Q 47: Quanteninformation (Quantenkommunikation)

Zeit: Mittwoch 16:30–18:45 Raum: 5L

Q 47.1 Mi 16:30 5L

Towards the Solution of NP Problem: Indistinguished controllable single photons from independent atomic ensembles — •Yu-Ao Chen[1], Shuai Chen[1], Markus Koch[1], Thorsten Strassel[1], Zhen-Sheng Yuan[1], Jörg Schmiedmayer[2], and Jian-Wei Pan[1] — [1]Physikalisches Institut, Universität Heidelberg, Philosophenweg 12, D-69120 Heidelberg, Germany — [2]Atominstitut der Österreichischen Universitäten, TU-Wien, A-1020 Vienna, Austria

Quantum repeater hold the promise for revolutionary advances to solve the NP problem from the losses and decoherence in the communication channel by a distribution of quantum resources over remote locations and quantum memory.

We use collective spin excitation of atoms as a media for quantum memory. Here we present an implementation of feed forward control of two atomic memories. We use independent "write" laser sources to map the quantum states to the collective spin excitation and again we use independent "read" lasers to retrieve the quantum states from the two atomic memories respectively. We will show that, by using a feed forward circuit, the probability of simultaneously obtaining a pair of single photons will be increased by orders of magnitude. As an application, we show the indistinguishability of independently generated single photons by the observation of destructive interference of their wave packets. Our results demonstrate experimentally a basic principle for enabling scalable quantum communication networks and linear optical quantum computation.

Q 47.2 Mi 16:45 5L

Secret key rates for quantum key distribution scenarios with finite number of signals — •Tim Meyer, Hermann Kampermann, Matthias Kleinmann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany

We analyze the success of privacy amplification [1] (in terms of secret key rates) in the six-state protocol subjected to a symmetric, collective eavesdropping attack, for any finite number of signals [2]. Starting from a simple entanglement-based scheme, we can include multiphoton pulses into our model, and study its applicability for a realistic prepare-and-measure version.

[1] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[2] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß, Phys. Rev. A **74**, 042340 (2006).

Q 47.3 Mi 17:00 5L

The role of memory errors in quantum repeaters — •Lorenz Hartmann[1], Barbara Kraus[1], Hans Briegel[1,2], and Wolfgang Dür[1,2] — [1]Institut für Theoretische Physik, Universität Innsbruck, Österreich — [2]Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Innsbruck, Österreich

We investigate the influence of memory errors in the quantum repeater scheme for long-range quantum communication. We show that the communication distance is limited in standard operation mode due to memory errors resulting from unavoidable waiting times for classical signals. We show how to overcome these limitations by (i) improving local memory, and (ii) introducing two new operational modes of the quantum repeater. In both operational modes, the repeater is run blindly, i.e. without waiting for classical signals to arrive. In the first scheme, entanglement purification protocols based on one-way classical communication are used allowing to communicate over arbitrary distances. However, the error thresholds for noise in local control operations are very stringent. The second scheme makes use of entanglement purification protocols with two-way classical communication and inherits the favorable error thresholds of the repeater run in standard mode. One can increase the possible communication distance by an order of magnitude with reasonable overhead in physical resources. We outline the architecture of a quantum repeater that can possibly ensure intercontinental quantum communication.

Q 47.4 Mi 17:15 5L

Private States, Privacy Amplification, and the Uncertainty Principle in Quantum Cryptography — •Joseph Renes[1] and Jean-Christian Boileau[2,3] — [1]Institut für Angewandte Physik, TU Darmstadt, Darmstadt, Germany — [2]Institute for Quantum Computation, University of Waterloo, Waterloo, Canada — [3]Perimeter Institute for Theoretical Physics, Waterloo, Canada

Quantum cryptography has typically dealt with the problem of extracting a secret key from a partially private string in one of three ways, corresponding to different treatment of the parties to the cryptographic protocol. Use of two-universal hash functions, termed classical privacy amplification, comes from considering the eavesdropper's quantum state. Alternatively, focusing on the state held by the honest parties can be done either concretely in private state distillation or abstractly as in the approach based on the uncertainty principle. We show that these three are equivalent and interchangeable, unifying the corresponding security proofs of quantum key distribution. By adapting the security proof based on the uncertainty principle, we construct a new protocol for private state distillation which we then prove is identical to classical privacy amplification. Underlying this approach is a new characterization of private states, quantum states capable of generating a secret key, whose relation to their standard formulation is again understood as an instance of the uncertainty principle: A key corresponding to measurement of a given observable is private when the honest parties have full knowledge of the conjugate observable.

Q 47.5 Mi 17:30 5L

Photon Number Statistics of Waveguided Parametric Downconversion — •Malte Avenhaus, Andreas Eckstein, and Christine Silberhorn — Max-Planck-Nachwuchsgruppe für Integrierte Quantenoptik, Erlangen, Germany

Quantum cryptography requires precise knowledge about the quantum states which are communicated over a quantum channel. Especially, the photon number distribution of the quantum light source characterizes the security and performance of practical systems. By detecting impinging photons on highly efficient APDs in Geiger mode, one can only gain binary information, but no resolution regarding actual photon numbers. In our experiment, we use a time multiplexing device distributing photons randomly over several temporal slots. For reconstruction of the actual photon statistics, one needs to take into account losses and the possibilities of n photons being observed in m temporal slots.

We investigate the properties of photon number statistics from a Type-II parametric downconversion (PDC) processes at different pump powers. The resulting statistics from different experimental configurations are compared against correlated thermal and Poissonian distributions, which can be expected for PDC sources.

Q 47.6 Mi 17:45 5L

Quantum key distribution over 144 km — •Martin Fürst[1], Henning Weier[1], Tobias Schmitt-Manderbach[2], Sebastian Schreiner[1], Christian Kurtsiefer[3], and Harald Weinfurter[1,2] — [1]LMU München, Schellingstr 4/III, 80799 München — [2]Max Planck Institut für Quantenoptik, Hans-Kopfermann-Str. 1, 85748 Garching — [3]National University of Singapore, 2, Science Drive 3, Singapore 117542

Quantum mechanics ensures the possibility of secure exchange of information between two parties. Several implementations of free space quantum key distribution (QKD) systems exist achieving distances on the order of ten kilometres. QKD on a global scale could be accomplished by free space systems connecting satellites and ground stations. As first steps towards this goal we performed an experiment over a distance of 144 km on the Canary Islands. The transmitter unit including a 15 cm diameter telescope was located on mount Roque de los Muchachos on La Palma. On Tenerife the Optical Ground Station (OGS), developed for optical communication to and from satellites, was used as the receiving telescope. Thanks to an actively controlled bidirectional tracking system the transmission loss of the link was stable with an attenuation between 25 dB and 35 dB over the whole night. We implemented the decoy state QKD protocol to establish a secure key at a rate of 40 bits/s. As this attenuation is also expected for downlinks from low earth orbit (LEO) satellites to ground stations, our experiment thus demonstrates the feasibility for space-based secure communication across the globe.

Q 47.7 Mi 18:00 5L

Quantum Key Distribution: Closing the Gap to Perfect Sources — •Wolfgang Mauerer and Christine Silberhorn — University Erlangen-Nuremberg, Max-Planck Research Group IOIP, Integrated Quantum Optics Group

Quantum key distribution (QKD) allows two parties to communicate securely even in the presence of an arbitrarily powerful eavesdropper. A multitude of protocols have been suggested in the last decades. They were shown to be secure in the presence of

the bit rates over which secure communications can be guaranteed are strongly constricted by experimental imperfections. Decoy-state QKD improves the situation, but achieves only about (70%) of the maximal secure distance imposed by fundamental physics with conventional implementations.

In this talk, we show how we can close the gap between practical QKD implemented with state-of-the-art devices and idealized QKD assuming perfect single-photon signals. A parametric downconversion (PDC) source in conjunction with a photon number resolving detector is utilized to implement a decoy-like QKD scheme. It allows to improve the effectively sent signal statistics. Strict photon-number correlations between the two PDC outputs allow to infer the complete statistical information about one of them by measuring the photon number distribution of the other. For all practical purposes, our protocol accomplishes up to few percent the power of a single photon source in terms of distance, while the key generation rate is on par with the best available schemes.

Q 47.8 Mi 18:15 5L

Experimental realisation of a quantum communication protocol using entangled photons — •Nino Walenta and Martin Ostermeyer — Universität Potsdam, Institut für Physik, 14469 Potsdam

Quantum cryptography protocols using entangled qubit pairs can increase the rate and security of information exchange. The ping pong coding scheme based on entangled photons allows asymptotically secure key distribution and, theoretically, quasi secure direct communication, too [1]. In this presentation we show the experimental realisation of this communication protocol.

Polarisation-entangled photon pairs are generated by parametric down conversion with ps laser pulses. Two out of 4 Bell states are used in order to represent two bits of information. The information is encoded by switching between these two states via the unitary transformation of a Pockels cell applied to one of the photons. The two Bell states are distinguished by a modified Bell state analysis evaluating the arrival time and also the polarisation of the photons. The detection time of every photon is analysed using time-correlated single photon counting (TCSPC) modules in time-tag mode for every detector.

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

Q 47.9 Mi 18:30 5L

Quantum teleportation between light and matter — •Hanna Krauter[1], Jacob Sherson[1], Rasmus Olsson[1], Brian Julsgaard[1], Klemens Hammerer[2], Ignacio Cirac[2], and Eugene Polzik[1] — [1]Niels Bohr Institute, Blegdamsvej 17, Copenhagen, Denmark — [2]Max Planck Institut für Quantenoptik, Hans-Kopfermann-Str. 1, Garching, Germany

In this talk the first experimental demonstration of interspecies teleportation between an atomic and a photonic object will be discussed.

The state of a mesoscopic light pulse containing up to a few hundred photons is transferred onto the collective state of an atomic ensemble of 10ˆ12 Cesium atoms over a distance of 0.5m. This is an important step towards e.g. distributed quantum networks.

The general principles of disembodied transfer via teleportation will be introduced and our physical implementation presented in greater detail. Furthermore the possibility to improve the protocol by including higher order temporal modes and the use of a squeezed light beam will be discussed.