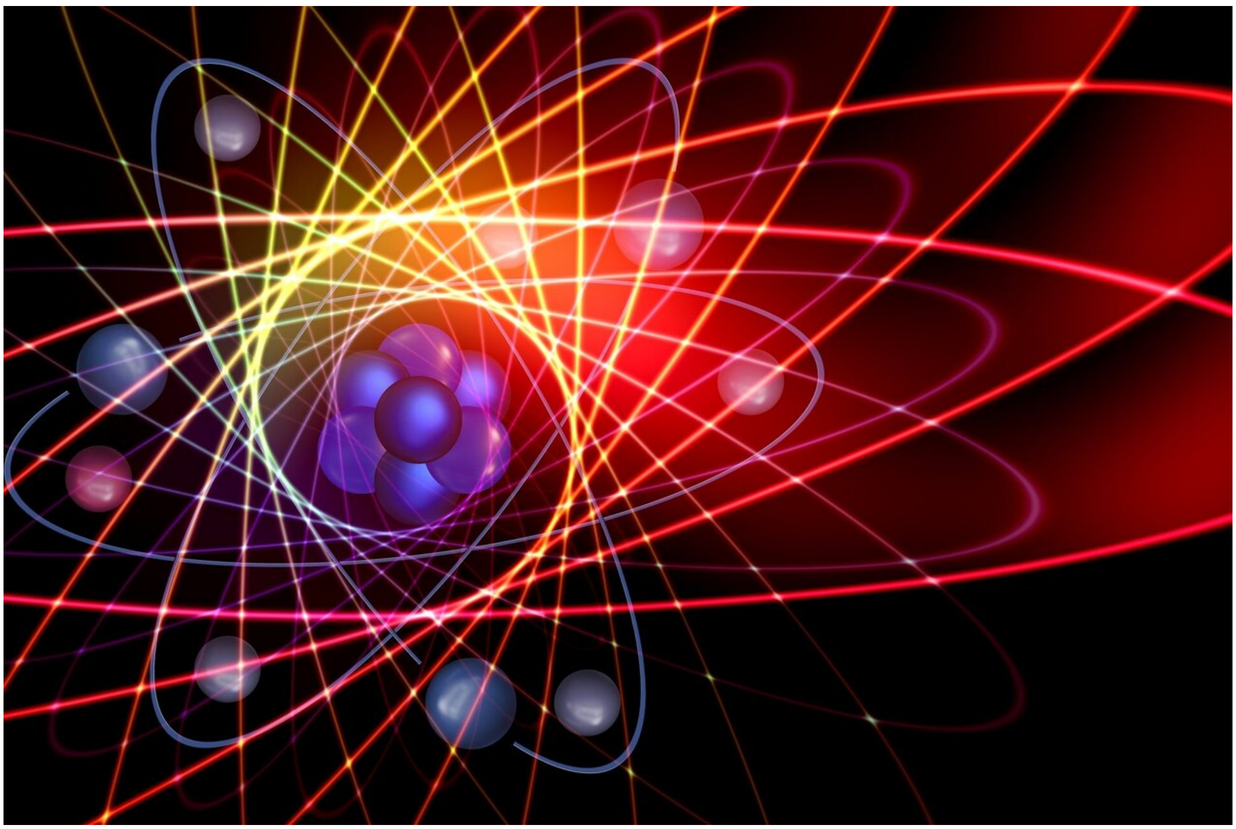
Secure communication with light particles that sidesteps the reliance on polarization

May 25 2022



Credit: Pixabay/CC0 Public Domain

A new communication system has been developed 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, 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 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 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 from 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 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. The research is published in *PRX Quantum*.

More information: Erik Fitzke et al, Scalable Network for Simultaneous Pairwise Quantum Key Distribution via Entanglement-Based Time-Bin Coding, *PRX Quantum* (2022). DOI: 10.1103/PRXQuantum.3.020341

Provided by Technische Universitat Darmstadt