: Universal quantum computation using the discrete-time quantum walk, Phys. Rev. A**81**, 042330 (2010).

[7] Kendon V.: Decoherence in quantum walks a review, Mathematical Structures in Computer Science, V17, 6, pp1169-1220 (2007).

[8] Attal S., Petruccione F. and Sinayskiy I, Phys. Lett. A (2012, in press); Attal S. *et al*, http://hal.archives-ouvertes.fr/fr/ (2011);

Superadditivity of classical capacity revisited

Oleg Pilyavets, Evgueni Karpov and Joachim Schäfer

QuIC, Ecole Polytechnique, C.P. 165, Université Libre de Bruxelles, B-1050 Brussels, Belgium

Characterization of quantum channels capacities is one of the most important tasks in the theory of quantum communications. It attracted much interest because of possible superadditivity owing to the use of entangled states. A memoryless quantum channel is the simplest basic channel model. Its n invocations (uses) act on the total n-partite input state $\hat{\rho}_{\mathrm{in}}$ as a sequence $\Phi^{\otimes n}$ of identical maps Φ. Alternatively, these invocations can be thought of as a single multidimensional channel or n parallel identical channels acting at once. It was believed that the capacity of such channels is additive. However, in 2008 it was shown by Hastings that this hypothesis does not hold in general, *i.e.* non-correlated channels acting together may have higher capacity than they have acting separately. This superadditivity arises because the channels are allowed to share an arbitrary joint n-partite input state.

We focus on continuous variables (CV) bosonic Gaussian channels. They are highly relevant to experimental implementations. For these channels the capacity is defined under the energy restriction on the input state which can be translated into the average amount of photons nN given to n uses of the channel. Then the capacity C for a kth single use of the memoryless channel becomes a function of the number of photons N_k given to this use. In this setting another type of superadditivity maight be possible. Indeed, if $C(N)$ is not concave, then the superadditivity may arise just due to non-uniform distribution of photons between the uses. For lossy [1] and additive noise [2] bosonic Gaussian channels we have found that the capacity restricted to Gaussian encoding and modulation is concave. Therefore for these channels this superadditivity does not exist. However, if one finds a CV channel with non-concave dependence $C(N)$ its capacity will be superadditive. Note that our result on the concavity of $C(N)$ for the lossy and additive noise channels allowed us to find the capacity for both of these channels in the presence of memory by using convex separable programming [1].

The action of the channel may be equivalently represented by a unitary transformation applied to the product state of channel's input and environment. Using this fact in the context of superadditivity we make a natural step further and pose a question: what happens with the capacity of n parallel channels if their "environments" are allowed to be in a joint arbitrary n-partite state similarly to the channels inputs. Then, the average amount of photons in the environments nN_{env} plays the role similar to that of input [1]. Now the capacity becomes a function of two variables: $C(N, N_{\mathrm{env}})$, and we propose a new formulation of superadditivity problem:

Given the average numbers of photons for the channels input nN and for their environment nN_{env},
- *What is the channel capacity?*
- *What is the optimal channel input state?*
- *What is the optimal state of the channel environment?*

In this setting the problem originally formulated for n identical parallel channels is transformed to a problem for n parallel channels of the same type which may differ only by their noise (average amount of photons in their environments). Thus, the optimal environment and input will be defined by average photon number distributions between "black boxes" represeting parallel channels characterized by $C(N, N_{\mathrm{env}})$.

Interestingly, for the lossy channel we have shown that the optimal photon number distribution between channels environments may be non-uniform which can be interpreted as a "violation of mode symmetry" [1]. In addition, this solution presents superadditivity in the form we are proposing. The reason is that despite C is concave as a function of N for any fixed N_{env}, it is generally neither a concave nor a monotonic function of N_{env} for fixed values of N.

The solution of the optimal environment problem may be applied to the problem of "optimal channel memory", because some important memory channels can be *unravelled*, so that the capacity of memory channel becomes equal to the capacity of parallel independent channels with the non-uniform distribution of photons between the environments. The optimality of non-uniform distribution is translated to superiority of the capacity of memory channel over the memoryless one under the same energy constraints for both input and environment. Note that this result straightforwardly follows from the results of paper [3] though remained unnoticed by its authors. Since information transmission rates may also be non-monotonous functions of N_{env}, the problem of optimal channel memory can be posed for them as well [1].

We have shown that the non-uniform distribution is not always optimal and the transition between the "uniform" and "non-uniform" optimal solutions is governed by so-called "critical" and "supercritical" parameters introduced for both lossy [1] and additive noise [2] channels. For our astonishment despite the complexity of the optimization problem some of these parameters are fundamental channel constants which we were able to compute analytically and they are expressed by simple relations in radicals, e.g.

$$N = \left[\sqrt{3/2 + 5/(2\sqrt{3})} - 1 \right]/2 \qquad (1)$$

or the values $1 - 1/\sqrt{3}$ and $2/e$ for a channel transmissivity. We expect that these constants can also be used to characterize the boundaries between the additive and superadditive cases.

References

[1] O. V. Pilyavets, C. Lupo and S. Mancini, arXiv:0907.1532v3 (2011). To appear in IEEE Tran. Inf. Theor. **58**:12 (2012).

[2] J. Schäfer, E. Karpov and N. J. Cerf, Proc. of SPIE **7727** (Bellingham, WA), 77270J (2010); J. Schäfer, E. Karpov and N. J. Cerf, Phys. Rev. A **84**, 032318 (2011).

[3] N. J. Cerf, J. Clavareau, J. Roland and P. Macchiavello, Int. J. Quant. Inf. **4**, 439 (2006).

Moments of nonclassicality quasiprobabilities

__Saleh Rahimi-Keshari__[1], **Thomas Kiesel**[2], and **Werner Vogel**[2]

[1]*Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, St Lucia, Queensland 4072, Australia*
[2]*Arbeitsgruppe Quantenoptik, Institut für Physik, Universität Rostock, D-18051 Rostock, Germany*

A clear characterization and interpretation of quantum phenomena, including the quantum interference effects, play a central role for beating the technical limitations known in classical physics. In the field of quantum optics, the characterization of quantum effects of light was based on the Glauber-Sudarshan P representation of the density operator [1, 2]. If the P function fails to be interpreted as a probability density the quantum state is said to be nonclassical. Nonclassicality of this type is indispensable for the occurrence of quantum interferences, which play the key role for most of the presently considered applications of quantum physics, in particular in the field of quantum information processing. However, as for many quantum states the P function is a highly singular function, nonclassicality of quantum states cannot be directly verified by measuring the P function.

In this poster, we introduce a method for verification of nonclassicality in terms of moments of nonclassicality quasiprobability distributions [3], which are readily available from experimental data. The nonclassicality quasiprobability distribution (NQP) is a regularized version of the Glauber-Sudarshan P function that is obtained by the filtering procedure

$$P_\Omega(\alpha, \alpha^*) = \frac{1}{\pi^2} \int d^2\xi \Phi(\xi, \xi^*) \Omega_w(\xi, \xi^*) e^{\alpha\xi^* - \xi\alpha^*}, \quad (1)$$

where $\Phi(\xi, \xi^*)$ is the characteristic function of the P function, the filter function $\Omega_w(\xi, \xi^*)$ has to satisfy certain conditions, and the real parameter w controls the width of the filter so that $\lim_{w\to\infty} \Omega_w(\xi, \xi^*) = 1$ [4]. The NQP of a nonclassical state takes on negative values for sufficiently large values of w, and their moments are referred to as *nonclassicality moments*. The advantage of using NQP is that it is a regular function that can be directly sampled by balanced homodyne detection [5]. However, for some nonclassical states a large value of w is required to observe the negativity of NQP such that the inherent statistical uncertainties due to experimental measurement may hide all nonclassical effects.

In this presentation, we derive a relation between the normally-ordered moments and the nonclassicality moments. This relation enables us to verify nonclassicality by using well established criteria based on normally-ordered moments [6], which are obtained from the nonclassicality moments for a given value of the width w, and eliminates the need for seeking negativity in the NQP. This is equivalent to calculating the moments for infinite w, but does not require the reconstruction of the corresponding quasiprobability.

Alternatively, we show that nonclassicality criteria can be directly formulated in terms of nonclassicality moments. To illustrate this method, we consider sub-Poissonian photon statistics and squeezing. We show that for sufficiently large
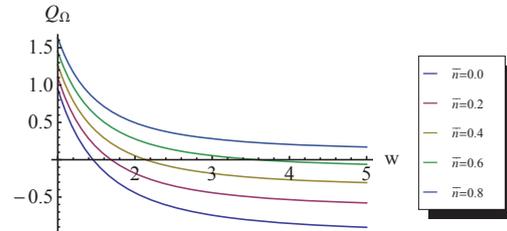
Figure 1: Dependence of the Mandel-Q-parameter [7] in terms of the nonclassicality moments Q_Ω on the filter width, for single-photon added thermal state with different mean thermal photon numbers $\bar{n}$. For $\bar{n} < \sqrt{2}/2$ and sufficiently large values of w the parameter Q_Ω becomes negative; this is an indication of nonclassicality.

values of w the Mandel-Q-parameter and the quadrature variance in terms of the nonclassicality moments exhibit the corresponding nonclassical effects, e.g. see Fig. 1.

An interesting feature of the derived relation is that in the limiting case of large values of the width parameter w the nonclassicality moments converge to normally-ordered ones. We show that the difference between nonclassicality moments and normally-ordered moments scales inversely with the square of w. Hence for sufficiently large values of w, the normally-ordered moments can be approximated with arbitrary degree of accuracy by nonclassicality moments.

Moreover, our theory yields expectation values of any observable in terms of the nonclassicality moments. Therefore, the knowledge of these moments enables one to obtain well-known physical quantities.

References

[1] E. C. G. Sudarshan, Phys. Rev. Lett. **10**, 277 (1963).

[2] R. J. Glauber, Phys. Rev. **131**, 2766 (1963).

[3] S. Rahimi-Keshari, T. Kiesel, and W. Vogel, arXiv:1201.0861v1 [quant-ph].

[4] T. Kiesel and W. Vogel, Phys. Rev. A **82**, 032107 (2010).

[5] T. Kiesel, W. Vogel, B. Hage, and R. Schnabel, Phys. Rev. Lett **107**, 113604 (2011).

[6] E. Shchukin, T. Richter, and W. Vogel, Phys. Rev. A **71**, 011802 (2005).

[7] L. Mandel, Opt. Lett. **4**, 205 (1979).

Applications of Noiseless Linear Amplification

T.C.Ralph, A.P.Lund and N.Walk

Centre for Quantum Computation and Communication Technology,
School of Mathematics and Physics, University of Queensland, Brisbane, Australia

Recently there has been considerable interest in the concept of noiseless linear amplifiers [1]. These are probabilistic, but heralded devices which, if acted on a coherent state of amplitude α, perform the transformation $|\alpha\rangle \rightarrow |g\alpha\rangle$ when successful. More generally, when acted on arbitrary states, they change the amplitude weighting of the number state components of the state according to $|n\rangle \rightarrow g^n|n\rangle$ [1, 2]. The probability of success, P, is bounded by $P < 1/g^2$. Currently, techniques for saturating this bound are only known for small amplitude input distributions.

Noiseless linear amplifiers have been demonstrated experimentally via several different approaches [3, 4, 5, 6] employing linear optics and photon counting. Applications including distillation of entanglement [3], qubit purification [7], phase metrology [5] and continuous variable error correction [8] have been identified. Never-the-less much still remains to be understood about the consequences of noiseless amplification on arbitrary states and how it can be combined with other operations to produce new protocols. In this paper we will explore these questions and discuss new applications of noiseless linear amplifiers and improvements to existing protocols. Some examples follow.

Signal to Noise Preserving Amplifier: Deterministic linear amplification must add noise in such a way that signal to noise in a coherent state communication protocol will be reduced. Probabilistic noiseless amplification can *increase* signal to noise in such a scenario. However for some communication protocols it might be sufficient to simply maintain signal to noise in the amplification process. Such amplification must still be probabilistic, but would have a higher probability of success. We show how a signal to noise preserving linear amplifier can be constructed from a combination of noiseless amplification and deterministic linear amplification and describe its properties (see Figure 1).

Virtual Noiseless Amplification: We show that for certain types of Gaussian post-selection the virtual channel corresponding to the post-selected data consists of the actual quantum channel followed by noiseless linear amplification and then the addition of some thermal noise. The probability of post-selecting the data corresponds to the probability of success of the virtual noiseless amplifier. Although this technique cannot be used to herald an amplified quantum state, it can be used to determine the security of post-selected data obtained over a quantum channel with an eavesdropper and hence is directly applicable to protocols such as quantum key distribution. As well as providing a tool for analysing security, the virtual channel gives a clear intuition about how post-selection can improve channel characteristics that might be applied to other protocols.

Distillation of Thermalised Entanglement: It has previously been shown that noiseless amplification can distill and purify entanglement that has been subjected to a lossy chan-

nel [3]. However, in these cases the reservoir coupled to by the loss was at zero temperature. An experimentally relevant, but more difficult case is when the loss couples to a non-zero temperature bath and thus is accompanied by an injection of thermal noise - leading to some thermalisation of the distributed entanglement. Here we show that distillation and purification of entanglement is still possible via noiseless amplification for such situations and describe the conditions and strategies for which improved entanglement may be obtained. These results allow for the possibility of error correction of continuous variable states against arbitrary Gaussian noise.
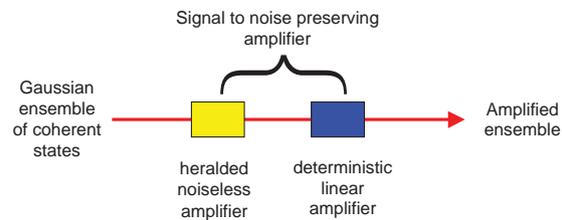
Figure 1: *Protocol for producing heralded signal to noise preserving amplification of a Gaussian state ensemble. If the required intensity amplification is $G = G_n G_l$, where G_n is the gain of the noiseless amplifier and G_l is the gain of the linear amplifier, then the gain of the noiseless amplifier must be chosen to be $G_n = 2\,G/(1 + G)$. Given this condition the amplified ensemble will have the same signal to noise as the original ensemble. Notice that the gain of the noiseless amplifier never exceeds 2, even for $G \gg 1$, thus good probabilities of success can be achieved even for high total gains.*

References

[1] T.C.Ralph and A.P.Lund, in Proceedings of 9th International Conference on Quantum Communication Measurement and Computing (ed. Lvovsky, A.) 155 (AIP, 2009).

[2] J.Fiurasek, Phys. Rev. A **80**. 053822 (2009).

[3] G.Y.Xiang et al., Nature Photonics **4**, 316 (2010).

[4] F.Ferreyrol, et al, Phys. Rev. Lett. **104**, 123603 (2010).

[5] M.A. Usuga et al., Nature Physics **6**, 767 (2010).

[6] A. Zavatta, et al, Nature Photonics **5**, 52 (2011).

[7] N. Gisin, et al, Phys. Rev. Lett. **105**, 070501 (2010).

[8] T.C.Ralph, Phys. Rev. A **84**, 022339 (2011).

Gaussian matrix-product states for coding in bosonic memory channels

Joachim Schäfer, Evgueni Karpov and Nicolas J. Cerf

QuIC, Ecole Polytechnique de Bruxelles, CP 165/59, Université Libre de Bruxelles, B-1050 Brussels, Belgium

A central problem of information theory is to derive the capacity of communication channels, which is the maximal information transmission rate. Here we focus on the classical capacity of quantum channels.

In the last years, a particular interest has been devoted to Gaussian bosonic channels as they model common physical links such as the optical information transmission via free space or optical fibers. Moreover, Gaussian bosonic channels with *memory*, where the noise over subsequent uses is correlated, has recently attracted much interest.

Quantum-water filling: We have studied the classical capacity and optimal encoding for the bosonic Gaussian channel with additive correlated noise, when restricted to Gaussian encodings [1, 2]. For noise model that we investigated we exploited the fact that the capacity and the input energy constraint are invariant under basis rotations which *unravels* the noise correlations. In this new basis, the unraveled channel system is a collection of n uncorrelated single mode Gaussian channels which in general act differently on the individual input states. For this system, we discovered an optimal encoding which is given by a *quantum water-filling*. This solution goes beyond the water-filling solution in classical information theory, because the n optimal modulated output variances (which are now all equalized) are sums of the variances of the modulation, the noise and the individual quantum input states. As the optimal input states may be squeezed states, the additional energy cost for the creation of the states has to be taken into account. We derived an input energy threshold, above which the quantum water-filling solution holds and we restrict here our study to energies above this threshold. We found that when the optimal input state is rotated back to the original, correlated basis it may be entangled.

Can we implement the optimal input state? As an example, we have studied a noise model that is given by a Markov process and determined the optimal entangled multi-mode input [1, 2]. Similar results were obtained in [3] for the lossy channel with a non-Markovian correlated noise. However, for both noise models and channels, it is unknown how to generate experimentally the optimal input state. This could in principle be a very challenging task. Nevertheless, one may use a non-optimal input state with a known implementation, as an approximation to the optimal state.

Gaussian matrix-product states are close-to-optimal: This motivates the study of so-called Gaussian matrix-product states (GMPS) [4, 5] as input states which have a known optical implementation. In particular, we determine the parameters of the GMPS that achieves the highest transmission rate and that can be generated by the optical scheme introduced in [5]. This state can be created sequentially although it remains heavily entangled for an arbitrary number of modes. We show that the best GMPS can achieve more than 99.9% of the capacity of the additive noise channel

and lossy channel for both, a Markovian and non-Markovian noise, in a wide range of noise parameters [6]. Furthermore, we point out that the squeezing strengths that are required to generate this state are achievable within present technology [7].

Link to many-body physics? Finally, we introduce a new noise class for which the GMPS is the exact optimal input state. Interestingly, GMPS are known to be ground states of particular quadratic Hamiltonians in harmonic lattices. We present an example of a noisy channel where the GMPS is at the same time the optimal input state and the ground state of a bosonic n-partite system. We believe this could serve as a starting point to find useful connections between quantum information theory and quantum statistical physics.

References

[1] J. Schäfer, D. Daems, E. Karpov and N. J. Cerf, Phys. Rev. A **80**, 062313 (2009).

[2] J. Schäfer, E. Karpov and N. J. Cerf, Phys. Rev. A **84**, 032318 (2011).

[3] O. V. Pilyavets, C. Lupo and S. Mancini, e-print arXiv:0907.1532v3 [quant-ph] (to appear in IEEE Trans. Inf. Th.)

[4] N. Schuch and J. I. Cirac and M. M. Wolf, *Proc. of Quantum Information and Many Body Quantum Systems*, edited by M. Ericsson and S. Montangero, Vol. 5, (Eidizioni della Normale, Pisa, 2008) pp. 129-142; e-print arXiv:quant-ph/0509166v2

[5] G. Adesso and M. Ericsson, Phys. Rev. A **74**, 030305(R) (2006).

[6] J. Schäfer, E. Karpov and N. J. Cerf, Phys. Rev. A **85**, 012322 (2012).

[7] H. Vahlbruch *et. al.*, Phys. Rev. Lett **100**, 033602 (2008); M. Mehmet *et. al.*, arXiv:1110.3737v1 [quant-ph] (2011).

Decomposing continuous-variable logic gates

Seckin Sefi[1,2] and Peter van Loock[1,2]

[1]*Optical Quantum Information Theory Group, Max Planck Institute for the Science of Light, Günther-Scharowsky-Str.1/Bau 26, 91058 Erlangen, Germany*
[2]*Institute of Theoretical Physics I, Universität Erlangen-Nürnberg, Staudstr.7/B2, 91058 Erlangen, Germany*

Since the proposal of quantum computation as a generalization of computer science, an important theoretical field has been decomposing logic gates into elementary gate sets. In contrast to discrete-variable theory, there is not an established method to decompose an arbitrary operator in the continuous-variable (CV) regime except a proof-of-principle result on universal gate sets in Ref. [1].

In our recent work [2], we presented a general, systematic, and efficient method for decomposing any given exponential operator into a universal and finite gate set. Thus, we can describe an arbitrary multi-mode Hamiltonian evolution in terms of a set of experimentally realizable operations.

Although our approach is mainly oriented towards CV quantum computation, it may be used more generally whenever quantum states are to be transformed deterministically, e.g. in quantum control, discrete-variable quantum computation, or Hamiltonian simulation.

In our setting, there are two important criteria for CV gate decompositions: how systematic and how efficient the decompositions are. We derive methods according to these criteria and present a systematic and efficient framework for decomposing any given unitary operator that acts on bosonic modes into a universal set of elementary CV gates. Our general method consists of first expressing operators in terms of linear combinations of commutation operators and then realizing each commutation operator and their combinations through approximations. We discuss the efficiency of the decompositions and present guidelines to obtain an arbitrary order of error. For this purpose, we employ a powerful technique for obtaining efficient approximations.

In our work we used the following gate set:

$$\{e^{i\frac{\pi}{2}(X^2+P^2)}, e^{it_1 X}, e^{it_2 X^2}, e^{it_3 X^3}\}. \tag{1}$$

Thus, we decompose an arbitrary operator in terms of the gate set above. This gate set includes three Gaussian operations and a single non-Gaussian, third order operator (here, order is defined as the polynomial order of the mode operators in the Hamiltonian of a given operator). However, it is possible to use any other universal gate set as well.

We illustrate our scheme by presenting decompositions for various nonlinear Hamiltonians including fourth order Kerr interactions. For example, in the figure below you see position wave functions of two states: in the top figure, a fourth order interaction is applied to a coherent state, in the middle figure, same state is under evolution of the operators from the gate set above, hence, the fourth order interaction is simulated up to a negligible error [3]. The third figure is showing the absolute value of the differences between two functions.

As another possible application, we also aim to derive a deterministic recipe for an arbitrary state transformation in finite dimensional space, i.e, in a space spanned by finite num-
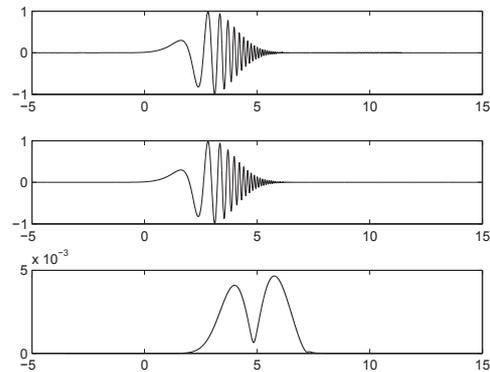
Figure 1: Decomposition of a fourth order gate.

ber of Fock eigenstates [4]. In order to do so, we present a set of Hamiltonians which correspond to a discrete variable universal logic set on the Fock space. Than, using continuous variable gate decomposition theory, we decompose these Hamiltonians to an experimentally accessible gate set, thus, providing a scheme for deterministic Fock state processing.

Different from previous proof-of principle demonstrations, our treatment brings the abstract notions of decomposition theory for CV quantum computation close to experimental implementations. Highly nonlinear quantum gates may then be realized in a deterministic fashion by concatenating hundreds of quadratic and cubic gates. We discuss two potential experiments utilizing offline-prepared optical cubic states and homodyne detections, in which quantum information is processed optically or in an atomic memory using quadratic light-atom interactions [2]. Hence, the complication of realizing nonlinear gates is shifted offline into the preparation of the cubic ancillae.

References

[1] S. Lloyd and S.L. Braunstein, Quantum Computation over Continuous Variables, Phys.Rev.Lett., **82**, 1784 (2011).

[2] S. Sefi and P. van Loock, How to decompose arbitrary continuous-variable quantum operations, Phys.Rev.Lett., **107**, 170501 (2011).

[3] S. Sefi, V. Vaibhav and P. van Loock, Implementing nonlinear continuous variable gates, in preparation.

[4] S. Sefi and P. van Loock, Deterministic Fock state processing, in preparation.

Entanglement dynamics in the presence of unital noisy channels

Assaf Shaham, Assaf Halevy, Liat Dovrat, Eli Megidish and Hagai S. Eisenberg

The Hebrew University of Jerusalem, Jerusalem, Israel

Quantum entanglement is a key resource for many quantum information techniques. Decoherence - the coupling of a quantum system to other surrounding systems results in quantum noise which reduces the degree of entanglement that the subsystems share. Thus, decoherence is a major obstacle which encumbers the realization of many quantum information applications. In this work we study the entanglement dynamics of a pair of qubits that are transmitted through uncorrelated unital noisy channels. The Bloch sphere representation of the noise and the entanglement level are shown to be related in a simple relation, which is verified experimentally using an all-optical setup.

Consider a quantum channel that acts on a single-qubit state $\hat{\rho}$. The operation of the channel can be uniquely described using the elements of the process matrix χ: $\mathcal{E}(\hat{\rho}) = \sum_{m,n} \chi_{mn} \hat{E}_m \hat{\rho} \hat{E}_n^\dagger$ where $\hat{E}_m$ are the Kraus operators. Alternatively it can be represented as the mapping of the Bloch sphere surface into a smaller contained ellipsoid. If the channel is unital (i.e. $\mathcal{E}(\hat{I}) = \hat{I}$), the sphere surface and the mapped ellipsoid are concentric. A general loss of information in a channel does not depend on the channel rotations. Therefore, for unital channels, the primary axis lengths of the mapped ellipsoid $\{R_1, R_2, R_3\}$ are sufficient to characterize the channel decoherence properties. These values can be easily calculated from the eigenvalues of the χ matrix.

The entanglement of a qubit pair is commonly quantified using the concurrence measure [1]: $C(\hat{\rho}) = \max\{0, Q(\hat{\rho})\}$; $0 < C(\hat{\rho}) < 1$, where Q is a nonlinear function of $\hat{\rho}$, which does not depend on local rotations. If a maximally entangled state with $C = 1$ is subjected to a known process, the value of its concurrence can be expressed using the elements of the corresponding process matrix. Consider the case when the channel is unital. The concurrence can be written then using the channel R_i values. Given this channel had operated on one qubit of the pair, the Q value would be $(|R_1|+|R_2|+|R_3|-1)/2$. If both qubits experience the same process, the Q value is calculated to be $(R_1^2+R_2^2+R_3^2-1)/2$. Thus, a dephasing channel that always has $R_1 = 1$ can't break entanglement.

We implemented a photonic unital quantum channel with controlled noise properties, and demonstrated the above-mentioned relation for the cases of one-side and two-side local channel. The quantum channel was composed of two equal length and perpendicularly fixed birefringent crystals. Its operation was previously characterized in [2]. Control over the decoherence amount is achieved with the rotation of a half-wave plate which is placed in between these crystals. Quantum process tomography of the channel has shown that the channel is unital, and that $\{R_1 = 2R_2 - 1, R_2 = R_3\}$ [2]. Photon-pairs where generated by collinear spontaneous parametric down conversion. A pulsed 390 nm laser pumped two perpendicularly oriented type-I BBO crystals and generated the state $|\psi\rangle = 1/\sqrt{2}(|hh\rangle + e^{i\varphi}|vv\rangle)$. The φ angle could
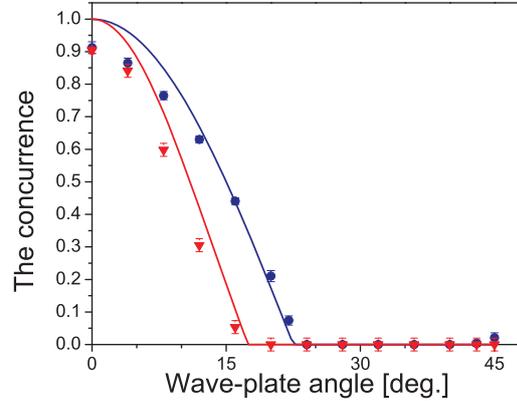
Figure 1: Experimental results of the entanglement dynamics when the channel is applied on a single qubit (blue circles) and on two qubits (red triangles). Lines represent the theoretical predictions.

be changed by tilting another compensating crystal that was placed after the generating crystals. With the addition of more wave-plates, this state can be rotated to any other symmetric maximally entangled state. Before entering the quantum channel, the state was filtered spatially and temporally using a single-mode fiber, and 3 nm interference bandpass filters. In the state characterization unit, photons were split probabilistically by a beam splitter (BS), and their post-selected two-port polarization state was measured by a two-qubit quantum state tomography procedure. In order to implement a two-qubit local noise, the quantum channel was placed before the BS, whereas to implement a one-side noisy channel the channel was moved behind one of the BS output ports.

We tested the one- and the two-qubit channels on the maximally entangled states of $|\psi_1\rangle = 1/\sqrt{2}(|hh\rangle - |vv\rangle)$ and $|\psi_2\rangle = 1/\sqrt{3}(|hh\rangle - |vv\rangle) - 1/\sqrt{6}(|hv\rangle + |vh\rangle)$, respectively. The initial concurrence of both of the states was better than 90%. It was measured when the channel was tuned not to induce noise. Experimental results for the output concurrence as a function of the channel wave-plate are shown in Fig. 1. As predicted, the concurrence of the two-side channel vanishes before the one-side concurrence does. All the results agree well with the theoretical calculation of the concurrence.

In this work we studied the cases where the channels were unital, and that the noise was the same when applied to both sides. Generalizing these results to different types of noise is currently under investigation.

References

[1] W. K. Wootters, Phys. Rev. Lett. **80**, 2245, (1998).

[2] A. Shaham and H. S. Eisenberg, Phys. Rev. A **83**, 022303 (2011).

Microscopic derivation of Open Quantum Walks

Ilya Sinayskiy[1] and Francesco Petruccione[1]

[1]*NITheP and School of Chemistry and Physics, University of KwaZulu-Natal, Durban, South Africa*

It is well-known that the concept of classical random walks has found wide applications in physics, computer science, economics and biology. The trajectory of a classical random walk consists of a sequence of random steps on some underlying set of connected nodes [1]. Due to its success in the classical case, the concept of random walk has been extended to the quantum domain. Quantum walks can be introduced in a discrete time [2] and in a continuous time [3] way. The principal difference between quantum and classical random walks is, that in the classical random walk case the probability of transition is defined only by the transfer matrix, while in the quantum walk case the probability of transition strongly depends on the state of an internal degree of freedom of the walker.

Quantum walks are widely used as a tool for the formulation of algorithms for quantum computing. Although, practical implementation of any quantum coherent process is typically difficult due to the unavoidable dissipation and decoherence effects [4], experimental realizations of quantum random walks have been reported. Implementations with negligible effect of decoherence and dissipation were realized in optical lattices [5], on photons in waveguide lattices [6], with trapped ions [7] and free single photons in space [8].

During the last few years attempts were made to take into account the destructive influence of decoherence and dissipation in the description of quantum walks [9]. However, in these approaches decoherence is treated as an extra modification of the Hadamard quantum walk scheme, the effect of which needs to be minimized and eliminated.

Recently, a formalism for discrete time open quantum walks was introduced [10]. This formalism is exclusively based on the non-unitary dynamics induced by the environment. This approach is similar to the formalism of quantum Markov chains [11] and rests upon the implementation of appropriate completely positive maps [4, 12]. Open quantum walks include the classical random walk and through a realization procedure a connection to the Hadamard quantum walk is established. Furthermore, the open quantum walks allow for an unravelling in terms of quantum trajectories. It was shown [10] that open quantum walks can perform universal quantum computation and can be used for quantum state engineering. Here, a microscopic derivation of open quantum walks will be presented. Possible experimental realization will be discussed as well.

References

[1] M. Barber and B.W. Ninham, Random and Restricted Walks: Theory and Applications, Gordon and Breach, New York, (1970).

[2] Y. Aharonov, L. Davidovich, and N. Zagury, Phys. Rev. A **48**, 1687 (1993).

[3] E. Farhi and S. Gutmann, Phys. Rev. A **58**, 915 (1998)

[4] H.-P. Breuer, F. Petruccione, The Theory of Open Quantum Systems, Oxford University Press (2002).

[5] M. Karski *et al.*, Science **325**, 174 (2009).

[6] H. B. Perets *et al.*, Phys. Rev. Lett. **100**, 170506 (2008).

[7] H. Schmitz *et al.*, Phys. Rev. Lett. **103**, 090504 (2009); F. Zähringer *et al.*, Phys. Rev. Lett. **104**, 100503 (2010).

[8] M. A. Broome *et al.*, Phys. Rev. Lett. 104, 153602 (2010).

[9] V. Kendon, Math. Struct. Comput. Sci. **17**, 1169 (2007); T. A. Brun, H. A. Carteret, and A. Ambainis, Phys. Rev. Lett. **91**, 130602 (2003); A. Romanelli, R. Siri, G. Abal, A. Auyuanet, and R. Donangelo, Physica A **347**, 137 (2005); P. Love and B. Boghosian, Quant. Info. Proc. **4**, 335 (2005); R. Srikanth, S. Banerjee, C.M. Chandrashekar, Phys. Rev. A **81**, 062123 (2010).

[10] Attal S., Petruccione F. and Sinayskiy I, Phys. Lett. A (2012, in press); Attal S. *et al*, http://hal.archives-ouvertes.fr/hal-00581553/fr/ (2011).

[11] S. Gudder, Found. Phys. **40** Numbers 9-10, 1566, (2010); S. Gudder, J Math. Phys., **49** 072105, (2008).

[12] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer Verlag 1983).

Remote resource preparation

Cornelia Spee[1], **Julio de Vicente** [1] **and Barbara Kraus**[1]

[1]*Institute for Theoretical Physics, University of Innsbruck, Innsbruck, Austria*

Remote resource preparation is a multipartite quantum communication scheme, in which one party (A) wants to provide some other parties (B_i's) with arbitrary multipartite entanglement. These parties can be spatially seperated. The preparation should be done without actually sending the state. Since local operations can be done by the B_i's themselves, it is sufficient to provide the entanglement, i.e. prepare the states up to local unitaries.

This can be achieved by A and all B_i's (B) sharing a certain entangled state. By performing local measurement A can decide on the entanglement B gets. In order to identify these states we made use of a way to deterministically implement arbitrary gates. We computed these states for the three- and four-qubit case explicitly. Given a Standardform for n-qubit states up to local unitaries this approach can be easily generalized.

We show that (2n-1)/n classical bits per qubit suffice to accomplish this task, which is less than is required in previously known oblivious state preparation [1].

Furthermore we consider the resource preperation of a certain class of states, namely the locally maximally entanglable states (LMESs) [2]. This restriction allows us to also transmit classical information provided the quantum state is known to B.

Our protocol has the feature that A does not only have the control over the entanglement she transmits. Via restricting the classical information about the correction operations A has also some control over the way the B_i's can use the resource.

References

[1] D. W. Leung and P. W. Shor, Phys. Rev. Lett., **90**, 127905 (2003).

[2] C. Kruszynska and B. Kraus, Phys. Rev. A, **79**, 052304 (2009).

Modeling single photon production in RASE

__Robin Stevenson__[1], Sarah Beavan[1], Morgan Hedges[1], Andre Carvalho[1], Matt Sellars[1] and Joseph Hope[1]

[1]*Research School of Physics and Engineering, The Australian National University, Canberra, Australia*

Rephased Amplified Spontaneous Emission (RASE) is a process that can address two issues in implementing quantum communications. The first issue is the difficulty in generating pure single-photon states, which are required for many quantum encryption or key distribution protocols. The second issue is that the range of transmission of photonic quantum states is primarily limited by loss in optical fibres, and classical amplification repeaters do not work with quantum states. RASE can be a solution to these issues, either being a single photon source, or, in a modified protocol, it can be used to establish entanglement between two remote states as part of a "quantum repeater" to extend the range of quantum communications. Here I focus on using RASE to produce single photon states.

The process of RASE involves first detecting and then rephasing a spontaneously emitted photon (or collection of photons) emitted from an ensemble of atoms. The ensemble is first prepared in the ground state, and then fully transferred to the excited state using a π pulse. The atomic ensemble then spontaneously emits, and depending on the optical thickness of the sample, these emitted photons can be amplified. Photons emitted in a specific mode are collected and then detected using a photodetector. After some time, another π pulse is applied to the ensemble, which reverses the excitations of the atomic sample, putting all ions that were in ground state into the excited state, and vice versa. The collective atomic excitations caused by the spontaneous emissions, and subsequent π pulse flip, then rephase, and with high probability emit into the same mode, with a time symmetry around the second π pulse.

Figure 1: An illustration of the output you would expect of the RASE protocol on a photon detector if you had a 100% efficient detector

With a perfectly efficient photodetector, amplified spontaneous emission with 2 or more photons could be detected and then be rephased to create many-photon Fock states. However, with the current experimental realisation, the photodetector has an efficiency that is far from 100%, and it is impossible to distinguish between a 1-photon state or a 2-photon state where one of the photons has been missed by the detector. The focus of this work is, therefore, to model the (spontaneous) emission of single photon states and their subsequent rephasing, and to calculate the probability of a multiple photon emission. We can then adjust the parameters of the system to ensure the maximum possible amount of single photon emissions, while minimising the number of multiple photon events. The modeling of this protocol is done without coherent-state approximations: when the initial spontaneous emission is detected by the photodetector, the atomic ensemble is projected into a distributed Fock-like state, and any rephased photons will also be in a Fock state, and thus the coherent-state approximation breaks down.

References

[1] P. Ledingham, W. Naylor, J. Longdell, S. Beavan and M. Sellars, Nonclassical photon streams using rephased amplified spontaneous emission, PRA, __81__, 012301 (2010)

[2] P, Ledingham, Optical rephasing techniques with rare earth ion dopants for applications in quantum information science, PhD Thesis, University of Otago, June 2011

[3] S. Beavan, Photon-echo rephasing of spontaneous emission from and ensemble or rare-earth ions, PhD thesis, The Australian National University, January 2012

Thresholds of surface codes on the general lattice structures suffering biased error and loss

Keisuke Fujii[1], <u>Yuuki Tokunaga</u>[2][3]

[1]*Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2]*NTT Secure Platform Laboratories, NTT Corporation, 3-9-11 Midori-cho, Musashino, Tokyo 180-8585, Japan*
[3]*Japan Science and Technology Agency, CREST, 5 Sanban-cho, Chiyoda-ku, Tokyo 102-0075, Japan*

Recently, topological order has attracted much interest in both condensed matter physics and quantum information science [1, 2]. The ground state degeneracy of topologically ordered phase cannot be distinguished by local operations and hence robust against local perturbations. By encoding quantum information into such topologically degenerate subspaces, so-called topological quantum error correction (QEC) codes [2, 3], logical information can be protected from decoherence by repeated quantum error correction. There have been two types of the topological QEC codes, so-called surface codes [2] and color codes [3], both of which are the CSS (Calderbank-Shor-Steane) codes [4]. In both cases, the threshold values under perfect syndrome measurements have been calculated to be $\sim 11\%$ [5, 6], which is close to the quantum Gilbert-Varshamov bound [4] in the limit of zero asymptotic rate with symmetric X and Z errors. In the case of the color codes, their performances have been compared among different lattice geometries, and their thresholds result in similar values $\sim 11\%$ [6, 7]. This result is reasonable by considering the fact that the color codes are self-dual CSS codes, that is, they are symmetric under a Hadamard transformation. The surface codes, on the other hand, are not self-dual CSS codes, and hence it is possible to break the symmetry between properties of X and Z error-corrections. The surface code, however, has been intensively investigated so far only on the square lattice, which is a self-dual lattice, and therefore its error-correction properties are symmetric.

In this work, we investigate the surface codes with general lattice geometries [8]. Their constructions and error-correction procedures are basically the same as those of the original surface code. Since the stabilizer operators are not always symmetric under the duality transformation of the lattice (i.e. exchange of the vertexes and faces with each other), the error-tolerances of the surface codes with general lattice geometries are not always symmetric between X and Z errors. Interestingly, we find that such asymmetry in the error-tolerance is related to the connectivity of the lattice which defines the surface; *error chains on a lattice of lower connectivity can be corrected easily*. Intuitively, this can be understood that finding appropriate pairs of incorrect error syndromes, which are the boundaries of the error chains, on the lattice of lower connectivity is easier, since the incorrect error syndromes are more isolated and less percolative. From the above observation and our numerical simulations for various lattice geometries such as the Kagome, hexagonal and $(3, 12^2)$, we find that the threshold values for independent X and Z errors exhibit a universal behavior; they, independent of the lattice geometries, approach the quantum Gilbert-Varshamov bound [4] in the limit of zero asymptotic rate with asymmetric X and Z errors. In this sense, the family of the surface codes can be said to be efficient. We also provide a recursive way to construct highly asymmetric surface codes on fractal-like lattices. In many experimental situations, dephasing is a dominant source of errors [9], and therefore the present family of asymmetric surface codes will help us to correct such biased noise efficiently.

We also perform numerical simulations on which the system suffers both loss errors and computational errors, and obtain threshold curves $(p^{\mathrm{loss}}, p^{\mathrm{th}})$ for various lattice geometries. The loss-tolerant scheme is based on a bond percolation phenomenon, where a reliable logical operator can be reconstructed even on the lossy surface as long as the survival probability of the qubits is higher than the bond percolation threshold [10]. Thus *the logical information on a lattice of higher connectivity is robust against qubit loss*. As a result, we come upon a fundamental trade-off between error- and loss-tolerances of the surface codes depending on the connectivity of the underlying lattices; the logical information on a lattice of higher connectivity is robust against qubit loss, but the error chains on such a lattice are difficult to correct (and vice versa). It is interesting to note that such a trade-off between error- and loss-tolerances has been also discussed in a far different situation [11].

References

[1] C. Nayak, S. H. Simon, A. Stern, M. Freedman, S. Das Sarma, Rev. Mod. Phys. **80**, 1083 (2008).

[2] A. Yu. Kitaev, Ann. Phys. **303**, 2 (2003).

[3] H. Bombin and M. A. Martin-Delgado, Phys. Rev. Lett. **97**, 180501 (2006); *ibid.* **98**, 160502 (2007).

[4] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996); A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[5] E. Dennis, A. Yu. Kitaev, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).

[6] H. G. Katzgraber, H. Bombin, and M. A. Martin-Delgado, Phys. Rev. Lett. **103**, 090501 (2009).

[7] M. Ohzeki, Phys. Rev. E **80**, 011141 (2009).

[8] K. Fujii and Y. Tokunaga, arXiv:1202.2743.

[9] P. Aliferis *et al.*, New J. Phys. **11**, 013061 (2009).

[10] T. M. Stace, S. D. Barrett, and A. C. Doherty, Phys. Rev. Lett. **102**, 200501 (2009); T. M. Stace and S. D. Barrett, Phys. Rev. A **81**, 022317 (2010).

[11] P. P. Rohde, T. C. Ralph, and W. J. Munro, Phys. Rev. A **75**, 010302(R) (2007).

A class of group covariant signal sets and its necessary and sufficient condition

Tsuyoshi Sasaki Usuda[1], **Yoshihiro Ishikawa**[1] **and Keisuke Shiromoto**[2]

[1]*Aichi Prefectural University, Ibaragabasama, Nagakute, Aichi, Japan*
[2]*Kumamoto University, Kurokami, Kumamoto, Japan*

In quantum information theory, to study signals that have symmetry is important in both fundamentals and applications (e.g. [1, 2]). Group covariant signals defined by Davies [3] are typical symmetric signals. If signals are group covariant, we can use fruitful results in quantum information theory [1, 2, 3, 4]. However, for a given signal set, it is not easy to find whether it is group covariant or not. In [5], a definition of narrow sense group covariant was proposed for a set of pure-state signals and a necessary and sufficient condition was shown. And many important quantum signals (e.g. M-ary PPM signals, M-ary CPPM signals, coded PSK coherent-state signals by any linear code over $\mathbb{Z}_m$) have been shown to be group covariant by using the condition. However, some group covariant signal sets (e.g. a SIC set [1]) are not narrow sense covariant, so that any generalization of the definition is desired.

In this paper, we define $(G, \hat{\chi})$-covariant, which is a generalization of narrow sense group covariant. Then a necessary and sufficient condition for $(G, \hat{\chi})$-covariant signals is shown.

Definition 1 *Let $(G; \circ)$ be a finite group and be a set of parameters characterizing pure quantum state signals $\{|\psi_i\rangle | i \in G\}$. The set of signals is called $(G, \hat{\chi})$-covariant if there exist unitary or anti-unitary operators $V_k (k \in G)$ such that*

$$V_k|\psi_i\rangle = \hat{\chi}(k, i)|\psi_{k \circ i}\rangle, \ \forall i, k \in G, \tag{1}$$

where $\hat{\chi}$ is a map from $G \times G$ into $\mathbb{U} = \{x \in \mathbb{C} \mid |x| = 1\}$.

Note that there is the case $\hat{\chi}(i, j) = \chi(i * j)$. Here, χ is a character [6] of the group G and $*$ is an operation on G. Moreover, if χ is the trivial character, i.e., $\chi(i) = 1 (\forall i \in G)$, the set of signals is narrow sense group covariant.

We have the following proposition for $(G, \hat{\chi})$-covariant quantum state signals.

Proposition 2 *A set of pure quantum state signals $\{|\psi_i\rangle | i \in G\}$ is $(G, \hat{\chi})$-covariant if and only if, for any $i, j \in G$,*

$$\langle\psi_{k \circ i}|\psi_{k \circ j}\rangle = \begin{cases} \hat{\chi}(k, i)\overline{\hat{\chi}(k, j)}\langle\psi_i|\psi_j\rangle \\ \text{or} \\ \hat{\chi}(k, i)\overline{\hat{\chi}(k, j)}\langle\psi_j|\psi_i\rangle \end{cases} \tag{2}$$

for all $k \in G$.

Proof of Proposition 2 : First, the necessity directly follows from the definition of $(G, \hat{\chi})$-covariant signals.

To show the sufficiency, define bounded linear operators $V_k (k \in G)$ and bounded conjugate-linear operators $V_k' (k \in G)$ as, for any $|\phi\rangle = \sum_i a_i|\psi_i\rangle \in \mathcal{H} := \mathrm{span}(\{|\psi_i\rangle | i \in G\})$,

$$V_k|\phi\rangle = \sum_i a_i\hat{\chi}(k, i)|\psi_{k \circ i}\rangle,$$

$$V_k'|\phi\rangle = \sum_i \overline{a_i}\hat{\chi}(k, i)|\psi_{k \circ i}\rangle.$$

Then for any fixed $k \in G$, we can prove that for any $|\phi\rangle, |\psi\rangle \in \mathcal{H}$,

$$\langle\phi|V_k^\dagger V_k|\psi\rangle = \langle\phi|\psi\rangle \ \text{ or } \ \langle\phi|V_k'^\dagger V_k'|\psi\rangle = \langle\psi|\phi\rangle.$$

□

In the following, we show examples of $(G, \hat{\chi})$-covariant signals which are not narrow sense group covariant. Let $\mathbb{F}_4 = GF(2^2) = \{0, 1, \omega, \omega^2\}$ be the extension field of $GF(2)$.

Example 3 *The set of qubit-state signals with tetrahedral symmetry [3]*

$$|\psi_0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |\psi_1\rangle = \begin{bmatrix} (1/3)^{1/2} \\ (2/3)^{1/2} \end{bmatrix}$$

$$|\psi_\omega\rangle = \begin{bmatrix} (1/3)^{1/2} \\ (2/3)^{1/2}e^{2\pi i/3} \end{bmatrix} \quad |\psi_{\omega^2}\rangle = \begin{bmatrix} (1/3)^{1/2} \\ (2/3)^{1/2}e^{4\pi i/3} \end{bmatrix}$$

is $(\mathbb{F}_4, \hat{\chi})$-covariant, where $\mathbb{F}_4$ is the additive group of the field $\mathbb{F}_4$ and $\hat{\chi}$ is defined as follows:

$\hat{\chi}(i,j)$		j			
		0	1	ω	ω^2
i	0	1	1	1	1
	1	1	1	$\mathbf{i}$	$-\mathbf{i}$
	ω	1	$-\mathbf{i}$	1	$\mathbf{i}$
	ω^2	1	$\mathbf{i}$	$-\mathbf{i}$	1

Example 4 *The set of coded 4-ary PSK (phase shift keying) coherent-state signals by the linear code $\{000, 1\omega\omega^2, \omega\omega^2 1, \omega^2 1\omega\}$ over $\mathbb{F}_4$ is $(\mathbb{F}_4, \hat{\chi})$-covariant when the average number of photons of the coherent states is $\pi/4$. Here, $\hat{\chi}$ is the same map as that in Example 3.*

We will show other examples of $(G, \hat{\chi})$-covariant signals at the conference.

References

[1] C.A. Fuchs, QCMC2010, Prize Talk, (2010).

[2] T.S. Usuda and K. Shiromoto, Proc. of QCMC2010, AIP, New York, pp.97-100, (2011).

[3] E.B. Davies, IEEE Trans. Inf. Theory **IT-24**, pp.596-599, (1978).

[4] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Inter. J. Theor. Phys. **36**, pp.1269-1288, (1997).

[5] T.S. Usuda and I. Takumi, in Quantum Communication, Computing, and Measurement 2, Plenum Press, New York, pp.37-42, (2000).

[6] I.M. Isaacs, *Character theory of finite groups*, Academic Press, NewYork-London, (1976).

A monomial matrix formalism to describe quantum many-body states

Maarten Van den Nest

Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1, D-85748 Garching, Germany.

The Pauli stabilizer formalism (PSF) is an important tool in quantum information theory. This formalism regards many-body quantum states, called Pauli stabilizer states, that occur as joint eigenstates of sets of commuting Pauli operators. By exploiting the description of states in terms of their stabilizers, the PSF provides a powerful method to analyze the properties and dynamics of stabilizer states in a variety of settings—in fact, the PSF is commonly used in virtually all subfields of quantum information. Important applications include quantum error-correction, measurement-based computing and classical simulations of quantum circuits (cf. the Gottesman-Knill theorem). In addition, the PSF is used in condensed matter physics, cf. the study of topological order.

Notwithstanding its success, a drawback of the PSF is that it describes a small class of states. In particular, there are only finitely many stabilizer states for each given system size. Furthermore these states have very particular properties. For example, (modulo some trivial cases) they cannot be unique ground states of two-body Hamiltonians, every qubit is either maximally entangled with the rest of the system or completely disentangled from it, most interesting Pauli stabilizer states have zero correlation length etc. In addition, by definition the PSF only regards commuting stabilizers operators. This situation prompts the question of whether it is possible to enlarge the class of stabilizer states while maintaining a transparent stabilizer-type description. Such generalizations could lead to new insights in many-body quantum states as well as novel applications, such as better error-correcting codes, new information-theoretic protocols and new quantum states/processes that can be simulated efficiently classically.

A central feature of the PSF is that relevant information about stabilizer states can transparently and efficiently be extracted by suitably manipulating their stabilizer groups. Our goal is to identify a framework which is richer than the PSF while maintaining similarly clearcut maps from the "stabilizer picture" to the "state picture". To do so we start with the following observation: all Pauli operators are *monomial* matrices i.e. precisely one matrix entry per row and per column is nonzero. The basic premise of this work is then to consider *arbitrary* monomial unitary operators (with efficiently computable matrix elements) as stabilizer operators, giving rise to a general "monomial stabilizer formalism" (MSF).

In this work we argue that the MSF is a promising generalization of the PSF. We will do so by means of the following two contributions:

(a) We show that—perhaps surprisingly—a variety of important quantum many-body states are covered by the MSF. Examples include the ground level of the Affleck-Kennedy-Lieb-Tasaki model, the ground levels of Kitaev's quantum double models, the Laughlin wavefunction at filling fraction $\nu = 1$, the family of locally maximally entanglable (LME) states, coset states of Abelian groups, W states and Dicke states. These examples demonstrate the richness of the MSF. They also show that monomial stabilizer states ("M-states") generally do not display the "special" features of Pauli stabilizer states. For example there do exist interesting M-states which have non-commuting stabilizer groups and which are unique ground states of two-body Hamiltonians.

(b) We show that basic properties of monomial stabilizer spaces can be transparently described by manipulating their monomial stabilizer groups. In particular we will establish basic maps from the "stabilizer picture" to the "state picture" by showing how a designated orthonormal basis (called here the *orbit basis*) of any monomial stabilizer space can be constructed when the latter is described in terms of a set of monomial stabilizers. The procedure yields an explicit formula for each basis state, formulated entirely in terms of manipulations on the stabilizer group. This general result applies in particular to all examples given above. In other words one obtains a single unified method to treat a number of seemingly unrelated state families. It will also follow from our analysis that all M-states have a common, particularly simple structure viz. the nonzero-amplitudes of any M-state are all equal in modulus.

We subsequently use the orbit basis construction to investigate classical simulations. Whereas within the PSF many quantities of interest can be computed efficiently for *all* Pauli stabilizer states, the situation is different for general M-spaces. We will show that one cannot hope for general efficient algorithms for several basic problems (such as estimating local density operators), as we will prove their NP-hardness. In other words the MSF is too rich a framework to allow for generally applicable efficient simulations. However, it is important that these results regard worst-case complexity. In fact, based on our characterization of the orbit basis, we will identify a relevant subclass of M-states for which *efficient* classical simulations can nonetheless be achieved; this subclass contains essentially all examples in (a).

It is noteworthy that our methods allow to recover, with one unified method, the classical simulatability of a variety of state families including the Pauli stabilizer states and the quantum double models. In addition, the MSF allows to rederive, in a new and unified way, the standard basis expansion of stabilizer states as well as the matrix product state basis of the ground level of the AKLT model. Although going beyond the scope of the present submission, we finally point out that the methods developed here have recently been applied to arrive at new efficient classical simulations of quantum Fourier transforms (cf. M. Van den Nest, arXiv:1201.4867).

Calculating Unknown Eigenvalues with a Quantum Algorithm

Xiao-Qi Zhou[1], Pruet Kalasuwan[1], Timothy C. Ralph[2] and Jeremy L. O'Brien[1]

[1]Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, BS8 1UB, United Kingdom
[2]Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane 4072, Australia

Many quantum computations can be roughly broken down into two stages: read-in and processing of the input data; and processing and read-out of the solution. In the first phase the initial data is read in to a quantum register and processed with quantum gates. This produces a quantum state in which the solution is encoded. In the second phase the quantum state may be subjected to further processing followed by measurement, producing a classical data string containing the solution. Even though quantum computers are currently limited to a small number of qubits, there is considerable interest in the small scale demonstration of quantum algorithms even if the size of the problems solved means that they remain easily tractable with classical techniques. Such demonstrations remain challenging even for small numbers of qubits as they typically require the sequential application of a large number of quantum gates.

In recent years a number of elegant demonstrations of the read-out phase of Shor's factoring algorithm [1, 2, 3, 4] and a quantum chemistry simulation algorithm [5, 6] have been made. In these demonstrations, quantum gates have been used to produce the quantum state corresponding to a particular solution of the algorithm. It was then shown that the corresponding solution could be read-out with high fidelity from this state. However, in each case, the method for producing the quantum state explicitly required the solution to already be known from a classical calculation. That is, the solution was put into the quantum state by hand, before being read-out through further processing and measurement. It is clearly important to go beyond this restriction and demonstrate both stages of a quantum algorithm.

We present a demonstration of the iterative quantum phase estimation algorithm (IPEA) for a one-qubit unitary, in which no prior knowledge of the unitary is required for the implementation of the algorithm. The key part of the IPEA is implementing a sequence of controlled-unitary gates. Here we access a higher-dimensional Hilbert space to build the required controlled-unitary gates [7], where the control qubits are added to the unitary without knowing the eigenvalue decomposition of the unitary. The results are shown in Fig.1. These results point the way to efficient quantum simulations and quantum metrology applications in the near term, and to factoring large numbers in the longer term. This approach is architecture independent and thus can be used in other physical implementations.

Figure 1: Phase estimation data for 12 different Us. Each U is composed of two half-waveplates (HWPs); the first is set to $0°$, the second HWP is oriented at (a) $0°$, (b) $15°$, (c) $30°$, (d) $45°$, (e) $60°$, (f) $75°$, (g) $90°$, (h) $105°$, (i) $120°$, (j) $135°$, (k) $150°$ and (l) $165°$. For each U, three iterations of the algorithm are implemented and thus a three-digits estimated phase $\tilde{\varphi}$ is obtained. Compared with the phase φ the error in $\tilde{\varphi}$ is always less then 0.0001 in binary, which is consistent with theoretical prediction.

References

[1] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature, **414**, 883 (2001).

[2] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, Phys. Rev. Lett., **99**, 250504 (2007).

[3] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, Phys. Rev. Lett., **99**, 250505 (2007).

[4] A. Politi, J. C. F. Matthews, and J. L. OBrien, Science, **325**, 1221 (2009).

[5] B. P. Lanyon, J. D. Whitfield, G. G. Gillett, M. E. Goggin, M. P. Almeida, I. Kassal, J. D. Biamonte, M. Mohseni, B. J. Powell, M. Barbieri, A. Aspuru-Guzik, and A. G. White, Nature Chem., **2**, 106 (2010).

[6] J. Du, N. Xu, X. Peng, P. Wang, S. Wu, and D. Lu, Phys. Rev. Lett., **104**, 030502 (2010).

[7] X.-Q. Zhou, T. C. Ralph, P. Kalasuwan, M. Zhang, A. Peruzzo, B. P. Lanyon, and J. L. OBrien, Nat. Commun., **2**, 413 (2011).

Dynamics of 1d quasicondensates after quenching the external trapping potential

Wolfgang Rohringer[1], **Dominik Fischer**[1], **Florian Steiner**[1], **Jörg Schmiedmayer**[1] and **Michael Trupke**[1]

[1] *Vienna Center for Quantum Science and Technology,
Atominstitut, TU Wien, Stadionallee 2, 1020 Vienna, Austria*

The theoretical description of nonequilibrium dynamics in many-body quantum systems ist a challenging problem which is relevant to many branches of modern physics. Ultracold atom experiments offer a high degree of control over external parameters as well as a number of measurement methods for observables of interest in such many-body quantum systems, and therefore lend themselves to the investigation of their nonequilibrium dynamics.

We present experimental results considering the relaxation of ^{87}Rb 1d-quasicondensates trapped on an atom chip, in the regime of weak interactions, after a quench of the external trapping potential. In our setup, as for a broad class of interacting many-particle systems, the nonequilibrium state after the quench is known to be related to the initial equilibrium state by a spatial scaling transformation [1, 2, 3, 4, 5]

$$\Phi\left(\{\mathbf{x}_i\}, t\right) = \frac{1}{b^{D/2}} e^{i \sum_{i=1}^{N} \frac{m\mathbf{X}_i^2 \dot{b}}{2b\hbar} - i\mu\tau(t)/\hbar} \Phi\left(\left\{\frac{\mathbf{x}_i}{b}\right\}, 0\right),$$

(1)

with particle number N, dimensionality of the system D, chemical potential μ, $\tau(t) = \int_0^t dt'/b^2(t')$ and a time dependent scaling parameter $b(t)$ that is a solution of the Ermakov equation

$$\ddot{b} + \omega^2(t)b = \omega(0)/b^3$$

(2)

where $\omega(t)$ denotes the trap frequency in a harmonic trapping potential.

The 1d geometry and finite temperature in the equilibrium state of our system leads to a finite average phase coherence length, which can be measured by analysing density correlations after free expansion of the cloud [6, 7]. By measuring density profiles and phase coherence length after different evolution times in the trap after the quench, we study the validity of the scaling ansatz within the range of experimental parameters, as well as the possible influence of thermalisation processes inherent in the system.

Given the validity of a scaling transformation (1), it has been proposed [8, 9] and shown [10, 11] that the scaling parameter $b(t)$ can be engineered to provide a shortcut to the adiabatic state, which otherwise is only reached on timescales $t \gg (\omega)^{-1}$. Prospects of our work include an extension of such shortcut to adiabaticity schemes to 1d systems, with the possibility to implement a microscope for correlations present in the initial equilibrium state [5].
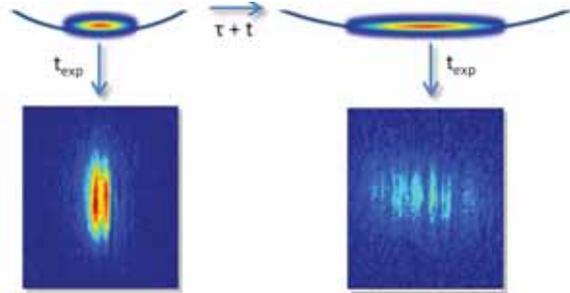
Figure 1: Measurement scheme. We repeatedly prepare 1d quasicondensates in an initial equilibrium state under identical conditions in a trapping potential with a longitudinal trapping frequency ω. Afterwards, we relax ω on a timescale $\tau \ll \omega^{-1}$ to a final value ω_f and let the atom clouds evolve for different evolution times t. For each of these evolution times, we take 150 absorption images after an additional free expansion time $t_{exp} = 10$ ms to extract average density profiles as well as normalised autocorrelation functions of the images, yielding the average phase coherence length λ.

References

[1] P. Öhberg and L. Santos, Phys. Rev. Lett **80**, 3678 (2002).

[2] Y. Castin and R. Dum, Phys. Rev. Lett **77**, 5315 (1996).

[3] Y. Kagan *et. al*, Phys. Rev. A **54**, R1753 (1996).

[4] V. Gritsev, P. Barmettler and E. Demler, New J. Phys. **12**, 113005 (2010).

[5] A. del Campo, Phys. Rev. A **84**, 031606 (2011).

[6] A. Imambekov *et. al*, Phys. Rev. A **80**, 033604 (2009).

[7] S. Manz *et. al*, Phys. Rev. A **81**, 031610 (2010).

[8] J. G. Muga *et. al*, J. Phys. B: At. Mol. Opt. Phys. **42**, 241001 (2009).

[9] Xi Chen *et. al*, Phys. Rev. Lett. **104**, 063002 (2010).

[10] J.-F. Schaff *et. al*, Phys. Rev. A **82**, 033430 (2010).

[11] J.-F. Schaff *et. al*, Europhys. Lett. **93**, 23001 (2011).

Simulation of driven open quantum systems with trapped ions.

Philipp Schindler[1], **Markus Müller**[4], **Daniel Nigg**[1], **Julio Barreiro**[1], **Thomas Monz**[1],
Michael Chwalla[3], **Markus Hennrich**[1], **Sebastian Diehl**[2,3], **Peter Zoller**[2,3] **and Rainer Blatt**[1,3]

[1]*Institut für Experimentalphysik, Universität Innsbruck, Austria*
[2]*Institut für Theoretische Physik, Universität Innsbruck, Austria*
[3]*Institut für Quantenoptik und Quanteninformation, Innsbruck, Austria*
[4]*Departamento de Fisica Teorica I, Univerisdad Complutense, Madrid, Spain*

Simulating interacting many-particle quantum-systems on a classical computer is in general inefficient as the required resources increase exponentially with the system size. Therefore the simulation of quantum dynamics with the aid of another, well-controlled quantum system has gained a lot of attention in the last few years. Generally two approaches for quantum simulators are explored. In the analog approach the Hamiltonian of the system of interest is directly implemented in the simulator system. This means that only systems with the same Hamiltonian as the simulator can be covered, but the requirements on the control are less stringent. In the digital approach, the dynamics is split in small discrete steps, which can be implemented efficiently. This leads to time dynamics with small systematic but bounded errors from the ideal continuous dynamics. For this approach, a universal quantum information processor is required which also implies that a faithful simulation is expected to be possible based on the toolbox provided by quantum error correction.

Most current quantum simulators replicate closed quantum systems governed only by coherent dynamics. However, it seems natural that large systems need to be treated as open systems, which are even harder to simulate on a classical computer. Building a quantum simulator for arbitrary open systems is challenging because in addition to a tremendous amount of control over the system, a well-controlled coupling to the environment is necessary. Recently, a proof of principle experiment of this coupling was demonstrated in our ion trap quantum information processor [1]. Dissipative many-body dynamics can then be realized by entangling an additional auxiliary qubit with the remaining quantum register and subsequent controlled dissipation of this qubit. With the aid of these tools it was possible to prepare an entangled four-qubit state from a completely mixed state using only dissipative interactions.

Recently, our group also demonstrated the building blocks for a universal closed-system digital simulator by digitally simulating the time evolution of various interacting spin models for system sizes up to six particles [2]. In this work we apply coherent and dissipative techniques in a combined way, to simulate the dynamics of an open and interacting many-body spin system, which shows a variety of novel non-equilibrium effects. In Ref. [3] a many-body system of bosons was studied theoretically, and it was shown how tailored dissipative dynamics can drive the system into a superfluid steady-state. It was predicted that the system should undergo a non-equilibrium phase transition as coherent dynamics is applied, which is incompatible with the steady state of the dissipative dynamics. It was shown how increasing the strength of coherent interactions leads to a transition from the superfluid phase to a thermal state. Here, we show how to map this bosonic system onto our ion-trap quantum simulator and demonstrate the interplay between dissipative and coherent dynamics in a small system. Since the dynamics requires many quantum operations, the errors induced by performing the gates play a major role. Universal quantum error correction protocols are very costly. We therefore develop and benchmark error detecting and correcting methods tailored to the simulated system.

Another major challenge for a large scale digital quantum simulator is the analysis of the final state. Naively one can perform full quantum state tomography to infer the output state. However, this is inefficient as the effort needed to perform state tomography increases exponentially with the number of qubits. We propose an alternative route to detect the described non-equilibrium phase transition, based on the observation of "many-body quantum jumps", as suggested recently in Ref. [4]. The detection of such "collective" quantum jumps should be accessible within our open-system simulator architecture.

References

[1] J. T. Barreiro, M. Müller, P. Schindler, D. Nigg, T. Monz, M. Chwalla, M. Hennrich, C. F. Roos, P. Zoller, R. Blatt, An open-system quantum simulator with trapped ions, Nature **470**, 486 (2011).

[2] B. Lanyon, C. Hempel, D. Nigg, M. Müller, R. Gerritsma, F. Zähringer, P. Schindler, J. T. Barreiro, M. Rambach, G. Kirchmair, M. Hennrich, P. Zoller, R. Blatt, C. F. Roos, Universal digital quantum simulation with trapped ions, Science **334**, 57 (2011).

[3] S. Diehl, A. Micheli, A. Kantian, B. Kraus, H. Büchler, P. Zoller, Quantum States and Phases in Driven Open Quantum Systems with Cold Atoms, Nature Physics **4**, 878, (2008).

[4] J. P. Garrahan and I. Lesanovsky. Thermodynamics of Quantum Jump Trajectories. Phys. Rev. Lett. **104**, 160601 (2010)

Entanglement of two ions by single-photon detection

L. Slodička[1], N. Röck[1], P. Schindler[1], M. Hennrich[1], G. Hétet[1], R. Blatt[1,2]
[1] *Institute for Experimental Physics, University of Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria*
[2] *1. Institute for Quantum Optics and Quantum Information of the Austrian Academy of Sciences, A-6020 Innsbruck, Austria*

The generation of distant entanglement of single atoms is an essential primitive for quantum networks. Experimental realizations generally rely on the detection of two photons [2]. Cabrillo's protocol based on single photon detection could significantly improve the entanglement rate [1]. We report on the experimental realization of this scheme by generating local entanglement of two Barium ions within one trap.

In the Cabrillo proposal, the atoms are both prepared in the same long-lived electronic state from which they can be excited through a Raman process to another metastable state with a small probability. For each atom, the Raman process entangles the atomic state and the emitted photon. Entanglement swapping from atom-photon to atom-atom entanglement is then provided by mixing the optical path in the same spatial mode followed by a Bell measurement in this mode. With a high indistinguishability and phase stability of the photon emission paths, detection of one photon heralds the entangled state $|\Psi\rangle = |ss'\rangle + e^{i\phi}|s's\rangle$, where ϕ is the path length difference between the two photonic channels, and $|s\rangle$, $|s'\rangle$ are the two ground states used in the Raman scattering process.

In our experiment, two Barium ions are trapped and cooled to the Doppler limit in a linear Paul trap. Experimental setup and entanglement generation procedures including the electronic level-scheme of $^{138}Ba^+$ are shown in Fig. 1-a). Laser light at 493 nm is used to Doppler-cool the ions and to detect their electronic state. Two high numerical aperture lenses collect the atomic fluorescence and a distant mirror retro-reflects the light of the upper ion to the second one in the same spatial mode. The elastic part of the fluorescence interferes and provides a means to lock the interferometer. After passing through a polarizing beam splitter the fluorescence of the two ions is then collected by a single mode fiber and detected by an avalanche photodiode.

To generate the entangled two-ion state, the two ions are first initialized in the m_j=-1/2 level of the $6S_{1/2}$ state ($|s\rangle$) via optical pumping along the magnetic field (see Fig. 1-b)). A weak horizontally polarized beam (Raman) then excites the ions through a spontaneous Raman process to the other Zeeman sublevel (m_j=+1/2) of the $6S_{1/2}$ state ($|s'\rangle$). The electronic state of each ion is then entangled with the number of photons in the σ^- polarized photonic mode. Detection of a single σ^- photon then effectively projects the two-ion state onto the entangled state $|\Psi\rangle$.

Following the heralding detection event we apply a set of resonant radio-frequency pulses and state read-out using a highly stabilized fiber laser at $1.76\mu m$ tuned to the long lived quadrupolar transition [3]. This allows us to measure the two-ion density matrix from which we estimated the overlap (the fidelity) with $|\Psi^+\rangle = |ss'\rangle + |s's\rangle$ to be $F = 63.5\%$, limited mostly by atomic motion and two-photon excitations from the
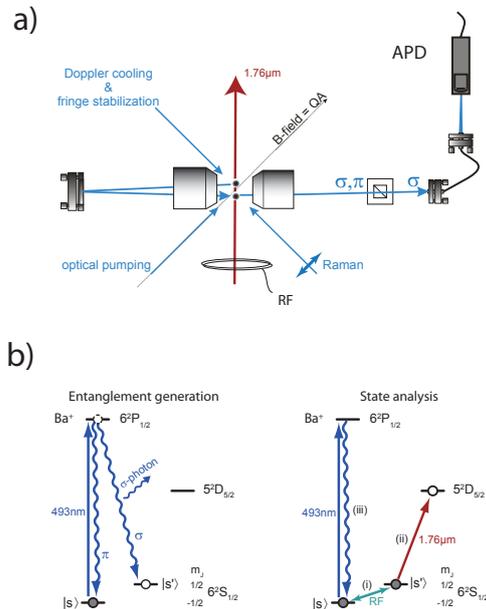
Figure 1: a) Experimental set-up. Two Barium ions are trapped and cooled in a linear Paul trap. The fluorescence from one ion is superimposed onto the second ion via a distant mirror. b) Level scheme showing the Raman scattering that triggers the single photon emission and the entanglement generation. The state analysis is performed via global radio-frequency pulses resonant with the two $S_{1/2}$ levels and via shelving to a long lived state ($D_{5/2}$).

ions. The fidelity is much higher than the classical bound of 50%, which demonstrates the entanglement of the two Barium ions using single-photon detection.

A two orders of magnitude increase in the entanglement generation rate was also measured compared to remote entanglement schemes that use two-photon coincidence events [2]. This result is important for efficient distribution of quantum information over long distances using trapped ion architectures.

References

[1] C. Cabrillo et al. , Phys. Rev. A **59**, 1025-1033 (1999)

[2] D. L. Moehring et al., Nature **449**, 68 (2007).

[3] L. Slodička et al., to appear in Phys. Rev. A

Towards an ion-cavity system with single Yb$^+$ ions

Matthias Steiner[1]**, Hendrik-Marten Meyer**[1] **and Michael Köhl**[1]

[1]*Cavendish Laboratory, University of Cambridge, UK*

The realization of an efficient ion-photon interface is one of the major challenges which prevent large scale ion-based quantum networks. Such an interface could consist of a single ion coupled to high finesse optical cavity. Existing ion-cavity systems operate in a regime, where the coupling of light and ion is smaller than the excited state decay rate[1]. In order to enhance the coupling, smaller cavity mode volumes must be used. However, macroscopic mirrors cannot be brought close enough to the ion since uncontrollable charging effects on the dielectric surface would disturb the electric trapping potential.

In this talk, I will report on our ongoing efforts to implement an ion-cavity system operating on the ^{3}D[3/2]$_{1/2}$-^{2}D$_{3/2}$ (935 nm) transition of Yb$^+$. The mirrors used for the cavity are directly machined onto the tips of optical fibres to reduce the mode volume while keeping the dielectric surface exposed to the ion small[2]. In order to achieve a high ion excitation rate on the cavity transition a laser system at 297 nm (^{2}S$_{1/2}$-^{3}D[3/2]$_{1/2}$ transition) has been built[3]. Besides the absolute frequency measurements of this transition for even isotopes we also show that this light can be used for laser cooling of trapped Yb$^+$ ions.

References

[1] G. R. Guthöhrlein et al., Nature, **414**, (2001).

[2] D. Hunger et al., New Journal of Physics, **12**, (2010).

[3] H.-M. Meyer et al., PR A, **85**, (2012).

Precise manipulation of a Bose-Einstein condensate's wavefunction

Stuart Szigeti[1], **Russell Anderson**[2], **Lincoln Turner**[2] **and Joseph Hope**[1]

[1]*The Australian National University, Canberra, Australia*
[2]*Monash University, Melbourne, Australia*

Arbitrary engineering of a Bose-Einstein condensate's (BEC's) quantum state at the healing length scale has many applications across ultracold atomic science, including atom interferometry [1], quantum simulation and emulation [2, 3] and topological quantum computing [4]. However, to date the BEC wavefunction is most commonly manipulated with laser light, which is diffraction limited. Here we present a scheme, based upon radiofrequency (RF) resonance and magnetic field gradients, that can be used to apply arbitrary spatially-dependent phase shifts to the BEC order parameter at the healing length scale.

To demonstrate our scheme, we consider the specific example of writing a soliton (i.e. a phase discontinuity) onto a BEC with two internal states. We assume that these internal states can be coupled via RF radiation, and that the BEC can be modelled semiclassically with a two-component order parameter. Provided the RF field interacts with the condensate quickly, we can ignore the kinetic and potential energies of the BEC. In this limit the wavefunction evolves purely due to the RF coupling:

$$i\frac{d\psi_g}{dt} = -\frac{\Delta(x,t)}{2}\psi_g + \frac{\Omega(t)}{2}\psi_e \qquad (1)$$

$$i\frac{d\psi_e}{dt} = \frac{\Delta(x,t)}{2}\psi_e + \frac{\Omega(t)}{2}\psi_g, \qquad (2)$$

where ψ_g and ψ_e are the two internal states of the BEC, $\Omega(t)$ is the Rabi frequency of the coupling and $\Delta(x,t)$ is the detuning, which can be made spatially dependent by adjusting the splitting of the levels via a magnetic field gradient and the Zeeman shift.

A schematic of our wavefunction engineering protocol is shown in Fig. 1. For this illustration, we invert a slice of the population using a simple sweep of the detuning. This transfers population via adiabatic passage wherever the sweep crosses the resonance, and leaves the population otherwise unaffected. Specifically, from (a) to (b) in Fig. 1 we have used an RF pulse with hyperbolic secant amplitude, and varied the detuning in time according to a hyperbolic tangent:

$$\Omega(t) = \Omega_0 \mathrm{sech}\beta(t - t_0) \qquad (3)$$

$$\Delta(x,t) = \Delta_0(x) + \Omega_0 \tanh\beta(t - t_0), \qquad (4)$$

where t_0 and $1/\beta$ define the temporal centre and duration of the pulse, respectively, and $\Delta_0(x)$ is the spatially-dependent detuning offset due to the magnetic field gradient.

Numerical simulations of this process show that the discontinuity in the phase can be as small as 10-100 nm. This is smaller than the healing length of a typical Rb condensate, which is on the order of 300 nm. However, healing length scale structures can only be written with pulse durations no longer than the healing time, which is the characteristic time over which an atom in the condensate will move a distance
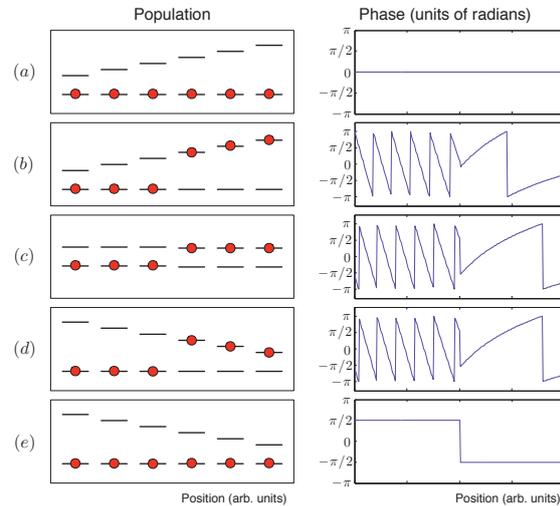
Figure 1: Diagram illustrating the change of the atomic population and the phase of populated states under the proposed wavefunction engineering protocol. Between (a) and (b) an RF pulse and magnetic field gradient are used to transfer a slice of the ground state population to the excited state. This results in a nontrivial global phase evolution. At (c) the magnetic field gradient and RF pulse are turned off. The atoms are allowed to freely evolve until there is an additional π phase shift between the ground and excited populations. The magnetic field gradient is turned on but with a reversed sign in (d), and between (d) and (e) a time-reversed version of the RF pulse returns all the population to the ground state. This also unwinds the spurious phase due to the (a)-(b) stage, but leaves the imprinted phase (stage (c)) unaffected.

equal to the healing length. Basing our wavefunction engineering protocol on adiabatic sweeps of the detuning restricts the duration of the scheme to a minimum of 100 μs, which is 100 times larger than typical healing times. Our current efforts are devoted to designing faster pulses using the techniques of optimal control theory and numerical optimization.

References

[1] B. Benton, M. Krygier, J. Heward, M. Edwards and C. W. Charles, Phys. Rev. A, **84**, 043648 (2011).

[2] I. Buluta and F. Nori, Science, **326**, 5949 (2009).

[3] D. Jaksch and P. Zoller, Annals of Physics, **315**, 52–79 (2005).

[4] C. Nayak, S. H. Steven, A. Stern, M. Freedman and S. Das Sarma, Rev. Mod. Phys., **80**, 1083–1159 (2008).

Spectroscopy of mechanical dissipation in micro-mechanical membranes

A. Jöckel[1], **M. T. Rakher**[1], **M. Korppi**[1], **S. Camerer**[2], **D. Hunger**[2], **M. Mader**[2], and **P. Treutlein**[1]

[1]*Department of Physics, University of Basel, Switzerland*
[2]*Max-Planck-Institute of Quantum Optics and Ludwig-Maximilians-University, Munich, Germany*

Micro-mechanical membrane oscillators are currently investigated in many optomechanics experiments, where lasers and optical cavities are used for cooling, control, and readout of their mechanical vibrations. Applications lie in the area of precision force sensing and in fundamental experiments on quantum physics at macroscopic scales [1]. The quality factor Q of the mechanical modes of the membranes is a key figure of merit in such experiments. However, the origin of mechanical dissipation limiting the attainable Q is not completely understood and a subject of intense research [2, 3].

Here we report an experiment [4] in which we observe a variation of Q by more than two orders of magnitude as a function of the fundamental mode frequency of a SiN membrane. Several distinct resonances in Q are observed that can be explained by coupling to mechanical modes of the membrane frame. The frequency of the membrane modes is tuned reversibly by up to 40% through local heating of the membrane with a laser. This method of frequency tuning has the advantage that the frequency dependence of Q can be studied with a single membrane *in situ*, resulting in a detailed spectrum of the coupling to the environment of this particular mode. Other methods that compare Q between various structures of different sizes have to rely on the assumption that the environment of these structures is comparable.

We investigate "low-stress" SiN membranes that are supported by a Si frame. The frame is glued at one edge to a holder inside a vacuum chamber, see Fig. 1a. To tune the membrane frequency, a power stabilized 780 nm laser (red) is focused onto the membrane. This causes the membrane to heat up and expand, resulting in reduced tensile stress and lower frequency. A Michelson interferometer at 852 nm (blue) is used to read out the membrane motion. The interferometer signal is also used for feedback driving of the membrane with a piezo. The Q factor is determined by measuring the decay time of the membrane amplitude in ring-down measurements. We use laser tuning to record a spectrum of the quality factor Q of the fundamental mode as a function of the mode frequency.

The upper plot in Fig. 1b shows the dissipation of the frame mode, showing resonances and a variation over two orders of magnitude. The resonances in Q can be attributed to coupling of the membrane mode to modes of the frame. By pointing the interferometer onto the frame next to the membrane and recording the amplitude response to a driving with the piezo, one can measure the frame mode frequencies. They can be related to the dissipation resonances, as shown in the lower plot in Fig. 1b. This mechanism can be exploited to reduce clamping loss by tuning the membrane frequency to a gap be-

tween frame modes. Other dissipation mechanisms are found to be independent of membrane frequency and temperature in the measured range. We also studied higher order modes and find approximately the same maximum Q.
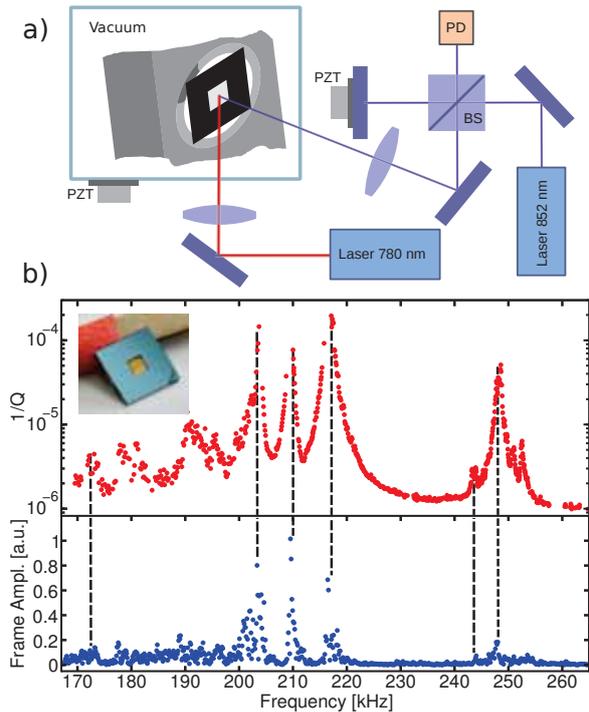
Figure 1: Spectroscopy of micro-mechanical membranes. (a) Experimental setup. (b) Upper plot: spectrum of membrane dissipation Q^{-1} for the fundamental mode. Lower plot: vibrations of the frame measured close to the membrane.

References

[1] T. J. Kippenberg and K. J. Vahala, Science **321**, 1172 (2008).

[2] G. D. Cole, I. Wilson-Rae, K. Werbach, M. R. Vanner, and M. Aspelmeyer, Nature Commun. **2**, 231 (2011).

[3] P.-L. Yu, T. P. Purdy, and C. A. Regal, Phys. Rev. Lett. **108**, 083603 (2012).

[4] A. Jöckel, M. T. Rakher, M. Korppi, S. Camerer, D. Hunger, M. Mader, and P. Treutlein, Appl. Phys. Lett. **99**, 143109 (2011).

Time-bin interferometry of short coherence down-conversion photon pairs

__Thomas Kauten__[1], Harishankar Jayakumar[1], Ana Predojevic[1] and Gregor Weihs[1]

[1]*Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, 6020 Innsbruck, Austria*

Photons can be entangled in polarization, energy, time of arrival and/or momentum and can be generated from variety of systems. Our interest lies in the generation of time-bin entangled photons from single self-assembled semiconductor quantum dots [1]. The scheme requires a pump interferometer and an analyzing interferometer with a long delay (3 ns) due to the long lifetime of the excitons in a quantum dot.

Phase stability of the pump and the analyzing interferometers is critical in a time-bin entanglement scheme. The large length difference between the arms makes the interferometers extremely sensitive to thermal fluctuations in the environment. In order to separate the effects of dephasing in the quantum dots and instability of the interferometers we tested our interferometers using reduced coherence photon pairs generated via spontaneous parametric down-conversion (SPDC).

The photon pairs are generated by pumping a SPDC source with a short coherence length laser that passes the pump interferometer [2]. The signal and the idler photons are sent to the two input ports of the analyzing interferometer and the visibility of the two-photon interference is used to determine the stability of the setup [3].

Conditioned on coincident detection of the two SPDC photons the produced state is:

$$|\Psi\rangle = \frac{1}{2}\{e^{i\phi_0(t-\tau)+\phi}|S_p; L_s L_i\rangle + e^{i\phi_0(t-\tau)+\phi_P}|L_p; S_s S_i\rangle$$
$$+ e^{i\phi_0(t)}|S_p; S_s S_i\rangle + e^{i\phi_0(t-2\tau)+\phi+\phi_P}|L_p; L_s L_i\rangle\} \quad (1)$$

where ϕ_p is the relative phase in the pump interferometer, $\phi_0(t)$ is the finite coherence phase of the pump laser, $\phi(t)$ are the relative phase differences in the analyzing and pump interferometers, respectively, τ is the long-short delay and the labels S, and L refer to the short and long paths of the interferometers for signal (s), idler (i), and pump (p).

Based on the arrival time of the photon pairs it is impossible to predict if the pump photon took the short or the long path of the interferometer. Thus the first and the second term interfere with the other two terms providing an incoherent background, leading to a maximum visibility of 50% if there is no correlation between $\phi(t)$ and $\phi(t - \tau)$. Then the coincidence count rate is given by:

$$R_C = 1 - \frac{1}{2}\cos(\phi_p - \phi) \quad (2)$$
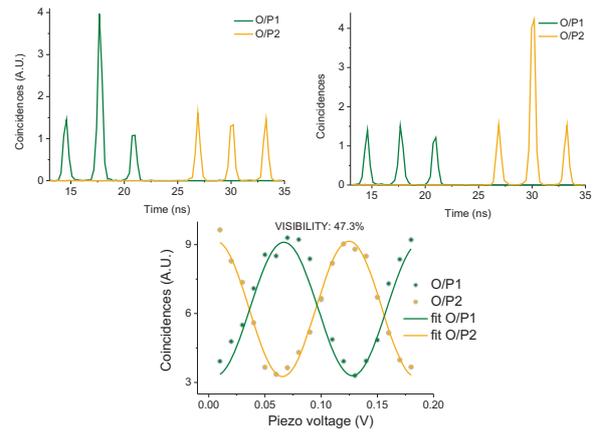
Figure 2: Coincidence counts between O/P3 and O/P1, O/P2.

Coincidence counts were recorded between the signal (O/P3) and idler (O/P1, O/P2) (as seen in Fig. 2) while the phase of both paths of the analyzing interferometer is varied by a piezo actuator. The correlation between the outputs O/P3 and O/P1 was transfered to outputs O/P3 and O/P2 by changing the phase. Visibility of 47.3% was observed.

This measurement allows an estimation of the quality of our setup and the active stabilization scheme. Based on this characterization the effects of quantum dot exciton dephasing on the time-bin entanglement can be quantified.

Figure 1: **Setup:** Light derived from a short coherence length diode laser operating at wavelength of 404 nm is sent through a Michelson interferometer. This interferometer serves as the pump interferometer. One of the outputs is coupled into a polarization maintaining fiber for spatial filtering. Further, the light is focused onto a BBO-crystal, which creates photon pairs via spontaneous parametric down conversion. The produced photon pairs are coupled into single mode fibers and directed into the analyzing interferometer. We recorded the coincidences of the single photons between the different interferometer outputs. Both, the pump and the analyzing interferometer, are actively phase-stabilized. Glass plate and piezo is used to change the phase between the two interferometers.

References

[1] C. Simon and J.P. Poizat, Phys. Rev. Lett., **94**, 030502 (2005)

[2] J. Brendel et al., Phys. Rev. Lett., **82**, 2594-2597 (1999)

[3] J. Liang et al., Physical Review A **83**, 033812 (2011)

The Synchronisation of Nano-Mechanical Resonators Coupled via a Common Cavity Field in the Presence of Quantum Noise

Casey R. Myers[1], Thomas. M. Stace[1] and Gerard J. Milburn[1]

[1]Centre for Engineered Quantum Systems, School of Mathematics and Physics, The University of Queensland, QLD, Australia 4072

The synchronisation of coupled oscillators appear in many different physical systems. Recent experimental advances in the synchronisation of mechanical oscillators using light [1, 2] suggest a full quantum description is now required. The model considered by Heinrich *et. al* in [1] consists of direct mechanical resonator to mechanical resonator coupling in addition to resonator to cavity mode coupling and is related to the model by Kuramoto [3]. In this presentation we do not consider direct coupling between nano-mechanical resonators, only coupling to the common cavity mode. Holmes *et. al* [4] analysed this model in the semi-classical picture, showing that the nano-mechanical resonators do synchronise. In this presentation we endeavour to answer the question: does synchronisation survive in the presence of quantum noise? Specifically, does quantum phase diffusion destabilise synchronisation? We approach this problem in three ways:

1. We derive a Fokker-Planck like equation from the master equation for the system. From this master equation we can derive the set of stochastic differential equations (SDE) and solve these numerically.

2. We directly solve a truncated master equation *centred* around the semi-classical solutions.

3. How can we detect synchronisations? Will there be a signature of synchronisation on the common cavity mode that we can see if we homodyne detect?

The Hamiltonian, in the coherent driving field interaction picture, describing the N nano-mechanical resonators interacting with the driven common cavity mode via a radiation pressure coupling is:

$$\hat{H}_I = \hbar\delta\hat{a}^\dagger\hat{a} + \sum_{i=1}^N \hbar\omega_i\hat{b}_i^\dagger\hat{b}_i + \hbar\epsilon(\hat{a}+\hat{a}^\dagger) + \sum_{i=1}^N \hbar g_i\hat{a}^\dagger\hat{a}\hat{x}_i,$$

where $\hat{x}_i = (\hat{b}_i + \hat{b}_i^\dagger)/2$ and we assume ϵ is real. The master equation for this system is given by

$$\frac{d\hat{\rho}}{dt} = -\frac{i}{\hbar}[\hat{H}_I, \rho] + \kappa\mathcal{D}[\hat{a}]\hat{\rho} + \sum_{i=1}^N \gamma_i\mathcal{D}[\hat{b}_i]\hat{\rho},$$

where κ is the amplitude decay for the resonant cavity, γ_i amplitude decay ith nano-mechanical resonator and $\mathcal{D}[\hat{a}]\hat{\rho} = 2\hat{a}\hat{\rho}\hat{a}^\dagger - \hat{a}^\dagger\hat{a}\hat{\rho} - \hat{\rho}\hat{a}^\dagger\hat{a}$.

We first numerically solve the SDEs resulting from this master equation by using the corresponding Fokker-Planck like equation [5]:

$$\frac{dP(\vec{\chi})}{dt} = -\sum_i \frac{\partial}{\partial\chi_i}\mathbf{A}(\vec{\chi})P(\vec{\chi}) + \frac{1}{2}\sum_{ij}\frac{\partial^2}{\partial\chi_{i,j}}\mathbf{B}(\vec{\chi})\mathbf{B}(\vec{\chi})^{\mathrm{T}}P(\vec{\chi})$$

where $P(\vec{\chi})$ is the Positive P function. The corresponding SDEs are given by [6] $d\vec{\chi} = \mathbf{A}(\vec{\chi})dt + \mathbf{B}(\vec{\chi})d\vec{W}(t)$, where $d\vec{W}(t) = \xi(t)\sqrt{dt}$.

We next directly solve the master equation *centred* around the semi-classical solutions [4]. That is, instead of solving the master equation for $\hat{\rho}$, we solve for a density matrix displaced to the vacuum: $\bar{\rho} = D^\dagger\hat{\rho}D$, where the time dependent displacement is given by:

$$\hat{D} = \exp\left(\alpha(t)\hat{a}^\dagger - \alpha^*(t)\hat{a} + \sum_{i=1}^N(\beta_i(t)\hat{b}_i^\dagger - \beta_i^*(t)\hat{b}_i)\right)$$

In this case we need to take the time derivative of $\hat{D}$:

$$\frac{d\hat{D}}{dt} = \left(-\frac{1}{2}\frac{d\alpha}{dt}\alpha^* + \frac{1}{2}\frac{d\alpha^*}{dt}\alpha + \frac{d\alpha}{dt}\hat{a}^\dagger - \frac{d\alpha^*}{dt}\hat{a}\right)\hat{D}$$

The new master equation becomes

$$\frac{d\bar{\rho}}{dt} = -\frac{i}{\hbar}[\hat{D}^\dagger\hat{H}_I\hat{D}, \bar{\rho}] + \kappa\mathcal{D}[\hat{D}^\dagger\hat{a}\hat{D}]\bar{\rho} + \sum_{i=1}^N \gamma_i\mathcal{D}[\hat{D}^\dagger\hat{b}_i\hat{D}]\bar{\rho}$$
$$- D^\dagger\frac{d\hat{D}}{dt}\bar{\rho} - \bar{\rho}\frac{d\hat{D}^\dagger}{dt}\hat{D},$$

where we have used $\hat{D}^\dagger\hat{a}\hat{D} = \hat{a} + \alpha$, $\hat{D}^\dagger\hat{b}_i\hat{D} = \hat{b}_i + \beta_i$ [7].

Finally, we ask, how can we detect synchronisations? Will there be a signature of synchronisation on the common cavity mode that we can see if we homodyne detect? From the numerically solved displaced, truncated density matrix above, we calculate the output photo-current obtained when we homodyne detect the common cavity mode by using [6, 8]:

$$d\hat{\rho}_c = \mathcal{L}\hat{\rho}_c(t)dt + dW(t)\mathcal{H}[\hat{a}]\hat{\rho}_c(t)$$
$$I_c(t) = \eta\langle\hat{a}+\hat{a}^\dagger\rangle_c(t) + \sqrt{\eta}\xi(t),$$

where $\langle\hat{a}+\hat{a}^\dagger\rangle_c(t) = \mathrm{Tr}[(\hat{a}+\hat{a}^\dagger)\hat{\rho}_c(t)]$.

References

[1] G. Heinrich *et. al*, Phys. Rev. Lett. **107**, 043603 (2011).

[2] M. Zhang *et. al*, arXiv:1112.3636

[3] Y. Kuramoto, Lecture Notes in Physics **39**, 420.

[4] C.A. Holmes, C.P. Meaney & G.J. Milburn, arXiv:1105.2086v2

[5] C.P. Meaney, Ph.D thesis submitted to The University of Queensland, 2011.

[6] C.W. Gardiner & P. Zoller, *Quantum Noise*, Springer-Verlag, Berlin (2000).

[7] D.F. Walls & G.J. Milburn, *Quantum Optics*, Springer-Verlag, Berlin (1994).

[8] H.M. Wiseman and G.J. Milburn, *Quantum Measurement and Control*, Cambridge University Press, Cambridge (2009) .

All Optical Resonant Excitation and Coherent Manipulation of a Single InAs Quantum Dot for Quantum Information Experiments

Harishankar Jayakumar[1], Ana Predojević[1], Thomas Kauten[1], Tobias Huber[1], Glenn S. Solomon[2], and Gregor Weihs[1]

[1]*University of Innsbruck, Innsbruck, Austria*
[2]*Joint Quantum Institute, National Institute for Standards and Technology and University of Maryland, Gaithersburg, United States*

Single self-assembled semiconductor quantum dots are proven emitters of single photons and entangled photon pairs [1]. While coherent creation and manipulation of spin states of a quantum dot provide tools for manipulation of both stationary and flying qubits [2], this task is still very challenging. A common way to observe an optical signal from a quantum dot is above-band excitation, where a laser pulse has significantly higher energy than the quantum dot emission and creates charges in the surrounding material which can be randomly trapped in the quantum dot potential. Nevertheless, if one aims to use a quantum dot in quantum optics experiments where coherent properties of the excitation need to be transferred to the system [3], the resonant excitation and coherent control become essential.

We demonstrated an all optical resonant two-photon excitation of the biexciton state of a single InAs quantum dot embedded in a micro-cavity. In particular, we used pulsed laser light of adjustable pulse length to excite a single quantum dot using the micro-cavity as the light-guiding medium. In contrast to the previous work [4] where the excited state population was measured electrically in photo-current signal our measurements directly prove the coherence of the photon emission in photo-luminescence. A quantum dot biexciton-exciton cascade emission consists of two photons with energy separation equal to the biexciton binding energy. For the excitation of the system from the ground state to the biexciton state we used a two-photon virtual resonance placed energy-wise half way between exciton and biexcition. The resonant nature of the excitation was confirmed by the observation of the Rabi oscillations (Fig.1b). Damping of the Rabi oscillations can be attributed to a competing non-resonant process of two-photon absorption in the surrounding material present at high excitation powers. Due to the deterministic nature of the excitation process the measurements of the auto-correlations of both exciton and biexciton photons show the full suppression of multiple photon emission (Fig.1a).

In addition, we measured the level of quantum coherence in the ground-biexciton state qubit by performing a Ramsey interference measurement [5]. Also, and to our knowledge for the first time, we performed a measurement of the spin-echo in such a system. The result yields increase of the coherence time from 145 ps to 254 ps. The results of this measurement are shown in Fig.1c.

The combination of the full suppression of the multiple photon events and the resonant excitation makes this system well suitable for schemes like time-bin entanglement or probabilistic interaction of the photons originating from dissimilar sources.
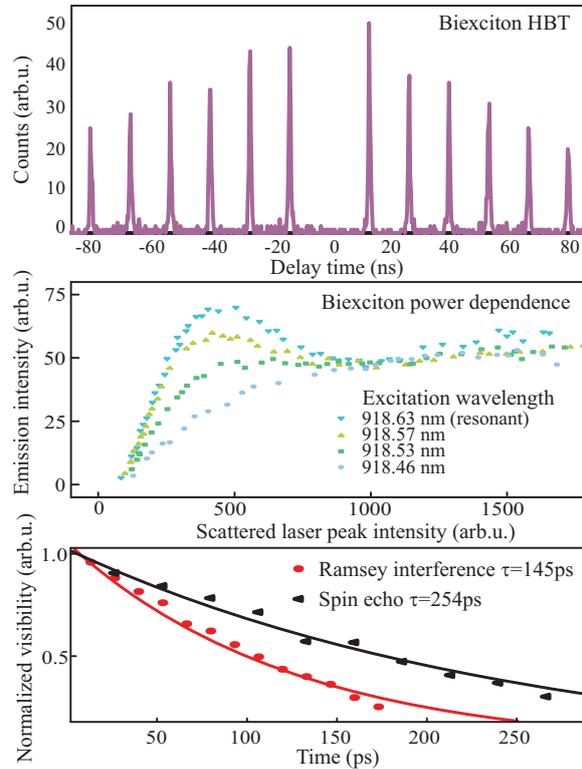
Figure 1: a: Hanbury Brown-Twiss measurement showing the full suppression of the multiple photon emission. b: Rabi oscillations of the biexciton emission probability for different detunings from the two-photon resonance. c: Spin echo measurement yields the increase of the coherence time; lines present exponential fits which yield presented coherence times.

References

[1] R. M. Stevenson, et. al., Nature, **439**, 179 (2006).

[2] A. J. Ramsay, Semicond. Sci. Technol., **25**, 103001, (2010).

[3] J. Brendel, N. Gisin, W. Titel, H. Zbinden, Phys. Rev. Lett., **82**, 2594, (1999).

[4] S. Stufler, et. al., Phys. Rev. B, **73**, 125304, (2006).

[5] T. Flissikowski, A. Betke, I. A. Akimov, F. Henneberger, Phys. Rev. Lett., **92**, 227401, (2004).

Fluorescence photon measurements from single quantum dots on an optical nanofiber

Ramachandrarao Yalla, K. P. Nayak, and K. Hakuta

Center for Photonic Innovations, University of Electro-Communications, Chofu, Tokyo 182-8585, Japan

Abstract: We experimentally demonstrate the systematic and reproducible deposition of single q-dots along an optical nanofiber. For single q-dots on an optical nanofiber, we measure the fluorescence photons coupled into the nanofiber guided modes and the normalized photon correlations, by varying the excitation laser intensity.

Introduction: Single photon manipulation is one of the major issues in the contemporary quantum optics, especially in the context of quantum information technology. For this purpose many novel ideas have been proposed so far. Recently, the sub-wavelength diameter silica fiber, termed as optical nanofiber has becoming a promising tool for manipulating single photons.

Experimental setup: Figure 1 illustrates the schematic diagram of the experimental setup. The nanofiber is located at the central part of a tapered optical fiber. For depositing q-dots on the nanofiber, we use a sub-pico-liter needle-dispenser and an inverted microscope. The q-dots are deposited periodically at 8 positions on the nanofiber along the fiber axis in 20 μm steps. The q-dots are excited using cw diode-laser at a wavelength of 640 nm through a microscope objective lens. The fluorescence photons emitted from q-dots

Figure 2: (a) The photon counts as a function of time. (b) The normalized photon correlations as a function of delay time. (c) The observed recovery rates for different excitation laser intensities. (d) The observed photon-counts for different excitation intensities.

Table 1: Obtained parameters for q-dots

τ [ns]	100 ±40	195 ±90	130 ±20	126 ±13	140 ±45	190 ±50	130 ±50
$n_o(\infty)$ [kC/s]	30.0 ±1.0	20.0 ±0.8	38.4 ±1.2	42.0 ±2.5	39.8 ±0.9	44.7 ±5.6	45.7 ±2.2
$\eta_q\eta_c$	0.033 ±.014	0.043 ±.020	0.054 ±.010	0.057 ±.009	0.060 ±.021	0.094 ±.030	0.064 ±.028

Figure 1: The schematic diagram of the experimental setup.

are coupled to the guided modes of the nanofiber and are detected through a single mode optical fiber. At one end of the fiber, arrival times of photons at both APDs are recorded using a two-channel single-photon-counter. The photon correlations are derived from the record. At the other end of the fiber, the fluorescence emission spectrum is measured using an optical-multichannel-analyzer (OMA).

Results: In order to know the spatial distribution of q-dots, we first scan the focusing point along the nanofiber by observing the fluorescence photon counts through the guided modes [1]. Fluorescence photon measurements are carried out for each deposited position by varying the excitation laser intensity from 20 to 900 W/cm^2. Typical measured results for one position are shown in Fig. 2 (a)-(b) at laser intensity of 50 W/cm^2. Fig. 2 (a) shows the photon counts as a function of time. One can readily see the blinking behavior with a single-step, which is a signature of a single q-dot emission. Fig. 2 (b) shows the normalized correlations, which reveal clearly

the anti-bunching behavior. The anti-bunching signal is fitted by a single exponential curve (red curve). The obtained recovery rate is $1/55 \ ns^{-1}$.

Analysis: In Fig. 2 (c), observed recovery rates are plotted versus excitation laser intensity. One can readily see the linear dependence. The fitted results are shown by solid lines. The intercept at the zero-intensity gives the decay rate of the excited state ($1/\tau$). In Fig 2 (d), observed fluorescence photon-counts are plotted versus excitation laser intensity. One can readily see the saturation behaviors for all plots. The fitted results are shown by dashed lines to obtain the $n_o(\infty)$. The analyzed results are summarized in the Table 1. As shown in the Table 1 third column, the obtained highest value of $\eta_q\eta_c$ to be 0.094 (± 0.030). We obtained the lowest limit for the coupling efficiency (η_c) to be 9.4 (± 3.0)% by assuming quantum efficiency (η_q) of q-dots to be 100%. We will also discuss the direct measurement of coupling efficiency.

References

[1] R. R. Yalla *et al.*, Opt. Express **20**, 2932-2941 (2012).

Heralded quantum entanglement between two crystals

Imam Usmani[1], Christoph Clausen[1], Félix Bussières[1], Nicolas Sangouard[1], Mikael Afzelius[1] and Nicolas Gisin[1]

[1]*Group of Applied Physics, University of Geneva, CH-1211 Geneva 4, Switzerland*

Quantum networks must have the crucial ability to entangle quantum nodes. A prominent example is the quantum repeater [1, 2], which allows the distance barrier of direct transmission of single photons to be overcome, provided remote quantum memories(QM) can be entangled in a heralded fashion.

Our approaches focuses on rare-earth doped crystals, i.e. solid state QM. By the use of photon-echo based techniques, these systems have great potential. Several impressive results have been reached: storage time of 1s [3], efficiency of 69% [4] and storage of 64 weak light pulses[5]. Recently, storage of true single photons and time-bin entanglement has also been demonstrated[6].

Here we demonstrate heralded entanglement between two crystals separated by 1.3 cm[7]. The setup is depicted in fig.1. A non linear crystal is pumped to produce photons pair through spontaneous parametric down conversion(SPDC). When the probability of pair creation is small, a detection in the idler mode heralds the presence of a single photon in the signal mode. This single photon is sent through a beamsplitter, which creates a single photon entangled state $\frac{1}{\sqrt{2}}(|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B)$ between the two spatial output modes A and B. In each path, a Nd^{3+}:$\mathrm{Y_2SiO_5}$ crystal acts as a QM (M_A and M_B). Upon absorption, the detection of the idler photon heralds the creation of a single collective excitation delocalized between the two crystals: $\frac{1}{\sqrt{2}}(|W\rangle_A|G\rangle_B + |G\rangle_A|W\rangle_B)$, where $|G\rangle_{A(B)}$ is the ground state of $\mathrm{M}_{A(B)}$ and $|W\rangle$ is a Dicke like state, when a crystal has absorbed a single photon.

To characterize the entanglement of the memories, the atomic collective excitation is reconverted into optical excitation by the use of a photon echo based technique, the atomic frequency comb protocol(AFC) [8]. The resulting field can be probed using single photon detectors. The entanglement is then measured via the concurrence, a function ranging from zero for a separable state to one for a maximally entangled state. A lower bound on the concurrence is:

$$C \geq max(0, V(p_{01} + p_{10}) - 2\sqrt{p_{00}p_{11}})$$

where V is the visibility obtained by recombining mode A and B, and p_{mn} is the probability of detecting m photons in mode A and n photons in mode B. In practice, optical losses, memories and detector efficiencies and double pair creation will decrease C. However, a positive concurrence is sufficient to demonstrate that the retrieved photonic state is entangled. Since entanglement cannot increase through local operations, it also proves that the memories must have been entangled. We measured the concurrence for different pumping powers of the SPDC source and obtained always positive values up to $C = (1.13 \pm 0.06) \cdot 10^{-4}$.

In conclusion, we have reported an experimental observation of heralded quantum entanglement between two separate solid-state quantum memories. We emphasize that although the entangled state involves only one excitation, the observed entanglement shows that the stored excitation is coherently delocalized among all the neodymium ions in resonance with the photon, meaning $\sim 10^{10}$ ions in each crystal. Our results demonstrate that rare earth ensembles, naturally trapped in crystals, have the potential to form compact, stable and coherent quantum network nodes.

In this experiment, the storage time is short (33ns) and must be decided in advance. Hence, the next challenge is to realize a QM that can store quantum states for longer time and that allows on demand read out. Also, to achieve quantum repeaters, one needs to herald entanglement between QM distant from kilometers, which must be achieved in a different setup, using for example two single photons sources.
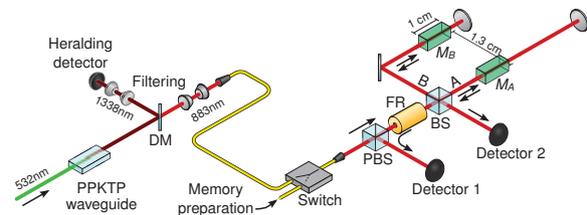
Figure 1: Experimental setup to herald entanglement between two QM

References

[1] Briegel *et al.* Phys Rev.Lett. **81**, 5932 (1998)

[2] Sangouard *et al.* Rev. Mod. Phys. 83, 33-80 (2011)

[3] Longdell *et al.* Phys. Rev. Lett. **95** 063601 (2005)

[4] Hedges *et al.* Nature **465** 1052 (2010)

[5] Usmani *et al.* Nat. Commun. **1**, 12 (2010)

[6] Clausen *et al.*, Nature **469**, 508-511 (2011), Saglamyurek *et al.*, Nature **469**, 512-515 (2011)

[7] Usmani *et al.*, Nat. Photon., doi:10.1038/nphoton.2012.34 (2012)

[8] Afzelius *et al.* Phys Rev. A **79**, 052329 (2009)

Quantum Discord as Resource for Remote State Preparation

Borivoje Dakić[1†], Yannick Ole Lipp[1†], Xiaosong Ma[2,3†], Martin Ringbauer[1†], Sebastian Kropatschek[3], Stefanie Barz[2], Tomasz Paterek[4], Vlatko Vedral[4,5], Anton Zeilinger[2,3], Časlav Brukner[1,3] and Philip Walther[1,3]

[1]*Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria.*
[2]*Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria.*
[3]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria.*
[4]*Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, 117543 Singapore.*
[5]*Department of Atomic and Laser Physics, University of Oxford, Oxford OX1 3PU, UK.*
†*These authors contributed equally to this work.*

Quantum computation and quantum communication is widely believed to provide significant enhancements in the efficiency of information processing as compared to their classical counterparts. These advantages appear in a variety of applications such as universal quantum computation, reduction of computational complexity or secret key distribution. Quantum entanglement is widely recognised as the key resource for Quantum Information Processing (QIP). While it has been intensely studied and is well understood by its relation to quantum state teleportation, there exists no proof, that quantum entanglement is necessary for enhanced information processing. In fact, recent findings such as quantum computational models and quantum search algorithms which rely solely on separable states, casted doubt on this status of quantum entanglement. Thus, when quantum discord was introduced as a novel measure of non-classical correlations [1], including entanglement as a subset, it created a lot of interest, despite lacking an intuitive interpretation.

Here we provide an operational meaning to quantum discord by directly relating it to the fidelity of one of the most fundamental quantum information protocols, remote state preparation (RSP). In this protocol, which is a variant of quantum state teleportation, the sender (Alice) wants to prepare a known quantum state on the equatorial plane to a given direction $\vec{\beta}$ on the receivers (Bob) Bloch sphere. This can be achieved using only one classical bit of communication. In the protocol, Alice and Bob share an arbitrarily correlated two-qubit state. Alice then performs a local measurement and sends her result to Bob, who performs a conditional π-rotation of his qubit to obtain the state envisaged by Alice. In every run of the protocol a payoff function is evaluated, which is essentially given by the quantum state fidelity of the experimentally created state with the theoretical one. To assess different resource states according to their suitability for RSP, we investigated the fidelity of the protocol, which we defined as the minimum over the achievable payoff, to cover also the worst cases.

We identify quantum discord as the crucial resource for remote state preparation. We find that for a broad class of states the fidelity of RSP is directly given by the geometric measure of quantum discord [2]. These states are described by a local Bloch vector, which is parallel to the direction of the largest eigenvalue of $E^T E$, where E is the correlation tensor of the investigated two-qubit state. This class in particular includes the important sets of states with maximally mixed marginals as well as isotropically correlated states such as Werner states. This provides an operational meaning to quantum discord as a measure of the "quantumness" of correlations in quantum information. We further showed in theory and experiment, that separable, yet non-zero discord states can outperform entangled states in accomplishing RSP. This underlines that not entanglement, but quantum discord quantifies the non-classical correlations required for the task.
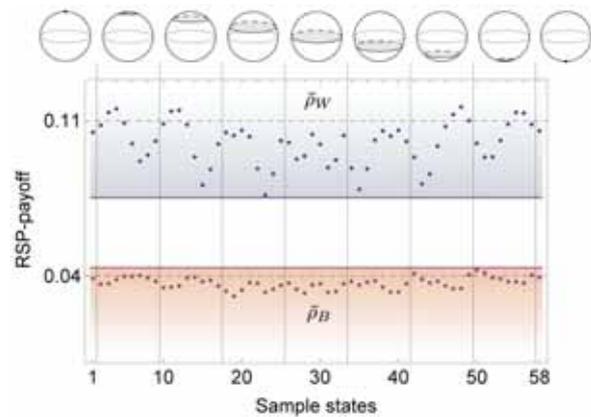
Figure 1: Shown are the experimentally achieved payoffs for the separable state $\tilde{\rho}_W$ and the entangled state $\tilde{\rho}_B$ as a resource in the RSP protocol. In both cases, Alice remotely prepared 58 distinct quantum states, evenly distributed on Bob's Bloch sphere. The visible separation of 0.0434 ± 0.0007 confirms the better performance of the separable, yet higher discord state $\tilde{\rho}_W$ by 62 standard deviations.

References

[1] H. Ollivier, W. H. Zurek, Phys. Rev. Lett., **88**, 017901 (2001)

[2] B. Dakic, V. Vedral, and C. Brukner, Phys. Rev. Lett., **105**, 190502 (2010)

Photonic platform for experiments in higher dimensional quantum systems

Christoph Schaeff, Robert Polster, Radek Lapkiewicz, Robert Fickler, Sven Ramelow, and Anton Zeilinger

Institute for Quantum Optics and Quantum Information
Boltzmanngasse 3, 1090 Vienna, Austria
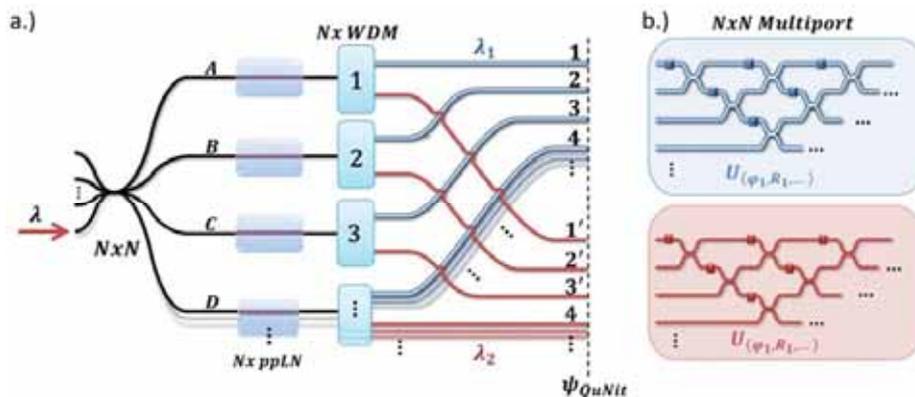
Schematic of the experiment. The realization using a 4-level system (ququarts) is shown explicitly, a possible extension to higher-dimensional systems is indicated. **a.)** Scalable in-fiber source for creating two path-entangled ququarts: 4 non-linear crystals for spontaneous parametric down-conversion are pumped coherently by a common pump beam. This leads to a superposition of the down-conversion process happening in on of the four crystals. Separation of the photon pair by wavelength leads to an entangled ququart state. **b.)** Each ququart enters a Multiport consisting out of combinations of beam splitters and phase shifters. By choosing the corresponding phases and reflectivities any unitary transformation can be realized in any dimension.

The aim of our work is to access and explore higher dimensional photonic quantum systems. In terms of stability and complexity normal bulk-optic setups greatly limit the capabilities of reaching higher dimensional systems. However, the rapid development in integrated photonic circuits in recent years opens new possibilities [1]. Our approach is to use integrated photonic circuits on-chip as well as in fiber to reach photonic states of higher dimension.

We are working on a fully integrated realization of a device called a Multiport (Fig. b) [2] capable of applying any unitary transformation depending on its internal (tunable) parameters. The basic unit of the Multiport is a QuBit operation consisting of one phase shifter and one (integrated) beam splitter. Combining a certain number of QuBit operations at different settings results in a specific unitary transformation on the full Hilbert Space in any dimension. Furthermore, we have built an integrated source using purely in-fiber components for creating higher dimensional path-entangled photons (Fig. a). Due to its special design it allows good scalability in terms of complexity with increasing dimension of the photonic system.

Combining the source and the Multiport results in a very general platform for experiments in higher dimensional Hilbert spaces. By externally setting the device to a variety of different incoming entangled states followed by applying any desired unitary transformation, different experimental setups can be realized. Possible experiments range from fundamental questions of quantum information [3] to interesting applicational possibilities due to the compatibility to telecom technology and fiber networks.

[1] Alberto Peruzzo, Anthony Laing, Alberto Politi, Terry Rudolph and Jeremy L. O'Brien,
    Nature Communications **2**, 224 (2011).
[2] M.Reck and A.Zeilinger, PRL Vol.73, No.1 (1994)
[3] M.Zukowski, A.Zeilinger and M.A.Horne, PRA Vol.55, No.1 (1997)

A 2D Quantum Walk Simulation of Two-Particle Dynamics

A. Schreiber[1,2]**, A. Gábris**[3]**, P. P. Rohde**[1,4]**, K. Laiho**[1,2]**, M. Štefaňák**[3]**, V. Potoček**[3]**, C. Hamilton**[3]**, I. Jex**[3] **and C. Silberhorn**[1,2]

[1]*Applied Physics,University of Paderborn, Paderborn, Germany*
[2]*Max Planck Institute for the Science of Light, Erlangen, Germany.*
[3]*Department of Physics, FNSPE, Czech Technical University in Prague, Praha, Czech Republic*
[4]*Centre for Engineered Quantum Systems, Department of Physics and Astronomy, Macquarie University, Sydney, Australia*

In recent years quantum walks have been found to be a promising candidate for quantum computation and quantum simulations of complex physical phenomena. Although theoretical models already exploit the high potential of nontrivial graph structures experiments are still restricted to evolution in one dimension due to the large amount of required physical resources. Here we present an experimental implementation of photonic quantum walks on a 2D grid, allowing for a coherent evolution over 12 steps and 169 positions [1]. By controlling the underlying conditions of the quantum walk we were able to simulate the creation of bipartite entanglement with conditioned interactions. Dynamic manipulations during the propagation enabled us to investigate the behavior of two interacting particles forming a bound state.

We implemented 2D quantum walks with a coherent laser pulse traveling through an optical fiber network (Fig.1a). To circumvent the drastic increase of physical resources with the number of steps we employed the time-multiplexing technique [2]. With each round trip in the setup the pulse can travel four paths of different lengths corresponding to the four directions possible in a 2D quantum walk. The initial pulse spreads across discrete time bins, with each time bin corresponding to a specific vertex on the spatial grid (Fig.1b). The direction of each step is determined by the coin states $|c_{1,2}\rangle$ for dimensions one and two, given by polarization and spatial modes of the pulse. With half-wave plates (HWP) and a fast electro-optic modulator (EOM) we were able to switch between various different coin operations. While quantum coins acting on both coin states independently lead to a separable arrival distribution concerning the two dimensions, quantum walks with controlled operations show strong spatial correlations. We reconstructed the final probability distributions by measuring the polarization and timing informations of the photons with four avalanche photo diodes (APDs).

One of the major advantages of 2D quantum walks is the possibility to simulate two-particle dynamics with controlled interactions. One quantum walker on a 2D lattice is topologically equivalent to two particles evolving on a 1D line, with the coin states $|c_{1,2}\rangle$ corresponding to the coin states of particles one and two. Hence, with controlled operations acting on both coin states we are able to simulate the behavior of two particles interacting with each other. Measuring the position of the walker on the 2D grid is equivalent to a coincidence measurement of both particles on the line.

An example of two-particle quantum walks with strong nonlinearities can be seen in Fig.1c, showing coincidence probabilities of two scattering bosons. Here the particles only interact when meeting at the same position. This Bose-Hubbard type nonlinearity was found to create bound molecule states [3], resulting in strong particle bunching.
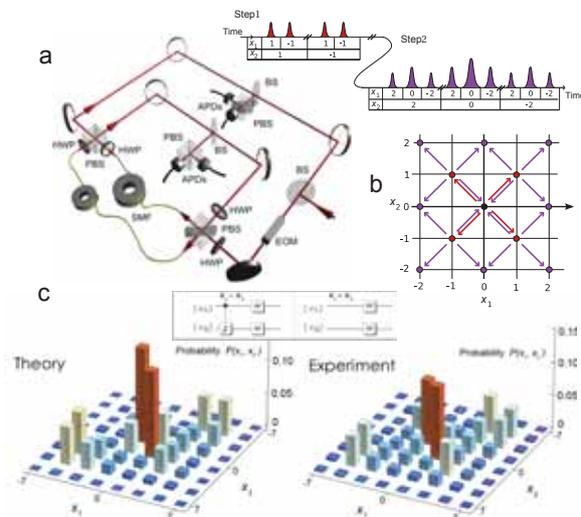
Figure 1: (**a**) Schematic of the setup. A coherent laser pulse is send to two single-mode fibers (SMF) of different lengths inducing a temporal shift for a vertical step and subsequently to two free space paths for the horizontal step respectively. Each time bin of the created pulse train corresponds to a spatial position in the 2D quantum walk (**b**). After multiple round trips several pulses overlap temporarily, allowing for interference effects. (**c**) Probability distribution for two simulated bosons after seven steps of a quantum walk. A controlled-phase interaction is applied only when both particles meet, mimicking a scattering effect. The bosons tend to arrive at the same position (diagonal) as a result of creating a bound state.

The analogy between classical and quantum coherence allowed us to demonstrate archetypal quantum phenomena with a system using a classical light source. Our experiment is a perfect testbed for future studies of complex quantum phenomena based on quantum interference, as for example higher dimensional Anderson localization [4]. While being important for simulation applications, our experiment is equally interesting for understanding the connection between classical and quantum coherence theory.

References

[1] A. Schreiber *et al.*, Science
    DOI: 10.1126/ science.1218448, (2012)

[2] A. Schreiber *et al.*, Phys. Rev. Lett. **104**, 05502 (2010)

[3] A. Ahlbrecht *et al.*, arxiv: quant-ph/1105.1051 (2011)

[4] A. Schreiber *et al.*, Phys. Rev. Lett. **106**, 180403 (2011)

Permutationally invariant tomography of symmetric Dicke states

Christian Schwemmer[1,2], Géza Tóth[3,4,5], Alexander Niggebaum[1,2], Tobias Moroder[6], Philipp Hyllus[3], Otfried Gühne[6] and Harald Weinfurter[1,2]

[1]Max-Planck-Institut für Quantenoptik, Garching, Germany
[2]Fakultät für Physik, Ludwig-Maximilians-Universität, München, Germany
[3]Department of Theoretical Physics, The University of the Basque Country, Bilbao, Spain
[4]IKERBASQUE, Basque Foundation for Science, Spain
[5]Research Institute for Solid State Physics and Optics, Hungarian Academy of Sciences, Budapest, Hungary
[6]Department für Physik, Universität Siegen, Germany

Multi-partite entangled quantum states are a crucial prerequisite for potential applications like quantum metrology or quantum communication. Therefore, practical tomographic schemes for analyzing these states are needed which provide an appropriate data acquisition protocol and enable approximate state reconstruction from an incomplete set of measurements. For standard quantum state tomography the measurement effort scales exponentially with the number of qubits. Moreover, also non-linear optimization on an exponentially increasing set of data required for typical state reconstruction becomes a challenging task itself. Hence the limit of the standard approach will soon be surpassed.

Recently, we developed a method where the measurement effort under the restriction of permutational invariance scales only polynomially [1]. This is of great importance since many prominent quantum states, like for example GHZ states, symmetric Dicke states or W states are permutationally invariant. A further advantage of our method is that the single qubits do not have to be individually manipulable since for each basis setting the same local measurement is applied to all qubits. The highest accuracy of our scheme is achieved when the basis settings are evenly distributed on the Bloch sphere (see Fig. 1).
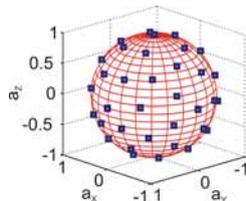
Figure 1: Optimized measurement settings visualized on the Bloch sphere. Each point on the sphere (a_x, a_y, a_z) corresponds to the projection measurements $\frac{1}{2}(\mathbf{1} \pm a_i \sigma_i)$ with $i = \{x, y, z\}$.

Our state reconstruction algorithm is tailored to the permutational invariant nature of the problem leading to a drastic reduction of its dimensionality. Additionally, it employs convex optimization [3] making it superior to other numerical optimization methods in terms of speed, accuracy and control. It is applicable for the most common reconstruction principles like maximum likelihood and least squares methods. Our simulations show that state reconstruction of 20 qubits can be done within 20 minutes on an ordinary computer.

Here, we present experimental results of the tomographic analysis of a photonic six-qubit symmetric Dicke state as observed with our high-rate multi-photon set-up [2]. Instead of $3^6 = 729$ basis settings for full tomography only 28 basis settings for permutationally invariant tomography have to be measured. Our tomographic analysis of the experimental state, observing the state with a fidelity of $65.7\% \pm 1.0\%$, clearly reveals all the characteristic features including effects of higher order noise typical for such multi-photon sources (see fig. 2).
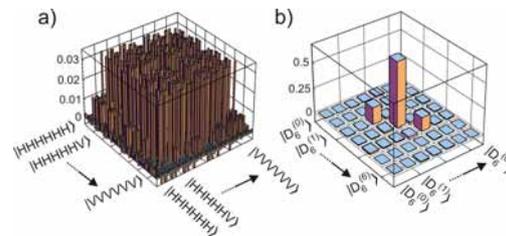
Figure 2: Real part of the computational basis (a) and the symmetric subspace (b) of the experimental state after applying our reconstruction algorithm. The count rate was $2.3\,\mathrm{min}^{-1}$ at a UV pump power of $3.7\,\mathrm{W}$. The fidelity with respect to the theoretical state is $65.7\% \pm 1.0\%$. The central bar of the symmetric subspace can be associated with the ideal state and the small bars next to it can be associated with higher order noise.

Our experiment shows clearly that when restricting to the permutational invariant subspace a detailed analysis of states of very high qubit number is feasible both in terms of data acquisition and data processing.

References

[1] G. Tóth, W. Wieczorek, D. Gross, R. Krischek, C. Schwemmer and H. Weinfurter, Phys. Rev. Lett. **105**, 250403 (2010).

[2] R. Krischek, W. Wieczorek, A. Ozawa, N. Kiesel, P. Michelberger, T. Udem and H. Weinfurter, Nature Photonics **4**, 170-173 (2010).

[3] S. Boyd and S. Vandenberghe, *Convex Optimization*, Cambridge Universtiy Press, (2004).

Integrated photonic quantum gates for polarization qubits

L. Sansoni[1], **I. Bongioanni**[1], **F. Sciarrino**[1,2], **G. Vallone**[1,*], **P. Mataloni**[1,2], **A. Crespi**[3,4], **R. Ramponi**[3,5] and **R. Osellame**[3,4]

[1]*Dipartimento di Fisica, Sapienza Università di Roma, Piazzale Aldo Moro, 5, I-00185 Roma, Italy*
[2]*Istituto Nazionale di Ottica, Consiglio Nazionale delle Ricerche (INO-CNR), Largo Enrico Fermi, 6, I-50125 Firenze, Italy*
[3]*Istituto di Fotonica e Nanotecnologie, Consiglio Nazionale delle Ricerche (IFN-CNR), Piazza L. da Vinci, 32, I-20133 Milano, Italy*
[4]*Dipartimento di Fisica, Politecnico di Milano, Piazza Leonardo da Vinci, 32, I-20133 Milano, Italy*
[*]*present address: Department of Information Engineering, University of Padova, I-35131 Padova, Italy*

In the last few years photonic quantum technologies have been adopted as a promising experimental platform for quantum information science. The realization of complex optical schemes consisting of many elements requires the introduction of waveguide technology to achieve desired scalability, stability and miniaturization of the device. Recently, silica waveguide circuits on silicon chips have been employed in quantum applications to realize stable interferometers for two-qubit entangling gates. Such approach with qubits encoded into two photon optical paths yielded the first demonstration of an integrated linear optical controlled-NOT (CNOT) gate [1]. However, many quantum information pro-

Figure 1: (a) Scheme of the integrated CNOT gate, (b) measured truth table, (c) measured probabilities of the output Bell states corresponding to the different input separable states.

cesses and sources of entangled photon states are based on the polarization degree of freedom, which allows one to implement quantum operations without the need of path duplication and thus with the simplest and most compact circuit layout. Femtosecond laser written waveguides have been demonstrated to be able to support and manipulate the polarization degree of freedom [2]. Here we report on the first integrated photonic CNOT gate for polarization-encoded qubits and on the complete characterization of its quantum behaviour. The demonstration of this quantum gate has been made possible by the fabrication in a glass chip of integrated devices acting as partially polarizing beam splitters (PPBSs). Precisely, we show that femtosecond laser writing enables direct inscription of directional couplers with fine and independent control on the splitting ratio for the horizontal (H) and vertical (V) polarizations [3]. PPBSs have been realized with the directional coupler geometry: two distinct waveguides

are brought close together for a certain propagation length, called interaction length, so that the two propagating modes become coupled through evanescent field overlap. Thanks to the low but not zero glass birefringence different splitting ratios for horizontal and vertical polarization can be achieved by varying the interaction length of the directional coupler. This technology can be exploited to realize quantum optical gates. In the polarization-encoding approach, a generic qubit $\alpha|0\rangle + \beta|1\rangle$ is implemented by a coherent superposition of H and V polarization states, $\alpha|H\rangle + \beta|V\rangle$, of single photons. The most commonly exploited two-qubit gate is the CNOT that flips the target qubit (T) depending on the state of the control qubit (C). The CNOT action is described by a unitary transformation acting on a generic superposition of two qubit quantum states. In the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ for the systems C and T, the matrix associated to the CNOT is:

$$\mathcal{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1}$$

A striking feature of this gate is given by the ability to entangle and disentangle qubits. We realized a CNOT gate composed by a cascade of PPBSs arranged as in the scheme shown in Fig. 1(a). First of all, by injecting in the device two-photon states, we measured the truth table as reported in Fig. 1(b) obtaing a fidelity of $\mathcal{F} = 0.970 \pm 0.008$, furthermore we exploited the CNOT as an entangling and disentangling gate: we injected the four separable states $|\pm\rangle_{\mathsf{C}}|0\rangle_{\mathsf{T}}$ and $|\pm\rangle_{\mathsf{C}}|1\rangle_{\mathsf{T}}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, which evolve into the entangled Bell states $|\Phi^\pm\rangle$ and $|\Psi^\pm\rangle$ and performed tomographic reconstructions of the output states (Fig. 1(c)). Finally, in order to completely characterize the gate, we performed a quantum process tomography [4] of the gate obtaining a process fidelity between the reconstructed map and the expected one of $\mathcal{F}_{\mathcal{CNOT}} = 0.906 \pm 0.003$.

The present results open new perspectives towards joint integrated handling of hybrid quantum states based on different degrees of freedom of light, such as polarization, path and orbital angular momentum

References

[1] A. Politi *et al.*, Science **325**, 1221 (2009).

[2] L. Sansoni *et al.*, Phys. Rev. Lett. **105**, 200503 (2010).

[3] A. Crespi *et al.*, Nat. Comm. **2**, 566 (2011).

[4] I. Bongioanni *et al.*, Phys. Rev. A **82**, 042307 (2010).

Silicon Quantum Photonic Technology Platform: Sources & Circuits

Damien Bonneau[1], **Erman Engin**[1], **Josh Silverstone**[1], **Chandra M. Natarajan**[2], **M. G. Tanner**[2], **R. H. Hadfield**[2], **Sanders N. Dorenbos**[3], **Val Zwiller**[3], **Kazuya Ohira**[4], **Nobuo Suzuki**[4], **Haruhiko Yoshida**[4], **Norio Iizuka**[4], **Mizunori Ezaki**[4], **Jeremy L. OBrien**[1], **Mark G. Thompson**[1]

[1]*Centre for Quantum Photonics, Department of Electrical and Electronic Engineering, University of Bristol, Bristol, UK*

[2]*Scottish Universities Physics Alliance & School of Engineering & Physical Sciences, Heriot-Watt University, Edinburgh, UK*

[3]*Kavli Institute of Nanoscience, TU Delft, The Netherlands*

[4]*Corporate Research & Development Center, Toshiba Corporation, Japan*

Since the first demonstration of the on-chip CNOT gate [1] in a silica-on-silicon waveguide circuit, there has been a growing interest in more complex and miniaturised on-chip quantum integrated circuits (QIC) where both generation, routing and manipulation of photons could be realised. In this regard, silicon photonics is a promising material platform. It presents a very high index contrast, enabling the guidance of light around sharp bends, mature fabrication technology, and CMOS compatibility. In addition, silicons large χ^3 non-linearity can be utilized to generate photon pairs through spontaneous four-wave-mixing (sFWM) on chip, allowing us to miniaturise another important quantum optical element. In this study we present the basic building blocks of a linear-optical quantum circuit, namely the beam-splitter and Mach-Zender interferometer (MZI), as well as a bright and high-CAR (coincidence-to-accidental ratio) photon pair source based on a micro-ring resonator. The circuits and sources are fabricated on the same layer structure hence can be easily integrated. The beamsplitter operation are implemented with multimode-interference (MMI) couplers having a footprint of $27x2.8\mu m^2$. As a proof of principle demonstration we have performed Hong-Ou-Mandel (HOM) interference measurements realising an intrinsic non-classical visibility of $88 \pm 3\%$. We developed a theoretical model to account for loss inside the MMI and the probability of multiphoton events of the photon source, with good agreement with the measured results [2]. We also designed an MZI composed of two cascaded MMIs separated by a phase shifter as shown in Fig.1(a). We observed two-photon interference fringes as shown in Fig.1(b), which beats the shot-noise limit of the classical measurement. Photon pair generation in silicon nano-wires (SinW) has been studied by several groups and proven to perform better than fibre based sources working at cryogenic temperatures [3]. A major problem with high-power applications in SinWs is a reduced pair production rate resulting from the free-carrier absorption (FCA) induced by two-photon absorption (TPA). Here we have used a ring resonator to enhance the pump intensity inside the SinW to improve the pair generation rate, and we have also successfully demonstrated FCA suppression by integrating a reverse-biased p-i-n junction around each ring to sweep free-carriers from the SinW and suppress FCA. The setup is shown in Fig.1(c). Fig.1(d) shows the on-chip pair production rate (compensating for detection and collection efficiencies) and the CAR for various input powers to the device. We consider three cases: detuned, where we pump the ring off-resonance, no power couples into the ring, and the pairs are only generated in the straight bus waveguide; tuned, where the pump is resonant with the ring, and optical energy builds up within
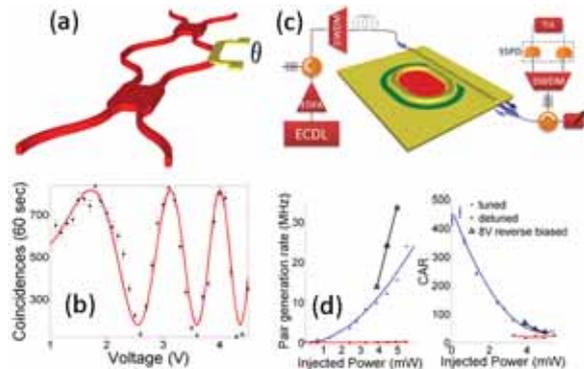
Figure 1: (a) Illustration of the MZI made of two cascaded MMIs. (b) Measured two photon interference fringes. (c) Setup diagram for photon pair generation in silicon ring resonator. (d) Coincidence counts and CAR versus input power

it, and; reverse biased, where an 8-V reverse bias is applied across a p-i-n junction straddling the ring, while the pump is on-resonance. The pair generation rates were found to be 15 KHz/mW^2 for the detuned and 713 KHz/mW^2 for the tuned case which implies a 47-fold enhancement in the pair generation rate due to the presence of the ring. On the other hand when reverse biased we achieve up to a 2.1 times increase in the number of photon pairs generated, while preserving the CAR. The maximum achieved CAR was 456 ± 18, obtained in tuned case for low pump powers. In summary, we have studied fundamental components for integrated quantum photonics sources and circuits, demonstrating the potential of silicon photonics as a promising platform for future integrated quantum photonic technologies.

References

[1] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, "Silica-on-Silicon waveguide quantum circuits," Science 320 (5876), 646-649 (2008).

[2] D. Bonneau et al., "Quantum interference and manipulation of entanglement in silicon wire waveguide quantum circuits," New Journal of Physics (to be published).

[3] K.-i. Harada, H. Takesue, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, Y. Tokura, and S.-i. Itabashi, "Generation of high-purity entangled photon pairs using silicon wirewaveguide," Opt. Express 16 (25), 20 368-20 373 (2008).

3D integrated photonic quantum interferometry

Nicolò Spagnolo[1], **Lorenzo Aparo** [1], **Chiara Vitelli**[1], **Andrea Crespi**[2,3], **Roberta Ramponi**[2,3], **Roberto Osellame**[2,3], **Paolo Mataloni**[1,4] **and Fabio Sciarrino**[1,4]

[1]*Dipartimento di Fisica, Sapienza Università di Roma, Rome, Italy*
[2]*Istituto di Fotonica e Nanotecnologie, Consiglio Nazionale delle Ricerche (IFN-CNR), Milano, Italy*
[3]*Dipartimento di Fisica, Politecnico di Milano, Milano, Italy*
[4]*Istituto Nazionale di Ottica (INO-CNR), Firenze, Italy*

One of the main features of quantum mechanics is represented by quantum interference which derives from the superposition principle and characterizes the interaction between coherent quantum systems. In this perspective the capability of getting the interference of more than two photons on a beam splitter is a challenging task both for observing quantum phenomena in systems with increasing size and for engineering quantum states. The concept of a tritter, that is, the three-mode extension of the two-mode conventional beam-splitter was first pointed out by Greenberger, Horne and Zeilinger [1]. Such device can be realized by the combination of two port beam splitters and phase shifters. However, in the perspective of a generalization of this device to n modes, a bulk approach leads to complex interferometric structures. Recently, a strong research effort has been devoted to integrated photonic technology, leading to promising results for the implementation of complex, intrinsically stable, integrated multimode-multiphoton interferometers.

Here, we first address the main features of an integrated tritter based on a 3D multi-waveguide directional coupler, a structure in which the waveguides are brought close together for a certain interaction length, and are coupled by evanescent fields. The tritter device can be realized by adopting femtosecond laser writing technology [2], which can be adopted to produce integrated devices with a 3D structure. Referring to our scheme, we investigate the case when three photons are simultaneously injected in the three input waveguides. The triangular geometry of the tritter allows to consider the evolution of the three photons, without decomposing the overall interaction into the mutual two-photon beam splitter interaction [Fig. 1 (a)]. Within this scenario we investigate the quantum features of the output fields arising from the injection of Fock states and compare the obtained results with the classical ones.

We then introduce the concept of three-dimensional (3D) interferometry [3]. We investigate the use of tritter within novel interferometric schemes, demonstrating relevant metrological advantages for phase estimation tasks [Fig. 1 (b)]. In this context, the aim is to measure an unknown phase shift ϕ introduced in an interferometer with the best possible precision by probing the system with a N-photon state, and by measuring the resulting output state. The classical limit is provided by the stantard quantum limit (SQL), which sets a lower bound to the minimum uncertainty $\delta\phi_{\mathrm{SQL}} \geq 1/\sqrt{MN}$ which can be obtained on ϕ by exploiting classical N-photon states on two modes and M repeated measurements. Recently, it has been shown that the adoption of quantum states can lead to a better scaling with N, setting the ultimate precision to $\delta\phi_{\mathrm{HL}} \geq 1/(\sqrt{M}\, N)$, corresponding to the Heisenberg limit. We show that the present integrated technology can lead to a sub-SQL performance in the estimation of an optical phase, exploiting multi-mode interferometry. To this end, we provide a complete numerical simulation of a phase estimation strategy which can saturate the maximum attainable measurement precision, quantified by the quantum Fisher information, which allows to overcome the SQL achievable with classical fields. The same results are then extended to a four-mode interferometer, which can be built by using two cascaded four-modes splitters (a tetrater).

The present technology can lead to the development of new phase estimation protocols able to reach Heisenberg-limited performances, and to the simultaneous measurement of more than one optical phase. Further perspectives may lead to the application of this multiport splitters in other contexts. These include the realization of "proof-of-principle" quantum simulators, the implementation of linear-optical computational tasks beyond the one of a classical computer, and the implementation of fundamental tests of quantum mechanics, such as nonlocality tests, for increasing dimensionality quantum systems.

References

[1] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Fortschr. **48**, 243 (2000).

[2] G. Della Valle, R. Osellame, and P. Laporta, Journal of Optics A, **11**, 013001 (2009).

[3] N. Spagnolo, L. Aparo, C. Vitelli, A. Crespi, R. Ramponi, R. Osellame, P. Mataloni, and F. Sciarrino, submitted (2012).
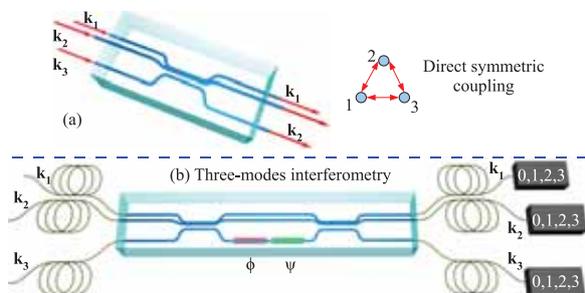
Figure 1: (a) Integrated 3-dimensional three-mode beam-splitter. (b) 3-dimensional interferometer built by using two cascaded tritters.

QCMC 2012
Vienna, Austria

Generating non-Gaussian states using collisions between Rydberg polaritons

Jovica Stanojevic[1], **Valentina Parigi**[1], **Erwan Bimbard**[1], **Alexei Ourjoumtsev**[1], **Pierre Pillet**[2] and **Philippe Grangier**[1]

[1]*Laboratoire Charles Fabry, Institut d'Optique, CNRS, Univ Paris-Sud, Palaiseau, France*
[2]*Laboratoire Aimé Cotton, Univ Paris-Sud, Orsay, France*

We investigate the deterministic generation of quantum states with negative Wigner functions which arise due to giant non-linearities originating from collisional interactions between Rydberg polaritons. The state resulting from the polariton interactions may be transferred with high fidelity into a photonic state, which can be analyzed using homodyne detection followed by quantum tomography. We obtain simple analytic expressions for the evolution of polaritonic states under the influence of Rydberg-Rydberg interactions. In addition to generating highly non-classical states of the light, this method can also provide a very sensitive probe of the physics of the collisions involving Rydberg states.

Qudits implementation with broadband entangled photons

André Stefanov[1]**, Christof Bernhard**[1]**, Bänz Bessire**[1]**, and Thomas Feurer**[1]

[1]*Institute of Applied Physics, University of Bern, Switzerland*

Entanglement is a fundamental resource for the quantum processing of information and to study the fundamental nature of quantum correlations. Entangling higher dimensional bipartite systems (qudits) has been shown to give more insight on the nature of entanglement compared to the simplest entanglement system composed of two two level systems (two qubits) [1, 2]. For quantum key distribution, increasing the dimension of the alphabet by using qudits increases the effective bit rate of the protocol, still being secure [3]. Experimentally, higher dimensional entanglement in photonic systems have been demonstrated for various degrees of freedom of light. Entangled qudits can be implemented in the timing of entangled photons [4, 5, 6], in the transverse momentum [7, 8] or in orbital angular momentum modes [9].

Here we propose and demonstrate the ability to encode qudits in the energy spectrum of entangled photon.

When pumped by a CW laser, broadband entangled photons generated by parametric down-conversion show strong correlations in their energies. With methods used for pulse shaping of fs laser pulses, it is possible to arbitrarily shape the two photon wave function [10]. A spatial light modulator (SLM) allows to individually change the phase and transmission of each component of the spectrum, which has been spatially separated by a prism compressor (Fig. 1). By discretizing the energy spectrum of the photons into energy bins, the following state is generated

$$
\begin{aligned}
|\psi\rangle &= \sum_{i=0}^{n} c_i \, |\omega_{cp} - \Omega_i\rangle_i \, |\omega_{cp} + \Omega_i\rangle_s \\
&= \sum_{i=0}^{n} c_i \, |i\rangle_i \, |i\rangle_s
\end{aligned}
$$

where ω_{cp} is the central energy of the photons spectrum and the coefficients c_i are controlled by the SLM. It is thus possible to generate non-maximally entangled qudits which have been shown to be of great interest for Bell inequalities violations.

The dimension of the spanned Hilbert space n is in principle only limited by the bandwidth of the pump laser, this sets the smallest width of each frequency bin. In practice the finite point spread function of the optical system together with the pixel size of the SLM are limiting the effective useful dimension of the Hilbert space.

We show experimental violation of Bell inequalities for qubits and qutrits and study the violation of Bell inequalities as a function of the entanglement. We show ongoing work towards the realization of states with larger dimension.

Figure 1: Setup of the experiment: Broadband entangled photons are generated in a PPKTP crystal, their spectrum is shaped by a SLM and the coincidences are detected by upconversion in another PPKTP crystal.

References

[1] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, "Bell Inequalities for Arbitrarily High-Dimensional Systems," *Physical Review Letters*, vol. 88, pp. 2–5, Jan. 2002.

[2] T. Vértesi, S. Pironio, and N. Brunner, "Closing the Detection Loophole in Bell Experiments Using Qudits," *Physical Review Letters*, vol. 104, pp. 1–4, Feb. 2010.

[3] L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," *Physical Review A*, vol. 82, pp. 1–4, Sept. 2010.

[4] R. Thew, a. Acín, H. Zbinden, and N. Gisin, "Bell-Type Test of Energy-Time Entangled Qutrits," *Physical Review Letters*, vol. 93, pp. 1–4, July 2004.

[5] H. de Riedmatten, I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin, "Tailoring photonic entanglement in high-dimensional Hilbert spaces," *Physical Review A*, vol. 69, pp. 4–7, May 2004.

[6] D. Richart, Y. Fischer, and H. Weinfurter, "Experimental implementation of higher dimensional timeenergy entanglement," *Applied Physics B*, vol. 106, pp. 543–550, Jan. 2012.

[7] M. OSullivan-Hale, I. Ali Khan, R. Boyd, and J. Howell, "Pixel Entanglement: Experimental Realization of Optically Entangled d=3 and d=6 Qudits," *Physical Review Letters*, vol. 94, pp. 1–4, June 2005.

[8] a. Halevy, E. Megidish, T. Shacham, L. Dovrat, and H. Eisenberg, "Projection of Two Biphoton Qutrits onto a Maximally Entangled State," *Physical Review Letters*, vol. 106, pp. 11–14, Mar. 2011.

[9] A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson, "Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities," *Nature Physics*, pp. 1–12, May 2011.

[10] B. Dayan, A. Peer, A. Friesem, and Y. Silberberg, "Nonlinear Interactions with an Ultrahigh Flux of Broadband Entangled Photons," *Physical Review Letters*, vol. 94, pp. 2–5, Feb. 2005.

Generation of time-bin qubits for continuous-variable quantum information processing

Shuntaro Takeda, Takahiro Mizuta, Maria Fuwa, Jun-ichi Yoshikawa, Hidehiro Yonezawa, and Akira Furusawa

Department of Applied Physics, School of Engineering, The University of Tokyo, Tokyo, Japan

Among the various physical implementations of a qubit, the time-bin qubit is known as one of the most robust realizations [1]. It consists of two optical pulses separated temporally, and can be described as a superposition of a photon in either pulse: $|\psi\rangle = \alpha|0,1\rangle + \beta|1,0\rangle$. This qubit can be prepared and measured with pulsed lasers and photon-detections, and has been used as a key resource for quantum information processing, such as quantum cryptography and quantum teleportation [2, 3].

We have demonstrated a preparation scheme of arbitrary time-bin qubits using continuous-wave (CW) light. A strong point unique to our qubit is its coherence with the CW light source. Taking advantage of this, an analysis scheme via a CW dual-homodyne measurement was devised and implemented, which gave the complete characterization of the qubits with high efficiencies and fidelities. Unlike the photon-detection scheme where the vacuum $|0,0\rangle$ is neglected and the higher-photon-number components are projected into the qubit subspace spanned by $\{|0,1\rangle, |1,0\rangle\}$, our scheme enables the reconstruction of the complete two-mode density matrices of the quantum states.

Furthermore, our qubit is well compatible with deterministic continuous-variable (CV) quantum operations [4] due to its coherence with the CW light source. As an important example, it can be straightforwardly used as an input state for the CV quantum teleportation circuit reported in Ref. [5], since it has a single polarization and a frequency spectrum suitable for the circuit. This enables *unconditional* quantum teleportation of a qubit in which no post-selection is required. Our qubit should open the way for new approaches where more powerful quantum operations of a qubit are realized via CV-based circuits.

Our schematic (Fig. 1) is an extended version of the setup for generating single photons in Ref. [6]. The output beam of a weakly-pumped nondegenerate optical parametric oscillator is spatially divided onto signal and idler modes. By introducing a Mach-Zehnder interferometer with an optical delay in one arm, the photon-detection of the idler mode will produce a heralded time-bin qubit on the signal mode. The coefficients α and β of the qubit are determined by the splitting ratio and the recombining phase in the idler channel: these are experimentally tunable. The complete characterization of this qubit requires two-mode quadrature statistics at various phase sets. A dual homodyne measurement enabled this, and the maximum likelihood algorithm allows for the reconstruction of the two-mode density matrix.

We observed four types of qubits: $(|0,1\rangle \pm |1,0\rangle)/\sqrt{2}$ and $(|0,1\rangle \pm i|1,0\rangle)/\sqrt{2}$. A selection of the reconstructed density matrices are shown in Fig. 2. In addition to the qubit subspace where the information of the qubit is encoded, we can explicitly observe the vacuum and higher-photon-number contributions as well. The off-diagonal elements appear in the

imaginary part of Fig. 2, demonstrating the superposition of $|0,1\rangle$ and $|1,0\rangle$ at the target phase. The overall efficiency of the qubit subspace is estimated from four data sets as $78\pm1\%$. The average fidelity of each qubit with its target state is calculated as 0.992 ± 0.003 by extracting and renormalizing the 2×2 qubit submatrix. These results show the highly efficient and precise preparation of time-bin qubits.
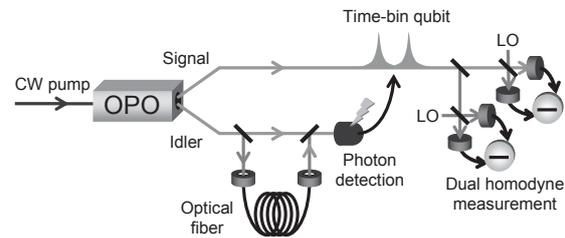
Figure 1: Experimental setup. CW, continuous wave; OPO, optical parametric oscillator; LO, local oscillator.
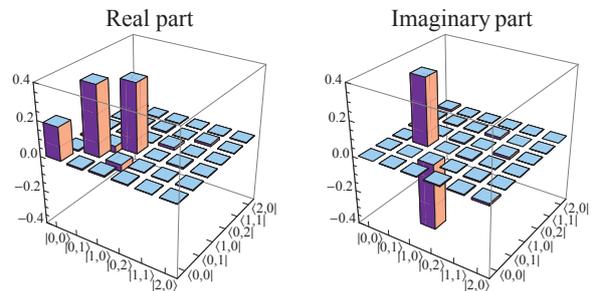
Figure 2: A selection of experimental density matrices. The target state is $|\psi\rangle = (|0,1\rangle - i|1,0\rangle)/\sqrt{2}$.

References

[1] W. Tittel and G. Weihs, Quant. Inform. Comput. **1**, 3 (2001).

[2] R. Hughes *et al.*, J. Mod. Opt. **47**, 533 (2000).

[3] I. Marcikic *et al.*, Nature **421**, 509 (2003).

[4] A. Furusawa and P. van Loock, *Quantum Teleportation and Entanglement: A Hybrid Approach to Optical Quantum Information Processing* (WILEY, 2011).

[5] N. Lee *et al.*, Science **332**, 330 (2011).

[6] J. S. Neergaard-Nielsen *et al.*, Opt. Exp. **15**, 7491 (2007).

Photonic multipartite entanglement conversion using nonlocal operations

T. Tashima[1], **M. S. Tame**[2], **Ş. K. Özdemir**[3], **M. Koashi**[4], **H. Weinfurter**[1]

[1] *Ludwig-Maximilians-Universität, München, Germany, Max-Planck-Institut für Quantenoptik, Garching, Germany*
[2] *Imperial College London, United Kingdom*
[3] *Washington University in St. Louis, St. Louis, USA*
[4] *Photon Science Center, The University of Tokyo, Tokyo, Japan*

Entanglement is at the heart of the power of quantum information processing and quantum computation. Two-qubit entanglement is well understood with good entanglement measures. Although there are a lot of work on entanglement measure, understanding multi-qubit entanglement remains a considerable challenge. There are many distinct classes for mutlipartite entanglement under local operation and classical communication (LOCC). Among these classes, it is well known that there are GHZ, W, Dicke and Cluster state classes. Gates to generate, to expand, and to fuse states of the same class have been studied [1-6]. On the other hand, it is also well known that these distinct classes cannot be interconverted under any LOCC, i.e., GHZ state cannot be converted into a W state. Recently Walther et al [4] experimentally demonstrated that $|W\rangle_3$ can be approximately generated from $|GHZ\rangle_3$ by LOCC. In this method, there is a trade-off between the success probability and the fidelity of the final state such that the fidelity approaches unity only in the limit of zero success probability, which reflects the fact that $|GHZ\rangle_3$ and $|W\rangle_3$ belong to distinct classes of states.

Here we show that conversion among distinct classes of multipartite entanglement can be achieved using a two qubit nonlocal operation implemented with a linear optics toolbox. In Fig. 1 (a), we show a schematic of a polarization dependent beamsplitter (PDBS) which could perform the conversion tasks. A tunable PDBS can be constructed using the scheme in the bottom of Fig. 1 (a), where the transmission and reflection coefficients of the PDBS are tuned with the help of two half-wave plates (HWP). Compared with a conversion of entangled states by a PDBS with fixed transmission and reflection coefficients, this conversion system enables one to select how to convert among GHZ, cluster and Dicke states. This gate translates the qubits encoded in the polarization degree of freedom of two photons in its input modes 1 and 2 to the output ports a and b as

$$
\begin{aligned}
|1_H\rangle_1|1_H\rangle_2 &\rightarrow \{\cos^2(2\theta_1) - \sin^2(2\theta_1)\}|1_H\rangle_a|1_H\rangle_b \\
|1_H\rangle_1|1_V\rangle_2 &\rightarrow -\sin(2\theta_1)\sin(2\theta_2)|1_V\rangle_a|1_H\rangle_b \\
&\quad +\cos(2\theta_1)\cos(2\theta_2)|1_H\rangle_a|1_V\rangle_b \\
|1_V\rangle_1|1_H\rangle_2 &\rightarrow \cos(2\theta_1)\cos(2\theta_2)|1_V\rangle_a|1_H\rangle_b \\
&\quad -\sin(2\theta_1)\sin(2\theta_2)|1_H\rangle_a|1_V\rangle_b \\
|1_V\rangle_1|1_V\rangle_2 &\rightarrow \{\cos^2(2\theta_2) - \sin^2(2\theta_2)\}|1_V\rangle_a|1_V\rangle_b
\end{aligned}
$$

If the input photons of the conversion gate are from the four-photon cluster state $|C_4\rangle = (|1_H\rangle_1|1_H\rangle_2|1_H\rangle_3|1_H\rangle_4 + |1_H\rangle_1|1_V\rangle_2|1_H\rangle_3|1_V\rangle_4 + |1_V\rangle_1|1_H\rangle_2|1_V\rangle_3|1_H\rangle_4 -$
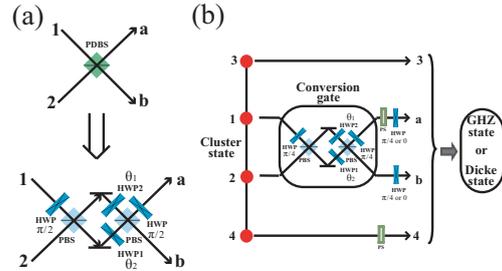
Figure 1: (a) Entanglement conversion gate. (b) Conversion scheme from a Cluster state to a Dicke or to a GHZ state.

$|1_V\rangle_1|1_V\rangle_2|1_V\rangle_3|1_V\rangle_4)/2$, the output becomes

$$
\begin{aligned}
|C_4\rangle \rightarrow &\{\cos^2(2\theta_1) - \sin^2(2\theta_1)\}|1_H\rangle_3|1_H\rangle_a|1_H\rangle_b|1_H\rangle_4 \\
&-\sin(2\theta_1)\sin(2\theta_2)|1_H\rangle_3|1_V\rangle_a|1_H\rangle_b|1_V\rangle_4 \\
&+\cos(2\theta_1)\cos(2\theta_2)|1_H\rangle_3|1_H\rangle_a|1_V\rangle_b|1_V\rangle_4 \\
&+\cos(2\theta_1)\cos(2\theta_2)|1_V\rangle_3|1_V\rangle_a|1_H\rangle_b|1_H\rangle_4 \\
&-\sin(2\theta_1)\sin(2\theta_2)|1_V\rangle_3|1_H\rangle_a|1_V\rangle_b|1_H\rangle_4 \\
&-\{\cos^2(2\theta_2) - \sin^2(2\theta_2)\}|1_V\rangle_3|1_V\rangle_a|1_V\rangle_b|1_V\rangle_4.
\end{aligned}
$$

The phase shifters (PS) at modes a and 4 are used to correct for the unwanted phases, whereas HWPs at modes a and b are used to manipulate the polarization of the photons in these modes. For example, by setting $1 - 2\sin^2(2\theta_1) = \sqrt{5}/5$ and $2\sin^2(2\theta_2) - 1 = \sqrt{5}/5$, and by rotating the polarization of the photons in modes a and b by $\pi/2$ one can prepare the four photon Dicke state $|D_4^2\rangle$ with two H and two V photons. The success probability of $|C_4\rangle \rightarrow |D_4^2\rangle$ conversion is $3/10$. On the other hand, if we choose $\theta_1 = 0$ and $\theta_2 = \pi/4$ and set HWPs at modes a and b such that they do not affect the polarizations of the photons, the output becomes the four-photon GHZ state $|GHZ_4\rangle = (|H\rangle_3|H\rangle_a|H\rangle_b|H\rangle_4 + |V\rangle_3|V\rangle_a|V\rangle_b|V\rangle_4)/\sqrt{2}$ with the success probability of $1/2$.

References

[1] W. Dür, et al. Phys. Rev. A **62**, 062314 (2000).

[2] P. Walther, et al. Phys. Rev. Lett. **94**, 240501 (2005).

[3] N. Kiesel, et al. Phys. Rev. Lett. **95**, 210502 (2005).

[4] W. Wieczorek, et al. Phys. Rev. Lett. **103**, 020504 (2009).

[5] T. Tashima, et al. Phys. Rev. Lett. **105**, 210503 (2010).

[6] S. K. Özdemir, et al. New J. Phys. **13**, 103003 (2011).

Spatial eigenmodes of traveling-wave phase-sensitive parametric amplifiers

Muthiah Annamalai,[1] **Nikolai Stelmakh,**[1] **Michael Vasilyev,**[1] **and Prem Kumar**[2]

[1]*Department of Electrical Engineering, University of Texas at Arlington, Arlington, TX, USA*
[2]*Center for Photonic Communication and Computing, EECS Department, Northwestern University, Evanston, IL, USA*

Spatially-broadband phase-sensitive optical parametric amplifiers (PSAs) are important tools of quantum information processing: they can generate multimode squeezed vacuum for parallel continuous-variable quantum information protocols [1] and can noiselessly amplify faint images [2, 3]. A precise knowledge of their spatial quantum correlations, however, is difficult to obtain because the traveling-wave PSAs use tightly focused pump beams: the resulting spatially-varying gain, together with the limited spatial bandwidth, couples and mixes up the modes of the quantum image.

We have recently found the orthogonal set of independently squeezed eigenmodes [4] of a traveling-wave PSA with spatially inhomogeneous pump by using the Hermite-Gaussian (HG) expansion [5, 6]. Such expansion reduces the PSA's partial differential equation to a system of coupled ordinary differential equations for the expansion coefficients $A_{mn}(z)$ over the HG_{mn} modes. The natural HG expansion basis has the signal waist $\sqrt{2}$ times wider than the pump waist to match the signal and pump beam curvatures. Examples of three eigenmodes are shown in Fig. 1 for circular (a,b; 200×200 μm pump waist) and elliptical (d,e; 800×50 μm pump waist) pumps at the same PSA gain of ~ 15 for the fundamental (most squeezed) eigenmode #0. The eigenmode profiles (a) and (d) resemble Laguerre-Gaussian (LG) and HG mode patterns, respectively, even though their representations (b) and (e) in our original HG basis look complicated.

Recently, we have found an optimal LG (for circular pump) or HG (for elliptical pump) expansion basis (whose waist size is no longer $\sqrt{2}$ times pump waist) for which the eigenmode representation is compact (see Fig. 1c and 1f, respectively). In such an optimal basis, all eigenmodes with gains within 3 dB from that of eigenmode #0 are represented by just a few HG or LG modes, with some eigenmodes closely matching one of the HG or LG modes (e.g., eigenmodes #0 and #5 shown in Fig. 1 have $> 96.5\%$ overlaps with one of LG or HG modes). This eigenmode structure of the PSA has recently been verified experimentally [7]. The PSA eigenmodes are closely related to the Schmidt modes of spontaneous parametric down conversion: at very low PSA gains, the eigenmodes correspond to frequency-degenerate transverse Schmidt modes.

The precise knowledge of the PSA eigenmodes will be important for optimizing parametric image amplifiers and multimode entanglement generators, and for generating matched local oscillators to optimally detect continuous-variable quantum information.

This work was supported by DARPA QSP Program.

Figure 1: PSA eigenmodes for circular (a–c) and elliptical (d–f) pump waists, in original (b,e) and compact (c,f) bases.

References

[1] V. Boyer, A. M. Marino, R. C. Pooser, and P. D. Lett, Science **321**, 544 (2008).

[2] S.-K. Choi, M. Vasilyev, and P. Kumar, Phys. Rev. Lett. **83**, 1938 (1999).

[3] E. Lantz and F. Devaux, J. Sel. Top. Quant. Electron. **14**, 635 (2008).

[4] M. Annamalai, N. Stelmakh, M. Vasilyev, and P. Kumar, Opt. Express **19**, 26710 (2011).

[5] C. Schwob *et al.*, Appl. Phys. B **66**, 685 (1998).

[6] K. G. Köprülü *et al.*, Phys. Rev. A **60**, 4122 (1999).

[7] G. Alon, O.-K. Lim, A. Bhagwat, C.-H. Chen, M. Annamalai, M. Vasilyev, and P. Kumar, in preparation.

Photon-Photon Interaction in Strong-Coupling Cavity-Quantum Dot System

Jian Yang and **Paul Kwiat**

University of Illinois at Urbana-Champaign, United States

The photon, as a fundamental information carrier, plays a critical role in quantum communication and quantum computation. Photon-photon interaction is essential to construct efficient quantum logic gates, but it is typically extremely weak in nonlinear media. Exploiting cavity-quantum dot (C-QD) interactions in the strong coupling regime, we found that photons with "time-reversed" [1] line-shapes of the C-QD emissions can excite the system with 100% efficiency. In this way, photons acquire strong and efficient interactions with each other, which could eventually possibly be used to build up the all optical switch [2, 3] down to single-photon level and quantum non-demolition (QND) measurement [4], a crucial building block for coherent state based multi-photon logic gate[5].
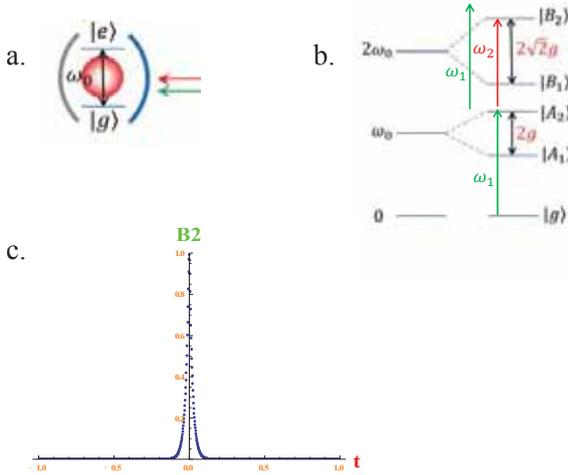
Figure 1: a. Schematic of resonant coupling between a single quantum dot and a single-sided single mode cavity. b. Nonlinear energy levels of C-QD system in dressed state in strong coupling regime. A_1 and A_2 form the first manifold of the dressed energy levels, while B_1 and B_2 form the second. c. Perfect excitation of the B_2 state by only two photons followed by subsequent decay out of this level. The two input photons are with the "time-reversed" line-shapes of the C-QD emissions from B_2 state.

As shown in Fig. 1a, a quantum dot, which is taken as a two-level system, is located inside a single-sided single-mode cavity. It is resonant with the cavity mode of ω_0. As a result, the effective Hamiltonian of the system can be written as

$$\widetilde{H} = \hbar g \left(a_c^\dagger \sigma_- + a_c \sigma_+ \right) +$$
$$+ \hbar \sqrt{\frac{\kappa}{2\pi}} \sum_{\omega_1} \left(a_c^\dagger a_{\omega_1} e^{i\Delta_1 t} + a_c a_{\omega_1}^\dagger e^{-i\Delta_1 t} \right) +$$
$$+ \hbar \sqrt{\frac{\kappa}{2\pi}} \sum_{\omega_2} \left(a_c^\dagger a_{\omega_2} e^{i\Delta_2 t} + a_c a_{\omega_2}^\dagger e^{-i\Delta_2 t} \right) \quad (1)$$

where g is the coupling rate between cavity and quantum dot, κ is the cavity decay rate, a_c is the cavity mode, $a_{\omega_{i(i=1,2)}}$ is the ith photon that coupled with cavity, and $\Delta_i = \omega_i - \omega_0 \, (i = 1, 2)$.

In the strong coupling regime where $g > \kappa$, Jaynes-Cummings energy levels exhibit high nonlinearity [6] to photon number at low photon numbers. As shown in 1b, the energy difference between the first manifold (A_2 and A_1) in dressed state is $2g$, while that between the second manifold (B_2 and B_1) is $2\sqrt{2}g$. Therefore, the "target" photon with the central frequency of $\omega_2 = \omega_0 + g \left(\sqrt{2} - 1 \right)$ can get inside the C-QD system only when the "control" photon with the central frequency of $\omega_1 = \omega_0 + g$ is already there. Furthermore, as shown in Fig. 1c, the probability to excite the C-QD to B_2 state would be 100%, if these two input photons have a "time-reversed" [1] line-shapes of the C-QD emissions from the B_2 state. As a result of strong interaction, each photon acquires a temporal delay that equal to their coherent time respectively. Therefore, by monitoring the arrival timing of the "target" photon, we can predict whether there is a "control" photon or not without measuring it, i.e., a QND measurement. Since the timing of the "target" photon is governed by the "control" photon, it is possible to realize an all-optical switch at the single-photon level.

References

[1] M. Stobiska, G. Alber and G. Leuchs, Perfect excitation of a matter qubit by a single photon in free space, EPL **86**, 14007 (2009).

[2] Vilson R. Almeida, Carlos A. Barrios, Roberto R. Panepucci and Michal Lipson, All-optical control of light on a silicon chip, Nature **431**, 1081 (2004).

[3] M. Bajcsy, S. Hofferberth, V. Balic, T. Peyronel, M. Hafezi, A. S. Zibrov, V. Vuletic, and M. D. Lukin, Efficient All-Optical Switching Using Slow Light within a Hollow Fiber, PRL **102**, 203902 (2009).

[4] G.J. Milburn and D.F. Walls, State reduction in quantum-counting quantum nondemolition measurements, PRA **30**, 56 (1984).

[5] W.J. Munro, K. Nemoto and T.P. Spiller, Weak nonlinearities: a new route to optical quantum computation, NJP **7**, 137 (2005).

[6] K.M. Birnbaum, A. Boca, R. Miller, A.D. Boozer, T.E. Northup and H.J. Kimble, Photon blockade in an optical cavity with one trapped atom, Nature **436**, 87 (2005).

Engineering a Factorable Photon Pair Source

Kevin Zielnicki[1] and **Paul Kwiat**[1]

[1]*University of Illinois, Urbana-Champaign, United States*

Pairs of polarization-entangled photons are a critical resource for optical quantum information processing. However, using spontaneous parametric downconversion (SPDC) to produce photon pairs can easily generate undesired correlations in frequency and spatial mode [1, 2]. Typical sources achieve high purity using spectral filtering, but this significantly decreases source brightness. Avoiding such filtering allows more efficient, brighter pair sources to be developed. This is particularly useful for creating multi-photon states, where the production rate enhancement scales exponentially in the number of photons. We have implemented a method using group-velocity matching and a broad-bandwidth pump to achieve a nearly indistinguishable source without the need for narrow spectral filtering. We discuss the design and characterization of this scheme.

A theoretical model from Vicent et al. provides the basis for the unentangled source [3]. By Taylor-expanding the phasematching function for type-I, non-collinear SPDC, one can obtain a set of conditions for factorability of the signal and idler modes, involving group velocity matching, pump focus and collection optimization, and an appropriate choice of a large pump bandwidth. We have focused on applying these conditions to type-I degenerate SPDC in β-barium borate (BBO) pumped with a pulsed 405-nm source, which is produced by frequency doubling an ultrashort pulsed 810-nm Ti-Sapphire laser.

(a)

(b)

Figure 1: a: Diagram of the 2D Fourier spectrometer. A polarization interferometer uses a half-wave plate (HWP) to rotate light into the diagonal basis, followed by birefringent quartz for a variable polarization-dependent phase offset. Two of these polarization interferometers are used to analyze the joint spectrum. b: Diagram of the two-source HOM interferometer using four-fold coincidence detection.

We employ two methods for characterizing our source, diagrammed in Figure 1. To measure the joint frequency spectrum from a single source of photon pairs, we use a modified version of the coincidence Fourier spectroscopy technique described by Wasilewski et. al. [4]. In the original scheme, scanning interferometers are placed in both the signal and idler arms, and coincidence counts are collected. The time-domain data collected by independently scanning the interferometers is then related to the joint spectrum by a two-dimensional Fourier transform. This procedure is time consuming compared to one dimensional Fourier spectroscopy, requiring N^2 rather than N points to obtain the same resolution. However, we can take advantage of the structure of the two-dimensional spectrum to measure the relevant parameters with a one-dimensional scan along the $t_s + t_i$ axis. The Fourier transform then gives the projection of the 2D spectrum along the $f_s + f_i$ axis. If we model the joint frequency spectrum as a 2D Gaussian ellipse, the relevant parameter for spectral correlation is the ratio of the $f_s + f_i$ and $f_s - f_i$ axes. This can be extracted directly from the 1D scan described above by simply measuring the widths of the peaks corresponding to these axes. Applying this technique to our source yields an implied heralded single photon purity of 0.96±0.02.

A second, more direct, measurement instead relies on interfering pairs photons produced from two independent sources. Pairs of photons are produced in orthogonally oriented crystals such that one produces horizontal polarized photons, and the other vertical. Two signal detectors herald the production of a single photon from each crystal. A variable amount of birefringent quartz introduces a relative time delay between the two photons in the idler path. The photons are then analyzed in the diagonal basis, where Hong-Ou-Mandel interference will lead to a suppression of coincidence counts if the photons arriving at the beamsplitter are indistinguishable. Thus, the visibility of the HOM dip in four-photon coincidence counts is determined by the heralded single-photon purity.

References

[1] W. P. Grice, A. B. U'ren, and I. A. Walmsley, Phys. Rev. A, **64**, 63815 (2001).

[2] A. B. U'Ren, K. Banaszek, and I. A. Walmsley, Quantum Inf. Comput. **3**, 480-502 (2003).

[3]] L. E. Vicent, A. B. U'Ren, R. Rangarajan, C. I. Osorio, J. P. Torres, L. Zhang, and I. A. Walmsley, New J. Phys. **12**, 093027 (2010).

[4] W. Wasilewski, P. Wasylczyk, P. Kolenderski, K. Banaszek, and C. Radzewicz, Opt. Lett. **31**, 1130-1132 (2006).

Spin-orbit-induced strong coupling of a single spin to a nanomechanical resonator

András Pályi[1], Philipp R. Struck[2], Mark Rudner[3], Karsten Flensberg[4] and Guido Burkard[2]

[1]*Institute of Physics, Eötvös University, Budapest, Hungary*
[2]*University of Konstanz, Germany*
[3]*Ohio State University, US*
[4]*Niels Bohr Institute, Copenhagen, Denmark*

Recent experiments in nanomechanics have reached the ultimate quantum limit by cooling a nanomechanical system close to its ground state [1]. Among the variety of available nanomechanical systems, nanostructures made out of atomically-thin carbon-based materials such as graphene and carbon nanotubes (CNTs) stand out due to their low masses and high stiffnesses. These properties give rise to high oscillation frequencies, potentially enabling near ground-state cooling using conventional cryogenics, and large zero-point motion, which improves the ease of detection.

Recently, a high quality-factor suspended CNT resonator was used to demonstrate strong coupling between nanomechanical motion and single-charge tunneling through a quantum dot (QD) defined in the CNT [2]. In the present work [3], we theoretically investigate the coupling of a single electron spin to the quantized motion of a discrete bending mode of a suspended CNT (see Fig.1), and show that the strong-coupling regime of this Jaynes-Cummings-type system is within reach. This coupling provides means for electrical manipulation of the electron spin via microwave excitation of the CNT's bending mode, and leads to strong nonlinearities in the CNT's mechanical response which may potentially be used for enhanced functionality in sensing applications.

In addition to their outstanding mechanical properties, carbon-based systems also possess many attractive characteristics for information processing applications. The potential for single electron spins in QDs to serve as the elementary qubits for quantum information processing[4] is currently being investigated in a variety of systems. In many materials, such as GaAs, the hyperfine interaction between electron and nuclear spins is the primary source of electron spin decoherence which limits qubit performance. However, carbon-based structures can be grown using starting materials isotopically-enriched in ^{12}C, which has no net nuclear spin, thus practically eliminating the hyperfine mechanism of decoherence, leaving behind only a spin-orbit contribution. Furthermore, while the phonon continuum in bulk materials provides the primary bath enabling spin relaxation, the discretized phonon spectrum of a suspended CNT can be engineered to have an extremely low density of states at the qubit (spin) energy splitting. Thus very long spin lifetimes are expected off-resonance.On the other hand, when the spin splitting is nearly resonant with one of the high-Q discrete phonon "cavity" modes, strong spin-phonon coupling can enable qubit control, information transfer, or the preparation of "Schrödinger cat"-like entangled states.

The interaction between nanomechanical resonators and single spins was recently detected [5], and has been theoretically investigated [6] for cases where the spin-resonator coupling arises from the relative motion of the spin and a source
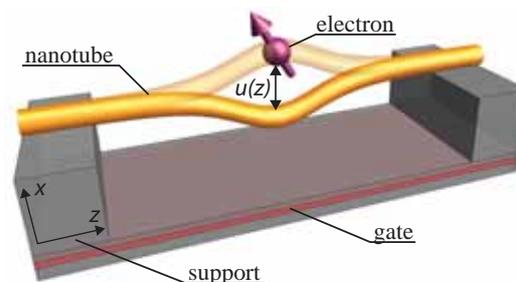
Figure 1: Schematic of a suspended carbon nanotube (CNT) containing a quantum dot filled with a single electron spin. The spin-orbit coupling in the CNT induces a strong coupling between the spin and the quantized mechanical motion $u(z)$ of the CNT.

of local magnetic field gradients. Such coupling is achieved, e.g., using a magnetic tip on a vibrating cantilever which can be positioned close to an isolated spin fixed to a non-moving substrate. Creating strong, well-controlled, local gradients can be challenging for such setups. In contrast, as we here describe, in CNTs the spin-mechanical coupling is *intrinsic*, supplied by the inherent strong spin-orbit coupling which was recently discovered experimentally by Kuemmeth *et al.*[7].

References

[1] A. D. O'Connell *et al.*, Nature **464**, 697 (2010).

[2] G. A. Steele *et al.*, Science **28**, 1103 (2009).

[3] A. Pályi, P. R. Struck, M. Rudner, K. Flensberg and G. Burkard, arXiv:1110.4893 (unpublished).

[4] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998).

[5] D. Rugar, R. Budakian, H. J. Mamin and B. W. Chui, Nature **430**, 329 (2004)

[6] P. Rabl *et al.*, Phys. Rev. B **79**, 041302(R) (2009), P. Rabl *et al.*, Nat. Phys. **6**, 602 (2010).

[7] F. Kuemmeth, S. Ilani, D. C. Ralph, P. L. McEuen, Nature **452**, 448 (2008).

Hybrid Quantum System: Coupling Atoms and Diamond Color Centers to Superconducting Cavities

__S. Putz__[1,2], **R. Amsüss**[1], **Ch. Koller**[1,2], **T. Nöbauer**[1], **R. Voglauer**[1], **A. Maier**[1], **S. Rotter**[3], **K. Sandner**[4], **S. Schneider**[1], **H. Ritsch**[4], **J. Schmiedmayer**[1], and **J. Majer**[1,2]

[1]*Vienna Center for Quantum Science and Technology, Atominstitut, TU Wien, 1020 Vienna, Austria*
[2]*Center for Micro- and Nanostructures ZMNS, TU Wien, 1040 Vienna, Austria*
[3]*Institute for Theoretical Physics, TU Wien, 1040 Vienna, Austria*
[4]*Institute for Theoretical Physics, Universität Innsbruck, 6020 Innsbruck, Austria*

Reversible transfer of quantum information between long-lived memories and quantum processors is a favorable building block for scalable quantum information devices. Furthermore desirable are interfaces which combine flying and stationary qubits, for establishing long range quantum communication networks. Such a device could be an ensemble of nitrogen-vacancy centres joined with superconducting circuits. We present recent experimental results of strong coupling between an ensemble of nitrogen-vacancy center electron spins in diamond and a superconducting microwave coplanar waveguide resonator.

Although the coupling between a single spin and the electromagnetic field is typically rather weak, collective enhancement allows entering the strong coupling regime. A single spin couples with a strength on the order of $g_0/2\pi \sim 12$ Hz, by coupling to an ensemble of $\sim 10^{12}$ nitrogen-vacancies we observe strong coupling. With our experimental set-up we are able to directly observe this characteristic scaling of the collective coupling strength with the square root of the number of emitters by a parametric sweep of the applied magnetic field (see figure:1). By using the dispersive shift of the cavity resonance frequency we measure the relaxation time T_1 of the nitrogen-vacancy center ensemble at millikelvin temperatures in a non-destructive way.

Additionally, we see in transmission spectra a sub ensemble of nitrogen vacancy centres which are each surrounded by a ^{13}C carbon isotope. The shift in resonance frequency by the hyperfine interaction of a nearest neighbour ^{13}C nuclear spin is on the order of 130 MHz (see figure: 2). Due to the smaller gyromagnetic ratio of nuclear spins they are less prone to dipolar inhomogeneous broadening, meaning intrinsic coherence times of nuclear spin ensembles are much longer compared to ensembles of paramagnetic impurities. Information could be stored via the electron spins in the nuclear spin ensemble and by decoupling both longer coherence times become achievable. This is a first step towards a nuclear spin quantum memory which preserves a quantum state for long times.

One of our recent experiments for coupling superconducting circuits to an electron spin ensemble, uses a lumped element microwave resonator design. The combination of a discrete capacitance and inductance defining the resonance frequency $\nu_{res} = 1/\sqrt{LC}$, allows to spatially separate the magnetic and electrical field in the resonator. The structures are typically much smaller than the wavelength of the resonance frequency, resulting in a smaller mode volume due to smaller flux focussing they are also less sensitive to external magnetic fields. These features could help to increase coupling strengths and building robust hybrid quantum devices.
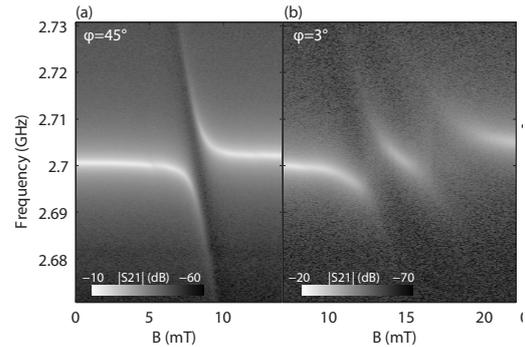
Figure 1: Resonator transmission spectroscopy for different magnetic field angles (a) $\phi = 45°$ and (b) $\phi = 3°$. The collective coupling strength in (a) is $g/\pi = 18.5$ MHz and the coupled system is in the strong coupling regime.
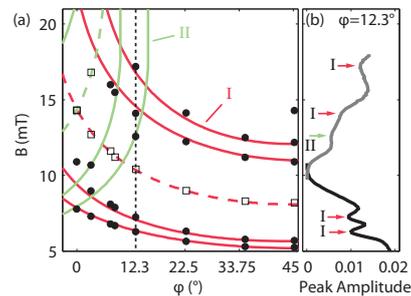
Figure 2: (a) Calculated and measured resonance frequencies as a function of the external magnetic field B. The dashed lines and squares show the bare nitrogen-vacancy resonance frequency, while solid lines and dots are nitrogen-vacancies surrounded by a nearest neighbour ^{13}C nuclear spins. (b) Peak amplitudes as a function of magnetic field at $\phi = 12.3°$

References

[1] R. Amsüss, Ch. Koller, T. Nöbauer, S. Putz, S. Rotter, K. Sandner, S. Schneider, M. Schramböck, G. Steinhauser, H. Ritsch, J. Schmiedmayer, and J. Majer. Cavity qed with magnetically coupled collective spin states. *Phys. Rev. Lett.*, 107:060502, Aug 2011.

[2] K. Sandner, H. Ritsch, R. Amsüss, Ch. Koller, T. Nöbauer, S. Putz, J. Schmiedmayer, and J. Majer. Strong magnetic coupling of an inhomogeneous nitrogen-vacancy ensemble to a cavity. *Phys. Rev. A*, 85:053806, May 2012.

Optomechanical quantum information processing with photons and phonons

K. Stannigel[1,2], P. Komar[3], S. J. M. Habraken[1], S. D. Bennett[3], M. D. Lukin[3], P. Zoller[1,2], and P. Rabl[1]

[1] Institute for Quantum Optics and Quantum Information, 6020 Innsbruck, Austria
[2] Institute for Theoretical Physics, University of Innsbruck, 6020 Innsbruck, Austria
[3] Physics Department, Harvard University, Cambridge, Massachusetts 02138, USA

Optomechanics describes the radiation pressure interaction between an optical cavity mode and the motion of a macroscopic mechanical object, as it appears, for example, in a Fabry-Perot cavity with a moveable mirror [1]. The tremendous progress in the development of new fabrication methods and experimental techniques for controlling optomechanical interactions at the quantum level has recently enabled laser-cooling of micron-sized resonators to their vibrational ground state [2, 3]. This achievement paves the way for a new type of quantum light-matter interface and gives rise to interesting perspectives for novel optomechanics-based quantum technologies. As a solid state approach, such an all optomechanical platform would benefit directly from advanced nanofabrication and scalable integrated photonic circuit techniques.

In this work we study strong optomechanical coupling effects in *multimode* optomechanical systems and describe how resonant or near-resonant interactions in this setting allow us to exploit the intrinsic nonlinearity of radiation pressure in an optimal way. Our approach is based on the resonant exchange of photons between two optical modes mediated by a single phonon, as depicted schematically in Figure 1(a). This resonance induces much stronger nonlinearities than achievable in single-mode optomechanical systems, where due to the frequency mismatch between optical and mechanical degrees of freedom only off-resonant couplings occur. Consequently, multimode optomechanical systems provide a promising route for accessing the single photon strong coupling regime, where the coupling g_0 as well as the mechanical frequency ω_m exceed the cavity decay rate κ. Using state of the art nanoscale devices as depicted in Figure 1(b) [3, 4], this regime is within experimental reach.

We discuss several ways in which strong optomechanical interactions in a multimode setup can be harnessed for applications in quantum information processing [5]. First, we describe how they can be used to generate single photons and point out quantum signatures of the multimode interaction that could be observed in future experiments. Second, we present a phonon-photon transistor as shown in Figure 1(c), which can be used to entangle qubits stored in mechanical excitations with photonic ones. Third, we propose a scheme realizing controlled phonon-phonon interactions, which can be exploited to perform an entangling gate between the mechanical resonators. Augmented by photon-phonon mapping techniques, this also enables gate operations between photonic qubits (see Figure 1(d)).

Our results provide a realistic route towards the quantum nonlinear regime of multimode optomechanical systems. The schemes we present can serve as building blocks for efficient optomechanical classical and quantum information processing, and therefore represent interesting and relevant applications for these systems.
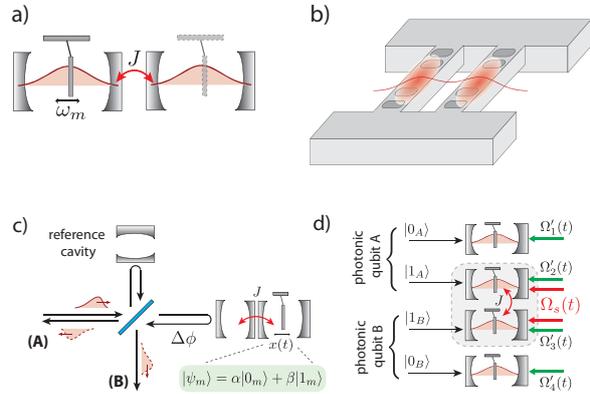
Figure 1: (a) Schematic setup of two tunnel-coupled optomechanical systems. Resonant coupling occurs when the tunnel splitting $2J$ between the optical modes is comparable to the mechanical frequency ω_m. (b) Possible realization based on optomechanical crystal cavities (see Ref. [3, 4] for more details). (c) Phonon-photon transistor: Depending on the state of the mechanical resonator, an incident photon is routed to port A or B. (d) Array of optomechanical systems, where a nonlinear interaction can be induced between neighboring sites in order to realize a phonon-phonon gate.

References

[1] See for example T. J. Kippenberg and K. J. Vahala, Science **321**, 1172 (2008).

[2] J. D. Teufel *et al.*, Nature **471**, 204 (2011).

[3] J. Chan *et al.*, Nature **478**, 89 (2011).

[4] M. Eichenfield *et al.*, Nature **462**, 78 (2009).

[5] K. Stannigel, P. Komar, S. J. M. Habraken, S. D. Bennett, M. D. Lukin, P. Zoller, and P. Rabl, arXiv:1202.3273

Heralded photon amplification for quantum communication

C. I. Osorio, N. Bruno, N. Sangouard, A. Martin, H. Zbinden, N. Gisin, R. T. Thew

Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

Transmission loss is a fundamental limitation in quantum communication. A photon $|1\rangle$ propagating in a channel with a transmission efficiency η_t, ends up in a state given by $\eta_t|1\rangle\langle1| + (1-\eta_t)|0\rangle\langle0|$. Amplifying the single-photon component $|1\rangle$ is not possible in a deterministic, noiseless and coherent operation. But, an approximate quantum amplification is possible.

Probabilistic noiseless amplifiers have recently attracted a lot of attention. Of particular interest are those where the success of the amplification process is heralded [1]. This includes techniques based on single-photon addition [2, 3], or thermal noise addition followed by heralded photon subtraction [4, 5].

Reference [1] presents an interesting protocol for realizing heralded quantum amplification. Inspired by the concept of quantum scissors [6], the authors propose a scheme requiring only single-photon sources and linear optics. This is an attractive proposal from a practical point of view, and it has already triggered a couple of proof-of-principle experiments [7, 8]. These experiments focus on the applications of the amplifiers in continuous variable based quantum information science, e.g. distilling continuous variable entanglement [7], or improving continuous-variable quantum key distribution [8, 9].

Unlike previous realizations, we focus on the potential of the amplifier in Ref. [1] for tasks based on discrete variables. Our heralded single-photon amplifier (see Fig. 1) uses photons at telecom wavelengths, so it is ideally suited for long-distance quantum communication. Furthermore, since it is based on polarization independent elements, our device could also be used as a qubit amplifier [10].

We will present the main results obtained with our system where we have direct access to the behavior of the gain, and we demonstrated the coherence preserving nature of the process (see Fig. 2). Additionally, we showed that no specific phase stability is needed between the input photon and the auxiliary photon, as required in a distributed quantum network [11]. We will also report the progress on the implementation of the qubit amplifier scheme.

All of these results highlight the potential of heralded quantum amplifiers in long-distance quantum communication based on quantum repeaters [11]. The experiment reported here also brings, for the first time, device-independent quantum key distribution into the realm of experimental physics [10].

Figure 1: A schematic of the set-up used to demonstrate heralded single photon amplification.
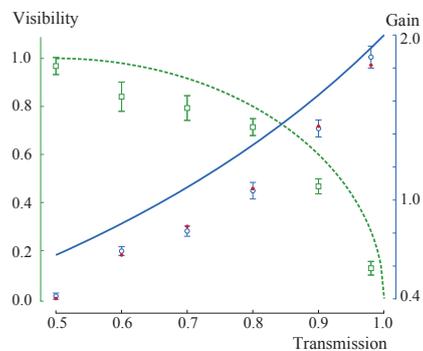
Figure 2: Measured values of the interference visibility and gain as a function of the transmission t (squares and circles respectively). The dashed green line is the maximum possible visibility. The solid blue line is the maximum gain with non photon-number resolving detectors, and without losses, the full circles are the values expected when including losses.

References

[1] T.C. Ralph and A.P. Lund, in *Proceedings of 9th international Conference on Quantum Communication, Measurement and Computing* (ed. A. Lvovsky) 155160 (AIP, 2009).

[2] J. Fiurášek, Phys. Rev. A **80**. 053822 (2009).

[3] A. Zavatta, J. Fiurášek, and M. Bellini, Nature Photonics **5**, 52 (2011).

[4] P. Marek and R. Filip, Phys. Rev. A **81**, 022302 (2010).

[5] M.A. Usuga *et al.*, Nature Physics **6**, 767 (2010).

[6] D.T. Pegg, L.S. Phillips, and S.M. Barnett, Phys. Rev. Lett. **81**, 1604 (1998).

[7] G.Y. Xiang *et al.*, Nature Photonics **4**, 316 (2010).

[8] F. Ferreyrol *et al.*, Phys. Rev. Lett. **104**, 123603 (2010).

[9] S. Fossier *et al.*, J. Phys. B **42**, 114014 (2009).

[10] N. Gisin, S. Pironio and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).

[11] J. Minář, H. de Riedmatten, and N. Sangouard, Phys. Rev. A **85**, 032313 (2012).

Ultrafast superconducting nanowire single-photon detectors for femtosecond-pulsed multi-photon experiments

Lorenzo Procopio[1] , **Max Tillmann**[1] and **Philip Walther**[1]

[1]*University of Vienna, Vienna, Austria*

Scalable quantum information processing experiments have an increasing demand for new technologies that improve the detection efficiency of entangled multi-photon states. To date, the process of spontaneous parametric down-conversion (SPDC) is still the best available source for the generation of individually addressable multi-photon states. The downside of this photon source is the intrinsic probabilistic character that limits current experiments to generate up to 8 photons [1] within reasonable detection time when using conventional single-photon detection technology. On the other hand superconducting nanowire single-photon detectors (SNSPDs) are very promising to open a new experimental parameter regime by superior detection efficiencies combined with picosecond timing resolution and low dark counts [2]. Here, we will report on the investigation of operating SNSPDs in femtosecond-pulsed multi-photon experiments. We will also present perspectives of linear-optical quantum computation and quantum simulation experiments that are within reach when using efficient SNSPDs.

References

[1] Xing-Can Yao, Tian-Xiong Wang, Ping Xu, He Lu, Ge-Sheng Pan, Xiao-Hui Bao, Cheng-Zhi Peng, Chao-Yang Lu, Yu-Ao Chen and Jian-Wei Pan. Observation of eight-photon entanglement, *Nature Photonics*, **6**, 225-228 (2011).

[2] Aleksander Divochiy, Francesco Marsili, David Bitauld, Alessandro Gaggero, Roberto Leoni, Francesco Mattioli, Alexander Korneev, Vitaliy Seleznev,Nataliya Kaurova, Olga Minaeva, Gregory Goltsman, Konstantinos G. Lagoudakis, Moushab Benkhaoul, Francis Lvy and Andrea Fiore. Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths, *Nature Photonics*, **2**, 302-306 (2008).

Precision Spectral Manipulation Using a Coherent Optical Memory

B. M. Sparkes[1], C. Cairns[1], **M. Hosseini**[1], **D. Higginbottom**[1], G. T. Campbell[1], **P. K. Lam**[1], and B. C. Buchler[1]

[1]*Centre for Quantum Computation and Communication Technology, The Australian National University, Canberra*

An optical quantum memory allows coherent, noiseless and efficient storage and recall of optical quantum states. They are an essential building block for quantum repeaters [1], which will extend the range of quantum communication. They could also find applications as a synchronization tool for optical quantum computers, and in a deterministic single-photon sources [2]. If we move towards manipulation of the stored information, a new range of possible uses for quantum memories appear. For instance, the ability to perform multiplexing inside a quantum memory could lead to improved bit rates though quantum information networks, or potentially to perform operations inside an optical quantum computer.

The gradient echo memory scheme (GEM) has been shown to have efficiencies up to 87% [4] and not add noise to the quantum state [5], making it a promising candidate as an optical quantum memory. Here we present experiments that combine a multi-element coil with the three-level GEM scheme in a warm vapor cell to perform precision spectral manipulation of optical pulses [6, 7]. By using eight independently controlled solenoids placed along the memory, we can achieve much finer control over the magnetic field gradient than was possible in previous GEM experiments. This fine control allows us to perform precise frequency filtering and spectral manipulation of pulses, as well as pulse recombination and interference. Some of these operations are illustrated in Fig. 1.

The choice of a warm vapor as the storage medium for a quantum memory is one of convenience and cost. There are, however, limitations to warm vapor quantum memories, especially if storage times longer than 10s of μs are needed. One solution is to move to a cold atomic system. Though this brings with it added complexity, it could also lead to both high efficiencies and longer storage times, as discussed in [8]. Here we will also present our latest work towards demonstrating GEM in a cold atomic medium.

Figure 1: (a) Bandwidth Manipulation - (i) demodulated input pulse, (ii) demodulated output pulses achieved by varying output to input gradient ratios (bracketed terms). (b) Spectral Processing - (i) non-demodulated input pulse containing three frequency components, (ii)-(iv) demodulated retrieval of these three components sequentially. (c) Pulse Intereference - (i), (ii) demodulated input pulses entering the memory, (iii) retrieval of interfered pulses. Insert: retrieval of single pulses P1 (E1) or P2 (E2). ω_c, ω_o values are centre frequencies of pulses, demodulated pulses are averaged over 100 heterodyne data traces.

References

[1] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).

[2] A. I. Lvovsky, B. C. Sanders, and W. Tittel, Nature Photon. **3**, 70 (2009).

[3] G. Hetet, J. J. Longdell, A. L. Alexander, P. K. Lam, and M. J. Sellars, Phys. Rev. Lett. **100**, 023601 (2008).

[4] M. Hosseini, B. M. Sparkes, G. Campbell, P. K. Lam, and B. C. Buchler, Nature Commun. **2**, 174 (2010).

[5] M. Hosseini, G. Campbell, B. M. Sparkes, P. K. Lam, and B. C. Buchler, Nature Phys. **7**, 794 (2011).

[6] B. C. Buchler, M. Hosseini, G. Hétet, B. M. Sparkes, and P. K. Lam, Opt. Lett. **35**, 1091 (2010).

[7] B. M. Sparkes, C. Cairns, M. Hosseini, D. Higginbottom, G. T. Campbell, P. K. Lam, and B. C. Buchler, arXiv:1102.6096v1 (2012).

[8] B. M. Sparkes, M. Hosseini, H. Hétet, P. K. Lam, and B. C. Buchler, Phys. Rev. A **82**, 043847 (2010).

		1		2,3,4		1		2,3		5		5		6
		7		8		1,10		1,9		3,4				1,10

[1] ICFO-Institut de Ciencies Fotoniques, Castelldefels, Spain
[2] qutools GmbH, München, Germany
[3] Fakultät für Physik, Ludwig-Maximilians-Universität München, München Germany
[4] Max-Planck-Institut für Quantenoptik, Garching, Germany
[5] European Space Agency, Noordwijk, The Netherlands
[6] Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Ontario, Canada
[7] Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Vienna, Austria
[8] Department of Electrical and Electronic Engineering, University of Bristol, Bristol, United Kingdom
[9] Dept. Signal Theory and Communications, Universitat Politecnica de Catalunya, Barcelona Spain
[10] ICREA-Institució Catalana de Recerca i Estudis Avançats, Barcelona, Spain

Several e perimental demonstrations of communication protocols, relying on quantum entanglement as a resource, have proven that entangled photons are not only paramount to fundamental e periments about the nature of physical reality, but can also nd real world applications in quantum enhanced metrological schemes, quantum communication protocols and quantum cryptography. One of the requirements for envisaged satellite link e periments is the development of ef cient, robust and space quali ed sources of entangled photons. In collaboration with the European space agency (ESA), we have developed and engineered a highly ef cient source of polari ation entangled photons [1], designed specifically for the distribution of entangled photons via long-distance free-space links. The source is based on, 40 nm laser diode (LD) pumped, spontaneous parametric down conversion (SPDC) from crossed bulk periodic poled potassium titanyl phosphate (PPKTP) crystals, phase-matched for collinear type-0 SPDC with non-degenerate signal and idler wavelengths[2]. The photons were generated around 810 nm, whereby this operation wavelength was determined taking into account the atmospheric transmission characteristics, beam-diffraction, currently available detector technology, as well as the availability of compact, space-quali able diode-based pump sources. The non-degenerate photons were isolated using a ber-based wavelength division multiple er (DM) with the single-mode output bers providing a versatile interface and ensuring minimum initial beam-diffraction. The access to the large non-linear d_{33} coef cient of PPKTP as well as the use of 20 mm crystals in an optimi ed focusing geometry, allowed us to achieve unprecedented normali ed pair detection rates: for photon pairs created at the wavelengths 783nm (signal) and 837 nm (idler) we detect 0.6 million photon pair events per second m and a high two-photon entanglement quality, with an overlap delity with the ideal Bell state of 0.98 at low pump powers. The source was tested under emulated link scenarios via added attenuation and the fundamental limitations imposed due multiple pair emission events were evaluated. ith emphasis put on robustness and compactness the hardware including pump laser and driving electronics t on a small footprint breadboard. e believe that our entangled photon source will provide a valuable tool for future e periments outside laboratory environments.

Figure 1: Schematic of the compact entangled photon source mounted on $40 \times 30 \text{cm}^2$ breadboard.

Figure 2: E periment and Simulation: The visibility decreases with pump power due the detrimental effect of multiple pair emission and remains constant up to high link-attenuation.

[1] F. Steinlechner, P. Tro ek, M. ofre, H. eier, D. Pere , T. ennewein, R. rsin, . Rarity, M. . Mitchell, . P. Torres, H. einfurter and . Pruneri, A high brightness source of polari ation entangled photons optimi ed for applications in free space (accepted for publication), Optics E press, (to be published).

[2] P. Tro ek and H. einfurter, Collinear source of polari ation-entangled photon pairs at nondegenerate wavelengths, Applied Physics Letters 2, 211103 (2008).

Towards efficient photon pairs production in Bragg reflection waveguides

Jiří Svozilík[1,2], Adam V. Marí[1], Michal Mičuda[3] , Martin Hendrych[1] and Juan P. Torres[1]

[1]*ICFO - Institute of Photonic Sciences, Castelldefels (Barcelona), Spain*

[2]*Joint Laboratory of Optics, RCPTM, Palacký University and Institute of Physics of Academy of Science of the Czech Republic, 17. listopadu 50A, 772 07 Olomouc, Czech Republic*

[3]*Department of Optics, Faculty of Science, Palacky University, 17. listopadu 50, 77900 Olomouc, Czech Republic*

E-mail: jiri.svozilik@icfo.es

Semiconductor Bragg reflection waveguides based on $Al_xGa_{1-x}As$ and $Al_xGa_{1-x}N$ exhibit several advantages, such as a large non-linear coefficient, broad transparency window and low linear propagation loss. They present an efficient source of photon pairs using the process of the spontaneous parametric down-conversion [1]. The propagation properties of guided modes can be easily controlled via structure design allowing one to tailor on demand the spectral correlations between photons in a pair. In this manner, Bragg reflection waveguides are capable to generate photons with ultra-broad spectra (almost hundreds of nanometers at a central wavelength of 1550 nm) that have mutually orthogonal polarizations, high degree of entanglement and high photon emission rate. The broad tunability of the spectral features also enables the generation of spectrally uncorrelated photon pairs [2].
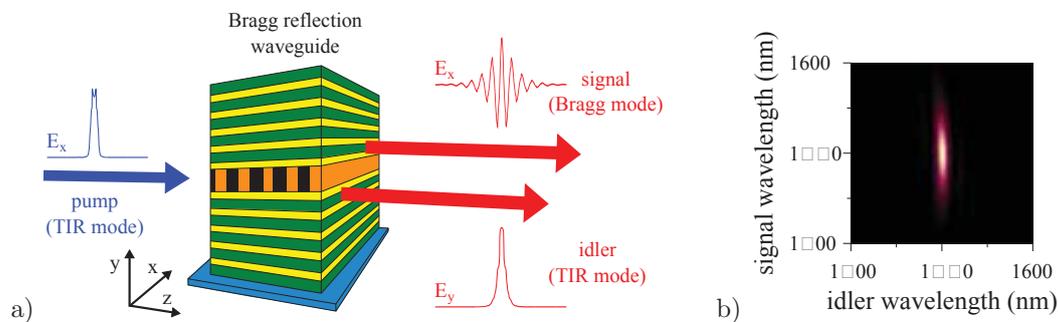
Figure 1: The scheme of the spectrally uncorrelated photon pairs generation a) and the corresponding asymmetrical joint-spectral amplitude b).

References

[1] P. Abolghasem, M. Hendrych, X. Shi, J. P. Torres, and A. S. Helmy, Bandwidth control of paired photons generated in monolithic Bragg reflection waveguides, Opt. Lett. 34, 2000 (2009).

[2] J. Svozilík, M. Hendrych, A. S. Helmy and J. P. Torres, Generation of paired photons in a quantum separable state in Bragg reflection waveguides, Opt. Express 19, 3115 (2011).

[1,4], **Thomas Herbst**[1,2], **Sebastian Kropatschek**[1], **Xiaosong Ma**[1,2], **Anton Zeilinger**[1,2,3] **and Rupert Ursin**[1]

[1]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria*
[2]*Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria*
[3]*Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria*
[4]*Abbe School of Photonics, Friedrich-Schiller University Jena, Max-Wien Platz 1, 07743 Jena, Germany*

Silicon Single Photon Avalanche Diodes (Si-SPADs) are nowadays widely accepted components for single photon detection. Common commercial Si-SPADs have limited sensitive area, which would be a potential limitation of their applications in free-space quantum optical experiments, especially in long-distance experiments where the turbulence-induced beam wander effect is present. Under this condition, efficient detection of the photons would require uniformity of the quantum efficiency over the sensitive area. Therefore, it is of importance to investigate the dependence of quantum efficiency on the injecting position of the photons, that is, the spatial quantum efficiency profile. On the other hand, the detectors might have to work in high count rates. Exploration of the saturation behavior of the detectors is also essential.

In this work, we present the results of experiments performed on three different detection models (Laser Components Photon Counting Module [1], passively quenched Laser Components SAP 500 SPAD [2] and actively quenched Perkin Elmer C30902SH SPAD [3]). We were able to measure the 2-Dimensional relative quantum efficiency profile and saturation behavior of the detectors.

As a result, we found out that the Laser Component Photon Counting Module has a small sensitive area with Full-Width at Half-Maximal diameter around 120 μm. However, it exhibited stably low dark count rates, and no saturation behavior up to 2 MHz count rates. Therefore, it would be a suitable candidate to be used at the sender's side in free-space experiments. In contrast, the Laser Components SAP 500 detector has a sensitive area with diameter of 510 μm, but only capable to count up to 80 kHz. It can essentially be used at the receiver's side.
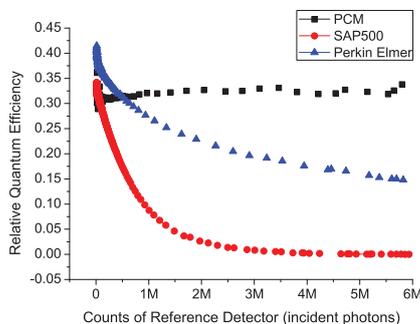
Figure 1: Relative quantum efficiency of the tested detectors with respect to the count rates of a reference detector (linearly responses to the number of incident photons within testing range). PCM: Laser Components Photon Counting Module; SAP500: Laser Components SAP 500 SPAD; Perkin Elmer: Perkin Elmer C30902SH SPAD.
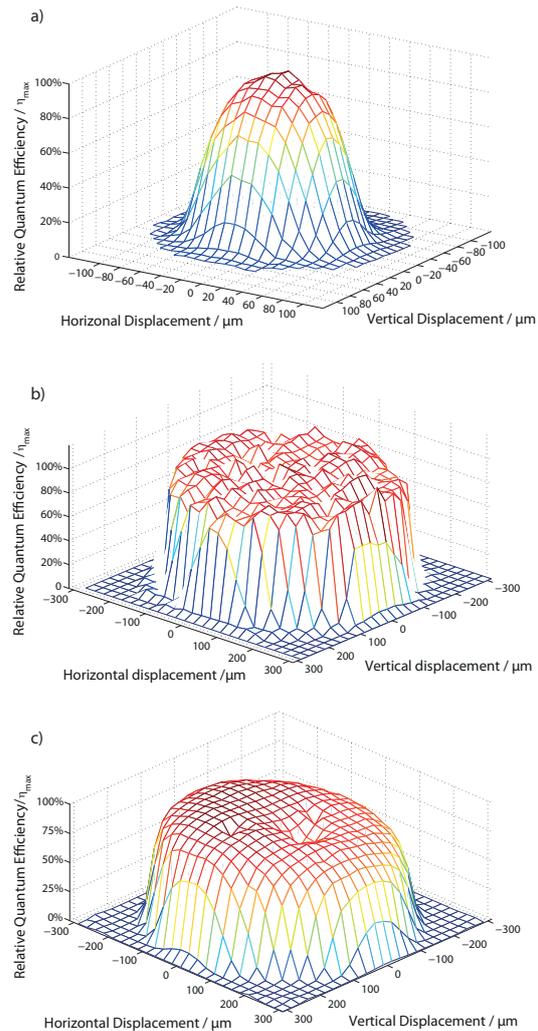
Figure 2: Spatial quantum efficiency (relative) profile of the detectors: a) Laser Components Photon Counting Module; b) Laser Components SAP 500 SPAD; c) Perkin Elmer C30902SH SPAD.

References

[1] "Single Photon Counting Module COUNT-Series", (data sheet), Laser Components Germany, 2011.

[2] "Silicon Geiger Mode Avalanche Photodiode", (data sheet), Laser Components Germany, 2011.

[3] "Silicon Avalanche Photodiodes C30902 Series", (data sheet), Perkin Elmer USA, 2008.

ano ber ased abr erot Microresonators haracteristics and Applications

hristian uttke[1], and Arno Rauschenbeutel[1]

[1] VCQ, Atominstitut, Technische Universität Wien, Stadionallee 2, A-1020 Wien

Tapered optical fibers (TOFs) with a nanofiber waist have proven to be a powerful tool for the efficient coupling of light and matter due to the strong lateral confinement of the light field in the waist region. The coupling can be further enhanced with a resonant structure that also confines the light along the TOF. Such a TOF microresonator is highly attractive because the strong coupling regime of light and matter can be reached even with a moderate finesse of about 30 [1]. For this purpose, fiber ragg gratings (F Gs) are an advantageous candidate as mirrors: They can be integrated into the unprocessed fiber ends of the TOF and can be tailored for a range of wavelengths and re ectivities. We present a realization of such a TOF microresonator for a design wavelength of 852 nm based on two F G mirrors which enclose a TOF with a subwavelength-diameter waist as schematically shown in Fig. 1. The TOF microresonator offers advantageous fea-
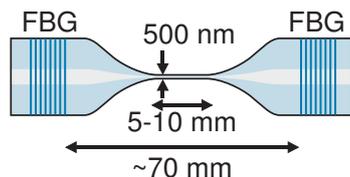
Figure 1: Schematic picture of the TOF microresonator

tures such as tunabilty, high transmission outside of the F G stop band and a monolithic design enabling alignment-free operation. Combined with its high coupling strength over the full length of the nanofiber waist, this makes the TOF microresonator a promising tool for, e.g., cavity quantum electrodynamics with fiber-coupled atomic ensembles and for the realization of quantum network nodes.

Furthermore, this resonator is an ideal tool for measuring properties of the TOF, like, e.g., the equilibrium temperature at a given guided optical power, the thermalization time constant, and the mechanical eigenmodes. All these processes in uence the optical pathlength inside the resonator and thereby lead to a frequency shift of the resonance frequencies of the resonator and yield spectral signatures that can be measured with high precision.

References

[1] F. Le ien and . Hakuta, Phys. Rev. A , 05382 (2009).

[2] C. Wuttke, M. ecker, S. ruckner, M. Rothhardt, A. Rauschenbeutel, Opt. Lett., accepted (2012); (ar iv:1202.1 30).

Experimental Investigation of the Evolution of Gaussian Quantum Discord in an Open System

Lars S. Madsen[1], **Adriano Berni**[1], **Mikael Lassen**[1] **and Ulrik L. Andersen**[1]

[1]*Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kgs. Lyngby, Denmark*

Gaussian quantum discord is a measure of quantum correlations in Gaussian systems. Using Gaussian discord we quantify the quantum correlations of a bipartite entangled state and a separable two-mode mixture of coherent states. We experimentally analyze the effect dissipation on Gaussian discord and show that for the two-mode mixture of coherent states it can lead to an increase in discord. In particular we experimentally demonstrate the transition from the quantum correlations to classical correaltions, as well as the revival of quantum correlations through dissipation [5].

The quantum discord is a measure of the one-way quantum correlations in a bipartite system [1]. The measure captures entanglement but also other types correlations which cannot be extracted by measurements on a single mode of the bipartite system. It is based on the subtraction of the quantum mutual information (I) and the one-way classical information J. Recently it was show how the measure can be calculated for the set of Gaussian states when retricting the set of measurements used to calculate J to the Gaussian measurements [2, 3].

The Gaussian discord has mainly been explored from the theoretical point of view. Latest it was show that non-trivial behavior of squeezed thermal states can be expected in disspative channels [4]. In this poster we will present some of the first experimental work Gaussian quantum discord.

References

[1] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).

[2] G. Adesso and A. Datta, Phys. Rev. Lett. **105**, 030501 (2010);

[3] P. Giorda and M. G. A. Paris, Phys. Rev. Lett. **105**, 020503 (2010).

[4] F. Ciccarello and V. Giovannetti, Phys. Rev. A **85**, 022108 (2012)

[5] L. S. Madsen, A. Berni, M. Lassen and U. L. Andersen, Phys. Rev. Lett. **109**, 030402 (2012)

Spin squeezing via QND measurement in an Optical Magnetometer

R.J. Sewell[1], **M. Koschorreck**[2], **M. Napolitano**[1], **B. Dubost**[1,3], **N. Behbood**[1], **G. Colangelo**[1], **F. Martin**[1] **and M.W. Mitchell**[1,4]

[1]*ICFO-Institut de Ciencies Fotoniques, Av. Carl Friedrich Gauss, 3, 08860 Castelldefels, Barcelona, Spain.*
[2]*Cavendish Laboratory, University of Cambridge, JJ Thompson Avenue, Cambridge CB3 0HE, United Kingdom.*
[3]*Univ. Paris Diderot, Sorbonne Paris Cité, Laboratoire Matériaux et Phénomènes Quantiques, UMR 7162, Bât. Condorcet, 75205 Paris Cedex 13, France.*
[4]*ICREA-Institució Catalana de Recerca i Estudis Avançats, 08015 Barcelona, Spain.*

A qauntum non-demolition (QND) measurement provides information about a quantum variable of interest while leaving it unchanged and accessible for future measurements. To be considered QND, the measurement should reduce the uncertainty in the measured variable, known as 'quantum state preparation' (QSP), and do so without introducing significant damage to the state. In an optical measurement of atomic spins, successful QSP leads to spin squeezing, and can be evaluated by measuring the conditional variance of two successive QND measurements. For metrological applications, spin squeezing of atomic ensembles via QND measurement has the advantage of allowing continuous measurements of macroscopically large atomic ensembles, with demonstrated advantage in high-bandwidth magnetometry. Large-spin systems similarly offer metrological advantage in magnetometry. However, demonstrating spin-squeezing via QND measurement in large-spin systems has proved a technical challenge.

We work with an ensemble of $f = 1$ atoms interacting with pulses of near-resonant light via the effective Hamiltonian $H_{\mathrm{eff}} = \kappa_1 S_z F_z + \kappa_2 (S_x J_x + S_y J_y)$, where $\kappa_{1,2}$ are coupling constants. The light is described by the collective Stokes operators S_i, and the atoms by collective spin orientation and alignment operators F_z and $J_{x,y}$. The κ_1 term describes a QND interaction: paramagnetic Faraday rotation. The κ_2 terms describe the coupling of light to collective Raman coherences, and couple both quantum and technical noise into the QND variables, destroying the QND measurement. To recover the ideal QND interaction, we have developed a two-polarization probing technique based on dynamical decoupling methods which allows us to cancel the κ_2 term in the Hamiltonian, and demonstrated projection-noise limited measurement of the QND variable F_z for an input J_x–aligned state [2], with a measurement sensitivity of $515\,\mathrm{spins}^2$ as calibrated with a thermal spin-state [1].

Here we report the demonstration of spin squeezing, and the first experimental verification of a QND measurement of a material system according to the non-classicality criteria of Grangier *et al* [3]. We prepare a J_x polarized state with maximal Raman coherence via optical pumping. QND measurement produces squeezing of the collective orientation F_z, verified by the conditional variance of repeated measurements. We observe up to 3.2 dB of conditional noise reduction and 1.8 dB of metrologically-relevant squeezing, demonstrating entanglement among the spin-1 atoms [4] (see Fig. 1(a)). We quantify the excess noise introduced into the atomic and light variables via a third successive measurement [5], demonstrating non-classicality in both the QSP and information-damage tradeoff and criteria, as required for QND measurement (see Fig. 1(b)).
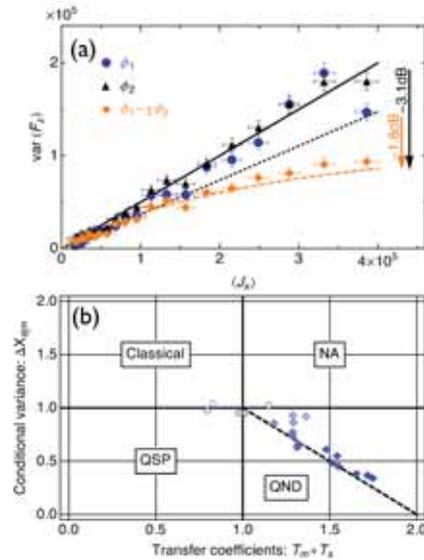
Figure 1: **(a)**: Variances (blue circles and black diamonds) and conditional variance (orange diamonds) of the two QND measurements. Curves are theoretical calculations of the projection-noise (solid black line) and expected conditional noise reduction (orange dashed line). **(b)**: Conditional variance and transfer coefficients $T_m = 1/(1 + \Delta S_y)$ and $T_s = 1/(1 + \Delta F_z)$ quantified via three successive QND measurements. Shading represents a change in $\langle J_x \rangle$ from 1.75×10^4 (light blue) to 3.85×10^5 (dark blue).

References

[1] M. Koschorreck *et al.*, "Sub-projection-noise sensitivity in broadband atomic magnetometry," Phys. Rev. Lett. **104**, 093602 (2010).

[2] M. Koschorreck *et al.*, "Quantum Nondemolition Measurement of Large-Spin Ensembles by Dynamical Decoupling," Phys. Rev. Lett. **105**, 093602 (2010).

[3] P. Grangier *et al.*, "Quantum non-demolition measurements in optics," Nature **396**, 537 (1998).

[4] R. Sewell *et al.*, "Spin-squeezing of a large-spin system via QND measurement," arXiv:1111.6969v2 [quant-ph].

[5] M.W. Mitchell *et al.*, "Certified quantum-non-demolition measurements of material systems," arXiv:1203.6584v1 [quant-ph].

A quantum key distribution system immune to detector attacks

A. Rubenok[1], J. A. Slater[1], P. Chan[2], I. Lucio-Martinez[1] and W. Tittel[1]

[1] Institute for Quantum Information Science and Department of Physics & Astronomy, University of Calgary, Calgary, Canada.
[2] Institute for Quantum Information Science and Department of Electrical & Computer Engineering, University of Calgary, Calgary, Canada.

Quantum key distribution (QKD) promises the distribution of cryptographic keys whose secrecy is guaranteed by fundamental laws of quantum physics[1, 2]. After more than two decades devoted to the improvement of theoretical understanding and experimental realization, recent results in quantum hacking have reminded us that the information theoretic security of QKD protocols does not necessarily imply the same level of security for actual implementations. Of particular concern are attacks that exploit vulnerabilities of single photon detectors[3, 4, 5, 6], whose effectiveness may have led potential users to conclude that QKD is not viable. Here we report the first proof-of-principle demonstration of a new protocol[7] that removes the threat of any such attack [8]. More precisely, we demonstrated this approach to QKD in the laboratory over more than 80 km of spooled fiber, as well as across different locations within the city of Calgary. The robustness of our fiber-based implementation, which establishes the possibility for Bell-state measurements in a real-world environment, along with the enhanced level of security offered by the protocol, confirms QKD as a realistic technology for safeguarding secrets in transmission. Furthermore, our technological advance removes a remaining obstacle to realizing future applications of quantum communication, such as quantum repeaters[9] and, more generally, quantum networks.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74,** 145 (2002).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81,** 1301 (2009).

[3] A. Lamas-Linares, and C. Kurtsiefer, Opt. Express **15** (15), 9388 (2007).

[4] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78,** 042333 (2008).

[5] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4,** 686 (2010).

[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18** (26), 27938 (2010).

[7] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108,** 130503 (2012).

[8] A. Rubenok, J. A. Slater, I. Lucio-Martinez, P. Chan, and W. Tittel, arXiv:1204.0738.

[9] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, Rev. Mod. Phys. **83,** 33 (2011).

Author Index

Quantum Communication, Measurement and Computing – Program at a Glance

Time	Sunday 29 July	Monday 30 July	Tuesday 31 July	Wednesday 1 August	Thursday 2 August	Friday 3 August
9:00		Milburn	Zeilinger	Cirac	Gisin	Oberthaler
9:50		Kielpinski	Kwiat	Kraus	Rau	Langen
10:10		Treutlein	Fickler	Gu	Ng	Hasegawa
10:30		coffee break	coffee break	coffee break	coffee break	coffee break
11:00		Bertet	Leibfried	Pan	Sasaki	Gavinsky
11:30		Painter	Roos		Giovannetti	Makarov
12:00		Munro	Rosenfeld	Lloyd	Dorenbos	Lim
12:20		Brukner	Nagaj		Gerrits	Tame
12:45		Lunch	Lunch	Lunch	Lunch	Lunch
14:00		Silberhorn	Rabitz		Tittel	Grangier
14:30		White	Montangero	Excursion: visit of Abbey Melk and boat trip to Vienna	Walmsley	Brune
15:00		Laing	Bowen		Timoney	Ritter
15:30		Wiseman	Deutsch		Nemoto	Donner
15:45		break	break		break	break
16:15	Registration and Reception (TU Main building 2nd floor)	Mitchell	Renner		Furusawa	Wrachtrup
16:45		Vuletič	Yao		Caves	Cappellaro
17:00		Chen	Garćia-Patrón		Ferrie	Bernien
17:30		Volz	Yoshida		Rakher	Bar-Gill
17:50		poster session and company exhibition (TU Main building Prechtl hall, 1st floor)	poster session and company exhibition (TU Main building Prechtl hall, 1st floor)		poster session and company exhibition (TU Main building Prechtl hall, 1st floor)	closing event: Heurigen (traditional wine tavern) sponsored by CITY of Vienna
19:00		beer, wine, and pretzels sponsored by AIT	beer, wine, and pretzels		beer, wine, and pretzels	