Q 67: Quantum Information: Quantum Communication II

Time: Friday 11:00–13:00 Location: K/HS1

Q 67.1 Fri 11:00 K/HS1

Quantum Metrology based on Multi-Photon Interference — •Alexander Müller, Simon Laibacher, Vincenzo Tamma, and Wolfgang Schleich — Institut für Quantenphysik, Universität Ulm, D 89069 Ulm

It is known that phase super-resolution and super-sensitivity can be achieved with entangled quantumstates, so called NOON-states. Unfortunately they are complicated to produce and to measure, especially for higher numbers of photons. On the other hand are thermal light sources easy to prepare and widely available. We investigate thermal states as the input sources of an interferometer and derive circumstances, under which they also show supersensitivity and superresolution. To make them practically usable, it is important to keep the visibility at a high level, even for high photon numbers.

Q 67.2 Fri 11:15 K/HS1

Novel criteria for quantum non-Gaussianity — •Lucas Happ[1], Maxim A Efremov[1,2], Hyunchul Nha[3,4], and Wolfgang P Schleich[1,5] — [1]Institut für Quantenphysik and Center for Integrated Quantum Science and Technology (IQST), Universität Ulm, D-89081 Ulm, Germany — [2]A.M. Prokhorov General Physics Institute, Russian Academy of Sciences, 119991 Moscow, Russia — [3]School of Computational Sciences, Korea Institute for Advanced Study, Seoul 130-012, Korea — [4]Department of Physics, Texas A&M University at Qatar, PO Box 23874, Doha, Qatar — [5]Institute for Quantum Science and Engineering (IQSE), Department of Physics and Astronomy, Texas A&M University, College Station, TX 77843

Gaussian states play a major role in quantum information with continuous variables. An important question for any practical implementation of such a state is to provide the user with a criterion or condition to verify whether a given state is a Gaussian one. The fundamental criterion for a pure state to be a Gaussian one is the positivity of the corresponding Wigner function. However, such a simple criterion of Gaussianity is not easy to verify in practice. For this reason, in order to distinguish a non-Gaussian state from a Gaussian one, we present a new condition which relies on the sum of all the moments of the coordinate and momentum operators. Moreover, we examine the proposed condition for pure and mixed states.

Q 67.3 Fri 11:30 K/HS1

Degradability of Fermionic Gaussian Channels — •Eliška Greplová[1,2] and Géza Giedke[1,3] — [1]Max-Planck-Institut für Quantenoptik, H.-Kopfermann-Str 1, D-85748 Garching — [2]Aarhus University, Ny Munkegade 120, DK-8000 Aarhus C — [3]Donostia International Physics center, Paseo M. de Lardizabal 4, E-20018 San Sebastian

We study the degradability of fermionic Gaussian channels. We derive a simple standard form that allows the characterization of all degradable and antidegradable fermionic Gaussian channels. We also provide a full weak-degradability classification of these channels. Consequences for the quantum capacity of those channels are discussed.

Q 67.4 Fri 11:45 K/HS1

Design and evaluation of a handheld Quantum Key Distribution sender module — •Gwenaelle Mélen[1,2], Markus Rau[1], Lukas Fuchs[1], Giacomo Corrielli[3], Henning Weier[2], Sebastian Nauerth[2], Andrea Crespi[3], Roberto Osellame[3], and Harald Weinfurter[1,4] — [1]Fakultät für Physik, Ludwig-Maximilians-Universität, 80799 München, Germany — [2]qutools GmbH, 81371 München, Germany — [3]Dipartimento di Fisica, Politecnico di Milano, and Istituto di Fotonica e Nanotecnologie (IFN-CNR), 20133 Milano, Italy — [4]Max-Planck-Institut für Quantenoptik, 85748 Garching, Germany

Complementary to long distance Quantum Key Distribution (QKD) schemes, secure short-distance communication could also benefit daily-life applications such as banking. The design of our free-space QKD add-on for mobile devices allows to generate a secure key, e.g. at an ATM, for future online authentication or direct transaction.

The ultra-flat architecture (25×2×1 mm) includes an array of four attenuated VCSELs with uniform emission properties at 850 nm. 100 ps pulses with low degree of polarization are produced at 100 MHz repetition rate. Four wire-grid polarizers fabricated using Focused Ion Beam Milling and exhibiting extinction ratios up to 29 dB control the qubit states. The polarized beams are spatially overlapped in a low-birefringence, single-mode waveguide array with one main output manufactured via femtosecond laser micromachining. An Android App controls the driving electronics and establishes a classical Wi-Fi channel with the receiver to provide full QKD functionality.

Q 67.5 Fri 12:00 K/HS1

Large-Alphabet Quantum Key Distribution Using Spatially Encoded Light — •Tristan Tentrup, Peter Hooijschuur, Reinier van der Meer, Georgios Ctistis, and Pepijn Pinkse — University of Twente, Enschede, The Netherlands

Secure communication between a sender (Alice) and a receiver (Bob) is a challenging task in today's society. In order to be able to exchange information in a secure way, Alice and Bob have to share a key to encrypt/decode the information. One method to do that is Quantum Key Distribution (QKD) using the BB84 protocol with single photons. Usually, the two-dimensional polarization basis is used to transmit information, but going to a higher dimensional basis (larger alphabet) increases security and amount of information carried by a single photon. We present our experimental results with an encoding scheme using a spatial light modulator (SLM) allowing in principle an alphabet of the order of 10^4 characters (>13 bit per photon).

Q 67.6 Fri 12:15 K/HS1

Sub-μs spin state detection of single trapped atoms for a loophole-free test of Bell's inequality — •Norbert Ortegel[1], Kai Redeker[1], Daniel Burchardt[1], Robert Garthoff[1], Wenjamin Rosenfeld[1,2], and Harald Weinfurter[1,2] — [1]Ludwig-Maximilians-Universität, München — [2]Max-Planck Institut für Quantenoptik, Garching

We plan a test of Bell's inequality with the detection and the locality loophole closed simultaneously in a single experiment. It consists of analyzing the Zeeman spin states of two ^{87}Rb-atoms in the $5S_{1/2}, F = 1$ ground state separated by 400m. Using entanglement swapping we create *heralded* entanglement between the atoms which allows closing the detection loophole.

To close the locality loophole we implemented an ultra-fast readout of the trapped atoms based on Zeeman-state selective ionization and subsequent detection of the ionization fragments with two channel electron multipliers (CEMs). Photo-ionization is done by Zeeman-state dependent excitation to $5P_{1/2}, F = 1$ at 795nm and subsequent ionization at 450nm, where the polarization of the first exciting laser pulse determines the measurement basis of the readout.

We achieve a combined probabilty to detect the ion OR the electron from the ionization of a single atom of above 98%. This enables a fidelity for the state readout of 95%, mainly limited by off-resonant excitation to $5P_{1/2}, F = 2$ during the photo-ionization. Including random setting of the measurement basis the overall duration of the readout is below 1μs.

Q 67.7 Fri 12:30 K/HS1

Trojan-horse attacks on practical continuous-variable quantum key distribution systems — •Imran Khan[1,2], Nitin Jain[1,2], Birgit Stiller[1,2], Paul Jouguet[3], Sébastien Kunz-Jacques[3], Eleni Diamanti[4], Vadim Makarov[5], Christoph Marquardt[1,2], and Gerd Leuchs[1,2] — [1]Max Planck Institute for the Science of Light, Guenther-Scharowsky-Str. 1/Bldg. 24, 91058 Erlangen, Germany — [2]Institute for Optics, Information and Photonics, University of Erlangen-Nuernberg, Staudtstraße 7/B2, 91058 Erlangen, Germany — [3]SeQureNet, 23 avenue d'Italie, 75013 Paris, France — [4]LTCI, CNRS - Telecom ParisTech, 46 rue Barrault, 75013 Paris, France — [5]Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada

Practical quantum key distribution (QKD) implementations may deviate from the assumptions made in security proofs for QKD protocols. Quantum hacking uses this potential gap to demonstrate possible attacks on such systems. Here, we experimentally demonstrate a Trojan-horse attack on a laboratory continuous-variable QKD system with a success rate of 98.73 % to read out the state of Alice's modulator. Furthermore, we study the feasibility of this attack on a similar commercial system. At the same time we offer possible countermeasures.

Q 67.8 Fri 12:45 K/HS1

Renormalising entanglement distillation — Stephan Wäldchen[1], •Janina Gertis[2], Earl T. Campbell[3], and Jens Eisert[2] — [1]Humboldt Universität Berlin, Germany — [2]Freie Universität Berlin, Germany — [3]University of Sheffield, United Kingdom

Entanglement distillation refers to the task of transforming a collection of weakly entangled pairs into fewer highly entangled ones. It is a core ingredient in quantum repeater protocols, needed to transmit entanglement over arbitrary distances in order to realise quantum key distribution schemes. Usually, it is assumed that the initial entangled pairs are i.i.d. distributed and uncorrelated with each other, an assumption that may be very much inappropriate in any entanglement generation process involving memory channels. Here, we introduce a framework that captures entanglement distillation in the presence of natural correlations arising from memory channels. Conceptually, we bring together ideas of condensed-matter physics - that of renormalisation - with those of local entanglement manipulation. Formally, we introduce ideas of tensor networks and matrix product operators to the context of entanglement distillation, and rigorously prove convergence to maximally entangled states in various meaningful settings, introducing notions of renormalisation of matrix-product operators.