Advances in Quantum Cryptography using Quantum Dot Devices

David Becker[1], Daniel A. Vajner[1], Koray Kaymazlar[1], Mareike Lach[1], Fenja Drauschke[2], Lucas Rickert[1], Martin von Helversen[1], Robert Behrends[1], Hanqing Liu[3], Shulun Li[3], Haiqiao Ni[3], Zhichuan Niu[3], Jochen Kaupp[4,5], Yorick Reum[4,5], Tobias Huber-Loyola[5,6], Sven Höfling[4,5], Andreas Pfenning[4,5], Anna Pappa[2] and Tobias Heindel[7]

[1] Institute of Physics and Astronomy, Technical University Berlin
[2]Electrical Engineering and Computer Science Department, Technical University of Berlin, Berlin, Germany
[3]State Key Laboratory of Optoelectronic Materials and Devices, Institute of Semiconductors, Chinese Academy of Sciences, Beijing, China
[4]University of Würzburg, Physikalisches Institut and Würzburg-Dresden Cluster of Excellence ctd.qmat, Lehrstuhl für Technische Physik, Germany
[5]Technische Physik, Physikalisches Institut, University of Würzburg
[6]Institute of Photonics and Quantum Electronics (IPQ) and Center for Integrated Quantum Science and Technology (IQST)
[7] Department for Quantum Technology, Univeristät Münster, Münster, Germany

Quantum key distribution (QKD) can be used to establish a secret key between trusted parties, a task for which quantum light sources based on quantum dots proved useful [1]. Many practical use-cases in communication networks, however, involve parties who do not trust each other. A fundamental cryptographic building block for such distrustful scenarios is quantum coin flipping (QCF), which has been investigated only in few experimental studies to date (e.g., [2-4]), all of which used probabilistic quantum light sources imposing fundamental limitations.

This poster reviews our recent advances in the field of quantum cryptography using quantum dot light sources. One focus will be on our first step in the field of quantum cryptography beyond QKD. Employing a deterministically fabricated quantum dot single-photon source, we experimentally implement a QCF protocol [5]. Using fast, random polarization-state encoding of single-photon pulses with sufficiently low quantum bit error ratio, we demonstrate an advantage compared to both classical realizations and implementations using faint laser pulses. While this first implementation was realized with single photons at 930 nm wavelength and at a standard clockrate of 80 MHz, our recent efforts target operation wavelengths in the telecom C-band as well as clock-speeds in the GHz-regime. Based on our progress on ultra-fast coherent quantum dot light sources emitting at 1550 nm [6], we present our most recent advances in the generation of single-photons at clock-rates of 2.5 GHz [7]. These results are expected to enable GHz-clocked implementations of single-photon QKD and other cryptographic primitives in the foreseeable future.

References

[1] D. A. Vajner et al., Advanced Quantum Technologies, 2100116 (2022)
[2] A. Pappa et al., Nature Communications 5, 1–8 (2014)
[3] G. Molina-Terriza et al., Physical Review Letters 94, 040501 (2005)
[4] S. Neves et al, Nature Communications 14(1), 1855 (2023)
[5] D. A. Vajner, K. Kaymazlar, F. Drauschke et al., Nature Communcations 17, 2074 (2026)
[6] R. Behrends et al., Highly-indistinguishable single-photons at 1550 nm from a two-photon resonantly excited Purcell-enhanced quantum dot, arXiv: 2602.06140 (2026)
[7] R. Behrends et al., manuscript in preparation (2025)