doi:10.1038/nature23655

Satellite-to-ground quantum key distribution

Sheng-Kai Liao[1,2], Wen-Qi Cai[1,2], Wei-Yue Liu[1,2], Liang Zhang[2,3], Yang Li[1,2], Ji-Gang Ren[1,2], Juan Yin[1,2], Qi Shen[1,2], Yuan Cao[1,2], Zheng-Ping Li[1,2], Feng-Zhi Li[1,2], Xia-Wei Chen[1,2], Li-Hua Sun[1,2], Jian-Jun Jia[3], Jin-Cai Wu[3], Xiao-Jun Jiang[4], Jian-Feng Wang[4], Yong-Mei Huang[5], Qiang Wang[5], Yi-Lin Zhou[6], Lei Deng[6], Tao Xi[7], Lu Ma[8], Tai Hu[9], Qiang Zhang[1,2], Yu-Ao Chen[1,2], Nai-Le Liu[1,2], Xiang-Bin Wang[2], Zhen-Cai Zhu[6], Chao-Yang Lu[1,2], Rong Shu[2,3], Cheng-Zhi Peng[1,2], Jian-Yu Wang[2,3] & Jian-Wei Pan[1,2]

Quantum key distribution (QKD) uses individual light quanta in quantum superposition states to guarantee unconditional communication security between distant parties. However, the distance over which QKD is achievable has been limited to a few hundred kilometres, owing to the channel loss that occurs when using optical fibres or terrestrial free space that exponentially reduces the photon transmission rate. Satellite-based QKD has the potential to help to establish a global-scale quantum network, owing to the negligible photon loss and decoherence experienced in empty space. Here we report the development and launch of a low-Earth-orbit satellite for implementing decoy-state QKD—a form of QKD that uses weak coherent pulses at high channel loss and is secure because photon-number-splitting eavesdropping can be detected. We achieve a kilohertz key rate from the satellite to the ground over a distance of up to 1,200 kilometres. This key rate is around 20 orders of magnitudes greater than that expected using an optical fibre of the same length. The establishment of a reliable and efficient space-to-ground link for quantum-state transmission paves the way to global-scale quantum networks.

Private and secure communication is of fundamental importance in the modern world. Traditional public-key cryptography relies on the computational intractability of certain mathematical functions. In contrast, QKD[1]—which was proposed in the mid-1980s and is the best known example of a task involving quantum cryptography—provides an information-secure solution to the key exchange problem, ensured by the laws of quantum physics. QKD enables two distant users who do not initially share any information to produce a common, random string of secret bits, called a secret key. Using one-time-pad encryption, this key provides a provably secure[2] way of encrypting (and decrypting) a message, which can then be transmitted over a standard communication channel. In QKD, the information is encoded in the superposition states of physical carriers at the single-quantum level; as the fastest-travelling qubits, and owing to their intrinsic robustness to decoherence and the ease with which they can be controlled, photons are usually used as the physical carriers. Any eavesdropper on the quantum channel attempting to gain information about the key will inevitably introduce disturbances into the system, and so can be detected by the communicating users.

Since the first table-top QKD experiment[3] in 1989, with a quantum channel distance of 32 cm, much research has been devoted to achieving secure QKD over long distances, with the ultimate aim being global-scale secure QKD for practical use. The most straightforward method of QKD is sending single photons through optical fibres or terrestrial free-space directly. However, in both of these cases channel loss causes a decrease in the number of transmitted photons that scales exponentially with the length over which they are transmitted. Unlike classical telecommunications, the quantum signal in QKD cannot be noiselessly amplified, owing to the quantum non-cloning theorem[4], limiting the maximum distance for secure QKD to a few hundred kilometres[5]. Beyond this length scale, quantum communications become extremely challenging[6].

One solution to this problem is to use quantum repeaters[7] that combine entanglement swapping[8], entanglement purification[9] and quantum memories[10]. But despite remarkable progress in demonstrations of the three building blocks[11–13] and even prototype quantum repeater nodes[14–18], these laboratory technologies are still far from being applicable in practical long-distance quantum communications.

A more direct and promising solution for global-scale QKD involves satellites in space. Compared with terrestrial channels, the satellite-to-ground connection has greatly reduced losses[19]. This is mainly because the effective thickness of the atmosphere is only about 10 km, and most of the propagation path of the photons is in empty space with negligible absorption and turbulence. A ground test[20] in 2004 demonstrated the distribution of entangled photon pairs over a noisy near-ground atmosphere of 13 km—greater than the effective thickness of the atmosphere—and showed the survival of entanglement and a violation of Bell's inequality. Under the simulated conditions of huge attenuation and various types of turbulence, the feasibility of satellite-based QKD has been further verified over even longer distances[21–23], on rapidly moving platforms[24,25] and using satellite corner-cube retroreflectors[26,27].

We developed a sophisticated satellite, 'Micius', dedicated for quantum science experiments, which was successfully launched on 16 August 2016 from Jiuquan, China, and now orbits at an altitude of about 500 km (Fig. 1a; see Methods for the project timeline and design details). Using one of the satellite payloads—a decoy-state QKD transmitter at a wavelength of 850 nm—and cooperating with Xinglong ground observatory station (near Beijing, 40° 23′ 45.12″ N, 117° 34′ 38.85″ E, altitude of 890 m), we establish decoy-state QKD with

[1]Department of Modern Physics and Hefei National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Hefei 230026, China. [2]Chinese Academy of Sciences (CAS) Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China. [3]Key Laboratory of Space Active Opto-Electronic Technology, Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai 200083, China. [4]National Astronomical Observatories, Chinese Academy of Sciences, Beijing 100012, China. [5]Key Laboratory of Optical Engineering, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China. [6]Shanghai Engineering Center for Microsatellites, Shanghai 201203, China. [7]State Key Laboratory of Astronautic Dynamics, Xi'an Satellite Control Center, Xi'an 710061, China. [8]Xinjiang Astronomical Observatory, Chinese Academy of Sciences, Urumqi 830011, China. [9]National Space Science Center, Chinese Academy of Sciences, Beijing 100190, China.

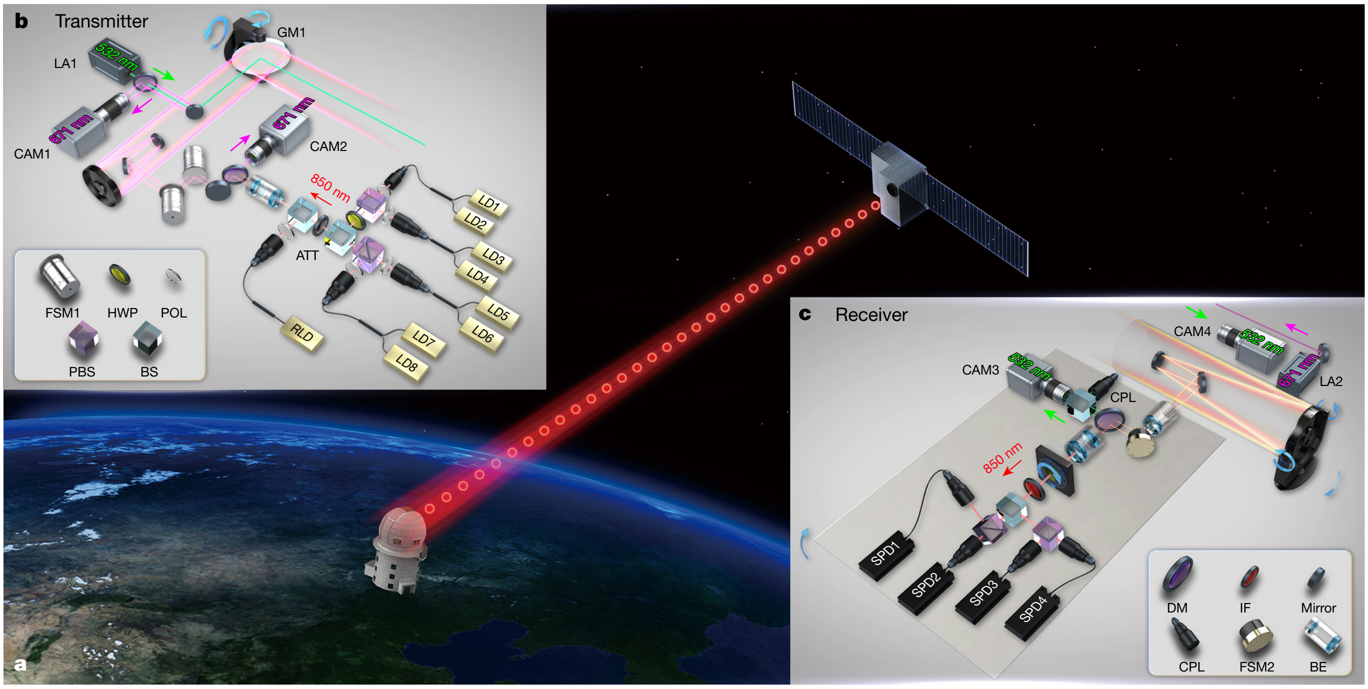


Figure 1 | Illustration of the experimental set-up. a, Overview of the satellite-to-ground quantum key distribution (QKD). The Micius satellite, weighing 635 kg, flies along a Sun-synchronous orbit at an altitude of around 500 km. It is equipped with three payloads, designed and tested to be suitable for operation in low-Earth orbit and to enable a series of space-to-ground-scale quantum experiments including QKD, a Bell test and teleportation. **b**, Schematic of the decoy-state QKD transmitter, one of the satellite's payloads. Attenuated laser pulses (with wavelengths of about 850 nm) from eight separate laser diodes (LD1–LD8) pass through a BB84 encoding module, which consists of two polarizing beam splitters (PBSs), a half-wave plate (HWP) and a beam splitter (BS). The resultant beam is then co-aligned with a green laser beam (LA1; 532 nm) for system tracking and time synchronization, and sent out through a 300-mm-aperture Cassegrain telescope. After the BB84 module, an approximately 5-μW laser is used as a polarization reference. A two-axis gimbal mirror (GM1) in the output of the telescope and a large-field-of-view camera (CAM1) are combined to control the coarse-tracking loop. Two fast steering mirrors (FSM1s) and a fast camera (CAM2) are used for fine tracking. ATT, attenuator; POL, polarizer; RLD, polarization reference laser diode; both cameras (CAM1 and CAM2) detect 671-nm light. **c**, Schematic of the decoy-state QKD decoder at the Xinglong ground station, which is equipped with a 1,000-mm-aperture telescope. The received 532-nm-wavelength laser is separated by a dichromic mirror (DM) and split into two paths: one is imaged by a camera (CAM3, which detects 532-nm light) for tracking and the other is detected for time synchronization. The 850-nm-wavelength decoy-state photons are analysed by a BB84 decoder, which consists of a beam splitter and two polarizing beam splitters, and detected by four single-photon detectors (SPD1–SPD4). The ground station sends a red laser (LA2; 671 nm) beam to the satellite for system tracking. IF, interference filter; BE, beam expander; CPL, coupler; both cameras (CAM3 and CAM4) detect 532-nm light. See Extended Data Table 1 for more technical parameters.

polarization encoding from the satellite to the ground with a kilohertz key rate over a distance of up to 1,200 km.

Experimental challenges and solutions

Robust and efficient satellite-to-ground QKD places a more stringent requirement on the efficiency of the link than do conventional satellite-based classical communication systems. To obtain a high signal-to-noise ratio, one cannot increase the signal power, only reduce the channel attenuation and background noise. In our experiment, several effects contribute to channel loss, including beam diffraction, pointing error, atmospheric turbulence and absorption.

In our QKD experiment, we adopt the downlink protocol—from the satellite to the ground (see Fig. 1a). In the downlink, beam wandering caused by atmospheric turbulence occurs at the very end of the transmission path (near the surface of Earth), where the beam size due to diffraction is typically much larger than the beam wandering. Therefore, the downlink has reduced beam spreading compared to the uplink and thus higher link efficiency.

The beam diffraction depends mainly on the size of the telescope. To narrow the beam divergence, we use a 300-mm-aperture Cassegrain telescope in the satellite (Fig. 1b), optimized to eliminate chromatic and spherical aberrations; this telescope sends the light beam with a near-diffraction-limited far-field divergence of about 10 μrad. After travelling a distance of 1,200 km, we expect that the beam diameter expands to about 12 m. At the ground station, a Ritchey–Chretien telescope with an aperture of 1 m and a focal length of 10 m (Fig. 1c) is used to receive the QKD photons (see Methods). The diffraction loss is estimated to be 22 dB at 1,200 km.

The narrow divergence beam from the fast-moving satellite (speed of about 7.6 km s^{-1}) necessitates a high-bandwidth and high-precision acquiring, pointing and tracking (APT) system to establish a stable link. We designed cascaded multi-stage APT systems in the transmitter (Fig. 1b) and the receiver (Fig. 1c). Initial coarse orientation of the telescope is based on the forecasted orbital position of the satellite, with an uncertainty of less than 200 m. The satellite's attitude control system ensures that the transmitter is pointing to the ground station with a precision of approximately 0.5°. The satellite and the ground station send beacon lasers to each other with a divergence of 1.25 mrad (satellite to ground) and 0.9 mrad (ground to satellite) (Fig. 2a). The coarse pointing stage in the satellite transmitter consists of a two-axis gimbal mirror (with a range of 10° in both azimuth and elevation) and a complementary metal–oxide semiconductor (CMOS) camera with a field-of-view of 2.3° × 2.3° and frame rates of 40 Hz. The fine pointing stage uses a fast-steering mirror driven by piezo ceramics (with a tracking range of 1.6 mrad) and a camera with a field-of-view of 0.64 mrad × 0.64 mrad and frame rates of 2 kHz. Similar coarse and fine APT systems are also installed in the ground station (see Extended Data Table 1 for details). Using closed-loop feedback, the transmitter achieves a tracking accuracy of approximately 1.2 μrad (Fig. 2b), much smaller than the beam divergence. We estimate that at 1,200 km the loss due to atmospheric absorption and turbulence is 3–8 dB and that due to pointing error is less than 3 dB.

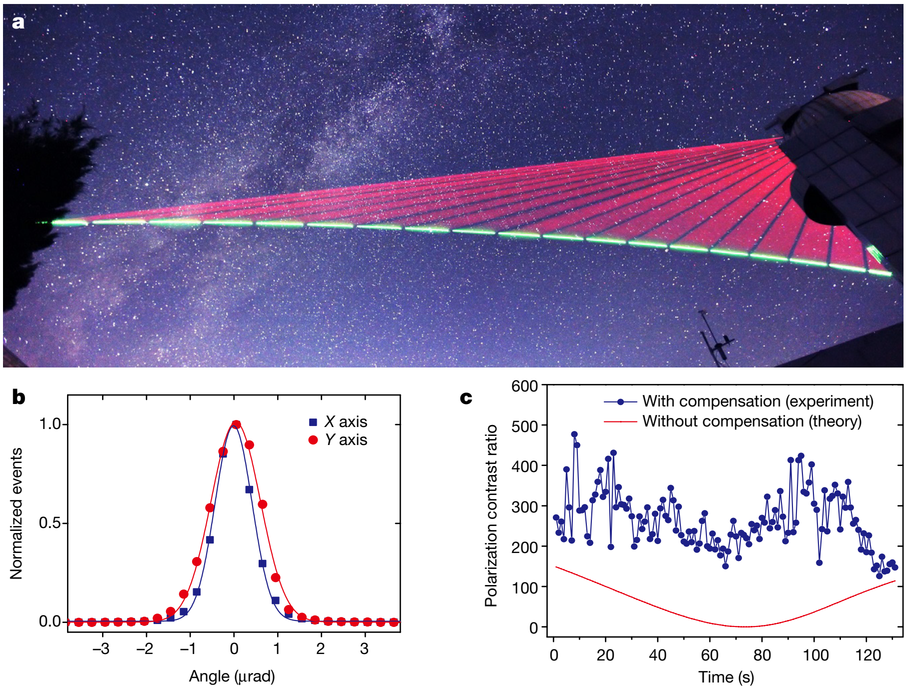


Figure 2 | Establishing a reliable space-to-ground link for quantum state transfer. a, Overlaid and time-lapse photographs of tracking laser beams as the satellite flies over the Xinglong ground station. The red and green lasers are sent from the ground and the satellite, respectively, with a divergence of 0.9–1.25 mrad. **b**, Distribution of long-time tracking error (shown as the number of detected events normalized by the maximum count in each bin) of the *X* and *Y* axes extracted from the real-time images read out from the fast camera. **c**, Polarization contrast ratio with (corresponding to our experiment) and without (determined theoretically) dynamical compensation during one orbit.

We use temporal and spectral filtering to suppress the background noise. The beacon laser, with a pulse width of 0.9 ns and a repetition rate of about 10 kHz, is used for both APT and synchronization. In good co-alignment with the QKD photons, the beacon laser can be separated by a dichroic mirror and detected by a single-photon detector in the ground station to obtain timing information. We thus avoid the space–ground clock drift, obtaining a synchronization jitter of 0.5 ns, which is used to tag the received signal photons within a 2-ns time window and filter out the background noise. In addition, we use a bandwidth filter in the receiver to reduce the background scattering. In the current experiment, we limit ourselves to night-time operation to avoid sunlight.

Finally, the relative motion of the satellite and the ground station induces a time-dependent rotation of the photon polarization seen by the receiver. We predict theoretically that the polarization contrast ratio would decrease from 150:1 to 0 during one orbit (Fig. 2c). To solve this problem, we calculate rotation angle offset by taking into account the relative motion of the satellite and the ground station and all of the birefringent elements in the optical path. Using a motorized half-wave plate for dynamical polarization compensation during the satellite passage, the average polarization contrast ratio increases to 280:1 (Fig. 2c).

Experimental procedure and results

We use the decoy-state[28,29] Bennett–Brassard 1984 (BB84)[1] protocol for QKD, which can detect photon-number-splitting eavesdropping and thus enable secure QKD using weak coherent pulses over very large distances and with very high key rates. The main idea is to use multiple intensity levels at the source of the transmitter: one signal state (the mean photon number μ_s) and several randomly interspersed decoy states (μ_1, μ_2, …). Here we use a protocol with three intensity levels: high μ_s, moderate μ_1 and zero μ_2 (vacuum), sent with probabilities of 50%, 25% and 25%, respectively. These intensity levels are optimized by performing simulations to maximize the secret bit rate for the satellite-to-ground channel.

For downlink QKD, a transmitter (designed and tested to be suitable for operation in low-Earth orbit) is integrated in the satellite (see Fig. 1b). Eight fibre-based laser diodes—four used as signal and four as decoy states—emit laser pulses (848.6 nm, 100 MHz, 0.2 ns). The output power of the eight laser didoes is monitored in real time by internal integrated photodetectors and controlled remotely by closed-loop systems, which precisely set the required intensity of the signal and decoy states and stabilize with less than 5% variation. In-orbit measurements show that with independent temperature tuning of the eight lasers their wavelengths are matched to within 0.006 nm, much smaller than their intrinsic bandwidth (about 0.1 nm). The lasers are synchronized to be within <10 ps, much smaller than their pulse duration of around 200 ps. The output beams are coaligned to ensure that both concentricity and coaxiality are better than 95%.

The light beams are then sent to a BB84-encoding module consisting of a half-wave plate, two polarizing beam splitters and a beam splitter, which randomly prepares the emitted photons in one of the four polarization states: horizontal, vertical, linear +45° or linear −45°. A physical thermal noise device generates a 4-bit random number for each run that drives the eight lasers and determines the output polarization and intensity levels. Independent electric control of the eight lasers and adjustment of the attenuation allow us to accurately obtain the average photon number in the output of the telescope: $\mu_s = 0.8$, $\mu_1 = 0.1$ and $\mu_2 = 0$. In the ground station, a compact decoding set-up consisting of a beam splitter, two polarizing beam splitters and four single-photon detectors (efficiency, 50%; dark counts, <25 Hz; timing jitter, 350 ps) is used for polarization-state analysis (see Fig. 1c and Methods). The overall optical efficiency, including the receiving telescope and the fibre coupling on the ground station, is approximately 16%. The satellite uses a radio-frequency channel for classical communication with the ground station (with an uplink and downlink bandwidth of 1 Mbit s^{-1} and 4 Mbit s^{-1}, respectively), and its experimental control-box payload to perform the sifting, error correction and privacy amplification.

The satellite passes Xinglong ground station along a Sun-synchronous orbit once every night starting at around 00:50 local time, for a duration of about 5 min. About 10 min before the satellite enters the shadow zone, its attitude is adjusted to point at the ground station. When the satellite exceeds an elevation angle of 5° from the horizon

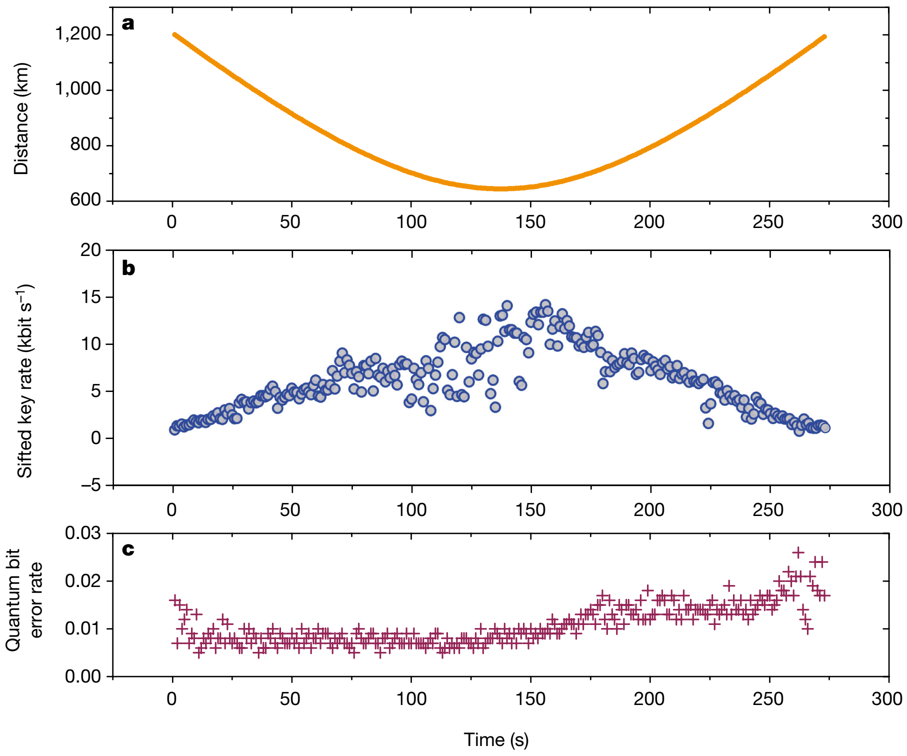


Figure 3 | Performance of satellite-to-ground QKD during one orbit. **a**, The trajectory of the Micius satellite measured from Xinglong ground station. **b**, The sifted key rate as a function of time and physical distance from the satellite to the station. **c**, Observed quantum bit error rate. See text for detailed discussion of the results, and Extended Data Table 2 and Extended Data Fig. 1 for additional data on different days.

plane of the ground station, a pointing accuracy of better than 0.5° is achieved. The APT systems then start bidirectional tracking and pointing to guarantee that the transmitter and receiver are robustly locked throughout the orbit. From an elevation angle of about 15°, the QKD transmitter sends randomly modulated signal and decoy photons, together with the beacon laser for timing synchronization, which are received and detected by the ground station. A single-orbit experiment ends when the satellite again reaches an elevation angle of 10°, this time on its descent (see Methods).

Since September 2016, we have routinely been able to successfully perform QKD under good atmospheric conditions. In Fig. 3a we show the data for the orbit on 19 December 2016, with a minimal (maximal) separation of 645 km (1,200 km). Within a duration of 273 s for the QKD data collection, the ground station collected 3,551,136 detection events, corresponding to 1,671,072 bits of sifted keys (see Fig. 3b). The sifted key rate decreases from about 12 kbit s^{-1} at 645 km to 1 kbit s^{-1} at 1,200 km, owing to the increase both in the physical separation distance and in the effective thickness of the atmosphere near Earth at smaller elevation angles. The time trace of the sifted key rate in Fig. 3b demonstrates that we are reliably able to obtain the keys throughout the duration of the data collection. However, more pronounced fluctuation in the key rate is observed near the central points of the orbit, when the satellite passes directly over the ground station and its effective angular velocity reaches its maximum (about 1° s^{-1}), thus placing stringent demands on the APT system. In Fig. 3c we show the observed quantum bit error rate, with an average of 1.1%, consistent with the expected error rate due to background noise and polarization visibility. The quantum bit error rates are slightly higher in the second half of the orbit, when the ground telescope faces towards Beijing and so there is more background light from the city.

We then perform error correction and privacy amplification to obtain the final keys. After randomly shuffling the sifted key, a hamming algorithm is used for error correction. We perform privacy amplification to reduce the possible knowledge of an eavesdropper by applying a random matrix over the corrected keys. Moreover, we take into account the intensity fluctuations for the signal and decoy states (<5%) and, when the statistical failure probability is set to 10^{-9}, calculate a secure final key of 300,939 bits, corresponding to a key rate of approximately 1.1 kbit s^{-1}.

As in previous experiments[24,25], here the key analysis does not consider information leakage due to possible side channels from the imperfect spatial, temporal and spectral overlap of the quantum light sources. The use of multiple laser diodes for different (signal and decoy) states and intensities can cause small (a few per cent here), non-ideal state overlap, which can be straightforwardly mitigated in future work by using narrowband spectral filtering or by adopting decoy-state QKD transmitters with only a single laser diode and modulating the created state externally.

The QKD experiments performed on 23 different days, with different physical distances between the satellite and the ground station, are summarized in Extended Data Table 2 and Extended Data Fig. 1. The shortest satellite-to-station distance depends on the highest altitude angle of the day, and varies from 507.0 km at 85.7° to 1,034.7 km at 25.0°. The sifted key that is obtained has a peak key rate of 40.2 kbit s^{-1} at 530 km and decreases for larger distances, for instance to 1.2 kbit s^{-1} at 1,034.7 km. From Extended Data Fig. 1, we also observe the fluctuation in the key rate due to different weather conditions. The quantum bit error rates are measured to be 1%–3%.

We compare the performance of our satellite-based QKD with that expected from the conventional method of direct transmission through optical telecommunication fibres. In Fig. 4 we show the link efficiency over distances of 645–1,200 km extracted from the observed count rate, together with theoretically calculated link efficiency assuming fibres with loss of 0.2 dB km^{-1}. Despite the short coverage time using the Micius satellite (273 s per day) and the need for reasonably good weather conditions, we observe an enhancement in efficiency compared to telecommunication fibres, which increases for larger distances; at 1,200 km, the channel efficiency of the satellite-based QKD over the 273-s coverage time is 20 orders of magnitudes higher than that achieved using the optical fibre. As a comparison with our data in Fig. 3b, over a distance of 1,200 km, even with a perfect 10-GHz single-photon source and ideal single-photon detectors with no dark count, transmission through optical fibres would result in only a 1-bit sifted key over six million years.

Discussion and outlook

We have reported satellite-to-ground quantum communication over a distance scale of 1,200 km. Our satellite can be further used as a

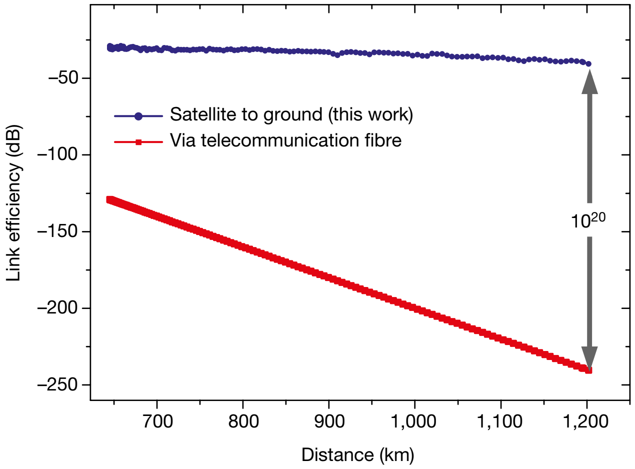


Figure 4 | QKD link efficiencies. Link efficiencies are shown for direct transmission through telecommunication optical fibres (red) and the satellite-to-ground approach (blue). The link efficiencies for the latter were calculated by dividing the photon intensity that arrived in front of the detectors at the ground station by that at the output of the satellite's transmitter. At a distance of 1,200 km, the satellite-to-ground approach (within the satellite coverage time) is more efficient than direct transmission by 20 orders of magnitude.

reliable relay to conveniently connect any two points on Earth for high-security key exchange. For example, we can first implement QKD in Xinglong, after which the key is stored in the satellite for 2 h until it reaches Nanshan station near Urumqi, a distance of about 2,500 km from Beijing. By performing another QKD between the satellite and the Nanshan station and using one-time-pad encoding, a secure key between Xinglong and Nanshan can be established. Future experimental plans include intercontinental secure-key exchanges between China and Austria, Italy and Germany.

Thus far, the shortcomings of the low-Earth-orbit satellite are limited coverage area and amount of time spent within range of each ground station. To increase the coverage, we plan to launch satellites with higher orbits and to construct a satellite constellation, requiring the development of new techniques to increase the link efficiency, including larger telescopes, better APT systems and wave-front correction through adaptive optics. However, higher-orbit satellites will spend less time in Earth's shadow; daytime QKD can be implemented using telecommunication-wavelength photons and improved spatial and spectral filtering[30].

The satellite-based QKD can be linked to metropolitan quantum networks, in which fibres are sufficient and convenient to connect numerous users in a city over distance scales of approximately 100 km (ref. 31). We thus envision a space–ground integrated quantum network, enabling useful quantum cryptography—probably the first commercial application of quantum information—at the global scale.

Online Content Methods, along with any additional Extended Data display items and Source Data, are available in the online version of the paper; references unique to these sections appear only in the online paper.

Received 20 March; accepted 21 July 2017.
Published online 9 August 2017.

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. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28,** 656–715 (1949).
3. Bennett, C. H. & Brassard, G. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working! *ACM Sigact News* **20,** 78–80 (1989).
4. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299,** 802–803 (1982).
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. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85,** 1330–1333 (2000).
7. 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).
8. Żukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. K. 'Event-ready-detectors' Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71,** 4287–4290 (1993).
9. Bennett, C. H. *et al.* Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76,** 722–725 (1996).
10. Duan, L.-M., Lukin, M. D., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414,** 413–418 (2001).
11. Pan, J.-W., Bouwmeester, D., Weinfurter, H. & Zeilinger, A. Experimental entanglement swapping: entangling photons that never interacted. *Phys. Rev. Lett.* **80,** 3891–3894 (1998).
12. Pan, J.-W., Gasparoni, S., Ursin, R., Weihs, G. & Zeilinger, A. Experimental entanglement purification of arbitrary unknown states. *Nature* **423,** 417–422 (2003).
13. 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,** 381–384 (2016).
14. Chou, C.-W. *et al.* Functional quantum nodes for entanglement distribution over scalable quantum networks. *Science* **316,** 1316–1320 (2007).
15. Yuan, Z.-S. *et al.* Experimental demonstration of a BDCZ quantum repeater node. *Nature* **454,** 1098–1101 (2008).
16. Sangouard, N., Simon, C., De Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83,** 33–80 (2011).
17. Ritter, S. *et al.* An elementary quantum network of single atoms in optical cavities. *Nature* **484,** 195–200 (2012).
18. Bernien, H. *et al.* Heralded entanglement between solid-state qubits separated by three metres. *Nature* **497,** 86–90 (2013).
19. Rarity, J. G., Tapster, P. R., Gorman, P. M. & Knight, P. Ground to satellite secure key exchange using quantum cryptography. *New J. Phys.* **4,** 82 (2002).
20. 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).
21. Ursin, R. *et al.* Entanglement-based quantum communication over 144 km. *Nat. Phys.* **3,** 481–486 (2007).
22. Yin, J. *et al.* Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature* **488,** 185–188 (2012).
23. Ma, X.-S. *et al.* Quantum teleportation over 143 kilometres using active feed-forward. *Nature* **489,** 269–273 (2012).
24. Wang, J.-Y. *et al.* Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. *Nat. Photon.* **7,** 387–393 (2013).
25. Nauerth, S. *et al.* Air-to-ground quantum communication. *Nat. Photon.* **7,** 382–386 (2013).
26. Yin, J. *et al.* Experimental quasi-single-photon transmission from satellite to earth. *Opt. Express* **21,** 20032–20040 (2013).
27. Vallone, G. *et al.* Experimental satellite quantum communications. *Phys. Rev. Lett.* **115,** 040502 (2015).
28. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
29. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
30. Liao, S.-K. *et al.* Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photon.* **11,** 509–513 (2017).
31. Chen, T.-Y. *et al.* Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **18,** 27217–27225 (2010).

Acknowledgements We thank many colleagues at the National Space Science Center, especially B.-M. Xu, J. Li, J.-C. Gong, B. Chen and J. Liu for their management and coordination. We thank X.-F. Ma, C. Jiang, L. Li, X.-M. Zhang and Y.-W. Chen for discussions. This work was supported by the Strategic Priority Research Program on Space Science, Chinese Academy of Sciences, and the National Natural Science Foundation of China.

Author Contributions C.-Z.P. and J.-W.P. conceived the research. C.-Z.P., J.-Y.W. and J.-W.P. designed the experiments. S.-K.L., W.-Q.C., Y.L., C.-Z.P. and J.-W.P. developed the spaceborn QKD source. S.-K.L., W.-Q.C., L.Z., J.Y., J.-J.J., J.-C.W., L.D., Y.-L.Z., Z.-C.Z., R.S., C.-Z.P., J.-Y.W. and J.-W.P. designed and developed the satellite and payloads. S.-K.L., L.Z., J.-J.J., R.S., C.-Z.P. and J.-Y.W. developed the ATP technique. S.-K.L., J.Y., L.Z., C.-Z.P. and J.-W.P. developed the polarization compensation method. X.-B.W. contributed to the decoy-state analysis. C.-Y.L., C.-Z.P. and J.-W.P. analysed the data and wrote the manuscript, with input from S.-K.L., W.-Y.L., Q.S., Y.L. and F.-Z.L. All authors contributed to the data collection, discussed the results and reviewed the manuscript. J.-W.P. supervised the whole project.

Author Information Reprints and permissions information is available at www.nature.com/reprints. The authors declare no competing financial interests. Readers are welcome to comment on the online version of the paper. Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. Correspondence and requests for materials should be addressed to C.-Z.P. (pcz@ustc.edu.cn), J.-Y.W. (jywang@mail.sitp.ac.cn) or J.-W.P. (pan@ustc.edu.cn).

METHODS

Timeline and details of China's Micius project. 2003: A pre-study project, 'free-space quantum communications', was assigned by the Chinese Academy of Sciences (CAS) to test the feasibility of satellite-based quantum communications.

2004: Distribution of entangled photons over 13 km through a noisy near-ground atmosphere over Hefei city was achieved, reaching a distance of more than the effective thickness of the aerosphere[1].

2007: The 'Quantum Experiments at Space Scale' project, aimed at developing important techniques for performing quantum experiments at the space scale, was supported by CAS.

2007: Quantum teleportation[2] over the Great Wall in Beijing, a distance of 16 km, was achieved.

2010: Direct and full-scale experimental verifications towards ground–satellite QKD were implemented near Qinghai Lake in western China, on a moving platform (using a turntable), on a floating platform (using a hot-air balloon) and with a high-loss channel (96 km, about 50 dB)[3].

2011: Quantum teleportation and bidirectional entanglement distribution over an approximately 100-km free-space channel were achieved over Qinghai Lake[4]. These results demonstrated the technical ability of handling the high-loss ground-to-satellite uplink channel and satellite-to-ground two-downlink channel.

2011: The 'Quantum Science Satellite' project was officially approved by CAS.

2012: Construction of the first prototype satellite began.

2014: The first prototype satellite was completed. The observatory station in Xinglong was completed.

2015: The flight model of the satellite was completed. The observatory stations in Nanshan and Delingha were completed. QKD and entanglement distribution experiments were conducted between the payloads of the first prototype satellite and the Delingha observatory station, over a distance of 17 km. A quantum teleportation experiment was also conducted between the payloads of the first prototype satellite and a transmitter placed in the Delingha station.

2016: The satellite passed through a series of environmental tests, including thermal vacuum, thermal cycling, shock, vibration and electromagnetic compatibility. The observatory stations in Lijiang and Ngari were completed.

2016: The Micius satellite, weighing 635 kg, was launched at 01:40 Beijing time on 16 August 2016 by a Long March 2D rocket from the Jiuquan Satellite Launch Centre, China. (A full view of the satellite before being assembled in the rocket is shown in Extended Data Fig. 2a).

The satellite's payloads. The satellite's payloads for the QKD experiment are composed of an experimental control box (with a weight of 7.56 kg, Extended Data Fig. 2b), an APT control box (9.9 kg, Extended Data Fig. 2c) and an optical transmitter (115 kg, Extended Data Fig. 2d).

The experimental control box has six functions: experimental process management, random-number generation and storage, modulation for the decoy-state photon source, synchronization-pulse recording, QKD post-processing (including raw-key sifting, error correction and privacy amplification to obtain the secure final keys) and encryption management.

The optical transmitter is composed of eight laser diodes with their drivers, a BB84 polarization-encoding module (Extended Data Fig. 2e, f), a telescope and an APT system (including a beacon laser, a coarse camera, a two-axis mirror, a fine camera, a fast-steering mirror (FSM), and so on). The QKD photons are generated and transmitted to the ground station by the optical transmitter.

The APT control box contains mainly the control electronics for the coarse-tracking loop and the fine-tracking loop. The specific functions include motor driver, FSM driver, coarse-feedback-loop controller and fine-feedback-loop controller.

Ground station in Xinglong. The Xinglong observatory is located about 110 km to the northeast of Beijing. The observatory station in Xinglong consists of a Ritchey–Chretien telescope (aperture of 1 m, focal length of 10 m) mounted on a two-axis gimbal (Extended Data Fig. 3a), a red beacon laser (671 nm, 2.7 W, 0.9 mrad), a coarse camera (field-of-view (FOV) of 0.33° × 0.33°, 512 × 512 pixels, frame rate of 56 Hz; Extended Data Fig. 3b) and an optical receiver box located on the arm of the gimbal (Extended Data Fig. 3a).

The coarse-tracking system consists of a two-axis gimbal in a control loop with a coarse camera. The coarse camera is used to detect the 532-nm beacon laser coming from the satellite. Guided by the 532-nm beacon laser, the 671-nm beacon laser installed on the ground telescope can point to the satellite precisely.

The fine-tracking system and the 850-nm photon receiver are mounted in the receiver box (part of the receiver box is shown in Extended Data Fig. 3c). The fine-tracking system consists mainly of a FSM based on a voice-coil and a fine camera (FOV of 1.3 mrad × 1.3 mrad, 128 × 128 pixels, frame rate of 212 Hz). A dichromic mirror is used to separate the 850-nm photons from the 532-nm beam. A beam splitter is used to divide the 532-nm beam into two parts. One is sent to the fine camera for tracking and the other is sent to an optical coupler linked to a single-photon detector for synchronization.

After passing through a beam expander, a motorized half-wave plate (HWP) and an interference filter, the 850-nm photons are received by a customized BB84 polarization-analysis module. Four multimode fibres with core diameters of 105 μm are used to connect the receiver module with four single-photon detectors. The electric output pulses from all five single-photon detectors and a global positioning system (GPS) pulse-per-second (PPS) signal are fed into a time-to-digital convertor (TDC), which records the detecting time and the channel numbers of the detectors. The acquired data are stored in the computer for further processing.

APT systems. The optical transmitter in the satellite and the receiver in the ground station both have cascaded multistage APT systems (Extended Data Fig. 4).

In the transmitter, there is a three-stage APT system. The first stage is the satellite attitude control system, which keeps the QKD photons pointing to the ground station with an error of less than 0.5°. The second stage is the coarse-control loop, which includes a two-axis gimbal mirror (azimuth and elevation rotation ranges of 10°) and a CMOS camera (FOV of 2.3° × 2.3°, frame rate of 40 Hz). The third stage is the fine-control loop, which is composed of a FSM driven by piezo ceramics (tracking range of 1.6 mrad) and a camera (FOV of 0.64 mrad × 0.64 mrad, frame rate of 2 kHz).

In the receiver, a two-stage APT system is used. The first stage is the coarse-control loop, including a two-axis gimbal telescope (azimuth rotation range of about −270° to +270°, elevation rotation range of about −5° to +95°) and a CCD camera (FOV of 0.33° × 0.33°, frame rate of 56 Hz). The second stage is the fine-control loop, including a FSM driven by a voice-coil (tracking range of ±35 mrad) and a CCD camera (FOV of 1.3 mrad × 1.3 mrad, frame rate of 212 Hz).

At the beginning, on the basis of the predicted orbit of the satellite, the receiver points a 671-nm beacon laser (2.7 W) towards the satellite in real time. The coarse camera in the satellite detects the 671-nm beacon laser to obtain the tracking error of the line-of-sight. With the feedback control of the two-axis gimbal mirror and the coarse camera, the coarse tracking error is less than 10 μrad, much smaller than the FOV of the fine camera. The fine tracking error is less than 2 μrad, owing to the feedback control of the FSM and the fine camera.

The optical transmitter in the satellite simultaneously points a beacon laser (wavelength of 532 nm, optical power of 160 mW, divergence angle of 1.25 mrad) towards the ground station. The ground station uses this beacon laser to correct its pointing direction, with an error of about 1–2 μrad. Finally, the link is locked onto the transmitter and the receiver in a closed-loop tracking.

The optical transmitter sends the QKD photons with a 'point-ahead angle' to the receiver. The 'point-ahead angle' is a series of angles to compensate for the transverse velocity of the two terminals and the speed of light, achieved by adjusting the tracking reference of the transmitter's fine-tracking loop in real time.

Synchronization. Because the transmitter and the receiver are separated by a large distance and have independent reference clocks, time synchronization is used to label QKD photon pulse sequences by their arrival time, which can be used to distinguish the QKD photons from the background noise. Because the distance between the transmitter and the receiver changes as the satellite passes over the ground station, we use both the GPS PPS signal and an assistant pulse laser in our synchronization scheme.

In the transmitter, the 532-nm beacon laser is designed as a pulse laser to perform synchronization, which is a passive Q-switching-type laser with about 10-kHz repetition frequency and 0.88-ns optical pulse width. Part of the laser is guided into a fast photodiode to convert it into an electrical pulse signal. This pulse signal and the GPS PPS signal from the satellite are fed into the TDC module of the transmitter. The acquired data are stored in the memory for further processing. Note that the time base of the TDC module is synchronized with that of the QKD photon-modulation module because they share a common clock.

In the receiver, part of the 532-nm laser beam is sent to a single-photon detector. The output signal of the single-photon detector, together with the electrical output pulses of the four single-photon detectors and the GPS PPS signal, is fed into a TDC. The acquired data are stored in the computer for further processing.

The time synchronization between the satellite and the ground can be divided into two steps. First, according to the predicted flight time of the light and the GPS PPS signal, the synchronization laser pulse sequence that is received on the ground can be matched with the satellite. Second, on the basis of the result of the first step, the time between the satellite and the ground is synchronized. We observe a typical temporal distribution of QKD photons with a standard deviation around 500 ps (Extended Data Fig. 5). A signal time window of 2 ns is used. Only events in the time window are valid.

Measuring the far-field pattern. Before the launch of the satellite, we measured the far-field pattern of the 850-nm laser in a thermal-vacuum test to simulate the in-orbit environment. Using a beam analyser, the divergence is measured to be 8 μrad × 11 μrad. The result is shown as Extended Data Fig. 5.

After the launch of the satellite, we could not measure the far-field profile directly as in the ground test. Alternatively, we adopted a scanning method, measuring the intensity distribution of the 850-nm photons as a function of the pointing angle of the transmitter. The profile that we obtained is shown in Extended Data Fig. 5. Such a complete scan usually took a few minutes. Because the satellite is fast-moving, the satellite-to-ground distance and the atmospheric conditions vary with time. Atmospheric turbulence can be fast and can occur within a scanning cycle, which can distort the scanning plot. We observe that the result of the in-orbit test are qualitatively consistent with those from the ground test (Extended Data Fig. 5).

Experimental procedure. The experimental instruction and data process of satellite-to-ground QKD is shown in Extended Data Fig. 6. Six systems work together to implement the QKD experiment, including the scientific experiment planning centre, the ground support centre, the ground tracking telemetry and command centre, the optical ground station and the satellite platform with the payloads.

The satellite-to-ground QKD procedure is as follows (Extended Data Fig. 6). First, the experiment planning centre arranged the experiment, if the following conditions are guaranteed: (a) the calculated maximum elevation angle of the satellite to the ground station is greater than 25° (on the basis of predicted satellite orbits); and (b) the weather is forecasted to be clear and sunny. If so, instruction sequence files for the satellite are made and sent to the ground support centre. The instruction sequence file, the predicted curve data file and the polarization base compensation curve file for the motorized HWP are sent to the optical ground stations.

Second, the instruction file is translated to a coding file at the ground support centre and then sent to the ground tracking telemetry and command centre for upload to the satellite.

Third, the satellite platform and the payloads along with the optical ground station execute the instructions to transmit QKD photons from satellite to ground as follows:

(a) The satellite starts to change the pointing mode from geocentric to ground-station centric 10 min before entering the shadow zone. When the satellite exceeds an elevation angle of 5° from the horizon plane of the ground station, a pointing accuracy of better than 0.5° is achieved. At the same time, system initialization of the payloads is set.

(b) Before the satellite appears above the horizon, the telescope at the ground station activates its beacon laser at an elevation angle of 10° above the horizon to wait for the satellite. Once the elevation angle of the satellite to the ground station is more than 10°, open-loop pointing according to the predicted orbit is automatically executed. Meanwhile, the receiver at the ground station initiates data recording and starts to rotate the motorized HWP according to the polarization base compensation curve file.

(c) After reaching an elevation angle of 10° above the horizon, the satellite is fully covered by the beacon laser (671 nm) at the ground station. When the coarse-tracking camera of the optical transmitter obtains an image of the ground beacon laser, the APT is initiated to precisely track the ground beacon laser. At the same time, the beacon laser of the optical transmitter (532 nm) points towards the ground station.

(d) When the ground station receives the beacon laser from the optical transmitter, the APT control begins to precisely track the satellite beacon laser. Bidirectional tracking and locking between the transmitter and receiver is then achieved.

(e) At an elevation angle of about 15°, the satellite begins to read the random numbers and modulate the lasers for the decoy-state protocol. Both the satellite and the ground station record the GPS PPS signals and detect the 532-nm synchronous laser pulse for timing information. At the same time, the ground station records the output signals of the four single-photon detectors for the QKD measurement. All of the data are stored.

(f) When the satellite reaches an elevation angle of approximately 10° on its descent, the transmission of QKD photons and the tracking loop are terminated.

(g) After the transmission of the photons, experiment data are stored for further processing.

Decoy-state protocol and key rates. In practical QKD with a lossy channel, the security can be undermined by a photon-number-splitting attack if an imperfect single-photon source is used. For security, we need to use the decoy-state method[28,29], which verifies the lower bound on the single-photon counts.

The main idea of the decoy-state method is to change intensities randomly among several different values when sending out each pulse. Equivalently, we can regard pulses of different intensities as pulses from different sources. In this experiment, we use three different intensities: $\mu_2 = 0$ for vacuum, and μ_1 and μ_s for the decoy and signal states, respectively. In photon-number space, the state of the pulse from a non-vacuum source can be written as

$$\rho_l = \sum_k a_k^l |k\rangle\langle k|$$

where

$$a_k^l = \frac{\mu_l e^{-\mu_l}}{k!}$$

is the photon-number (k) distribution of the source of phase-randomized weak coherent states, with intensity $\mu_l = \mu_2 = 0$, $\mu_l = \mu_1$ and $\mu_l = \mu_s$ for vacuum, decoy and signal sources.

In practice, the number of pulses is finite and we have to consider the possible statistical fluctuations[28]. In such a case, we introduce an average value $\langle s_k\rangle$ for the counting rate of a k-photon state in a certain basis and use the constraints

$$S_l = \sum_k a_k^l \langle s_k\rangle$$

S_l is the directly observed value for the counting rate of source l in experiments and is regarded as a known value, but we need the average values $\langle S_l\rangle$ to calculate the secure final key rate. In general, any average value $\langle A\rangle$ can be related to its observed value A, with a fixed failure probability ξ by

$$\langle A\rangle = A(1+\delta)$$

$$\delta \in [-\delta_1(\xi), \delta_2(\xi)]$$

$$\langle \underline{A}\rangle = A[1-\delta_1(A,\xi)]$$

$$\langle \overline{A}\rangle = A[1+\delta_2(A,\xi)]$$

where the under- and overbars indicate upper and lower bounds, respectively. With these preparations, we can determine a lower bound on the counting rate of a single-photon pulse $\underline{s_1}$, given the observed values of S_l in each basis. Similarly, given the observed values of error E_l, we can determine an upper bound on bit-flip error rate of a single-photon pulse in each basis and hence an upper bound on the phase-flip error rate $\overline{e_1^{\mathrm{ph}}}$. Finally, we can calculate the secure final key rate per emissive pulse:

$$R = p_{\mu_s}\{a_1'\underline{s_1}[1 - H(\overline{e_1^{\mathrm{ph}}})] - fS_{\mu_s}H(E_{\mu_s})\}$$

where f is the error correction inefficiency, $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, $a_1' = \mu_s e^{-\mu_s}$ and E_{μ_s} is the observed error rate for source intensity μ_s.

The values of the parameters used in the experiment are listed in Extended Data Table 3. We send out 1.36×10^{10} pulses in the whole experiment. The results of the experiment are listed in Extended Data Table 4; all data listed except Y_0 are results after basis correction.

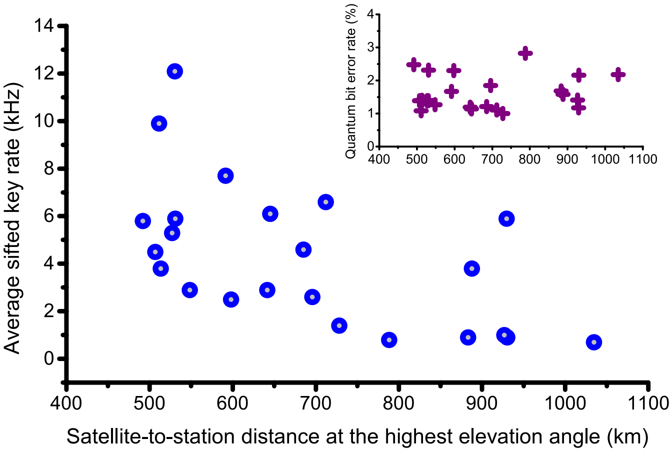
Setting the failure probability to $\xi = 10^{-9}$ and the error correction inefficiency to $f = 1.4742$, as in our actual key-distillation system, we find a secure final key rate of $R = 1.38 \times 10^{-5}$, corresponding to 377,100 final keys if we had used the Chernoff bound[32].

We can also consider higher-level security by taking into consideration the uncertainties of the intensity of the source light[33]. Here we have both the light-intensity uncertainties and the statistical fluctuation. According to the experimental data, we know that $\sigma < 5\%$, and we set the failure probability to 10^{-9} with a Chernoff bound for the statistical fluctuation. We obtain a secure final key rate of $R = 1.10 \times 10^{-5}$, corresponding to 300,939 final keys.

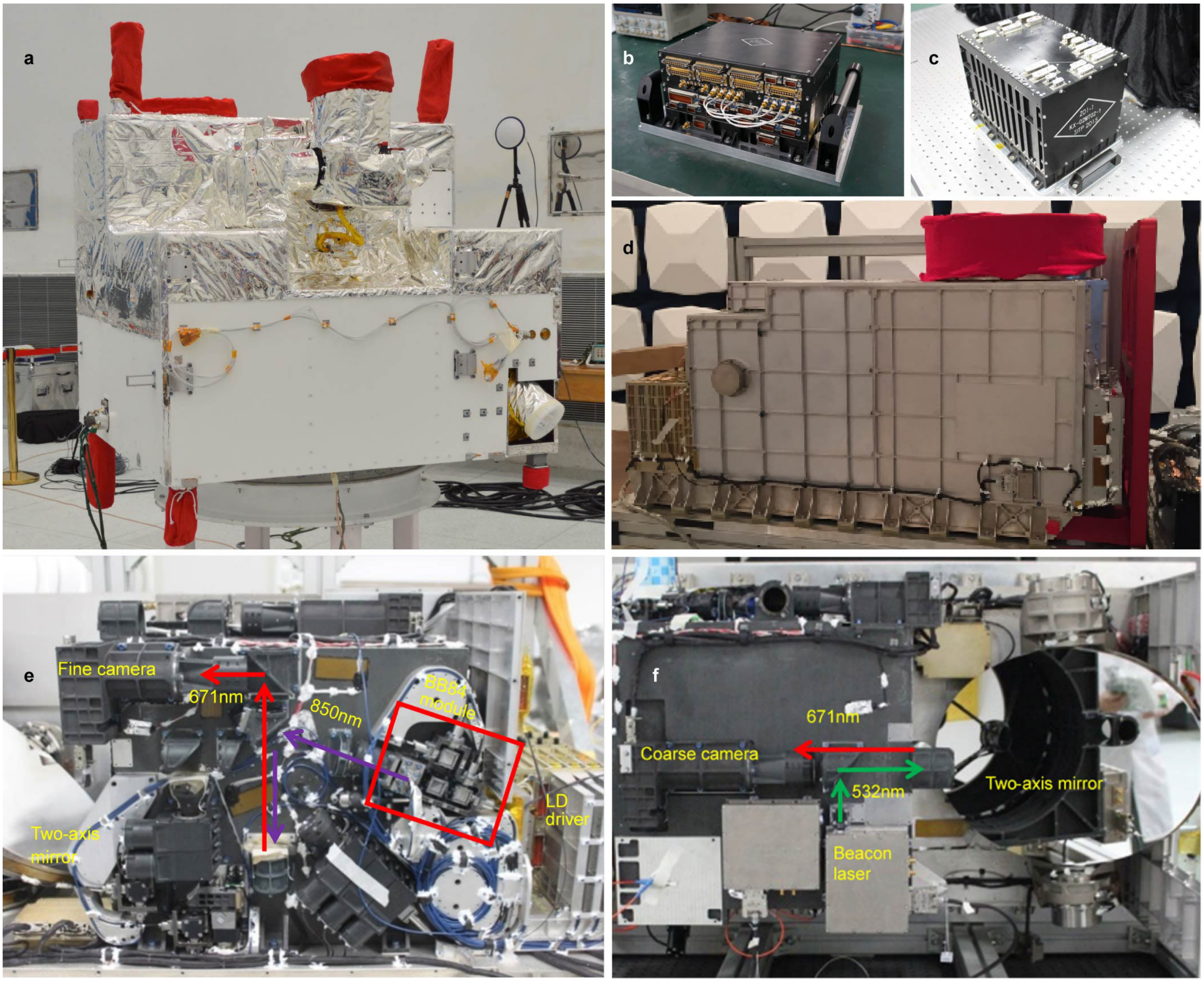
Data availability. The data that support the findings of this study are available from the corresponding authors on reasonable request.

32. Curty, M. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5,** 3732 (2014).

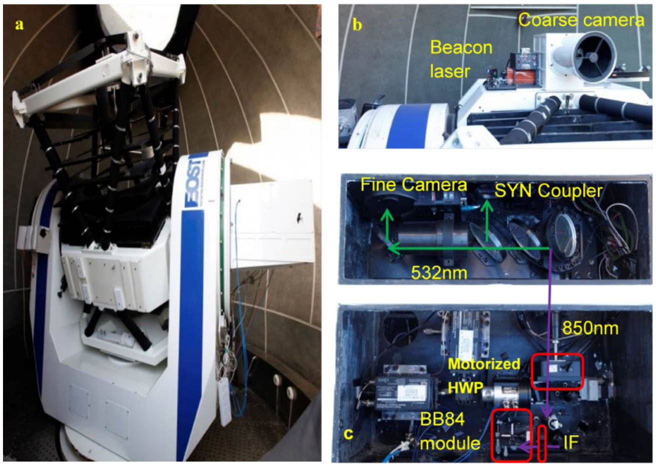
33. Wang, X.-B., Yang, L., Peng, C.-Z. & Pan, J.-W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New J. Phys.* **11,** 075006 (2009).



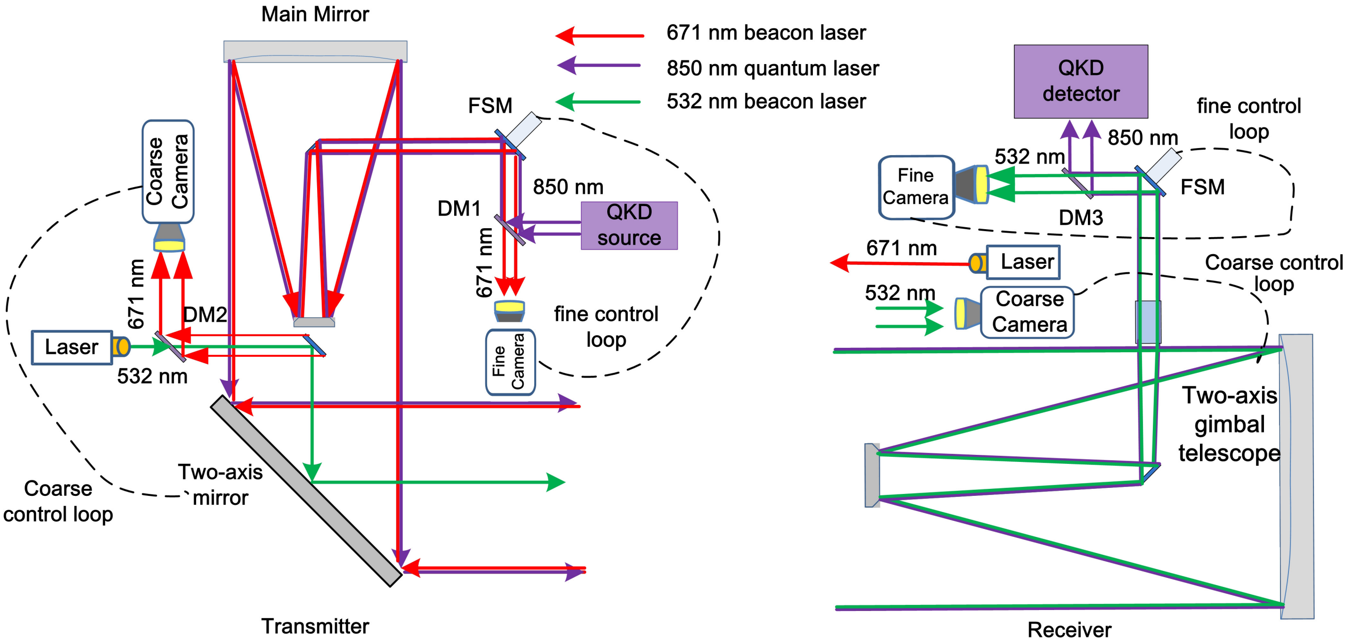
Extended Data Figure 1 | Summary of the QKD data obtained for 23 different days. The *x* axis is the shortest satellite-to-station distance, which occurs at the highest elevation angle and varies for different days. The *y* axis is the average sifted key rate that is obtained over the 273-s orbit. The inset shows the quantum bit error rate.



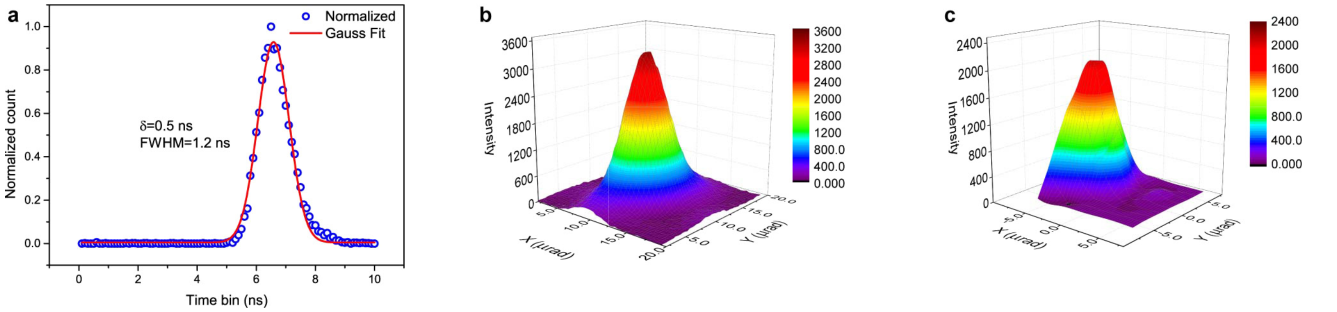
Extended Data Figure 2 | The Micius satellite and the payloads. a, A full view of the Micius satellite before being assembled into the rocket. **b**, The experimental control box. **c**, The APT control box. **d**, The optical transmitter. **e**, Left side view of the optical transmitter optics head. **f**, Top side view of the optical transmitter optics head.



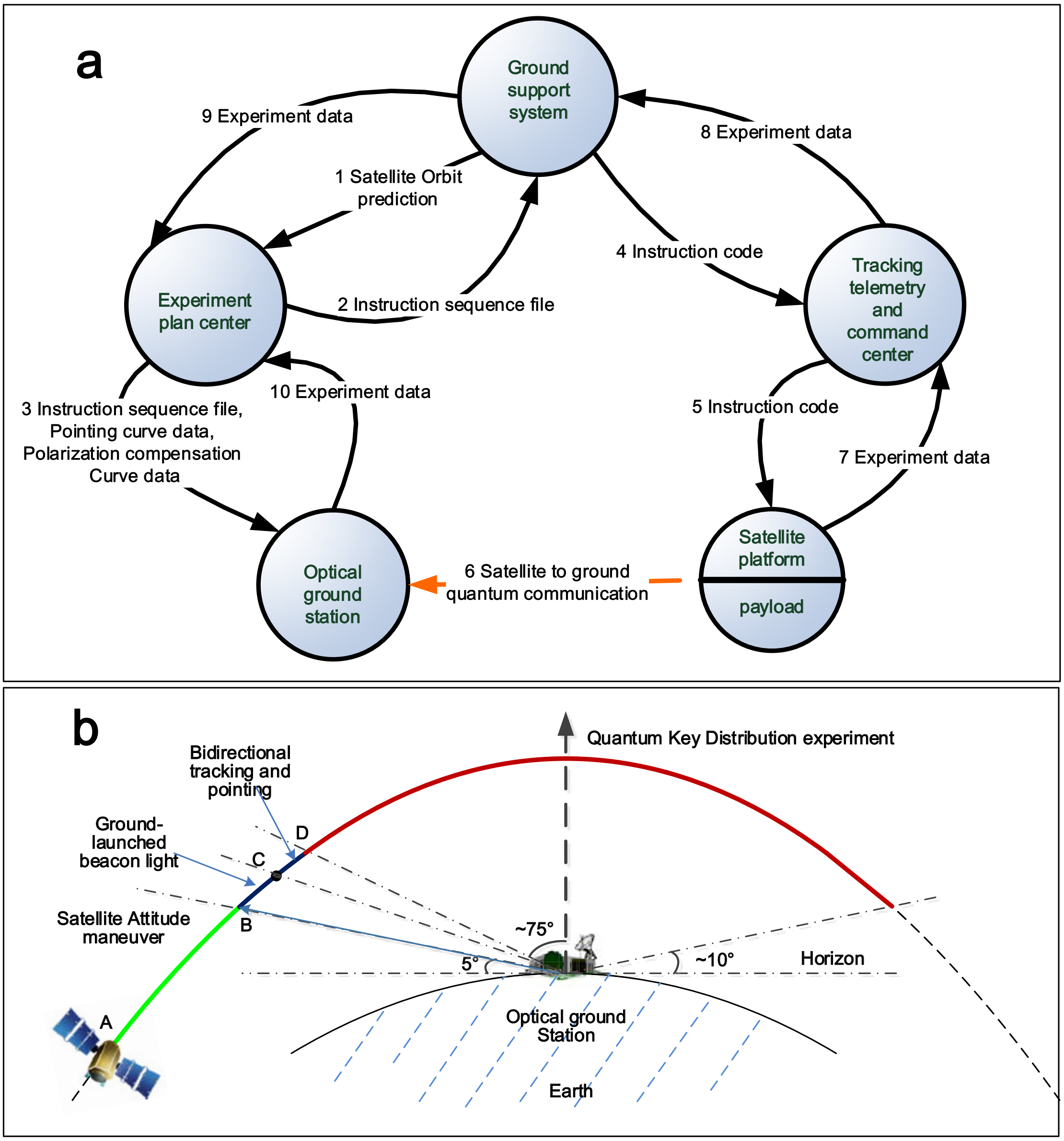
Extended Data Figure 3 | Hardware at Xinglong ground station. a, The two-axis gimbal telescope. **b**, Beacon laser and coarse camera. **c**, One of the two layers of the optical receiver box.



Extended Data Figure 4 | Sketch of the tracking systems on the satellite and at the ground station. DM1: dichroic mirror transmitting 671-nm light and reflecting 850-nm light. DM2: transmitting 532-nm light; reflecting 671-nm light. DM3: transmitting 532-nm light; reflecting 850-nm light.



Extended Data Figure 5 | A typical temporal distribution of 850-nm photons and the measured far-field pattern. a, A typical temporal distribution of 850-nm photons after the time synchronization process. The data measurement time is 1 s. Each time bin is 100 ps. The counts are normalized and a variance of $\delta = 0.5$ ns is obtained with Gaussian fitting. **b**, Far-field pattern measured from the thermal-vacuum test on the ground. The divergence angles (full angle at $1/e^2$ maximum) are 8 μrad for the *X* axis and 11 μrad for the *Y* axis. **c**, Far-field pattern measured from the satellite-to-ground scanning test. The divergence angles (full angle at $1/e^2$ maximum) are 9 μrad for the *X* axis and 11 μrad for the *Y* axis.


a
Ground support system
Experiment plan center
Tracking telemetry and command center
Optical ground station
Satellite platform
payload
1 Satellite Orbit prediction
2 Instruction sequence file
3 Instruction sequence file, Pointing curve data, Polarization compensation Curve data
4 Instruction code
5 Instruction code
6 Satellite to ground quantum communication
7 Experiment data
8 Experiment data
9 Experiment data
10 Experiment data
b
Quantum Key Distribution experiment
Bidirectional tracking and pointing
Ground-launched beacon light
Satellite Attitude maneuver
A
B
C
D
~75°
5°
~10°
Horizon
Optical ground Station
Earth

Extended Data Figure 6 | The experimental procedure. a, Instruction and data processes. **b**, Tracking and QKD processes during an orbit.

Extended Data Table 1 | Performance of the APT systems

Components		Transmitter terminal	Receiver terminal
Coarse pointing mechanism	Type	Two-axis gimbal mirror	Two-axis gimbal mount
	Tracking range	Azimuth:±5 ° Elevation: ±5 °	Azimuth:-270 °~+270 ° Elevation:-5 °~+95 °
Coarse camera	Type	CMOS	CCD
	Field of view	2.3 ° × 2.3 °	0.33 ° × 0.33 °
	Pixels & frame rates	1024 × 1024 & 11 Hz 512 × 512 & 40 Hz	512 × 512 & 56 Hz
Fine pointing mechanism	Type	PZT fast steering mirror	Voice-oil fast steering mirror
	Tracking range	±0.8 mrad	±17.5 mrad
Fine camera	Field of view	0.64 mrad × 0.64 mrad	1.3 mrad × 1.3 mrad
	Pixels & frame rates	60 × 60 & 2000 Hz	128 × 128 & 212 Hz
Beacon laser	Power	160 mW	2.7 W
	Wavelength	531.9 nm	671 nm
	Divergence	1.25 mrad	0.9 mrad
Tracking error (1δ)		0.6~1.5 μrad	1~2 μrad

Extended Data Table 2 | QKD data of 23 different orbits from 23 September 2016 to 22 May 2017

Date	Highest altitude angle	Shortest distance	Peak sifted key rate	Average sifted key rate	Quantum bit error rate
	(°)	(km)	(kHz)	(kHz)	
23/09/2016	67.35	527.07	22.1	5.3	1.39 %
29/09/2016	54.25	591.56	24.1	7.7	1.67 %
09/10/2016	28.67	930.2	2.7	0.9	2.16 %
10/10/2016	28.87	926.82	2.1	1.0	1.41 %
19/12/2016	47.79	645.08	14.1	6.1	1.14 %
04/01/2017	43.4	685.04	10.8	4.6	1.21 %
06/01/2017	71.68	513.46	11.1	3.8	1.40 %
12/01/2017	35.8	788.19	2.1	0.8	2.82 %
01/12/2016	24.99	1034.66	1.2	0.7	2.18 %
13/02/2017	44.5	695.76	13.9	2.6	1.85 %
14/02/2017	85.7	507.00	13.6	4.5	1.39 %
21/02/2017	29.64	929.67	9.0	5.9	1.17 %
08/03/2017	79.6	511.35	21.4	9.9	1.08 %
11/03/2017	42.69	711.94	15.6	6.6	1.11 %
20/04/2017	82.85	491.92	11.5	5.8	2.48 %
27/04/2017	40.04	728.20	6.1	1.4	1.00 %
07/05/2017	68.24	530.33	40.2	12.1	1.39 %
11/05/2017	54.85	598.09	17.2	2.5	2.30 %
14/05/2017	49.45	641.65	7.9	2.9	1.19 %
17/05/2017	65.24	548.41	11.4	2.9	1.27 %
18/05/2017	31.49	883.23	1.9	0.9	1.68 %
20/05/2017	70.34	531.05	17.8	5.9	2.31 %
22/05/2017	31.31	887.84	6.5	3.8	1.58 %

Extended Data Table 3 | Performance of the transmitter and receiver

Components			Data
Transmitter (weak coherent pulses)	Telescope diameter		300 mm
	Wavelength		848.62 nm
	Offset of wavelength		<0.006 nm
	Linewidth (3 dB)		~0.1 nm
	Pulse width (FWHM)		~200 ps
	Polarization contrast ratio		>225:1
	Divergence		~10 μrad
	Frequency		100 MHz
	Mean photon number	Signal	0.8
		Decoy	0.1
		Vacuum	0
	Probability	Signal	0.5
		Decoy	0.25
		Vacuum	0.25
Receiver	Telescope diameter		1 m
	Optical efficiency @850nm		~16%
	Detector efficiency @850nm		~50%
Synchronization	Laser pulse (FWHM)		0.88 ns
	Laser frequency		10.7 kHz
Synchronization jitter of transmitter and receiver (1δ)			~0.5 ns

Extended Data Table 4 | Observed data for a single orbit at Xinglong station

T (s)	Y_0	S_{μ_s}	S_{μ_1}	E_{μ_s}	E_{μ_1}	R_{pulse}	R_{total}
273	5.89×10^{-7}	1.22×10^{-4}	1.52×10^{-5}	1.1 %	1.8 %	1.10×10^{-5}	300939

T is the effective time for QKD, Y_0 is the yield for the vacuum states, s_l is the counting rate for a source of intensity μ_l, E_l is the quantum bit error rate of the states of intensity μ_l, R_{pulse} is final key rate per clock cycle and R_{total} is the total final key size of the experiment.