nature Accelerated Article Preview

ARTICLE
doi:10.1038/nature23655

Satellite-to-ground quantum key distribution

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

This is a PDF file of a peer-reviewed paper that has been accepted for publication. Although unedited, the content has been subjected to preliminary formatting. *Nature* is providing this early version of the typeset paper as a service to our customers. The text and figures will undergo copyediting and a proof review before the paper is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers apply.

Cite this article as: Liao, S. *et al.* Satellite-to-ground quantum key distribution. *Nature* http://dx.doi.org/10.1038/nature23655 (2017).

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

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. In practice, the achievable distance for QKD has been limited to a few hundred kilometres, owing to the channel loss of fibers or terrestrial free space that exponentially reduced the photon rate. Satellite-based QKD promises to establish a global-scale quantum network by exploiting the negligible photon loss and decoherence in the empty out space. Here we develop and launch a low-Earth-orbit satellite to implement decoy-state QKD with over kHz key rate from the satellite to ground over a distance of up to 1,200 km, which is up to 20 orders of magnitudes more efficient than that expected using an optical fiber (with 0.2 dB/km loss) of the same length. The establishment of a reliable and efficient space-to-ground link for faithful quantum state transmission paves the way to global-scale quantum networks.

Private and secure communications are fundamental human needs. Traditional public key cryptography usually relies on the perceived computational intractability of certain mathematical functions. In contrast, quantum key distribution (QKD)[1] proposed in the mid-1980s—the best known example of quantum cryptographic tasks—is a radical new way to offer an information-theoretically secure solution to the key exchange problem, ensured by the laws of quantum physics. QKD allows two distant users, who do not share a long secret key initially, to produce a common, random string of secret bits, called a secret key. Using the one-time pad encryption, this key is proven to be secure by Shannon[2] to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. In the QKD, the information is encoded in the superposition states of physical carriers at single-quantum level, where photons, the fastest flying qubits with their intrinsic robustness to decoherence and ease of control, are usually used. Any eavesdropper on the quantum channel attempting to gain information of the key will inevitably introduce disturbance to the system, and 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, a strong research effort has been devoted to achieve secure QKD at long distance, eventually aiming at global scale for practical use. The most straightforward method is directly sending single photons through optical fibers or terrestrial free-space. In both cases, however, the channel loss cause a decrease of the transmitted photons that scales exponentially with the length. Unlike classical telecommunications, the quantum signal in QKD cannot be noiselessly amplified due to the quantum non-cloning theorem[4]. This limits the maximal distance for secure QKD to a few hundred kilometers[5]. Beyond this length scale, quantum communications become extremely challenging[6].

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

A more direct and promising solution for global-scale QKD is through satellites in space. Compared with terrestrial channels, the satellite-to-ground connection has significantly reduced losses[19]. This is mainly because that the effective thickness of the atmosphere is ~10 km, and most of the photon's propagation path is in empty space with negligible absorption and turbulence. A ground test[20] in 2004 has demonstrated the distribution of entangled photon pairs over a noisy ground atmosphere of 13 km—beyond the effective thickness of the aerosphere—and showed the survival of entanglement and violation of Bell's inequality. Further verifications of the feasibilities of the satellite-based QKD, under the simulated conditions of huge attenuation and various turbulence, have been performed at even longer distance[21–23], on rapidly moving platforms[24,25], and exploiting satellite corner cube retroreflectors[26,27].

We have developed a sophisticated satellite, named after *Micius*, dedicated for quantum science experiments (for the project timeline and its design details, see Methods), which was successfully launched on 16th August 2016, from Jiuquan, China, orbiting at an altitude of ~500 km (Fig. 1a). Using one of the satellite payloads—a decoy-state QKD transmitter at 850 nm wavelength—and cooperating with Xinglong ground observatory station (near Beijing, 40°23'45.12"N, 117°34'38.85"E, altitude 890m), we establish the decoy-state QKD with polarization encoding from the satellite to the ground with ~kHz rate over a distance up to 1200 km.

Experimental challenges and solutions

A robust and efficient satellite-to-ground QKD places a more stringent requirement on the link efficiency than conventional satellite-based

[1]Shanghai Branch, Department of Modern Physics and National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Shanghai 201315, China. [2]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, The 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, Urumqi 830011, China. [9]National Space Science Center, Chinese Academy of Sciences, Beijing 100190, China.

classical communication systems. To obtain a high signal-to-noise ratio, one cannot increase the signal power, but 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 ground (see Fig. 1a). In the downlink, beam wandering caused by the atmospheric turbulence occurs in the very end of the transmission path (near the earth surface), 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 has higher link efficiency.

The beam diffraction mainly depends on telescope size. 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, which sends the light beam with a near-diffraction-limited far-field divergence of ~10 µrad. After a travel distance of 1200 km, we expect the beam diameter expands to about 10 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 1200 km.

The narrow divergence beam from the fast-moving satellite (with a speed of ~7.6 km/s) demands a high-bandwidth and high-precision acquiring, pointing, and tracking (APT) system to establish a stable link. We design cascaded multi-stage APT systems in the transmitter (Fig. 1b) and the receiver (Fig. 1c). Initial coarse orientation of the telescope is based on forecasted satellite orbit position with an uncertainty below 200 m. The satellite attitude control system itself ensures the transmitter pointing to the ground station with ~0.5° precision. The satellite and the ground station send beacon lasers to each other with a divergence of 1.25 mrad and 0.9 mrad, respectively (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 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 equipped in the ground station (see Extended Data Table 1 for details). Using a feedback closed-loop, the transmitter achieves a tracking accuracy of ~1.2 µrad (see Fig. 2b), much smaller than the beam divergence. We estimate that at 1200 km the loss due to atmospheric absorption and turbulence is in the range of 3 dB to 8 dB, and the loss due to pointing error is less than 3 dB.

Furthermore, we use temporal and spectral filtering to suppress the background noise. The beacon laser, with a 0.9-ns pulse width and a ~10-kHz repetition rate, serves for both the APT and synchronization. In a 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 for timing information. Thus, we avoid the space-ground clock drift, and obtain 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, spectrally, we use a bandwidth filter in the receiver to reduce the background scattering. In the current experiment, we limit ourselves to night-time operation only to avoid sun light.

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

Experimental procedure and results

In our experiment, we use the decoy-state[28,29] Bennett-Brassard 1984 (BB84)[1] protocol for the QKD, which can detect photon-number-splitting eavesdropping and thus allow secure QKD using weak coherent pulses with significantly increased distance and rate. The key method is to use multiple intensity levels at the transmitter's source, one signal state (mean photon number μ_s) and several decoy states (μ_1, μ_2, …) which are randomly interspersed. Here we adopt a 3-intensity protocol using three levels of μ: a high μ_s, a moderate μ_1 and a zero μ_2 (vacuum), sent with probabilities of 50%, 25%, and 25%, respectively, which are optimized by performing simulations to maximize the secret bit rate for the satellite-to-ground channel.

For downlink QKD, a space-qualified transmitter is integrated in the satellite (see Fig. 1b). Eight fiber-based laser diodes—four used as signal and four as decoy state—emit laser pulses (848.6 nm, 100 MHz, 0.2 ns). The output power of the eight laser didoes are monitored in real time by internal integrated photodetectors and remotely controlled 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 within 0.006 nm, much smaller than their intrinsic bandwidth (~0.1 nm). The lasers are synchronized to be within <10 ps, much smaller than their pulse duration of ~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 HWP, two polarizing beam splitters (PBSs), and a beam splitter (BS), which randomly prepares the emitted photons in one of the four polarization states: horizontal, vertical, linear +45° and -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: $\mu_s = 0.8$, $\mu_1 = 0.1$, $\mu_2 = 0$. In the ground station, a compact decoding setup consisting of a BS, two PBSs, and four single-photon detectors (efficiency 50%, dark counts <25 Hz, timing jitter 350 ps) are used for polarization state analysis (see Fig. 1c and Methods). The overall optical efficiency including the receiving telescope and the fiber coupling on the ground station is ~16%. The satellite uses radio frequency channel for classical communication with the ground station (with an uplink and downlink bandwidth of 1 Mbps and 4 Mbps, respectively), and exploits 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 12:50 PM local time, for a duration of about 5 minutes. About 10 minutes 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 ground station's horizon plane, a pointing accuracy of better than 0.5° is achieved. Then the APT systems start bidirectional tracking and pointing to guarantee that the transmitter and receiver are robustly locked through the whole orbit. From about 15° elevation angle, 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 reaches 10° elevation angle in the other end (see Methods).

Since September 2016, we have been able to successfully perform QKD routinely under good atmospheric condition. Figure 3a shows the data for the orbit on 19th December 2016 with the minimal (maximal) separation of 645 km (1200 km). Within a duration of 273 s for the QKD data collection, the ground station collected 3,551,136 detection events, and thereof 1,671,072 bits of sifted keys (see Fig. 3b). The sifted key rate decrease from ~12 kbit/s at 645 km to ~1 kbit/s at 1200 km, because of the increase of both the physically separated distance and the effective thickness of the atmosphere near the earth at smaller elevation angles.

The time trace of the sifted key rate in Fig. 3b demonstrates that we are able to obtain the keys through the whole duration reliably. We note, however, more pronounced key rate fluctuation is observed in the central points when the satellite passes through the ground station around the top, where its effective angular velocity reaches maximum, ~1°/s, thus placing stringent demand on the APT system. Figure 3c shows the observed quantum bit error rate (QBER) with an average of 1.1%, consistent with the expected error rate due to background noise and polarization visibility. The QBERs become slightly higher in the second half of the orbit when the ground telescope points to Beijing that brings more city stray light.

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

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

The QKD experiments performed at 23 different days is summarized in Extended Data Table 2 and Extended Data Figure 1, where the physical distance between the satellite and the ground station varies for different days. The shortest satellite-to-station distance depends on the highest altitude angle of the day, which varies from 507.0 km at 85.7° to 1034.7 km at 25.0°. The obtained sifted key has a peak rate of 40.2 kbits/s at 530 km and decreases at larger distances, for instance, to 1.2 kbits/s at 1034.7 km. From Extended Data Figure 1, we also observe the key rate fluctuation due to different weather conditions. The QBERs are measured to be in the 1%-3% range.

We compare the performance of our satellite-based QKD with what expected from the conventional method of direct transmission through telecommunication fibers. Figure 4 shows the extracted link efficiency at the distance from 645 km to 1200 km from the observed count rate, together with theoretically calculated link efficiency using fibers with 0.2 dB/km loss. Despite the short coverage time (273 s per day) using the *Micius* satellite and the need for reasonably good weather condition, an increasing efficiency enhancement is pronounced at long distances. At 1200 km, the satellite-based QKD within the 273 s coverage time demonstrates a channel efficiency that is ~20 orders of magnitudes higher than using the optical fiber. As a comparison with our data in Fig. 3b, through a 1200 km fiber, even with a perfect 10-GHz single-photon source and ideal single-photon detectors with no dark count, one would obtain only 1-bit sifted key over six million years.

Discussion and outlook

We have reported the first satellite-to-ground quantum communication experiment over 1200 km distance scale. Our satellite can be further exploited as a trustful relay to conveniently connect any two points on the 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 hours until it reaches Nanshan station near Urumqi, by a distance of ~2500 km from Beijing. By performing another QKD between the satellite and the Nanshan station, and using one-time-pad encoding, secure key between Xinglong and Nanshan can then be established. Future experimental plan also includes intercontinental secure key exchanges between China and Austria, Italy, and Germany.

Thus far, the low-Earth-orbit satellite has shortcomings of limited coverage area and amount of time spent in each ground station. To increase the coverage, we plan to launch satellites at higher orbit and construct a satellite constellation, which require the development of new techniques to increase the link efficiency, including larger-size telescopes, better APT systems, and wave-front correction through adaptive optics. Higher-orbit satellites, however, will spend less time in the earth's shadow. Day-time 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 where fibers are sufficient and convenient to connect numerous users within a city at ~100 km scale[31]. We can thus envision a space-ground integrated quantum network, enabling quantum cryptography—most likely the first commercial application of quantum information—useful at a 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 cryprography: public key distribution and coin tossing. in *Int. Conf. on Computers, Systems & 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! *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., Lutkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330 (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. Zukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. K. 'Event-ready-detectors' Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287–4290 (1993).
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 (2015).
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 3 meters. *Nature* **497**, 86–90 (2012).
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.* Ground test of satellite constellation based quantum communication. Preprint available at http://arxiv.org/abs/1611.09982.
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, J. Liu for their management and coordination. We thank X.-F. Ma, C. Jiang, L. Li, X.-M. Zhang, Y.-W. Chen for discussions. This work was supported by the Strategic Priority Research Program on Space Science, Chinese Academy of Sciences, and 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., J.Y., L.Z., W.-Q.C., 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. L.Z., J.-J.J., S.-K.L., 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. analyzed 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) and J.-W.P. (pan@ustc.edu.cn).

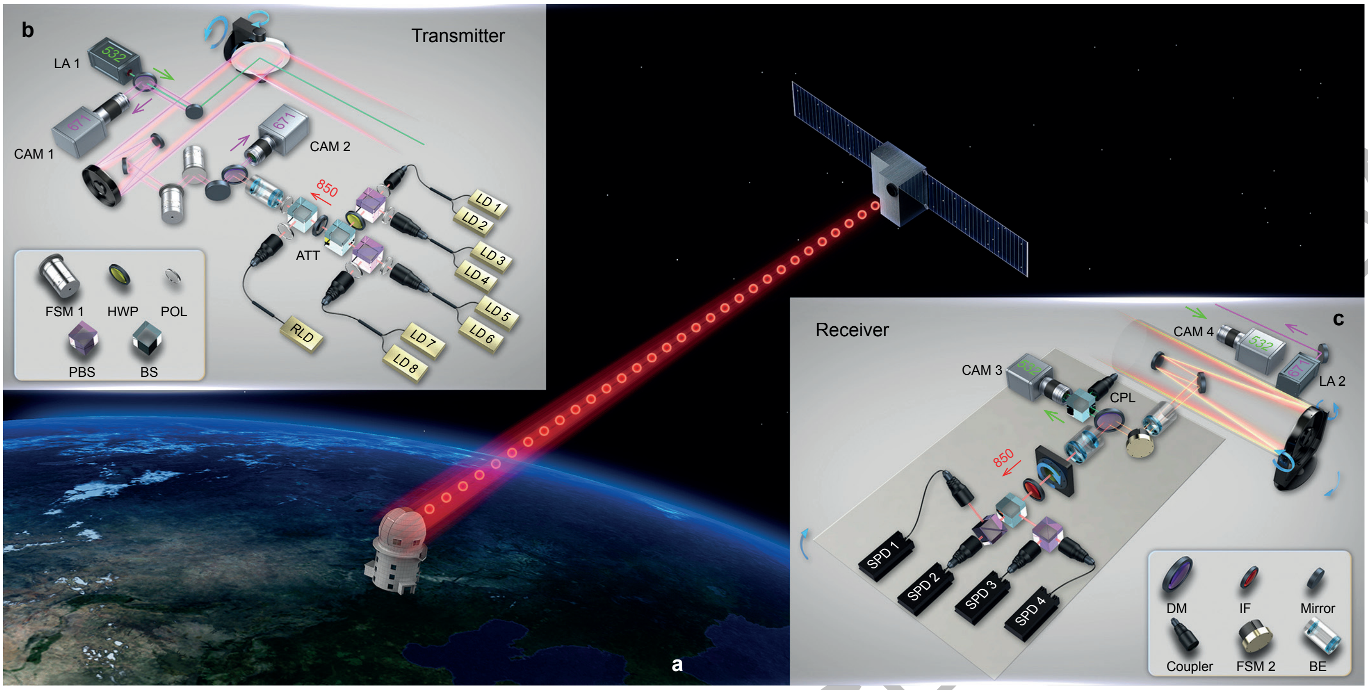


Figure 1 | Illustration of the experimental set-up. a, Overview of the satellite-to-ground QKD. The *Micuis* satellite, weighted 635 kg, flies along a sun-synchronous orbit at an altitude of ~500 km. It is equipped with three space-qualified payloads to accomplish a series of space-scale quantum experiments including QKD, Bell test, and teleportation. **b,** Schematic of the decoy-state QKD transmitter which is one of the satellite payloads. Attenuated laser pulses (~850 nm) from eight separate laser diodes (LD1, ···, LD8) pass through a BB84 encoding module (that consists of two PBSs, a HWP and a BS), co-aligned with a green laser beam (LA1) for system tracking and time synchronization, and is sent out through a 300 mm aperture Cassegrain telescope. After the BB84 module, a ~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 for coarse tracking loop control. Two fast steering mirrors (FSM) and a fast camera (CAM2) are used for fine tracking. **c,** Schematic of the decoy-state QKD decoder in the Xinglong ground station that equipped with a 1000-mm-aperture telescope. The received 532 nm laser is separated by a dichromic mirror (DM) and split into two paths: one is imaged by a camera (CAM3) for tracking, and the other one is detected for time synchronization. The 850 nm decoy-state photons are analyzed by a BB84 decoder that consists of a BS and two PBS, and detected by four single-photon detectors (SPDs). The ground station sends a red laser (LA2) beam to the satellite for system tracking. See Table I for more technical parameters.

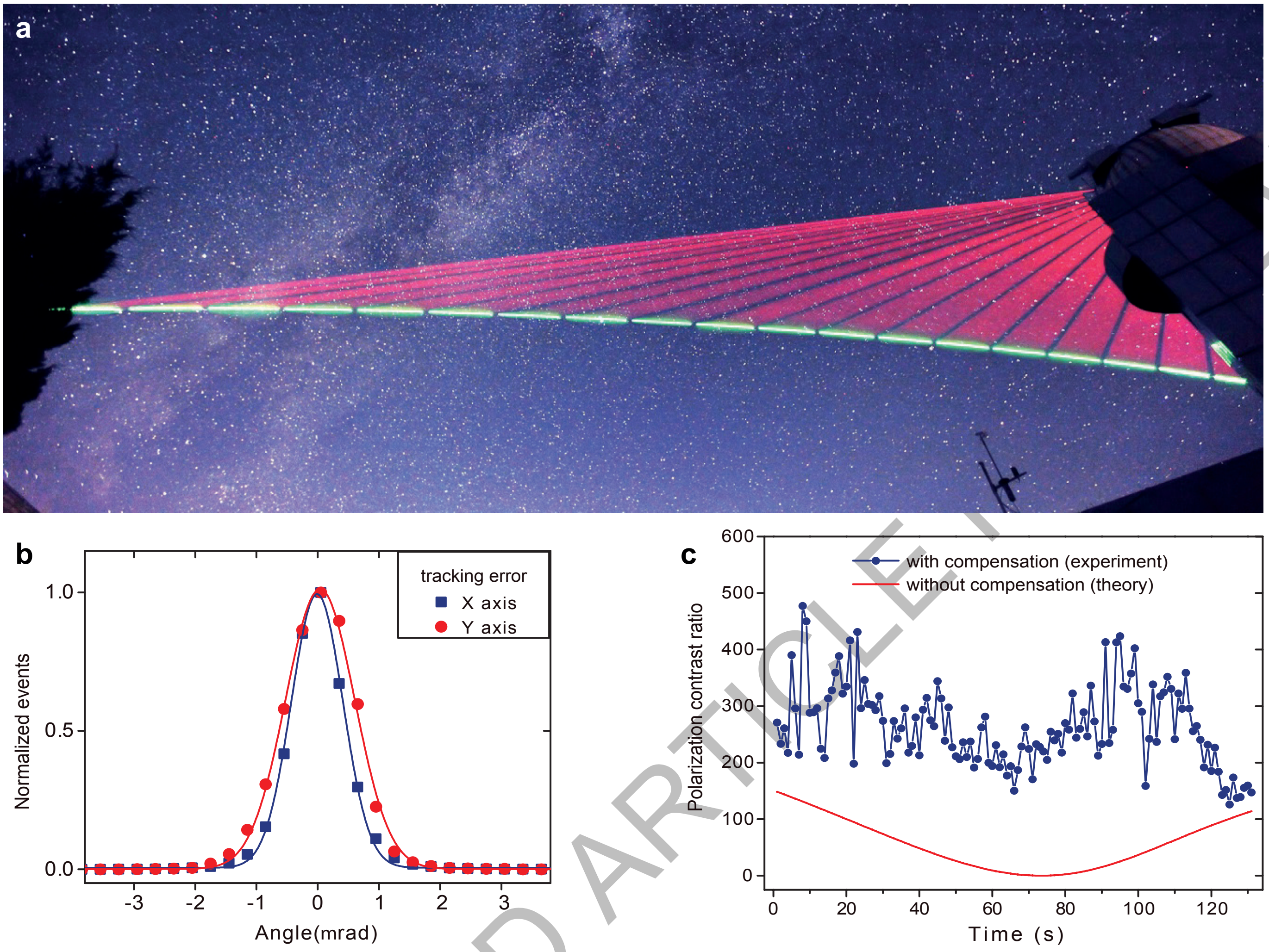


Figure 2 | Establishment of a reliable space-to-ground link for quantum state transfer. a, Overlaid and time-lapse photographs of tracking laser beams as the satellite flies over the Xinglong station. The red and green lasers are sent from the ground and the satellite, respectively, with a divergence of 1.2 mrad. **b,** Long-time tracking error of both X and Y axis extracted from the real-time images read out from the fast camera. **c,** Polarization contrast ratio with and without dynamical compensation during one orbit.

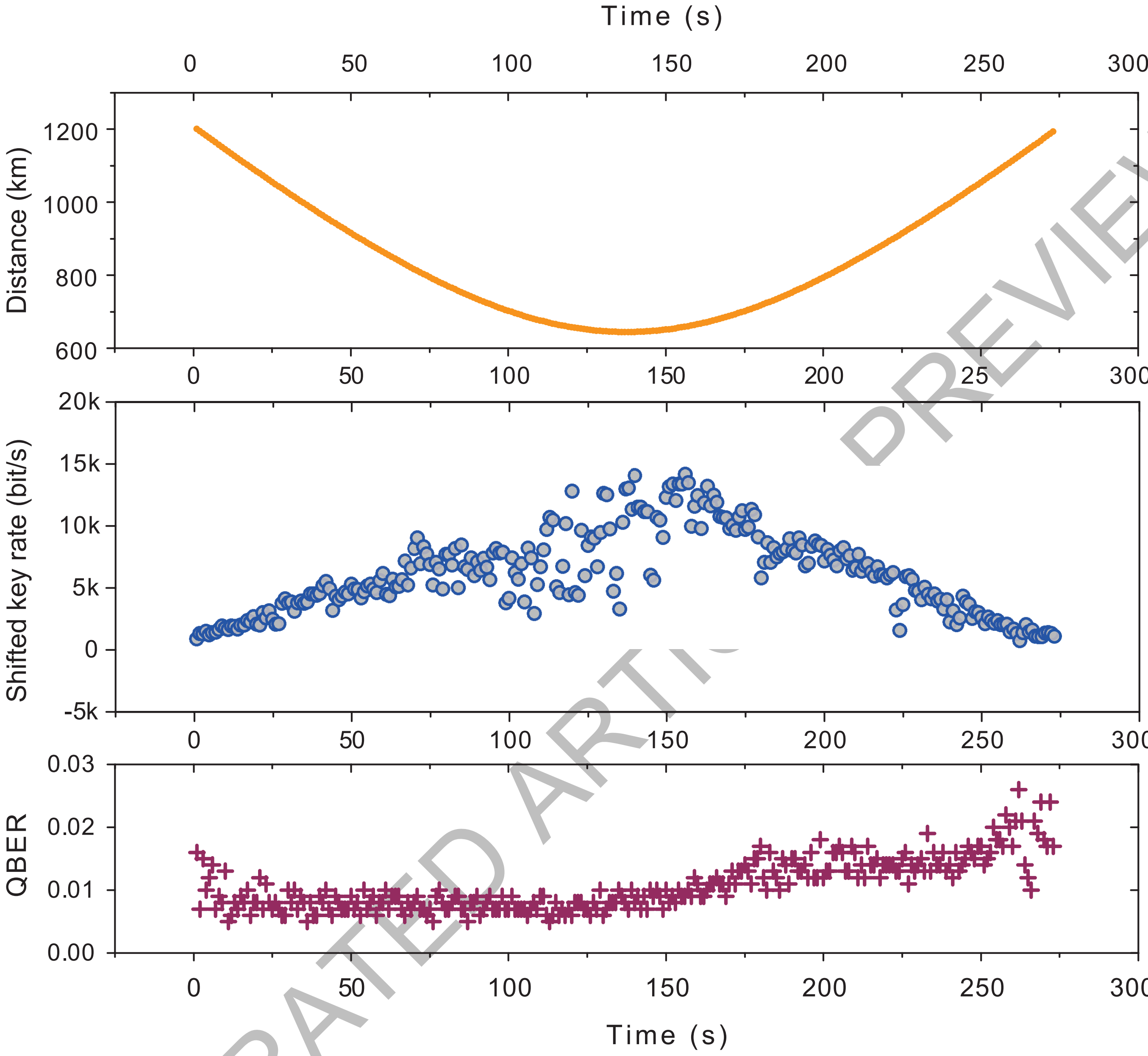


Figure 3 | Performance of satellite-to-ground QKD performance during one orbit. a, The trajectory of the *Micuis* satellite measured from Xinglong ground station. **b,** The sifted key rate as a function of time and physical distance from the satellite to the station. **c,** Observed quantum bit error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

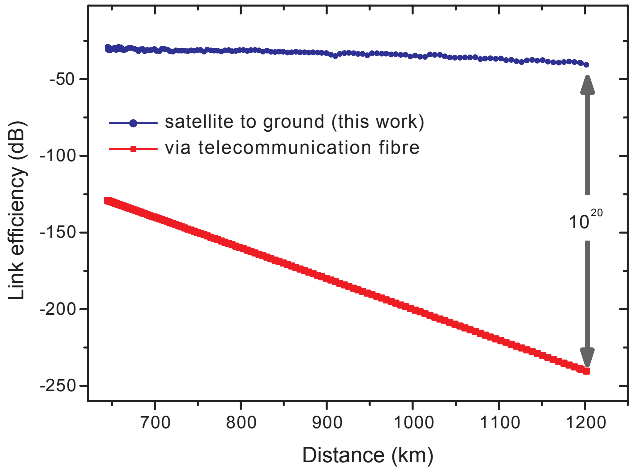


Figure 4 | A comparison of the QKD link efficiencies between the direct transmission through telecommunication optical fibers (red points) and the satellite-to-ground approach (blue points). The link efficiency was calculated by dividing the photon intensity arrived in front of the detectors in the receiving ground station by that at the satellite transmitter's output. At a distance of 1200 km, the latter (within the satellite coverage time) is more efficient than the former by 20 orders of magnitude.

METHODS

China's *Micius* Project: timeline and details. 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 noisy ground atmosphere over Hefei city was achieved, reaching a distance beyond the effective thickness of the aerosphere for the first time[1].

2007: The "Quantum Experiments at Space Scale" project aiming at developing key techniques for performing quantum experiments at the space scale was supported by CAS.

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

2010: Direct and full-scale experimental verifications towards ground-satellite QKD were implemented near Qinghai Lake in West 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, $\sim$50dB)[3].

2011: Quantum teleportation and bidirectional entanglement distribution over $\sim$100 km free-space channel were achieved over the Qinghai Lake[4]. The work showed 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: The construction of the first prototype satellite started.

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. Quantum key distribution experiment and entanglement distribution experiment were conducted between the first prototype satellite payloads and the Delingha observatory station for a distance of 17 km, Quantum teleportation experiment was also conducted between the first prototype satellite payloads and a transmitter placed in the Delingha station.

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

2016: The *Micius* satellite, weighted 635 kg was launched at 1:40AM Beijing time, 16th 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 Figure 2a).

The satellite payloads. The satellite payloads for the QKD experiment are composed of an experimental control box (with a weight of 7.56 kg, Extended Data Figure 2b), an APT control box (9.9 kg, Extended Data Figure 2c) and an optical transmitter (115kg, Extended Data Figure 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 the raw-key sifting, error correction and privacy amplification to get the final secure keys), and encryption management.

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

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

The ground station in Xinglong. The Xinglong observatory is located to the Northeast of Beijing with a distance of $\sim$110 km. The observatory station in Xinglong consists of a Ritchey-Chretien telescope (aperture of 1 m and focal length of 10 m) mounted on a two-axis gimbal (Extended Data Figure 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°, pixels of 512 × 512, frames rates of 56 Hz) (Extended Data Figure 3b), and an optical receiver box located on the arm of the gimbal (Extended Data Figure 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 satellite. Guided by the 532 nm beacon laser, the 671 nm beacon laser equipped 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 Figure 3c). The fine tracking system mainly consists of a FSM based on voice-coil and a fine camera (FOV of 1.3mrad × 1.3mrad, pixels of 128 × 128, frames rates of 212 Hz). A dichromic mirror is used to separate the 850 nm photons from the 532 nm beam. A BS 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 HWP and an interference filter (IF), the 850 nm photons are received by a customized BB84 polarization analysis module. Four multi-mode fibers with core diameter of 105 μm are used to connect the receiver module with four single-photon detectors. All the five single-photon detectors' electric output pulses and a 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. Both the optical transmitter in the satellite and the receiver in the ground station have cascaded multi-stage APT systems (Extended Data Figure 4).

In the transmitter, there is a three-stage APT system. The first stage is the satellite attitude control system that keeps the QKD photons pointing to the ground station with error less than 0.5 degree. The second stage is the coarse control loop that includes a two-axis gimbal mirror (both azimuth and elevation rotation range of 10°) and a CMOS camera (FOV of 2.3° × 2.3° and frames rates of 40 Hz). The third stage is the fine control loop that 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 and frames rates of 2 kHz).

In the receiver, a two-stage APT system is employed. The first stage is the coarse control loop including a two-axis gimbal telescope (azimuth rotation range of -270° $\sim$ +270° and elevation rotation range of -5° $\sim$ +95°) and a CCD camera (FOV of 0.33° × 0.33° and frames rates of 56 Hz). The second stage is the fine control loop that includes a FSM driven by voice-coil (tracking range of ±35 mrad) and a CCD camera (FOV of 1.3 mrad × 1.3 mrad and frames rates of 212 Hz).

At the beginning, based on the predicted orbit of the satellite, the receiver points the satellite with 671 nm beacon laser (2.7 W) in real time. The coarse camera in the satellite detects the 671nm beacon laser to get the tracking error of 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, which is much smaller than the fine camera's FOV. The fine tracking error is below 2 μrad attributed to the feedback control of the FSM and the fine camera.

Simultaneously, optical transmitter in the satellite points a beacon laser (wavelength of 532 nm, optical power of 160 mW and divergence angle of 1.25 mrad) to the ground station. The ground station uses this beacon laser to correct its pointing direction with an error of 1$\sim$2 μrad. Finally, the link is locked on 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 angle to compensate transverse velocity of the two terminals and the speed of light, which is achieved by adjusting the tracking reference of the transmitter's fine tracking loop in real time.

Synchronization. Since the transmitter and the receiver are separated far away and have independent reference clocks, the time synchronization is used to label QKD photon pulse sequences by their arrival time, which can be exploited to distinguish the QKD photons from the background noise. As the distance between the transmitter and receiver changes all the time when the satellite passes over the ground station, both the GPS PPS signal and an assistant pulse laser are employed 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. A part of the laser is guided into a fast photodiode to convert it into electrical pulse signal. Both the pulse signal and the GPS PPS signal from the satellite are fed into the time-to-digital convertor (TDC) module of the transmitter. Acquired data are stored in the memory for further processing. Note that the time base of the TDC module has been synchronized with that of QKD photons modulation module since they share a common clock.

In the receiver, a 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 four single-photon detectors' electrical output pulses and the GPS-PPS signal, is fed into a TDC. Acquired data are stored in the computer for further processing.

The time synchronization between the satellite and the ground can be divided to two steps. First, according to the predicted light-flight-time and the GPS-PPS signal, the received synchronization laser pulse sequence on the ground can be matched with the satellite. Second, based on the result of step 1, the time between the satellite and the ground will be synchronized. Finally, we observe a typical temporal distribution of QKD photons with a standard deviation around 500 ps (Extended Data Figure 5). The signal time window of 2 ns is used. Only the event in the time window is valid.

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

After the satellite launching, we couldn't measure the far-field profile directly as in the ground test. Alternatively, we adopted a scanning method, i.e., measuring the intensity distribution of the 850 nm photons as a function of the transmitter's pointing angle. The obtained profile is shown in Extended Data Figure 5. Such a complete scan usually took a few minutes. As the satellite is fast moving, the satellite-to-ground distance and the atmospheric condition vary with time. The atmospheric turbulence can be fast and occur within a scanning cycle, which can cause the scanning plot distorted. We observe that the in-orbit test (Extended Data Fig. 5) is qualitatively consistent with the ground test results (Extended Data Fig. 5).

The experimental procedure. The experimental instruction and data process of Satellite-to-Ground QKD is shown as Extended Data Figure 6. Six systems work together to implement the QKD experiment, including the scientific experiment plan center, the ground support center, the ground tracking telemetry and command center, the optical ground station, the satellite platform with the payloads.

The whole satellite-to-ground QKD procedure is described as follows (Extended Data Figure 6):

1. The experiment plan center arranged the experiment when the following conditions are guaranteed:

a) the calculated maximum elevation angle of the satellite to the ground station is greater than 30° (based on predicted satellite orbits);

b) the weather is forecasted to be clear and sunny. If so, instruction sequence files for satellite are made and sent to Ground support center. 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.

2. The instruction file is translated to a coding file in ground support center and then sent to the ground tracking telemetry and command center to upload to the satellite.

3. The satellite platform and the payloads along with the optical ground station execute the instructions to transmit QKD photons from satellite to ground:

a) The satellite starts changing the pointing mode from geocentric mode to ground station centric mode at 10 minutes before entering the shadow zone. When the satellite exceeds an elevation angle of 5° from the ground station's horizon plane, 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 appearing above the horizon, the ground station's telescope activates its beacon laser at an elevation angle of 10° above the horizon to wait for the satellite. Once the satellite's elevation angle to the ground station is more than 10°, the open-loop pointing according to the predicted orbit is automatically executed. Meanwhile, the ground station's receiver initiates the data recording and starts to rotate the motorized HWP according to the polarization base compensation curve file.

c) After having an elevation angle of 10° above the horizon, the satellite will be fully covered by the ground station's beacon laser (671 nm). 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 at the ground station.

d) When the ground station receives the beacon laser from the optical transmitter, the APT control will be started to precisely track the satellite beacon laser. Then the bi-directional tracking and locking between the transmitter and receiver is achieved.

e) At an elevation angle of about 15°, the satellite begin 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 the data is stored.

f) When the satellite reaches an elevation angle of approximately 10° in the opposite direction, the transmission of QKD photons and the tracking loop are terminated.

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

Decoy state protocol and key rates. In practical QKD with a lossy channel, the security is undermined by the 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 can be used to verify the lower bound of the single-photon counts.

The main idea of the decoy-state method is to change intensities randomly among several different values in sending out each pulse. Equivalently, we can regard pulses of different intensities as pulses from different sources. In this experiment, we use 3 different intensities 0 for vacuum, μ, and μ' for the decoy state and signal state. In photon-number space, the state of the pulse from a non-vacuum source can be written in

$$\rho_l = \sum_k a_k^l |kk| \tag{1}$$

where

$$a_k^l = \frac{\mu_l e^{-\mu_l}}{k!} \tag{2}$$

is the photon-number distribution of phase-randomized weak coherent states source with intensity μ_l which can be 0, μ, or μ' 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 can introduce averaged value s_k for the counting rate of k-photon state in a certain basis and use constraints

$$S_l = \sum_k a_k^l s_k \tag{3}$$

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

$$S_l = S_l(1+\delta) \tag{4}$$

$$\delta \in [-\delta_1(\xi), \delta_2(\xi)] \tag{5}$$

$$\underline{S_l} = S_l[1-\delta_1(S_l, \xi)] \tag{6}$$

$$\overline{S_l} = S_l[1+\delta_2(S_l, \xi)] \tag{7}$$

With these preparations, we can lower bound the counting rate of single photon pulse $\underline{s_1}$, given the observed values S_l in each bases. Similarly, given the observed values of error E_l, we can also upper bound of single photon pulse bit-flip error rate in each bases and hence upper bound the phase-flip error rate $\overline{e_1}^{ph}$. Finally, we can calculate the secure final key rate of per emissive pulse, R by,

$$R = p_{\mu'}\{a_1'\underline{S_l}[1-H(\overline{e_1}^{ph})] - fS_{\mu'}H(E_{\mu'})\} \tag{8}$$

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

The values of parameters used in experiment are listed in Extended Data Table 3. And 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.

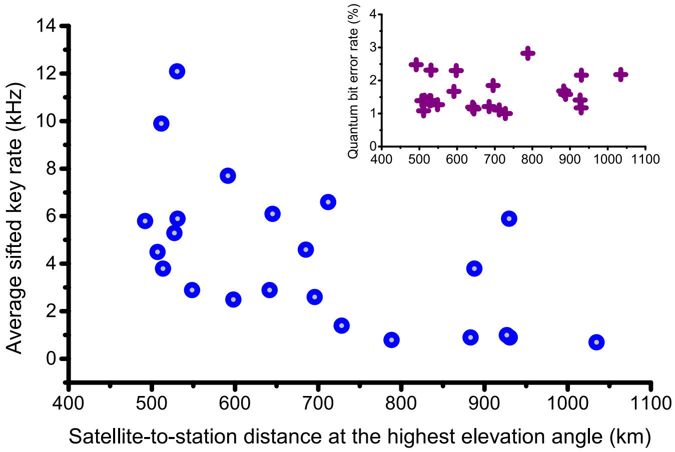
Setting the failure probability $\xi = 10^{-9}$ and the error correction inefficiency $f = 1.4742$ as appeared in our actual key-distillation system, we can get the secure final key rate $R = 1.38 \times 10^{-5}$ corresponding to 377,100 final keys if we use Chernoff bound[32].

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

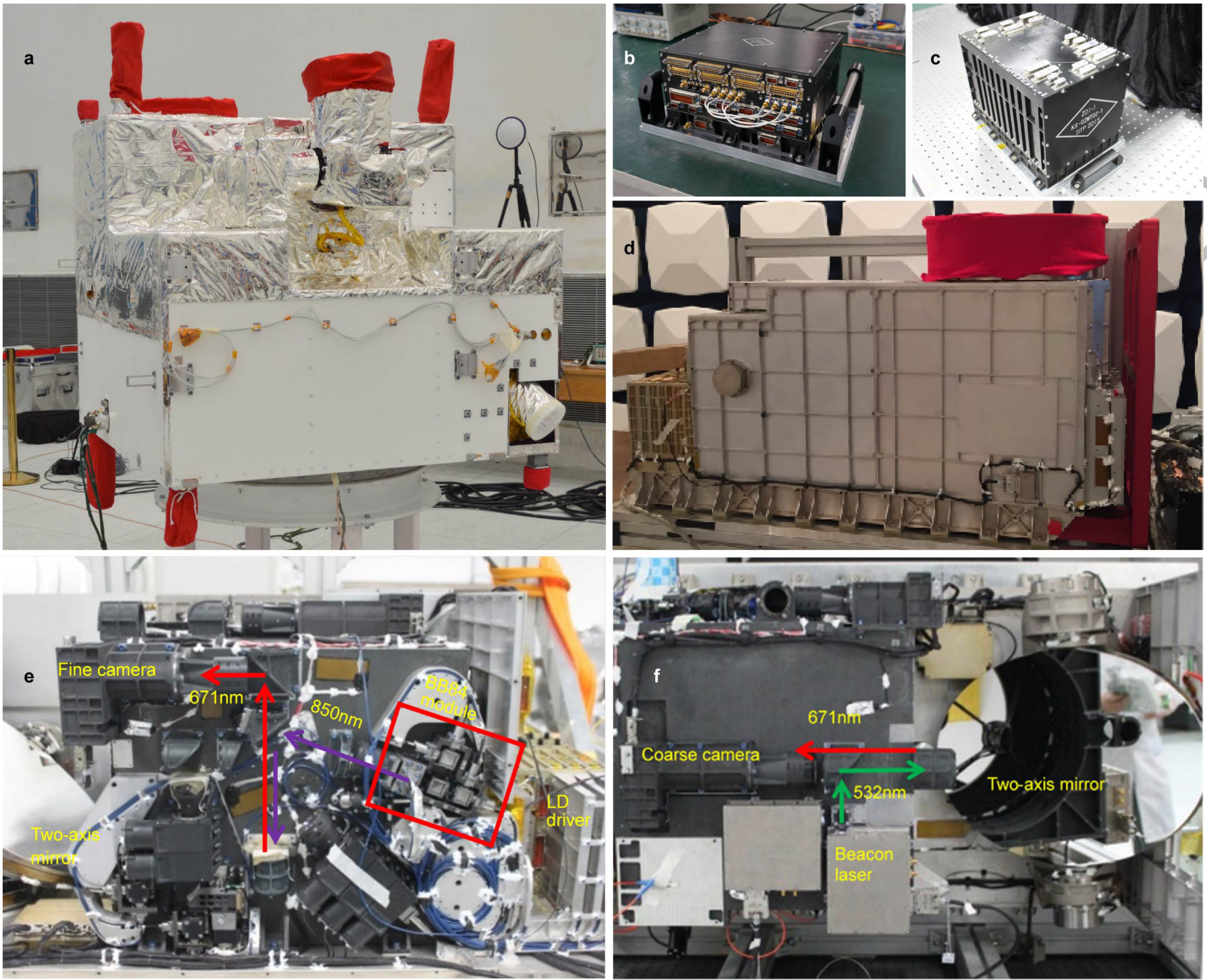
Data availability. The data that support the plots within this paper and other findings of this study are available from the corresponding author upon reasonable request.

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

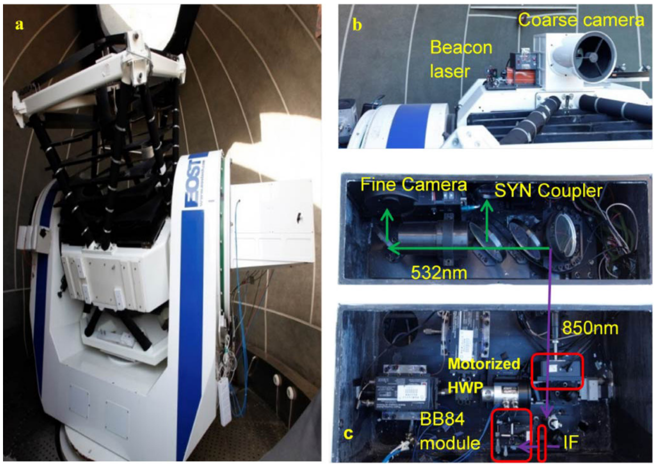
33. Wang, X.-B., Yang, L., Peng, C.-Z. & Pan, J.-W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New J. Phys.* **11**, 075006 (2009).



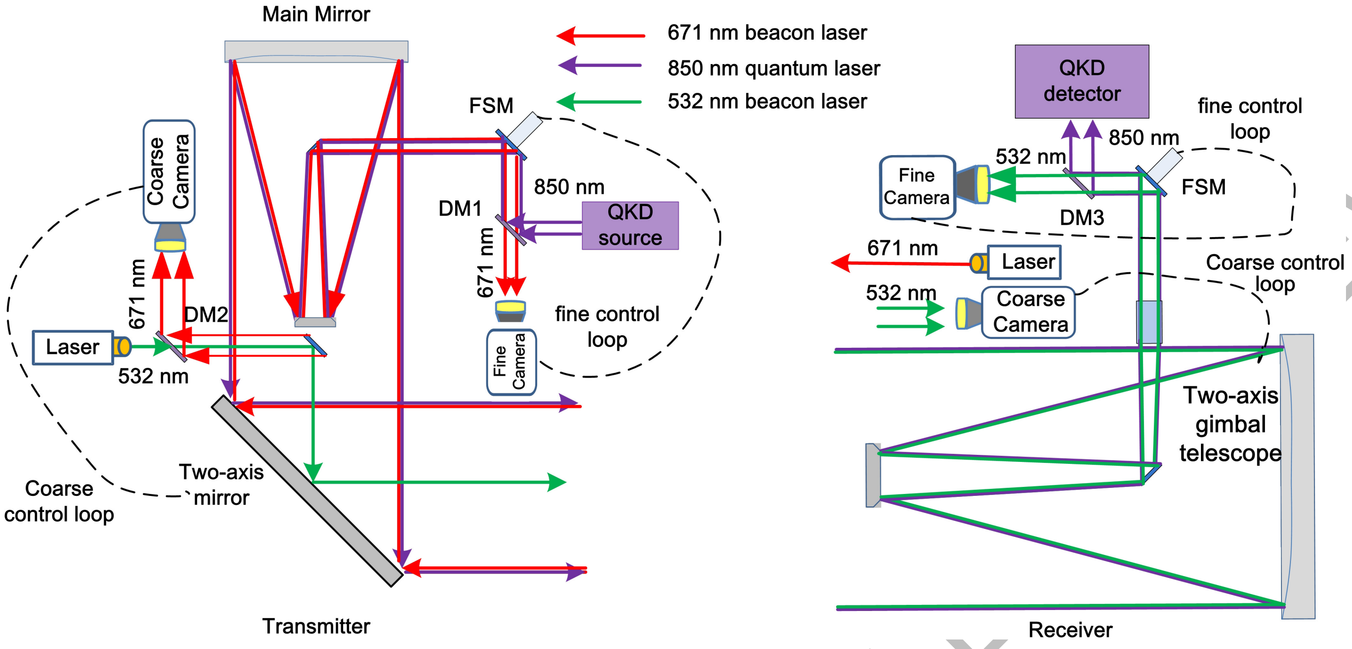
Extended Data Figure 1 | A summary of the QKD data obtained for 23 different days. The *x* axis is the shortest satellite-to-station distance at the highest elevation angle which varies for different days. The *y* axis is the obtained averaged sifted key rate over the whole orbit of 273 s. The inset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



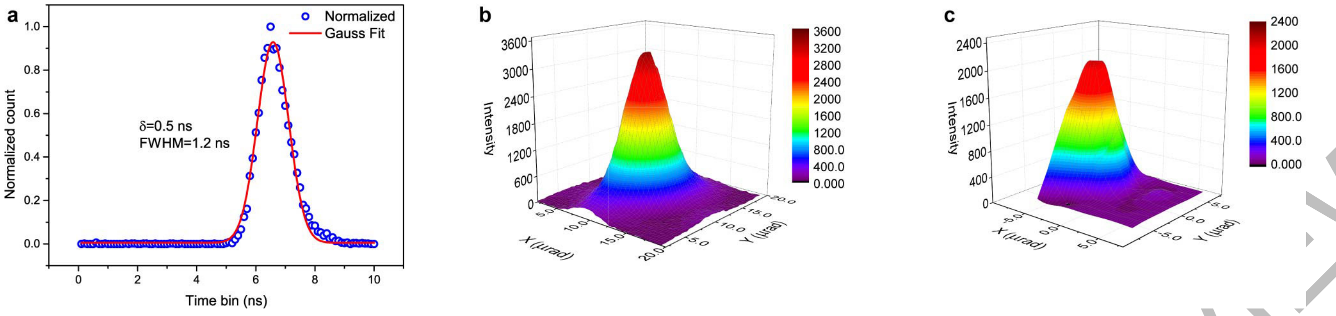
Extended Data Figure 2 | the Micius satellite and the payloads. a, A full view of the Micius satellite before being assembled into the rocket. **b,** The experimental control box. **c,** The APT control box. **d,** Optical transmitter. **e,** Optical transmitter optics head left side view. **f,** Optical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



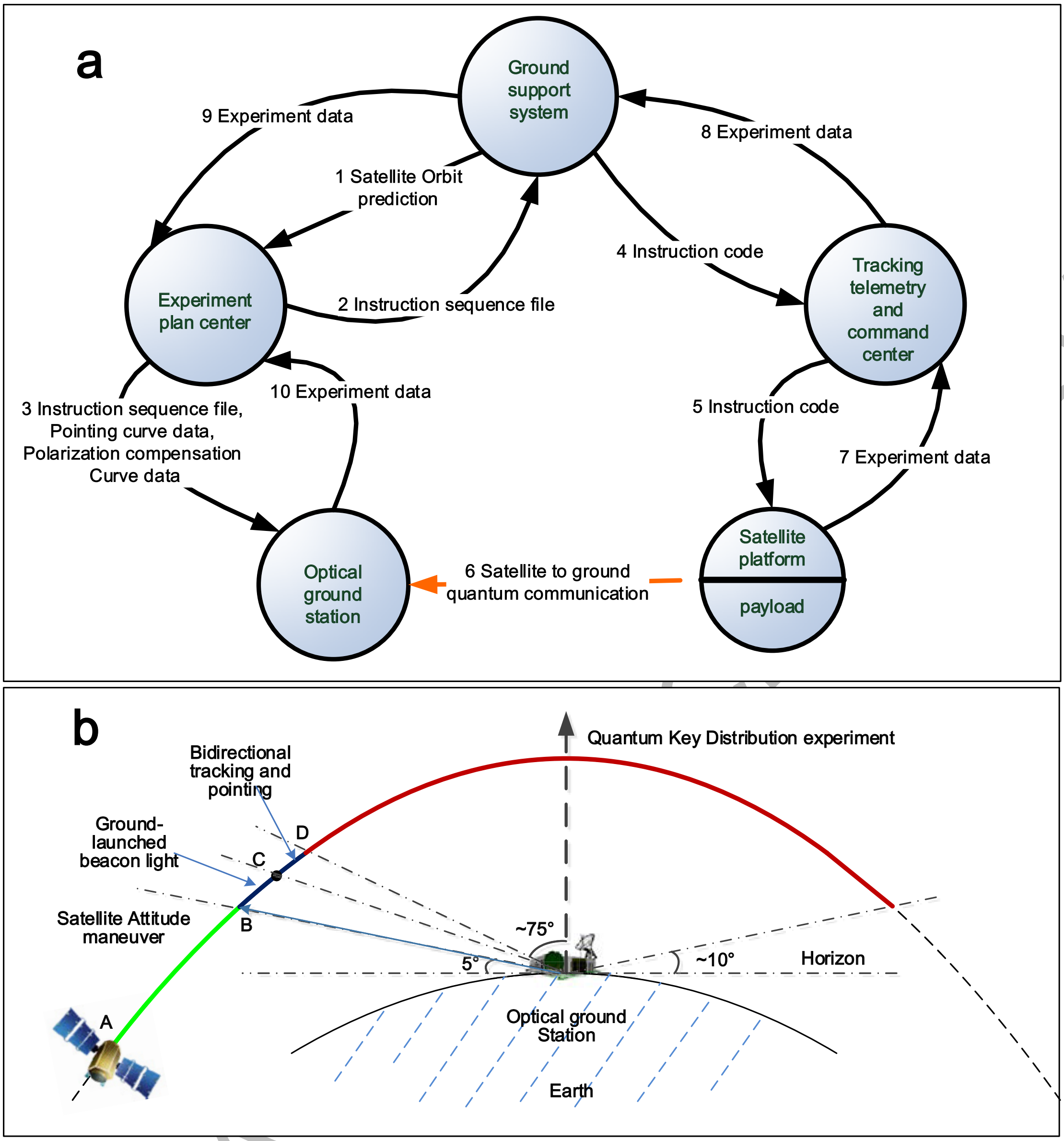
Extended Data Figure 3 | Hardware of Xinglong Ground Station. a, The two-axis gimbal telescope. **b,** Beacon laser and coarse camera. **c,** One of the two layers of the optical receiver box.



Extended Data Figure 4 | A sketch of the tracking systems equipped on satellite and Ground station. DM1: dichroic mirror (T:671 nm; R:850 nm); DM2: dichroic mirror (T:532 nm; R:671 nm); DM3: dichroic mirror (T:532 nm; R:850 nm).



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


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

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

Extended Data Table 1 | Summary of the 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 | A summary of QKD data of 23 different orbits from 23/09/2016 to 22/05/2017

Date	Highest altitude angle (°)	Shortest distance (km)	Peak sifted key rate (kHz)	Average sifted key rate (kHz)	Quantum bit error rate
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 | A summary of the 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	$S_{\mu'}$	S_μ	$E_{\mu'}$	E_μ	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

In the table, T is the effective time for QKD, $Y_0$is the yield for the vacuum states, s_l is the counting rate for source of intensity μ_l, E_l is the QBER 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.