Q 33: Quantum Information: Quantum Communication 2

Time: Wednesday 14:30–16:00 Location: SCH A118

Q 33.1 Wed 14:30 SCH A118

Quantum key distribution with finite resources: Coherent vs. Collective attacks — •Markus Mertz, Silvestre Abruzzo, Sylvia Bratzik, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Germany

In QKD with finite resources it is known for the assumption of collective attacks, where the eavesdropper is forced to interact with each signal independently, how to quantify the length of a secure key. But for the most general attack (coherent attack), we have to adjust the security analysis. Based on the ideas of paper [1] we calculate the quantitative difference between coherent and collective attacks for the BB84 and the six-state protocol, with finite number of signals. Here, we use the smooth min entropy to bound the secure key rate.

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

Q 33.2 Wed 14:45 SCH A118

Probabilistic Phase-Covariant Cloning of Coherent States — •Christian R. Müller[1,3], Christoffer Wittmann[1,3], Petr Marek[4], Radim Filip[4], Mario A. Usuga[2], Christoph Marquardt[1,3], Ulrik L. Andersen[1,2], and Gerd Leuchs[1,3] — [1]Max-Planck-Institut für die Physik des Lichts , Günther-Scharowsky-Str. 1 / Bau 24, 91058 Erlangen, Germany — [2]Department of Physics, Technical University of Denmark, Building 309, 2800 Lyngby, Denmark — [3]Institute for Optics, Information and Photonics, University Erlangen-Nuremberg, Staudtstr. 7/B2, 91058 Erlangen, Germany — [4]Department of Optics, Palacký University 17, listopadu 50, 772 07 Olomouc, Czech Republic

Duplicating an unknown quantum state with high fidelity is at the heart of many quantum information and quantum communication protocols. The laws of quantum mechanics impose strict bounds on the average fidelity that can be achieved deterministically. However, in a probabilistic regime one can overcome these bounds. We present the concept of a novel probabilistic quantum cloner for coherent state alphabets based on the phase concentration scheme presented in [1]. The scheme relies solely on phase-covariant displacements and photon counting ensuring a feasible and robust implementation. We show that our scheme surpasses the deterministic approach with the hitherto highest performance for phase-covariant alphabets [2].

[1] M.A. Usuga, C.R. Müller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs and U.L. Andersen, Nat. Phys. 6, 767 (2010). [2] M.F. Sacchi, Phys. Rev. A 75, 042328 (2007)

Q 33.3 Wed 15:00 SCH A118

Squashing model and applications to quantum key distribution protocols — •Oleg Gittsovich[1], Varun Narasimhachar[1], Ruben Andrei Romero Alvarez[4], Normand Beaudry[5], Tobias Moroder[6], and Norbert Lütkenhaus[1,2,3] — [1]Institute for Quantum Computing & Department of Physics and Astronomy, University of Waterloo, 200 University Avenue West, N2L 3G1 Waterloo, Ontario, Canada — [2]Quantum Information Theory Group, Institute of Theoretical Physics I, University Erlangen-Nuremberg, Staudtstraße 7/B2, 91058 Erlangen, Germany — [3]Max Planck Institute for the Science of Light, Günther-Scharowsky-Straße 1/24, 91058 Erlangen, Germany — [4]Department of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada — [5]Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland — [6]Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Technikerstraße 21A, A-6020 Innsbruck, Austria

Measurements are one of the main ingredients in physics. The description of a particular measurement depends on a variety of factors. First, one has a measurement device, which is assumed to perform a measurement of some physical observable. Second, based on the knowledge what observable one wants to measure, a theoretical model for the device is constructed. This theoretical model is believed to describe the processing of the device faithfully. In this talk we address the question of device modeling and its application to the quantum key distribution (QKD) protocols.

Q 33.4 Wed 15:15 SCH A118

Analysis of the certification of quantum random number generators by Bell's theorem — •Rainer Plaga — Bundesamt für Sicherheit in der Informationstechnik (BSI), 53175 Bonn, Godesberger Allee 185-189

S.Pironio et al. describe a qualitatively novel method to certify quantum random number generators ("Random numbers certified by Bell's theorem" (Nature 464, 1021 (2010)). A qualitative simplification and/or improvement of the IT-security certification of a component which is as important for IT-security as random number generators is a potentially important new practical application of quantum information technology.

The new method is systematically compared to the standard "model based" approach recommended by the BSI for the certification of physical random number generators when it would be applied to Pironio et al.'s device. The possible advantages of and remaining problems with Pironio et al.'s methodology are discussed.

Q 33.5 Wed 15:30 SCH A118

Gaussian Errors and Gaussian Quantum Error Correction — •Ricardo Wickert[1,2] and Peter van Loock[1,2] — [1]Optical Quantum Information Theory Group, Max Planck Institute for the Science of Light, Erlangen, Germany — [2]Institute of Theoretical Physics I, Universität Erlangen-Nürnberg, Erlangen, Germany

In the context of optical Quantum Information Processing schemes, Gaussian operations are those most easily implemented in the laboratory. However, it has been recently proved that these operations are of no use in protecting Gaussian states from the ubiquitous class of Gaussian errors [1]. In this talk, we report on ongoing efforts towards understanding and characterizing these errors and their effect on continuous-variable entanglement resources [2]. We investigate the potential implementation of correction strategies within the Gaussian regime against errors of Gaussian character acting on quantum states of non-Gaussian nature [3], and also as a countermeasure to stochastic, non-Gaussian error models [4].

[1] J. Niset et al., Phys. Rev. Lett. 102, 120501 (2009)
[2] R. Wickert et al., Phys. Rev. A 81, 062344 (2010)
[3] R. Wickert and P. van Loock, in preparation
[4] P. van Loock, J. Mod. Optics 57, 19 (2010)

Q 33.6 Wed 15:45 SCH A118

Non-zero key rates for "small" numbers of signals using the min-entropy — •Sylvia Bratzik, Markus Mertz, Hermann Kampermann, and Dagmar Bruss — Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, 40225 Düsseldorf, Germany

We calculate an achievable secret key rate for quantum key distribution with a finite number of signals, by evaluating the min-entropy explicitly [1]. The min-entropy can be expressed in terms of the guessing probability [2], which we calculate for different d-dimensional QKD protocols. We compare these key rates to previous approaches using the von Neumann entropy [3] and find non-zero key rates for only $10^4 - 10^5$ signals. An interesting conclusion can also be drawn from the additivity of the min-entropy and its relation to the guessing probability: for a set of symmetric tensor product states the optimal minimum-error discrimination (MED) measurement is the optimal MED measurement on each subsystem.

[1] S. Bratzik et al., arXiv:1011.1190 [quant-ph].
[2] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Th. **55**, 4337 (2009), arXiv:0807.1338 [quant-ph].
[3] R. Renner, Int. J. Quant. Inf. **6**, 1 (2008); V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008); R. Cai and V. Scarani, New J. Phys. **11**, 045024 (2009).