idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Technische Universität Darmstadt
Silke Paradowski

25.05.2022
http://idw-online.de/de/news794442

Forschungsergebnisse, Wissenschaftliche Publikationen
Informationstechnik, Physik / Astronomie
überregional

Secure communication with light particles - Researchers at TU Darmstadt develop anti-eavesdropping quantum network

Darmstadt, May 25, 2022. While quantum computers offer many novel possibilities, they also pose a threat to internet security since these supercomputers make common encryption methods vulnerable. Based on the so-called quantum key distribution, researchers at TU Darmstadt have developed a new, tap-proof communication network. Their results have now been presented in the renowned journal "PRX Quantum".

The new system is used to exchange symmetric keys between parties in order to encrypt messages so that they cannot be read by third parties. In cooperation with Deutsche Telekom, the researchers led by physics professor Thomas Walther succeeded in operating a quantum network that is scalable in terms of the number of users and at the same time robust without the need for trusted nodes. In the future, such systems could protect critical infrastructure from the growing danger of cyberattacks. In addition, tap-proof connections could be installed between different government sites in larger cities.
The system developed by the Darmstadt researchers enables the so-called quantum key exchange, providing several parties in a star-shaped network with a common random number. Individual light quanta, so-called photons, are distributed to users in the communication network in order to calculate the random number and thus the digital key. Due to quantum physical effects, these keys are particularly secure. In this way, communication is particularly highly protected, and existing eavesdropping attacks can be detected.
So far, such quantum key methods have been technically complex and sensitive to external influences. The system of the Darmstadt group from the Collaborative Research Center CROSSING is based on a special protocol. The system distributes photons from a central source to all users in the network and establishes the security of the quantum keys through the effect of so-called quantum entanglement. This quantum-physical effect produces correlations between two light particles, which are observable even when they are far apart. The property of the partner particle can be predicted by measuring a property of the light particle from a pair.
Polarization is often used as a property, but this is typically disturbed in the glass fibers used for transmission due to environmental influences such as vibrations or small temperature changes. However, the Darmstadt system uses a protocol in which the quantum information is encoded in the phase and arrival time of the photons and is therefore particularly insensitive to such disturbances. For the first time, the group has succeeded in providing a network of users with quantum keys by means of this robust protocol.
The high stability of the transmission and the scalability in principle were successfully demonstrated in a field test together with Deutsche Telekom Technik GmbH. As a next step, the researchers at TU Darmstadt are planning to connect other buildings in the city to their system.

Collaborative Research Center CROSSING
More than 65 scientists from the fields of cryptography, quantum physics, system security and software engineering work together in the Collaborative Research Center CROSSING and conduct both fundamental and application-oriented research. The goal is to develop security solutions which will enable secure and trustworthy IT systems for the future. CROSSING has been funded by the German Research Foundation (DFG) since 2014.

About TU Darmstadt
TU Darmstadt is one of Germany's leading technical universities and a synonym for excellent, relevant research. We are crucially shaping global transformations – from the energy transition via Industry 4.0 to artificial intelligence – with outstanding insights and forward-looking study opportunities. TU Darmstadt pools its cutting-edge research in three fields: Energy and Environment, Information and Intelligence, Matter and Materials. Our problem-based interdisciplinarity as well as our productive interaction with society, business and politics generate progress towards sustainable development worldwide. Since we were founded in 1877, we have been one of Germany's most international universities; as a European technical university, we are developing a trans-European campus in the network, Unite! With our partners in the alliance of Rhine-Main universities – Goethe University Frankfurt and Johannes Gutenberg University Mainz – we further the development of the metropolitan region Frankfurt-Rhine-Main as a globally attractive science location.

www.tu-darmstadt.de

MI-No. 32e/2022, Fitzke/Walther/mih/cst

wissenschaftliche Ansprechpartner:

Professor Thomas Walther
Department of Physics
Institute for Applied Physics
E-Mail: thomas.walther@physik.tu-darmstadt.de

Originalpublikation:

Erik Fitzke, Lucas Bialowons, Till Dolejsky, Maximilian Tippmann, Oleg Nikiforov, Thomas Walther, Felix Wissel, and Matthias Gunkel: "Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding", in PRX Quantum
DOI: https://doi.org/10.1103/PRXQuantum.3.020341
https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.3.020341