Q 58 Quantenkommunikation

Zeit: Donnerstag 11:10–12:40 Raum: HVI

Q 58.1 Do 11:10 HVI

Provable entanglement and security bounds of two-basis QKD protocols using qudits — •Georgios Nikolopoulos and Gernot Alber — Institut für Angewandte Physik, Technische Universität Darmstadt, D-64289 Darmstadt

It has been shown that a necessary precondition for secret key-distillation is that the two legitimate users can prove the presence of entanglement (quantum correlations) in their data. Recently [1], we investigated the values of the average disturbance up to which this condition is satisfied in the context of quantum cryptographic protocols using d-level systems. We mainly focused on schemes that use two mutually unbiased bases, thus extending the BB84 quantum key-distribution scheme to higher dimensions. Under the assumption of general coherent attacks, we obtained an analytic expression for the threshold disturbance up to which the two legitimate users of the protocol share provable entanglement. As long as the two legitimate users focus on their sifted key and treat each pair of data independently during the post-processing, our results are valid for arbitrary dimensions. Moreover we investigated the conditions under which an eavesdroper can saturate this theoretical bound, in the context of incoherent and two-qubit coherent attacks [2].

[1] G.M.Nikolopoulos, G.Alber, Phys. Rev. A. 72, 032320 (2005).
[2] G.M.Nikolopoulos, A.Khalique, G.Alber, EPJD (in print).

Q 58.2 Do 11:25 HVI

Quantum Memory and Two-Mode-Squeezing in Atomic Ensembles — •Christine Muschik, Klemens Hammerer, and J. Ignacio Cirac — Max-Planck-Institut für Quantenoptik, Hans Kopfermann-Strasse, D-85748 Garching, Germany

We propose two protocols for atomic ensembles interacting with light. The atomic ensemble is thereby placed in an external magnetic field and provides a fully passive beam-splitter-like or a purely active two-mode-squeezing-like interaction depending on the orientation of the external field. The passive version of the proposed experiment can be used as a quantum memory. A coherent pulse of light or a light-qubit can be written onto the spin state of the atoms and subsequently be read out. Remarkably the fidelity of the state transfer approaches unity exponentially in the coupling strength. The active version of the setup creates an EPR state between atoms and light respectively. The produced interspecies correlations produced in the scheme can be used to perform quantum teleportation and unconditional squeezing on the collective spin of the atomic sample. Spin squeezing which grows exponentially in the coupling can be achieved. Both protocols are shown to be robust against the dominant sources of noise.

Q 58.3 Do 11:40 HVI

Practical quantum key distribution with two-way classical communication — •Aeysha Khalique, Georgios M. Nikolopoulos, and Gernot Alber — Institut für Angewandte Physik, Technische Universität Darmstadt, D-64289 Darmstadt.

We investigate the key generation rates and achieveable distances for conventional Bennett-Brassard and six state protocols under realistic conditions using two-way purification protocols and Calderbank-Shor-Steane codes. In particular, we analyse the photon number splitting attack where legitimate users lack single photon sources and have lossy channels and inefficient detectors. Our analysis shows that two-way classical communication protocols increase the distance up to which a secret key can be distilled without compromising much on the key generation rate. Two-way classical communication protocols also help to suppress the sudden dip in key generation rate due to dark counts.

[1] D. Gottesman, H-K Lo, N. Lütkenhaus and J. Preskill, Quant. Inf. and Comp. **4**, 325 (2004).
[2] D. Gottesman, H.-K. Lo, IEEE Trans. Inf. Th. **49**, 457 (2003).
[3] A. Khalique, Georgios M. Nikolopoulos and G. Alber (in preparation).

Q 58.4 Do 11:55 HVI

Effective Channels in Quantum Key Distribution — •Joseph Renes[1] and Markus Grassl[2] — [1]University of Darmstadt — [2]University of Karlsruhe

Quantum key distribution highlights the power of quantum mechanics to improve information-theoretic tasks, showing that even a modest use of quantum information can have a profound impact on which sorts of possible protocols. For distributing a secret classical key to two separated parties, only the ability to prepare, transmit, and measure quantum states is needed; delicate mulitparticle superpositions are not required. Upon completion of the quantum phase of the protocol, classical means of distilling the key can begin.

Formulating both parts of the protocol in entirely quantum-mechanical terms enables us to describe the whole enterprise as a quantum channel. From this perspective, the goal of the protocol is then to use this channel to create virtual entanglement between the parties. Then the monogamy of entanglement implies that classical keys reated from it are truly secret. While entanglement is not physically required, it arises virtually since to an eavesdropper the prepare and measure scheme is consistent with a protocol using actual entanglement.

For QKD schemes possessing a high degree of symmetry, including essentially all protocols studied to date, the effective quantum channel takes on an especially simple form. We show how to determine the relevant symmetry operations and employ them to arrive at this description. This enables us to establish the security of a wide range of protocols, including in particular those based on equiangular spherical codes.

Q 58.5 Do 12:10 HVI

Vakuum Squeezing durch Austauschen von Seitenbändern — •Jessica Schneider, Oliver Glöckl, Ulrik Andersen und Gerd Leuchs — Institut für Optik, Information und Photonik, Max-Planck Forschungsgruppe, Universität Erlangen-Nürnberg, Günther-Scharowsky-Str. 1, 91058 Erlangen

Gequetschte Vakuumzustände sind ein wichtiger Baustein in der Quantenoptik. Wir stellen ein Experiment vor, das es ermöglicht, Vakuum Squeezing für bestimmte Seitenbandfrequenzen aus gequetschtem, hellem, gepulstem Licht mit Hilfe eines Mach-Zehnder-Interferometers zu produzieren[1,2].

Mit diesem Interferometer, welches zwei verschieden lange Arme besitzt, wird Vakuum Squeezing erzeugt, indem die Seitenbänder eines hellen amplitudengequetschten Strahls (entstanden in einem Faser-Sagnac-Interferometer durch Ausnutzen der Kerr-Nichtlinearität) mit denen eines Vakuumeingangs vertauscht werden.

Wir zeigen experimentelle Ergebnisse, die 2 dB squeezing im dunklen Ausgangsstrahl belegen.

[1] O. Glöckl et al., Opt. Lett. 29, 1936 (2004)
[2] E. H. Huntington et al., Phys. Rev. A 71, 041802 (R) (2005)

Q 58.6 Do 12:25 HVI

Remote State Preparation of a Single Atom — •Wenjamin Rosenfeld[1], Stefan Berner[1], Markus Weber[1], Jürgen Volz[1], and Harald Weinfurter[1,2] — [1]Department for Physics of LMU, 80799 München — [2]Max-Planck-Institute of Quantum Optics, 85748 Garching

Entanglement is a key element of quantum information and communication applications. Of special interest is entanglement between different quantum objects like photons and atoms because it enables one to transfer an arbitrary quantum state from one atom to another at a remote location. This forms the basic ingredient for quantum repeater and quantum networks.

Here we demonstrate the remote state preparation of a single optically trapped Rb atom. In the first step the spin state of the atom is entangled with the polarization of a spontaneously emitted photon. Then an additional degree of freedom (spatial mode in an interferometer) is imprinted onto the photon. Performing a projective Bell state measurement on the resulting two-qubit photonic state, together with four local unitary transformations, finally allows to transfer any desired quantum state to the remote atom.