Kolloquium des Instituts für Angewandte Physik

TECHNISCHE UNIVERSITÄT DARMSTADT

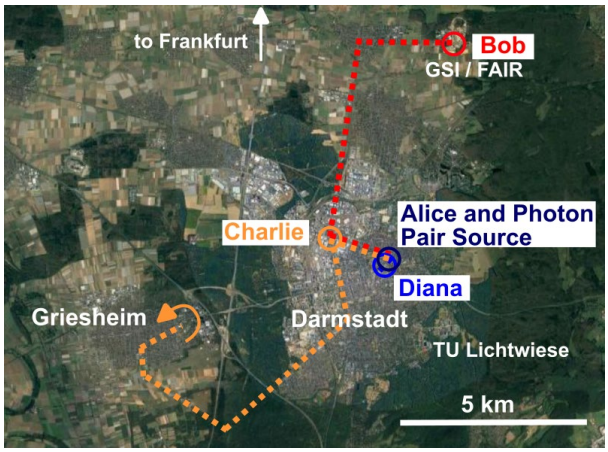
Zeit: **Dienstag 15.07.2025, 16 Uhr**

Ort: Gebäude S2|15, Raum 134 (Handbibliothek)

City-Wide Multi-User Quantum Key Distribution Network without Trusted Nodes

Maximilian Tippmann, M.Sc.
Institut für Angewandte Physik, TU Darmstadt

Large parts of today's cryptography solutions are threatened by the potential speed up of algorithms, such as Shor's algorithm, when utilizing quantum computers. Quantum key distribution (QKD) offers a new means for secure generation of symmetric, random keys, based on the no-cloning theorem of quantum mechanics rather than relying on mathematical hardness assumptions.



As part of the DFG collaborative research center CROSSING, the Laser and Quantum Optics Group (LQO) at the TU Darmstadt investigates scalable QKD networks with a focus on field tests. Setting up real-world QKD networks remains a challenge as distortions on the transmission links, such as polarization drifts, deteriorate the system's overall secure key generation rate. Furthermore, extensive data post-processing is required. Both factors complicate continuous recalibration of the setup, as the available data is either (partly) locally constrained or more complex setups are required to compensate for potential drifts. Scalability to more than two users is another issue, which is often neglected in experiments. Employing more point-to-point QKD links requires additional hardware and, in some network scenarios, introduces intermediary stations that have complete knowledge of the secure key (i.e. trusted nodes).

The main topic of this colloquium is the setup and first city-wide field test of the Darmstadt Quantum Local Area Network (DaQLAN). Being an all-fiber QKD system, it utilizes energy-time entangled photon pairs to employ a time-bin variant of the 1992 Bennett-Brassard-Mermin (BBM92) protocol, making it resilient against polarization drifts in the transmission fibers without active stabilization techniques. A wide type-0 SPDC spectrum supports simultaneous pairwise key exchange from the same photon pair source for more than 100 users. For the demonstration, four users have been distributed over the city of Darmstadt with fiber links of up to 62 km length and feature a complete post-processing software to enable real-time key generation. The network is reconfigurable, i.e., each user can be connected to any other endpoint, while the photon source is untrusted due to the employed protocol, thus making our network trusted-node-free. In this talk, the source setup and characterization, as well as results from the field tests, are presented, with a focus on optimizing the secure key generation rate.

Der Sprecher wird betreut von Herrn Prof. Dr. T. Walther