FM 86: Poster: Secure Communication & Computation

Time: Thursday 16:30–18:30 Location: Tents

FM 86.1 Thu 16:30 Tents

Relevance of POVMs for Bell nonlocality — •Lucas Tendick, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany

We discuss the relevance of general positive-operator valued measures (POVMs) for Bell nonlocality. Despite the fact that POVMs outperform projective measurements in many other quantum information tasks, about the benefit of POVMs with respect to nonlocality only little is known. We study Bell inequalities which involve up to four outcomes with multiple settings and discuss their properties. Especially the advantage of POVMs compared to projective measurements on qubits in terms of maximal violation and robustness of the inequality is analysed. We discuss both facet and non-facet defining inequalities of the local polytope from the literature, as well as new inequalities found by linear programming. Furthermore, possible connections between Bell inequalities and tasks where an advantage of POVMs is well-known are analysed.

FM 86.2 Thu 16:30 Tents

Tripartite Device-independent Quantum Key Distribution Beyond CHSH Violation — •Timo Holz, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany

Security proofs for device-independent (DI) quantum key distribution (QKD) rely on a loophole-free violation of Bell inequalities. We introduce a novel Bell inequality including three parties, where each of them measure two dichotomic observables. This Bell inequality functions as a DI witness for genuine tripartite entanglement, given a particular violation is observed. We furthermore present a DIQKD protocol based on the violation of this new Bell inequality. The connection between achievable conference-key rates and the violation of the multipartite Bell inequality is established with the semidefinite programming techniques introduced in Ref. [1]. Thus, our approach goes beyond breaking the multipartite-Bell setting down into an effective bipartite one, violating the Clauser-Horne-Shimony-Holt inequality, and the results of Ref. [2]. We suggest a suitable tripartite QKD protocol and study the effect of different noise models on achievable asymptotic secret-conference-key rates.

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

FM 86.3 Thu 16:30 Tents

Test of a time-bin entanglement-based QKD system in a commercial optical link. — •Oleg Nikiforov, Erik Fitzke, Daniel Hofmann, Kai Roth, and Thomas Walther — AG Laser und Quantenoptik, Institut für Angewandte Physik, Technische Universität Darmstadt, Schlossgartenstr. 7, 64289 Darmstadt, Germany

Quantum Key Distribution offers means for cryptographic key exchange, superior in security to the majority of contemporary classical key distribution schemes. We are working on a time-bin entanglement-based system for quantum key distribution. We test its performance in a real-world commercial telecommunication environment of Deutsche Telekom. In this contribution, we discuss the recent progress of our experiment and show first results.

FM 86.4 Thu 16:30 Tents

Fiber-based source for QKD around 1550 nm — •Maximilian Tippmann, Oleg Nikiforov, Erik Fitzke, and Thomas Walther — AG Laser und Quantenoptik, Institut für Angewandte Physik, Technische Universität Darmstadt, Schlossgartenstr. 7, 64289 Darmstadt, Germany

We develop an all-fiber system for quantum key distribution in a commercial telecom network via energy-time entangled photons. Our source consists of a PPLN crystal pumped by a MOPA with subsequent SHG and can be operated in cw as well as pulsed. A modular setup guarantees robust and flexible operation outside of a controlled lab environment. In the contribution, we discuss the performance of the whole system and its components.

FM 86.5 Thu 16:30 Tents

Photoluminescence excitation spectroscopy of single quantum dots emitting in the 2^{nd} and 3^{rd} telecom windows — •H. Salamon[1], P. Wyborski[1], A. Maryński[1], A. Musiał[1], P. Podemski[1], T. Heusler[2], N. Srocka[2], D. Quandt[2], A. Strittmatter[2], S. Rodt[2], A. Kors[3], J.P. Reithmaier[3], M. Benyoucef[2], S. Reitzenstein[3], and G. Sek[1] — [1]Wrocław University of Science and Technology, Poland — [2]Technical University of Berlin, Germany — [3]University of Kassel, Germany

Photoluminescence excitation spectroscopy (PLE) allows for energy structure determination and energy transfer processes observation in semiconductor structures. Single dot PLE has always been challenging in the spectral range above 1 μm . Here, we present how this technique was adapted to single quantum dots (InGaAs/GaAs and InAs/InP) emitting in the 2^{nd} and 3^{rd} telecom windows, including demonstration of excited states detection in single nanostructures. This kind of quantum dots are promising candidates for non-classical photon sources required for quantum communication and computation applications.

We acknowledge financial support via the "Quantum dot-based indistinguishable and entangled photon sources at telecom wavelengths" project carried out within the HOMING programme of the Foundation for Polish Science co-financed by the European Union under the European Regional Development Fund. This work was also financially supported by the German Federal Ministry of Education and Research (BMBF) within projects Q.com-H and Q.Link.X.

FM 86.6 Thu 16:30 Tents

Spectral Characterization of Photon Pairs for Quantum Key Distribution — •Erik Fitzke, Daniel Hofmann, Till Dolejsky, Oleg Nikiforov, and Thomas Walther — TU Darmstadt, Institute of Applied Physics, 64289 Darmstadt

We are developing a QKD system with energy-time entangled photon pairs around 1550 nm. The system will later be integrated in a standard telecommunication network. Our system requires characterization of the spectra of the emitted photon pairs and of the influence of transmission through several kilometers of telecommunication fiber. Thus, we compare different methods of analysis such as a grating spectrograph, the arrival time shift due to chromatic dispersion or autocorrelation function measurement. Results of the different approaches with photon pairs from SPDC will be presented.

FM 86.7 Thu 16:30 Tents

Towards efficient single-photon sources at telecom wavelengths — •J. Jasiński[1], N. Srocka[2], W. Rudno-Rudziński[1], P.-I. Schneider[3], S. Burger[3,4], D. Quandt[2], A. Strittmatter[2], S. Rodt[2], A. Musiał[1], S. Reitzenstein[2], and G. Sek[1] — [1]Wrocław University of Science and Technology, Poland — [2]Technical University of Berlin, Germany — [3]JCMwave, Berlin, Germany — [4]Zuse Institute Berlin, Germany

Extraction efficiency is the main limiting factor in applications (e.g. QKD) of single-photon sources at telecom wavelengths required for integration with existing fiber networks. Epitaxial quantum dots (QDs) embedded in the solid-state matrix are very attractive in view of their integration, scalability and compatibility with current semiconductor technology. Here we present epitaxial In0.75Ga0.25As/GaAs QDs grown on a DBR and capped with strain reducing layer. QDs were deterministically embedded into cylindrical photonic mesa structures using in-situ electron beam lithography. The extraction efficiency has been determined based on single QD emission spectrum measured at saturation in a calibrated setup under non-resonant pulsed excitation using single photon counting modules. Values exceeding 10% have been achieved, but theoretical calculations show possibility of reaching 40% following optimized mesa geometry design.

We acknowledge financial support via the QuanTel project carried out within the HOMING programme of the Foundation for Polish Science co-financed by the EU under the European Regional Development Fund and by the Polish National Agency for Academic Exchange.

FM 86.8 Thu 16:30 Tents

Photonic integrated circuits 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, Er-

langen, Germany — [2]Institute of Optics, Information and Photonics, Friedrich-Alexander University Erlangen-Nürnberg, Germany

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

In this work, we present our payload intended for the demonstration of integrated quantum communication technology in space. It is based on two Indium-Phosphide PICs implementing a source for modulated weak coherent states as well as a quantum random number generator (QRNG) based on homodyne measurements of the quantum mechanical vacuum state. The whole system is implemented on a 10 cm x 10 cm PCB including electronics, making it compatible to the CubeSat standard.

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

FM 86.9 Thu 16:30 Tents

True randomness certified from loop-hole free Bell test — •Xing Chen[1], Ilja Gerhardt[1], Jörg Wrachtrup[1], Robert Garthoff[2], Kai Redeker[2], and Wenjamin Rosenfeld[2] — [1]3. Institute of Physics, University of Stuttgart and Institute for Quantum Science and Technology, IQST, Pfaffenwaldring 57, D-70569 Stuttgart, Germany — [2]Fakultät für Physik, Ludwig-Maximilians-Universität, D-80799 Munich, Germany

The loop-hole free test of Bell's inequality allows us to certify quantum random numbers with a very limited set of prior assumptions [1]. The randomness certified by Bell's theorem was extracted by singlet probability $p(a|x)$ in previous studies, which does not fully extract the device-independent (DI) randomness in the Bell test data. A more precise and smaller upper bound could be deduced by semi-defined-programs, but it is not convenient and not secure for practical use. Here, we develop an analytic upper bound for the joint outcome probability $p(ab|xy)$, so we can extract all the DI randomness from the Bell test data. In a weaker semi-device-independent conditions, with dimension witnesses [2], substantial more randomness can be extracted than in the device-independent cases. We use our models on the loop-hole free Bell test experiment [3], and certify more randomness than previous models.

[1] S. Pironio, *et al.*, Nature 464.7291 (2010): 1021.
[2] J. Bowles, *et al.*, Physical Review Letters 112.14 (2014):140407.
[3] W. Rosenfeld, *et al.*, Physical Review Letters 119.1 (2017): 010402.