Q 52: Quanteninformation: Quantenkommunikation II

Zeit: Donnerstag 16:30–19:00 Raum: Audi-B

Q 52.1 Do 16:30 Audi-B

Towards device independent security in quantum cryptography — •Torsten Franz and Reinhard Werner — Institut für Mathematische Physik, TU Braunschweig

Quantum cryptography enables two parties to perform private communication. Crucial for the security are the assumptions, which have to be made about the practical implementation of the theoretical protocol. In the device independent scenario one tries to consider only as few assumptions as possible, while still guaranteeing security even against the most general, i.e. coherent, attacks. We will present results on the problem in a black-box scenario.

Q 52.2 Do 16:45 Audi-B

Sicherheitsanalyse eines quantenkryptographischen Protokolls von Barrett, Hardy & Kent — •Rainer Plaga — Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Barrett, Hardy and Kent haben ein quantenkryptographisches Protokoll vorgeschlagen, dessen Sicherheit bewiesen werden kann, ohne die Annahme zu machen, dass die Gesetze des Quantenphysik absolut korrekt sind (Phys. Rev. Lett. 95 (2005), 010503). Benötigt wird auschliesslich die Annahme dass keine überlichtschnellen Signal ausgetauscht werden können. Ich analysiere die Rolle einer weiteren Zusatzanahme, die von den Autoren explizit gemacht wird. Ein Angriff der die spezielle Relativitättheorie respektiert und ohne diese Zusatzanahme erfolgreich ist, wird vorgestellt.

Q 52.3 Do 17:00 Audi-B

Quantum control of noisy channels — •Raffaele Romano and Peter van Loock — OQI Group, Max-Planck Research Group, Institute of Optics, Information and Photonics, University of Erlangen-Nuernberg

Title: Quantum control of noisy channels
Abstarct: We present a formalism that paves the way to the application of control theoretical tools to the analysis of noisy channels [1]. The control parameters are given by the resources available to sender and receiver, that is local operations and classical communication (LOCC), and entanglement shared among the two parties through their local ancillas. By using the Choi-Jamiolkowski isomorphism between completely positive maps and (non-normalized) states [2], we show how a noisy channel is manipulated by these controls, and provide some preliminary results based on this formalism. In particular, we prove that standard Quantum Teleportation is the only deterministic scheme that can perfectly correct an arbitrary noisy channel relying on a single use of the channel (that is, with one-way communication) [3]. Moreover, we discuss a hybrid protocol based on both Quantum Teleportation and Quantum Error Correction to faithfully transmit quantum states through specific noisy channels.
References:
[1] R. Romano, P. van Loock, arXiv:0811.3014
[2] A. Jamiolkowski, Rep. Math. Phys. 3, 275 (1972)
[3] R. Romano, P. van Loock, in preparation

Q 52.4 Do 17:15 Audi-B

On superdense coding with noisy channels — •zahra shadman, hermann kampermann, and dagmar bruss — Heinrich-Heine-Universität, Institut für Theoretische Physik III, Düsseldorf, Deutschland

We study the capacity of a superdense coding protocol in the case of a noisy channel. We consider the case where the channel acts on Alice's side, and the one where it acts both on Alice's and Bob's side. In the latter case, the noise can be correlated or uncorrelated. We study various noise models and various bipartite input states, and derive the optimal capacity.

Q 52.5 Do 17:30 Audi-B

Quantum error correction for hybrid quantum repeater — •Nadja Bernardes and Peter van Loock — OQI Group, Max Planck Research Group, Institute of Optics, Information and Photonics, University Erlangen-Nuremberg, Germany

We discuss quantum error correction (QEC) protocols for quantum repeaters based upon atomic qubit-entanglement distribution through optical coherent-state communication (hybrid quantum repeater). The effect of photon losses on a coherent-state qubit is a decrease of the coherent-state amplitude and a random phase flip error; the latter effect leads to the distribution of imperfect entanglement between neighboring repeater stations, when the light field is sent through the lossy communication channel and subsequently measured for conditional two-qubit entangled-state preparation. The conceptually simplest approach is then to perform entanglement distillation and swapping on the level of the qubit states in order to enhance the fidelity and increase the distance of the distributed entangled states. However, this approach requires complicated local quantum logic. Here we consider alternative ways to suppress the effect of photon losses for entanglement distribution. In particular, QEC codes can be applied to the optical mode that mediates the interaction between the qubits. An example for a possible QEC scheme is similar to the well-known 3-qubit phase flip code. We describe a scheme in which this code is employed for entanglement distribution and compare its performance with the canonical schemes based upon entanglement distillation.

Q 52.6 Do 17:45 Audi-B

Communicating at the quantum speed limit using optimal control — •Michael Murphy[1], Tommaso Caneva[3], Simone Montangero[1], Vittorio Giovanetti[2], Tommaso Calarco[1], Rosario Fazio[2,3], and Guiseppe Santoro[3] — [1]Institut für Quanteninformationsverarbeitung, Universität Ulm, Albert-Einstein-Allee 11, D-89069 Ulm, Germany — [2]NEST-CNR-INFM & Scuola Normale Superiore, P.zza dei Cavalieri 7,56126 Pisa, Italy — [3]International School for Advanced Studies (SISSA), Via Beirut 2-4, I-34014 Trieste, Italy

Optimal control theory is a promising candidate for a drastic improvement of the performance of quantum information tasks. We explore its ultimate limit in the case of a one-dimensional chain of coupled spin-1/2 particles, and demonstrate that it coincides with the ultimate speed limit allowed by quantum evolution (the quantum speed limit), such that optimal control reaches the best performance allowed by the laws of quantum mechanics.

Q 52.7 Do 18:00 Audi-B

Optimizing Gaussian communication for hybrid quantum repeater — •Ludmila Praxmeyer and Peter van Loock — OQI Group, Max Planck Research Group, Institute of Optics, Information and Photonics, University Erlangen-Nuremberg

For long distance quantum communication, distribution of entanglement over large distances, overcoming effects of noise and decoherence, is needed. Various quantum repeater schemes [1] were proposed to provide a theoretical solution to this problem. We shall present an optimized version of the hybrid quantum repeater [2,3], based on Gaussian optical-state communication and Gaussian, homodyne-based, conditional entangled state preparation. We show that use of squeezed light significantly increases the fidelity of states obtained while probability of success is aintained. We also show that hybrid entanglement swapping [4] between squeezed states of light and atoms in the cavity makes scheme [2] more practical compared to the case when entanglement swapping is performed solely on the level of the atoms.

References:
[1] H.-J. Briegel *et al.*, Phys. Rev. Lett. **81**, 5932 (1998),
[2] P. van Loock *et al.*, Phys. Rev. Lett. **96**, 240501 (2006),
[3] T. D. Ladd *et al.*, New J. Phys. **8**, 164 (2006),
[4] P. van Loock *et al.*, Phys. Rev. A **78**, 062319 (2008).

Q 52.8 Do 18:15 Audi-B

Quantum key distribution based on general finite-dimensional systems — •Kedar S. Ranade and Gernot Alber — Institut für Angewandte Physik, Technische Universität Darmstadt

It is well-known that qubit-based quantum key distribution protocols can be generalised to protocols based on higher dimensional information carriers (so-called qudits). We prove security bounds for qudit-based prepare-and-measure protocols, which may use both one-way and two-way error correction, by generic means of evaluating such bounds through associated entanglement-based protocols.

Q 52.9 Do 18:30 Audi-B

Continuous-variable quantum key distribution with qudits —

•Ulrich Seyfarth and Gernot Alber — Institut für Angewandte Physik, Technische Universität Darmstadt, D-64289 Darmstadt

A generalisation of the continuous-variable protocol investigated by Grosshans and Grangier [1] is proposed. Secret key rates are evaluated for cases in which an eavesdropper can extract information by beam-splitting attacks. These rates are calculated for direct and reverse reconciliation over the channel transmittivity. Optimisations of this protocol are discussed.

[1] F. Grosshans and P. Grangier, Phys. Rev. Lett. 88,57902 (2002).

Q 52.10 Do 18:45 Audi-B

Quantum key distribution using phase-shift keying — •Denis Sych and Gerd Leuchs — Max-Planck-Institut für die Physik des Lichts, IOIP, Universität Erlangen-Nürnberg, Günther-Scharowsky-Str. 1, Bau 24, 91058 Erlangen, Deutschland

We report on the detailed analysis of a new protocol for continuous variable quantum key distribution using phase-shift keying. The novelty of the protocol is a multi letter alphabet consisting of coherent states of light with a fixed amplitude and variable phase. Information is encoded in the phase of a coherent state which can be chosen from a regular discrete set consisting, however, of an arbitrary number of letters from two to infinity. Thus our protocol can be regarded as a smooth transition between the protocols based on discrete and continuous modulation of coherent states.

We evaluate the security of the protocol against the beam-splitting and intercept-and-resend attacks. For error correction we consider the direct and reverse reconciliation schemes, both idealized and realistic. We investigate how imperfections of the realistic error correction schemes affect the key rate. As a result we show that the secret key generation rate of the proposed protocol can be of an order higher than that of the binary phase encoding. The optimal parameters (number of letters, amplitude of the signal, and postselection thresholds) are explicitly presented.