Q 45: Quantum Information (Quantum Communication) II

Time: Thursday 10:30–12:15 Location: S HS 002 Chemie

Q 45.1 Thu 10:30 S HS 002 Chemie

New insights in phase diffusion process in a gain-switched semiconductor laser for quantum random number generation (QRNG) — Brigitta Septriani, Oliver de Vries, and •Markus Gräfe — Fraunhofer Institute for Applied Optics and Precision Engineering IOF, Jena, Germany

Randomness is used for application in cryptography, stochastic simulation, gaming and gambling, and fundamental science experiments. Common practice is to generate random numbers from mathematical algorithm using Pseudo-random number generators. We are interested in tackling this problem with quantum technology. Phase diffusion in spontaneous emission events is a quantum phenomena 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 mainly focused on and motivated by the speed of the random number generations. Little has been stated about the performance of quantum phase noise as a randomness source in QRNG, from the perspective of the physics involved. We reanalyze the process of phase diffusion based QRNG and give a intuitive explaining picture of the underlying physics. Our findings show that a pulsed process is beneficial over the continuous-wave approach and give a upper bound of maximum random bit rate for a given experimental setting. 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.

Q 45.2 Thu 10:45 S HS 002 Chemie

Towards a 1 Gbit/s quantum random number generator — •Benedict Tohermes, Julian Göttsch, Sebastian Steinlechner, and Roman Schnabel — Institut für Laserphysik und Zentrum für Optische Quantentechnologie, Universität Hamburg, Luruper Chaussee 149, 22761 Hamburg, Deutschland

With higher speeds being achieved in quantum key distribution and rising demand for random keys in regular cryptography, the need for fast quantum random number generators arises. A common implementation of such a random number generator employs quadrature measurements of an optical vacuum state as its entropy source, using balanced homodyne detection. Here we report on our progress for such a setup with a target bit rate of 1 Gbit/s. We present our implementation and discuss the signal processing steps that are required to achieve a high bit rate while ensuring randomness of generated keys.

Q 45.3 Thu 11:00 S HS 002 Chemie

Atmospheric quantum optics: the role of fluctuating losses — •Martin Bohmann[1,2], Jan Sperling[3], Andrii A. Semenov[1,4], and Werner Vogel[1] — [1]Theoretische Quantenoptik, Universität Rostock — [2]QSTAR, INO-CNR, and LENS, Firenze, Italy — [3]Integrated Quantum Optics Group, University of Paderborn — [4]Institute of Physics, National Academy of Sciences of Ukraine

Global quantum communication based on atmospheric free-space channels is a rapidly developing and growing research area. In this contribution, we address the question of how fluctuating losses in such channels affect the quantum properties of light. We perform a rigorous analysis of the quantum states after passing through the turbulent atmosphere and study different quantum effects including single-mode nonclassicality and Gaussian, non-Gaussian, and multi-partite entanglement. The survival of nonclassical effects in free-space channels is shown to depend on the mean photon number and on coherent displacements. Therefore, it differs essentially from constant-loss scenarios. We propose optimal strategies for the transmission of nonclassical quantum states. Eventually, our results will help to improve free-space quantum communication.

Q 45.4 Thu 11:15 S HS 002 Chemie

Satellite-based links for Quantum Key Distribution: beam effects and weather dependence — •Carlo Liorni, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich Heine Universität, Universitätstr. 1, Düsseldorf 40225, Germany

The establishment of a world-wide quantum communication network relies on the synergistic integration of satellite-based links and fiber-based networks.

Optical satellite links have the drawback of being strongly dependent on the weather conditions. The presence of turbulent eddies and scattering particles like haze or fog induce random deviations and deformations of the optical beam. In this work we generalize a recently proposed approach [D. Vasylyev et al., PRA 96, 043856] to satellite-based links, taking into account both phenomena. We analytically compute the beam parameters at the receiver and the correspondent Probability Distribution of the Transmittance (PDT), depending on the weather conditions.

The expected transmittance of the link is then used to study the performances of the polarization-based BB-84 cryptographic protocol in different real-life scenarios and configurations (Up- and Down-links). The model presented here supports the analysis of new protocols or proposals for future satellite missions.

Q 45.5 Thu 11:30 S HS 002 Chemie

A payload for satellite quantum communication on a CubeSat — •Ömer Bayraktar[1,2], Jonas Pudelko[1,2], Imran Khan[1,2], Gerd Leuchs[1,2], and Christoph Marquardt[1,2] — [1]Max Planck Institute for the Science of Light, Erlangen, Germany — [2]Institute of Optics, Information and Photonics, Friedrich-Alexander University Erlangen-Nürnberg

The limited range of quantum key distribution (QKD) in fiber based systems lead to several projects aiming for the development of a satellite based QKD infrastructure. For smaller satellite missions with a stringent demand on size, weight and power photonic integrated circuits (PICs) are a convenient way to implement all necessary optical functions.

In this work, we present a CubeSat payload for the demonstration of quantum communication technology in space. It contains an integrated sender for modulated weak coherent states, as well as an integrated quantum random number generator (QRNG) based on measurements of the quantum optical vacuum state. In practice, both systems are implemented on Indium-Phosphide PICs and contained on a 10x10cm PCB.

These developments will be tested as a part of the CubeSat mission QUBE.

Q 45.6 Thu 11:45 S HS 002 Chemie

Communication with a binary alphabet over a phase noise channel — •Ludwig Kunz[1,2], Matthew DiMario[3], Konrad Banaszek[1,2], and Francisco Elohim Becerra[3] — [1]Centre of New Technologies, University of Warsaw, Warszawa, Poland — [2]Faculty of Physics, University of Warsaw, Warszawa, Poland — [3]Center for Quantum Information and Control, University of New Mexico, Albuquerque, New Mexico

For reliable optical communication state discrimination is a critical task. Quantum measurements can provide significant enhancement in information transfer compared to classical techniques. However, noise in the communication channel or the measurement limits the benefits of quantum techniques. While linear losses result in simple rescaling of the complex field amplitude, the effects of phase diffusion are less trivial and require new strategies for information retrieval. We investigate a single-shot measurement which shows robustness when communicating over a phase noise channel. In this communication scenario the information is encoded in a binary alphabet of coherent states where the average energy is limited. We consider a measurement based on a displacement operation followed by photon counting with finite photon number resolution. By optimizing the displacement operation, the information transfer can be maximized while at the same time the effect of phase noise is minimized. This communication strategy provides enhancement compared to classical detection when the amplitudes of the alphabet have been optimized for both techniques.

Q 45.7 Thu 12:00 S HS 002 Chemie

Device-independent quantum key distribution beyond CHSH violation — •Timo Holz, Sarnava Datta, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany

In early proposed protocols for quantum key distribution (QKD) one imposes in general too strong assumptions on the devices that reality

cannot match. Any realistic implementation is imperfect, which can be exploited by a malicious eavesdropper. The strongest form of security is thus achieved by avoiding any assumption about the internal working of the devices, which is called device-independent (DI) QKD. Security proofs for DIQKD rely on a loophole-free violation of Bell inequalities. The violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality is directly connected to the DI secret-key rate [1]. We aim at generalizing this connection to the case of n parties, m measurement settings and k measurement outcomes. In particular, we establish a connection between the DI secret-key rate and the violation of a Bell inequality other than CHSH, by numerically lower bounding the secret-key rate via semidefinite programming, based on [2]. In principle, this numerical approach allows a calculation of lower bounds on the secret-key rate in terms of the violation of a general (n,m,k)-Bell inequality, which is constructed in a preceding step from the measurement data, cf. [3]. We illustrate our method with an example.

[1] A. Acin et al., Phys. Rev. Lett. 98, 230501 (2007)
[2] L. Masanes et al., Nat. Commun. 2, 238 (2011)
[3] J. Szangolies et al., Phys. Rev. Lett. 118, 260401 (2017)