QI 7: Quantum Communication and Networks

Time: Wednesday 15:00–17:45 Location: H8

QI 7.1 Wed 15:00 H8

Quantum networks and symmetries — •Kiara Hansenne[1], Zhen-Peng Xu[1], Tristan Kraft[2], and Otfried Gühne[1] — [1]Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Siegen, Germany — [2]Institute for Theoretical Physics, University of Innsbruck, Innsbruck, Austria

Quantum networks are promising tools for the implementation of long-range quantum communication. The characterization of quantum correlations in networks and their usefulness for information processing is therefore central for the progress of the field, but so far only results for small basic network structures or pure quantum states are known. Here we show that symmetries provide a versatile tool for the analysis of correlations in quantum networks. We provide an analytical approach to characterize correlations in large network structures with arbitrary topologies. As examples, we show that entangled quantum states with a bosonic or fermionic symmetry can not be generated in networks; moreover, cluster and graph states are not accessible. Our methods can be used to design certification methods for the functionality of specific links in a network and have implications for the design of future network structures.

QI 7.2 Wed 15:15 H8

Secure Anonymous Conferencing in Quantum Networks — •Federico Grasselli[1], Gláucia Murta[1], Jarn de Jong[2], Frederik Hahn[3], Dagmar Bruss[1], Hermann Kampermann[1], and Anna Pappa[2,4] — [1]Heinrich-Heine-Universität Düsseldorf — [2]Technische Universität Berlin — [3]Freie Universität Berlin — [4]Fraunhofer Institut for Open Communication Systems

Users of quantum networks can securely exchange classical messages via quantum conference key agreement (CKA), which requires the users' identities to be publicly known. In numerous scenarios, however, communicating users demand anonymity with respect to the other network users, the network manager and even between themselves.

We introduce a security framework for anonymous conference key agreement with different levels of anonymity, generalizing the security of quantum key distribution (QKD). We present efficient and noise-tolerant protocols exploiting multipartite Greenberger-Horne-Zeilinger (GHZ) states and prove their security against general quantum attacks in the finite-key regime. We analyze their performance in noisy and lossy quantum networks and compare with protocols that only use bipartite entanglement to achieve the same functionalities. Our simulations show that GHZ-based protocols can outperform protocols based on bipartite entanglement and that the advantage increases for protocols with stronger anonymity requirements.

Our work advocates the use of multipartite entanglement for cryptographic tasks involving several users and enables the implementation of quantum communication protocols beyond QKD and CKA.

QI 7.3 Wed 15:30 H8

Prepare-and-measure conference key agreement protocol based on single-photon interference — •Giacomo Carrara, Federico Grasselli, Gláucia Murta, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Germany

Quantum Key Distribution (QKD) and its multipartite counterpart, Conference Key Agreement, (CKA) are fundamental cryptographic tasks, where two or more parties try to establish a common, secret key. The so-called Twin-Field Quantum Key Distribution (TF-QKD) setup recently received great attention as it only requires lasers and linear optical devices. TF-QKD has been generalized to many parties, where a CKA protocol based on single-photon interference has been proposed [F. Grasselli *et al*, 2019, New J. Phys., **21** 123002]. This multipartite protocol, however, has a big drawback: it does not have a prepare-and-measure formulation and thus lacks a simple, practical implementation. In this work we propose a CKA protocol that allows for a prepare-and-measure implementation, where the parties are required only to produce weak coherent pulses. We provide for this protocol a security analysis based on the decoy state method and analyze how the protocol performs compared to the well-known repeaterless bound, considering different network architectures.

QI 7.4 Wed 15:45 H8

Experimental anonymous conference key agreement using linear cluster states — •Lukas Rückle, Jakob Budde, and Stefanie Barz — Institute for Functional Matter and Quantum Technologies and IQST, University of Stuttgart, 70569 Stuttgart

Quantum networks allow for secure communication between more than just two parties. One example is the conference key agreement, where multiple parties exchange a secure key. Interestingly, quantum networks can provide another security feature: protecting the identity of the participants. Here, we realize such anonymous quantum conference key agreement in a linear network architecture using photonic cluster states. We show how different parties of the network can exchange a key anonymously by extracting a smaller GHZ state from the cluster state. We further study how noise affects the finite and asymptotic key rate and show that we achieve a positive asymptotic key rate.

QI 7.5 Wed 16:00 H8

Average waiting times for entanglement links in multiplexed quantum networks — •Lisa Weinbrenner, Lina Vandré, and Otfried Gühne — Universität Siegen, Deutschland

In quantum communication protocols using noisy channels, the error probability typically scales exponentially with the length of the channel. To reach long-distance entanglement distribution, one can use quantum repeaters. These schemes involve first a generation of elementary bipartite entanglement links between two nodes and then measurements to combine the elementary links to a long-distance link.

Since the generation of an elementary link is probabilistic and quantum memories have a limited storage time, the generation of a long-distance link is probabilistic, too [1]. One possibility to speed up the generation of a long-distance link is a multiplexed system, in which there is more than one elementary link between two nodes [2]. In this contribution, we will present estimates and bounds on waiting times in such a system. Our results rely on an analytical treatment of the underlying stochastic process, as well as numerical investigations using the matrix product state formalism.

[1] S. Khatri et al., Phys. Rev. Research 1, 023032 (2019)
[2] O. A. Collins et al., Phys. Rev. Lett 98, 060502 (2007)

QI 7.6 Wed 16:15 H8

Fiber communication with collective quantum measurements: a machine learning perspective with applications — •Matteo Rosati[1] and Janis Nötzel[2] — [1]Electrical Engineering and Computer Science, Technische Universität Berlin, 10587 Berlin, Germany — [2]1Emmy-Noether Gruppe Theoretisches Quantensystemdesign Lehrstuhl für Theoretische Informationstechnik Technische Universität München.

The transmission rate of classical bits on optical fiber is ultimately governed by the Holevo capacity. Achieving such rate requires writing information into coherent states of light and then performing a collective quantum measurement on multiple received signals at once, known as quantum joint-detection receiver (QJDR).

We find that the realization of a QJDR would enable two key advantages in current communication networks: (i) an estimated 55% decrease in energy consumption of optical amplifiers; (ii) an unbounded logarithmic growth of the channel capacity with the signal pulse rate, as opposed to the bounded rate attained by conventional detectors.

We then develop a machine learning framework to discover approximate implementations of the QJDR with a state-of-the-art photonic circuit. We compute the theoretical learning complexity of such photonic circuits, showing that it is polynomial in the number of optical modes, and introduce a simple algorithm to optimize them. Finally, we show that our algorithm is able to discover decoder setups that are both realizable at the state of the art and can attain a decoding success rate as high as 93% of the optimal QJDR.

15 min. break

QI 7.7 Wed 16:45 H8

A Graphical Formalism for Entanglement Purification — •Lina Vandré and Otfried Gühne — Universität Siegen, Germany

Hypergraph states form an interesting family of multi-qubit quantum states which are useful for quantum error correction, non-locality and measurement-based quantum computing. They are a generalisation of graph and cluster states. The states can be represented by hypergraphs, where the vertices and hyperedges represent qubits and entangling gates, respectively.

For quantum information processing, one needs high-fidelity entangled states, but in practice most states are noisy. Purification protocols address this problem and provide a method to transform a certain number of copies of a noisy state into single high-fidelity state. There exists a purification protocol for hypergraph states [1]. In my talk, I will first reformulate the purification protocol in a graphical manner, which makes it intuitively understandable. Based on this, I will propose systematic extensions, which naturally arise from the graphical formalism.

[1] T. Carle et al., Phys. Rev. A 87, 012328 (2013))

QI 7.8 Wed 17:00 H8

Quantum memories for space: from ideas to experimental roadmap — •Mustafa Gündoğan, Martin Jutisz, Elisa Da Ros, and Markus Krutzik — Humboldt-Universität zu Berlin, Berlin, Germany

Quantum communication is usually limited to around a few hundred kilometers due to the exponential losses in optical fibers. Quantum repeaters (QR) based on the heralded storage of entangled states have been proposed to overcome this direct transmission limit. However, they are still limited to around a few thousand kms. On the other hand, space-based quantum links where channel loss scales mainly polynomially offer another solution to this problem. In this case, however, the communication distance is limited to the line-of-sight distance of the satellite which is around 2000 km for low earth orbit. In order to reach truly global distances, we have recently proposed an architecture that combines the above two approaches [1]: a quantum repeater operating in space. We show that this scheme provides a three orders of magnitude faster entanglement distribution rate across global distances than ground-based and hybrid space-ground architectures.

In this talk, after summarizing our findings and presenting a comparison of our scheme with already existing architectures I will finish with presenting our experimental work towards building space-compatible quantum memories with warm and cold atomic gases.

[1] M. Gündoğan *et. al.*, npj Quantum Information **7**, 128 (2021)

(This work has been supported by DLR through the funds provided by BMWi: 50WM1958, 50WM2055 and 50RP2090.)

QI 7.9 Wed 17:15 H8

Employing Atomically-thin Single-Photon Sources in Quantum Communication — •Timm Gao[1], Martin v. Helversen[1], Carlos Anton-Solanas[2], Christian Schneider[2], and Tobias Heindel[1] — [1]Institut für Festkörperphysik, Technische Universität Berlin, 10623 Berlin, Germany — [2]Institut für Physik, Carl von Ossietzky Universität Oldenburg, 26111 Oldenburg, Germany

Confined excitons in monolayers of transition metal dichalcogenides (TMDCs) emerged as a novel type of quantum emitter showing appealing prospects for large-scale and low-cost device integration for quantum information technologies. Here, we pioneer the practical suitability of TMDC devices in quantum communication by evaluating the performance of a single-photon source (SPS) based on a strain engineered WSe_2 monolayer for applications in quantum key distribution (QKD) [1]. Employed in a QKD-testbed emulating the BB84 protocol we achieve raw key rates of up to 66.95 kHz and antibunching values down to 0.034 - competitive with QKD experiments using semiconductor quantum dots or color centers in diamond [2]. Furthermore, we exploit routines for the performance optimization developed in our group. Our work thus sets the direction for wider applications of emerging materials in quantum information processing.

[1] T. Gao, M. v. Helversen, C. Anton-Solanas, C. Schneider, and T. Heindel, Atomically-thin Single-photon Sources for Quantum Communication, arXiv:2204.06427 (2022)
[2] D. Vajner et al., Adv. Quantum Technol. 2100116 (2022).

QI 7.10 Wed 17:30 H8

Restoring quantum communication efficiency over high loss optical fibres — •Francesco Anna Mele — Scuola Normale Superiore, Pisa, Italy

In the absence of quantum repeaters, quantum communication proved to be nearly impossible across optical fibres longer than approximately 20 km due to the drop of transmissivity below the critical threshold of 1/2. However, if the signals fed into the fibre are separated by a sufficiently short time interval, memory effects must be taken into account. In this talk we show that by properly accounting for these effects it is possible to devise schemes that enable unassisted quantum communication across arbitrarily long optical fibres at a fixed positive qubit transmission rate. We also demonstrate how to achieve entanglement-assisted communication over arbitrarily long distances at a rate of the same order of the maximum achievable in the unassisted noiseless case.

This talk is based on https://arxiv.org/abs/2204.13128 and https://arxiv.org/abs/2204.13129 .