ARTICLES
https://doi.org/10.1038/s41566-021-00928-2

nature photonics

Check for updates

Twin-field quantum key distribution over 830-km fibre

Shuang Wang[1,2,3,7], Zhen-Qiang Yin[1,2,3,7], De-Yong He[1,2,3] ✉, Wei Chen[1,2,3] ✉, Rui-Qiang Wang[1,2,3], Peng Ye[1,2,3], Yao Zhou[1,2,3], Guan-Jie Fan-Yuan[1,2,3], Fang-Xiang Wang[1,2,3], Wei Chen[4,5], Yong-Gang Zhu[5], Pavel V. Morozov[6], Alexander V. Divochiy[6], Zheng Zhou[1,2,3], Guang-Can Guo[1,2,3] and Zheng-Fu Han[1,2,3] ✉

Quantum key distribution (QKD) provides a promising solution for sharing information-theoretic secure keys between remote peers with physics-based protocols. According to the law of quantum physics, the photons carrying signals cannot be amplified or relayed via classical optical techniques to maintain quantum security. As a result, the transmission loss of the channel limits its achievable distance, and this has been a huge barrier towards building large-scale quantum-secure networks. Here we present an experimental QKD system that could tolerate a channel loss beyond 140 dB and obtain a secure distance of 833.8 km, setting a new record for fibre-based QKD. Furthermore, the optimized four-phase twin-field protocol and high-quality set-up make its secure key rate more than two orders of magnitude greater than previous records over similar distances. Our results mark a breakthrough towards building reliable and efficient terrestrial quantum-secure networks over a scale of 1,000 km.

Quantum key distribution (QKD) is the art of distributing secret bits based on the fundamental laws of physics, and it enables information-theoretic secure communication, regardless of the unlimited computational power of a potential eavesdropper[1]. Over the past three decades, QKD has attracted widespread attention and has matured to real-world deployment over optical-fibre networks[2,3]. However, the wider application of QKD is curtailed by channel loss, which limits increases in the key rate and the range of QKD[4–7]. In a QKD system, photons, as the carriers of quantum keys, are prepared at the single-photon level and will be mostly scattered and absorbed by the transmission channel. However, they cannot be amplified, causing the receiver to detect them with very low probability. For a direct fibre-based link from the transmitter to the receiver, the key rate decreases exponentially with the transmission distance and cannot surpass the fundamental rate–distance limit of $O(\eta)$, where η denotes the transmittance of the link[8,9].

Twin-field (TF) QKD builds a promising rate–distance relationship of $O(\sqrt{\eta})$ to overcome this limitation without quantum repeaters, and achieves a considerable secret key rate even over long distances[10]. Great efforts have been made to develop its theory[11–28] and to experimentally demonstrate its unique advantages[29–39]. References [11] and [12] first proved the general security of TF-QKD, then an experiment based on ref. [11] was realized over a 502-km ultra-low-loss (ULL) optical fibre[33]. By removing the global phase randomization and phase post-selection in the code mode, another variant called no phase post-selection (NPP) TF-QKD was proposed[14–16] and demonstrated in several experiments[30,32,35]. Because all detection events in the code mode were used for key generation, NPP TF-QKD could achieve relatively high key rates, for example, a 2-kbps asymptotic key rate over 300 km of fibre[30]. Meanwhile, sending-or-not-sending (SNS) TF-QKD generates key bits from the single-photon components and shows good tolerance against misalignments[13,18–20,24]. Recently, the SNS TF-QKD system has overcome the barriers of 100-dB channel loss and a 600-km fibre distance in the asymptotic scenario[36], and has even been tested over field fibre[37–39].

Figure 1 summarizes the recent long-distance fibre-based QKD experiments[6,7,33,34,36,38,39]. For fibre lengths beyond 450 km, all experiments revolved around TF-QKD protocols. These results not only illustrate the huge advantages of TF-QKD, but also clearly show the advances of our work. First, we provide a description of the four-phase TF-QKD protocol, which combines the merits of the original TF-QKD protocol and NPP TF-QKD to achieve a high key rate and long theoretical distance simultaneously in the finite-size scenario. In the experimental realization, we develop a high-speed and low-noise TF-QKD system and optimize its performance by reducing the effect of noises that originate from the source, the channel and the detector. Compared with previous experiments[33,34,36,38,39], one key advantage of our system is the lack of requirement for the optical amplifiers that are inserted in servo channels to increase the power of classic auxiliary signals. This advantage helps to remotely generate high-quality twin fields and reduces the complexity and cost, especially for further field and network applications.

Protocol

The four-phase TF-QKD protocol is summarized in the following five steps:

Step 1: Alice and Bob independently prepare a weak coherent state with intensity randomly chosen from μ, μ_0, μ_1 and μ_2 with probabilities p_0, p_{10}, p_{11} and p_2, respectively. Here μ corresponds

[1]CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, China. [2]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, China. [3]State Key Laboratory of Cryptology, Beijing, China. [4]Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai, China. [5]Jiangsu Hengtong Optical Fiber Technology Co. Ltd., Suzhou, China. [6]Scontel, Moscow, Russia. [7]These authors contributed equally: Shuang Wang, Zhen-Qiang Yin. ✉e-mail: hedeyong@mail.ustc.edu.cn; weich@ustc.edu.cn; zfhan@ustc.edu.cn

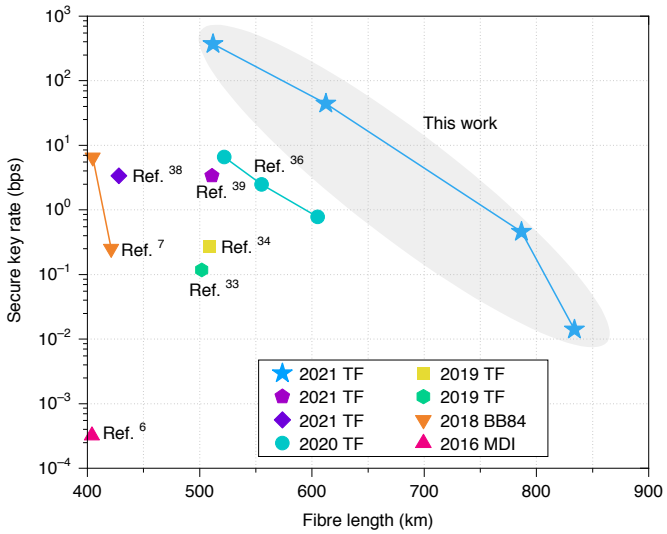

Fig. 1 | Summary of recent long-distance QKD experiments beyond 400 km. All demonstrations are provided with the fibre length, secure key rate per second (the data of ref. [34] is from ref. [3]), submitted year and implemented protocol.

to the code mode and the other intensities correspond to the decoy mode.

Step 2: In the code mode, Alice (Bob) picks a 'key' bit $a(b) \in \{0, 1\}$ and a 'basis' bit $a'(b') \in \{0, 1\}$ randomly, prepares weak coherent state $\left|e^{ia\pi+a'\frac{\pi}{2}}\sqrt{\mu}\right\rangle$ ($\left|e^{ib\pi+b'\frac{\pi}{2}}\sqrt{\mu}\right\rangle$). If the decoy mode is active, Alice (Bob) simply modulates a random phase from 0 to 2π on her (his) weak coherent state and prepares a mixture of Fock states with mean photon number μ_0, μ_1 or μ_2.

Step 3: Alice and Bob send their weak coherent states to an untrusted middle station Charlie, who may make the two incoming states interfere on a beamsplitter (BS). Two single-photon detectors (SPDs) are located at two distinct outputs of the BS, which are named D0 and D1, respectively. Charlie must publicly announce the clicks of D0 and D1. The first three steps will be repeated N_{tot} times.

Step 4: Among the N_{tot} trials, only when just one of D0 and D1 clicks are they retained for further processing. Alice and Bob broadcast the intensities for each retained trial, and 'basis' bit a' and b' if relevant. For each retained trial satisfying $a' = b'$, Alice and Bob record their key bits a and b sequentially to form the sifted key string. Note that if the click of D1 was announced, Bob may flip his corresponding key bit b. We denote the length of the sifted key string as K_0. Let us also denote the numbers of retained trials in which they both prepare the same intensities μ_0, μ_1 or μ_2 as K_{10}, K_{11} and K_2, respectively, and $K_1 \equiv K_{10} + K_{11}$.

Step 5: According to K_0, K_1 and K_2, Alice and Bob can share a secret key string with length G from their sifted key string with a failure probability no larger than ϵ_{sec} (see Methods for details).

There are some potential advantages of our protocol. In the code mode, the NPP TF-QKD protocol[14–16] only modulates two phases by setting $a' = b' = 0$ for all trials, whereas the original TF-QKD protocol[10] modulates phases continuously. Similar to phase-coding measurement-device-independent (MDI) QKD[40,41], our protocol modulates four phases in the code mode and thus can be seen as an intermediate protocol between NPP TF-QKD and the original TF-QKD protocol. The additional two phases lead to a longer secure distance compared with the two-phase NPP TF-QKD protocol[26]. On the other hand, the four-phase protocol simplifies the phase post-selection step in the original TF-QKD protocol and leads to a relatively higher key rate, especially considering the finite-size effect. In this article we also developed a finite-key analysis for the four-phase TF-QKD protocol (see Methods and Supplementary Information for details), which was employed in the experimental set-up.

Set-up

TF-QKD requires that the optical pulses from two remote users (Alice and Bob) stably interfere in the intermediate station (Charlie). Except where they have the same state of polarization, the wavelength difference and phase difference between Alice's and Bob's sources should be relatively stable over time. Here, both Alice's and Bob's sources are locked with a free-running common laser to reconcile their central wavelength values, and a time division multiplexing strategy is adopted to actively compensate the fast phase drift introduced by the fibre channels. These fibre channels include the servo channel that is used to transmit the light from the common laser to Alice (Bob) and the quantum channel that is used to transmit the time-multiplexed signal (divided into a reference part and a quantum part) from Alice (Bob) to Charlie.

The experimental set-up that meets the requirements of TF-QKD is shown in Fig. 2. The common laser is free-running with a central wavelength of 1,550.12 nm and a linewidth of 0.1 kHz (X15 laser, NKT Photonics Inc.), and its continuous-wave (c.w.) light is split into two parts, which are sent to Alice and Bob through corresponding servo channels, respectively. The c.w. light beam of Alice's (Bob's) local laser is also split into two parts: one part interferes with the received light from the common laser to lock her (his) laser's central wavelength (source in Fig. 2), and the other part is directly passed through the chopper, encoder and regulator before entering the quantum channel.

In the source part, the weak light from the common laser is first stabilized to a fixed state of polarization by a polarization compensation module (PCM), then interferes with the light from Alice's (Bob's) local laser and is eventually detected by two positive-intrinsic-negative (PIN) detectors. Based on the detected phase-sensitive error signal, the homodyne optical phase-locked loop (OPLL) makes the phase difference between the received light from the common laser and the local light stable, makes their wavelength difference substantially zero, and the negative-feedback phase modulator (PM) further reduces the residual phase noise. The local laser is composed of a 14-pin butterfly laser diode (PLANEX, RIO Inc.) with a linewidth of 2 kHz and a homemade driving circuit with a temperature control accuracy of 0.001 °C. Error signals for both phase-locking and negative feedback are from the homodyne detectors.

The chopper consists of an intensity modulator (IM) and a pair of acousto-optic modulators (AOMs). IM_1 modulates the locked c.w. light into a pulse train at 4 GHz with width of 60 ps. AOM+ and AOM− chop the pulse train into the time-multiplexed reference part and quantum part, and the duration time of either part will change depending on the rate of the phase drift. The reference part is comparatively bright and would provide error signals for the compensation of phase drift and an indicator for the compensated result. Here, AOM+ and AOM− denote the positive and negative 80-MHz frequency shift AOM, respectively, and both of them are driven by the same signal. This pair of AOMs exhibit a stable and high extinction ratio between the reference and quantum parts, and a rise time of 120 ns.

The encoder is composed of three IMs and two PMs and only works on the quantum part. As required by the protocol, the encoder randomly switches between code and decoy modes. In the code mode, the three IMs only need to create the state with μ intensity, PM_1 and PM_2 independently modulate phases $\{0, \pi\}$ and $\{0, \pi/2\}$ according to their corresponding 'key' and 'basis' bit values, respectively. In the decoy mode, IM_2, IM_3 and IM_4 randomly create the states with the other three intensities μ_0, μ_1 and μ_2, PM_1 and PM_2 add random phase from 0 to 2π onto each pulse.

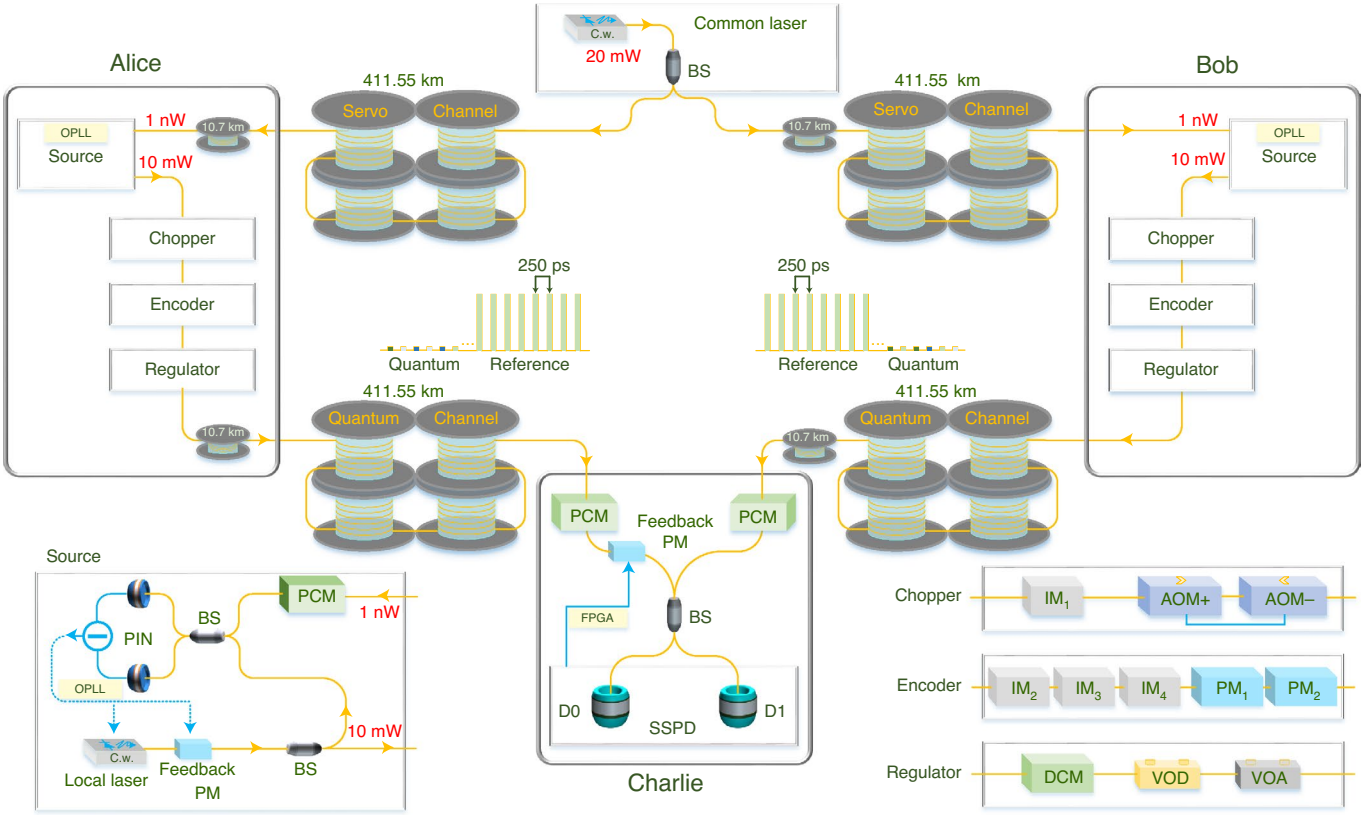

Fig. 2 | Optical layout of the TF-QKD system. To remotely generate the twin fields between Alice and Bob, both of them lock their local laser sources to a free-running common laser via a homodyne OPLL. The common light beam is transmitted though the servo channel. Alice's and Bob's twin fields then enter 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.

The regulator is employed to achieve high interference visibility by regulating certain parameters and is made up of a dispersion compensation module (DCM), a variable optical delay (VOD) and a variable optical attenuator (VOA). A DCM based on fibre-Bragg-grating technology pre-compensates the distortion introduced by the chromatic dispersion of the quantum channel. VOD adjusts the time delay of Alice's (Bob's) optical pulses to overlap as much as possible on Charlie's BS. VOA attenuates the global intensity of output pulses to meet the security requirements.

The quantum channels are composed of spools of G.654.E ULL optical fibre with a typical attenuation of 0.158 dB km^{-1} and a chromatic dispersion of 20 ps nm^{-1} km^{-1} at 1,550 nm (ULL-G.654.E, Jiangsu Hengtong Optical Fiber Technology Co.). The ULL fibre was made from a silica-glass preform whose core was doped with alkalis by vapour axial deposition. The attenuation caused by Rayleigh scattering was reduced by optimizing the viscosity mismatch between the core and the cladding[42,43].

After passing through corresponding quantum channels and PCMs, Alice's and Bob's encoded twin fields interfere on Charlie's BS, and are finally detected by two superconducting single-photon detectors (SSPDs) based on superconducting nanowires. These two SSPDs (D0 and D1) are fabricated with NbN thin films cooled at 2.1 K (ref. [44]) and feature an average detection efficiency of 57.6% and a dark count rate (DCR) of less than 0.13 Hz (refs. [45,46]). One feedback PM (with ~1.7-dB insertion loss) is added in the path from Alice to Charlie's BS to compensate the fast relative phase drift introduced by fibre channels (details are provided in the Methods). Because there is no feedback PM in the path from Bob to Charlie's BS, one fibre spool with length of 10.7 km is added in this path to balance the loss. Accordingly, one fibre spool with the same length is added in the servo channel from Charlie to Bob, and two fibre spools are added in Alice's site to balance the time delay.

Results

To reduce the noise from the source and the servo channel we developed a highly sensitive and repeater-like laser source. The local sources belonging to Alice and Bob receive the weak light (attenuated by servo channels to ~1 nW) from the common laser, then are locked with the weak light to copy its phase and finally generate twin fields with 10-mW output power, just like repeaters in intermediate nodes. If optical amplifiers were added into the servo channel[33,34,36,38,39] to increase the power of the received weak light, they would not only introduce extra noise, but also complexity and cost. One favourable approach is to improve the sensitivity of the repeater-like laser source, which can still work with very weak input power (~1 nW in our experiment). By taking advantage of homodyne detection, the source could work stably even with input power as low as 0.2 nW. We first tested the source noise without fibre channels (Supplementary Information). With 1-nW input power, two sources (Alice and Bob) were locked to a common laser, and their corresponding output beams interfered on a polarization-maintaining BS. The corresponding interference outcomes were recorded over 400 s with an acquisition time of 200 µs (Supplementary Information). By avoiding the noise of an electronic phase detector and electronic local oscillator, which are widely employed in heterodyne OPLL, the source based on homodyne OPLL with 80-kHz loop bandwidth shows a reasonable interference outcome. The interference outcomes of two phase-locked lasers were similar to the interference pattern of two light beams from a single laser, and the stable duration of all interference outcomes was on the order of a second (Supplementary

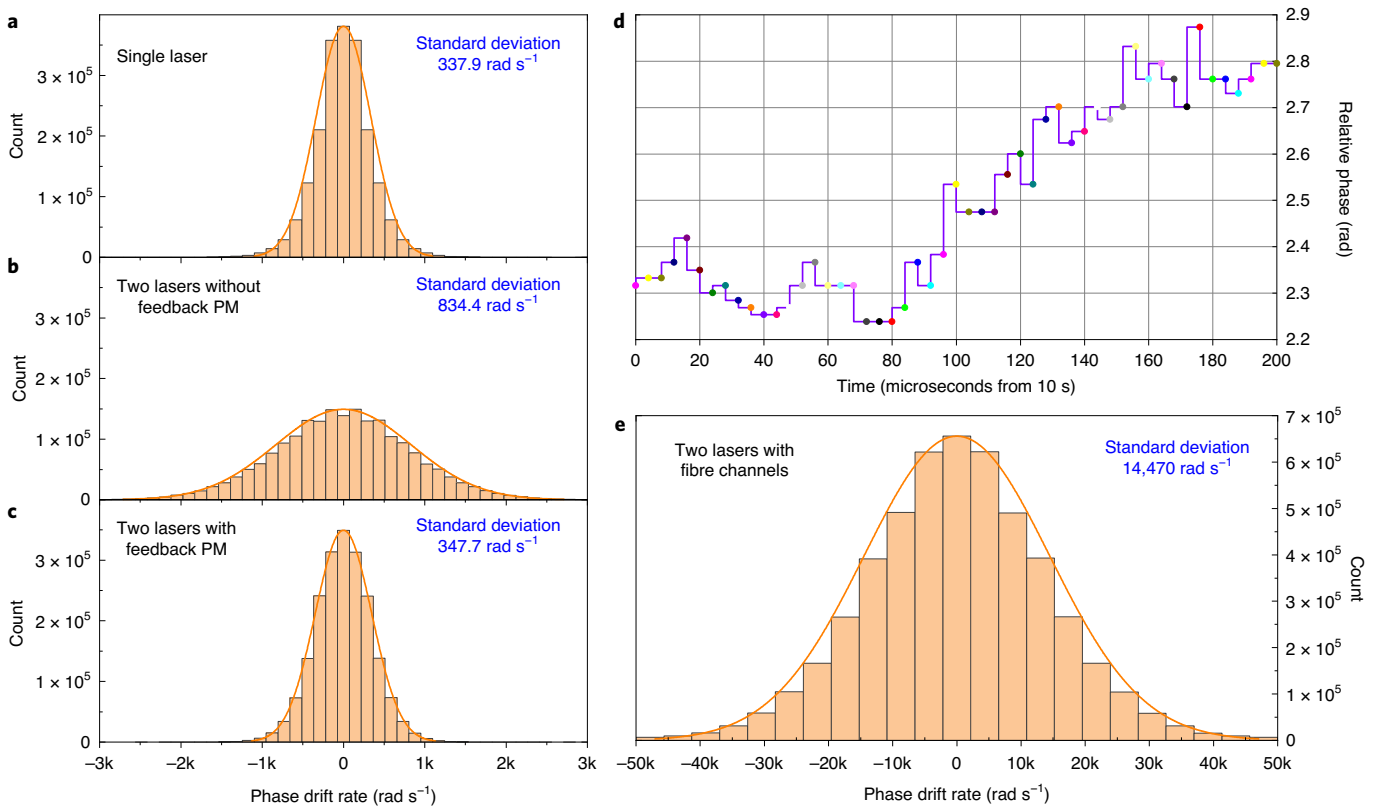

Fig. 3 | Results of source noise and phase drift with fibre channels. a–c, Comparison of the source noise of three sources versus the phase drift rate of two light beams from a single laser (**a**), two phase-locked lasers without feedback PM in the source (**b**) and two phase-locked lasers with feedback 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'.

Information). The standard deviation of the phase drift rate (Fig. 3a–c) is used to characterize the source noise. The noise level of this source is still ~2.5 times that of a single laser (Fig. 3b versus Fig. 3a). Furthermore, a feedback PM was added in the source to reduce the residual phase noise, leading to a noise level almost identical to that of a single laser (Fig. 3c versus Fig. 3a). Without fibre channels, the noise of interference mainly comes from the source. Meanwhile, after inserting long-distance servo fibre channels, the repeater-like sources were sensitive enough without using optical amplifiers. Accordingly, twin fields could be remotely generated with very high quality. Now, only the phase drift accumulating along the servo channels needs to be considered.

To characterize the phase drift of the whole system, we measured the interference outcome over 1,689 km of fibre (including servo and quantum channels). The measurement set-up could be considered as a large Mach–Zehnder interferometer, with arms consisting of servo and quantum channels connected together by a corresponding repeater-like phase-locked source (Supplementary Information). The interference outcome was recorded by a supersensitive avalanche photodiode-based detector and an oscilloscope with an acquisition time of 4 μs over 20s. Even though the noise of the sources was minimized, the fast phase drift accumulated along the servo channels and quantum channels made the interference fringe indiscernible on the timescale of a second. Taking data from 10 s to 10.0002 s, we calculated the relative phase (Fig. 3d), and the maximum drifted phase between two adjacent points was up to 0.172 rad. Based on 5×10^6 recorded points over 20 s, the relative phase drift rate was quantified by its standard deviation, with a value of 14,470 rad s^{-1} (Fig. 3e).

Based on the measured value of relative phase drift rate, we chose 20 μs as the frame period, which was divided into reference and quantum parts by Alice's and Bob's choppers. For the scenario with 833.80-km quantum channels, the stable durations of the reference and quantum parts were 10.4 μs and 8 μs, respectively (details are provided in the Methods). With the participation of Charlie's feedback PM, a 9-μs duration time of the reference part was used to estimate the value of the relative drifted phase after quadrature interference, and the corresponding calculated error signal was loaded immediately, within 0.6 μs. After 0.8-μs in-phase interference of the bright reference pulses, the compensated result was indicated by the visibility of the interference. Finally, the 8-μs in-phase interference quantum part was employed to implement the four-phase TF-QKD protocol.

The interference photons were detected by two optimized SSPDs with relatively high detection efficiency and low DCR. The SSPD was first manufactured with a high level of saturation of intrinsic quantum efficiency by changing the thickness of the superconducting NbN film, and was then coupled to a cooled bandpass filter (passband of ~10 nm @1,550 nm) with bent pigtailed single-mode optical fibre[45,46]. Both the bent optical fibre (with a bending diameter of 20 mm) and passband filter were placed in the same cryostat as the detectors, but at the first stage of cooling at 40 K to reduce the noise introduced by background radiation. With an efficiency of 57.6%, we achieved an average DCR of 0.1274 Hz per detector and a time jitter of less than 50 ps. We set a window of 120 ps (by post-processing the detection events recorded by a time-to-digit converter) to further reduce the influence of DCR, and the efficiency of the window was more than 83%. Thus, the average DCR of one detector of the TF system was 1.529×10^{-11} per window.

We also optimized the system parameters to achieve low multipath interference (MPI) noise in the quantum channels. with relatively high interference visibility. As an essential part of a TF-QKD system, more and stronger reference pulses will lead to high visibility of interference. Meanwhile, MPI noise caused by multiple discrete reflections of strong reference pulses will interfere with the quantum pulses and create additional errors. The sources of forward MPI noise include double Rayleigh backscattering, splicing and connecting reflections combined with single Rayleigh backscattering, and double reflections[47]. The G.654.E ULL fibre used here has a low Rayleigh backscattering coefficient of $3.21\times10^{-5}\,km^{-1}$, and all spools of fibre were spliced together. The number of reference pulses in each estimation region (9 μs) was increased to 36,000 for the 833.80-km transmission distance. With this distance we measured the visibility of in-phase interference in the reference part and MPI noise in the quantum part over different intensities of reference pulses. As shown in Fig. 4, the MPI noise was quantified in units of DCR and increased approximately linearly with the intensity of the reference pulses. The visibility of the reference's in-phase interference first increased rapidly and then gradually when the intensity of the reference pulses varied from 38.4 to 230.4 photons per pulse. We set the intensity of the reference pulses to 115.2 photons per pulse for the scenario with 833.80-km quantum channels, and the corresponding visibility and MPI noise were 96.11% and 1.03 times the DCR, respectively.

To obtain a positive key rate over an ultra-long distance in the finite-key scenario, the stability of the TF system plays an important role if we want to collect enough counts of quantum pulses. As well as fast compensation of phase drift, we added real-time modules to compensate the drifts of polarization and time delay of the fibre channels. The entire QKD system could operate continuously for several weeks. In the ULL fibre scenario, the total number of transmitted quantum signals was 3.2×10^{14}, and the corresponding runtime was 2×10^{5} s for a fibre length of 833.80 km. Figure 5 shows the visibility of the reference's in-phase interference and the quantum bit error rate (QBER) of the quantum pulses with respect to time, over 833.80 km of fibre channel (for other distances see Supplementary Information). The visibility distribution was concentrated around 96.13% with a standard deviation of 0.18%, and the corresponding average QBER was 3.79% with a standard deviation of 2.59%.

Figure 6 presents the results for the secure key rate (SKR) and QBER of the TF-QKD system (for details of the results see Supplementary Information). The experiments were performed with channel losses between 69.72 dB and 140.10 dB in a VOA scenario (cyan and magenta triangles, Fig. 6) and with fibre lengths between 511.86 km and 833.80 km in the ULL fibre scenario (blue and red stars, Fig. 6), respectively. In addition to the ULL fibre scenario, the VOA scenario, in which the servo and quantum channels were replaced by VOAs (~1–80-dB range), was tested to evaluate the performance limit of TF-QKD. For each case we chose the optimized intensities and probabilities to maximize the SKR per quantum pulse. All experimental SKRs exceeded the absolute SKR bound (black line, Fig. 6), which is calculated as $-\log_2(1-\eta)$ with the detection efficiency of Charlie's apparatus being $\eta_d=100\%$ (ref. [9]). In the VOA scenario, the SKR was 7.53×10^{-11} bits per quantum pulse, 1,091 times as much as the absolute bound (6.90×10^{-14}), when the channel loss was 133.20 dB. Even in the ULL fibre scenario, the SKR reached 573 times the absolute bound when the fibre length was 786.67 km. The maximum channel loss over which we could obtain a positive SKR was up to 140.10 dB, which is equivalent to almost 1,000 km of ULL optical fibre with a loss coefficient of $0.1419\,dB\,km^{-1}$ (ref. [42]). The longest fibre length over which we could keep a relatively high interference visibility (96.13%) and achieve a positive key rate was 833.80 km.

We also changed the duration of the quantum part to maximize the SKR per second. With a frame period of 20 μs, the total duration of the estimation region (in the reference part) and quantum part was kept at 17 μs. In the VOA scenario, the relative phase drift was very slow and just a 2-μs estimation region was enough to obtain an interference visibility of ~98.77–98.91%. There was 15 μs left for the stable quantum part, so the equivalent rate of quantum pulses was 3 GHz. An SKR of 2.64 kbps was obtained with 69.72-dB channel loss. In the ULL fibre scenario, the duration of the quantum part was 8 μs for a fibre length of 833.80 km (1.6-GHz equivalent rate) and 10 μs for the other three fibre lengths (2-GHz equivalent rate). For 511.86-km and 612.42-km transmission distances, the SKRs were 368.9 bps and 44.05 bps, respectively, substantially (~50–1,000 times) exceeding previous results for similar distances. Even at a fibre length of 833.80 km, an SKR of 0.014 bps was achieved in the finite-size regime.

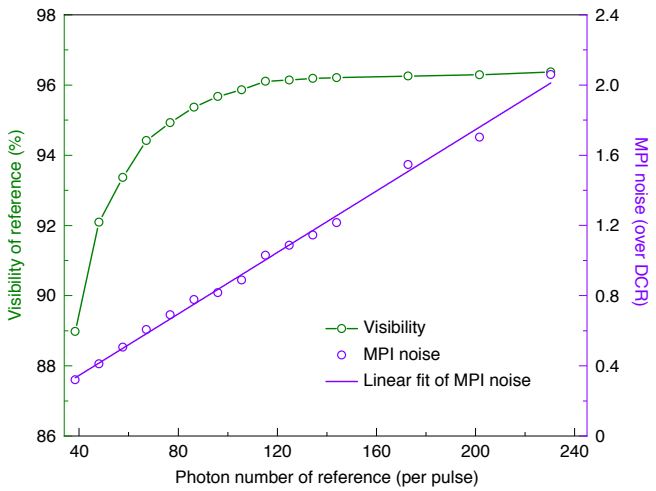

Fig. 4 | Interference visibility and MPI noise versus the intensity of the reference pulses. For the scenario with 833.80-km quantum channels, the visibility of the in-phase interference in the reference part and MPI noise in the quantum part were measured simultaneously. MPI noise is quantified in units of DCR.

Discussion

One of the main goals of our experiment was to attempt to obtain the maximum distance for a fibre-based QKD system. Here we have shown that our set-up can tolerate a channel loss beyond 140 dB and obtain a secure transmission distance of 833.80 km. These results are largely due to the low-noise properties of the whole set-up, apart from the protocol. We have minimized the noises that originate from the source, the channel and the detector.

The noise reduction of the source is directly related to controlling the phase evolution between twin fields, which can be written as[10]

$$\delta\varphi=\frac{2\pi}{c}(\Delta\nu\times(nL)+2\nu\times\Delta(nL)),\qquad(1)$$

where c is the speed of light in vacuum, n is the refractive index of the fibre and L is the fibre length of the quantum channel. The first term would be zero if both twin fields were from the same source ($\Delta\nu=0$). Both locking modules and optical amplifiers were required to remotely generate twin fields in previous works[33,34,36,38,39], and both would inevitably introduce noise into the source. Our highly sensitive and repeater-like laser source not only effectively suppresses the noise of the locking module, but also avoids the extra noise that might be contributed by optical amplifiers. With only 1 nW of input power, both Alice's and Bob's sources were locked to

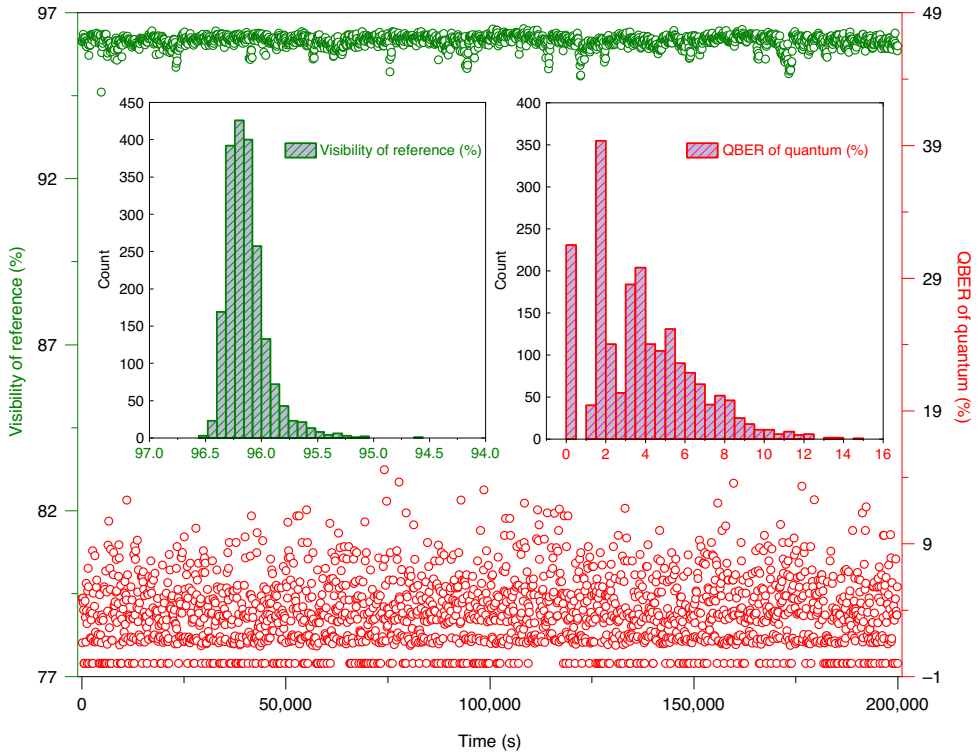

Fig. 5 | System stability over a distance of 833.80 km of quantum channel. The olive and red open circles respectively represent the in-phase interference visibilities of Alice's and Bob's reference parts and the QBER of their quantum parts. Each circle corresponds to data gathered in 100 s. The insets show the corresponding distributions of interference visibility and QBER.

a common laser, and the interference pattern of the two sources was almost identical to that of two light beams from the same laser. Thus the noises of the sources are close to the limit, and the first term of the phase evolution is negligible.

Although twin fields could be prepared almost perfectly, the TF-QKD system came across a quandary: as the transmission distance increased both the phase drift rate and MPI noise increased, but the yields of the reference and quantum pulses decreased. On the one hand, the phase drift becomes quite intense in a long fibre channel, according to the second term of equation (1), in particular high-speed drift due to the photoelastic effect of environmental vibrations and large-amplitude drift due to variation in the ambient temperature, indicating that an effective compensation of the increased phase drift requires more counts from the reference pulses. On the other hand, because MPI noise introduced by reference pulses accumulates along the quantum fibre channel and increases linearly with the intensity of the reference pulses, the intensity of the reference pulses should be comparatively weaker to obtain a high quantum signal-to-noise ratio. To address this dilemma, we carefully chose three factors that determine the QBER of quantum pulses: intensity, repetition rate and the duration of the reference pulses. In our set-up, the repetition rate was up to 4 GHz and the duration of the estimation region of the reference pulses was increased to 9 μs in each 20-μs frame period for the scenario with 833.80-km quantum channels. Even though the phase drift has been well compensated, the QBER of the quantum pulses was constrained by the MPI noise of the quantum fibre channel and the DCR of the detectors. By testing the interference visibility and MPI noise in relation to the intensity of the reference pulses, we set the intensity of the reference pulses to 115.2 photons per pulse to achieve a relatively high visibility (96.11%) with comparatively low MPI noise (1.03 times the DCR). Furthermore, we set a measurement window of 120 ps to limit the substantial contribution of MPI noise and DCR to the QBER.

An interesting question is whether we can further expand the transmission distance of QKD without a repeater. We have shown that the maximum channel loss of our system is beyond 140 dB. The limitations do not come from the source part, but from the detection part, because our highly sensitive sources are able to support the high-quality generation of twin fields, even beyond 150 dB in the repeater-like scenario. The DCR of the SSPD and the time jitter of the detection part could be improved to achieve a higher signal-to-noise ratio. The passband of the optical filter in the SSPD is 10 nm; if the filter were replaced by one with a 0.8-nm passband, the DCR of the SSPD would be notably reduced. Once the time jitter of the detection part is modified, we would increase the repetition rate to achieve more detections in unit time and narrow the measurement window to remove more noise. These improvements would increase the maximum channel loss up to 160 dB or more and make it possible for a 1,000-km fibre-based QKD. However, in the fibre scenario, we have to deal with the faster phase drift of longer fibre channels. Having longer fibre channels means fewer detection counts and more introduced noise from the reference pulses, which makes it impossible to continue compensation of the faster phase drift with the time-multiplexed strategy. To overcome this limitation, one choice might be to implement the SNS TF-QKD protocol[13], which has good tolerance against misalignment. A better strategy to compensate faster phase drift would be one based on wavelength division multiplexing[36], in which a bright signal at another wavelength could help the compensation system reduce the phase drift by three orders of magnitude, then fewer and weaker reference pulses would be able to compensate the residual phase drift.

Conclusion

In summary, we have demonstrated that fibre-based QKD could be realized with over 140 dB of channel loss and a distance of 833.8 km.

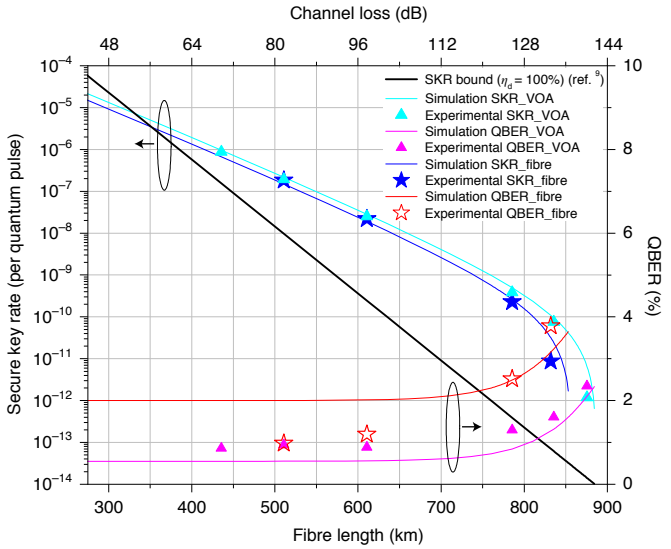

Fig. 6 | Simulation and experimental results for the SKR and QBER. In VOA and fibre scenarios, the total numbers of transmitted quantum signals were 3×10^{14} and 3.2×10^{14}, respectively.

After generalizing the four-phase TF-QKD protocol to finite-key scenarios, we have developed a corresponding high-speed system without using optical amplifiers, and optimized its performance by reducing the effect of noise originating from the source, the channel and the detector. Our set-up not only sets records for tolerant channel loss and the transmission distance of fibre-based QKD, but also achieves SKRs that clearly outperform previous TF-QKD experiments at similar distances. In addition, not using optical amplifiers in the TF-QKD helps to reduces the complexity and cost, especially in field and network applications. Hence our work indicates the great potential of TF-QKD for wider applications. We believe that this study provides a conceivable way to further extend the transmission distance and pave an avenue towards wider-range QKD networks.

Online content

Any methods, additional references, Nature Research reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41566-021-00928-2.

Received: 20 May 2021; Accepted: 8 November 2021;
Published online: 17 January 2022

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing* 175–179 (IEEE, 1984).
2. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
3. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
4. Wang, S. et al. 2-GHz clock quantum key distribution over 260 km of standard telecom fiber. *Opt. Lett.* **37**, 1008–1010 (2012).
5. Korzh, B. et al. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photon.* **9**, 163–168 (2015).
6. Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404-km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
7. Boaron, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).
8. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
9. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
10. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
11. Ma, X., Zeng, P. & Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **8**, 031043 (2018).
12. Tamaki, K., Lo, H.-K., Wang, W. & Lucamarini, M. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. Preprint at https://arxiv.org/abs/1805.05511 (2018).
13. Wang, X.-B., Yu, Z.-W. & Hu, X.-L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **98**, 062323 (2018).
14. Lin, J. & Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **98**, 042332 (2018).
15. Cui, C. et al. Twin-field quantum key distribution without phase postselection. *Phys. Rev. Appl.* **11**, 034053 (2019).
16. Curty, M., Azuma, K. & Lo, H.-K. Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Inf.* **5**, 64 (2019).
17. Grasselli, F. & Curty, M. Practical decoy-state method for twin-field quantum key distribution. *N. J. Phys.* **21**, 073001 (2019).
18. Jiang, C., Yu, Z.-W., Hu, X.-L. & Wang, X.-B. Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses. *Phys. Rev. Appl.* **12**, 024061 (2019).
19. Yu, Z.-W., Hu, X.-L., Jiang, C., Xu, H. & Wang, X.-B. Sending-or-not-sending twin-field quantum key distribution in practice. *Sci. Rep.* **9**, 3080 (2019).
20. Hu, X.-L., Jiang, C., Yu, Z.-W. & Wang, X.-B. Sending-or-not-sending twin-field protocol for quantum key distribution with asymmetric source parameters. *Phys. Rev. A* **100**, 062337 (2019).
21. Zhou, X.-Y., Zhang, C.-H., Zhang, C.-M. & Wang, Q. Asymmetric sending or not sending twin-field quantum key distribution in practice. *Phys. Rev. A* **99**, 062316 (2019).
22. Maeda, K., Sasaki, T. & Koashi, M. Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate–distance limit. *Nat. Commun.* **10**, 3140 (2019).
23. Lu, F.-Y. et al. Improving the performance of twin-field quantum key distribution. *Phys. Rev. A* **100**, 022306 (2019).
24. Xu, H., Yu, Z.-W., Jiang, C., Hu, X.-L. & Wang, X.-B. Sending-or-not-sending twin-field quantum key distribution: breaking the direct transmission key rate. *Phys. Rev. A* **101**, 042330 (2020).
25. Wang, W. & Lo, H.-K. Simple method for asymmetric twin-field quantum key distribution. *N. J. Phys.* **22**, 013020 (2020).
26. Wang, R. et al. Optimized protocol for twin-field quantum key distribution. *Commun. Phys.* **3**, 149 (2020).
27. Zeng, P., Wu, W. & Ma, X. Symmetry-protected privacy: beating the rate-distance linear bound over a noisy channel. *Phys. Rev. Appl.* **13**, 064013 (2020).
28. Currás-Lorenzo, G. et al. Tight finite-key security for twin-field quantum key distribution. *npj Quantum Inf.* **7**, 22 (2021).
29. Minder, M. et al. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photon.* **13**, 334–338 (2019).
30. Wang, S. et al. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. *Phys. Rev. X* **9**, 021046 (2019).
31. Liu, Y. et al. Experimental twin-field quantum key distribution through sending or not sending. *Phys. Rev. Lett.* **123**, 100505 (2019).
32. Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H.-K. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Phys. Rev. Lett.* **123**, 100506 (2019).
33. Fang, X.-T. et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photon.* **14**, 422–425 (2020).
34. Chen, J.-P. et al. Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **124**, 070501 (2020).
35. Zhong, X., Wang, W., Qian, L. & Lo, H.-K. Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses. *npj Quantum Inf.* **7**, 8 (2021).
36. Pittaluga, M. et al. 600-km repeater-like quantum communications with dual-band stabilisation. *Nat. Photon.* **15**, 530–535 (2021).
37. Clivati, C. et al. Coherent phase transfer for real-world twin-field quantum key distribution. Preprint at https://arxiv.org/abs/2012.15199 (2020).
38. Liu, H. et al. Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. *Phys. Rev. Lett.* **126**, 250502 (2021).
39. Chen, J.-P. et al. Twin-field quantum key distribution over 511-km optical fiber linking two distant metropolitans. *Nat. Photon.* **15**, 570–575 (2021).
40. Ma, X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 062319 (2012).
41. Tamaki, K., Lo, H.-K., Fung, C.-H. F. & Qi, B. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Phys. Rev. A* **85**, 042307 (2012).

42. Tamura, Y. et al. The first 0.14-dB/km loss optical fiber and its impact on submarine transmission. *J. Light. Technol.* **36**, 44–49 (2018).
43. Xiao, H., Lao, X.-G., Shen, Z.-Q. & Zhai, Y.-X. Research on manufacturing process of ultra-low loss optical fiber. *Modern Transmission* **2019**, 73–76 (2019).
44. Goltsman, G. et al. Picosecond superconducting single-photon optical detector. *Appl. Phys. Lett.* **79**, 705–707 (2001).
45. Smirnov, K., Vachtomin, Y., Divochiy, A., Antipov, A. & Goltsman, G. Dependence of dark count rates in superconducting single photon detectors on the filtering effect of standard single mode optical fibers. *Appl. Phys. Express* **8**, 022501 (2015).
46. Smirnov, K. et al. NbN single-photon detectors with saturated dependence of quantum efficiency. *Supercond. Sci. Technol.* **31**, 035011 (2018).
47. Woodward, S. & Darcie, T. A method for reducing multipath interference noise. *IEEE Photon. Technol. Lett.* **6**, 450–452 (1994).

Methods

Finite-key analysis for four-phase protocol. Let us consider an equivalent entanglement-based protocol, the flow of which is the same as for the actual four-phase protocol except the code mode in step 2. Specifically, in the code mode of step 2, Alice equivalently prepares $|\psi\rangle = \left(|0\rangle_{a'}|0\rangle_a|\sqrt{\mu}\rangle_A + |0\rangle_{a'}|1\rangle_a|-\sqrt{\mu}\rangle_A + |1\rangle_{a'}|0\rangle_a|i\sqrt{\mu}\rangle_A + |1\rangle_{a'}|1\rangle_a|-i\sqrt{\mu}\rangle_A\right)/2$ instead of directly preparing a weak coherent state, and Bob prepares his quantum state $|\phi\rangle = \left(|0\rangle_{b'}|0\rangle_b|\sqrt{\mu}\rangle_B + |0\rangle_{b'}|1\rangle_b|-\sqrt{\mu}\rangle_B + |1\rangle_{b'}|0\rangle_b|i\sqrt{\mu}\rangle_B + |1\rangle_{b'}|1\rangle_b|-i\sqrt{\mu}\rangle_B\right)/2$ analogously. Then Alice and Bob retain a, a', b and b' as their local qubits, send travelling states A and B to Charlie. After Charlie announces the clicks of D0 and D1, Alice and Bob measure their local qubits with the $Z = \{|0\rangle, |1\rangle\}$ basis to obtain sifted key bits satisfying $a' = b'$. Obviously, this entanglement-based protocol generates the same key bit as the actual four-phase protocol in the view of Alice and Bob. Moreover, it is also indistinguishable from the actual four-phase protocol in the view of an eavesdropper. Therefore, we can use the finite-key analysis for this entanglement-based protocol rather than the actual four-phase protocol.

To evaluate the secrecy of the key bits, one can resort to complementarity[48], that is, estimate a so-called phase error rate $e_{\rm ph}$, the error rate if Alice and Bob hypothetically measure a and b with the $X = \{|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$ basis instead of the Z basis. Evidently, if Alice and Bob observe $a' = b'$ and $a = b$, they actually prepare a non-classical quantum state $\rho_{\rm even}$ with probability $p_{\rm even}$ (the detailed forms of $\rho_{\rm even}$ and $p_{\rm even}$ are provided in Supplementary Section A). In this sense, if Alice and Bob are able to prepare $\rho_{\rm even}$, $e_{\rm ph}$ can be estimated by observing its yield. Unfortunately, the preparation of $\rho_{\rm even}$ is a challenging task. Indeed, what Alice and Bob are able to do in the actual protocol is to prepare weak coherent states $|\pm\sqrt{\mu}\rangle$ or $|\pm i\sqrt{\mu}\rangle$ in code mode with probability $p_0^2/2$, and mixed Fock states $\tau(\mu_0) = {\rm e}^{-\mu}\sum_{n=0}^{\infty}\mu_0^n|n\rangle\langle n|/n!$, $\tau(\mu_1)$ or $\tau(\mu_2)$ in decoy mode with probabilities p_{10}^2, p_{11}^2 and p_2^2, respectively.

To overcome this difficulty, we further develop an operator dominance inequality[22] applicable to this protocol. This inequality reads $p_{10}^2\tau(\mu_0)\otimes\tau(\mu_0) + p_{11}^2\tau(\mu_1)\otimes\tau(\mu_1) - \Gamma\tau(\mu_2)\otimes\tau(\mu_2) \geq \Lambda\rho_{\rm even}$, which holds for appropriate positive values of Γ and Λ. Leaving its proof in Supplementary Section A, we focus on the physics behind this inequality. Indeed, this inequality implies that the density matrix prepared in the decoy mode with intensities μ_0 and μ_1 can be interpreted as a mixture of $\rho_{\rm even}$, the decoy states with intensity μ_2 and some 'junk' state. Because any physical measurement cannot distinguish quantum states with the same density matrices, the yield of $p_{10}^2\tau(\mu_0)\otimes\tau(\mu_0) + p_{11}^2\tau(\mu_1)\otimes\tau(\mu_1)$ must upper bound the yield of $\Gamma\tau(\mu_2)\otimes\tau(\mu_2) + \Lambda\rho_{\rm even}$. As a result, $K_1 \equiv K_{10} + K_{11} \geq \Gamma K_2/p_2^2 + K_{\rm ph}/(p_0^2 p_{\rm even}^2)$ must hold asymptotically, where $K_{\rm ph}$ is the number of phase errors among K_0 bits of sifted keys. In the finite-key region, $K_{\rm ph}$ can be upper-bounded by a function $f(K_1, K_2)$ with failure probability ϵ due to statistical fluctuations. In detail, similar to the Chernoff bound used in ref. [22], we can estimate the upper bound of $e_{\rm ph}$ by

$$\begin{aligned} e_{\rm ph} &\leq \tfrac{f(K_1,K_2)}{K_0} \\ &= \tfrac{p_0^2 p_{\rm even}}{2K_0\Lambda}\left(K_1 - \tfrac{\Gamma}{p_2^2}K_2 + \nu(K_1,K_2)\sqrt{-\log\tfrac{\epsilon}{2}}\right), \end{aligned} \tag{2}$$

where

$$\begin{aligned} &\nu(K_1,K_2) \\ &\simeq \left\{\tfrac{\sqrt{2\Gamma(p_2^2+\Gamma)}}{p_2^2}\sqrt{K_2} + \sqrt{2\left(1+\tfrac{2\Lambda}{p_0^2 p_{\rm even}}\right)}\sqrt{K_1 - \tfrac{\Gamma}{p_2^2}K_2}\right\}. \end{aligned}$$

Now we are ready to calculate the final key length G. Let us define $H_{\rm EC} = 1.1K_0 h(e_{\rm bit})$ as the cost of error correction, where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$, and ζ' bits are consumed to ensure that the failure probability of error verification is up to $2^{-\zeta'}$. According to complementarity[48] and the composable security definition[49], the final key length $G = K_0(1 - h(e_{\rm ph})) - H_{\rm EC} - \zeta - \zeta'$. Meanwhile, the final key is $\sqrt{2}\sqrt{\epsilon + 2^{-\zeta}}$-secret and $2^{-\zeta'}$-identical, so the final security parameter is $\epsilon_{\rm sec} = \sqrt{2}\sqrt{\epsilon + 2^{-\zeta}} + 2^{-\zeta'}$. Note that, in this work, we fix $\epsilon_{\rm sec} = 2^{-31}$ by assuming $\epsilon = 2^{-66}$, $\zeta = 66$ and $\zeta' = 32$.

Simulation model. In the VOA scenario, the detection efficiency of Charlie's apparatus is $\eta_{\rm d} = 29.3\%$, the background noise (including the dark count rate) of one detector is $p_{\rm d} = 2.3\times10^{-11}$ per window, and the misalignment error rate is $e_{\rm m} = 0.55\%$. In the ULL fibre scenario, the detection efficiency of Charlie's apparatus is $\eta_{\rm d} = 28\%$, the background noise of one detector is $p_{\rm d} = 3\times10^{-11}$ per window, the misalignment error rate is $e_{\rm m} = 2\%$, and the channel transmittance from Alice (Bob) to Charlie is $\eta_{\rm ch} = 10^{-0.16(L-10.7)/20}$, in which L is the fibre length of the quantum channel. The overall transmittance from Alice (Bob) to Charlie is thus $\eta = \eta_{\rm d}\eta_{\rm ch}$. In the code mode, the asymptotical counting rate for the correct key bit is denoted by $Q_{\rm corr} = (1-(1-p_{\rm d}){\rm e}^{-2\eta(1-e_{\rm m})\mu}){\rm e}^{-2\eta e_{\rm m}\mu}(1-p_{\rm d})$, and $Q_{\rm err} = (1-(1-p_{\rm d}){\rm e}^{-2\eta e_{\rm m}\mu}){\rm e}^{-2\eta(1-e_{\rm m})\mu}(1-p_{\rm d})$ for the error key bit. Hence, the error rate for the sifted key is $e_{\rm bit} = \frac{Q_{\rm err}}{Q_{\rm err}+Q_{\rm corr}}$. In the decoy mode, the asymptotic counting rate conditioned on Alice and Bob both preparing $\tau(\mu_0)$ is denoted by $Q^{\rm d}_{\mu_0\mu_0} = 2(1-(1-p_{\rm d}){\rm e}^{-\eta\mu_0}){\rm e}^{-\eta\mu_0}(1-p_{\rm d})$. Denoting $N_{\rm tot}$ as the total number of quantum signals sent by Alice and Bob, we assume that the observed detection frequencies are just equal to their corresponding mean values, which means $K_0/N_{\rm tot} = p_0^2(Q_{\rm corr} + Q_{\rm err})/2$, $K_1/N_{\rm tot} = p_{10}^2 Q^{\rm d}_{\mu_0\mu_0} + p_{11}^2 Q^{\rm d}_{\mu_1\mu_1}$ and $K_2/N_{\rm tot} = p_2^2 Q^{\rm d}_{\mu_2\mu_2}$. Then, for any channel transmittance, we can optimize the group of parameters $(\mu, \mu_0, \mu_1, \mu_2, p_0, p_{10}, p_{11}, p_2)$ to maximize the secret key rate per pulse $G/N_{\rm tot}$.

Time sequence to compensate phase drift. To compensate the fast phase drift, we chose a frame period of 20 μs and designed its time sequence (a diagram is provided in the Supplementary Information). At Alice's (Bob's) site, the 4-GHz pulse train is chopped into a time-multiplexed reference part and a quantum part. At Charlie's site, quadrature interference and in-phase interference are produced by adding π/2 and 0 phases, respectively. The comparatively bright reference part is thus divided into three regions, the estimation region is used to estimate the value of the relative drifted phase, the phase transition region is used to calculate and add the corresponding error signal onto the feedback PM immediately, and the visibility indicator (noted as vis-indicator) region is used to indicate the compensated result by showing the visibility of interference. Over the estimation region, the photons of quadrature interference detected by two SSPDs (D0 and D1) are first recorded by a field-programmable gate array (FPGA). Then, according to the counting data, the FPGA calculates a compensated value, which is sent to a digital-to-analogue converter (DAC) and an amplifier to generate the corresponding voltage for the feedback PM. The clock rate of the FPGA is 100 MHz and it takes 10 clocks (100 ns) to accomplish the calculation. It needs more time (~400 ns) to achieve a high-precision and steady compensated voltage because of the response time of the DAC and amplifier. The durations of the three transition regions (intensity and phase transition region 0.8 μs, phase transition region 0.6 μs, intensity transition region 0.8 μs) and the vis-indicator region (0.8 μs) are unchanged, but those of the estimation region and quantum part are changed depending on the rate of the phase drift. In the VOA simulation experiment, the duration of the estimation region and quantum part are 2 μs and 15 μs, respectively. In the fibre channel experiment with less than 800 km of fibre, the duration of the estimation region and quantum part are 7 μs and 10 μs, respectively. In the experiment with fibre with length of 833.80 km, the duration of the estimation region and quantum part are 9 μs and 8 μs, respectively.

Data availability

All of the data that support the findings of this study are available in the main text or Supplementary Information. Source data are available from the corresponding authors on reasonable request.

References

48. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *N. J. Phys.* **11**, 045018 (2009).
49. Müller-Quade, J. & Renner, R. Composability in quantum cryptography. *N. J. Phys.* **11**, 085006 (2009).

Acknowledgements

We acknowledge financial support from the National Key Research and Development Program of China (grant no. 2018YFA0306400), the National Natural Science Foundation of China (grants nos. 61622506, 61627820, 61822115, 61875181 and 61675189) and the 111 Project (D20031), and the Anhui Initiative in Quantum Information Technologies.

Author contributions

S.W., Z.-Q.Y., D.-Y.H. and Wei Chen (University of Science and Technology of China) developed the experimental set-up, performed the measurements and analysed the data. P.Y., G.-J.F.-Y., F.-X.W. and Z.Z. supported the experimental work. R.-Q.W., Y.Z. and Z.-Q.Y. provided the simulations. Wei Chen (Shanghai University & Jiangsu Hengtong Optical Fiber Technology Co. Ltd.) and Y.-G.Z. provided the ultra-low-loss fibres. P.V.M., A.V.D., D.-Y.H. and S.W. designed the low-noise detector. Wei Chen (University of Science and Technology of China), G.-C.G. and Z.-F.H. guided the work. S.W. and Z.-Q.Y. wrote the manuscript, with contributions from all the authors.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41566-021-00928-2.

Correspondence and requests for materials should be addressed to De-Yong He, Wei Chen or Zheng-Fu Han.

Peer review information *Nature Photonics* thanks Marco Lucamarini and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.