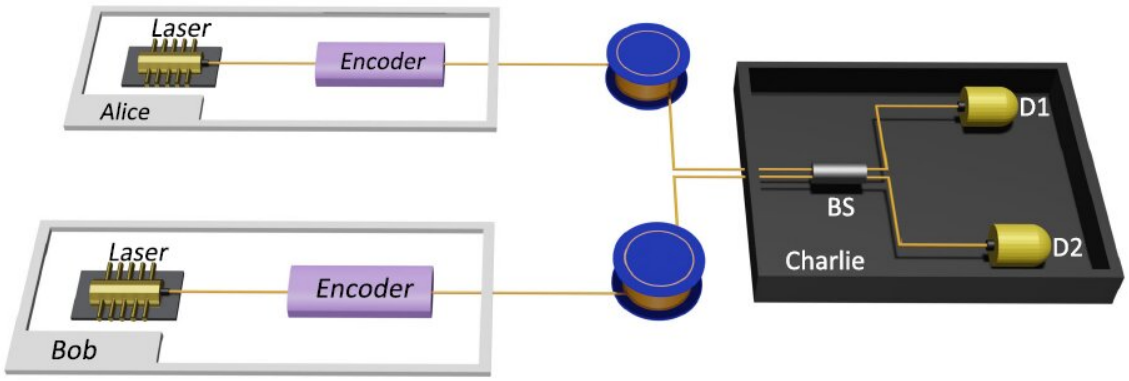
Experimental implementation of measurement-device-independent quantum key distribution

December 6 2022



At Alice's (Bob's) site, the simplified transmitter contains a laser source and an encoder. The encoder modulates the phase of the optical pulses. The modulation information of the encoder should be monitored to characterize the deviation between ideal and realistic pulses. If the untrusted Charlie is honest, he measures the signals received using an interference measurement. Credit: Science China Press

Recently, the research group of Prof. Zeng-Bing Chen and Associate Prof. Hua-Lei Yin (National Laboratory of Solid State Microstructures and School of Physics, Collaborative Innovation Center of Advanced

Microstructures, Nanjing University), cooperating with Beijing National Laboratory for Condensed Matter Physics and Institute of Physics, Chinese Academy of Sciences and other institutes, proposed a four-phase measurement- device-independent type quantum key distribution (QKD) protocol and implemented a proof-of-principle experiment to prove the feasibility.

The study guaranteed security of the protocol against arbitrary source imperfections and all attacks at the detector. It also characterized the source imperfections with measurable parameters in experimental implementations. The experimental result showed that the secure key rate could achieve 0.25 kbps when the channel loss is 20 dB.

Under a channel loss of 10 dB (about 50 km optical fiber), the security key rate could achieve 91 kbps, which can meet the one-time pad encryption requirements for voice calls. Compared with previous measurement- device-independent QKD protocols that take account of imperfect sources, this research has significantly improved the security key rate and transmission distance, demonstrating the huge application potential in the practical deployment of secure QKD with device imperfections.

The research result was published in *Science Bulletin*.

Compared with classical key distribution, QKD enables two distant participants to share secure key bits for the encryption and decryption of secret communication. Together with the one-time pad algorithm, QKD offers theoretical security for information exchanges based on the laws of quantum mechanics. However, for the practical operation of QKD systems, a serious security loophole still exists, which occurs due to the discrepancy between theoretical security assumptions and practical devices.

To be precise, a security proof of QKD is established with assumptions on the system devices, which cannot be satisfied for realistic devices because of inherent imperfections and the disturbance of eavesdroppers. This deviation results in more information leakage to eavesdroppers, which cannot be noticed by users. To narrow the discrepancy and further strengthen the security against device flaws, device independent QKD and measurement-device-independent QKD were proposed.

Device independent QKD guarantees the unconditional security of QKD by measuring the violation of Bell's inequality without any assumptions about devices. Recently, international researchers have realized proof-of-principle experiments of device-independent QKD with studies published in *Nature* and *Physical Review Letters*, respectively.

However, experimental implementations of device-independent QKD still suffer from short transmission distances and are far from being implemented in long-distance transmission. Measurement-device-independent QKD protocols can successfully close all the loopholes at detectors by introducing an untrusted intermediate node for interference measurement.

Compared with device independent QKD protocols, measurement-device-independent QKD protocols do not need to make any assumptions on the intermediate node with a higher secure key rate and longer transmission distance.

For example, the current world records of measurement-device-independent QKD protocols are the 404 km two-photon interference measurement-device-independent QKD achieved by Hua-Lei Yin et al., and the 833 km single photon interference twin-field QKD achieved by Shuang Wang et al. Measurement-device-independent QKD protocols are considered to be the best choice with practical security and efficiency. Therefore, it is significant to solve source imperfections in

measurement-device-independent QKD protocols.

There mainly exist four kinds of source imperfections in QKD protocols including state preparation flaws, side channels caused by mode dependency, Trojan horse attacks and pulse correlations. For solving loopholes caused by the above source imperfections, the study adopted the recently proposed reference technique method to fully characterize the referred source imperfections and prove the security of a four-phase measurement-device-independent QKD protocol.

Additionally, the study measured the parameters characterizing source imperfections and conducted a finite-key analysis of the protocol to help generate a secure key rate in the experiment.

Furthermore, the study implemented a proof-of-principle experiment to prove the feasibility of the protocol. The experiment utilized the Sagnac loop to stabilize the phase fluctuation of the channel automatically, and all optical fibers maintain polarization.

More information: Jie Gu et al, Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources, *Science Bulletin* (2022). DOI: 10.1016/j.scib.2022.10.010

Provided by Science China Press