Article

# An integrated space-to-ground quantum communication network over 4,600 kilometres

https://doi.org/10.1038/s41586-020-03093-8

Received: 1 March 2019

Accepted: 2 November 2020

Published online: 6 January 2021

Check for updates

Yu-Ao Chen[1,2]✉, Qiang Zhang[1,2], Teng-Yun Chen[1,2], Wen-Qi Cai[1,2], Sheng-Kai Liao[1,2], Jun Zhang[1,2], Kai Chen[1,2], Juan Yin[1,2], Ji-Gang Ren[1,2], Zhu Chen[1,2], Sheng-Long Han[1,2], Qing Yu[3], Ken Liang[3], Fei Zhou[4], Xiao Yuan[1,2], Mei-Sheng Zhao[1,2], Tian-Yin Wang[1,2], Xiao Jiang[1,2], Liang Zhang[2,5], Wei-Yue Liu[1,2], Yang Li[1,2], Qi Shen[1,2], Yuan Cao[1,2], Chao-Yang Lu[1,2], Rong Shu[2,5], Jian-Yu Wang[2,5], Li Li[1,2], Nai-Le Liu[1,2], Feihu Xu[1,2], Xiang-Bin Wang[4], Cheng-Zhi Peng[1,2]✉ & Jian-Wei Pan[1,2]✉

Quantum key distribution (QKD)[1,2] has the potential to enable secure communication and information transfer[3]. In the laboratory, the feasibility of point-to-point QKD is evident from the early proof-of-concept demonstration in the laboratory over 32 centimetres[4]; this distance was later extended to the 100-kilometre scale[5,6] with decoy-state QKD and more recently to the 500-kilometre scale[7–10] with measurement-device-independent QKD. Several small-scale QKD networks have also been tested outside the laboratory[11–14]. However, a global QKD network requires a practically (not just theoretically) secure and reliable QKD network that can be used by a large number of users distributed over a wide area[15]. Quantum repeaters[16,17] could in principle provide a viable option for such a global network, but they cannot be deployed using current technology[18]. Here we demonstrate an integrated space-to-ground quantum communication network that combines a large-scale fibre network of more than 700 fibre QKD links and two high-speed satellite-to-ground free-space QKD links. Using a trusted relay structure, the fibre network on the ground covers more than 2,000 kilometres, provides practical security against the imperfections of realistic devices, and maintains long-term reliability and stability. The satellite-to-ground QKD achieves an average secret-key rate of 47.8 kilobits per second for a typical satellite pass—more than 40 times higher than achieved previously. Moreover, its channel loss is comparable to that between a geostationary satellite and the ground, making the construction of more versatile and ultralong quantum links via geosynchronous satellites feasible. Finally, by integrating the fibre and free-space QKD links, the QKD network is extended to a remote node more than 2,600 kilometres away, enabling any user in the network to communicate with any other, up to a total distance of 4,600 kilometres.

A quantum network based on trusted relays is feasible with today's technology, and has a widely accepted roadmap for implementation: intracity metropolitan networks over fibre, intercity connections using a backbone and ultralong-distance communication via satellite. Although previous experiments have verified the feasibility of small-scale quantum metropolitan-area networks (QMANs)[11–14,19–22] and key services[23], constructing a practical large-scale quantum wide-area network requires several challenges to be overcome. A practical quantum wide-area network should: (1) be compatible with diverse topological structures that connect distributed users in a large-scale area; (2) address the basic network architecture and administration method; (3) use standard QKD devices that adapt to convenient extension; (4) maintain security against known[3,24] and potential attacks; (5) allow different practical services; and (6) preserve reliability and long-term stability. Similarly to the construction of a classical network, addressing these important issues is not only an engineering problem, but also a scientific one.

For long-distance or intercontinental users, satellite–ground QKD provides the most appealing solution, owing to the low transmission attenuation and negligible decoherence of quantum signals in space (see ref. [25] for a review). There has been substantial progress along this route. The satellite-based QKD with the Tiangong-II space lab

[1]Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Anhui, China. [2]Shanghai Branch, CAS Center for Excellence Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai, China. [3]China Cable Network Co, Beijing, China. [4]Jinan Institute of Quantum Technology, Shandong, China. [5]Key Laboratory of Space Active Opto-Electronic Technology, CAS Shanghai Institute of Technical Physics, Shanghai, China. ✉e-mail: yuaochen@ustc.edu.cn; pcz@ustc.edu.cn; pan@ustc.edu.cn

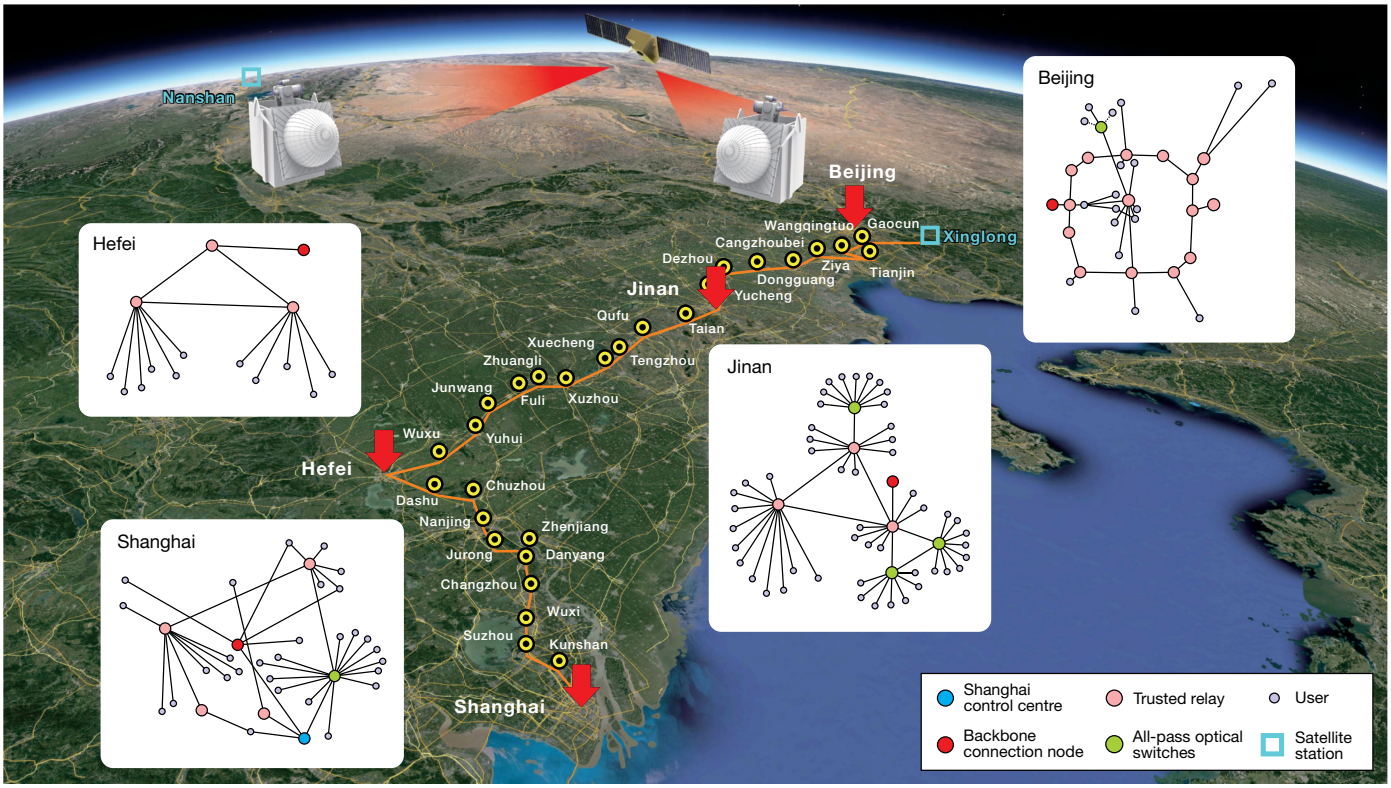



**Fig. 1 | Illustration of the integrated space-to-ground quantum network.** The network consists of four QMANs (in Beijing, Jinan, Shanghai and Heifei; red arrows), a backbone fibre link over 2,000 km (orange line) and two ground–satellite links that connect Xinglong and Nanshan (blue squares), separated by 2,600 km. There are three types of node in the network: user nodes (purple circles), all-pass optical switches (green circles) and trusted relays (pink circles). Each QMAN consists of all three node types (see insets). The backbone is connected by trusted relays (shown as yellow and black circles in the main image and red circles in the insets). A quantum satellite is connected to the Xinglong and Nanshan ground stations; Xinglong is also connected to the Beijing QMAN via fibre. In Beijing, the Beijing control-centre node is located at the same location as the backbone connection node (indicated by the red circle). Map data: Google, Data SIO, NOAA, US Navy, NGA, GEBCO, Landsat/Copernicus; copyright ZENRIN.

implemented a key rate of about 91 bits per second (bps) in a passage with a distance range from 388 km to 719 km[26]. Micius-satellite-based QKD has been implemented, achieving a secret key rate of about 1 kbps (1 kbps = $10^3$ bps) in a passage with a distance range from 645 km to 1,200 km[27]. Intercontinental quantum communication[28] has also been demonstrated, using the satellite as a relay. To push the technique further, suitable for practical applications, it is necessary to increase the key rate by developing high-speed satellite-based QKD.

Here we address the above issues by constructing a large-scale quantum network (Fig. 1), consisting of four fibre QMANs, a long-distance fibre backbone network and two satellite–ground links. On the ground, the fibre network serves more than 150 users, contains 700 QKD fibre links and covers a distance of 2,000 km—collectively more than 10 times larger than existing networks[11–14,19–22]. We develop different types of topology to investigate and address wide ranges of parameters such as the trade-offs between cost, security and performance. Furthermore, we demonstrate several core techniques, including InGaAs/InP and up-conversion single-photon detectors, dense wavelength-division multiplexing for multiple QKD systems, high-efficiency satellite–ground transmission, real-time post-processing and monitoring, adherence with information security standards and, most importantly, countermeasures against known quantum attacks[3].

**Table 1 | Network information**

| Network | Number of relays | Number of nodes | Number of users | Number of links | Average length (km) | Loss (dB) | | | Rate (kbps) | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Minimum | Average | Maximum | Minimum | Average | Maximum |
| Backbone | 32 | 0 | 0 | 135 | 63.8 | 10.3 | 16.0 | 20.5 | 28.1 | 79.3 | 235.4 |
| Beijing | 9 | 19 | 19 | 39 | 29.8 | 2.5 | 9.3 | 13.5 | 2.7 | 12.9 | 32.5 |
| Jinan | 3 | 50 | 95 | 437 | 7.6 | 3.0 | 5.8 | 12.5 | 12 | 26.3 | 47.6 |
| Hefei | 3 | 11 | 14 | 8 | 25 | 2.1 | 5.8 | 10.3 | 2.9 | 19.7 | 49.4 |
| Shanghai | 5 | 26 | 26 | 82 | 27.5 | 5.7 | 9.8 | 13.2 | 2.8 | 11.2 | 19.4 |
| Xinglong | 4 | 1 | 1 | 5 | 51.7 | 10.7 | 14.7 | 20.5 | 2.9 | 16.6 | 40.5 |
| Satellite | 1 | 2 | 2 | 2 | 500–2,043 | 20.0 | | 40.0 | 1.1 | | 47.8 |

The number of users refers to the number of users that are connected; each user node may have more than one user. The number of links refers to number of links between two users. The average length, loss and rate are only for the ground links.

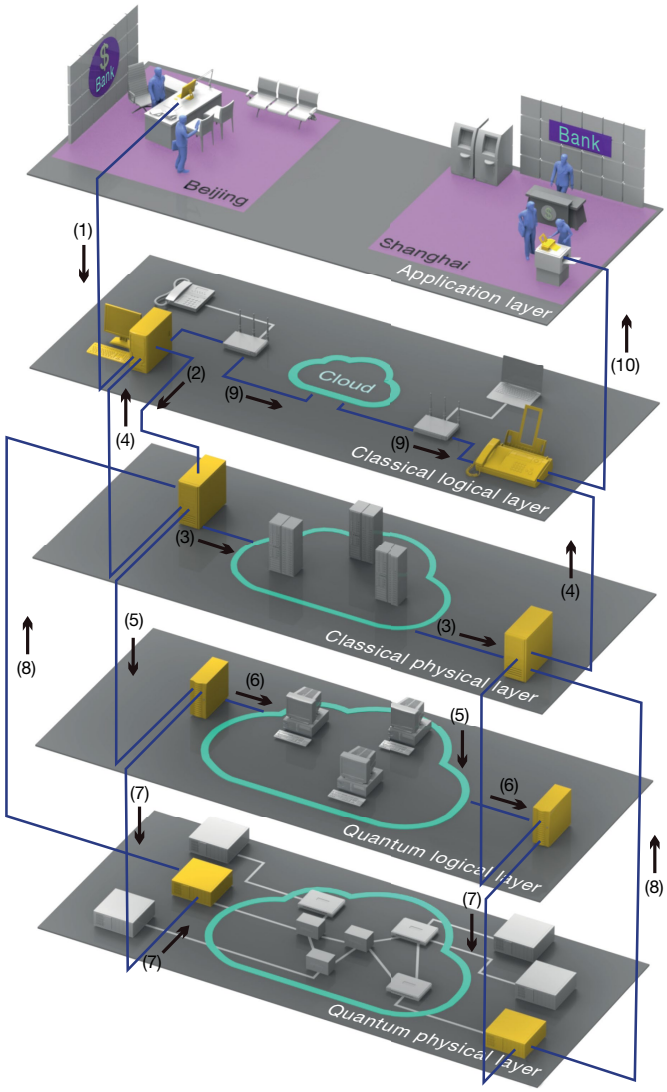



**Fig. 2 | Network architecture and administration.** The network consists of five layers: the application layer, the classical logical layer, the classical physical layer, the quantum logical layer and the quantum physical layer. As an example, we consider how a secure transmission from Beijing to Shanghai works. The message transmission order is sent from the user in Beijing to the computer (1). The computer sends an order to the key management system to ask for the key (2) and to the router to find the classical route for classical information transfer (3). The key management system checks whether the key is sufficient. If it is, it sends the key to the computer (4); otherwise, it sends an order to the quantum system server to generate more keys (5). The quantum system server sends the order to the quantum control system (6), which finds the optimal key generation route and sends the order to generate keys (7). The keys are generated in the quantum physical layer and stored in the key management system (8). After encoding or decoding the message with the key (9), the information can be transferred securely to the user in Shanghai (10).

For satellite–ground links, we achieve high-speed satellite–ground QKD by substantially enhancing the system design in hardware and software. In hardware, we optimize the optical systems in the ground receiver and increase the clock rate of the QKD system; in software, we apply a more efficient QKD protocol to generate secret keys[29–31]. Consequently, the achieved key rates are maintained at 47.8 kbps, 40 times higher than previous work[27]. Furthermore, we extend the satellite–ground QKD distance from 1,200 km[26–28] to 2,000 km, with a corresponding coverage angle of about 170° (nearly the whole sky). This channel loss is comparable to that between a medium-Earth-orbit satellite and the ground (roughly 40,000 km). Finally, by integrating the fibre-space links in our network, a remote user at Nanshan (Fig. 1) can perform QKD with any node in the backbone network without the need for additional ground stations or fibre links.

## Metropolitan networks

For the four metropolitan networks, we explore different types of topology. For the Beijing network (Fig. 1), circle, tree and star topologies are used (each line represents a QKD link). The circle network consists of 12 trusted nodes; the circle topology has the advantage of avoiding failure or denial of service of a single node. The Beijing control-centre node, one of the 12 circle nodes, takes the controlling role of the whole network. Most of the end users are connected to the trusted nodes, forming a star topology structure. Most of the end users are equipped with only QKD emitters, no single-photon detectors[21], which greatly reduces the cost (single-photon detectors are the most expensive part of a QKD system). However, some nodes have emitters and single-photon detectors for flexibility; for example, the starting node of the backbone line is connected to the Beijing control-centre node. The Xinglong observatory node, where the quantum key is generated between the Micius satellite and the ground station, is also connected to the Beijing control-centre node.

All the end users share a quantum key with their neighbouring trusted node, through which they can further share it with everyone in the network. However, there are some higher-level end users who, for example, in the future, would like to pay more for enhanced security. For these users, we offer an all-pass optical switch, which can maximally connect 16 users and help to generate quantum keys directly between any two connected users. Acting as an intermediate node for the all-pass optical switch, all the users can be connected via the switch, forming a tree-type network. In total, the Beijing network has 12 trusted-node users and 19 end users.

The Hefei, Jinan and Shanghai networks have similar designs to the Beijing network (Fig. 1). The Jinan network has the largest number of user nodes, up to 50. The Jinan network was constructed from November 2011 to November 2013. The network consists of 50 nodes, including 3 trusted relays as the major nodes for three subnetworks, 3 all-pass optical switches, 50 user nodes, 95 users and 437 QKD links. Details of the four networks are summarized in Table 1.

## Backbone network

The backbone network constitutes a line topology, with 32 trusted relay nodes and 31 links. To establish a large-scale quantum communication network that can efficiently support a large number of users, we use a network architecture that consists of five layers[12–14]: quantum physical layer, quantum logical layer, classical physical layer, classical logic layer and application layer (Fig. 2a). Taking an example of how the network works, we consider the procedure of secure data transfer from the Beijing QMAN to the Shanghai QMAN. At the application layer, the user sends the data transfer request, which distributes an order to the classical logic layer. To send the message in a classical network, the classical logic layer sends the order to the classical physical layer to prepare the message, and finds an optimal route for message transfer. The classical physical layer first checks whether there are sufficient shared keys. If there are too few, it sends an order to the quantum logical layer, which finds the optimal path for QKD; if there are enough, it encodes and then sends the message along the path provided by the classical logical layer. The quantum logical layer controls the generation, storage and transmission of the keys, and the routeing of two nodes via an optical switch. Note that using an optical switch cannot increase the transmission distance. The quantum physical layer generates nearly

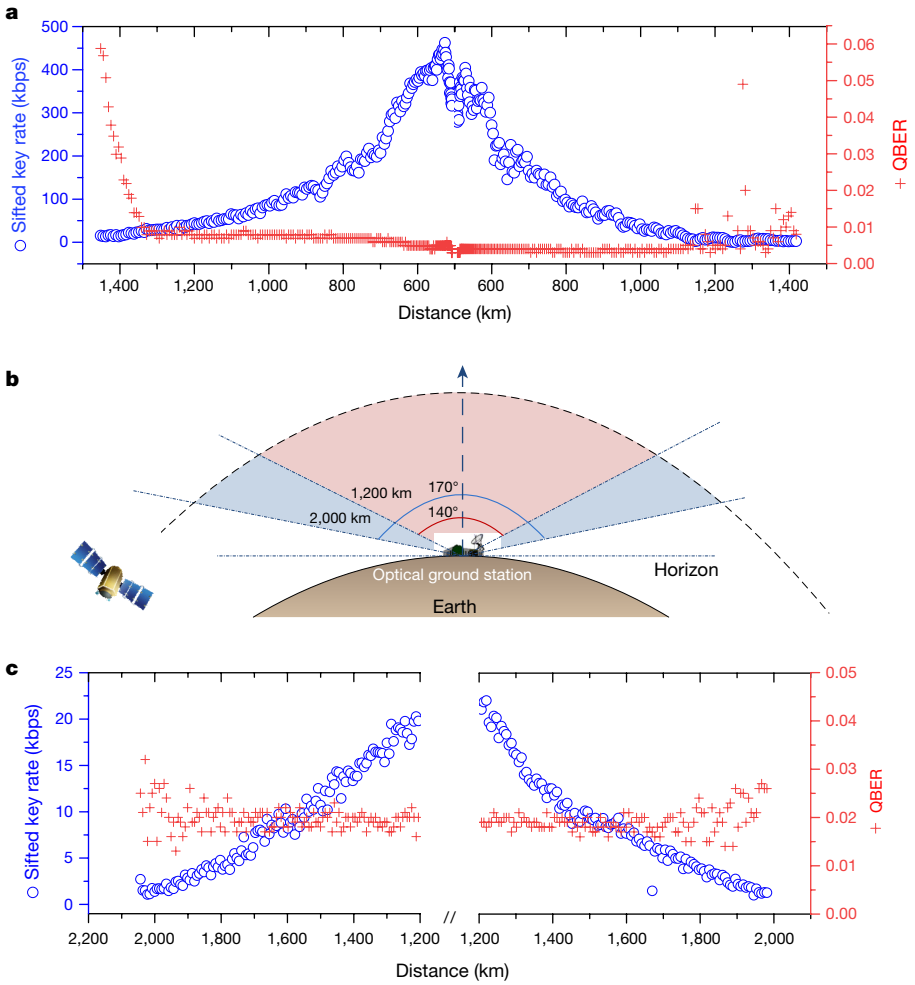



**Fig. 3 | Performance of high-speed satellite-to-ground QKD. a**, The sifted key rate (blue circles; left axis) and observed QBER (red plusses; right axis) as a function of physical distance from the satellite to the Nanshan station. **b**, Illustration of the coverage angle for high-speed satellite–ground QKD. The coverage angle (communication distance) has been extended from about 140° (about 1,200 km; red)[27] to about 170° (about 2,000 km; blue). **c**, The test for long-distance satellite–ground QKD, illustrated by the sifted key rate (blue circles; left axis) and observed QBER (red plusses; right axis) at a distances of more than 1,200 km.

the same number of keys in idler time, and offers prior key generation between two requested nodes. It is the physical layer that implements key generation between two nodes. The hardware at a backbone node is shown in Extended Data Fig. 1.

The network information and key generation rates for the quantum network are shown in Table 1. Each user node can connect multiple users. The average key rates for the Beijing, Jinan, Shanghai and Hefei networks, the backbone and the Xinglong ground network are 12.9 kbps, 26.3 kbps, 19.7 kbps, 11.2 kbps, 79.3 kbps and 19.6 kbps, respectively. To guarantee a higher secure key rate over the main backbone line, we explore using more than one pair of QKD systems. Specifically, we use dense wavelength-division multiplexing to run several pairs of devices simultaneously in a backbone fibre link. The insertion loss caused by normal dense wavelength-division multiplexing is less than 1 dB. Compared to one pair of devices, the key rate using several pairs may be increased by more than a factor of five.

## High-speed satellite-to-ground QKD

There are two ground stations, located in Xinglong and Nanshan (Fig. 1, Extended Data Fig. 2). The distance between them is about 2,600 km. A space-qualified QKD transmitter based on a decoy-state Bennett–Brassard 1984 (BB84) protocol was installed in Micius[27]. The repetition rate of the source was improved from 100 MHz to 200 MHz by using the backup design. We improve the optical spatial-mode matching between the incident beam and the collection system on the ground (Extended Data Fig. 3) by reducing the total magnification, including the receiving telescope and the expander in the optical box from 1,500 times to 450 times, to match the whole receiver system and to improve collecting efficiency. By reducing the magnification of the telescope, the field-of-view of the optical receiving system is increased and the signal strength is enhanced. Meanwhile, given the diameter of the receiving telescope is 1,200 mm, the beam waist size before entering the BB84 module is increased from 0.8 mm to 2.7 mm. The BB84 module is also modified to match the larger size of incident light beam. In total, after these enhancements, the receiving efficiency of the ground station is enhanced by a factor of three compared with the previous experiment[27]. At the same time, a new 5-nm spectral filter is used to replace the 10-nm one, to suppress the background noise further. To achieve highly productive satellite-based QKD, we applied an efficient decoy-state BB84 protocol with biased basis choice[29–31] (Methods).

The Micius satellite flies along a Sun-synchronized orbit with an altitude of about 500 km and passes over the ground stations at around 00:00 local time, allowing for a downlink QKD experiment. In Fig. 3a, we show the experimental data in a typical duration (364 s) between Micius and the Nanshan ground station. During the experiment process, the

communication distance ranges from 508 km to more than 1,200 km, a 58.1-Mbit sifted key is collected and the average quantum-bit error rate (QBER) is 0.50%. The highest sifted key rate (462 kbps) is reached near the central points of the orbit. We extracted the final secure key following the efficient BB84 post-processing procedure[30]. In security analysis, by considering statistical fluctuation, the failure probability is set to $10^{-9}$ and the final key rate of 47.8 kbps is achieved—40 times higher than in previous work[27] (Extended Data Table 2).

With the optimized detection efficiency, we are able to record data even when the satellite is near the horizon. By enabling a function that automatically adjusts the exposure time of the tracking cameras in the satellite and by adjusting the sample rate and exposure time of the tracking cameras in the ground station according to the distance variation, we successfully construct a link at an elevation angle of around 5°. This enables us to perform the QKD experiment from Micius to the Nanshan station with a longer data recording time (Fig. 3b). For the satellite, the adjustment of exposure time and sampling rate is controlled automatically by a pre-injected adaptive algorithm. For the cameras at the ground stations, it is realized by the operator's active judgment and intervention, but may be upgraded to an automatic realization in future.

In Fig. 3c, we show the data for standard QKD for a typical passage over a distance of more than 1,200 km. As the transmission distance increases, the QBER becomes higher and the sifted key rate and signal-to-noise ratio decrease. When the distance reaches the maximum of 2,043 km, at an elevation angle of 5°, the QBER is about 2.5% and a sifted key rate of 2 kbps is attained. The channel loss at 2,043 km is comparable to that between a geostationary satellite and the ground, which demonstrates the feasibility of constructing a quantum geosynchronous satellite. For such a satellite, the divergence angle of the satellite-based transmitting telescope will need to be reduced to 3 μrad and the diameter of the ground-based receiving telescope increased to 2 m (Extended Data Table 3).

We can typically obtain a total secret key size of about 36 Mbit per week. For application, we typically use the AES-128 protocol[28] in our implementation. For each pair of satellite users (mainly for banks), the secret keys are updated and refreshed at 8 Kbit (64 seeds of 128 secret keys) every 10 days. The keys generated via one satellite (36 Mbit per week) thus support about 6,000 users. So far, the key rate is limited by the passing time of the low-Earth-orbit Micius satellite (Methods). In future, with a geosynchronous satellite and multiple satellites that form a satellite constellation, the secret key rate may be enhanced substantially. The performance of a satellite constellation and the user–application cases are analysed thoroughly in ref. [25].

## QKD implementation, security and reliability

For the fibre network, we use a polarization-encoding decoy BB84[32,33] implementation, with commercial compact devices at two clock rates—40 MHz and 625 MHz for the metropolitan and backbone networks, respectively. The secret key rates are typically around 5 kbps and 80 kbps. The specific implementations of the QKD systems are shown in Extended Data Figs. 4–6. There are two types of single-photon detector, InGaAs/InP[34,35] and up-conversion[36]. The details of the implementation are provided in Methods.

As a key ingredient for a secure QKD network, the system should be resistant to the security issues due to the imperfections of realistic devices[24]. Several attacks have been demonstrated over the past few years[3], such as the photon-number-splitting attack, blinding attack, time-shift attack, wavelength-dependent attack and some potential Trojan-horse attacks. We have maintained resistance for the above known attacks; the specific implementations of countermeasures are shown in Methods and Extended Data Table 1.

A practical network should also maintain stability and reliability to unexpected events. In each QMAN, the QKD route between every two nodes is adjusted in real time to overcome node failures. As an illustration, in Fig. 4a, we plot the average key rate of the backbone for a one-year period (2017). Here, the key rate between two places is the minimal key rate of all the intermediate connections. We plot the key rates of the backbone between two nearby QMANs, that is, from Beijing to Jinan, Jinan to Hefei, and Hefei to Shanghai. The system tends to be stable, with a minimal key rate generally more than 20 kbps, except for the early stage while the link is initially stabilized. In Supplementary Information, we present the reliability test results of the Jinan QMAN, which has run continuously for 17 months and passed tens of thousands of service tests, with a success probability of more than 99%.

In Fig. 4b, we present an example one-month (December 2017) test of the backbone network, with average key rates between every two adjacent nodes shown (see Supplementary Information for further details). The key rates of all 31 backbone links are much higher than 28 kbps, with the maximal key rate reaching 235.4 kbps. Similarly to previous QKD networks[12–14], our secret key calculation uses the standard decoy-state analysis. In future, using the recent advances of security proofs for practical QKD[37], the effect of device imperfections may also be included in the key-rate calculation (Methods). More than two-thirds of the backbone links produce a key rate larger than 50 kbps. In future, another backbone will be built from Beijing to Shanghai to form a large circle-type backbone QKD network. In so doing, the whole network

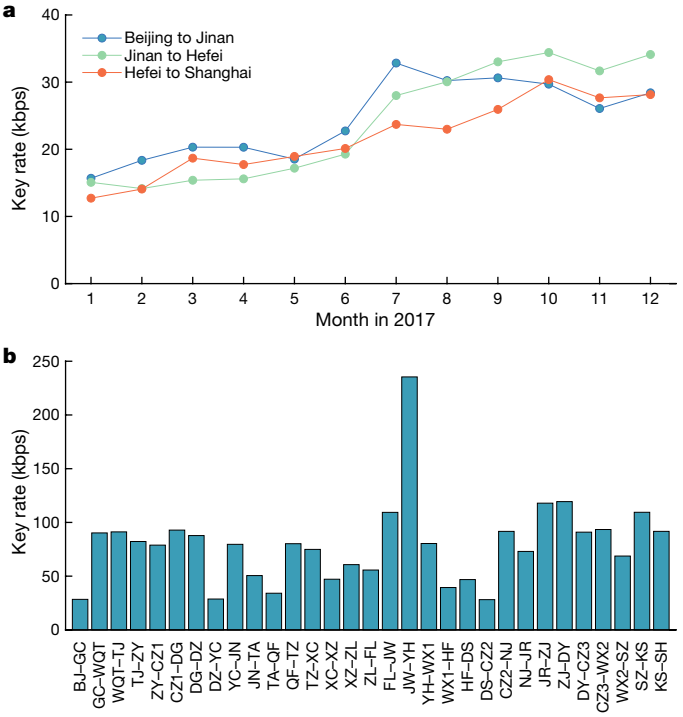



**Fig. 4 | Reliability test for the backbone network. a**, Illustration of the reliability test for the backbone network over a one-year period (2017). The plotted data points of key rates between two cities represent the minimal key rates of all the intermediate backbone connections involved. The error bars due to statistics are smaller than the data points. **b**, Reliability test for the backbone network in December 2017. The presented data are the average key rate between two adjacent backbone nodes. The key rates of all 31 links are higher than 28.4 kbps, with the maximal key rate reaching 235.4 kbps. More than two-thirds of the links produce a key rate larger than 50.0 kbps. BJ, Beijing; GC, Gaocun; WQT, Wangqingtuo; TJ, Tianjin; ZY, Ziya; CZ1, Cangzhoubei; DG, Dongguang; DZ, Dezhou; YC, Yucheng; JN, Jinan; TA, Taian; QF, Qufu; TZ, Tengzhou; XC, Xuecheng; XZ, Xuzhou; ZL, Zhuangli; FL, Fuli; JW, Junwang; YH, Yuhui; WX1, Wuxu; HF, Hefei; DS, Dashu; CZ2, Chuzhou; NJ, Nanjing; JR, Jurong; ZJ, Zhenjiang; DY, Danyang; CZ3, Changzhou; WX2, Wuxi; SZ, Suzhou; KS, Kunshan; SH, Shanghai.

will be able to maintain operation even when one trusted relay of the backbone fails. Furthermore, we have performed maintenance and other practicality issues during the real-life operation of the network (Methods).

## Discussion and conclusion

We have presented a practical large-scale quantum network that consists of four QMANs, a national-scale backbone and a satellite–ground network. This work shows that quantum technology is sufficiently mature for practical applications. A global quantum network can be realized by connecting more national quantum networks from different countries via ground connections or ground–satellite links. With developments in manipulating quantum signals between remote parties, future work could extend to new QKD schemes such as measurement-device-independent QKD[38], twin-field QKD[39] or generic quantum communication protocols. By combining measurement-device-independent QKD and well calibrated devices, practical QKD systems could provide sufficient security under realistic conditions[3]. Our backbone network can be updated directly to adopt these new schemes. First, measurement-device-independent QKD is well suited for star-type quantum access metropolitan networks[21,40]. The star-type topology is the key structure in our four metropolitan networks (Fig. 1). Second, the decoy-state transmitters for measurement-device-independent QKD and BB84 are essentially the same[38]. Hence, the transmitter systems in the current fibre network can also be used to realize the measurement-device-independent QKD network. Finally, it will be interesting to investigate the experimental implementation of twin-field QKD in the backbone network for long-distance transmission. Furthermore, with the extension of the backbone, more sophisticated topology (including a complete loop) will be formed, enabling possibilities such as secure time-frequency transfer[41], fundamental tests of quantum gravity[42] and large-scale interferometry for metrology applications[43,44]. With the development of quantum memory[18], it might also be possible to realize distributed quantum computing[45] and quantum repeaters[16,17] over large areas in the near future.

## Online content

Any methods, additional references, Nature Research reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41586-020-03093-8.


1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing* 175–179 (IEEE, 1984).
2. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett*. **67**, 661–663 (1991).
3. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys*. **92**, 025002 (2020).
4. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *J. Cryptol*. **5**, 3–28 (1992).
5. Rosenberg, D. et al. Long-distance decoy-state quantum key distribution in optical fiber. *Phys. Rev. Lett*. **98**, 010503 (2007).
6. Peng, C.-Z. et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Phys. Rev. Lett*. **98**, 010505 (2007).
7. Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett*. **117**, 190501 (2016).
8. Boaron, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett*. **121**, 190502 (2018).
9. Chen, J.-P. et al. Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett*. **124**, 070501 (2020).
10. Fang, X.-T. et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photon*. **14**, 422–425 (2020).
11. Elliott, C. et al. Current status of the DARPA quantum network. *Proc. SPIE* **5815**, 138–150 (2005).
12. Peev, M. et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys*. **11**, 075001 (2009).
13. Chen, T.-Y. et al. Field test of a practical secure communication network with decoy-state quantum cryptography. *Opt. Express* **17**, 6540–6549 (2009).
14. Sasaki, M. et al. Field test of quantum key distribution in the tokyo QKD network. *Opt. Express* **19**, 10387–10409 (2011).
15. Qiu, J. et al. Quantum communications leap out of the lab. *Nature* **508**, 441–442 (2014).
16. 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).
17. Duan, L.-M., Lukin, M., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413–418 (2001).
18. 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).
19. Stucki, D. et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys*. **13**, 123001 (2011).
20. Wang, S. et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **22**, 21739–21756 (2014).
21. Fröhlich, B. et al. A quantum access network. *Nature* **501**, 69–72 (2013).
22. Tang, Y.-L. et al. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X* **6**, 011024 (2016).
23. Tysowski, P. K., Ling, X., Lütkenhaus, N. & Mosca, M. The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD). *Quantum Sci. Technol*. **3**, 024001 (2018).
24. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon*. **8**, 595–604 (2014).
25. Vergoossen, T., Loarte, S., Bedington, R., Kuiper, H. & Ling, A. Modelling of satellite constellations for trusted node QKD networks. *Acta Astronaut*. **173**, 164–171 (2020).
26. Liao, S.-K. et al. Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab. *Chin. Phys. Lett*. **34**, 090302 (2017).
27. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
28. Liao, S.-K. et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett*. **120**, 030501 (2018).
29. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol*. **18**, 133–165 (2005).
30. Wei, Z. et al. Decoy-state quantum key distribution with biased basis choice. *Sci. Rep*. **3**, 2453 (2013).
31. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
32. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett*. **94**, 230503 (2005).
33. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett*. **94**, 230504 (2005).
34. Liang, X.-L. et al. Fully integrated InGaAs/InP single-photon detector module with gigahertz sine wave gating. *Rev. Sci. Instrum*. **83**, 083111 (2012).
35. Zhang, J., Itzler, M. A., Zbinden, H. & Pan, J.-W. Advances in InGaAs/InP single-photon detector systems for quantum communication. *Light Sci. Appl*. **4**, e286 (2015).
36. Shentu, G.-L. et al. Ultralow noise up-conversion detector and spectrometer for the telecom band. *Opt. Express* **21**, 13986–13991 (2013).
37. Pereira, M., Curty, M. & Tamaki, K. Quantum key distribution with flawed and leaky sources. *npj Quantum Inf*. **5**, 62 (2019).
38. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett*. **108**, 130503 (2012).
39. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
40. Wei, K. et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X* **10**, 031030 (2020).
41. Dai, H. et al. Towards satellite-based quantum-secure time transfer. *Nat. Phys*. **16**, 848–852 (2020).
42. Xu, P. et al. Satellite testing of a gravitationally induced quantum decoherence model. *Science* **366**, 132–135 (2019).
43. Clivati, C. et al. Large-area fiber-optic gyroscope on a multiplexed fiber network. *Opt. Lett*. **38**, 1092–1094 (2013).
44. Marra, G. et al. Ultrastable laser interferometry for earthquake detection with terrestrial and submarine cables. *Science* **361**, 486–490 (2018).
45. Ladd, T. D. et al. Quantum computers. *Nature* **464**, 45–53 (2010).

# Methods

### QKD implementations

We provide the details of the three different types of QKD implementation.

The first implementation—called the 625-MHz QKD system—is based on a passive modulated decoy-state QKD scheme[46]. As shown in Extended Data Fig. 4, the signal and decoy states are generated by four laser diodes, and four single-photon detectors are used to detect the four polarization states. Here, signal pulses in the C band are prepared and the pulse train is internally modulated to 70-ps width. The mean photon numbers of the signal state, decoy state and vacuum state are typically around 0.6, 0.2 and 0, respectively, with an emission ratio of 6:1:1 that is controlled by physical random number generators. Moreover, to guarantee the stability, the automatic polarization feedback system is implemented using two electric polarization controllers at Bob's site to adjust the extinction ratio between the orthogonal states. Meanwhile, a synchronized clock signal between Alice and Bob at 1,490 nm propagates along QKD signals with a repetition rate of 100 kHz and a received optical power of about −53 dBm.

A schematic of the second implementation—called the 40-MHz QKD system (type I)—is shown in Extended Data Fig. 5. In this system, four laser diodes are used to produce signal states with different polarization. The decoy state is achieved by directly modifying the current of each laser diode.

Different from the previous systems, one laser diode is used to produce the optical pulses in the third implementation—called the 40-MHz QKD system (type II) (Extended Data Fig. 6). The four polarization states are realized by using a Sagnac-based polarization encoding scheme. The decoy state is modified with an external intensity modulator.

In all these QKD systems, there are several critical devices and main system processes, as listed below.

**Single-photon detectors.** There are two types of detector. The frequently used one is a InGaAs/InP single-photon detector[35], using the technique of sine-wave gating[34]. The InGaAs/InP single-photon detectors are fully integrated on the basis of the standards of Advanced Telecommunications Computing Architecture, with a gating frequency of 1.25 GHz, an effective gating width of about 180 ps and a detector hold-off time of 1 μs. It is calibrated using the standard characterization approach[35], with a detection efficiency of 11% and a dark count rate per gate of $3 \times 10^{-7}$ on average. For longer distances, periodically poled lithium-niobate-waveguide-based up-conversion single-photon detectors are used[36]. The detector is composed mainly of a 1,950-nm pump laser, a system control module and four frequency-conversion modules. All the components are assembled into a standard 19-inch rackmount chasis (Extended Data Fig. 1). The typical detection efficiency and dark count of the up-conversion single-photon detector system are roughly 22% and 1,000 counts per second, respectively. Such performance could support QKD over an attenuation of around 27 dB or a typical fibre distance of 130 km.

**Delay scanning.** The transmitter (Alice) emits the quantum signals with random polarization under the control signals from a field-programmable gate array. Four detectors at the receiver (Bob) simultaneously adjust the delay of the detector gate signals in a step of 12.5 ps and count the clicks with a time duration of 100 ms. The time delay of each detector is set at the value at which it has the maximum counting rate. During the QKD process, the time delay of each detector is fixed at the optimal delay.

**Polarization feedback.** The polarization feedback is first performed in a rectangle basis. Alice emits optical pulses with horizontal polarization state H. The transmitter sends optical pulses with polarization H at a repetition rate of 625 MHz. The attenuator at the transmitter is adjusted to make the detection count of the receiver large enough for polarization control. The receiver counts the detection events of polarization H and V with a period of 50 ms. The polarization controller is adjusted until the count of H reaches 100 times of that of V. Then, the transmitter changes the polarization to V and the receiver performs a similar operation until the count of V reaches 100 times of that of H. If it is satisfied, a success is reported for the polarization feedback in the rectangle basis. If not, an abnormality is recorded and the polarization feedback in the rectangle basis is repeated. After polarization feedback in the rectangle basis is complete, polarization feedback in a diagonal basis is performed in a similar way.

**Synchronization calibration.** In the synchronization calibration process, Alice transmits optical pulses at a frequency of 100 kHz. At the receiver, each click is measured by the time-to-digital converter and the arrival time is recorded. Histogram statistics are performed on the clicks at an interval of 90 ps to find the time position of the largest frequency. This time position is set as the synchronization correction value. The four detectors are calibrated simultaneously. During the QKD process, the arrival time of each click is modified according to the correction value.

### Post-processing procedure

For the backbone and metropolitan networks, after the pulses are registered at Bob's detectors, a series of post-processing for real-time secure key extraction is performed in the commercial field-programmable gate array. The post-processing includes authentication, basis sift, error correction and privacy amplification. All the QKD devices use the Advanced Telecommunications Computing Architecture. We use commercial equipment that enables simultaneous transmission and reception of QKD signals. Hence, all users may be regarded as equivalent entities, and our network can be easily maintained and extended to larger ones.

Specifically, suppose that Alice encodes the key in photons and sends them Bob, who randomly measures the received photon in two different bases. After several runs of the protocol, Alice and Bob run the following post-processing procedure to get identical and secret keys. Here, we only briefly describe the protocol and refer to ref. [47] for details. In our secret key calculation, we select a failure probability of $\varepsilon = 10^{-9}$.

**Authentication.** Alice and Bob exchange messages by running an authentication protocol such that the exchanged message is unchanged and is from the legitimate party. Authentication requires pre-shared keys and is used in basis sift, error verification and privacy amplification in the post-processing procedure. The sending party encodes the message into a tag by using a hash function that is chosen randomly on the basis of a pre-shared key with the other party. The sending party encrypts the tag with one-time-pad encryption by using pre-shared keys and sends the encrypted tag to the other party. The receiving party also calculates the encrypted tag from the received message and the pre-shared keys. Authentication succeeds if the calculated tag is the same as the received tag.

**Key sift and basis sift.** Bob sends the locations of no-click events (not authenticated) and measurement basis choices (authenticated) to Alice, who, on the basis of the received information, discards the loss events and the part for which the bases are not matched. Alice sends information about their basis choices (authenticated), the decoy state, vacuum state and 10% of the signal state to Bob, such that Alice and Bob have sifted keys with the same measurement bases of the signal states. Alice counts the detection rate and Bob counts the bit error rate of the sifted keys.

**Error correction and verification of the sifted keys.** For each 256-kbit sifted key, Alice and Bob divide the key into small pieces and calculate

the sum of each piece. Alice sends the sum of each piece to Bob, who checks whether the sums are the same. If they are the same, Bob replies 'crc' to Alice. If they are different, Bob replies the hamming code for error correction. Alice and Bob randomly permutate the sifted key and repeat the above procedure until there is no error (authenticated).

**Privacy amplification.** On the basis of the detection rate and error rate, Alice and Bob calculate the phase error rate. On the basis of the phase error rate, the bits of leaked information during the error correction step and pre-shared keys, Alice constructs a Toeplitz matrix and sends it to Bob through an authenticated channel. Alice and Bob multiply the Toeplitz matrix by the sifted keys after error correction and verification to get the final key.

The Toeplitz matrix is an $n \times l$ matrix, with $n$ denoting the sifted raw key length and $l$ denoting the final key length, which is determined by the key rate formula. The Toeplitz matrix is generated by $n+l-1$ random bits, which are sent through an authenticated channel between Alice and Bob. In practice, $n$ is roughy a few hundred thousand bits and $l$ is around $0.4n$, depending on the error rates.

## Standardization

To be a practically operating communication network, the whole backbone network should be able to provide a confidential communication service to industry, banks, governments and individuals. Therefore, similar to existing information and telecommunication technologies, such a backbone network could refer to existing criteria for information security. In our case, the information system for the backbone network has passed grade III (meeting the requirements on grade III systems) under the Information Security Technology Baseline for Classified Protection of Information Systems, one of the National Standards of China concerning classified security protection. This standard is equivalent to international standards on guidelines and specifications developed for evaluating information security, such as the ISO/IEC 15408 standard, one of the Common Criteria for Information Technology Security Evaluation. The grade III level for classified security protection of information system is defined as follows: the destruction of a grade III information system would cause material damage to social order and public interests or would cause damage to national security. Therefore, most institutions and commercial companies and some financial and government sectors could use services offered by the backbone network for information security.

## Practicality

In our quantum network, we realize several services, including video call, audio call, fax, text transmission and file transmission. Because the key generation rate is not fast enough for one-time-pad encryption, we encode the message by using the secure key combined with the classical encryption method AES128. The secret key is repeatedly updated and the information exchange is secure as long as the shared key is not leaked during its usage. Suppose each two users consume a 128-bit key per minute; then, the minimal key rate of the backbone can serve at least $28.1 \times 10^3 \times 60/128 \approx 13{,}171$ users. In practice, the key consumption varies with different services. For example, considering the realized application of bank information transfer from Beijing to Shanghai, the key is updated 10 times per minute to ensure a higher level of security. Furthermore, with future developments of high-rate networks, one-time-pad encryption could be used to ensure information-theoretical security of information exchange[48] to ensure the highest security requirement.

After installing, running the whole backbone network under real-life situations and serving users, field tests, real-time monitoring and maintenance for the whole network is required. Any potential new attacks and misplays should be ruled out quickly. This aspect has been done by evaluating and testing the whole QKD network against quantum and classical communication aspects. Beyond the QKD system, systematic security, including key management equipment and application apparatus, has also been addressed. Moreover, necessary isolations are maintained either logically or physically for different components and functions. For the whole network system, additional evaluations and tests have also been performed, such as conformance testing, penetration testing, security functions, vulnerability scanning, key utilization, source codes, robustness, stability, scalability and maintenance. These tests and promotions were done for several rounds to ensure, to a large degree, complete and up-to-date security status and level. Some testing and improvements need regular routine updates, continuous monitoring and maintenance, similarly to popularly used information security systems. By combining expertise from all over the world, our accumulated techniques, generic methods and guidelines have contributed to the project ISO/IEC 23837 to advance to the first working draft specifying 'security requirements, test and evaluation methods for quantum key distribution' under the framework of ISO/IEC 15408 in the ISO/IEC JTC 1/SC 27 organization. The work aims to form an international standard in this area, by combining more contributions and attendance in future from experts of ISO/IEC national bodies and other organizations, from industrial, technical and business sectors.

To show the aspects of system interpretability using fibre and satellite, we take one real-use-case illustration as an example: the secure communication of the RMB Cross Border Payment and Receipt Management Information System (RCPMIS) of the People's Bank of China (PBOC) between Urumqi and Beijing, which can be completed in three steps. The first step is to perform QKD between the Urumqi and Beijing ground stations using the Micius satellite. The second step is to relay the secure keys to the corresponding data centres via the QMANs in Urumqi and Beijing. Finally, we utilize a standard encryption router to implement the data encryption and transmission.

The construction of the scientific infrastructure of the backbone network has finished. There are several demonstrations of applications, such as data collection and transfer. The network is used mainly for technological verification and real-world demonstrations, but will be put into commercial use in the near future.

## Implementation security

In practice, the imperfections of realistic devices might introduce deviations from the idealized models used in the security analyses of QKD. The device imperfections may be exploited by Eve to launch quantum attacks[24], such as a photon-number-splitting attack, detector-blinding attack, time-shift attack, wavelength-dependent attack or Trojan-horse attack. Our QKD systems have implemented countermeasures against all known attacks[3]. The specific countermeasures are summarized in Extended Data Table 1. We highlight a few facts regarding the implementation security below.

We have implemented countermeasures for some attacks against general implementations. First, for the Trojan-horse attack, we used two micro-electromechanical system (MEMS) optical attenuators and an optical circulator to ensure that the isolation is larger than 170 dB, which is generally sufficient for a practical QKD system[49]. Second, for the detector-blinding attack, we added an electrical monitor to monitor in real time the output current of the single-photon detectors; the monitor has a threshold current that corresponds to an optical power of −40 dBm, which is much smaller than the power required for a detector-blinding attack (−20 dBm)[50]. Further details are provided in Extended Data Table 1.

For a specific QKD implementation, we also implemented specific countermeasures. For instance, for the QKD system with multiple lasers, a potential security issue is the spectral mismatch between different lasers. To counter this issue, we added a narrow-band filter (10-GHz fibre Bragg grating) to filter out the spectrum of all lasers. The filter has a bandwidth of 80 nm. With the filter, the characterized spectrum shows that the mismatch of the central wavelength of different lasers is less than 2.9 nm. Nevertheless, during our system characterization,

we learnt that it is challenging to ensure that the multiple lasers have exactly the same characteristics (wavelength, temporal, polarization, and so on). Therefore, in future implementations, we will adopt the QKD implementation with a single laser (for example, Extended Data Fig. 5).

To quantify the security of practical QKD in a rigorous manner, Alice and Bob need to characterize the imperfections of each device and to consider the information leakage due to their effects in the key rate calculation[3,24]. Although we have implemented the characterizations and countermeasures against the critical side channels (Extended Data Table 1), research to fully analyse the security of practical QKD should continue. In particular, a refined security proof that includes all the device imperfections should be established. Recently, several advances have been made to security proofs for QKD with realistic devices, such as the ones for detector-efficiency mismatch[51], source flaws and Trojan-horse attacks[37], and the general covert channels[52]. These are important subjects for future study in our large-scale quantum network. We refer to ref. [3] for a comprehensive discussion on the subject.

More generally, there might be covert side channels such as X-ray, neutrons or neutrinos[52]. Also, classical post-processing units might pose a threat to security, such as through the memory attack[53]. However, covert side channels are problems for all cryptosystems, that is, not only to quantum cryptography but also to conventional cryptographic systems. For instance, the power consumption of the CPU performing encryption and decryption is a common side channel, which can threaten implementations of quantum and conventional cryptographic systems[54]. Therefore, closing the side channels is essential in all cryptographic technologies. Nonetheless, as discussed extensively in ref. [3], compared to conventional mathematical-based cryptography, QKD provides an accurate description of the physical realization of a cryptographic system, and the security may be proved on the basis of this description. Recently, it was proved[52] that redundancies and verified secret sharing may be used to achieve security against covert side channels in QKD.

### Satellite-to-ground QKD

The source repetition rate was improved from 100 MHz to 200 MHz by using the backup design for the Micius satellite. There are eight laser diodes (LDs) in the satellite-based QKD source of the Micius satellite[27]. In the default mode, LD1 and LD2 (LD3 and LD4) correspond to state H (V), LD1 outputs the signal state and LD2 outputs decoy states. The repetition frequency of the source is 100 MHz. In the backup mode, LD1 and LD2 output signal and decoy states simultaneously, which doubles the repetition frequency to 200 MHz.

To realize the efficient BB84 protocol[29–31], we uploaded a new controlling software to the experiment control box in the satellite, where the software is used to map the original random numbers to new random numbers, to change the probability of the four BB84 states and the decoy intensities. According to the efficient QKD protocol, some specific parameters are reset: the ratio of signal, decoy and vacuum states is set to 0.72:0.18:0.1. Here $\mu$ (average photon number of the signal states) and $\upsilon$ (average photon number of the decoy states) are set to 0.5 and 0.08, respectively. The ratio of the $Z$ and $X$ basis is set to 0.889:0.111 in the satellite and 0.9:0.1 in the ground station. In the BB84 module on the ground, the beam splitter with a bias of 10:90 for the $X$–$Z$ basis is used for the efficient BB84 protocol.

The final key rate is 40 times higher than in previous work[27], as a result of the following contributions. (1) The signal-state ratio increased from 0.5 to 0.72, and the $Z$ base ratio increased from 0.5 to 0.889 on the satellite and from 0.5 to 0.9 on the ground station, enhancing the key rate by a factor of 2.34. (2) The repetition frequency increased from 100 MHz to 200 MHz (contributing an enhancement by a factor of 2). (3) The ground telescope increased from 1 m to 1.2 m (enhancement factor of about 1.5). (4) The QBER reduced and the raw key size increased, corresponding to an enhancement factor of about 2. (5) The ground coupling efficiency increased from 14% to 40% (enhancement factor of about 3). Here we improve the optical spatial-mode matching between the incident beam and the collection system on the ground by reducing the total magnification, including the receiving telescope and the expander in the optical box from 1,500 times to 450 times, to match the whole receiver system and to improve collecting efficiency.

At present, the satellite–ground QKD does not work the whole day. The QKD can be carried out only when the satellite flies over the ground station. The times the satellite passes over the station every day are related to its orbit. For example, the quantum satellite (500 km height, Sun-synchronous orbit) passes over the station at 12:00 and 24:00 local time every night, and it works at night for about 8 min each time[27]. Tiangong-2 (400 km height, circular orbit) has a cycle of about 40 days for passing through a ground station[26]. In each cycle, it crosses the ground station on average more than once per night (at most four times a night, but sometimes not even once). Moreover, satellite–ground QKD works only in sunny weather with the current technology, not in rainy, foggy or hazy conditions. Nonetheless, with the development of a geosynchronous satellite in the future, it should be possible to achieve 24-h ground-to-ground QKD, with daylight QKD techniques being very important[55,56].

## Data availability

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

## Code availability

The code used for modelling the data is available from the corresponding authors on reasonable request.


46. Liu, Y. et al. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express* **18**, 8587–8594 (2010).
47. Fung, C.-H. F., Ma, X. & Chau, H. F. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **81**, 012318 (2010).
48. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949).
49. Lucamarini, M. et al. Practical security bounds against the Trojan-horse attack in quantum key distribution. *Phys. Rev. X* **5**, 031030 (2015).
50. Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686–689 (2010).
51. Fung, C.-H. F., Tamaki, K., Qi, B., Lo, H.-K. & Ma, X. Security proof of quantum key distribution with detection efficiency mismatch. *Quantum Inf. Comput.* **9**, 131–165 (2009).
52. Curty, M. & Lo, H.-K. Foiling covert channels and malicious classical post-processing units in quantum key distribution. *npj Quantum Inf.* **5**, 14 (2019).
53. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.* **110**, 010503 (2013).
54. Brumley, D. & Boneh, D. Remote timing attacks are practical. *Comput. Netw.* **48**, 701–716 (2005).
55. Hughes, R. J., Nordholt, J. E., Derkacs, D. & Peterson, C. G. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.* **4**, 43 (2002).
56. Liao, S.-K. et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photon.* **11**, 509–513 (2017).
57. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330–1333 (2000).
58. Li, H.-W. et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* **84**, 062308 (2011).
59. Qi, B., Fung, C.-H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **7**, 73–82 (2007).
60. Jain, N. et al. Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.* **107**, 110501 (2011).
61. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000).
62. Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **73**, 022320 (2006).
63. Xu, F., Qi, B. & Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **12**, 113026 (2010).
64. Sun, S.-H. et al. Effect of source tampering in the security of quantum cryptography. *Phys. Rev. A* **92**, 022304 (2015).


**Acknowledgements** This work was supported by the National Development and Reform Commission, the Department of Science and Technology of Shangdong province, Anhui Development and Reform Commission, the China Banking Regulatory Commission, the CAS, the NNSFC and the National Key R&D Program of China.

**Author contributions** Y.-A.C., C.-Z.P. and J.-W.P. conceived the research. Y.-A.C., Q.Z., T.-Y.C., J.Z., M.-S.Z. and J.-W.P. designed the backbone network. W.-Q.C., S.-K.L., J.Y., L.Z., Y.L., R.S., J.-Y.W., C.-Z.P. and J.-W.P. designed the satellite and payloads. S.-K.L., J.Y., J.-G.R., W.-Y.L., Q.S., Y.C., C.-Z.P. and J.-W.P. designed the ground stations. All authors contributed to the establishment of the integrated network. Q.Z., J.Z. and X.J. upgraded the detectors. K.C., T.-Y.W., L.L., N.-L.L., F.X. and X.-B.W. performed security analysis and tests for the backbone network. W.-Q.C., S.-K.L., W.-Y.L., Q.S. and C.-Z.P. upgraded the software for the payloads and the ground stations. Y.-A.C., Q.Z., T.-Y.C., Z.C., S.-L.H., Q.Y., K.L. and F.Z. maintained the whole fibre network and performed the robustness test. S.-K.L., J.Y., J.-G.R., Q.S., Y.C. and C.-Z.P. maintained the satellite network. All authors contributed to data collection and analysed the results. Y.-A.C., Q.Z., S.-K.L., X.Y., Y.C., C.-Y.L., F.X. and J.-W.P. wrote the manuscript, with input from all authors. Y.-A.C., Q.Z., T.-Y.C., W.-Q.C., S.-K.L., J.Z. and K.C. contributed equally to the paper.

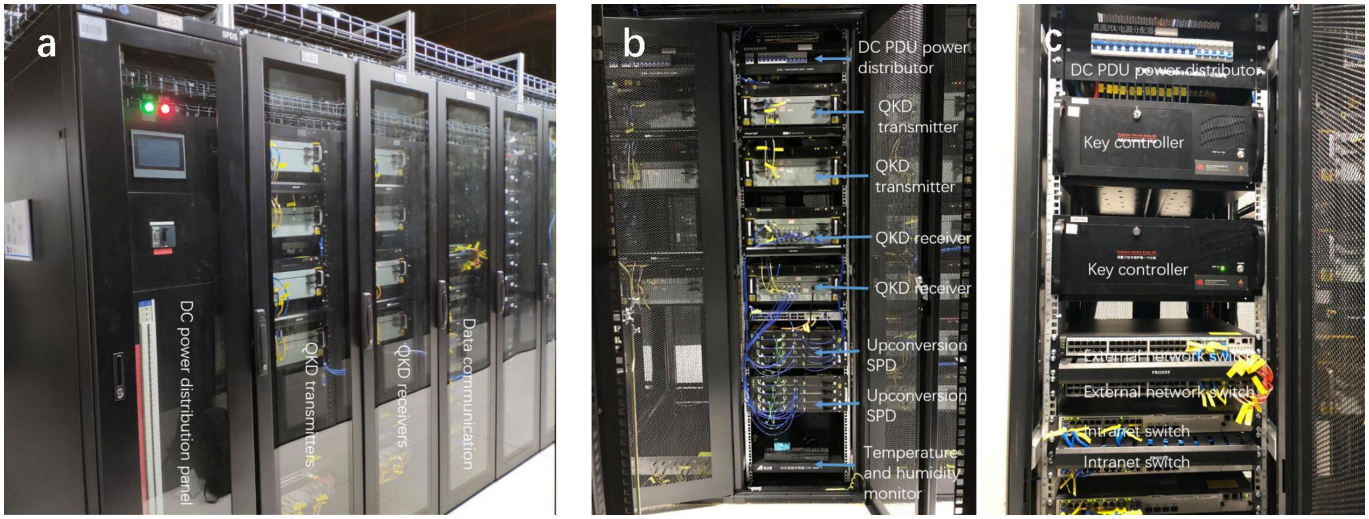
**Competing interests** Each of an entity controlled by USTC, C.-Z.P. and J.-W.P., holds shares in QuantumCTek Co., Ltd. ("QuantumCTek"), a public company listed on SSE STAR Market (Shanghai Stock Exchange Sci-Tech Innovation Board). C.-Z.P. is also the Chairman of QuantumCTek on behalf of the university without receiving any compensation.

**Additional information**

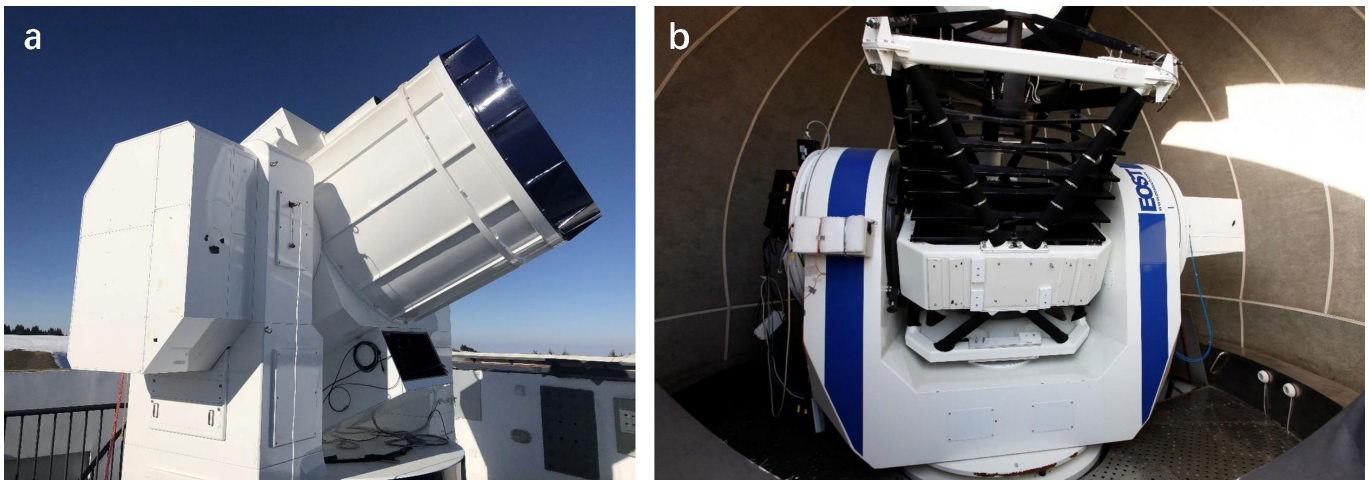
**Supplementary information** is available for this paper at https://doi.org/10.1038/s41586-020-03093-8.

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

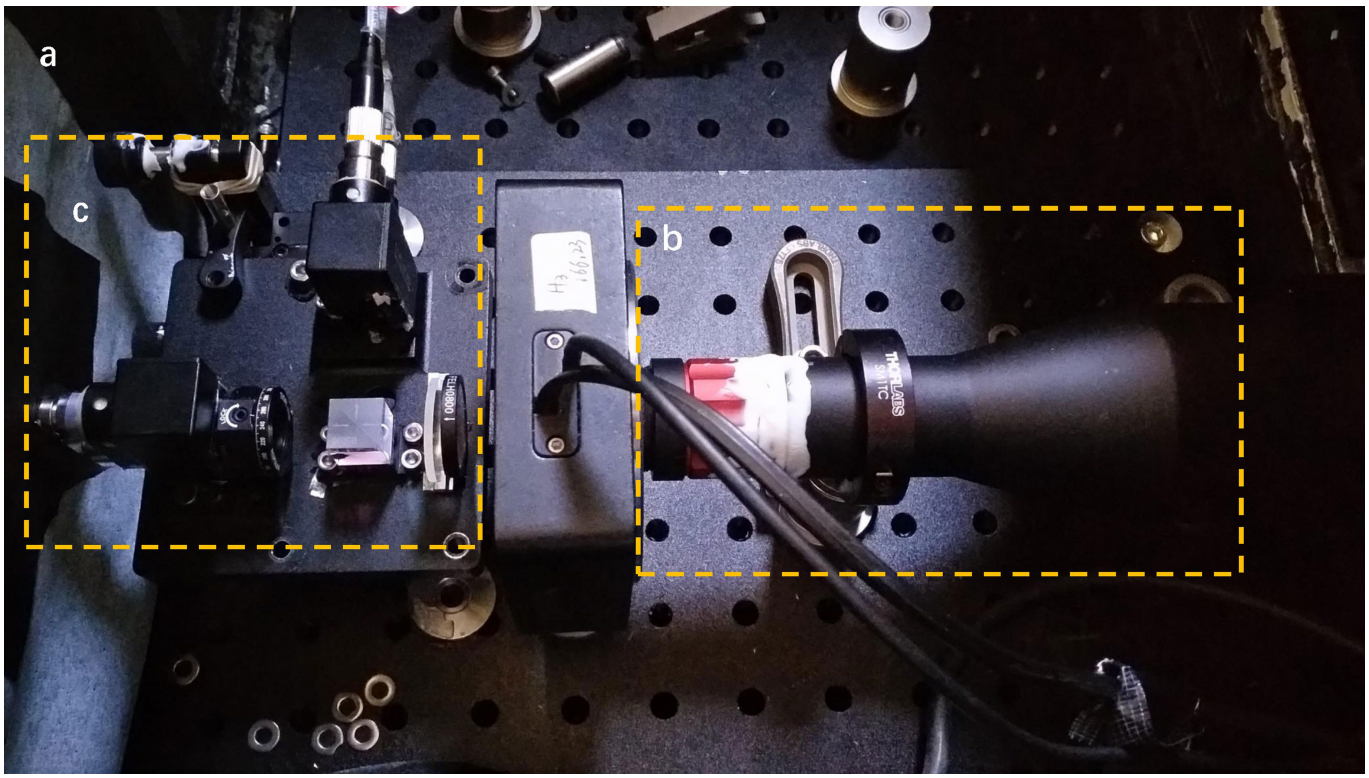
**Peer review information** *Nature* thanks the anonymous reviewer(s) for their contribution to the peer review of this work.



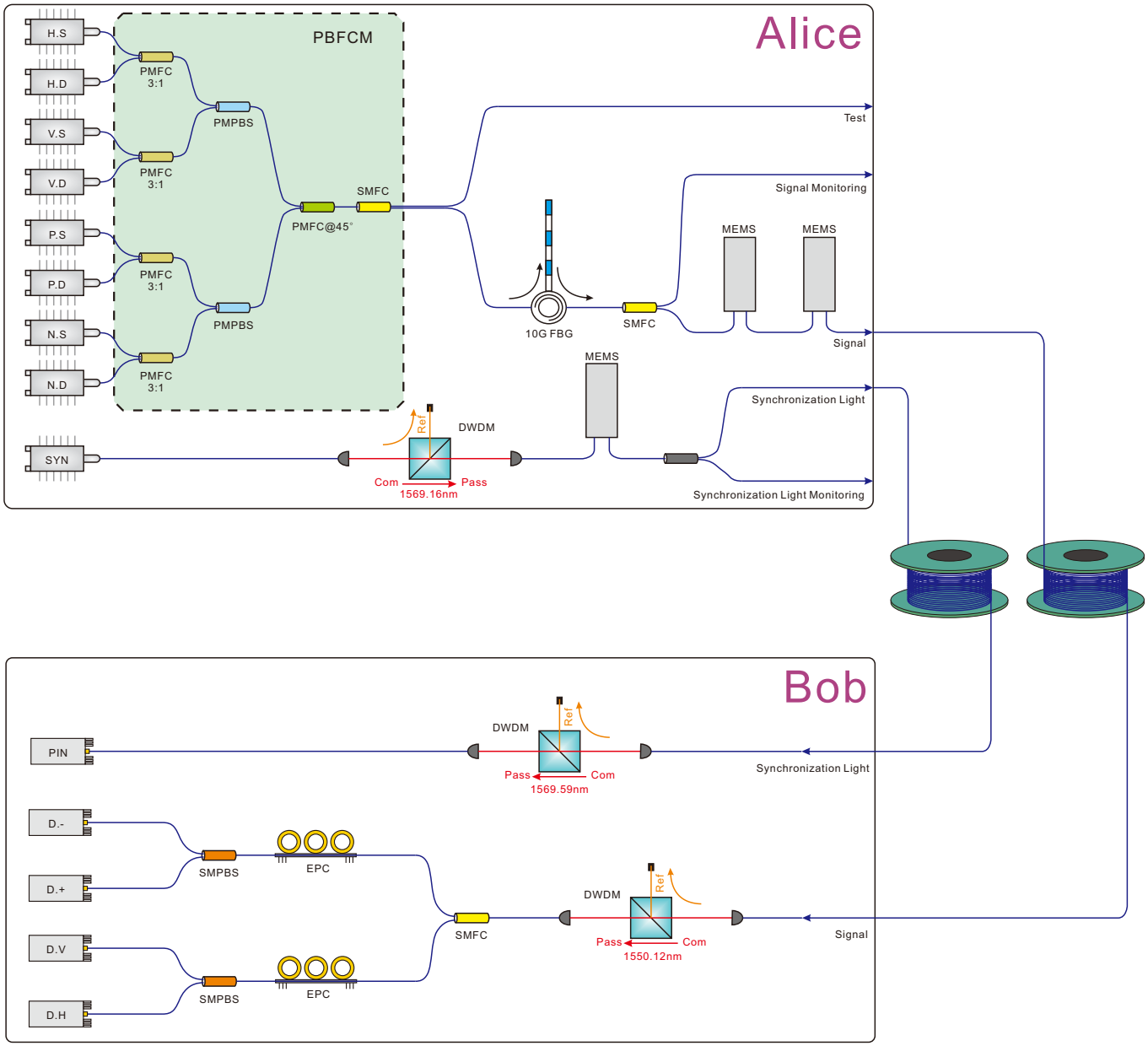

**Extended Data Fig. 1 | Hardware at the relay nodes of the backbone network. a**, Overview of the typical hardware. **b**, QKD devices. **c**, Control and classical communication devices. SPD, single-photon detector; PDU, power distribution unit.



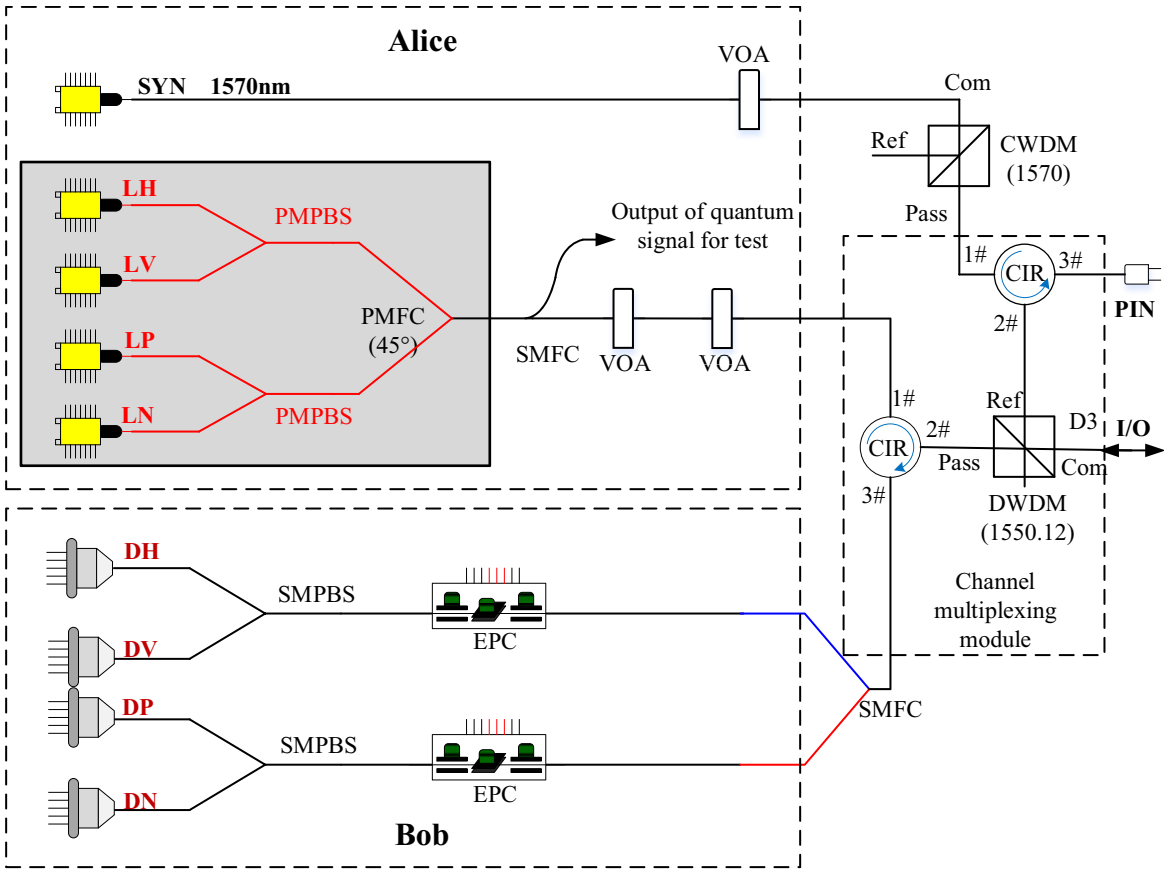

**Extended Data Fig. 2 | Photos of the hardware. a**, The 1.2-m telescope at the Nanshan ground station. **b**, The 1-m telescope at the Xinglong ground station.



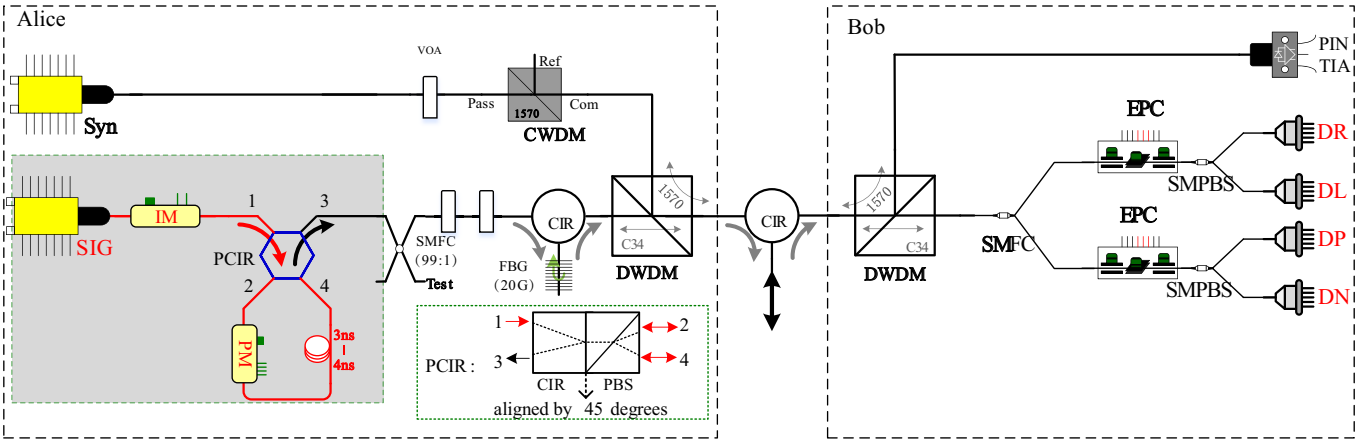

**Extended Data Fig. 3 | Hardware of follow-up optics at the Xinglong ground station. a**, The upgraded receiving optics at the Xinglong ground station. **b**, **c**, The two major changes were the beam expander (**b**) and the BB84 module (**c**). A beam expander with lower magnification is used to increase the field of view. The BB84 module is modified to match the larger size of the incident light beam. A beam splitter with a bias of 10:90 (50:50) for the *X*–*Z* basis in the BB84 module is used in Nanshan (Xionglong).




**Extended Data Fig. 4 | Schematic of the 625-MHz QKD system.** On Alice's side, four signal lasers (S) and four decoy lasers (D) are combined via polarization-maintaining filter couplers (PMFCs), and then combined again into a single PMFC (with 45° difference for fibre-axis inputs), before outputting through a single-mode fibre coupler (SMFC). One beam is for testing; another goes to the optical circulator associated with a 10G fibre Bragg grating filter (FBG) before monitoring and attenuating with two cascaded MEMS attenuators. The synchronization laser (SYN) goes through a dense wavelength-division multiplexing (DWDM) and then a MEMS attenuator, before splitting for monitoring and outputting to the communication channel. On Bob's side, the signal light enters first a DWDM and then a SMFC, with one set of electrically driven polarization controllers (EPCs) consisting of three components in every path, before single-mode polarizing beam splitters (SMPBSs) detect the four different signal states. The synchonization laser also propagates via a DWDM and is detected by a PIN photodetector. PMPBS, polarization-maintaining polarizing beam splitter; Com, common port for the coarse wavelength-division multiplexing (CWDM) device; Pass, pass port for the CWDM device; Ref, reflect port for the CWDM device; H, quantum state $|H\rangle$; V, quantum state $|V\rangle$; P and +, quantum state $|+\rangle$; N and −, quantum state $|-\rangle$.




**Extended Data Fig. 5 | Schematic of the 40-MHz transceiver QKD system with multiple lasers.** The transmitter and the receiver are combined in the same terminal, with a channel multiplexing module including a DWDM and two circulators (CIR). They are similar to those of the 625-MHz system. The main difference is that the system operates at a frequency of 40 MHz. The transmitter adopts one laser doide with two different driving signals for decoy-state modulation instead of two, and there is no a FBG for wavelength filtering. The InGaAs/InP detector of the receiver is operated in rectangular-wave gated mode at a frequency of 40 MHz, with a detection efficiency of about 15% at a gate width of 1.6 ns and a coincidence width of 400 ps. Its dark count rate is less than 250 counts per second, and the after pulse probability is less than 1% at a dead time of 5 μs. VOA, variable optical attenuator; LH, laser diode for quantum state $|H\rangle$; LV, laser diode for quantum state $|V\rangle$; LP, laser diode for quantum state $|+\rangle$; LN, laser diode for quantum state $|-\rangle$; DH, detector for quantum state $|H\rangle$; DV, detector for quantum state $|V\rangle$; DP, detector for quantum state $|+\rangle$; DN, detector for quantum state $|-\rangle$.




**Extended Data Fig. 6 | Schematic of 40-MHz transceiver QKD system with a single-laser transmitter and a passive receiver.** The transmitter and the receiver are combined in the same terminal by a channel multiplexing module including two DWDMs and a circulator. In the transmitter, the pulse generated by one laser diode first passes through an intensity modulator (IM) for decoy-state active modulation, and then a custom-made Sagnac interferometer module, which consists of a polarization-sensitive circulator (PCIR) and a phase modulator (PM) for polarization-state modulation. The polarization-sensitive circulator is an integrated micro-optical system that combines a circulator and a polarizing beam splitter (PBS), with their directions offset by 45° (inset). TIA, transimpedance amplifier; SIG, signal.

**Extended Data Table 1 | Summary of attacks and countermeasures**

| Attack | Countermeasure | | | |
|---|---|---|---|---|
| | 625-MHz QKD system | 40-MHz QKD system (type I) | 40-MHz QKD system (type II) | Realization |
| Photon-number-splitting [Phys. Rev. Lett. 85, 1330 (2000)] | Decoy-state method | Same | Same | Optics, electronics and software |
| Wavelength-selecting [Phys. Rev. A 84, 062308 (2011)] | A wavelength-flatted BS having almost uniform coupling ratio from 700 nm to 1700 nm, placing a wavelength filter before the BS | Same | Same | Optics |
| Time-shift [Quant. Inf. Comput. 7, 73 (2007)] | Setting the time delay of detectors to ensure that they have uniform counting rate once the system start | Same | Same | Software |
| Detector-blinding [Nat. Photon. 4, 686 (2010)] | Monitoring the output current of SPDs, and placing an alarm if the current exceeds presetting threshold (~20uA) which is much less than the required power ($> 1$ mW) for the blinding attack | Same | Same | Electronics, software |
| Channel calibration [Phys. Rev. Lett. 107, 110501 (2011] | Comparing the interval of the optimal time delay of each detector with the default setting after each calibration routine, and placing an alarm if the values exceed the preset threshold (30 ps) | Same | None | Software |
| Double-click [Phys. Rev. A 61, 052304 (2000)] | Allocating randomly bit 0 or 1 whenever a double-click event occurs | preserve the earlier click event | Same | Software |
| Trojan-horse [Phys. Rev. A 73, 022320 (2006)] | Intrinsically immune to such an attack because of none of active modulation components | Same | High isolation (>155 dB) | Optics |
| Spectra mismatch [Phys. Rev. A 84, 062308 (2011)] | Filter the spectra using 10 GHz FBG filter | None | Intrinsically immune | Optics |
| Phase-remapping [New J. Phys. 12, 113026 (2010)] | One-way system, intrinsically immune | Same | Same | Optics |
| Laser seeding [Phys. Rev. A 92, 022304 (2015)] | High isolation (>110 dB) to block the injection light, provided by a combination of optical components incldluing circulator, attenuator, laser isolator and etc | High isolation (>85dB) | High isolation (>180dB) | Optics |

'Same', the countermeasure is the same as that of the previous system. 'None', this system is immune to the attack. The attacks are reported in refs. [50,57–64].

**Extended Data Table 2 | Comparison of satellite-based QKD**

| Parameters | [Nature 549, 43 (2017)] | This work |
|---|---|---|
| Max sifted key rate (kbps) | 14 | 642 |
| Averaged secret key rate (kbps) | 1.1 | 47.8 |
| 1-orbit sifted key (Mbit) | 1.67 | 58.13 |
| 1-orbit secret key (Mbit) | 0.3 | 17.4 |

Comparison is shown between ref. [27] and this work.

**Extended Data Table 3 | Comparison of parameters for low-Earth-orbit (LEO) and geostationary (GEO) satellites**

| Item | LEO | GEO |
|---|---|---|
| Divergence angle of transmitters (urad) | 10 | 3 |
| Distance (km) | 2000 | 36000 |
| Elevation angle | 5° | 70° |
| Atmospheric efficiency | 0.2 | 0.8 |
| Pointing efficiency | 0.5 | 0.7 |
| Receiver telescope diameter (m) | 1.2 | 2 |
| Optical receiving efficiency | 0.3 | 0.5 |
| Total link efficiency (dB) | -37 | -40 |