Q 48: Quanteninformation (Quantenkommunikation)

Zeit: Donnerstag 16:30–19:00 Raum: 1B

Q 48.1 Do 16:30 1B

Two Photon Interference of Resonance Fluorescence Photons — •S. Gerber, D. Rotter, F. Dubin, and M. Mukherjee — Institut für Experimentalphysik, Universität Innsbruck, Austria

We report on two photon interference measurements of resonance fluorescence photons from trapped ions. Two indistinguishable photons impinging at two input ports of a 50/50 beam splitter coalesce, i.e. they both are leaving the device in one of the output ports. This Hong-Ou-Mandel interference is quantified by measuring correlations between the two output channels. The visibility of the two-photon interference effect determines the degree of indistinguishability of the input photons.

In a first experiment, a single trapped ion is converted into a pseudo two-photon source. The single ion resonance fluorescence is split in two parts, individually coupled into optical fibers of different length and then recombined on a beam splitter. A two-photon interference is observed with a contrast reaching 83%. The spectral brightness of our two-photon source is quantified and shown to be comparable to parametric down conversion devices [1].

In a successive experiment two-photon interference between two ions located in two separate traps is measured with up to 87% contrast. Thus, two-photon interference is used as a building block for quantum network operations.

[1] F. Dubin, D. Rotter, M. Mukherjee, S. Gerber, R. Blatt, Phys. Rev. Lett. 99, 183001 (2007)

Q 48.2 Do 16:45 1B

Quantum Repeaters using Coherent-State Communication — •Peter van Loock — Optical Quantum Information Theory Group, Max Planck Research Group, Institute of Optics, Information and Photonics, Staudtstr. 7/B2, 91058 Erlangen, Germany

We investigate quantum repeater protocols based upon atomic qubit-entanglement distribution through optical coherent-state communication. Various measurement schemes for an optical mode entangled with two spatially separated atomic qubits are considered in order to non-locally prepare conditional two-qubit entangled states. In particular, generalized measurements for unambiguous state discrimination enable one to completely eliminate spin-flip errors in the resulting qubit states, as they would occur in a homodyne-based scheme due to the finite overlap of the optical states in phase space [1]. As a result, by using weaker coherent states, high initial fidelities can still be achieved for larger repeater spacing, at the expense of lower entanglement generation rates. In this regime, the coherent-state-based protocols start resembling single-photon-based repeater schemes.

[1] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, Kae Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).

Q 48.3 Do 17:00 1B

Verbesserte Fehlerschwellen für das BB84 und 6-state Protokol — •Oliver Kern, Joseph M. Renes und Gernot Alber — Institut für Angewandte Physik, Technische Universität Darmstadt, 64289 Darmstadt, Germany

Es ist bekannt, dass lokale Randomisierung die Raten von Quantenkryptographie Protokollen welche Einwegkommunikation nutzen, verbessern kann. Ein noch größerer Vorteil kann für das BB84 Protokol erlangt werden, indem man eine Randomisierung mit strucktuiertern (nicht zufälligen) Blockcodes verknüpft. Wir zeigen, dass ein solcher Vorteil auch für das 6-state Protokol erlangt werden kann. Es ist möglich, die beste untere Schranke für die Bitfehlerrate von 14.12% mit Randomisierung auf mindestens 14.57% mit dem verknüpften Verfahren zu erhöhen.

Q 48.4 Do 17:15 1B

Continuous-variable quantum key distribution with qudits — •Ulrich Seyfarth and Gernot Alber — Institut für Angewandte Physik, Technische Universität Darmstadt, D-64289, Darmstadt

A qudit generalization of the recently discussed two-state continuous-variable quantum key distribution protocol of Heid and Lütkenhaus [1] is presented. Secret key rates are evaluated for cases in which an eavesdropper can extract information by beam splitting attacks. Resulting key generation rates for direct and reverse reconciliation are compared.

[1] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).

Q 48.5 Do 17:30 1B

Measurement induced decoupling of Gaussian Noise for quantum communication — •Metin Sabuncu[1,2], Radim Filip[3], Gerd Leuchs[2], and Ulrik L. Andersen[1,2] — [1]Department of Physics, Technical University of Denmark — [2]IOIP, Max-Planck Forschungsgruppe, Universität Erlangen-Nürnberg, Germany — [3]Department of Optics, Palacky University, Czech Republic

Every communication link is affected by noise. In classical communication the noise does not have a very detrimental influence and can be removed. For quantum communication, however, the effect of this noise becomes much more devastating, normally preventing quantum information processing tasks from being realised. Therefore when performing quantum communication protocols it is crucial to have efficient noise erasing procedures that renders the protocols fault tolerant. We investigate a protocol used in quantum key distribution, where the information is encoded into conjugate continuous variables of a coherent state. We then consider a Gaussian noisy interaction with the environment and show that by performing environmental measurements it is possible to decouple the noise after some suitable measurement induced operations. Using this strategy, the quantum information content of conjugate variables can be ideally recovered independent of the amount of environmental excess noise provided that the state of the environment is fully accessible. We present an experiment in which coherent states are inflicted by Gaussian noise and we present different scenarios how to decouple the noise in the channel via measurement induced operations and compare it to the theory.

Q 48.6 Do 17:45 1B

Time-Bin Encoding for Narrow-Band Single Photons — •Nils Neubauer, Matthias Scholz, and Oliver Benson — Humboldt-Universität zu Berlin, Institut für Physik, AG Nanooptik, Hausvogteiplatz 5-7, 10117 Berlin

For long-range applications in quantum information processing (e.g., quantum key distribution QKD), time-bin encoding of single photons is the favorable choice since this scheme does not suffer from polarization degradation in optical fibers. In order to build larger quantum networks, coherent storage and retrieval of single photons in atomic ensembles has been suggested and realized, e.g., by using electromagnetically induced transparency in optically dense media. Therefore, the spectrum of these photons needs to match the narrow linewidth of atomic resonances.

We realized a scheme for time-bin encoding of narrow-band single photons. The setup consists of two unbalanced Michelson interferometers acting as encoding and decoding units. Using a relative arm length difference of 100 m each, a path delay of 500 ns can be implemented, suitable for single photons with a bandwidth of 10 MHz. It is intended to show QKD via the BB84 protocol with attenuated light pulses of this bandwidth.

Q 48.7 Do 18:00 1B

Eavesdropping in quantum cryptography with six mixed states — •Zahra Shadman, Hermann Kampermann, Tim Meyer, and Dagmar Bruss — Institut für Theoretische Physik III,Düsseldorf,Germany

For the case of the six state protocol in the presence of white noise (six mixed states) we express the optimal mutual information for both cases Alice/Bob and Alice/Eve in terms of the noise parameter and the quantum bit error rate. In comparison to the pure state case the crossing point of the two mutual information curves moves to a higher quantum bit error rate. We conclude that the six state protocol with mixed states is more robust against eavesdropping than for pure states.

Q 48.8 Do 18:15 1B

Optical Free-Space Quantum Key Distribution — •Sebastian Schreiner[1], Henning Weier[1], Martin Fürst[1], Tobias Schmitt-Manderbach[1], Christian Kurtsiefer[2], and Harald Weinfurter[1,3] — [1]Department für Physik der LMU München, Schellingstr 4/III, 80799 München — [2]Department of Physics, National University of Singapore, 2, Science Drive 3, Singapore 117542 — [3]Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1,

85748 Garching

The security of quantum key distribution, (QKD) is based on physical laws rather than assumptions about computational complexity: An adversary will necessarily disturb the communication by his quantum measurement. This leads to an error rate in the generated keys which allows to calculate an upper bound on the information eavesdropped. However, real implementations will be sensitive to side-channel attacks, i.e. to information losses due to distinguishabilities in other degrees of freedom, which an adversary can measure without causing errors.

Here we report on progress of our implementation of the BB84 protocol installed on top of two university buildings in downtown Munich. Using attenuated laser pulses in combination with decoy states we can establish a key over a distance of 500˜m. Our system is fully remote controlled and allows for continuous and fast QKD. Additionally it is fully characterized with respect to spectral, temporal and spatial side-channels and so can guarantee secure key exchange. Our experiments proof free-space QKD to be feasible, providing high key rates while still staying both robust and simple.

Q 48.9 Do 18:30 1B

Distillation of entangled state after a fading channel — •Ruifang Dong[1], Mikael Lassen[2], Christoph Marquardt[1], Radim Filip[1], Ulrik L. Andersen[2], and Gerd Leuchs[1] — [1]Institute for Optics, Information and Photonics,Max-Planck Researchgroup, University Erlangen-Nuernberg, Guenther-Scharowsky-Str. 1, 91058, Erlangen,Germany — [2]Department of Physics, Technical University of Denmark, Building 309, 2800 Lyngby, Denmark

We report on the experimental distillation of a continuous variable polarization entangled state which is affected by a fading channel. We produce a polarization entangled state by mixing two fiber-based polarization squeezing states at a beam splitter [1]. After the beam splitter, one part of the entangled beams is subject to a fading channel. Such channel may exhibit any kind of random distribution of the attenuation. In the experiment, to simulate the fading channel and implement the distillation, we insert a variable optical attenuator into one of the entangled beams and tap off a small portion of the attenuated beam for post selection [2], the joint measurement on the corrupted entangled beams is also made for verification. Then by setting various different attenuation levels, we achieve a series of data from tap measurements and verification measurements which are collected by A/D card into computer. Later, all the measured data can be mixed in the computer with certain distribution form and a destroyed entangled state after a certain fading channel is simulated. Based on such procedure, the distillation can be succeeded and a recovery of the original entangled state is obtained with an accessible success probability.

Q 48.10 Do 18:45 1B

Experimental aspects of deterministic secure quantum key distribution — •Nino Walenta[1], Dietmar Korn[1], Dirk Puhlmann[1], Timo Felbinger[1], Kim Boström[2], Holger Hoffmann[1], and Martin Ostermeyer[1] — [1]Universität Potsdam, Institut für Physik, 14469 Potsdam — [2]Universität Münster, 48149 Münster

Most common protocols for quantum key distribution (QKD) use non-deterministic algorithms to establish a shared key. But deterministic implementations can allow for higher net key transfer rates and eavesdropping detection rates. The Ping-Pong coding scheme by Boström and Felbinger [1] employs deterministic information encoding in entangled states with its characteristic quantum channel from Bob to Alice and back to Bob.

Based on a table-top implementation of this protocol [2] with polarization-entangled photons fundamental advantages as well as practical issues like transmission losses, photon storage and requirements for progress towards longer transmission distances are discussed and compared to non-deterministic protocols. Modifications of common protocols towards a deterministic quantum key distribution as in [3] are addressed.

[1] K. Boström, T. Felbinger. Phys. Rev. Lett. 89 187902 (2002)

[2] M. Ostermeyer, N. Walenta. arXiv:quant-ph/0703242v1

[3] M. Lucamarini, J. S. Shaari, M.R.B. Wahiddin. arXiv:0707.3913v1