FM 7: Secure Communication & Computation I

Time: Monday 14:00–16:00 Location: 1009

FM 7.1 Mon 14:00 1009

A theoretical framework for PUFs and QR-PUFs — •Giulio Gianfelici, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Düsseldorf, Germany

We introduce a theoretical framework to describe Physical Unclonable Functions (PUFs), including extensions to quantum protocols, so-called Quantum Readout PUFs (QR-PUF).

(QR-) PUFs are physical systems with challenge-response behaviour intended to be hard to clone or simulate. Their use has been proposed in several cryptographic protocols, with particular emphasis on authentication.

We design a general authentication protocol, which is applicable to different physical implementations of (QR-) PUFs, and discuss the main properties which quantify the quality of such devices.

Our purpose is to find an agreement about theoretical assumptions and definitions behind the intuitive ideas of (QR-) PUFs, improving our ability to characterise the security of such devices in cryptographic protocols and to compare the performances between different (QR-) PUFs.

Such an agreement will allow us to derive security thresholds for (QR-) PUF authentication and possibly to develop further new authentication protocols.

FM 7.2 Mon 14:15 1009

Parameter regimes for surpassing the PLOB bound with error-corrected qudit repeaters — •Daniel Miller, Timo Holz, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany

A potential quantum internet would open up the possibility of realizing numerous new applications, including provably secure communication. Since losses of photons limit long-distance, direct quantum communication and widespread quantum networks, quantum repeaters are needed. The so-called PLOB-repeaterless bound [Pirandola et al., Nat. Commun. 8, 15043 (2017)] is a fundamental limit on the quantum capacity of direct quantum communication. Here, we analytically derive the quantum-repeater gain for error-corrected, one-way quantum repeaters based on higher-dimensional qudits for two different physical encodings: Fock and multimode qudits. We identify parameter regimes in which such quantum repeaters can surpass the PLOB-repeaterless bound and systematically analyze how typical parameters manifest themselves in the quantum-repeater gain. This benchmarking provides a guideline for the implementation of error-corrected qudit repeaters.

We have uploaded a preprint with the same title:
https://arxiv.org/abs/1906.05172

FM 7.3 Mon 14:30 1009

Secure quantum remote state preparation of squeezed microwave states — •S. Pogorzalek[1,2], K. G. Fedorov[1,2], M. Renger[1,2], Q.-M. Chen[1,2], M. Partanen[1], E. Xie[1,2], A. Marx[1], F. Deppe[1,2,3], and R. Gross[1,2,3] — [1]Walther-Meißner-Institut, Bayerische Akademie der Wissenschaften, 85748 Garching, Germany — [2]Physik-Department, TU München, 85748 Garching, Germany — [3]Munich Center for Quantum Science and Technology (MCQST), Schellingstr. 4, 80799 Munich, Germany

Quantum communication protocols employ nonclassical correlations as a resource for an efficient transfer of quantum states. As a fundamental protocol, remote state preparation (RSP) aims at the preparation of a known quantum state at a remote location using classical communication and quantum entanglement. We use flux-driven Josephson parametric amplifiers and linear circuit elements in order to generate propagating two-mode squeezed (TMS) microwave states acting as our quantum resource. Combined with a feedforward, we use the TMS states to experimentally demonstrate the continuous-variable RSP protocol by preparing single-mode squeezed states at a distant location [1]. Finally, security of RSP is investigated by using the concept of the one-time pad and measuring the von Neumann entropies.

We acknowledge support by Germany's Excellence Strategy EXC-2111-390814868, Elite Network of Bavaria through the program ExQM, the European Union via the Quantum Flagship project QMiCS (Grant No. 820505).

[1] S. Pogorzalek *et al.*, Nat. Commun. **10**, 2604 (2019).

Invited Talk FM 7.4 Mon 14:45 1009

Certification and estimation of quantum randomness — •Stefano Pironio — Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), Belgium

Contrarily to classical physics, quantum physics allows for the generation of numbers which are random even to a potential adversary that could have a complete knowledge of the randomness generating device. Furthermore, the generated entropy can be certified and estimated even if the devices are not entirely trusted thanks to the concept of self-testing. In this talk, I review and explain the theoretical framework used to assess the entropy generated by such self-testing quantum devices.

FM 7.5 Mon 15:15 1009

Quantum random number generation by phase diffusion in gain-switched semiconductor laser - new insights — •Sakshi Sharma, Brigitta Septriani, Oliver de Vries, and Markus Gräfe — Fraunhofer Institute for Applied Optics and Precision Engineering IOF, Jena, Germany

Randomness is essential for applications such as cryptography, stochastic simulation, gambling, and fundamental science experiments. Conventionally, random numbers are generated from mathematical algorithms using Pseudo-random number generators. We are interested in tackling this problem with quantum technology. Phase diffusion in spontaneous emission events is a quantum phenomenon with inherent randomness. Implementations of this scheme using pulsed lasers can yield high-speed quantum random number generation (QRNG). The general interest in the laser phase diffusion QRNG setup has been motivated by the speed of the random number generations. We reanalyze the process of phase diffusion based QRNG and give an intuitive explaining picture of the underlying physics. Our findings show that a pulsed process is beneficial over the continuous-wave approach and give an upper bound of the maximum random bit rate for a given experimental setting. Furthermore, we show how the QRNG probability distribution is influenced by several experimental factors such as the quality of the interference process and the noise in the detection system. Our theoretical, as well as experimental findings can help to find physical standards for QRNG verification rather than the ones based on classical statistical information theory.

FM 7.6 Mon 15:30 1009

Device-independent secret key rate from optimized Bell inequality violation — •Sarnava Datta, Timo Holz, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätstraße 1, D-40225, Düsseldorf, Germany

We introduce a Device-Independent Quantum Key Distribution(DIQKD) scenario where a Bell inequality (BI) will be constructed fromthe performed measurement data instead of using a predetermined BI. Given the observed data of a DIQKD protocol involving n parties, m measurement settings per party and k outcomes per measurement, our goal is to find an optimal (n,m,k) BI which maximizes the achievable DI secret key rate [1].

References: [1] L. Masanes, S. Pironio, and A. Acin, *Secure device-independent quantum key distribution with causally independent measurement devices,* Nature Communications, vol. 2, p. 238, 2011.

FM 7.7 Mon 15:45 1009

Bipartite and multipartite QKD via single-photon interference — •Federico Grasselli[1], Álvaro Navarrete[2], Marcos Curty[2], Hermann Kampermann[1], and Dagmar Bruss[1] — [1]Heinrich-Heine-Universität, Düsseldorf, Germany — [2]Escuela de Ingenieria de Telecomunicación, University of Vigo, Spain

Twin-Field (TF) QKD has been proven to beat the point-to-point private capacity of a lossy quantum channel, thanks to performing single-photon interference in an untrusted node. We focus on the TF-QKD protocol introduced by Curty et al., whose security relies on the estimation of the detection statistics of Fock-states through the decoy-state method. We derive analytical bounds on these quantities

assuming either two, three or four independent decoy intensity settings for each party, and we investigate the protocol's performance (arXiv:1902.10034). We show that two decoy intensity settings are enough to beat the point-to-point private capacity of the channel, that the protocol is fairly robust against uncorrelated intensity fluctuations of the optical pulses and that one can extract a secret key even when the losses in the two channels are highly asymmetric.

We then generalize the protocol to the multipartite scenario, by devising a conference key agreement (CKA) protocol where the users simultaneously distill a secret conference key through single-photon interference. The new CKA is better suited to high-loss scenarios than previous multipartite QKD schemes and employs for the first time a W-class state as its entanglement resource. We compare its performance with the iterative use of bipartite QKD protocols.