QI 11: Quantum Communication

Time: Thursday 14:00–16:00 Location: H4

Invited Talk QI 11.1 Thu 14:00 H4

Numerical Security Analyis for Quantum Key Distribution and Application to Optical Protocols — •Norbert Lütkenhaus — Institute for Quantum Computing, University of Waterloo, Canada

The security analysis of Quantum Key Distribution (QKD) protocols reveals the achievable secrete key rate as a function of observable parameters, such as loss and noise parameters. Calculating the secret key rate is equivalent to solving a convex optimization problem. While for highly symmetric protocols that optimization protocol can be solved analytically, in general it is of advantage to resort to numerical approaches.

We will review the progress of this research agenda accessible to a broader audience to show how researchers with different backgrounds can contribute. The resulting toolbox is available as open source code [1]. I will show some applications, including finite size analysis and the use for optical protocols, such as the Discrete Modulated Continuous Variable QKD protocol. Our approach also allows the evaluation of side-channels that result from device imperfections, including a tight analysis of combinations of such imperfections.

[1] https://openqkdsecurity.org

Invited Talk QI 11.2 Thu 14:30 H4

Photonic graph states for quantum communication and quantum computing — •Stefanie Barz — Institute for Functional Matter and Quantum Technologies, University of Stuttgart, Germany — Centre for Integrated Quantum Science and Technologies, University of Stuttgart, Germany

Multipartite entanglement and, in particular, graph states are useful resources both for quantum computing and quantum communication, especially in networked settings. In this talk, I will show a few examples where multipartite entanglement offers an advantage over classical or bipartite approaches. In particular, I will present how photonic graph states can serve as a resource for computation and, vice versa, how computation can be used as a tool to test certain states. Furthermore, I will show how graph states offer an advantage for communication protocols, in particular in networked settings and where one aims at keeping the identity of the communicating parties private. I will present implementations of these concepts and discuss challenges in scaling up photonic quantum technologies.

QI 11.3 Thu 15:00 H4

Anonymous Quantum Conference Key Agreement — •Frederik Hahn[1], Jarn de Jong[2], and Anna Pappa[2] — [1]Freie Universität Berlin, Berlin, Deutschland — [2]Technische Universität Berlin, Berlin, Deutschland

Conference Key Agreement (CKA) is a cryptographic effort by multiple parties to create a shared secret key. In future quantum networks, generating secret keys in an anonymous manner is of enormous importance for parties who wish to keep their shared key secret while protecting their own identities. We present a CKA protocol using multipartite entangled GHZ states that is provably anonymous in realistic adversarial scenarios. The existence of secure and anonymous protocols based on multipartite entangled states provides a new insight into their potential as resources and paves the way for further applications.

DOI:https://doi.org/10.1103/PRXQuantum.1.020325

QI 11.4 Thu 15:15 H4

Resource analysis for quantum-aided Byzantine agreement — •Zoltán Guba[1], István Finta[2,3], Ákos Budai[1,2,4], Lóránt Farkas[2], Zoltán Zimborás[4,5], and András Pályi[1] — [1]Department of Theoretical Physics and MTA-BME Exotic Quantum Phases Research Group, Budapest University of Technology and Economics, Hungary — [2]Nokia Bell Labs, Budapest, Hungary — [3]Óbuda University, Budapest, Hungary — [4]Wigner Research Centre for Physics, Budapest, Hungary — [5]BME-MTA Lendület Quantum Information Theory Research Group, Budapest, Hungary and Mathematical Institute, Budapest University of Technology and Economics, Budapest, Hungary

In distributed computing, a byzantine fault is a condition where a component shows different symptoms to different components of the system. Consensus among the correct components in the presence of byzantine faults can be reached by appropriately crafted communication protocols. Quantum-aided protocols built upon distributed entangled quantum states are worth considering, as they are more resilient than traditional ones. Based on earlier ideas, we introduce a parameter-dependent family of quantum-aided weak broadcast protocols. We analyze the resource requirements as functions of the protocol parameters, and locate the parameter range where these requirements are minimal. Following earlier work demonstrating the suitability of noisy intermediate-scale quantum (NISQ) devices for the study of quantum networks, we show how to prepare our resource quantum state on publicly available IBM quantum computers.

QI 11.5 Thu 15:30 H4

Squeezing-enhanced communication without a phase reference — Marco Fanizza[1], •Matteo Rosati[2], Michalis Skotiniotis[2], John Calsamiglia[2], and Vittorio Giovannetti[1] — [1]NEST, Scuola Normale Superiore and Istituto Nanoscienze-CNR, I-56126 Pisa, Italy — [2]Física Teòrica: Informació i Fenòmens Quàntics, Departament de Física, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona) Spain

We study the problem of transmitting classical information using quantum Gaussian states on a family of phase-noise channels with a finite decoherence time, such that the phase-reference is lost after m consecutive uses of the transmission line. This problem is relevant for long-distance communication in free space and optical fiber, where phase noise is typically considered as a limiting factor. We show that the optimal Gaussian encoding is generated by a Haar-random passive interferometer acting on pure product states. We upper- and lower-bound the optimal coherent-state rate and exhibit a lower bound to the squeezed-coherent rate that, for the first time to our knowledge, surpasses any coherent encoding for m=1 and provides a considerable advantage with respect to the coherent-state lower bound for m>1. This advantage is robust with respect to moderate attenuation, and persists in a regime where Fock encodings with up to two-photon states are also suboptimal. Finally, we show that the advantage carries over to the private capacity of the channel and that the use of part of the energy to establish a reference frame is sub-optimal even at large energies.

QI 11.6 Thu 15:45 H4

Evaluating a Plug&Play Telecom-Wavelength Single-Photon Source for Quantum Key Distribution — Timm Gao[1], •Lucas Rickert[1], Felix Urban[1], Jan Grosse[1], Nicole Srocka[1], Sven Rodt[1], Anna Musiał[2], Kinga Zołnacz[3], Paweł Mergo[4], Kamil Dybka[5], Wacław Urbańczyk[3], Grzegorz Sek[2], Sven Burger[6], Stephan Reitzenstein[1], and Tobias Heindel[1] — [1]Institute of Solid State Physics, Technical University Berlin, 10623 Berlin, Germany — [2]Department of Experimental Physics, Wrocław University of Science and Technology, 50-370 Wrocław, Poland — [3]Department of Optics and Photonics, Wrocław University of Science and Technology, 50-370 Wrocław, Poland — [4]Institute of Chemical Sciences, Maria Curie Sklodowska University, 20-031 Lublin, Poland — [5]Fibrain Sp. z o.o., 36-062 Zaczernie, Poland — [6]Zuse Institute Berlin, 14195 Berlin, Germany

We report on quantum key distribution (QKD) tests using a 19-inch benchtop single-photon source at 1321 nm based on a fiber-pigtailed quantum dot (QD) integrated into a Stirling cryocooler. Emulating the polarization-encoded BB84 protocol, we achieve an antibunching of $g^{(2)}(0) = 0.10 \pm 0.01$, a raw key rate of up to 4.72 ± 0.13 kHz, and a maximum tolerable loss of 23.19 dB exploiting optimized temporal filters in the asymptotic limit [1]. Our study represents an important step forward in the development of fiber-based quantum-secured communication networks exploiting sub-Poissonian quantum light sources.

[1] T. Kupko et al., arXiv.2105.03473 (2021)