QI 21: Quantum Communication II (joint session QI/Q)

Time: Wednesday 14:30–16:30 Location: B305

Invited Talk QI 21.1 Wed 14:30 B305

Qube and Qube-II – Towards Quantum Key Distribution with Small Satellites — •Lukas Knips for the Qube/Qube-II-Collaboration — Ludwig Maximilian University (LMU), Schellingstr. 4, D-80799 Munich, Germany — Max Planck Institute of Quantum Optics (MPQ), Hans-Kopfermann-Str. 1, D-85748 Garching, Germany — Munich Center for Quantum Science and Technology (MCQST), Schellingstr. 4, D-80799 Munich, Germany

Quantum Key Distribution (QKD) is a provably secure method for distributing secret keys between two trusted parties over a quantum channel for symmetric cryptography. As demonstrated by the Chinese satellite MICIUS, exchange of a secure key between a satellite and an optical ground station is possible, thereby indeed enabling QKD on a global scale. While this large satellite demonstrated its feasibility, the QUBE missions are focussing on a more economic solution for global key exchange.

In this talk, I will start with an overview of the first QUBE satellite, a so-called CubeSat with a size of only $30 \times 10 \times 10\,\mathrm{cm}^3$ and consequently with severe limitations on available power and space. The satellite includes two different quantum state sources and a quantum random number generator and is now ready for launch. QUBE will test performance and space readiness of those components. QUBE-II, a second satellite, is currently being designed and will be able to exchange a key mainly thanks to a much larger optical telescope with an optical aperture of about 80 mm and to a full QKD post-processing over an optical data communication channel.

QI 21.2 Wed 15:00 B305

Security of Time-Frequency Quantum Key Distribution — •Federico Grasselli, Nikolai Wyderka, Hermann Kampermann, and Dagmar Bruss — Heinrich-Heine-Universität Düsseldorf

One of the current drawbacks of Quantum key distribution (QKD) are the relatively low generation rates of secret keys, hindered by effects such as noise in the quantum channel and detector saturation. Such issues can be alleviated by increasing the dimension of the encoding space with time-frequency QKD, where log2(d) bits of information are encoded in 'd' time bins of a single photon, thereby increasing the efficiency of the communication.

We focus on a specific experimental implementation of time-frequency QKD that can be easily scaled to higher dimensions. For this setup, we discuss a method to prove its security by closing a critical loophole that has been often overlooked in QKD implementations based on the photons' temporal degree of freedom. Moreover, we provide preliminary experimental data demonstrating that our security method can be applied to practical time-frequency QKD setups.

QI 21.3 Wed 15:15 B305

Multipartite measurement device-independent quantum key distribution with quantum memories — •Julia Alina Kunzelmann, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf

Quantum repeaters build a useful tool to increase the communication distance in quantum networks. To achieve higher repeater rates, multiplexing between quantum memories can be used. We generalize the multiplexing scheme for quantum repeaters to N parties where the station performs GHZ measurements. This setup is used for measurement device-independent conference key agreement. In this work, we present a protocol that allows the distribution of a secret key in a multipartite star network via one central repeater station. We analyze the secret key rate of the protocol depending on various protocol parameters.

QI 21.4 Wed 15:30 B305

Easy-to-compute local Clifford invariants for graph states — •Frederik Hahn[1] and Adam Burchardt[2,3,4] — [1]Technische Universität Berlin, Berlin, Deutschland — [2]Universität Amsterdam, Amsterdam, Niederlande — [3]QuSoft, Amsterdam, Niederlande — [4]CWI, Amsterdam, Niederlande

In this work, we study easy-to-compute LC-invariants of graph states. Although previous studies have already led to finite sets of invariants that fully characterize the LC-equivalence classes of graph states, these invariants are computationally inefficient. Their computation requires knowledge of the given state's full stabilizer set, which is exponential in the number of its qubits n.

In this paper, without the need to calculate this entire stabilizer set, we instead present an easy-to-calculate LC-invariant of order O(n^3). It is closely related to the so-called foliage of a graph and has a simple graphical interpretation in terms of leaves, axils, and twins: For any graph, we define a partition of the set of its vertices based on a simple equivalence relation and call it the foliage partition of this graph. We further show that foliage partitions remain invariant under any local complementation of the corresponding graph. Foliage partitions then represent simple LC-invariants for graph states, since there is a one-to-one correspondence between LC-operations on a graph state and local complementations of its graph. Finally, we generalize foliage partitions from qubits to qudits and prove their invariance under the generalized local complementation operations.

QI 21.5 Wed 15:45 B305

Towards consumer-level quantum-secure cryptography - Entanglement based short-range Quantum Key Distribution — •Henning Mollenhauer[1], Daniel Tippel[1], Pius Gerisch[1], Donika Imeri[1,2], and Ralf Riedinger[1,2] — [1]Zentrum für Optische Quantentechnologien, Universität Hamburg, 22761 Hamburg — [2]The Hamburg Centre for Ultrafast Imaging, 22761 Hamburg

Many schemes for Quantum Key Distribution (QKD) have been proposed and realized over the years. A common challenge that arises in experimental implementations is the exponential loss of photons in quantum channels over long distances. Solutions to this challenge like purification protocols with quantum repeaters have not to date been efficiently implemented. A different approach to QKD is the key distribution over a short distance- and therefore low-loss- quantum channel. QKD over short distances can be used to exchange an information-theoretically secure root-of-trust that is safely stored on two end modules. Based on the root-of-trust, keys for encryption are generated in re-keying schemes on each end module. With this approach, it is possible to spatially separate the end modules and communicate classically over already existing communication infrastructure. Since no quantum channel is involved in the actual process of communication, encrypted messages can be sent between end modules over arbitrary distances. We here present an experimental setup that aims to realize short-distance QKD with end modules that in the future could be made compact enough to be implemented on small silicone-based chips.

QI 21.6 Wed 16:00 B305

A theoretical and experimental analysis of the single-photon advantage in quantum coin flipping — •Fenja Drauschke[1,2], Daniel A. Vajner[1], Tobias Heindel[1], and Anna Pappa[2] — [1]Institut für Festkörperphysik, TU Berlin — [2]Institut für Softwaretechnik und Theoretische Informatik, TU Berlin

Quantum coin flipping is a prominent cryptographic primitive within the framework of non-collaborative models, where two or more distrustful parties want to perform a fair coin flip. The parties are separated by a distance and wish to agree on a random bit. Quantum coin flipping has raised much interest recently, as it has various applications and holds enormous potential for improving the security of secure communications. At the same time, the use of single-photon sources for quantum communication setups is also attracting a lot of attention as it promises further security advantages compared to the usage of weak coherent laser pulses. In this work, we investigate the advantage of using single-photon sources compared to weak coherent pulses for different quantum communication setups of coin flipping in a theoretical, as well as experimental approach.

QI 21.7 Wed 16:15 B305

Optimization and readout-noise analysis of a hot vapor EIT memory on the Cs D1 line — •Luisa Esguerra[1,2], Leon Messner[1,3], Elizabeth Robertson[1,2], Norman Vincenz Ewald[1], Mustafa Gündoğan[1,3], and Janik Wolters[1,2] — [1]Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR), Institut für Optische Sensorsysteme, Rutherfordstr. 2, 12489 Berlin, Germany. — [2]TU Berlin, Institut für Optik und Atomare Physik, Hardenbergstr. 36, 10623 Berlin, Germany. — [3]Institut für Physik, Humboldt-Universität zu Berlin, Newtonstr. 15, 12489 Berlin, Germany.

Efficient, noise-free quantum memories are indispensable components for the realization of quantum repeaters, which will be crucial for long distance quantum communication [1, 2]. We have realized a technologically simple, in principle satellite-suited quantum memory in Cesium vapor, based on electromagnetically induced transparency (EIT) on the ground states of the Cs D1 line [3]. We focus on the simultaneous optimization of end-to-end efficiency and signal-to-noise level in the memory, and have achieved light storage at the single-photon level with end-to-end efficiencies up to 13(2)%. Simultaneously we achieve a minimal noise level corresponding to $\bar{\mu}_1 = 0.07(2)$ signal photons, for which we present strategies for further minimization. Furthermore, improvements for the next implementation of the experiment are introduced.

[1] M. Gündoğan et al., npj Quantum Information 7, 128 (2021)
[2] J. Wallnöfer et al., Commun Phys 5, 169 (2022)
[3] L. Esguerra, et al., arXiv:2203.06151 (2022)