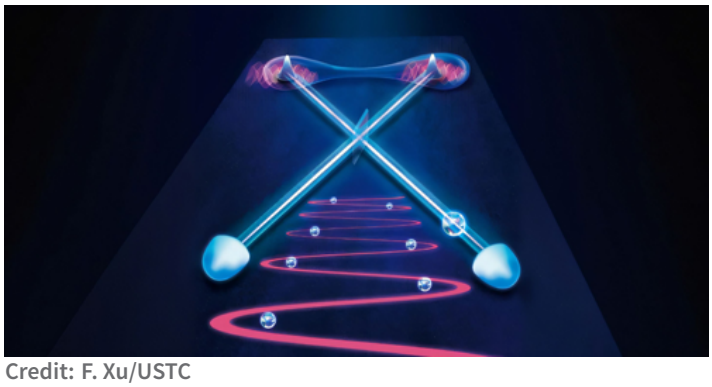
Toward Practical Quantum Cryptography

Researchers have shown that they can distribute quantum keys under realistic conditions using commercial lasers.

By **Charles Day**

Quantum key distribution (QKD) exploits the quantum features of photons to share cryptography keys between two parties in a way that makes any eavesdropping readily apparent. Keys have been exchanged successfully across cities and even between a spacecraft and a ground station. Such feats usually require complex, expensive equipment. Now Feihu Xu and Jian-Wei Pan of the University of Science and Technology of China (USTC) and their collaborators have demonstrated QKD over 403 km of standard optical fiber using off-the shelf lasers [**1**]. At nearly 48 bits per second (bit/s), their key distribution rate is high enough for some real-world applications.

Despite optical fiber's impressive transparency, QKD photons traveling through a fiber eventually get scattered or absorbed and lose their entanglement. One way to extend the transmission distance is to place an intermediary—based on an interferometer—halfway between the source and the receiver. The two parties don't have to trust the intermediary, but it does need to be able to accurately compare the streams of photons coming from them. This comparison can be achieved using a technique called mode pairing, which uses a clever way to pair up the incoming photons. The method requires tracking the photon frequencies, which ordinarily entails additional equipment, including high-quality lasers for both parties. Xu and his colleagues figured out that performing a fast Fourier transform on the photons serves to track the frequencies even when lower-quality lasers are used.



Credit: F. Xu/USTC

The QKD performance achieved by the USTC team falls short for securely sharing video and other high-bandwidth applications. But, Xu says, "Our result of 47.8 bit/s over 403 km is already sufficient for many high-security applications, such as secure messaging, key distribution for financial transactions, or authentication in communications over long distances."

Charles Day is a Senior Editor for *Physics Magazine*.

REFERENCES

1. L. Zhang *et al.*, "Experimental mode-pairing quantum key distribution surpassing the repeaterless bound," **Phys. Rev. X 15, 021037 (2025).**