QI 3: Quantum Communication

Time: Monday 9:30–13:15 Location: HFT-TA 441

QI 3.1 Mon 9:30 HFT-TA 441

Quantum Frequency Conversion for Entanglement Distribution — •Tommy Block[1,2], Yuya Maeda[3], Pooja Malik[1,2], Yiru Zhou[1,2], Florian Fertig[1,2], Chengfeng Xu[1,2], Tim van Leent[1,2], and Harald Weinfurter[1,2,4] — [1]Ludwig-Maximilians-Universität, Fakultät für Physik, Schellingstr. 4, 80799 München — [2]Munich Center for Quantum Science and Technology (MCQST), Schellingstr. 4, 80799 München — [3]Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan — [4]Max-Planck-Institut für Quantenoptik, 85748 Garching

Entanglement distribution between distant quantum nodes is one of the most crucial tasks for a future quantum network. In our experiment we utilize optical fibers as quantum channels to distribute the entanglement between two Rubidium-87 atom-based quantum memories via entanglement swapping. Since the emission wavelength of our Rb atoms is 780 nm, the photons would suffer high attenuation losses in optical fibers, limiting the maximum achievable distance for entanglement distribution. Here we describe how to convert the 780 nm photons to 1514nm (telecom S-band) with a second generation quantum frequency converter (QFC) with higher stability and signal to noise ratio, while preserving the quantum information encoded in the polarization state of photon. This QFC device will enable distribution of entanglement over suburban distances.

QI 3.2 Mon 9:45 HFT-TA 441

A highly compact and robust QKD sender unit for satellite applications — •Moritz Birkhold[1,2], Michael Auer[1,2,3], Adomas Baliuka[1,2], Peter Freiwang[1,2], Lukas Knips[1,2,4], and Harald Weinfurter[1,2,4,5] — [1]Ludwig Maximilian University, Munich, Germany — [2]Munich Center for Quantum Science and Technology, Munich, Germany — [3]Universität der Bundeswehr, Neubiberg, Germany — [4]Max Planck Institute of Quantum Optics, Garching, Germany — [5]University of Gdańsk, Poland

Quantum key distribution (QKD) offers fundamental advantages over classical distribution of secret keys. If done correctly, any eavesdropping attack will be detected, allowing to exchange a perfectly private key between two parties. The BB84 protocol with decoy state analysis enabeling use of highly attenuated laser pulses as a photon source is very promising for bringing QKD out of laboratories into the real world. Furthermore, provided the device is robust and efficient with space and energy consumption, deploying QKD sender units on satellites and transmitting the keys in free space can accelerate the creation of a global QKD network.

In this talk, we show our advances in creating such a compact and low-power sender unit using vertical cavity surface emitting lasers, micro optics and waveguide chips. This unit is tested for possible side channels and, together with an equally compact and low-power processing and control board handling the full QKD protocol including error correction, privacy amplification and authentication, is about to fly on the QUBE-II satellite mission.

QI 3.3 Mon 10:00 HFT-TA 441

Towards a Compact Quantum Key Distribution Receiver — •Michael Steinberger[1,2], Moritz Birkhold[1,2], Michael Auer[1,2,3], Adomas Baliuka[1,2], Lukas Knips[1,2,4], and Harald Weinfurter[1,2,4,5] — [1]Ludwig Maximilian University (LMU), Munich, Germany — [2]Munich Center for Quantum Science and Technology (MCQST), Munich, Germany — [3]Universität der Bundeswehr, Neubiberg, Germany — [4]Max Planck Institute of Quantum Optics (MPQ), Garching, Germany — [5]Institute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics, and Informatics, University of Gdańsk, Gdańsk, Poland

Quantum Key Distribution (QKD) provides a method to exchange a key between two parties that is secure of any eavesdropping attempts. Since it relies on single to few photons as information carriers, technical realizations often include complex and big detection systems. This talk focusses on the development of a compact receiver for implementing polarization-based decoy-state BB84 QKD. We choose CMOS-based single photon detectors (SPADs) to enable a high degree of integration, due to their small size and on-chip evaluation of the detections. The Technical University of Vienna provides us with diverse SPADs, that enable various very compact optical systems with improved detection efficiencies. These concepts will enable a new range of versatile and mobile QKD receiver devices.

QI 3.4 Mon 10:15 HFT-TA 441

QKD Post-Processing in Space — •Adomas Baliuka[1,2], Michael Auer[1,2,3], Moritz Birkhold[1,2], Lukas Knips[1,2,4], and Harald Weinfurter[1,2,4,5] — [1]Ludwig-Maximilian-University, Munich, Germany — [2]Munich Center for Quantum Science and Technology, Munich, Germany — [3]Universität der Bundeswehr München, Neubiberg, Germany — [4]Max Planck Institute of Quantum Optics, Garching, Germany — [5]Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-308 Gdańsk, Poland

Classical post-processing is an essential part of all quantum key distribution (QKD) protocols. For satellite-based QKD, additional challenges arise from the harsh conditions in earth's orbit, where classical communication throughput is scarce and available computational capabilities are limited by a tight power budget and the need for radiation-resistant components. At the same time, this high-loss QKD scenario leaves no room for compromises concerning, e.g., the efficiency of error correction, or the use of viable satellite overpasses for demanding computations and classical communication.

To meet these challenges, we minimize the amount of data transmitted for post-processing by dedicated compression methods. We further perform error correction using irregular quasi-cyclic (QC) low density parity check (LDPC) codes and state-of-the-art rate adaption techniques. Despite our large block sizes, this allows our QKD post-processing to stay within tight memory and time constraints without compromising on efficiency, and offloads demanding computations to the receiver on ground.

QI 3.5 Mon 10:30 HFT-TA 441

Limits on the repeater rate in multipartite quantum routers with quantum memories — •Julia Alina Kunzelmann, Nikolai Wyderka, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf

Quantum routers play an important role in quantum communication networks, enabling the transmission of quantum information over longer distances. To increase the repeater rate in multipartite networks, multiplexing between quantum memories can be used. In our work, we investigate the limitations of repeater rates in quantum networks with N parties, each equipped with m memories. Based on our generalized multiplexing scheme for N parties we analyze the relation between the maximally achievable repeater rate and the number of parties and memories included in the network. We present both, numerical and analytical results.

QI 3.6 Mon 10:45 HFT-TA 441

Quantum conference key agreement in networks with bipartite entanglement sources — •Anton Trushechkin, Giacomo Carrara, Justus Neumann, Hermann Kampermann, and Dagmar Bruss — Heinrich Heine University Düsseldorf, Faculty of Mathematics and Natural Sciences, Institute for Theoretical Physics III, Universitätsstr. 1, Düsseldorf 40225

We analyze quantum conference key agreement (QCKA) in networks with arbitrary topology and focus on decentralized networks with bipartite entanglement sources (rather than sources of multipartite entangled states like GHZ-states or W-states). Various strategies of QCKA are discussed. In particular, we compare the performance of genuine QCKA with parallel bipartite quantum key distribution (QKD) and derive the secret key rates based on the properties of the network. Also we show that QCKA on multipartite 2-entangled states cannot exceed the rates achievable by parallel bipartite QKD protocols.

15 min. break

QI 3.7 Mon 11:15 HFT-TA 441

Experimental anonymous quantum conferencing — Jonathan W. Webb[1], Joseph Ho[1], •Federico Grasselli[2,3], Gláucia Murta[2], Alexander Pickston[1], Andres Ulibarrena[1], and Alessandro Fedrizzi[1] — [1]Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh, United Kingdom — [2]HHU Düsseldorf — [3]Institut de Physique Théorique, CEA Paris Saclay

Anonymous quantum conference key agreement (AQCKA) allows a group of users within a network to establish a shared cryptographic key without revealing their participation. Although this can be achieved using bipartite primitives alone, it is costly in the number of network rounds required. By allowing the use of multipartite entanglement, there is a substantial efficiency improvement. We experimentally implement the AQCKA task in a six-user quantum network using Greenberger-Horne-Zeilinger (GHZ)-state entanglement and obtain a significant resource cost reduction in line with theory when compared to a bipartite-only approach. We also demonstrate that the protocol retains an advantage in a four-user scenario with finite-key effects taken into account.

QI 3.8 Mon 11:30 HFT-TA 441

Towards High Throughput Quantum Key Distribution with Quantum Dots — •Koray Kaymazlar, Martin von Helversen, Timm Gao, Lucas Rickert, Daniel Vajner, and Tobias Heindel — Institute of Solid State Physics, Technical University of Berlin

Quantum key distribution (QKD) systems using polarization encoding require fast modulation of the polarization states of single-photon pulses. Here, we present a prototype for a QKD system based on the BB84 protocol which aims for secure key generation at high rates. The setup consists of electronics based on a field programmable gate array (FPGA) and a digital to analog converter (DAC) driving a fiber-based electro optic modulator for quantum light from a cavity-enhanced semiconductor quantum dot emitting in the spectral range around 900 nm or 1550 nm. We characterize and optimize the performance of this setup in terms of secure key rate.

We also considered practical issues which are synchronization of sender (Alice) and receiver (Bob) side of the system, alongside random bit handling in the sender*s end. Various solutions were implemented to address these practical challenges, followed by an evaluation to discern their impact on the system*s functionality.

QI 3.9 Mon 11:45 HFT-TA 441

Microwave quantum tokens with time multiplexing — •Florian Fesquet[1,2], Valentin Weidemann[1,2], Fabian Kronowetter[1,2,3], Michael Renger[1,2], Wun K. Yam[1,2], Simon Gandorfer[1,2], Achim Marx[1], Rudolf Gross[1,2,4], and Kirill G. Fedorov[1,2,4] — [1]Walther-Meißner-Institut, Bayerische Akademie der Wissenschaften, 85748 Garching, Germany — [2]School of Natural Sciences, Technische Universität München, 85748 Garching, Germany — [3]Rohde & Schwarz GmbH & Co. KG, 81671 Munich, Germany — [4]Munich Center for Quantum Science and Technology, 80799 Munich, Germany

Quantum key distribution (QKD) holds the promise of delivering unconditionally secure distribution of classical keys between remote parties. So far, its implementation in the microwave regime, frequency-compatible with superconducting quantum circuits, has been missing. Here, we present a realization of a continuous-variable (CV) QKD protocol using propagating displaced squeezed microwave states and demonstrate an experimental unconditional security. We show that secret key rates can be increased by adding finite trusted noise to the preparation side and by exploiting the time multiplexing approach. Our results indicate feasibility of secure microwave quantum communication under cryogenic (up to 1200 meters) and open-air (up to 80 meters) conditions. Finally, we discuss coupling of the squeezed microwave states to spin ensembles, enabling long-term quantum memories for resulting quantum tokens.

QI 3.10 Mon 12:00 HFT-TA 441

Microwave quantum teleportation in a thermal environment — •Wun Kwan Yam[1,2], Simon Gandorfer[1,2], Florian Fesquet[1,2], Kedar E. Honasoge[1,2], Maria-Teresa Handschuh[1,2], Fabian Kronowetter[1,2,3], Achim Marx[1], Rudolf Gross[1,2,4], and Kirill G. Fedorov[1,2,4] — [1]Walther-Meißner-Institut, Bayerische Akademie der Wissenschaften, 85748 Garching, Germany — [2]School of Natural Sciences, Technische Universität München, 85748 Garching, Germany — [3]Rohde & Schwarz GmbH Co. KG, 81671 Munich, Germany — [4]Munich Center for Quantum Science and Technology, 80799 Munich, Germany

Microwave quantum teleportation enables efficient and unconditionally secure exchange of quantum states. It also paves the way towards distributed quantum computing based on superconducting qubits with natural frequency in the microwave regime. We perform quantum teleportation of microwave coherent states between spatially separated cryostats by exploiting two-mode squeezed states propagating over a cryogenic link between those fridges. We study the influence of the cryolink's temperature on the fidelity of teleported states and experimentally demonstrate robustness of our teleportation protocol. Finally, we analyze ultimate limits of this approach and discuss it in the context of microwave quantum local area networks.

QI 3.11 Mon 12:15 HFT-TA 441

Where are the photons in a transmission-line pulse? — •Evangelos Varvelis[1,2], Debjyoti Biswas[3], and David P. DiVincenzo[1,2,4] — [1]Institute for Quantum Information, RWTH Aachen University, 52056 Aachen, Germany — [2]Jülich-Aachen Research Alliance (JARA), Fundamentals of Future Information Technologies, 52425 Jülich, Germany — [3]Department of Physics, IIT Madras, Chennai 600036, India — [4]Peter Grünberg Institute, Theoretical Nanoelectronics, Forschungszentrum Jülich, 52425 Jülich, Germany

It is now common to say that photons can be transmitted along optical fibers or transmission lines. But in many cases the transmission pulse is defined by a time-profile of the field strength, i.e., the electric field or voltage V(t), at the transmission point. How does this turn into a precise description of the arrival profile of the photons in the pulse? We show that there is a highly nontrivial mathematical relation between the function V(t) and the arrival function of the photons. Paradoxically, even if V(t) is strictly limited in time, the photon arrival profile cannot be. This, and the counterintuitive relation between V(t) and the expected number of arriving photons, has consequences for the security of quantum cryptography.

QI 3.12 Mon 12:30 HFT-TA 441

Ultrafast quantum state transfer and the speed limit of quantum communication — •Przemyslaw Zielinski[1,2,3], Iñigo Arrazola[4], and Peter Rabl[1,2,3] — [1]Technical University of Munich, TUM School of Natural Sciences, Physics Department, 85748 Garching, Germany — [2]Walther-Meißner-Institut, Bayerische Akademie der Wissenschaften, 85748 Garching, Germany — [3]Munich Center for Quantum Science and Technology (MCQST), 80799 Munich, Germany — [4]Instituto de Física Teórica, UAM-CSIC, Universidad Autónoma de Madrid, Cantoblanco, 28049 Madrid, Spain

We investigate the controlled transfer of quantum states between two nodes of a quantum network with tunable couplings to a common waveguide. Specifically, we are interested in the performance of the state transfer protocol when the coupling is pushed into the ultrastrong coupling regime and the usual rotating wave approximation does no longer apply. In this regime we use optimal control theory to evaluate the minimal time for which a nearly perfect state transfer fidelity can still be achieved. We discuss the implications of these general findings for quantum communication strategies in superconducting quantum networks, where tunable ultrastrong couplers can be realized with flux-biased Josephson circuits.

QI 3.13 Mon 12:45 HFT-TA 441

Bounds on Conference Key Agreement in LOSR-Networks — •Justus Neumann, Giacomo Carrara, Anton Trushechkin, Hermann Kampermann, and Dagmar Bruss — Heinrich Heine Universität, Düsseldorf, Deutschland

Conference key agreement is the extension of quantum key distribution from two to arbitrary many participants. Typically, the parties need to prepare multipartite entangled states to establish a secret key. However, generating highly multipartite entangled quantum states can be challenging in practice. We consider networks with bipartite sources, where each party is allowed to perform local operations. In addition, all parties share a classical random variable indicating the operation the parties have to perform. In this scenario the parties are not allowed to communicate classically during the prepare and measure phase. Although this limits the parties' abilities to generate a high key rate, it has advantages for practical implementations because no memories are needed. We discuss how such networks can be used to establish a secret bit string shared by all parties. Through inflation techniques, we derive upper bounds on the asymptotic multipartite key rate and we show that in a BB84- multipartite protocol the states that can be prepared in these networks do not outperform biseparable states.

QI 3.14 Mon 13:00 HFT-TA 441

Entanglement-based free-space links for quantum networks — •Antonio Gallego Barrio[1,2], Jan Tepper[1], Michael Auer[2,3,4], Alberto Comin[1], and Harald Weinfurter[2,4,5] — [1]Airbus Central R&T, Munich, Germany — [2]Ludwig-Maximilians-Universität, Mu-

nich, Germany — [3]Universität de Bundeswehr München, Neubiberg, Germany — [4]Munich Center for Quantum Science and Technology, Munich, Germany — [5]Max-Planck-Institut für Quantenoptik, Garching, Germany

Quantum key distribution (QKD) protocols can be implemented with different technologies and means. For a future practical quantum network it will be valuable to combine them wisely and exploit the relative strengths of fiber based and free-space links.

Here we present some of the approaches and the main challenges which need to be overcome when implementing the links of a quantum network. The key topics are photon detection, time-correlated single photon counting and verification and use of entanglement.

There will also be a brief review about the limitations of the commercially available technologies and some of the implementation details of the QKD links, which will have a deep impact on the development of near-term QKD networks.