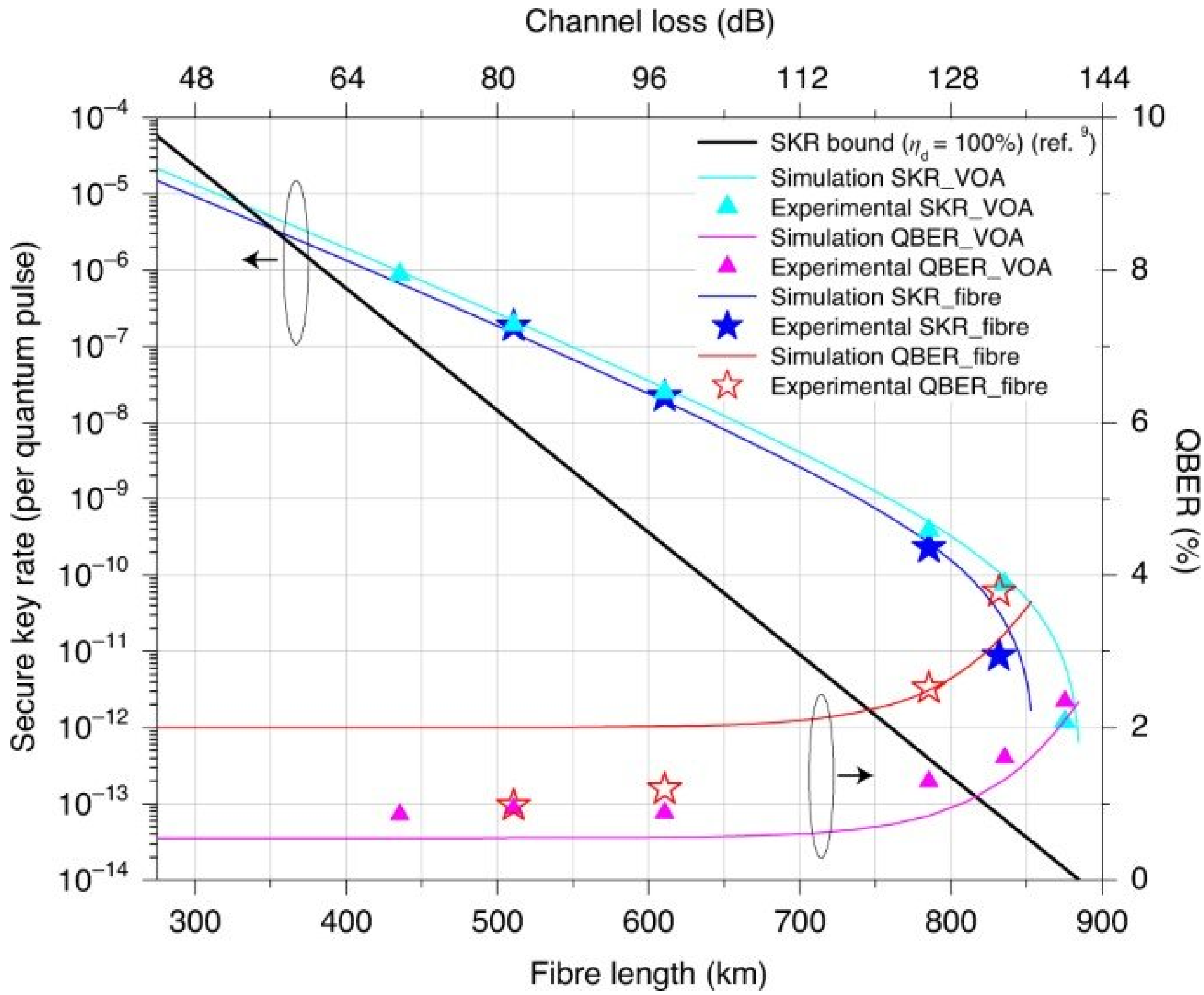
PHYS.ORG

# Twin-field quantum key distribution (QKD) across an 830-km fibre

January 24 2022, by Thamarasee Jeewandara

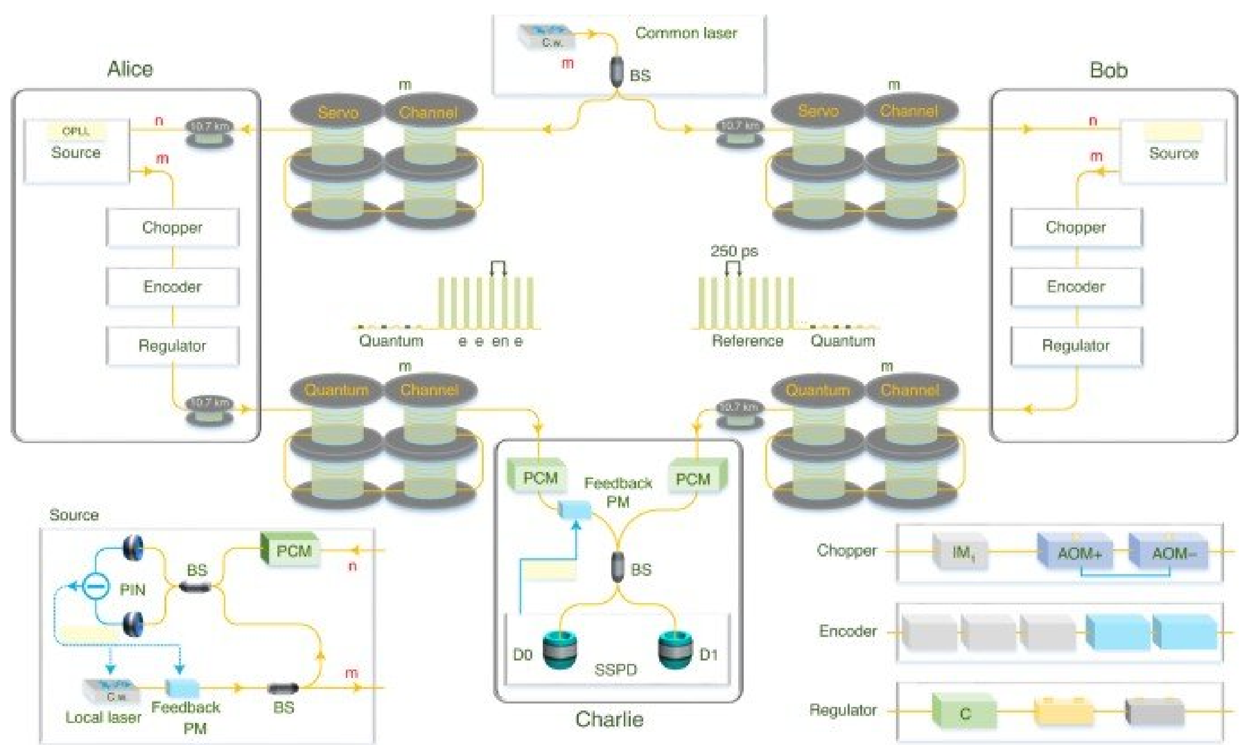



Summary of recent long-distance QKD experiments beyond 400 km. In VOA and fibre scenarios, the total numbers of transmitted quantum signals were 3 × 1014 and 3.2 × 1014, respectively. Nature Photonics, https://doi.org/10.1038/s41566-021-00928-2

By using quantum key distribution (QKD), quantum cryptographers can share information via theoretic secure keys between remote peers through physics-based protocols. The laws of quantum physics dictate that photons carrying signals cannot be amplified or relayed through classical optical methods to maintain quantum security. The resulting transmission loss of the channel can limit its achievable distance to form a huge barrier to build large-scale quantum secure networks. In a new report now published in *Nature Photonics*, Shuang Wang and a research team in quantum information, cryptology and quantum physics in China developed an experimental QKD system to tolerate a channel loss beyond 140 dB across a secure distance of 833.8 km to set a new record for fiber-based quantum key distribution. Using the optimized four-phase twin-field protocol and high quality setup, they achieved secure key rates that were more than two orders of magnitude greater than previous records across similar distances. The results form a breakthrough to build reliable and terrestrial quantum networks across a scale of 1000 km.

## Quantum cryptography and twin-field quantum key distribution (QKD)

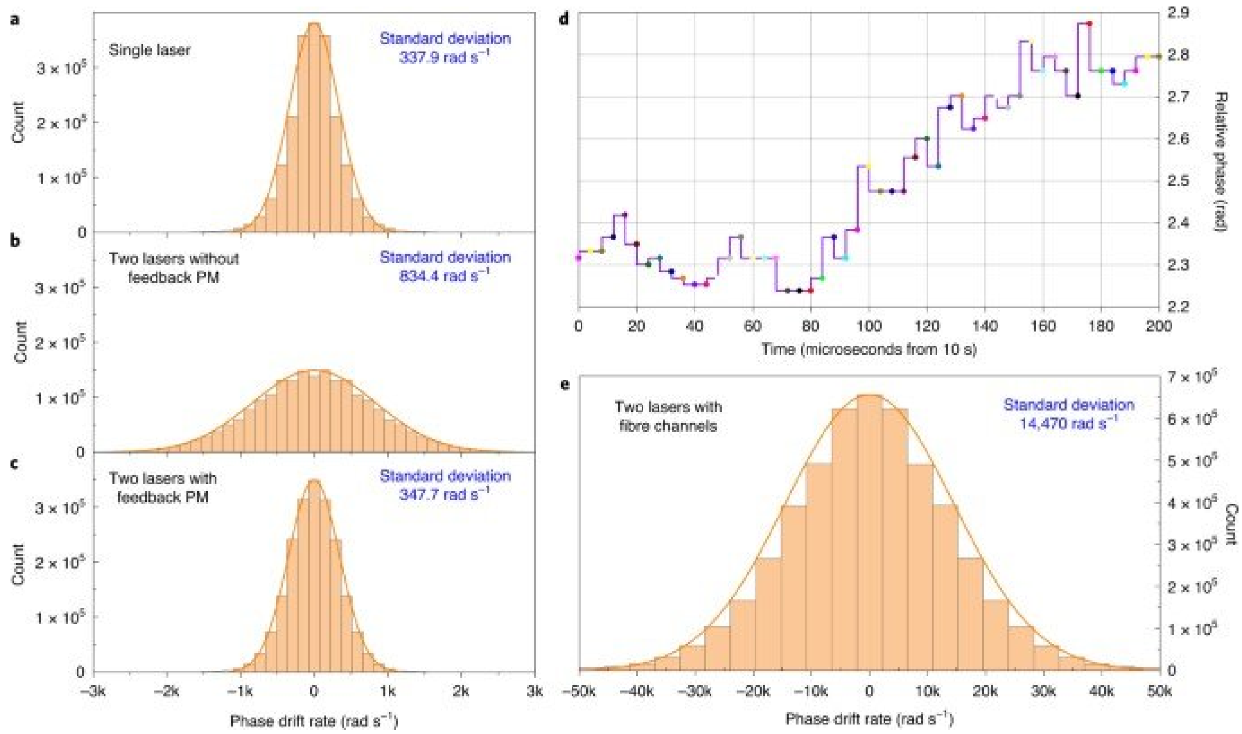
Quantum key distribution is based on fundamental laws of physics to distribute secret bits for information-theoretic secure communication, regardless of the unlimited computational power of a potential eavesdropper. The process has attracted widespread attention in the past three decades relative to the development of a global quantum internet, and matured to real-world deployment through optical-fiber networks. Despite this, wider applications of QKD are limited due to channel loss, limiting increase in the key rate and range of QKD. For example, photons are carriers of quantum keys in a QKD setup, and they can be prepared at the single-photon level to be scattered and absorbed by the transmission channel. The photons, however, cannot be amplified, and therefore the receiver can only detect them with very low probability. When transmitted via a direct fiber-based link from the transmitter to the receiver, the key rate can therefore decrease with transmission distance. As a result, twin-field QKD can build a promising rate-distance relationship to overcome limits and achieve a secret key rate across long distances. Researchers have taken great efforts to develop its theory and experimentally demonstrate the unique advantages of the system. Wang et al. analyzed the cumulative results of recent long-distance fiber-based QKD experiments for fiber lengths beyond 450 km, revolving around twin-field quantum key distribution (TF-QKD) protocols to illustrate huge advantages of TF-QKD, while highlighting advances of the present study.




Optical layout of the TF-QKD system. To remotely generate the twin fields between Alice and Bob, both of them lock their local laser sources to a free-running common laser via a homodyne OPLL. The common light beam is transmitted though the servo channel. Alice's and Bob's twin fields then enter their respective chopper, encoder and regulator to perform the four-phase TF-QKD protocol. After travelling through quantum channels, Alice's and Bob's encoded pulses interfere with each other on Charlie's BS, and are finally registered by two SSPDs, D0 and D1. Nature Photonics, https://doi.org/10.1038/s41566-021-00928-2

## The four-phase twin field quantum key distribution protocol

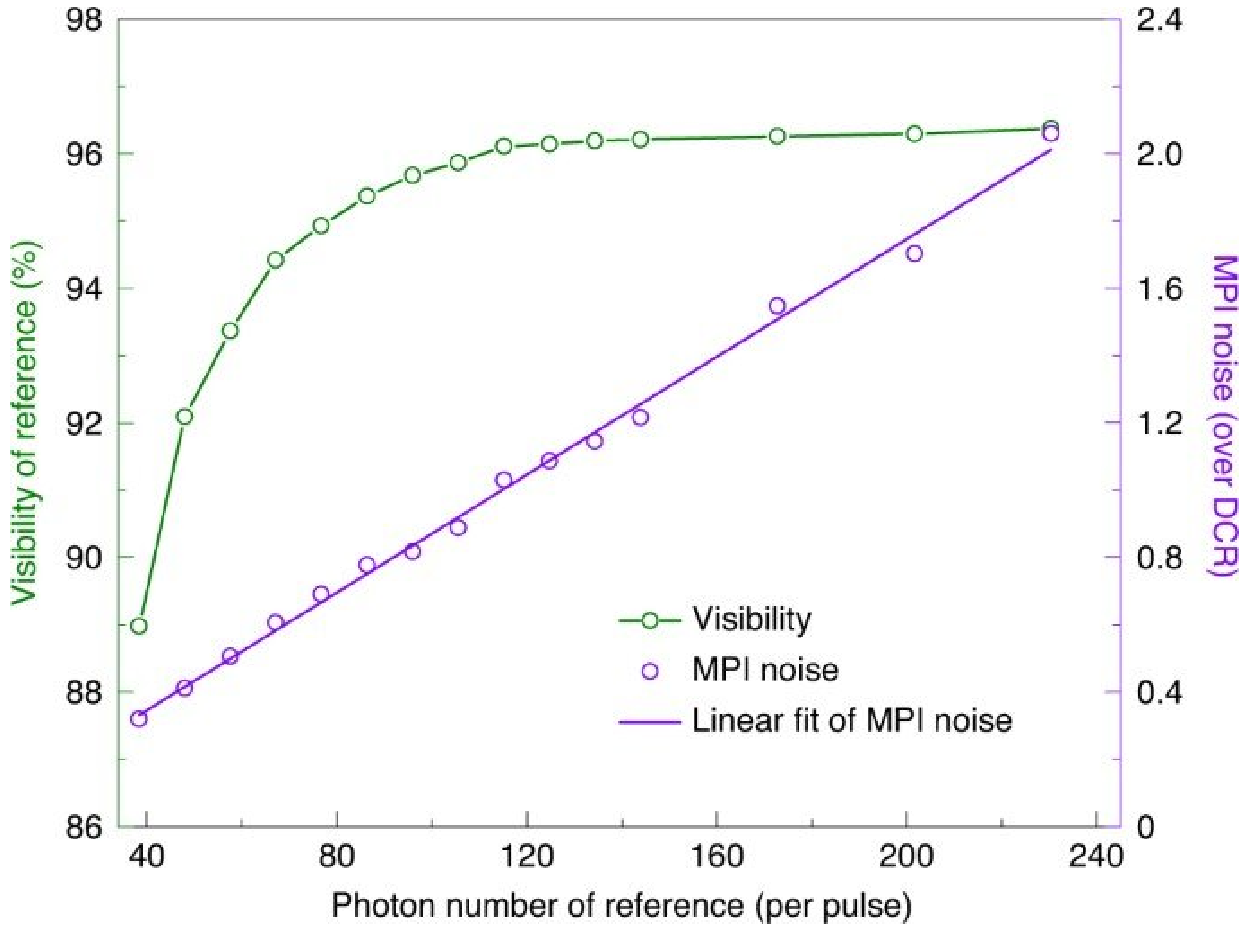
The protocol contained five steps: At step one, Alice and Bob independently prepared a weak coherent state with randomly chosen intensity and probabilities. In step two, within the code mode, Alice (or Bob) can pick a 'key' bit and a 'basis' bit to randomly prepare a weak coherent state. During step three, Alice and Bob sent their weak coherent states to an untrusted middle station Charlie, who could make the incoming states interfere on a beamsplitter. The experimental setup contained two single-photon detectors located at two distinct outputs of the beam splitter labeled $D_0$ and $D_1$, respectively, where Charlie must publicly announce the clicks of $D_0$ and $D_{1.}$ The team repeated the first three steps for a number of times (labeled $N_{tot}$). During step four, among the $N_{tot}$ trials, only when just one of $D_0$ and $D_1$ clicks were they retained for further processing. Alice and Bob then broadcast the intensities for each retained trial to ultimately form the sifted key string. Finally, according to resulting lengths, Alice and Bob could share a secret key string with length G, from their sifted key string with a failure probability not larger than a value of $\epsilon_{sec} = 2^{-31}$ computed in the study.




Results of source noise and phase drift with fibre channels. (a–c) Comparison of the source noise of three sources versus the phase drift rate of two light beams from a single laser (a), two phase-locked lasers without feedback PM in the source (b) and two phase-locked lasers with feedback PM in the source (c). d,e, The phase drift with fibre channels and two phase-locked lasers: the relative phase in a 200-μs timescale, calculated using recorded data from 10 s to 10.0002 s (d); histogram and distribution of the phase drift rate over 20 s (e). The orange lines in panels a,b,c, and e are distribution curves of the histogram (The histogram can be seen as a series of individual plots). Thus panels a,b,c, and e are 'histogram and distribution of phase drift rate'. Nature Photonics, https://doi.org/10.1038/s41566-021-00928-2

## The twin-field quantum key distribution (TF-QKD) experimental system

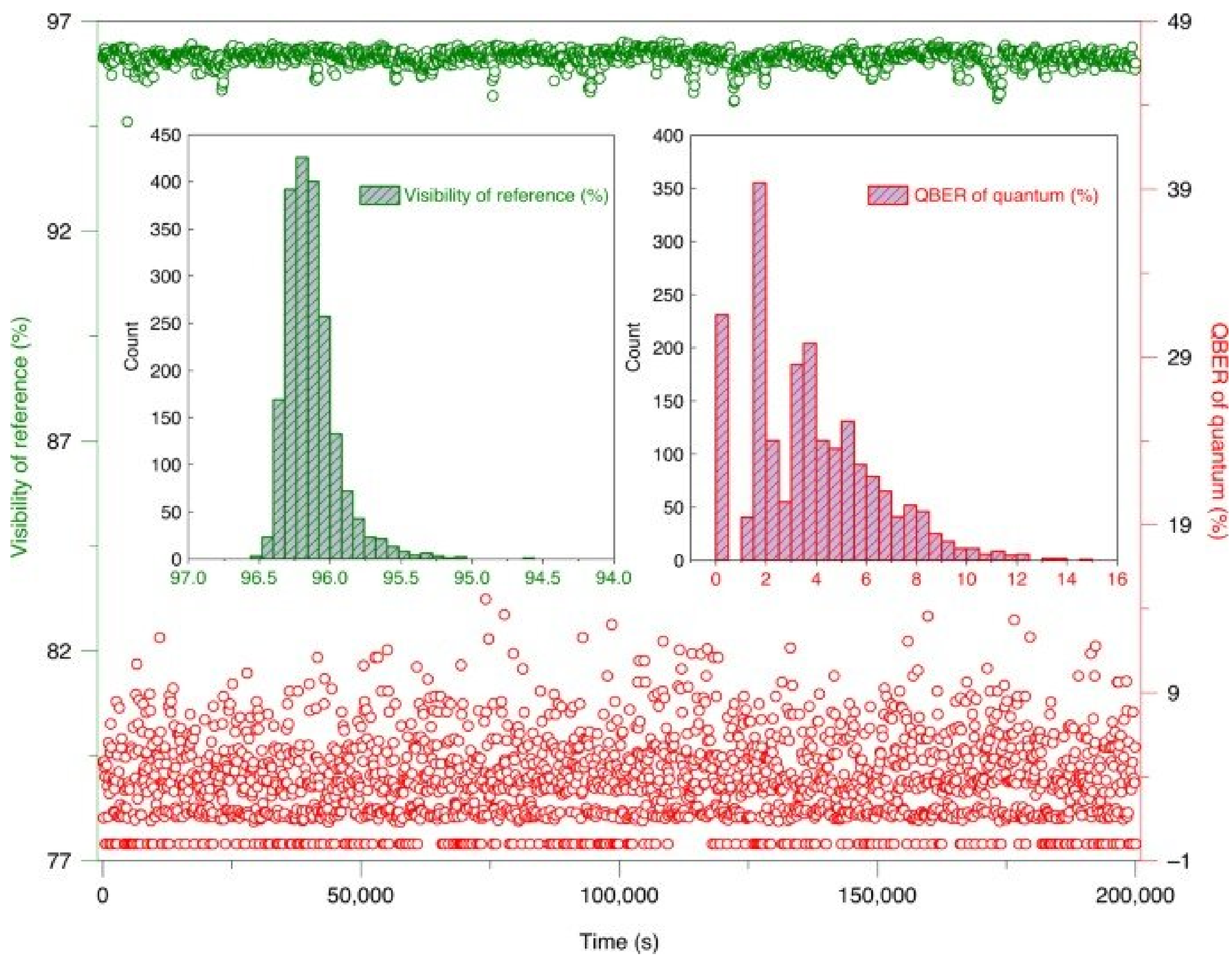
The experimental setup required optical pulses from two remote users to stably interfere in the intermediate station (Charlie). The wavelength difference and phase difference between Alice and Bob's sources were designated to be relatively stable across time. Using a free running common laser, the team locked both Alice's and Bob's sources to reconcile their central wavelength values and employed a time division multiplexing method to compensate for fast phase drift introduced by the fiber channels. These fiber channels included the servo channel to transmit light from the common laser to Alice (or Bob), and the quantum channel adopted to transmit the time-multiplexed signal from Alice and Bob to Charlie. During the experiments, after passing through corresponding quantum channels and polarization compensation modules, Alice's and Bob's encoded twin fields interfered on Charlie's beam splitter for detection by two superconducting nanowire single-photon detectors. During experimental realization, the team formed a high-speed and low-noise TF-QKD system and optimized its performance by reducing the effect of noises originating from the source, channel and the detector. When compared to earlier experiments, a key advantage of the current experiment was its lack of requirements for optical amplifiers inserted to increase the power of classical signals, while reducing the complexity of the setup for scientists to generate remote, high-quality twin fields with reduced complexity and cost.




Interference visibility and MPI noise versus the intensity of the reference pulses. For the scenario with 833.80-km quantum channels, the visibility of the in-phase interference in the reference part and MPI noise in the quantum part were measured simultaneously. MPI noise is quantified in units of DCR. Nature Photonics, https://doi.org/10.1038/s41566-021-00928-2

## Generating twin fields—optimizing the setup

Wang et al. reduced the noise from the source and the servo channel to develop a highly sensitive and repeater-like laser source to ultimately generate twin-fields with 10-mw output power. They improved the sensitivity of the repeater-like laser source to work with very weak input power, even as low as 0.2 nW. The resulting twin-fields were generated with very high quality, which they optimized to achieve low multipath interference (MPI) noise, with high interference visibility in the quantum channels. The stability of the twin-field system played an important role to collect enough counts of quantum pulses, for the QKD system to function continuously for several weeks. The longest fiber-length across which Wang et al. could keep a relatively high interference visibility and achieve a positive key rate was 833.80 km, with a secure key rate of 0.014 bps after maximizing the outcome.




System stability over a distance of 833.80 km of quantum channel. The olive and red open circles respectively represent the in-phase interference visibilities of

Alice's and Bob's reference parts and the QBER of their quantum parts. Each circle corresponds to data gathered in 100 s. The insets show the corresponding distributions of interference visibility and QBER. Nature Photonics, https://doi.org/10.1038/s41566-021-00928-2

## Outlook

In this way, Shuang Wang and colleagues showed how a fiber-based quantum key distribution (QKD) could be realized across a distance of 833.8 km with a channel loss of 140 dB. The new setup set records for tolerant channel loss and the long transmission distance of fiber-based QKD, while achieving secure key rates that outperformed previous twin-field quantum key distribution experiments at similar distances. The absence of optical amplifiers in the setup helped reduce the complexity and cost with great potential in field and network applications. The study provides a practical format to extend the transmission distance and pave the way towards a wider-range of QKD experiments.

**More information:** Shuang Wang et al, Twin-field quantum key distribution over 830-km fibre, *Nature Photonics* (2022). DOI: 10.1038/s41566-021-00928-2

Marcos Curty et al, Simple security proof of twin-field type quantum key distribution protocol, *npj Quantum Information* (2019). DOI: 10.1038/s41534-019-0175-6