Q 76 Poster Quantenkommunikation

Zeit: Donnerstag 16:30–18:30 Raum: Labsaal

Q 76.1 Do 16:30 Labsaal

Asymptotic correctability of Bell-diagonal quantum states and maximum tolerable bit error rates — •Kedar Ranade and Gernot Alber — Institut für Angewandte Physik, TU Darmstadt, 64289 Darmstadt

The general conditions are discussed which quantum state purification protocols have to fulfill in order to be capable of purifying Bell-diagonal qubit-pair states, provided they consist of steps that map Bell-diagonal states to Bell-diagonal states and they finally apply a suitably chosen Calderbank-Shor-Steane code to the outcome of such steps. As a main result a necessary and a sufficient condition on asymptotic correctability are presented, which relate this problem to the magnitude of a characteristic exponent governing the relation between bit and phase errors under the purification steps. These conditions allow a straightforward determination of maximum tolerable bit error rates of quantum key distribution protocols whose security analysis can be reduced to the purification of Bell-diagonal states.

Q 76.2 Do 16:30 Labsaal

Avalanche photodetection for applications with high repetition rates — •Hendrik Coldenstrodt and Christine Silberhorn — Max-Planck-Nachwuchsgruppe, Günther-Scharowsky Str.1 / Bau 24, 91058 Erlangen

Quantum communication requires single photon detection, implying the use of avalanche photo diodes (APDs). If one wants to operate APDs at the highest feasible bit rates in cw-operation, a correction factor is typically taken into account for increasing count rates. An other interesting field, where effective high repetition rates have to be considered, is the use of APDs in time multiplexing detectors for photon number resolution[1]. Thus an essential task is to determine the properties of the correction factor and a threshold frequency below which the APDs yield reliable data for pulsed systems.

We investigated the properties of APDs with a ps-pulsed diode laser at 805nm and repetition rates between 0.5MHz and 80MHz. Different levels of attenuation were applied, such that we were able to identify the regime of linear APD operation, in dependence of the repetition frequency and the mean optical power. The linearity at high repetition rates is limited by the APD dead time and a non-linearity arises at higher photon-numbers due to multiphoton events. Assuming Poissonian input light statistics we ascertained the mean photon-number of the incident light with high accuracy. The results are compared to the statistics obtained using an advanced time multiplexing detector, allowing for data rates up to 1MHz.

[1] D. Achilles et al. *J. Mod. Opt.* **51**, 1499 (2004)

Q 76.3 Do 16:30 Labsaal

Experimental Quantum State Distillation: comparison between single photon and homodyne detection — •Dominique Elser[1], Christoffer Wittmann[1], Stefan Lorenz[1], Radim Filip[1,2], Ulrik L. Andersen[1], and Gerd Leuchs[1] — [1]Institute of Optics, Information and Photonics (Max Planck Research Group), University of Erlangen-Nuremberg, Günther-Scharowsky-Str. 1, Building 24, 91058 Erlangen, Germany — [2]Department of Optics, Research Center for Optics, Palacky University, 17. Listopadu 50, 77200 Olomouc, Czech Republic

Every practical quantum channel degrades the quality of quantum states transmitted between two parties. In order to establish a communication with a low error rate, it is therefore important to determine and if possible to decrease the influence of noise in the quantum channel.

We investigate an optical quantum channel with non-Gaussian noise characteristics transforming a signal state into a statistical mixture of signal and vacuum. The task of the distillation process is to recover the pure signal state. A possible application of this device is a quantum relay.

In this contribution we compare the distillation performance of single photon detection and homodyne measurement. After coherent signal states have passed through a noisy channel, a part of the beam is tapped off and measured in the distillation device. The information obtained hereby is used to condition further measurements of the signal.

Q 76.4 Do 16:30 Labsaal

Free-Space QKD — •Ivan Ordavo[1], Henning Weier[1], Tobias Schmitt-Manderbach[1], Christian Kurtsiefer[1,2], and Harald Weinfurter[1,3] — [1]Sektion 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

Quantum information theory ensures the possibility of secure exchange of information between two parties.

A variety of real-world implementations promises the realisation of quantum-cryptography based metropolitan area networks within a few years. In this work we report on progress of our QKD test-system, a prototype for an urban link, located in downtown Munich. The apparatus consists of a transmitter and receiver unit, both sited on rooftops of two university buildings at a distance of 500 m; a free space link provides the quantum channel, while a public internet connection serves as the classical channel. A completely automated alignment procedure and data-processing software for key extraction and privacy amplification complete the setup. In our implementation, properly attenuated laser pulses are used, where raw-key bits are encoded into four photon polarisation-states. Tests with BB84 protocol were performed, leading to an average sifted-key rate of about 50kbit/s. Such a compact, stand-alone free space hardware is also an obvious prerequisite for future applications, e.g. earth-satellite global QKD system.

Q 76.5 Do 16:30 Labsaal

Generation of Single-Photon Pairs with Cold Atoms as Quantum Memory — •Thorsten Strassel, Yu-Ao Chen, Dennis Heine, Shuai Chen, Jörg Schmiedmayer, and Jian-Wei Pan — Physikalisches Institut , Universität Heidelberg, Philosophenweg 12, 69120 Heidelberg

A source of correlated photon pairs with controllable delay using quantum memory can be used in protocols for long-distance quantum communication such as the DLCZ scheme [1]. We report on our work towards extension of the memory time. The single photons are generated by spontaneous Raman scattering on the D1-line in cold Rubidium atoms. A cold atom cloud of ^{87}Rb serving as quantum memory is prepared in a magneto-optical trap (MOT). It can be demonstrated that the correlation measurements of the photon pairs violate the Cauchy-Schwarz inequality which is valid for classical light.

[1] L.-M. Duan, M. D. Lukin, J.I. Cirac, and P. Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414:413, Nov 2001.

Q 76.6 Do 16:30 Labsaal

STOKES PARAMETER SQUEEZING IN PHOTONIC CRYSTAL FIBERS — •Josip Milanovic, Ch. Marquardt, J. Heersink, U.L. Andersen, and G. Leuchs — Institute of Optics, Information and Photonics, Max Planck Research Group, University of Erlangen-Nuremberg, Guenther-Scharowsky-Str. 1, 91058 Erlangen

We report the generation of squeezing at 800nm of continuous variable Stokes parameters, i.e. polarization squeezing using a single pass through a photonic crystal fiber (PCF) exploiting the Kerr non-linearity. Squeezing in this case means that the variance of one of the Stokes operators is below the quantum noise limit. This is verified by a Stokes parameter measurement. Because it is an intensity dependent effect we use intense ultra short pulses (120 fs at 810 nm) in our experiments. A similar experiment has been performed at a different wavelength (1500 nm) using a standard step-index fiber (1). In our experiment, new features of the PCF are to be investigated especially the larger non-linearity compared to a standard step-index fiber. The choice of the wavelength is motivated by photodiodes with higher quantum efficiency and therefore better detection efficiency and nearby atomic transitions of alkali atoms.

References: (1) Joel Heersink et al., OPTICS LETTERS / Vol. 30, No. 10 / May 15, (2005) Q 76.7 Do 16:30 Labsaal

Secret key rate in tomographic quantum cryptography with a finite number of signals — •Tim Meyer, Matthias Kleinmann, Hermann Kampermann, and Dagmar Bruss — Institut für theoretische Physik, Universität Düsseldorf, Universtätsstr. 1, 40225 Düsseldorf

We calculate the minimum key length achievable with the "tomographic key distribution protocol" \Zitat{1}{D. Bruß et. al., PRL 91, 097901 (2003)}. This protocol is an extension of the six-state protocol, with the main twist that Alice and Bob do not discard events, in which they measured in a different basis, but use this data to do state tomography. We use recent results by \Zitat{2}{R. Renner, N. Gisin, and B. Kraus, PRA 72, 012332 (2005)} where bounds on the secret key rate for the limiting case of an infinite number of signals were derived. In contrast to their work, we explicitly calculate the key length for a finite number of signals, without taking the asymptotic limit. Thus, our method is useful for a realistic scenario of quantum key distribution.

Q 76.8 Do 16:30 Labsaal

Quantum key distribution with decoy states generated by photon number resolution — •Wolfgang Mauerer and Christine Silberhorn — University Erlangen-Nuremberg, Max-Planck Research Group IOIP, Integrated Quantum Optics Group

We present ongoing work on the security analysis of a novel quantum key distribution scheme (QKD) based on parametric downconversion with photon number resolving detectors (PNRDs) used to select decoy states. Although a growing number of security proofs for QKD schemes is available for different scenarios, it is still hard to realise such schemes in practice without introducing security flaws which are not considered in the theoretical description. Additionally, the efficiency of most schemes quickly fades away when longer distances and thus increased losses are taken into account. Possible countermeasures are setups which are simple and robust to implement and the use of decoy states; both form the core of our scheme.

We use the properties of a recently devised PNRD[1] to generate decoy states[2] by conditioning the decoy state preparation on the result of the photon number measurement (PNM). We expect this to be more efficient than signal state preparation based on the PNM as used by Ref.[3]; additionally, our scheme should be easier to implement in practice than other decoy state schemes because no active optical elements are necessary for our approach.

[1] H.-K. Lo, X. Ma, K. Chen, Physical Review Letters **94**, 230504 (2005)
[2] D. Achilles et al., J. Mod. Opt. **51**, 1499 (2004)
[3] T. Horikiri et al., Phys. Rev. A **72**, 012312 (2005)