LETTERS
https://doi.org/10.1038/s41566-020-0599-8

nature photonics

Check for updates

Implementation of quantum key distribution surpassing the linear rate-transmittance bound

Xiao-Tian Fang[1,2,7], Pei Zeng[3,7], Hui Liu[1,2,7], Mi Zou[1,2], Weijie Wu[3], Yan-Lin Tang[4], Ying-Jie Sheng[4], Yao Xiang[4], Weijun Zhang[5], Hao Li[5], Zhen Wang[5], Lixing You[5], Ming-Jun Li[6], Hao Chen[6], Yu-Ao Chen[1,2], Qiang Zhang[1,2], Cheng-Zhi Peng[1,2,4], Xiongfeng Ma[3]✉, Teng-Yun Chen[1,2]✉ and Jian-Wei Pan[1,2]✉

Quantum key distribution (QKD)[1,2] offers a long-term solution to secure key exchange. Due to photon loss in transmission, it was believed that the repeaterless key rate is bounded by a linear function of the transmittance, $O(\eta)$ (refs. [3,4]), limiting the maximal secure transmission distance[5,6]. Recently, a novel type of QKD scheme has been shown to beat the linear bound and achieve a key rate performance of $O(\sqrt{\eta})$ (refs. [7–9]). Here, by employing the laser injection technique and the phase post-compensation method, we match the modes of two independent lasers and overcome the phase fluctuation. As a result, the key rate surpasses the linear bound via 302 km and 402 km commercial-fibre channels, over four orders of magnitude higher than existing results[5]. Furthermore, our system yields a secret key rate of 0.118 bps with a 502 km ultralow-loss fibre. This new type of QKD pushes forward long-distance quantum communication for the future quantum internet.

In conventional point-to-point QKD, such as the BB84 protocol[1], the sender Alice encodes key information into quantum states and sends it to receiver Bob for detection. In measurement-device-independent QKD (MDI-QKD), Alice's and Bob's positions are symmetric. They both send out encoded optical pulses to a measurement site owned by Charlie, who interferes the pulses and publicly announces the results to correlate Alice's and Bob's key information. The security of MDI-QKD does not depend on how Charlie realizes the measurement or announces the results. As a result, this scheme is immune to all attacks on the detection and hence has a higher security level in practice.

In quantum communication, attenuated lasers are widely used as photon sources; these can be described by weak coherent states, $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{k=0}^{\infty}\frac{\alpha^k}{\sqrt{k!}}|k\rangle$, superpositions of k-photon states $|k\rangle$. The parameter $\alpha = \sqrt{\mu}e^{i\phi}$ is a complex number, where $\mu = |\alpha|^2$ is the mean photon number and ϕ is the phase. In the original MDI-QKD[10], the user encodes the key information into two weak coherent states on two orthogonal optical modes, such as polarization encoding. In the security analysis, only the information carried by the single-photon states can be used for the final key generation. The decoy-state method is widely employed to efficiently extract secret key information[11–13].

In reality, quantum information carriers—photons—can be lost easily during transmission. We define the transmittance between Alice and Bob, η, to be the probability of a photon being successfully transmitted through the channel and being detected. Hence, in the symmetric setting of MDI-QKD, the transmittance between Alice (Bob) and the measurement site is $\sqrt{\eta}$. Only the detections caused by Alice's and Bob's single-photon states can be used for secure key generation. This detection rate is then given by $O(\eta)$, as a natural upper bound of the key rate.

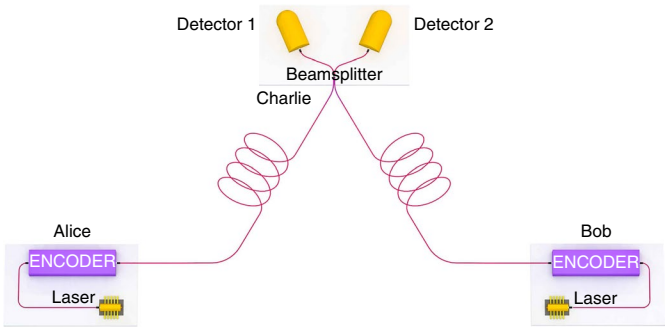


Fig. 1 | Schematic of PM-QKD. The encoder is a device to modulate the mean photon number μ and phase ϕ of coherent states. The beamsplitter and the single-photon detectors are used for interference detection. Phases $\phi \in [0, 2\pi)$ are divided into D slices, denoted by $\Delta_j = \left[\frac{\pi}{D}(2j-1), \frac{\pi}{D}(2j+1)\right)$ with index $0 \le j \le D-1$. In the experiment, we set $D = 16$. In each round of key distribution, Alice encodes a random bit κ_a into her coherent state $\left|\sqrt{\mu_a}e^{i(\kappa_a\pi+\phi_a)}\right\rangle$, after adding an extra discrete random phase $\phi_a = j_a 2\pi/D$, which is at the centre of the j_ath phase slice Δ_{j_a}. Similarly, Bob encodes κ_b, μ_b and ϕ_b on his pulse, $\left|\sqrt{\mu_b}e^{i(\kappa_b\pi+\phi_b)}\right\rangle$. Alice and Bob then send their pulses to Charlie, who is supposed to interfere these quantum states to measure phase differences. After Charlie announces the detection results, Alice and Bob publicly announce the slice indices j_a, j_b of the random phases. They post-select the key bits κ_a, κ_b as the raw key, according to Charlie's detection results and the sifting scheme depending on j_a, j_b, with the phase post-compensation technique.

[1]Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui, China. [2]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui, China. [3]Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China. [4]QuantumCTek Corporation Limited, Hefei, Anhui, China. [5]State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai, China. [6]Corning Incorporated, Corning, NY, USA. [7]These authors contributed equally: Xiao-Tian Fang, Pei Zeng, Hui Liu. ✉e-mail: xma@tsinghua.edu.cn; tychen@ustc.edu.cn; pan@ustc.edu.cn

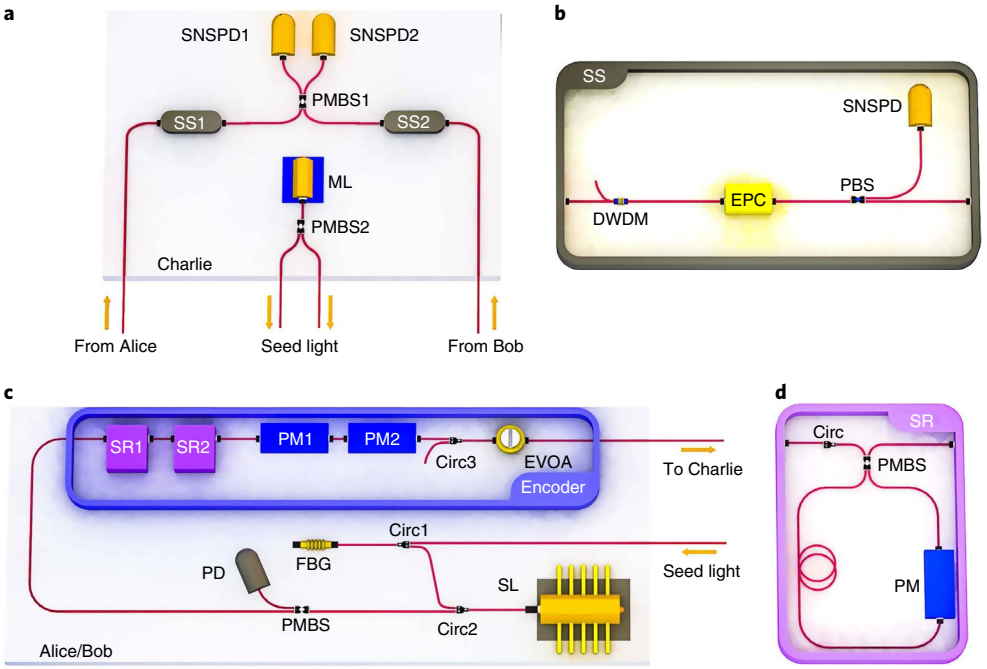


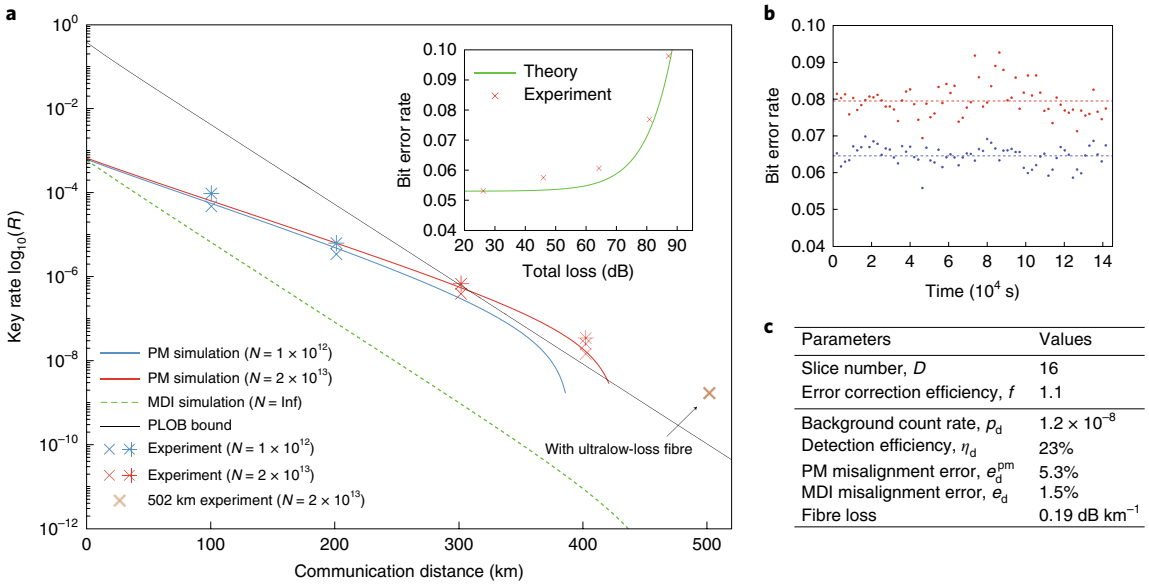
Fig. 2 | Experimental set-up. a, Light from the continuous-wave master laser (ML), used as the phase and wavelength reference, is split by a polarization-maintaining beamsplitter (PMBS2) and sent to Alice and Bob to lock their distributed feedback (DFB) lasers, which act as slave lasers (SLs). Two stabilization systems (SS1 and SS2) are placed to enhance the interference stability. Alice's and Bob's pulses are interfered at PMBS1 and then detected by two superconducting nanowire single-photon detectors (SNSPD1 and SNSPD2). **b**, Stabilization system. The dense wavelength division multiplexer (DWDM) filters out optical noises that disturb the detection results. A polarization beamsplitter (PBS), an SNSPD and an electric polarization controller (EPC) ensure that the polarization of the two pulses from Alice and Bob are indistinguishable. **c**, The quantum source. Alice (same as Bob) injects the seed light from the ML, which is filtered by the fibre Bragg grating (FBG), into her local DFB laser as the SL. The SL generates pulses, which are split by the PMBS. One of the output pulses goes to the encoder and the other is monitored by a photoelectric diode (PD). The encoder is composed of two Sagnac rings (SR1 and SR2) for modulating the intensities and two phase modulators (PM1 and PM2) for encoding the phases. A circulator (Circ3) is placed to isolate the source from the channel. The electrical variable optical attenuator (EVOA) reduces the pulse intensity to the single-photon level. **d**, The SR includes a circulator, a PMBS, a PM and optical fibre. The length difference between the optical fibre connecting the output and input of the PMs is delicately designed to meet twice the repetition frequency of the pulses.

To achieve a better rate-transmittance performance, a new phase-encoding MDI-QKD scheme, named phase-matching quantum key distribution (PM-QKD), has been proposed, as shown in Fig. 1. Alice (Bob) encodes the key information into the phase of a coherent state on a single optical mode. In this case, Charlie treats Alice and Bob's two optical modes as one quantum system and detects the relative phase between them. To do so, Charlie only needs one photon in the joint quantum system. Therefore, the detection rate is $O(\sqrt{\eta})$. Strict security analysis shows that PM-QKD enjoys a quadratic improvement on the rate-transmittance performance over the original MDI-QKD[8].

Despite the promising qualities of PM-QKD for both security and performance, its experimental implementation is very challenging. In PM-QKD, the interference results at the measurement site should reflect the difference between Alice's and Bob's encoded phases. In practice, an essential requirement is to match the phases of coherent states generated by two remote and independent lasers. The coherent states of Alice ($\left|\sqrt{\mu_a}e^{i(\kappa_a\pi+\phi_a)}\right\rangle$) and Bob ($\left|\sqrt{\mu_b}e^{i(\kappa_b\pi+\phi_b)}\right\rangle$) could have different phase references due to phase drift and fluctuation. We define the reference deviation ϕ_δ to be the phase difference when both Alice and Bob set $\kappa_{a(b)}=0$ and $\phi_{a(b)}=0$. There are three main factors determining the value of ϕ_δ: fluctuations of the laser initial phases, the optical lengths of the fibres and the laser frequencies. For example, with 1,550 nm telecom light through a 200 km fibre, a tiny change of transmission time, say by 10^{-15} s (corresponding to 200 nm optical length), or a small deviation of the angular frequency, say by 1 kHz, will cause a significant phase drift. Note that there are several recent experiments that attempt to deal with these challenges to demonstrate the advantages of the new type of MDI-QKD scheme[14–17].

In this work, we implement PM-QKD with the set-up shown in Fig. 2. To suppress fluctuations of the laser initial phases and frequencies, we use the laser injection technique[18–20]. The set-ups on Alice's and Bob's sides are exactly the same. In the following, we consider Alice's side as an example. The master laser at the measurement site, with 3 kHz linewidth and 1,550.12 nm centre wavelength, emits a seed light that passes through a long fibre to lock Alice's distributed feedback laser. Alice's laser generates optical pulses with a clock rate of 312.5 MHz. Two Sagnac rings are used to modulate the pulses into four different intensities. The pulses with the largest intensity are used as reference pulses for phase estimation, while the other three pulses are used as the signal state, weak decoy state and vacuum state to implement the decoy-state method. The extinction ratio between the signal state and the vacuum state is ~20 dB. Two phase modulators are employed to modulate 16 different phases. Details of the laser injection technique and phase estimation are presented in the Methods.

The pulses from Alice and Bob are transmitted through long optical fibres and interfered at the measurement site. The interference results are detected by two superconducting nanowire single-photon detectors. The dark count is ~10 counts per second and the detector efficiency is ~40%. The total detection efficiency reduces to ~23% owing to 1.2 dB insertion loss and 25% non-overlapping between the signal and detection windows. Two stabilization



Parameters	Values
Slice number, D	16
Error correction efficiency, f	1.1
Background count rate, p_d	1.2×10^{-8}
Detection efficiency, η_d	23%
PM misalignment error, e_d^{pm}	5.3%
MDI misalignment error, e_d	1.5%
Fibre loss	0.19 dB km^{-1}

Fig. 3 | Experimental parameters and results. a, Main panel: the experimental rate–distance performance of PM-QKD, compared with the theoretical expectation and the linear key rate bound[4]. Data points marked by crosses and stars are, respectively, the key rate without and with use of phase-mismatched signals. Here, N is the total number of QKD rounds. Inset: error rate against total loss. The solid line shows the bit error rate in the theoretical model and the crosses show the experiment data. **b**, The bit error rate with respect to experiment time in the 302 km experiment. Each data point represents a number of 3.31×10^5 effective clicks, which are collected in 21.91 min on average. Blue and red dots show the bit error rate for data with phase difference $j_d = 0$ and 1, respectively. **c**, The parameters used in the experiment and theoretical simulation. Note that the listed background count rate p_d, detection efficiency η_d, misalignment error e_d and fibre loss of PM-QKD are those used for the numerical simulation. The corresponding experimental values depend on the specific environment and are listed in the Supplementary Information.

systems are inserted before the interference to filter out the noise caused by the nonlinear effect of the fibre and to stabilize the incident pulses. Details of the implementation are presented in the Supplementary Information.

Due to fibre fluctuation, there is a slow phase drift between Alice and Bob. When the phase fluctuates slowly, pulses nearby share similar values of the reference deviation ϕ_δ. Inspired by this observation, we use a simple phase post-compensation technique[21]. During the experiment, Alice and Bob periodically send reference pulses and quantum pulses. The reference pulse is typically more than one order of magnitude stronger than the quantum pulse. Reference pulses are used to estimate in which slice j_δ the reference deviation ϕ_δ lies, according to the interference results. Quantum pulses are used to perform the PM-QKD experiment. After obtaining measurement results, Alice and Bob publicly announce the random phase slices j_a, j_b of the signal pulses. They calculate $j_s = j_a - j_b + j_\delta$ for raw key sifting, where j_δ works as the post-compensation shift. Clearly, if j_δ accurately reflects the real-time reference deviation of the system, perfect interference will happen when $j_s = 0$ or $j_s = 8$. Note that the estimated phase slice indices j_δ are only used in the post-processing, which frees us from active phase-locking during state transmission. Furthermore, compared with active locking, where the phase can only be locked well when ϕ_δ remains stable during the whole process of phase estimation and feedback, the phase post-compensation method can tolerate faster fluctuation, as long as ϕ_δ does not change much in the time between the reference and quantum pulses.

In the security analysis of PM-QKD[8], due to the encoded phase κ_a, κ_b, coherent signals $|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_k \frac{\alpha^k}{\sqrt{k!}} |k\rangle$, originally a coherent superposition of different photon number states $\{|k\rangle\}$, will be decoupled to a probabilistic mixture of odd and even photon number components ρ^{odd} and ρ^{even}. The final effective detection will then be caused by either ρ^{odd} or ρ^{even}. The contributed ratios of ρ^{odd} and ρ^{even} in the final effective detection are denoted q^{odd} and q^{even}, and obviously $q^{odd} + q^{even} = 1$. In a recent theoretical work[22], information leakage in PM-QKD is shown to be independent of channel disturbance. As a result, the privacy is only related to q^{even}, regardless of the bit error rate. The final key length is given by

$$K = M_\mu \left[1 - H(q_\mu^{even})\right] - l_{cor} \quad (1)$$

where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. Here, we consider the case where Alice and Bob use the same intensities of coherent states. The subscript μ represents the signal states with $\mu_a = \mu_b = \mu/2$. The raw key length M_μ is the number of detection events caused by signal states when Alice and Bob match their phases ($j_s = 0$ or 8). The even photon component ratio q_μ^{even} can be efficiently estimated by decoy-state methods[11–13]. The error correction cost l_{cor} can usually be estimated as a function of bit error rate E_μ ($l_{cor} = fM_\mu H(E_\mu)$), where f is the error correction efficiency depending on $E_\mu^{j_s}$. The key rate is defined by $R = K/N$, where N is the number of QKD rounds. Details of the decoy-state method and security analysis considering finite data size effects are presented in the Supplementary Information.

To further improve the key rate, one can take advantage of data with mismatched phases. Note that the phase-mismatched signals of $j_s = 1, 9$ can be regarded as ones with a fixed misalignment $\phi_\delta = 2\pi/D$, which results in a larger bit error rate compared with the phase-matched signals of $j_s = 0, 8$. Raw keys with different j_s have the same q^{even} in equation (1) and hence the same privacy. More explicitly, Alice and Bob can categorize the data from signal states into $D/2$ groups, where the data of $j_s = 0, 8$ are in the 0th group, the data of $j_s = 1, 9$ are in the first group, and so on. Alice and Bob can correct errors in each data group separately and perform privacy amplification altogether. Of course, if the error rate in a group is too large, they can simply discard that group of data.

Experiments were performed using 101, 201, 302 and 402 km standard optical fibres and a 502 km ultralow-loss optical fibre.

The experiment parameters and results are presented in Fig. 3, from which one can see that the key rate-transmittance relation follows $R = O(\sqrt{\eta})$, in contrast with the linear rate-transmittance bound. Specifically, the experimental results beat the linear bound for distances of 302 and 402 km. If we take the 302 km fibre case as an example, with the same channel transmission and detection efficiency, the linear key rate bound is given by $R_{up} = 5.44 \times 10^{-7}$. Our experiment yields a key rate of $R = 6.74 \times 10^{-7}$ with a failure probability of $\epsilon = 1.68 \times 10^{-10}$, when all the mismatched data are used. The key rate is 24.0% higher than the bound. For the case of 302 km, the data with mismatched phases have a significant contribution to the overall key rate, which is 72.6% larger than the value with only the phase-matched group considered. The key generation speed is 94.4 bps. Notably, our achieved key rate is three orders of magnitude higher than the asymptotic key rate of the original MDI-QKD scheme[10].

Meanwhile, in the 502 km experiment with an ultralow-loss optical fibre, we obtained a positive key rate, beating the current record 421 km fibre communication distance with QKD[6]. The channel loss in the 502 km experiment was 81.7 dB and the total loss was 87.1 dB. This new loss-tolerance record is comparable with the high-orbital satellite link loss in free space.

Our results show that the PM-QKD system is stable and economical, facilitating the promotion of practical QKD. In the future, we expect to use the phase post-compensation technique to keep the system robust by increasing the system repetition frequency and enhancing the performance of the detectors. We also expect that the PM-QKD experiment design will be helpful in the construction of quantum repeaters[23,24], as well as extending the reach of the quantum internet.

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/s41566-020-0599-8.

Received: 29 July 2019; Accepted: 2 February 2020;
Published online: 2 March 2020

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. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
3. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
4. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
5. Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
6. Boaron, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).
7. Lucamarini, M., Yuan, Z., Dynes, J. & Shields, A. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
8. Ma, X., Zeng, P. & Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **8**, 031043 (2018).
9. Lin, J. & Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **98**, 042332 (2018).
10. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
11. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
12. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
13. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
14. Minder, M. et al. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photon.* **13**, 334–338 (2019).
15. Liu, Y. et al. Experimental twin-field quantum key distribution through sending or not sending. *Phys. Rev. Lett.* **123**, 100505 (2019).
16. 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).
17. 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).
18. Yuan, Z. et al. Directly phase-modulated light source. *Phys. Rev. X* **6**, 031044 (2016).
19. Comandar, L. et al. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nat. Photon.* **10**, 312–315 (2016).
20. Lipka, M., Parniak, M. & Wasilewski, W. Optical frequency locked loop for long-term stabilization of broad-line DFB laser frequency difference. *Appl. Phys. B* **123**, 238 (2017).
21. Ma, X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 062319 (2012).
22. Zeng, P., Wu, W. & Ma, X. Symmetry-protected privacy: beating the rate–distance linear bound over a noisy channel. Preprint at https://arxiv.org/abs/1910.05737 (2019).
23. Zukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. K. Event-ready-detectors Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287–4290 (1993).
24. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).

Methods

Phase drift estimation. Rather than using extra devices to lock the phase, here we apply the phase estimation method to estimate the drifted phase. Alice and Bob need not obtain the exact value of the real-time phase deviation ϕ_δ, but only an estimate of the slice number j_δ for post-compensation. Moreover, the estimation of j_δ does not need to be announced in a real-time manner. Instead, it can be announced during the sifting process, as a post-selection shift factor. This makes our protocol practical without active feedback. The schematics of the phase estimation method are provided in the Supplementary Information.

In the reference pulse region, Alice and Bob send reference pulses to Charlie, who interferes them and announces the results. They use the interference results to estimate the phase slice difference between two reference pulses, ϕ_δ. The right detector click ratio P_r after interference is

$$\frac{n_r}{n_r + n_l} \approx P_r = \frac{1 + \cos\phi_\delta}{2} \tag{2}$$

where n_r and n_l are the counts of the right and left detector clicks, respectively. With this ratio, one can classify the phase fluctuation ϕ_δ to the phase slices Δ_{j_δ}, marked by j_δ according to the detection ratio.

Because the phase deviations ϕ_δ and $(2\pi - \phi_\delta)$ yield the same P_r, Alice and Bob cannot discriminate these two cases from the ratio P_r. To solve this problem, Alice loads a $\phi_0 = \pi/2$ phase on the pulses in the latter reference pulse region, making the phase difference $\phi_\delta + \pi/2$, and hence $P_r = \frac{1-\sin\phi_\delta}{2}$. In that case, one can distinguish the phase slice j_δ from $(16 - j_\delta)$. With the interference results P_r from case $\phi_0 = 0$ and $\phi_0 = \pi/2$, Alice and Bob can estimate j_δ accurately.

To yield an accurate estimation of j_δ, sufficient detection counts of the reference pulses are required. According to the transmittance and phase drift velocity, it is necessary to properly set the intensity and time duration of the reference pulse and the system repetition frequency.

Laser injection technique. Fluctuation of the reference deviation ϕ_δ is mainly caused by three factors: initial phase fluctuation of the lasers, optical length fluctuation and fluctuation of the laser frequencies. To minimize the fluctuation caused by the first and the third factors, we apply the laser injection technique.

In the experiment, a narrow-linewidth continuous-wave laser at Charlie's side works as the master laser, while a DFB laser at Alice's (and also Bob's) side works as the slave laser. The seed light generated by the master laser is divided into two parts and sent to the two slave lasers through long fibres, which induces stimulated emission. The set-up of the laser-injection device is described in the Supplementary Information.

In this case, the wavelength and phase of the light generated by the slave laser are the same as those of the seed light, which results in slower fluctuation of the laser initial phases. In a local experiment test, interference results for pulses generated by slave lasers show that the phase difference of two locked slave lasers fluctuates with a relatively low speed. Details for this are presented in the Supplementary Information. Here, the residual phase noise and fluctuation mainly come from the spontaneous emission in the slave lasers. The nonlocal phase drift test results are presented in the Supplementary Information. Although the phase fluctuates faster with longer fibre, we can still obtain an effective phase estimation in this case.

In the 101, 201, 302 and 402 km experiments, the master laser is located at the side of Charlie's interferometer. The fibres used to transmit the seed and signal light are different, but have the same length. Due to the limited power of the master laser and the low transmittance value, in the 502 km experiments we place the master laser and the slave lasers locally.

Data availability

The data that support the plots within this paper and other findings of this study are available from the corresponding authors upon reasonable request.

Acknowledgements

We thank H. Zhou for insightful discussions. This work was supported by the National Key R&D Program of China (2017YFA0303903), the Chinese Academy of Science, the National Fundamental Research Program, the National Natural Science Foundation of China (grants 11875173, 61875182 and 11674193) and Anhui Initiative in Quantum Information Technologies and Fundamental Research Funds for the Central Universities (WK2340000083).

Author contributions

X.M., T.-Y.C. and J.-W.P. conceived the research. Y.-A.C. Q.Z., C.-Z.P., X.M., T.-Y.C. and J.-W.P. designed the experiment. X.-T.F., H.Liu and T.-Y.C. carried out the experiment. P.Z., W.W. and X.M. performed the protocol security analysis and data post-processing. M.Z. and Y.-L.T. assisted with the experiment scheme discussion and verification. Y.-J.S. designed and developed the voltage pulse generator. Y.X. programmed the field-programmable gate array logic. W.Z., H.Li, Z.W. and L.Y. designed and fabricated the superconducting nanowire single-photon detector. M.-J.L. and H.C. provided the ultralow-loss fibres. P.Z., X.-T.F., H.Liu, X.M., T.-Y.C. and J.-W.P. co-wrote the manuscript, with input from the other authors. All authors discussed the results and proofread the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information is available for this paper at https://doi.org/10.1038/s41566-020-0599-8.

Correspondence and requests for materials should be addressed to X.M., T.-Y.C. or J.-W.P.