FM 31: Secure Communication & Computation II

Time: Tuesday 14:00–15:45 Location: 1009

Invited Talk FM 31.1 Tue 14:00 1009

Certifying randomness from quantum black-box devices — •Nicolas Brunner — Department of Applied Physics, University of Geneva, Switzerland

Besides its fundamental interest, randomness represents a key resource for many applications. Since quantum processes can be fundamentally random, they are ideally suited for the task of producing randomness. A strong research interest has thus been devoted to quantum randomness generation (QRNG), leading to first commercial products, but also to a deeper understanding of the concept of randomness in quantum theory. Current research explores the "device-independent" approach to QRNG, where quantum devices are viewed as black boxes. This represents a novel generation of QRNG protocols, achieving the highest level of security. Entropy can be estimated in real-time, based on minimal assumptions about the setup, allowing for the continuous generation of certified random numbers. Moreover, such schemes can now be implemented using only standard optical components and achieve rates comparable to commercial QRNG devices.

FM 31.2 Tue 14:30 1009

Exploring the potential of device-independent quantum cryptography — •Gláucia Murta — Heinrich-Heine-Universität Düsseldorf, Düsseldorf, Germany

Current secure communication is based on cryptographic methods whose security relies on computational assumptions. While this approach works well at the moment, if more powerful computers become available in the future, the content of encrypted messages exchanged today could be revealed (what is called retroactive attacks). Quantum key distribution (QKD) offers a solution to this problem because security is established directly from fundamental laws of physics. However, while unbreakable in principle, the security of QKD protocols relies on a very precise characterization of their physical implementation, which can be very hard to obtain in practice. In fact, this has led to hacking of several quantum cryptosystems. Surprisingly, quantum mechanics also offers a solution to this problem. In the so-called device-independent (DI) setting, security can be guaranteed even if the users are completely ignorant about the internal working of their devices. In this setting, security relies on the violation of a Bell inequality. So far, most of the proposed protocols are based on the CHSH inequality. Very little is known about the use of general Bell inequalities. A big challenge is that many theoretical tools used to deal with the CHSH inequality do not apply to Bell inequalities with more inputs and outputs. In order to get an insight on the potential of general Bell inequalities, we analyze the performance of different Bell inequalities for DIQKD under the assumption that the underlying system has a fixed dimension d.

FM 31.3 Tue 14:45 1009

Magneto-optical properties of InAs/InP quantum dots emitting at the C-band — •Marek Burakowski[1], Wojciech Rudno-Rudziński[1], Anna Musiał[1], Grzegorz Sek[1], Andrei Kors[2], Johann Peter Reithmaier[2], and Mohamed Benyoucef[2] — [1]Wrocław University of Science and Technology, Wrocław, Poland — [2]University of Kassel, Kassel, Germany

Hereby we experimentally determine magneto-optical properties of molecular beam epitaxy grown, symmetric and low-density InAs/InP quantum dots (QDs) emitting at the telecom C-band. Polarization-resolved microphotoluminescence, performed in magnetic field up to 5 T in Faraday and Voigt configuration, indicates exciton fine structure splitting below 20 μeV. The exciton g factor and the diamagnetic coefficient are determined in Faraday configuration to be in the range of $0.7-1.5$ and $9-12$ $\frac{\mu eV}{T^2}$, accordingly, and consequently extension of the exciton wavefunction is in the range of $14-18$ nm, confirming the strong confinement regime. Our results are important for modeling of the excitonic structure of the investigated QDs and indicate they are suitable for quantum photonics applications at the telecom C-band.

Supported by the "Quantum dot-based indistinguishable and entangled photon sources at telecom wavelengths" project, carried out within the HOMING programme of the Foundation for Polish Science co-financed by the European Union under the European Regional Development Fund. This work was also financially supported by the German Federal Ministry of Education and Research (BMBF) within projects Q.com-H and Q.Link.X.

FM 31.4 Tue 15:00 1009

Microphotoluminescence of symmetric InP based single quantum dots emitting in the telecom C-band — •M. Mikulicz[1], P. Wyborski[1], A. Musiał[1], G. Sek[1], A. Kors[2], J. P. Reithmaier[2], and M. Benyoucef[2] — [1]Wrocław University of Science and Technology, Poland — [2]University of Kassel, Germany

Single-photon sources are indispensable for implementation of quantum communication and cryptography schemes. Hereby we present microphotoluminescence (μPL) results of new generation of MBE-grown low-density symmetric InAs/InP quantum dots (QDs) on distributed Bragg reflector emitting in the 3rd telecom window suitable for non-classical light generation. The main focus is to determine the fundamental physical properties of these application relevant structures and to identify excitonic complexes, in particular, biexciton-exciton (XX-X) cascade. Nine QDs were investigated in detail by means of excitation power-dependent and polarization-resolved μPL. They all exhibit low fine structure splitting (below setup spectral resolution of 20 μeV) proving their symmetry, XX binding energy in the range of 1 meV and XX to X lifetime ratio of 2 suggesting strong spatial confinement and slow spin-flip. Supported by the "Quantum dot-based indistinguishable and entangled photon sources at telecom wavelengths" project, carried out within the HOMING programme of the Foundation for Polish Science co-financed by the European Union under the European Regional Development Fund. This work was also financially supported by the German Federal Ministry of Education and Research (BMBF) within projects Q.com-H and Q.Link.X.

FM 31.5 Tue 15:15 1009

Performance Optimization and Security Monitoring for Single-Photon QKD — •Timm Kupko, Lucas Rickert, Martin v. Helversen, Stephan Reitzenstein, and Tobias Heindel — Institut für Festkörperphysik, Technische Universität Berlin, 10623 Berlin, Germany

Solid-state single-photon sources (SPSs) have the potential to boost the performance of quantum-key-distribution (QKD) systems [1,2]. To fully exploit realistic sub-poissonian light sources for applications in quantum communication, however, a detailed analysis and optimization of the receiver side is necessary.

Here, we analyze the effect of temporal filtering on the performance of QKD systems implemented with realistic quantum-light sources. For this purpose, we developed a basic QKD testbed comprising a deterministically fabricated QD-based SPS and a receiver module designed for four-state polarization coding. We analyze the sifted key fraction, the quantum bit error ratio, and $g^{(2)}(0)$ expected in full implementations of the BB84 protocol under variation of the acceptance time-window. This routine enables us to choose optimal filter settings depending on the losses of the quantum channel. Furthermore, we demonstrate real-time security monitoring by evaluating $g^{(2)}(0)$ inside the quantum channel during key distillation. The presented approach can be adapted and extended for most other applications in quantum communication employing realistic quantum light sources.

[1] E. Waks et al., Phys. Rev. A **66**, 042315 (2002)
[2] T. Heindel et al., New J. Phys. 14, 083001 (2012)

FM 31.6 Tue 15:30 1009

Simulation of generation and transmission of photons from SPDC for quantum key distribution with phase-time coding — •Julian Nauth, Erik Fitzke, Alexander Sauer, Gernot Alber, and Thomas Walther — TU Darmstadt, Institute of Applied Physics, 64289 Darmstadt

We are working on a QKD system with phase-time coding. A source generates entangled photons which are measured by the parties to generate a secure key. In theory, the influence of a potential hacker is detected by determining the quantum bit error rate. In practice, however, these errors may also be caused by the effects of real-world component properties and environmental influences. Therefore, we developed a simulation to estimate these influences.

The simulation is a quantum mechanical description of the generation and transmission of photons modeling the states of the system and the processes that change these states. Modeling is based on a multi-mode Gaussian state description of the states and the SPDC is calculated by Schmidt decomposition. The description in frequency

space allows to model effects by the spectral distribution of the photons and chromatic dispersion.

Finally, the simulation predicts how the results of the detectors from the parties correlate at different times. On this basis, the assessment of the security of the key can be improved. We present the methodology and structure of the software and compare the calculations to experimental results.