QI 18: Quantum Communication

Time: Thursday 15:00–18:00 Location: BEY/0245

Invited Talk QI 18.1 Thu 15:00 BEY/0245

Multipartite Quantum states from guided-wave structures — •Virginia D'Auria[1], Adrien Bensemhoun[1], Silvia Cassina[2], Carlos Gonzalez-Arciniegas[3], Mohamed Fauzi Melalkia[1], Giuseppe Patera[4], Jonathan Faugier-Tovar[5], Quentin Wilmar[5], Ségolène Olivier[5], Alessandro Zavatta[6], Anthony Martin[1], Jean Etesse[1], Laurent Labonté[1], and Sébastien Tanzilli[1] — [1]University Côte d'Azur, Institut of Physics of Nice, Nice, FR — [2]University of Insubria, Como, IT — [3]University of Virginia, Charlottesville, VA, US — [4]University of Lille, Lille, FR — [5]CEA-LETI, Grenoble, FR — [6]Istituto Nationale di Ottica, Florence, IT

Our experimental work demonstrates multipartite quantum correlation in bright frequency combs out of a microresonator integrated on silicon nitride operating above its oscillation threshold. Multipartite features, going beyond so far reported two-mode correlation, naturally arise due to a cascade of non-linear optical processes, making a single-color laser pump sufficient to initiate their generation. Our results show the transition from two-mode to multipartite correlation.

QI 18.2 Thu 15:30 BEY/0245

Microwave quantum communication over thermal quantum networks — •Wun Kwan Yam[1,2], Simon Gandorfer[1,2], Maria-Teresa Handschuh[1,2], Achim Marx[1], Rudolf Gross[1,2,3], and Kirill G. Fedorov[1,2,3] — [1]Walther-Meißner-Institut, Bayerische Akademie der Wissenschaften, 85748 Garching, Germany — [2]School of Natural Sciences, Technical University of Munich, 85748 Garching, Germany — [3]Munich Center for Quantum Science and Technology, 80799 Munich, Germany

Quantum communication in the microwave regime is set to play an important role in distributed quantum computing and hybrid quantum networks. In a step towards practical quantum networks, we demonstrate quantum teleportation of microwave coherent states over a thermal quantum network composed of two spatially-separated dilution refrigerators, achieving teleportation fidelities of 72.3 % at channel temperatures of 1 K and 59.9 % at 4 K. Furthermore, we theoretically analyze quantum communication of discrete-variable qubit states using a continuous-variable two-mode squeezing resource state, paving the way towards hybrid quantum communication protocols. Our results show the experimental feasibility of distributed superconducting architectures and motivate further investigations of noisy quantum networks in various frequency regimes.

QI 18.3 Thu 15:45 BEY/0245

Entanglement distribution in hybrid-variable microwave networks — •Simon Gandorfer[1,2], Ivan Solomakhin[1,2], Maria-Teresa Handschuh[1,2], Joan Agustí[1,2], Achim Marx[1], Peter Rabl[1,2,3], Rudolf Gross[1,2,3], and Kirill G. Fedorov[1,2,3] — [1]Walther-Meißner- Institut, Bayerische Akademie der Wissenschaften, 85748 Garching, Germany — [2]School of Natural Sciences, Technische Universität München, 85748 Garching, Germany — [3]Munich Center for Quantum Science and Technology, 80799 Munich, Germany

Distributing entanglement between distant nodes of a large-scale quantum network is a fundamentally important milestone for quantum information processing. In particular, quantum entanglement is crucial for quantum teleportation protocols or logical quantum gates with remote qubits. In our experiment, we investigate remote entanglement of discrete-variable qubits by using contiunuos-variable entangled signals. The latter is represented by the two-mode squeezed microwaves generated with Josephson parametric circuits, while the former are given by superconducting transmons in 3D cavities. We observe a build-up of entanglement between the qubits due to their interaction with the common, quantum-correlated, reservoir. The corresponding entanglement conversion between continuous- and discrete-variables allows for promising and robust, hybrid-variable, quantum microwave networks. Finally, we discuss possible extensions and applications of our findings for distributed quantum computing architectures.

QI 18.4 Thu 16:00 BEY/0245

Quantum Key Distribution without Hidden Message Transmission — •Yien Liang, Anton Trushechkin, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, 40225 Düsseldorf, Germany

Steganography is the practice of hiding secret information within irrelevant information. A way to hide information within a valid digital signature is to take advantage of the random number required by a digital signature protocol, the adversary can maliciously choose a number that hides information instead of randomly choosing one. Such steganography technique is called subliminal channel [1]. A quantum key distribution (QKD) protocol involves communicating a large set of random random numbers, which can be used to establish a subliminal channel. The participants of a QKD protocol can intentionally hide information within the public announcement which is undetectable by any third party. Malicious QKD devices could also use a subliminal channel as a covert channel [2] to leak information to a third party. In our contribution, we propose a modified QKD protocol which is information-theoretic secure against eavesdropping and provable (more-than-one-bit-)subliminal-channel-free. We also generalize our results to quantum conference key agreement protocols.

[1] Simmons G J. Advances in cryptology: proceedings of crypto 83. Boston, MA: Springer US, 1984: 51-67. [2] Curty M, Lo H K. npj Quantum Information, 2019, 5(1): 14.

QI 18.5 Thu 16:15 BEY/0245

Verified delegated quantum computation requires techniques beyond cut-and-choose — •Fabian Wiesner and Anna Pappa — Technische Universität Berlin, Einsteinufer 17, 10587 Berlin, Germany

Delegated quantum computation enables a client with limited quantum capabilities to outsource computations to a more powerful quantum server while preserving correctness and privacy. Verification is crucial in this setting to ensure that the untrusted quantum server performs the computation honestly and returns correct results. A common verification method is the quantum cut-and-choose technique. Inspired by classical verification methods for two-party computation, the client uses the majority of the delegated rounds to test the server's honesty, while keeping the remaining ones for the actual computation. Combining this technique with other methods, such as quantum error correction, could help achieve negligible cheating probabilities for the server; however, such methods can impose significant overheads, making implementations unfeasible for the near-term future. In this work, we investigate whether cut-and-choose can yield efficient and secure verifiable quantum computation without additional costly techniques. We find that verifiable delegated quantum computation protocols relying solely on cut-and-choose techniques cannot be secure and efficient at the same time.

30min. break

QI 18.6 Thu 17:00 BEY/0245

Deployed BBM92 quantum key distribution using frequency-converted entangled photons emitted by a quantum dot — •Benjamin Breiholz[1], Michal Vyvlecka[1], Raphael Joos[1], Aurélien Marmasse[1], Ilenia Neureuther[1], Timo Schnieber[1], Anna Frederike Köhler[1], Tim Strobel[1], Tobias Bauer[2], Marlon Schäfer[2], Nand Lal Sharma[3], Caspar Hofmann[3], Simone Luca Portalupi[1], Christoph Becher[2], and Peter Michler[1] — [1]Institut für Halbleiteroptik und Funktionelle Grenzflächen, Center for Integrated Quantum Science and Technology (IQST) and SCoPE, 70569 Stuttgart, Germany — [2]Fachrichtung Physik, 66123 Saarbrücken, Germany — [3]Institute for Integrative Nanosciences, 01069 Dresden, Germany

We implemented an entanglement-based BBM92 quantum key distribution (QKD) protocol over approximately 700 m across the university campus buildings using the existing deployed fiber network. The entangled-photon pair at wavelength of 780 nm was emitted by an epitaxially grown droplet-etched GaAs quantum dot (QD) embedded in a dielectric antenna. The QD was excited via two-photon excitation using a pulsed laser that emits 10 ps pulses at 779 nm with a 380 MHz repetition rate. To minimize losses in silica fibers, we employed bidirectional, polarization-conserving quantum frequency conversion to shift the QD emission to a telecom wavelength. We achieved stable QKD operation for more than 10 hours, with a raw key rate exceeding 200 Hz and a quantum bit error rate below 4.5 %. After error correction and

privacy amplification, we distilled a secure key at a rate of 100 Hz.

QI 18.7 Thu 17:15 BEY/0245

GHz-clocked Single-photon Quantum Key Distribution in the Telecom C-band — •Koray Kaymazlar[1], Mareike Lach[1], Robert B. Behrends[1], Lucas Rickert[1], Martin von Helversen[1], Jochen Kaupp[2], Yorick Raum[2], Tobias Huber Loyola[2,3], Sven Höfling[2], Andreas Pfenning[2], and Tobias Heindel[4] — [1]Institute of Physics and Astronomy, Technische Univeristät Berlin — [2]Technische Physik, Physikalisches Institut and Würzburg-Dresden Cluster of Excellence — [3]Karlsruher Institut für Technologie, Institute of Photonics and Quantum Electronics — [4]Department for Quantum Technology, Univeristät Münster

High speed operation is one of the most desired properties for implementations of quantum key distribution (QKD). This requires however the generation and state-preparation of photonic qubits at high speed. Here, we report on a QKD system based on the BB84 protocol that operates at GHz clock-rates using a highly Purcell-enhanced single-photons source emitting in the telecom C-band. We use a laser with a repetition rate of 2.5 GHz to pump the quantum dot source and prepare the polarization states fot the protocol using a customized fiber-based electro-optic modulator (EOM) controlled by an arbitrary waveform generator (AWG) using the trigger output of the pump laser as common clock. Our results show that our system performs the BB84 protocol succesfully with a quantum bit error ratio (QBER) around 5 % at these unprecendeted high clock-rates.

QI 18.8 Thu 17:30 BEY/0245

Multiplexed multipartite quantum repeater rates in the stationary regime — •Anton Trushechkin, Julia Kunzelmann, Nikolai Wyderka, 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 consider a multipartite quantum repeater creating GHZ states between several parties from bipartite entanglement links. Each bipartite link is characterised by a success probability, i.e., probability of successful establishment of bipartite entanglement per round. We are interested in GHZ generation rate in such repeater on long times, i.e., in the stationary regime. On an abstract level, the mathematical description is also equivalent to the usual bipartite quantum repeater chain between two parties and the corresponding bipartite entanglement generation rate. We also consider the case of memory multiplexing and study its effect on the generation rate. We derive closed-form expressions for the stationary generation rate depending on the number of parties (or the segments in a chain of bipartite repeaters) and the multiplexing number.

QI 18.9 Thu 17:45 BEY/0245

Anonymous and private parameter estimation in networks of quantum sensors — Jarn De Jong[1], Santiago Scheiner[2], Naomi R. Solomons[2], •Ziad Chaoui[1], Damian Markham[2], and Anna Pappa[1] — [1]Technische Universität Berlin, Einsteinufer 19, 10587 Berlin, Germany — [2]LIP6, CNRS, Sorbonne Université, 4 place Jussieu, F-75005 Paris, France

Anonymity and privacy are two key properties of modern communication networks. In quantum networks, distributed quantum sensing has emerged as a powerful use case, with applications to clock synchronization, detecting gravitational effects, and more. In this work, we develop a new protocol that, for the first time, combines the different cryptographic properties of anonymity and privacy for the task of distributed parameter estimation. That is, we present a protocol that allows a selected subset of network participants to anonymously collaborate in estimating the average of their private parameters. Crucially, this is achieved without disclosing either the individual parameter values or the identities of the participants, neither to each other nor to the broader network.