Q 56: Quantum Information: Quantum Communication II

Time: Friday 10:30–12:15 Location: A 310

Q 56.1 Fr 10:30 A 310

Experimental demonstration of an exploit of detector dead-times in QKD — •Sebastian Nauerth[1], Henning Weier[1], Harald Krauss[1], Martin Fürst[1], Markus Rau[1], and Harald Weinfurter[1,2] — [1]Ludwig-Maximilians-Universität München — [2]Max-Planck-Institut für Quantenoptik Garching

The security of real world quantum key distribution (QKD) systems depends heavily on their thorough implementation. Eavesdroppers can benefit from technical imperfections to gain information on the generated keys. Because some of these attacks are beyond the scope of current security proofs, they possibly will remain unnoticed by the legitimate communicating parties.

One of these imperfections, which is common to almost all QKD systems, is the so called dead time of most single photon detectors (SPD), i. e. the time for which an SPD is rendered inactive after a detection event.

We present our experimental results of a very simple yet highly effective method to exploit this detector imperfection by sending carefully timed blinding pulses into the detectors. Without introducing additional quantum bit errors, thus without being detected by state of the art QKD protocols, an adversary could successfully guess each keybit with a probability greater than 98%. While, in this work, we attack a BB84 system with four detectors, many other schemes are vulnerable to the evesdropping strategy we developed. Yet, we propose an evenly simple and effective countermeasure to inhibit the demonstrated and similar attacks already by the detector electronics.

Q 56.2 Fr 10:45 A 310

Quantum key distribution and 1 Gbit/s data encryption over a single fibre — •Nino Walenta[1], Patrick Eraerds[1], Matthieu Legré[2], Nicolas Gisin[1], and Hugo Zbinden[1] — [1]Group of Applied Physics-Optique, University of Geneva, Rue de l'École-de-Médecine 20, 1205 Geneva, Switzerland — [2]idQuantique SA, Chemin de la Marbrerie 3, 1227, Geneva, Switzerland

Quantum key distribution (QKD) allows highly secure communication based on the laws of quantum mechanics. Until recently, one of the specifics of QKD systems was the need for a dedicated dark optical fibre, exclusively reserved for the quantum channel. Classical signals, assigned to perform key distillation and encrypted communication between the end users, were sent through separate fibres to not compromise the weak quantum signal.

With the aim for scalable and cost effective deployment we demonstrate QKD in the presence of 4 classical channels in a C-band dense wavelength division multiplexing (DWDM) configuration. The classical channels are used for key distillation and 1 Gbps encrypted communication, rendering the entire system independent from any other communication link than a single dedicated fibre. The separation between quantum channel and nearest classical channel is only 200 GHz, while the classical channels are all separated by 100 GHz. We successfully distil secret keys over fibre spans of up to 50 km. In this context we also discuss DWDM configurations with a quantum channel at 1310 nm.

Q 56.3 Fr 11:00 A 310

Quantum Key Distribution on Hannover Campus: Experiment — •Vitus Händchen, Tobias Eberle, and Roman Schnabel — Institut für Gravitationsphysik, Leibniz Universität Hannover und Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut), Callinstrasse 38, D-30167 Hannover

We currently prepare the experimental implementation of quantum key distribution on the campus of the Leibniz Universität Hannover. In this contribution we report on the entanglement (two-mode squeezing) based setup with continuous-wave light fields at a wavelength of 1550 nm, which provides a low absorption in optical fibers. The communication link will be established between the Albert Einstein Institute and the Institute of Quantum Optics through an existing telecom fiber of approximately 1 km length. The readout of the continuous variables at the two locations will be realized by a homodyne detection scheme.

Q 56.4 Fr 11:15 A 310

Quantum key distribution on Hannover Campus: Theory — •Jörg Duhme, Torsten Franz, and Reinhard Werner — Institut für theoretische Physik, Leibniz Universität Hannover

We report on an upcoming implementation of quantum key distribution on LUH campus, see talk by V. Händchen et al. The theoretical model for the experiment includes different noise sources, e.g. damping and phase noise. We discuss the security and expected secure bit rates and comment on the problem of extending security proofs from collective to coherent attacks for continuous variable key distribution.

Q 56.5 Fr 11:30 A 310

Implementation of an attack scheme on a practical QKD system — Qin Liu[1], Ilja Gerhardt[2], Antia Lamas-Linares[2], Vadim Makarov[1], and •Christian Kurtsiefer[2] — [1]NTNU Trondheim — [2]Centre for Quantum Technologies/Physics Department, Nat. Univ. Singapore

We report on an experimental implementation of an attack of a practical quantum key distribution system [1], based on a vulnerability of single photon detectors [2]. An intercept/resend-like attack has been carried out which revealed 100% of the raw key generated between the legitimate communication partners. No increase of the error ratio was observed, which is usually considered a reliable witness for any eavesdropping attempt. We also present an experiment which shows that this attack is not revealed by key distribution protocols probing for eavesdroppers by testing a Bell inequality [3], and discuss implications for practical quantum key distribution.

[1] I. Marcikic, A. Lamas-Linares, C. Kurtsiefer, Appl. Phys. Lett. **89**, 101122 (2006)
[2] V. Makarov, New J. Phys. **11**, 065003 (2009)
[3] A. Ling et al., Phys. Rev. A **78**, 020301(R), (2008)

Q 56.6 Fr 11:45 A 310

Quantum key distribution with finite resources: Smooth Min entropy vs. Smooth Rényi entropy — •Markus Mertz, Silvestre Abruzzo, Sylvia Bratzik, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Düsseldorf, Germany

We consider different entropy measures that play an important role in the analysis of the security of QKD with finite resources. The smooth min entropy leads to an optimal bound for the length of a secure key. Another bound on the secure key length was derived by using Rényi entropies. Unfortunately, it is very hard or even impossible to calculate these entropies for realistic QKD scenarios. To estimate the security rate it becomes important to find computable bounds on these entropies. Here, we compare a lower bound for the smooth min entropy with a bound using Rényi entropies. We compare these entropies for the six-state protocol with symmetric attacks.

Q 56.7 Fr 12:00 A 310

Extremal quantum correlations and cryptographic security — •Torsten Franz, Fabian Furrer, David Gross, Jukka Kiukas, Volkher Scholz, and Reinhard Werner — Institut für Theoretische Physik, Leibniz Universität Hannover

Results of quantum experiments are given by correlation tables, i.e. expectation values of joint measurements performed at different locations. We are interested in situations when these correlations are provably secure, i.e. when the measured results can be shown to be independent of any eavesdropper. We show that any extremal quantum correlation table is secure, and provide algebraic criteria for this.