Article

Entanglement-based secure quantum cryptography over 1,120 kilometres

https://doi.org/10.1038/s41586-020-2401-y

Received: 15 July 2019

Accepted: 13 May 2020

Published online: 15 June 2020

Check for updates

Juan Yin[1,2,3], Yu-Huai Li[1,2,3], Sheng-Kai Liao[1,2,3], Meng Yang[1,2,3], Yuan Cao[1,2,3], Liang Zhang[2,3,4], Ji-Gang Ren[1,2,3], Wen-Qi Cai[1,2,3], Wei-Yue Liu[1,2,3], Shuang-Lin Li[1,2,3], Rong Shu[2,3,4], Yong-Mei Huang[5], Lei Deng[6], Li Li[1,2,3], Qiang Zhang[1,2,3], Nai-Le Liu[1,2,3], Yu-Ao Chen[1,2,3], Chao-Yang Lu[1,2,3], Xiang-Bin Wang[2], Feihu Xu[1,2,3], Jian-Yu Wang[2,3,4], Cheng-Zhi Peng[1,2,3]✉, Artur K. Ekert[7,8] & Jian-Wei Pan[1,2,3]✉

Quantum key distribution (QKD)[1–3] is a theoretically secure way of sharing secret keys between remote users. It has been demonstrated in a laboratory over a coiled optical fibre up to 404 kilometres long[4–7]. In the field, point-to-point QKD has been achieved from a satellite to a ground station up to 1,200 kilometres away[8–10]. However, real-world QKD-based cryptography targets physically separated users on the Earth, for which the maximum distance has been about 100 kilometres[11,12]. The use of trusted relays can extend these distances from across a typical metropolitan area[13–16] to intercity[17] and even intercontinental distances[18]. However, relays pose security risks, which can be avoided by using entanglement-based QKD, which has inherent source-independent security[19,20]. Long-distance entanglement distribution can be realized using quantum repeaters[21], but the related technology is still immature for practical implementations[22]. The obvious alternative for extending the range of quantum communication without compromising its security is satellite-based QKD, but so far satellite-based entanglement distribution has not been efficient[23] enough to support QKD. Here we demonstrate entanglement-based QKD between two ground stations separated by 1,120 kilometres at a finite secret-key rate of 0.12 bits per second, without the need for trusted relays. Entangled photon pairs were distributed via two bidirectional downlinks from the Micius satellite to two ground observatories in Delingha and Nanshan in China. The development of a high-efficiency telescope and follow-up optics crucially improved the link efficiency. The generated keys are secure for realistic devices, because our ground receivers were carefully designed to guarantee fair sampling and immunity to all known side channels[24,25]. Our method not only increases the secure distance on the ground tenfold but also increases the practical security of QKD to an unprecedented level.

Our experimental arrangement is shown in Fig. 1. The two receiving ground stations are located at Delingha (37°22′44.43″N, 97°43′37.01″E; altitude 3,153 m) in Qinghai province, and Nanshan (43°28′31.66″N, 87°10′36.07″E; altitude 2,028 m) in Xinjiang province, China. The physical distance between Delingha and Nanshan is 1,120 km. To optimize the receiving efficiencies, both the two ground telescopes are newly built with a diameter of 1.2 m, specifically designed for the entanglement distribution experiments. All the optical elements, such as mirrors, in the telescopes maintain polarization.

The satellite is equipped with a compact spaceborne entangled photon source with a weight of 23.8 kg. A periodically poled $KTiOPO_4$ crystal inside a Sagnac interferometer is pumped in both the clockwise and anticlockwise directions simultaneously by a continuous-wave laser with a wavelength centred at 405 nm and a linewidth of 160 MHz, and generates down-converted polarization-entangled photon pairs at 810 nm close to the form of $|\Psi\rangle_{12} = (|H\rangle_1|V\rangle_2 + |V\rangle_1|H\rangle_2)/\sqrt{2}$, where $|H\rangle$ and $|V\rangle$ denote the horizontal and vertical polarization states, respectively, and the subscripts 1 and 2 denote the two output spatial modes. The entangled photon pairs are then collected and guided by two single-mode fibres to two independent transmitters equipped in the satellite. Both transmitters have a near-diffraction-limited far-field divergence of about 10 μrad. Under a pump power of 30 mW, the source distributes up to 5.9×10^6 entangled photon pairs per second.

The photons are collected by the telescopes on two optical ground stations. For each one, the follow-up optics is installed on one of the rotating arms and rotates along with the telescope. As shown in Fig. 1c,

[1]Hefei National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, China. [2]Shanghai Branch, CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai, China. [3]Shanghai Research Center for Quantum Science, Shanghai, China. [4]Key Laboratory of Space Active Opto-Electronic Technology, Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai, China. [5]The Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu, China. [6]Shanghai Engineering Center for Microsatellites, Shanghai, China. [7]Mathematical Institute, University of Oxford, Oxford, UK. [8]Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore. ✉e-mail: pcz@ustc.edu.cn; pan@ustc.edu.cn

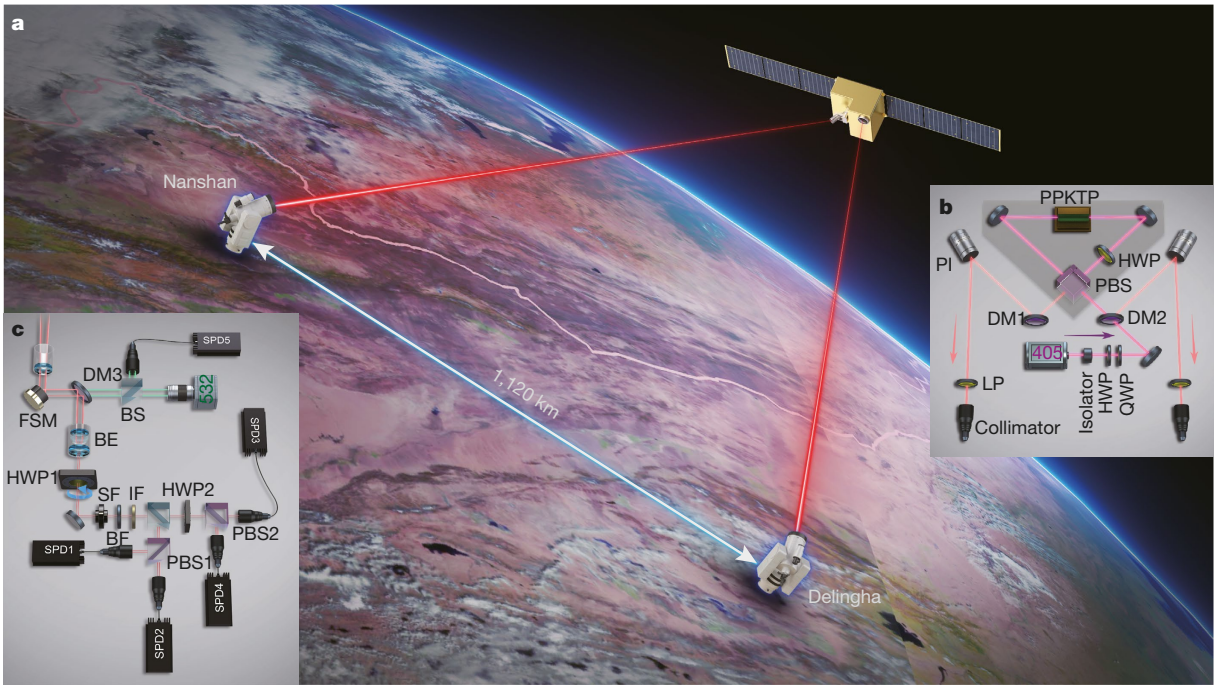


Fig. 1 | Overview of the experimental set-up of entanglement based quantum key distribution. a, An illustration of the Micius satellite and the two ground stations. Image credit: Fengyun-3C/Visible and Infrared Radiometer, with permission (2020). The satellite flies in a Sun-synchronous orbit at an altitude of 500 km. The physical distance between Nanshan and Delingha ground station is 1,120 km. **b**, The spaceborne entangled-photon source. A free space isolator is used to minimize back reflection to the 405-nm pump laser. A pair of off-axis concave mirrors is used to focus the pump laser and collimate the down-converted photon pairs. PBS, polarization beam splitter; DM, dichroic mirror; LP, long-pass edge filter; PI, piezo steering mirror; HWP, half-wave plate; QWP, quarter-wave plate; PPKTP, periodically poled $KTiOPO_4$. **c**, The follow-up optic at the optical ground station. The tracking and synchronization laser is separated from the signal photon by DM3 and detected by the single photon detector (SPD5). The spatial filter (SF), broad-bandwidth filter (BF) and interference filter (IF) are used to filter out the input light in frequency and spatial domains. BS, beam splitter; BE, beam expander; FSM, fast steering mirror.

a beam splitter, a half-wave plate and two polarized beam splitters are combined to analyse the polarization of the entangled photons randomly in the bases of $Z \in \{|H\rangle, |V\rangle\}$ and $X \in \{|+\rangle, |-\rangle\}$, where $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$. After being transmitted or reflected by the beam splitter and polarized beam splitters, the photons are collected by four multimode fibres with the core diameter of 105 μm and detected by four single photon detectors (SPDs) respectively. We carefully selected the four SPDs to ensure that the detector efficiency is better than 53%, the efficiency consistency is better than 98.5% and the dark counts are less than 100 counts per second (see Extended Data Table 1 for details). A motorized half-wave plate (HWP1) is used to compensate the relative rotation between the transmitter and the receiver, where the correction angle offsets are calculated in advance. The entangled photons are filtered in both the frequency and spatial domains to satisfy the fair sampling assumption and to guarantee practical security. In particular, an extra field diaphragm, consisting of two lenses with focal length of 8 mm and a pinhole of 100 μm, is used as the spatial filter to unify the field of view of different channels, where the field of view is narrowed to 27 μrad. A broad-bandwidth filter and a narrow-bandwidth filter of 5 nm are used to reject frequency side channels. These frequency filters can also help to reduce the background counts. The output signals of the SPDs are recorded by a time-to-digital converter.

To optimize the link efficiency, we develop cascaded multistage acquiring, pointing and tracking systems both in the satellite transmitters and the optical ground station receivers, achieving a tracking accuracy of 2 μrad and 0.4 μrad, respectively. The beacon laser (532 nm, 10 kHz) from the satellite is also used as a synchronization laser. It is sampled, frontier identified and recorded by the same time-to-digital converter as well as quantum signals. The distant time-to-digital converters are first roughly synchronized using a global positioning system (GPS) one-pulse-per-second (1PPS) signal. As the frequency of the synchronization laser is relatively stable, a least-squares method is used to fit the selected pulses, which can eliminate the time jitter of synchronization detectors. The time synchronization accuracy of entangled photon pairs is 0.77 ns (1σ). We set a narrow coincidence time gate of 2.5 ns to reduce the accidentally coincident events.

The satellite flies along a Sun-synchronous orbit, and comes into both Delingha's and Nanshan's view once every night, starting at around 2:00AM Beijing time and lasting for a duration of 285 s (>13° elevation angle for both ground stations). Figure 2a plots the physical distances from the satellite to Delingha and Nanshan during one orbit, together with the sum channel length of the two downlinks. As shown in Fig. 2b, the measured overall two-downlink channel attenuation varies from 56 dB to 71 dB. As compared to previous experiment[23], this two-photon count rate, and thus the signal-to-noise ratio, is greatly improved. To increase the collection efficiency for downlink entangled photons, we have upgraded both the main system of the telescope and the follow-up optics. For the main system, we improved the receiving efficiency by recoating the main lens (+1.5 dB) and redesigning the high-efficiency beam expander (+0.9 dB). For the follow-up optics, we increased the collection efficiency through optical pattern matching, especially shortening the optical path by 20 cm to avoid beam spreading by 0.65 mm (+0.6 dB).

As a result, we have increased the collection efficiency of each satellite-to-ground link by a factor of about 2 over the previous experiment[23]. This was quantified by measuring the single-downlink efficiencies of each ground station for several orbits. The best-orbit data were taken on a clear night with no clouds in the sky and no haze near the ground, which had the highest atmospheric transmittance (Extended Data Fig. 1). Under these conditions, the link efficiency is related only

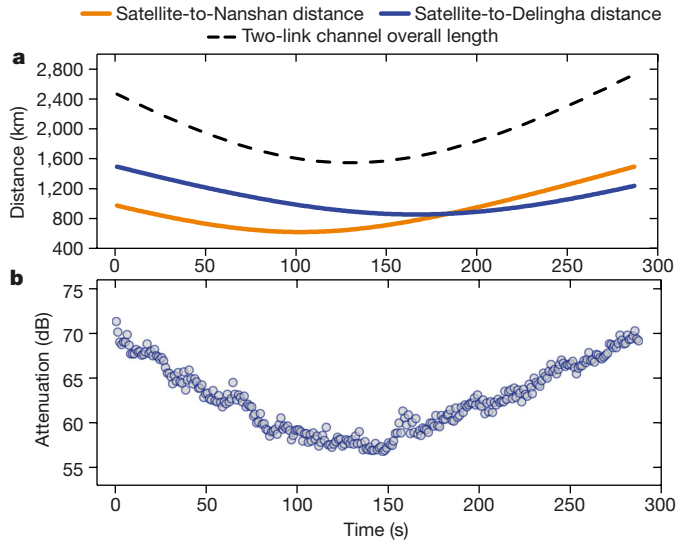


Fig. 2 | Distances and attenuations from satellite to Nanshan (Delingha). **a**, A typical two-downlink trial from satellite to Nanshan, and to Delingha, lasts about 285 s (>13° elevation angle for both ground stations) in a single pass of the satellite. The distance from satellite to Nanshan (Delingha) is from 618 km (853 km) to about 1,500 km, and the total length of the two downlinks varies from 1,545 km to 2,730 km. **b**, The measured satellite-to-ground two-downlink channel attenuation.

to the distance between the satellite and the ground (Extended Data Fig. 2). These data were selected to calibrate the improvement of the link efficiency, and a 3-dB enhancement in the collection efficiency was observed for each satellite-to-ground link (Extended Data Fig. 3). Overall, the collection efficiency of the two-photon distribution was improved by a factor of about 4 over the previous experiment[23].

To realize secure QKD against side-channel attacks, we add several single-mode filters to the receiver, which slightly decreases the collection efficiency. Even so, the system efficiency (with filters) still improves by a factor of about 2. A comparison of the results of this work and the previous experiment[23] is shown in Extended Data Table 2. We observe an average two-photon count rate of 2.2 Hz, with a signal-to-noise ratio of 15:1. The sifted key rate for QKD is 1.1 Hz. This enhancement is remarkable, because it decreases the quantum bit error rate (QBER) from about 8.1% (ref. [23]) to about 4.5%, thus enabling the realization of satellite-based entanglement QKD (Extended Data Fig. 4).

The entanglement-based QKD system was carefully designed to provide practical security against physical side channels[21,22]. We note that entanglement-based QKD is naturally source-independent[16,17], which guarantees that the system is secure against loopholes in the source. All we need is to ensure the security on the detection sides, that is, the two optical ground stations. In general, the side channels on the detection side primarily violate the key assumption of fair sampling. To guarantee this assumption, we add a series of filters with different degrees of freedom, including frequency, spatial and temporal modes, and implement countermeasures for the correct operation of the single-photon detectors.

Specifically, great attention has been paid to detection attacks, including: detector-related attack[26–28], wavelength-dependent attack[29], spatial-mode attack[30], and other possible side-channels. We have implemented countermeasures to all the above known attacks (see Methods and Extended Data Table 3). For the side channels targeting the operation of detectors, such as blinding attack[26], we install additional monitoring circuits. In particular, we install an additional circuit to monitor the anode of the load resistance in the detection circuit to counter the blinding attack (Extended Data Fig. 5). If there is a bright laser pulse illumination, the output of the monitoring circuit will exceed a secure threshold voltage and trigger the alarm (Fig. 3b). For the time-shift attack[27] and the dead-time attack[28], our countermeasure is to operate the detector in free-running mode, in which the detector records all the detection events and post-selects the detection windows such that the detection efficiency is guaranteed to be at a nominal level. For the side channels in other optical domains (Fig. 1c), we use optical filters to filter out the input light and eliminate the mismatch in the frequency and spatial domains. In particular, we use two cascaded broad-bandwidth and narrow-bandwidth filters (Fig. 3a) to eliminate the frequency dependency[29] of the transmission/reflection ratio of the beam splitter (Extended Data Fig. 6). Spatial filters are added to ensure identical efficiencies for different detectors (Fig. 3c), thus eliminating the spatially dependent loopholes[30]. Consequently, the secret key, generated by our QKD system, is practically secure for realistic devices.

To verify the entanglement established between the two distant optical ground stations, we use the distributed entangled photons for the Bell test with the Clauser–Horne–Shimony–Holt (CHSH)-type inequality[31], which is given by

$$S = |E(\varphi_1, \varphi_2) - E(\varphi_1, \varphi_2') + E(\varphi_1', \varphi_2) + E(\varphi_1', \varphi_2')| \le 2$$

where E is the joint correlation with measurement angles of the Delingha optical ground station and the Nanshan optical ground station, respectively. The angles are randomly selected from (0, π/8), (0, 3π/8), (π/4, π/8) and (π/4, 3π/8) to close the locality loophole. We run 1,021 trials of the Bell test during an effective time of 226 s. The observed result for parameter S is 2.56 ± 0.07, with a violation of the CHSH–Bell inequality $S < 2$ by 8 standard deviations (see Extended Data Table 4 for details). The Bell violation provides evidence of high-quality entanglement between the entangled photons observed over 1,120 km apart.

In our entanglement-based QKD demonstration, we adopted the BBM92 protocol[3], in which the measurements by Alice and Bob are symmetric, that is, each of them requires two measurement bases, that is, the Z (H/V) basis and the X (+/−) basis. As mentioned above, using filtering and monitoring, we guarantee that the single-photon detections were conducted on a nearly two-dimensional subspace and the system detection efficiencies for the four polarization states could be well characterized to satisfy the fair sampling condition without Eve's tampering. Experimentally, we have characterized the system detection efficiency of each detection path, where the efficiency mismatch has an upper bound of 1.47%. This efficiency mismatch is considered in the privacy amplification (PA) of the post-processing of the secret key rate (see Methods). Moreover, we use the post-processing to handle double clicks, by randomly assigning a classical bit, as well as the dead-time effect, by removing the sequential detections after a click. These implementations can ensure that the secret keys produced are secure against the issues of known side channels.

Following the security analysis for an uncharacterized source[19], the asymptotic secret key rate R_Z for the post-processed bits in the Z basis is given by:

$$R_Z \ge Q_Z[1 - f_e H(E_Z) - H(E_X)]$$

where Q_Z is the sifted key where Alice and Bob select the Z basis, f_e is the error correction inefficiency, and E_Z and E_X are the QBER in the Z and X bases, respectively. The analysis for the X basis is the same. The total asymptotic secret key rate is $R_A = R_Z + R_X$. The detailed security analysis for the finite key rate R_F, which takes into account the finite key size[32,33] and the detection efficiency mismatch, is shown in Methods.

Experimentally, we obtained 6,208 initial coincidences within 3,100 s of data collection. Discarding the events for which the two optical ground stations had chosen different bases, we obtained 3,100 bits of sifted key with 140 erroneous bits, which corresponded to an averaged QBER of 4.51% ± 0.37%. The QBERs in the H/V and +/− bases (Z and X bases) are, respectively, 4.63% ± 0.51% and 4.38% ± 0.54%. For

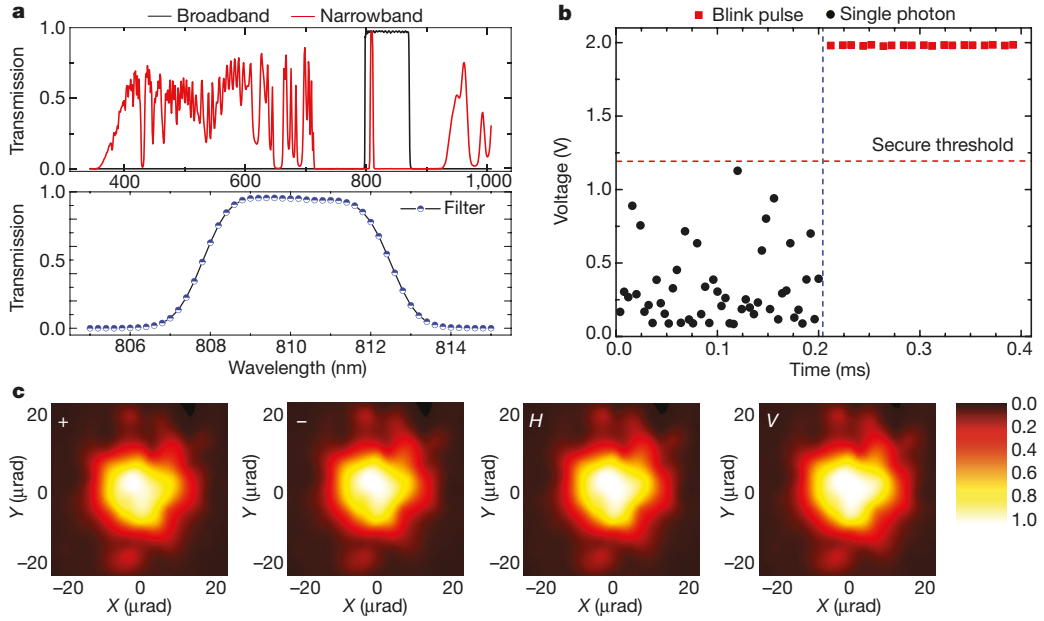


Fig. 3 | Monitoring and filtering against side channels. a, The transmission of broad-bandwidth and narrow-bandwidth wavelength filters. **b**, The output of monitoring circuit with/without blinding attack. Without blinding attack, the outputs are random avalanching single-photon-detection signals (black dots). With blinding attack (starting from 0.20 ms), the output signals are at around 2 V, which is clearly above the security threshold, thus triggering the security alarm. **c**, The system detection efficiency of the four polarizations in the spatial domain. With the spatial filter, the four efficiencies are identical. The colour scale shows the measured efficiencies normalized to the maximum efficiency.

the sifted bits, we performed an error correction with Hamming code and achieved an error correction inefficiency of $f_e = 1.19$. After the error correction and the PA, we obtained a secure key rate of $R_A = 0.43$ bits per second in the asymptotic limit of the infinitely long key. With a failure probability $\varepsilon = 10^{-10}$, the finite key rate is $R_F = 0.12$ bits per second (see Table 1 for a summary). In total, we obtained a 372-bit secret key. Compared to directly transmitting the entangled photons over a distance of 1,120 km using commercial ultralow-loss optical fibres (with a loss of 0.16 dB km^{-1}), we estimate that the effective link efficiency, and thus the secret key rate, of the satellite-based method is eleven orders of magnitude higher. The secure distance substantially outperforms previous entanglement-based QKD experiments[12,34].

In summary, we have demonstrated entanglement-based QKD between two ground stations separated by 1,120 km. We increase the link efficiency of the two-photon distribution by a factor of about 4 compared to the previous work[23] and obtain a finite-key secret key rate of 0.12 bits per second. The brightness of our spaceborne entangled photon source can be increased by about two orders of magnitude in our latest research[35], which could readily increase the average final key to tens of bits per second or tens of kilobits per orbit. The entanglement-based quantum communication could be combined with quantum repeaters[21] for general quantum communication protocols and distributed quantum computing[36]. Hence, our work paves the way towards entanglement-based global quantum networks. Overall, the results increase the secure distance of practical QKD on the ground from 100 km to more than 1,000 km without the need for trusted relays, thus representing an important step towards a truly robust and unbreakable cryptographic method for remote users over arbitrarily long distances.

Table 1 | Experimental results of entanglement-based QKD over 1,120 km

Parameter	Q	E_Z	E_X	R_A	R_F
Value	1.00 bps	4.63% ± 0.51%	4.38% ± 0.54%	0.43 bps	0.12 bps

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/s41586-020-2401-y.

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc. Int. Conf. on Computers, Systems and Signal Processing* 175–179 (1984).
2. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
3. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68**, 557 (1992).
4. Peng, C.-Z. et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Phys. Rev. Lett.* **98**, 010505 (2007).
5. Rosenberg, D. et al. Long-distance decoy-state quantum key distribution in optical fiber. *Phys. Rev. Lett.* **98**, 010503 (2007).
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. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43 (2017).
9. Liao, S.-K. et al. Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 Space Lab. *Chin. Phys. Lett.* **34**, 090302 (2017).
10. Yin, J. et al. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.* **119**, 200501 (2017).
11. Schmitt-Manderbach, T. et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* **98**, 010504 (2007).
12. Ursin, R. et al. Entanglement-based quantum communication over 144 km. *Nat. Phys.* **3**, 481 (2007).
13. Elliott, C. et al. Current status of the DARPA quantum network. In *Quantum Information and Computation III* Vol. 5815, 138–150 (International Society for Optics and Photonics, 2005).
14. Peev, M. et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001 (2009).
15. Chen, T.-Y. et al. Field test of a practical secure communication network with decoy-state quantum cryptography. *Opt. Express* **17**, 6540 (2009).
16. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD network. *Opt. Express* **19**, 10387–10409 (2011).
17. Qiu, J. et al. Quantum communications leap out of the lab. *Nature* **508**, 441 (2014).
18. Liao, S.-K. et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501 (2018).
19. Koashi, M. & Preskill, J. Secure quantum key distribution with an uncharacterized source. *Phys. Rev. Lett.* **90**, 057902 (2003).

20. Ma, X., Fung, C.-H. F. & Lo, H.-K. Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76**, 012307 (2007).
21. Briegel, H.-J., Dur, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).
22. Yang, S.-J., Wang, X.-J., Bao, X.-H. & Pan, J.-W. An efficient quantum light–matter interface with sub-second lifetime. *Nat. Photon.* **10**, 381 (2016).
23. Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140 (2017).
24. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8**, 595 (2014).
25. 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).
26. Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686 (2010).
27. Zhao, Y., Fung, C.-H., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78**, 042333 (2008).
28. Weier, H. et al. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New J. Phys.* **13**, 073024 (2011).
29. Li, H.-W. et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* **84**, 062308 (2011).
30. Sajeed, S. et al. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Phys. Rev. A* **91**, 062301 (2015).
31. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880 (1969).
32. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *New J. Phys.* **11**, 045018 (2009).
33. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
34. Peng, C.-Z. et al. Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication. *Phys. Rev. Lett.* **94**, 150501 (2005).
35. Cao, Y. et al. Bell test over extremely high-loss channels: towards distributing entangled photon pairs between earth and the moon. *Phys. Rev. Lett.* **120**, 140405 (2018).
36. Ladd, T. D. et al. Quantum computers. *Nature* **464**, 45–53 (2010).

Methods

Implementation against device imperfections

In practice, the imperfections of realistic QKD implementations may introduce deviations (or side channels) from the idealized models used in the security analysis. Eve might exploit these imperfections and launch quantum attacks[24]. Our entanglement-based QKD implementation is designed and characterized to provide practical security against both known quantum attacks and potential future loopholes.

The entanglement-based QKD is naturally source-independent[2,19]. All we need is to consider the side channels properly at the detection stage. Here, we design a detection system, choosing apparatus under strict criteria for satisfying the underlying security assumptions, and performing careful characterizations to test those assumptions. We note that our implementation is based on trusted and characterized devices, that is, in a device-dependent scenario. The implementations are mostly common techniques, but we can maintain immunity to all known detection attacks, including: detector efficiency-mismatch attack[37], time-shift attack[27,38], detector-blinding attack[26,39], detector-damage attack[40], detector dead-time attack[28], wavelength-dependent attack[29], spatial-mode attack[30], and other possible side channels[24]. In Extended Data Table 3, we list the reported attacks against the detection, as well as our countermeasures to avert them. In the following, we will give a more detailed description.

Efficiency-mismatch attack. In practice, it is difficult to manufacture two SPDs with the same responses for different degrees of freedom. That is, practical SPDs present efficiency mismatch. With the efficiency mismatch, Eve can partially control which detector clicks by subtly sending desired signals to Bob[37]. For example, most of QKD systems use two gated avalanche photodiode detectors, which produce a time-dependent efficiency mismatch. Eve can perform a time-shift attack[27,38], by shifting the arrival time of each signal, so that Bob's detection results are biased depending on the time shift. Our strategy to counter the time-shift attack is that our detector works in free-running mode. We record all the detection events and post-select the detection windows such that the detection efficiency is guaranteed to be at a nominal level. For efficiency mismatch in other degrees of freedom[37], we use optical filters to filter out the input light and eliminate the mismatch in the frequency and spatial modes.

Detector-blinding attack. In the detector-blinding attack[26], Eve uses a continuous bright laser illumination to force SPDs to work in the linear mode. The SPDs are then no longer sensitive to single photons, and are converted into classical intensity detectors. Eve can control which detector clicks by sending Bob properly tailored classical pulses. In the laser damage attack[40], Eve can use a strong damaging laser illumination to change the properties of the SPDs completely. To counter the detector-blinding attack and the laser-damage attack, as illustrated in Extended Data Fig. 5, we install an additional circuit to monitor the anode of the load resistance in the detection circuit. We test the attack during the experiment by sending a bright laser pulse illumination. These results are shown in Fig. 3b. In normal operation (without blinding pulses), the output voltage of the monitoring circuit is below 1.2 V, corresponding to standard avalanching signals. At time $t \approx 0.2$ ms, Eve performs the blinding attack using 12 μW and a 2-μs-long laser pulse at a repetition rate of 100 kHz. The output of the monitoring circuit clearly exceeds 1.2 V, because a large current caused by the bright laser illumination passes through the load resistance. Consequently, we could set a secure threshold on the voltage of monitoring circuit: if the voltage is higher than the threshold, it exposes the blinding attack.

Detector dead-time attack. The basic principle of this attack is the dead-time effect of a SPD[28]. After a detection event, a detector does not respond to the incoming photons during a time window ranging from several nanoseconds to tens of microseconds. If Bob has a detection event during a time period when one detector is in the dead-time period, while the other one is active, Eve could easily infer which detector has a click. Our detector works in the free-running mode, and all detection events are collected. The countermeasure is that we monitor the status of the detectors and use only those detection events for which all detectors are active to generate keys.

Beam-splitter attack. In a polarization-based QKD system, Bob typically exploits an 1×2 beam splitter to passively choose the measurement basis. In the standard case, a photon will randomly pass through the beam splitter, thus randomly selecting a rectilinear basis or a diagonal basis. However, in practice, the splitting ratio of the beam splitter is wavelength-dependent, that is, the centre wavelength has a coupling ratio of 50:50, whereas the coupling ratio varies for other wavelengths. Consequently, Eve can control the measurement basis by sending Bob photons with different wavelength[29]. To avoid this attack, we use broad-bandwidth and narrow-bandwidth wavelength filters to filter the input light on Bob's station. The characterizations of these two filters are shown in Fig. 3a. The beam splitter ratio within the filtered bandwidth is characterized in Extended Data Fig. 6.

Spatial-mode attack. In a free-space QKD system, the detector has different sensitivities for different spatial-mode photons, especially when the detector is coupled with a multi-mode fibre. Eve could exploit the spatial-mode efficiency mismatch and perform the spatial-mode attack[30]. To counter this attack, we place a spatial filter in front of the beam splitter to make the efficiencies of different detection paths uniform. With the spatial filter, the characterization of the detection efficiency in spatial domain is shown in Fig. 3c.

In general, the practical security of implementation is essentially guaranteed by the fair-sampling assumption. The countermeasures to the abovementioned attacks comprise the use of active components to guarantee the fair-sampling assumption. In the frequency mode, broad-band and narrow-band frequency filters are employed to filtering the input light. In the temporal mode, free-running detectors are applied to post-select the time windows of detection events. In the spatial mode, spatial filters are placed before the collimating lens of measurement devices. In polarization mode, we use the polarization encoding for QKD, thus monitoring the QBER to ensure the security. In future, we may also combine our entanglement-based QKD system with the measurement-device-independent QKD protocol[41] to make detection immune to all detector attacks.

Security analysis

The main goal of our security analysis is to calculate the practical security rate by considering the issues of the finite-key size and device imperfections. We remark that our security analysis is for entanglement-based QKD with trusted and characterized devices, that is, in a device-dependent scenario[42]. We start with a security proof for an ideal QKD protocol by following the Shor–Preskill security proof[43]. We then extend the security analysis to the practical case of the finite-key effect by using the approach of uncertainty relation for smooth entropies[33]. Finally, we extend the analysis to address the security issues of device imperfections by using the Gottesman–Lo–Lütkenhaus–Preskill (GLLP) framework[44].

Ideal QKD refers to the case where an infinite number of signals are generated and the devices to run the QKD protocol are as perfect as described by theoretical models. The security proof for ideal QKD was established in the early 2000s by Mayers[45], Lo and Chau[46] and Shor and Preskill[43].

Shor and Preskill employed the idea of the Calderbank–Shor–Steane quantum error correcting code to provide a simple framework for security proof. In an entanglement-based QKD such as the BBM92 protocol[3], when Alice and Bob both measure quantum signals in the Z

basis, an error may occur when the outcomes are different. We can call it a bit error. The phase error can be defined as the hypothetical error if those quantum signals were measured in the basis complementary to the Z basis. In the Shor–Preskill security proof, the bit error correction is classical error correction and the phase error correction is PA. The crucial part is to perform the PA, in which one needs to estimate the phase error rate. For the key bits measured in the Z basis, the phase error rate can be estimated by measuring the key bits in the X basis. The Z-basis security rate for ideal QKD is given by

$$R_Z \geq Q_Z[1 - H(E_Z) - H(E_X)]$$

where Q_Z is the sifted key rate per signal in which both Alice and Bob select the Z basis, E_Z and E_X are the QBER in the Z and X bases, and $H(\chi) = -\chi\log_2\chi - (1-\chi)\log_2(1-\chi)$. Similarly, secret keys can also be generated in the X basis, and the analysis for the rate R_X is the same. The total ideal key rate is $R_A = R_Z + R_X$. Note that an entangled source is basis-independent (or uncharacterized), and the security proof for QKD with an uncharacterized source is given in ref. [19].

We remark that in order for a successful estimation of PA, one needs to make sure the sampling in the complementary basis is fair, which in practical realizations raises two major issues: the finite-key effect (that is, statistical fluctuations) and device imperfections (that is, violating the fair sampling), discussed below.

Finite-key analysis

We first define the security in the finite-key scenario with the composable security definition framework[47,48]. A secure key should satisfy two requirements. First, the key bit strings possessed by Alice and Bob need to be identical, that is, to be correct. Second, from the view of anyone other than Alice and Bob, say Eve, the key bit string should be uniformly distributed, that is, should be secret. Practical issues, such as the finite data size and non-ideal error correction, mean that Alice and Bob cannot generate an ideal key via QKD. In reality, it is reasonable to allow the key to have small failure probabilities, ε_{cor} and ε_{sec}, for correctness and secrecy. We say that the QKD protocol is ε-secure with $\varepsilon \geq \varepsilon_{cor} + \varepsilon_{sec}$, if it is ε_{cor}-correct and ε_{sec}-secret[48]. Specifically, we define k_a and k_b to be the key bit strings obtained by Alice and Bob. A QKD protocol is defined to be ε_{cor}-correct if the probability satisfies $\Pr(k_a \neq k_b) \leq \varepsilon_{cor}$. A QKD protocol is defined in trace distance to be ε_{sec}-secret, if $[(1-P_{abort})/2]\|\rho_{AE} - U_A \otimes \rho_E\| \leq \varepsilon_{sec}$, where ρ_{AE} is the classical quantum state describing the joint state of k_a and Eve's system ρ_E, U_A is the uniform mixture of all possible values of k_a, and P_{abort} is the probability that the protocol aborts.

There are two main approaches to analyse the finite-key security of QKD: one is based on smooth min/max entropy[33,48] and the other one is based on complementarity[32]. Recently, these two approaches have been proved to be unified[49]. The estimation of the phase error rate is the most important part of the Shor–Preskill security analysis. Owing to statistical fluctuations in the finite-key case, the phase error rate used for evaluating the amount of PA cannot be measured accurately. Instead, Alice and Bob can bound the phase error rate via certain complementary measurements[32,33]. Specifically, for the Z-basis security key in entanglement-based QKD, Alice and Bob can bound the underlying phase error rate E_X' by sampling the qubits in the X basis. This is a typical random sampling problem. We can use the Serfling inequality[50] to estimate the probability that the average error on the sample deviates from the average error on the total string[51]. We obtain the upper bound for E_X' as

$$E_X' \leq E_X + \sqrt{\frac{(n_X+1)\log(1/\varepsilon_{sec})}{2n_X(n_X+n_Z)}}$$

where n_Z and n_X are the number of coincident counts in the Z and X bases.

By using the approach of the uncertainty relation for smooth entropies[33], the Z-basis secret key length l_Z is given by

$$l_Z = n_Z - n_Z H\left[E_X + \sqrt{\frac{(n_Z+1)\log\left(\frac{1}{\varepsilon_{sec}}\right)}{2n_X(n_X+n_Z)}}\right] - f_e n_Z H(E_Z) - \log\frac{2}{\varepsilon_{cor}\varepsilon_{sec}^2}.$$

Similarly, the X-basis finite-key secret key length l_X can be calculated, and the total key length is $l = l_Z + l_X$.

Security proof for imperfect devices

In practice, owing to device imperfections, there exist deviations between realistic QKD systems and the ideal QKD protocol[24]. To achieve practical security in a QKD system, Alice and Bob need to characterize these imperfections carefully and take them into account in the practical security analysis. Notably, a general framework for security analysis with realistic devices was established in ref. [44]. In this framework, Alice and Bob need to characterize their devices to see how much deviation there is from the ideal ones assumed in the security proofs. One can employ typical distance measures, like fidelity and trace distance, to quantify the deviation, and then consider this deviation in PA.

Our entanglement-based QKD is source-independent, which ensures that the imperfections in the source can be ignored. All we need is to carefully characterize the imperfections in the detection side. In general, the (known and to be known) side channels on the detection side[26–30,38–40] primarily violate the key assumption of fair sampling. We perform implementations by following the squashing model[44] to guarantee the fair sampling assumption. In a squashing model, an arbitrary quantum state (from the channel) is first projected to a two-dimensional subspace before the Z and X measurements. So, we implement a series of single-mode filters in different degrees of freedom, including the frequency, spatial and temporal modes. Nonetheless, practical filters normally have finite bandwidth, which will cause small deviations for detection efficiencies, that is, a detection efficiency mismatch[52,53]. Our security proof for imperfect devices will primarily consider the deviation of the detection efficiency, and analyse this imperfection into the PA by following the GLLP framework[44].

We assume the lower bound of detection efficiency is η_0, so the detection efficiency of the ith detector can be written as $\eta_0(1+\delta_i)$, where δ_i quantifies the deviation of efficiency. Suppose that if we can add attenuation with transmittance $1/(1+\delta_i)$ just before the ith detector, then we would obtain equal efficiency for all detectors. In doing so, the number of Z-bits (or X-bits) will be reduced by a fraction, upper bounded by $\Delta = 1 - 1/(1+\delta)^2$. In our experiment, we quantify that δ_i is upper bounded by $\delta_i \leq 1.47\%$ (see Extended Data Table 1). This deviation can be considered in PA, that is, the estimation of phase error rate as $E_X'/(1-\Delta)$ (ref. [44]). Overall, after considering the finite-key size effect and the efficiency deviation, the secret key length L_Z is given by:

$$L_Z = n_Z - n_Z H\left[\frac{E_X + \sqrt{\frac{(n_Z+1)\log\left(\frac{1}{\varepsilon_{sec}}\right)}{2n_X(n_X+n_Z)}}}{1-\Delta}\right] - f_e n_Z H(E_Z) - n_Z\Delta - \log\frac{2}{\varepsilon_{cor}\varepsilon_{sec}^2}.$$

The analysis of the secret key length L_X for the key bits in the X basis is the same. The total finite-key length is $L = L_Z + L_X$.

Data availability

The data that support the findings of this study are available from the corresponding authors on reasonable request.

37. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74**, 022313 (2006).
38. Qi, B., Fung, C.-H.F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput*. **7**, 73 (2007).
39. Gerhardt, I. et al. Experimentally faking the violation of Bell's inequalities. *Phys. Rev. Lett*. **107**, 170404 (2011).
40. Bugge, A. N. et al. Laser damage helps the eavesdropper in quantum cryptography. *Phys. Rev. Lett*. **112**, 070503 (2014).
41. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett*. **108**, 130503 (2012).
42. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys*. **81**, 1301–1350 (2009).
43. Shor, P. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett*. **85**, 441 (2000).
44. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput*. **4**, 325 (2004).
45. Mayers, D. J. Unconditional security in quantum cryptography. *J. Assoc. Comput. Mach*. **48**, 351–406 (2001).
46. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050 (1999).
47. Ben-Or, M., Horodecki, M., Leung, D. W., Mayers, D. & Oppenheim, J. In *Proc. 2nd Int. Conf. on Theory of Cryptography (TCC'05)* 386–406 (Springer, 2005).
48. Renner, R. *Security of quantum key distribution. PhD thesis*, ETH Zurich (2005); preprint at https://arxiv.org/abs/quant-ph/0512258.
49. Tsurumaru, T. Leftover hashing from quantum error correction: unifying the two approaches to the security proof of quantum key distribution. Preprint at https://arxiv.org/abs/1809.05479 (2018).
50. Serfling, R. J. Probability inequalities for the sum in sampling without replacement. *Ann. Stat*. **2**, 39–48 (1974).
51. Curty, M. et al. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun*. **5**, 3732 (2014).
52. Fung, C.-H. F., Tamaki, K., Qi, B., Lo, H.-K. & Ma, X. Security proof of quantum key distribution with detection efficiency mismatch. *Quantum Inf. Comput*. **9**, 131–165 (2009).
53. Marøy, Ø., Lydersen, L. & Skaar, J. Security of quantum key distribution with arbitrary individual imperfections. *Phys. Rev. A* **82**, 032337 (2010).

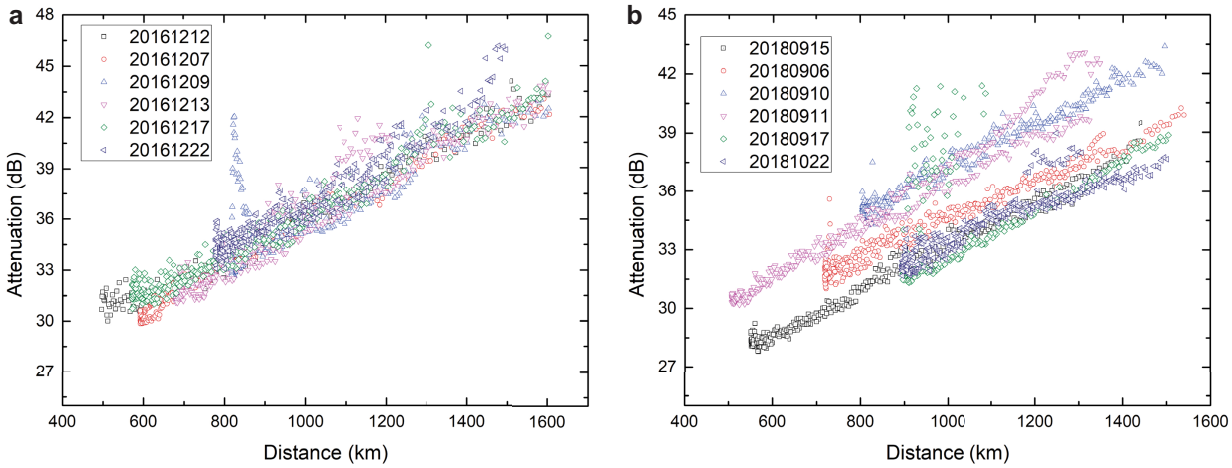
Acknowledgements We acknowledge discussions with X. Ma and C. Jiang. We thank colleagues at the National Space Science Center, China Xi'an Satellite Control Center, National Astronomical Observatories, Xinjiang Astronomical Observatory, Purple Mountain Observatory, and Qinghai Station for their management and coordination. We thank G.-B. Li, L.-L. Ma, Z. Wang, Y. Jiang, H.-B. Li, S.-J. Xu, Y.-Y. Yin, W.-C. Sun and Y. Wang for their long-term assistance in observation. This work was supported by the National Key R&D Program of China (grant number 2017YFA0303900), the Shanghai Municipal Science and Technology Major Project (grant number 2019SHZDZX01), the Anhui Initiative in Quantum Information Technologies, Science and Technological Fund of Anhui Province for Outstanding Youth (grant number 1808085J18) and the National Natural Science Foundation of China (grant numbers U1738201, 61625503, 11822409, 11674309, 11654005 and 61771443).

Author contributions C.-Z.P., A.K.E. and J.-W.P. conceived the research. J.Y., C.-Z.P. and J.-W.P. designed the experiments. J.Y., Y.-H.L., S.-K.L., M.Y., Y.C., J.-G.R., S.-L.L., C.-Z.P. and J.-W.P. developed the follow-up optics and monitoring circuit. J.Y., Y.-M.H., C.-Z.P. and J.-W.P. developed the efficiency telescopes. J.Y., S.-K.L., Y.C., L.Z., W.-Q.C., R.S., L.D., J.-Y.W., C.-Z.P. and J.-W.P. designed and developed the satellite and payloads. J.Y., L.Z., W.-Q.C., W.-Y.L. and C.-Z.P. developed the software. F.X., X.-B.W., A.K.E. and J.-W.P. performed the security proof and analysis. L.L., Q.Z., N.-L.L., Y.-A.C., X.-B.W., F.X., C.-Z.P., A.K.E. and J.-W.P. contributed to the theoretical study and implementation against device imperfections. F.X., C.-Y.L., C.-Z.P. and J.-W.P. analysed the data and wrote the manuscript, with input from J.Y., Y.-H.L., M.Y., Y.C. and A.K.E. All authors contributed to the data collection, discussed the results and reviewed the manuscript. J.-W.P. supervised the whole project.

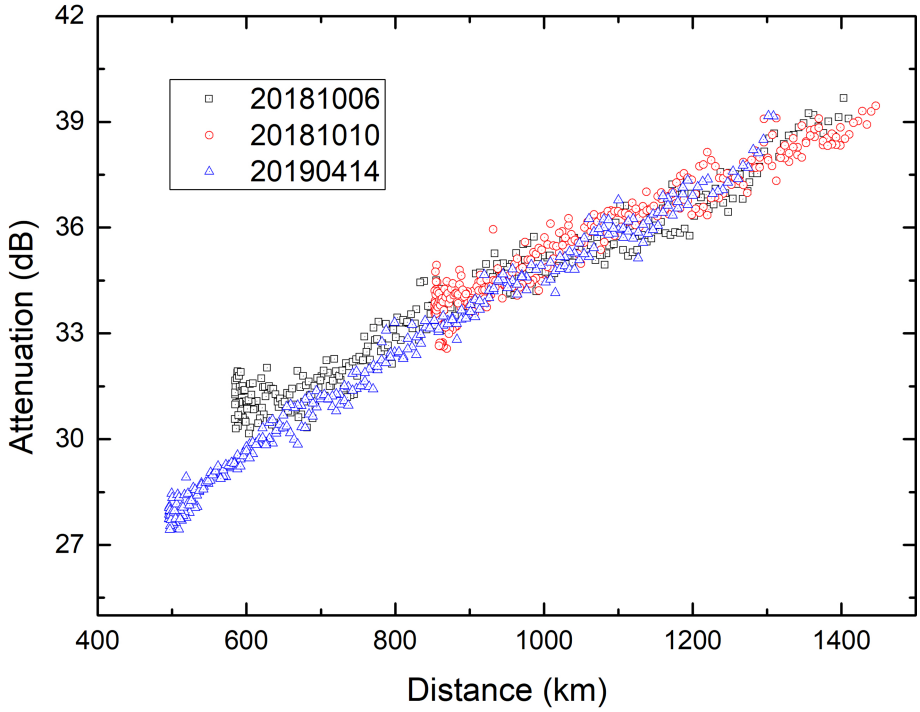
Competing interests The authors declare no competing interests.

Additional information

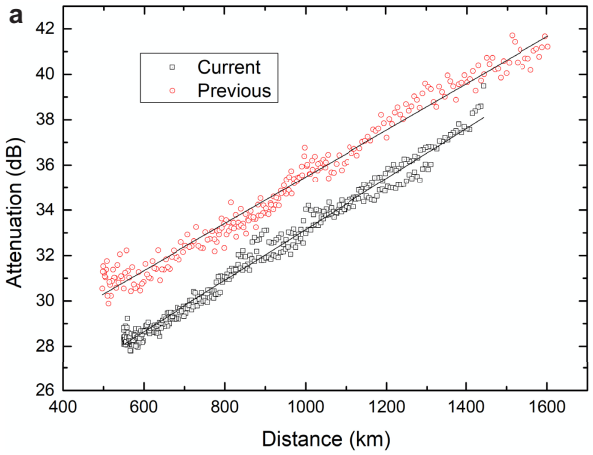
Correspondence and requests for materials should be addressed to J.-W.P. or C.-Z.P.



Extended Data Fig. 1 | Satellite-to-Delingha link efficiencies under different weather conditions. a, The data in previous work[23] was taken in different orbits during the period of 7 December 2016 to 22 December 2016. **b**, The data in current work was taken in different orbits during the period of 6 September 2018 to 22 October 2018. Here the change of link efficiencies on different days was caused by the weather conditions.



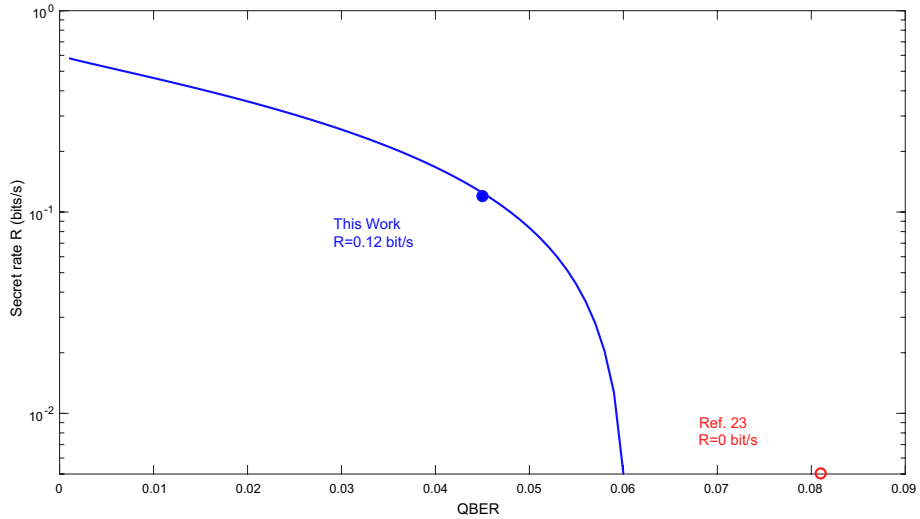
Extended Data Fig. 2 | Multiple orbits of satellite-to-Delingha link efficiencies under good weather conditions. Stable and high collection efficiencies were observed during the period of October 2018 to April 2019.



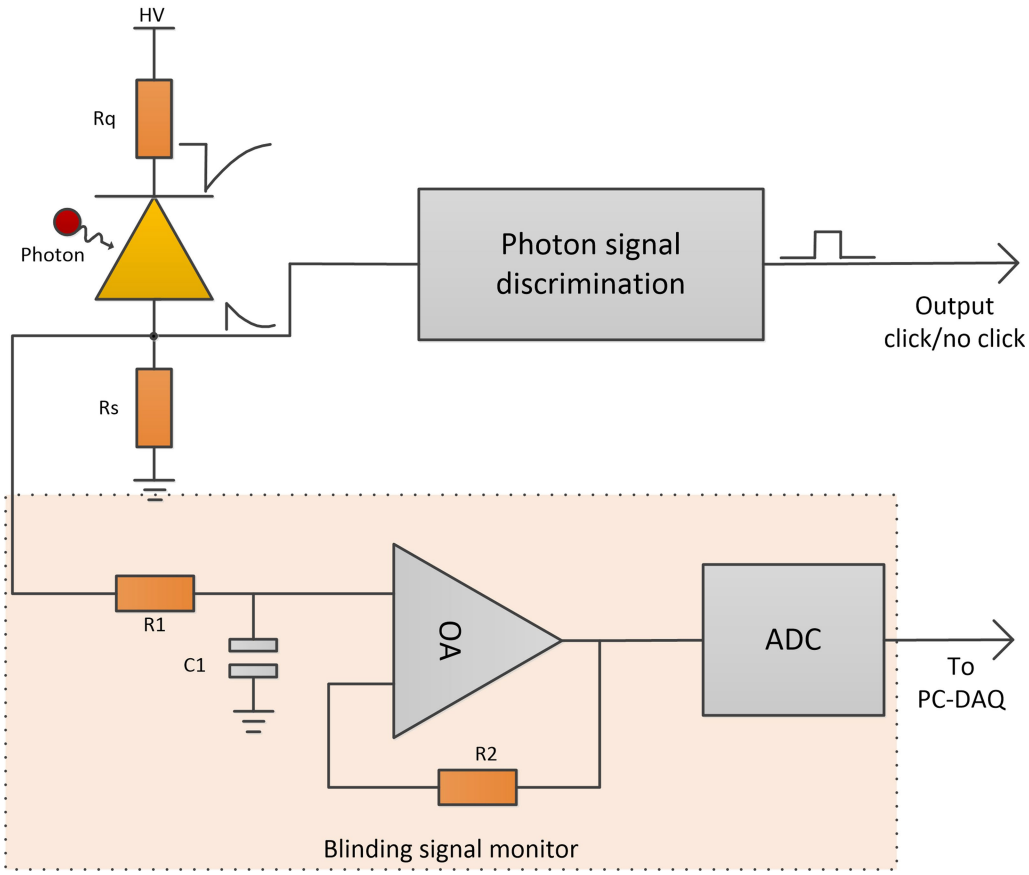
b

Distance (km)	Previous (dB)	Current (dB)	Improvement (dB)
600	31.63 ± 0.04	28.63 ± 0.03	3.00 ± 0.05
800	33.56 ± 0.06	30.94 ± 0.04	2.62 ± 0.07
1000	35.96 ± 0.07	32.97 ± 0.05	2.99 ± 0.09
1200	37.21 ± 0.08	34.84 ± 0.06	2.37 ± 0.1

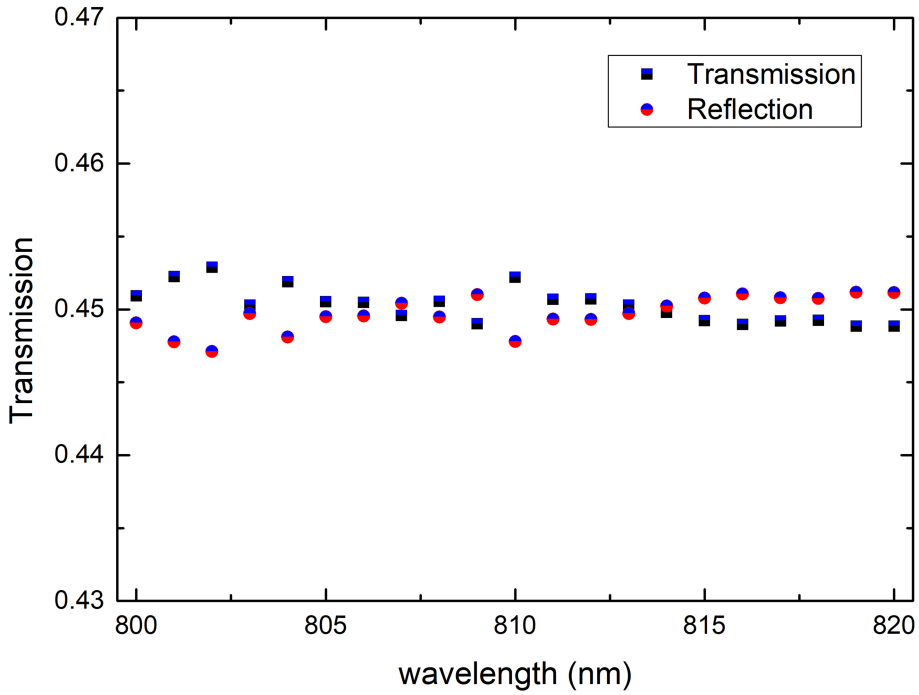
Extended Data Fig. 3 | The comparison of satellite-to-Delingha link efficiency under the best-orbit condition. a, After improving the link efficiency with high-efficiency telescopes and follow-up optics, on average, the current work shows a 3-dB enhancement in the collection efficiency over that of ref. [23]. The lines are linear fits to the data. **b**, Some representative values.



Extended Data Fig. 4 | The finite-key secret key rate *R* versus the QBER. For the 3,100 s of data collected in our experiment, a QBER of below about 6.0% is required to produce a positive key. The previous work[23] demonstrated a QBER of 8.1%, which is not sufficient to generate a secret key. In this work, a QBER of 4.5% and a secret key rate of 0.12 bits per second are demonstrated over 1,120 km. If one ignores the important finite-key effect, the QBER in ref. [23] is slightly lower than the well known asymptotic limit of 11% (ref. [43]).



Extended Data Fig. 5 | Schematics of the detection and blinding-attack monitoring circuit. The biased voltage (HV) is applied to an avalanche photodiode through a passive quenching resistance (R_q = 500 kΩ) and a sampling resistance (R_s = 10 kΩ). The avalanche signals are read out as click or no-click events through a signal-discrimination circuit. The blinding signal monitor is shown in the dot-dash diagram. A resistor-capacitor filter and a voltage follower are used to smooth and minimize the impact on the signals. The outputs of an analogue to digital converter (ADC), at a sampling rate of 250 kHz, are registered by computer data acquisition (PC-DAQ). R1, resistor; C1, capacitor; OA, operational amplifier.



Extended Data Fig. 6 | The transmission of the beam splitter within the selected bandwidth of wavelength.

Extended Data Table 1 | Parameters of the system detection efficiencies

Serial number	Current (A)	Dark counts (cps)	Efficiency (%)
B5213	0.956	55	53.31
B4973	0.9	207	53.64
B4976	1.064	60	53.16
B5214	0.984	55	53.16
B4972	0.966	32	53.78
B4974	0.929	55	53
B4977	1.067	64	53.16
B4978	0.965	26	53.16

cps, counts per second.

Extended Data Table 2 | Comparison of the results between this work and the earlier experiment[23]

	Time (orbit)	Coincidence counts	Fidelity	QBER	S
Earlier experiment [23]	250s (1)	268	0.869 ± 0.085	6.55% ± 4.25% (estimate)	
	1059s (6)	1167	--	8.10% ± 1.59% (estimate)	2.37 ± 0.09
This work	226s (1)	1021	--	4.74% ± 1.23% (estimate)	2.56 ± 0.07
	3100s	6200	0.910 ± 0.007 (estimate)	4.51% ± 0.37%	--

S, Bell parameter.

Extended Data Table 3 | Typical quantum attacks and our countermeasures

Attack	Brief Description	Countermeasure
Detector efficiency mismatch[27, 37, 38]	Eve exploits efficiency mismatch to control detectors	Free-running detectors
Detector blinding[26, 39]	Eve manipulates the detectors by sending bright light	Monitoring electronics
Detector damage[40]	Eve sends ultra-strong light to damage the detectors	Monitoring electronics
Detector dead-time[28]	Eve controls the detector by exploiting dead time	Free-running detectors
Beam-splitter[29]	Beam-splitter ratio is wavelength-dependent	Frequency filter
Spatial-mode[30]	Detectors have efficiency mismatch in spatial domain	Spatial filter

Data are from refs. [26–30,37–40].

Extended Data Table 4 | Measured correlation coefficients required for the CHSH inequality

E (φ_1, φ_2)	(0°, 22.5°)	(0°, 67.5°)	(45°, 22.5°)	(45°, 67.5°)
Value	-0.700	0.612	-0.700	-0.544
Deviation	0.0415	0.046	0.047	0.060

E, joint polarization correlation; φ_1 and φ_2, measurement angles of Delingha and Nanshan ground stations, respectively.