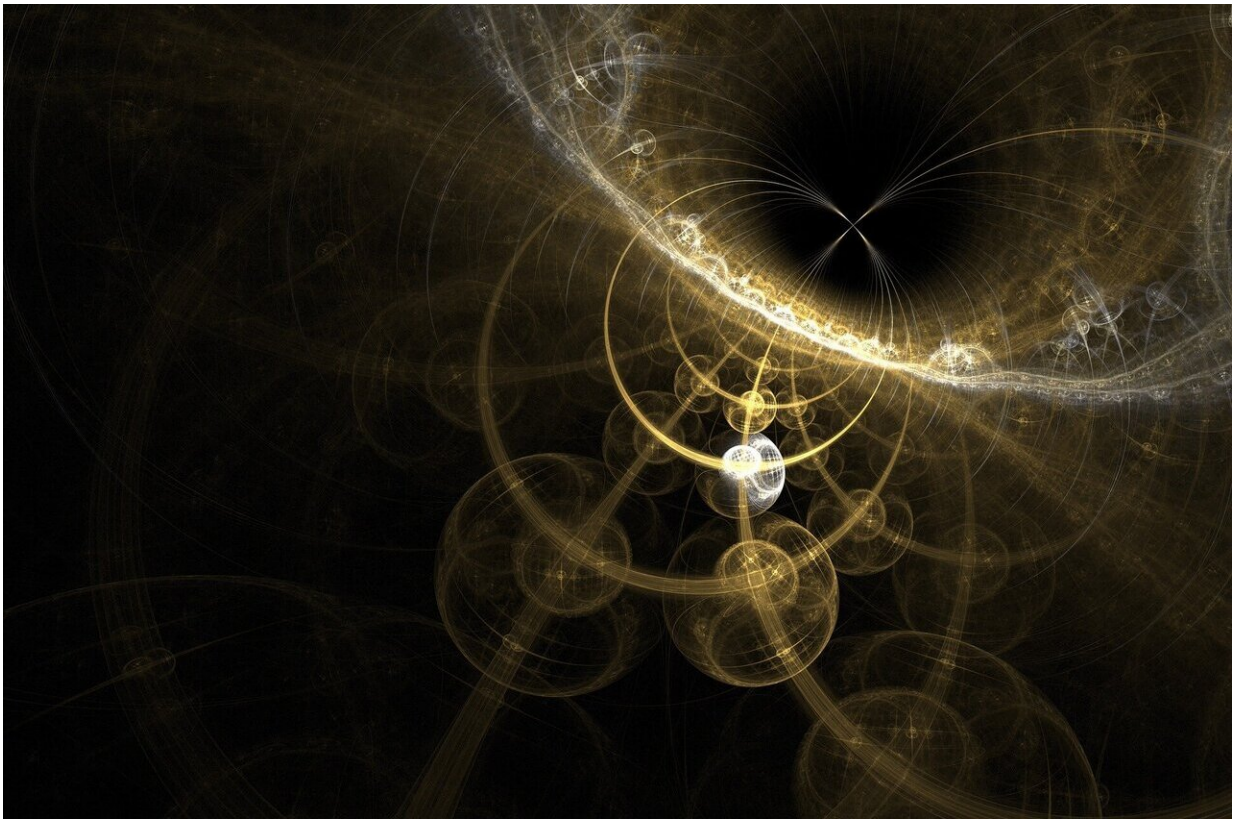
New approach takes quantum key distribution further

August 19 2020



Credit: CC0 Public Domain

In an important step toward practical implementation of secure quantum-based communication, researchers have demonstrated secure measurement-device-independent quantum key distribution (MDI-QKD)

transmission over a record-breaking 170 kilometers.

QKD can offer impenetrable encryption by using the quantum properties of light to generate secure random keys between users for encrypting and decrypting online data. The measurement-device-independent QKD protocol is among the most secure and practical because it is immune to attacks directed at the detection devices that measure the quantum properties of individual photons.

Qin Wang from Nanjing University of Posts and Telecommunications will discuss the proof-of-principle demonstration at the inaugural OSA Quantum 2.0 conference to be co-located as an all-virtual event with OSA Frontiers in Optics and Laser Science APS/DLS (FiO + LS) conference 14-17 September.

"We investigate the three-state MDI-QKD protocol with uncharacterized sources and conduct an experimental demonstration, where it allows imperfect state-preparation and the only assumption is the prepared states are in a two-dimensional Hilbert space," said Wang. "This work significantly improves both the security and practicability of QKD under current technology."

Boosting security over long distances

Although QKD has been demonstrated over relatively long distances, it has been difficult to accomplish this with high transmission rates while maintaining security. To overcome this challenge, Wang developed a new MDI-QKD transmission protocol that uses photons with three characterized quantum states to encode data.

The standard MDI-QKD protocol can resist all potential detection loopholes; unfortunately, it still assumes perfect state preparation that can be a great challenge in practice. To protect against state-preparation

imperfections, some countermeasures have been put forward. Yin et al. proposed a method called MDI-QKD with uncharacterized sources by incorporating mismatched-basis data that are normally discarded from the calculation of phase-error rate. Based on Yin and other people's work, the research team developed a practical scheme, where not only an improved phase estimation method, but also a simple three-state scheme is implemented to obtain substantially enhanced performance compared with other uncharacterized-source or loss-tolerant MDI-QKD schemes.

Using a state-of-the-art experimental setup for encoding and detection, the researchers showed that the new QKD approach could transmit keys over longer distances and at higher rates (10^{-7} /pulse key rate) than other similar measurement-device-independent QKD protocols. Theoretical calculations showed that secure transmission could be possible over distances up to 200 kilometers.

The present work can be further developed by incorporating either the highly efficient decoy-state method or the new proposed twin-field QKD protocols.

Provided by The Optical Society