npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Implementation of a 46-node quantum metropolitan area network

Teng-Yun Chen[1,2]✉, Xiao Jiang[1,2], Shi-Biao Tang[3], Lei Zhou[3], Xiao Yuan[4], Hongyi Zhou[4], Jian Wang[1,2], Yang Liu[1,2], Luo-Kan Chen[1,2], Wei-Yue Liu[5], Hong-Fei Zhang[1,2], Ke Cui[1,2], Hao Liang[1,2], Xiao-Gang Li[3], Yingqiu Mao[1,2], Liu-Jun Wang[1,2], Si-Bo Feng[3], Qing Chen[3], Qiang Zhang[1,2], Li Li[1,2], Nai-Le Liu[1,2], Cheng-Zhi Peng[1,2], Xiongfeng Ma[4], Yong Zhao[1,2,3] and Jian-Wei Pan[1,2]

Quantum key distribution (QKD) enables secure key exchanges between two remote users. The ultimate goal of secure communication is to establish a global quantum network. The existing field tests suggest that quantum networks are feasible. To achieve a practical quantum network, we need to overcome several challenges including realizing versatile topologies for large scales, simple network maintenance, extendable configuration and robustness to node failures. To this end, we present a field operation of a quantum metropolitan-area network with 46 nodes and show that all these challenges can be overcome with cutting-edge quantum technologies. In particular, we realize different topological structures and continuously run the network for 31 months, by employing standard equipment for network maintenance with an extendable configuration. We realize QKD pairing and key management with a sophisticated key control centre. In this implementation, the final keys have been used for secure communication such as real-time voice telephone, text messaging and file transmission with one-time pad encryption, which can support 11 pairs of users to make audio calls simultaneously. Combined with intercity quantum backbone and ground–satellite links, our metropolitan implementation paves the way toward a global quantum network.

npj Quantum Information (2021)7:134 ; https://doi.org/10.1038/s41534-021-00474-3

INTRODUCTION

The ultimate goal of quantum key distribution (QKD)[1,2] is to construct a global quantum network, wherein all communication traffics have information-theoretic security guarantees. A global QKD network consists of two main types of links: the ground network (mainly fibre based) and the satellite network (mainly free-space based). The ground network can be further divided into backbone, metropolitan and access networks, which cover intercity distances, metropolitan distances and fibre-to-the-home distances, respectively. The feasibility of QKD between two users has been extensively studied, for example, through long-distance free space[3], telecom fibres[4] and simulated ground–satellite links[5,6]. Field tests of QKD networks have been realized, including the three-user network by DARPA (2003)[7], the six-node SECOQC network in Europe (2008)[8], SwissQuantum network (2009)[9], the USTC network[10], the six-node mesh-type network in Tokyo (2011)[11] and the small-scale metropolitan all-pass and intercity quantum network[12,13]. The satellite network is a promising way to realize intercontinental secure communication due to the low transmission attenuation in space. The satellite can serve as a trusted relay, connecting remote user nodes or subnetworks[14]. Recently, a large-scale satellite network has been implemented[15], consisting of four metropolitan-area networks, a backbone network and two satellite–ground links. Here, we summarize the existing network implementations in Table 1. For a full review of the subject, one can refer to the recent review article[16] and references therein.

Nevertheless, these QKD experiments and networks are still preliminary demonstrations with limited scales with less than ten nodes, making it insufficient for meeting the demands of actual metropolitan communication. Furthermore, realizing a practical QKD network is not simply extending the number of nodes; while many scientific and practical issues, such as: (a) network topology; (b) network scalability; (c) key management; (d) practical applications; and (e) network robustness, need to be considered. Thus far, realizing a practical large QKD network still remains a major challenge in quantum communication.

In this work, we construct a 46-node quantum metropolitan-area network throughout the city of Hefei, which connects 40 user nodes, three trusted relays and three optical switches, as shown in Fig. 1. The network covers the entire urban area and connects several major organizations in the city districts, including governments, banks, hospitals, universities and research institutes. In our network, we: (a) implement versatile connection topologies for different hierarchies of users; (b) use standard equipment with a scalable configuration; (c) integrate systematic key management; (d) realize various robust application modules; and (e) deal with node failures. As a result, we address the major challenges in realizing a large-scale practical QKD network.

RESULTS

Network topology

We first review the basic topological structures in a network. There are three general ways of connecting and distributing keys between users in a quantum network. The most robust method uses a fully connected topology. Here, each user is directly connected to every other user in the network. This type of network contains no relays; hence it is robust against a single point of failure, and the users do not need to trust one another.

[1]Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui, China. [2]Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai, China. [3]QuantumCtek Co. Ltd., Hefei, Anhui, China. [4]Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China. [5]School of Information Science and Engineering, Ningbo University, Ningbo, Zhejiang, China. ✉email: tychen@ustc.edu.cn

Table 1. Existing QKD network implementations.

Network	No. of nodes	Running time (order of magnitude)	Topology	Key rate (at max distance/loss)
DARPA[7]	6	Unknown	Tree	0.5 kbps (10.2 km)
SECOQC[8]	6	Hour	Mesh	3.1 kbps (33 km)
SwissQuantum[9]	3	Year	Fully connected	1 kbps (17.1 km)
Tokyo[11]	6	Year	Mesh	2.2 kbps (90 km)
USTC[10]	5	Unknown	Star	0.4 kbps (14.8 dB)
USTC[12]	3	Week	Fully connected	1.5 kbps (20 km)
USTC[13]	5	Week	Star	0.2 kbps (130 km)
USTC[15]	109	Year	Mesh	1.1 kbps (2043 km)
Hefei (this work)	46	Year	Fully connected & star	49.5 kbps (18 km)

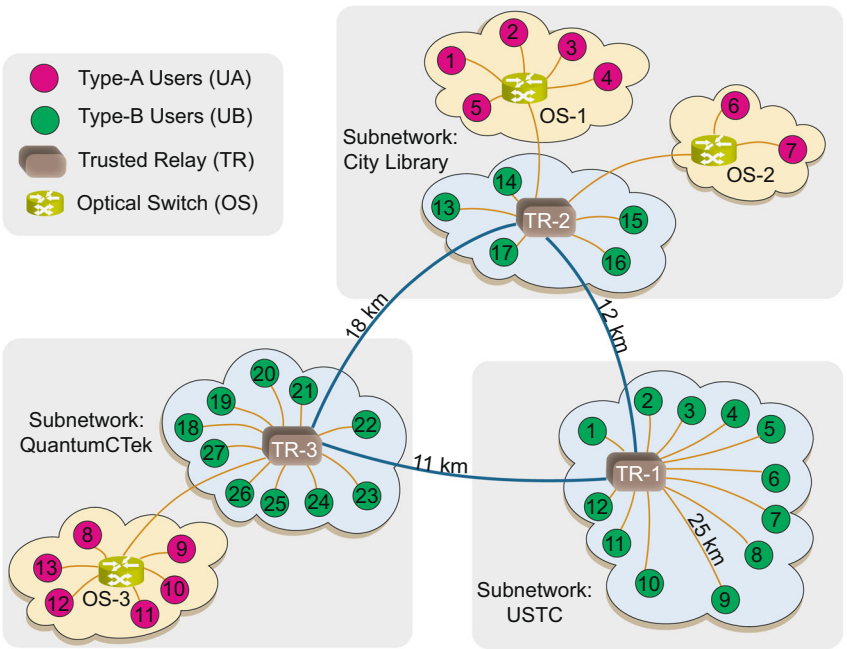

Fig. 1 The topological structure of our quantum network. The network mainly comprises three subnetworks that are directly connected to each other. In each subnetwork, there are multiple users connected to intermediate nodes in different ways, either by an all-pass optical switch (OS) or by a trusted relay (TR). Users connected by a switch are denoted as red dots (Type-A Users, UA), holding both a quantum transmitter and a receiver. Users connected to a trusted relay are denoted as green dots (Type-B Users, UB), only holding a quantum transmitter. Specifically, UA-1 to UA-5 are connected to OS-1, UA-6 and UA-7 are connected to OS-2, UA-8 to UA-13 are connected to OS-3, UB-1 to UB-12 are connected to TR-1, UB-13 to UB-17 are connected to TR-2, and UB-18 to UB-27 are connected to TR-3.

That is to say that a system failure or dishonest user would not affect the communication between other users. The main drawback of this type of network is that the number of links (and cost) of a fully connected network quadratically increases with the number of users. Thus, such a network is typically used for connections between a small number of major nodes.

Alternatively, the user nodes can also be connected via a central switch (relay). In this star-like network, the number of links linearly increases with the number of users. In addition, the users do not need to trust each other or the relay. Because the switch only transfers quantum signals, users can execute QKD protocols as if they are directly connected. The drawback of this type of network is that it is not robust against a single point of failure. That is to say that if the switch relay fails, the entire network will be brought down. The transmission distance of quantum signals is twice the length of the link between the users and the switch; hence this kind of network is typically used for local connections.

In the star-like topology, we can replace the switch with a trusted node. In this trusted node network, every user runs QKD protocols with a central relay, and two users can combine their keys between the central relay to form their own keys. In QKD, the secure key transmission distance is limited; thus, the size of a directly communicated quantum network is also limited. However, the size of the network can be extended by the introduction of trusted relays. Two distant users could also build secure keys with the help of a sufficient number of trusted relays. In practice, the Shanghai–Beijing backbone employs this technique to scale the QKD distance. The disadvantage of this type of network is that the users need to trust the relay. To construct a global quantum network, it is important to realize different topological structures in practice.

Our network consists of three subnetworks located at, USTC, QuantumCTek and the City Library, and are distributed approximately 15 km apart. The longest fibres connecting the east and west end-users is approximately 45 km, and that connecting the south and north end-users is approximately 42 km. The longest direct distance between two users in the network is approximately 18 km. We realize two basic types of topological connection structures, including the full connection between the three

subnetworks and the star-like connection for local access networks. The fully connected topology is applied to guarantee the robustness between the most important users; while the star-like connection is used for a more efficient network connection. At the centre of the star-like subnetwork, we use either a trusted node or an optical switch for different scenarios depending on the needs and distribution of the users.

The trusted node can be regarded as a classical router that assigns classical keys between users. The all-pass optical switches acted as quantum routers that redistribute quantum signals. Any two users connected to the same switch could communicate directly without interfering with other users. In the experiment, we made use of two types of optical switches. One is the 4×8 switch where four 1×8 optical switch modules and eight 1×4 modules are connected. This type of switch module comprises 4 input and 8 output ports, forming a 4×8 connecting matrix. The other is the 16-port all-pass optical switch where sixteen 1×15 optical switch modules are connected to form an optical path. When this 16-port switch was fully connected, it enables 8 pairs of users to communicate simultaneously. In our experiments, the losses in all these optical switches are below 1.2 dB, which are much lower than that in the channel isolation (50 dB).

Standard QKD equipment

In our network, we used the polarization-encoding BB84 QKD protocol[17–19] with a vacuum + weak decoy-state method[20] to generate secret keys between directly connected users and trusted relays. Two users could generate keys if one of them had a quantum transmitter and the other had a quantum receiver. As a quantum receiver is generally more expensive compared with a quantum transmitter, not all users in this network possessed quantum receivers. However, everyone at least had a quantum transmitter and was thus able to transmit signals. In this case, there were two types of users in this network: users directly connected to a switch have both quantum a transmitter and receiver, and users directly connected to a trusted relay have only a quantum transmitter. There were, correspondingly, two types of equipment: one only for transmitting signals and the other for transmitting and receiving signals at the same time.

Standard transmitter and receivers are applied in our network, whose internal structures are shown in Fig. 2. In the transmitters, we use the 14-pin butterfly distribute feedback lasers with a central wavelength of 1550 nm. Polarization states $\{|H\rangle, |V\rangle, |+\rangle, |-\rangle\}$ are produced with four different lasers, where each one can produce three different intensity pulses corresponding to the signal, decoy and vacuum states. Before key generation, a time calibration between the source and the single-photon detectors as well as polarization feedback is performed. In general, the calibration is more efficient with strong pulses. It will take more time to complete the calibration for longer transmission distance but no more than 5 min. The calibration process makes our network robust against environmental disturbances. After basis reconciliation and error correction, privacy amplification is performed after 256 kbit per second (kbps) keys are accumulated. Based on a field-programmable gate array (FPGA), the Winnow algorithm[21] is used for error correction, with a correction efficiency of 1.3~1.5. Then, privacy amplification is performed using an FPGA-implemented Toeplitz matrix Hash operation[22], which is constructed by true random numbers shared by the transmitter and receiver devices. The standardization of the QKD equipment can greatly reduce the quantity of devices required, allowing the number of devices to scale linearly with the number of user nodes.

Key management

A key management strategy enables the users whose keys are running out to generate keys in high priority. We realize systematic key management for our network by designing a switching strategy. The strategy is determined by the amount of keys stored in the local memories for the users. The user with the least key amount has priority in the queue for key distribution. Here we take the 16-port all-pass optical switch mentioned above as an example. Since it can be connected to 16 users, there are a total of $(0.0pt162) = 120$ possible key-pairing schemes by which two users are connected for the following QKD process. The queuing process for the key-pairing scheme is determined by the Roll-Call-Polling protocol that judges the amount of keys between users. When the key amounts of all devices are the same, QKD pairing is sequentially performed in the order of the network ID. For arbitrary communication partners, the latency for key pairing is heuristically set to be 10, 15 or 30 min according to experience. Then the optical paths of the optical switch are connected, and the QKD process begins. Such a pairing process will repeat whenever there are QKD tasks. The switching time can be configured, ranging from 10 to 60 min. If two users in different subnetworks wish to perform QKD, they first generate keys with intermediate nodes and then swap them. After key generation is activated, the user can obtain secure keys within 5 min, which are stored in local memories.

Since our network is scalable, we also need to consider the key management for new users. To join the network, a new user should first send a heartbeat frame from their QKD device to the

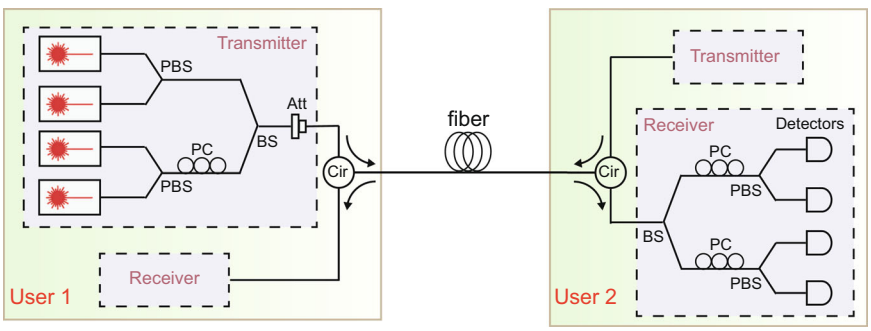

Fig. 2 A schematic for the QKD set-up. There are four laser sources in the transmitter emitting four corresponding polarization states in the BB84 protocol. The polarization is modulated via the PBS and the PC, and the average light intensity is modulated via the attenuator. Each laser produces three light pulses with different intensities including signal, decoy and vacuum states. The signal and decoy states contain mean photon numbers of 0.6 and 0.2 per pulse, respectively, and the ratio between the signal, decoy, and vacuum states is 6:1:1. The optical misalignment is less than 0.5%. In the detection side, a four-channel InGaAs single-photon detector is integrated with the following parameters. The detection efficiency is 10%, the dark count is 10^{-6}, the dead time is 2 μs, the afterpulse probability is less than 0.5% and the effective gate width is 500 ps. The receiver detects the light signal with the PC as a polarization feedback. The Cir is used to realize transmission and reception of light signals simultaneously. BS: beam splitter; PBS: polarizing beam splitter; PC: polarization controller; Att: attenuator; Cir: circulator.

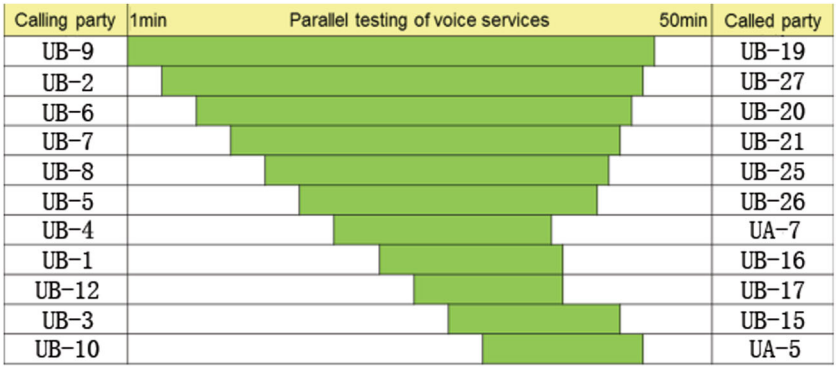

Fig. 3 Twenty-two users simultaneously make calls with QKD protocols. The green areas represent the duration over which users make calls.

key management server, i.e. its upstream optical switch or trusted relay node. A sequence of 32 kbit initial keys with the trusted relay or optical switch is used for authentication. The authentication is implemented by the HMAC algorithm based on the symmetric key algorithm SM4[23], which does not provide information-theoretic security. Within 2 min after power-on, the QKD device is connected to the network. Then, the device is in the queue for key generation.

Security analysis

We follow the standard decoy-state BB84 security analysis[18,20] and its finite size analysis[24]. The secret key rate of the BB84 protocol is given by[18,25]

$$r = -fQ_\mu H(E_\mu) + Y_1\mu e^{-\mu}[1 - H(e_1^p)], \quad (1)$$

where f is the error correction efficiency, μ is the mean photon number per pulse for a signal state, Q_μ is the overall gain for the signal states, E_μ is the quantum bit error rate (QBER), Y_1, e_1^p are the yield and phase error rate of the single-photon component and $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary Shannon entropy function. The single-photon yield and phase error rate can be well estimated by the decoy-state method[18]. In fact, only three intensities (signal, weak decoy and vacuum) are enough to give tight bounds[20], as implemented in our network.

In the finite-size case, there will be deviations in the estimations of parameters given above due to the statistical fluctuations. The main finite-size effect comes from the phase error rate estimation[24]. Suppose we use Z-basis states to generate key, then the single-photon phase error rate in this basis e_1^{pz} is bounded by the single-photon bit error rate in X basis e_1^{bx} and a small deviation θ optimized according to the experimental data[24]

$$e_1^{pz} \le e_1^{bx} + \theta \quad (2)$$

with a failure probability of

$$\epsilon_{ph} \le \frac{\sqrt{n_x + n_z}}{\sqrt{e_1^{bx}(1-e_1^{bx})n_x n_z}} 2^{-(n_x+n_z)\xi(\theta)} \quad (3)$$

where n_x and n_z are the numbers of bits measured in X and Z basis, respectively, and $\xi(\theta) = H(e_1^{bx} + \theta - n_x\theta/(n_x+n_z)) - n_x H(e_1^{bx})/(n_x+n_z) - (1 - n_x/(n_x+n_z))H(e_1^{bx} + \theta)$. There will also be failure probabilities in other steps including the authentication, error verification and privacy amplification. These failure probabilities are functions of the secure key consumption in the corresponding steps, and have additivity due to the composable security. In Supplementary Note 2, we will show how to calculate the finite-size key rate in detail.

Application

For the application of our network, users could make use of the generated secure keys to confidentially transfer information. The message is encoded in FPGA modules with an exclusive OR operation on the secure keys. We apply our network to transmit encrypted information such as real-time voice telephone, instant messaging and digital files with the one-time pad encryption method[26]. The total amount of information to be encrypted is 10 Gbit. The encryption speed is 800 Mbps. The total delay in the encryption process is less than 50 μs. In our network, the speed of real-time voice telephone was 2.4 kbps and the speed of file transmission was 320 kbps. The capacity of our network is tested for 50 min, as shown in Fig. 3. In all, 22 users simultaneously made calls in the quantum network for 6 min (see Supplementary Note 1 for more details).

Network robustness

In addition, the stability and robustness of the network were tested by running continuously for 31 months. We choose some representative nodes and show the key rates versus time in Fig. 4. The key rate results are summarized in Table 2, ranging from 6 to 60.5 kbps. Since the Hefei network is based on the Roll-Call-Polling protocol, all the results are average key rates during the QKD process. The key rate fluctuation mainly comes from the fast variations of photon polarization, which is determined by the internal structure and surrounding environment of the optical fibre. The error rate caused by the variations of photon polarization will accumulate with the propagation of the photons, leading to a drop in the key rate. Once the error rate is high enough, the QKD process is aborted and calibration is performed. Then the key rate will return to a normal value, corresponding to the ascensions in key rate performance.

DISCUSSION

In summary, we have presented a practical, large-scale metropolitan QKD network with standard commercial QKD products, systematic key management and practical usage in Hefei, China. This quantum network can be scaled by adding more users and relays, and it can be connected to the Shanghai–Beijing backbone to become a national network. Our network can be combined with other QKD protocols that are robust against device imperfections. For instance, to overcome the imperfection of measurement devices, measurement-device-independent (MDI) QKD protocols[27] can be employed. In experiment, the MDI-QKD protocol has been extensively verified and an MDI-QKD network over unreliable metropolitan has been recently realized[28]. Combined with the MDI-QKD network, one can imagine that communication in the future can be done in both efficient and

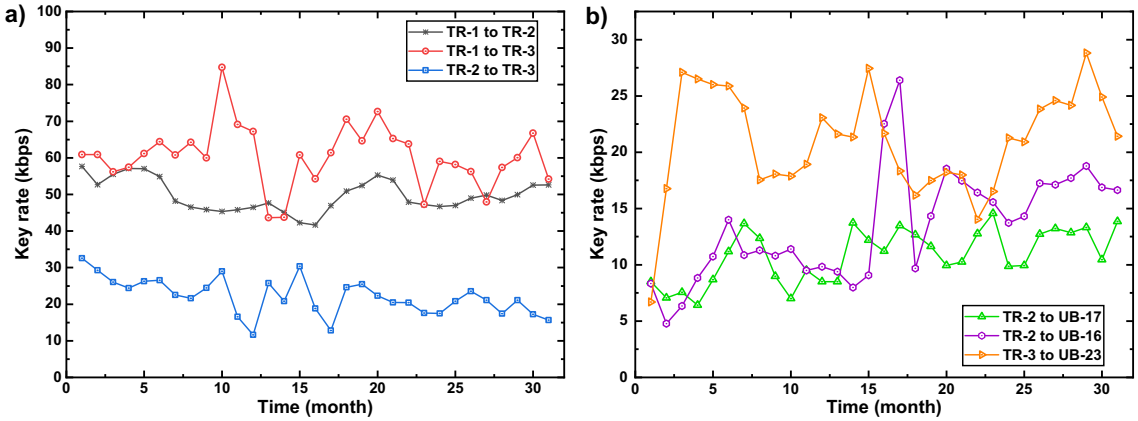

Fig. 4 The key rates versus time for some representative links. a The key rates between the three trusted relays. **b** The key rates between trusted relay and user. In the robustness test, 11 user nodes have continuously run for 31 months. The key rates are recorded every 30 s and taken average over a month. The detailed key rates are given in Supplementary Tables V and VI.

Table 2. List of the average key rates between subnetworks and the key rate ranges with in the three subnetworks (lower).

	TR1-TR2	TR1-TR3	TR2-TR3
Average key rate (kbps)	22.1	49.7	60.5
	TR1 subnetwork	TR2 subnetwork	TR3 subnetwork
Key rate range (kbps)	6~17	10~30	6~37

The detailed key rates are presented in Supplementary Tables II, III and IV.

secure ways. Recently an intercontinental QKD network was reported[15], connecting several metropolitan networks with a satellite. Our practical implementations and applications of a metropolitan network can be well combined with[15] for future directions.

DATA AVAILABILITY

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Received: 6 March 2021; Accepted: 3 August 2021;
Published online: 07 September 2021

REFERENCES

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems, and Signal Processing* 175–179 (IEEE, New York, 1984).
2. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
3. Ursin, R. et al. Entanglement-based quantum communication over 144 km. *Nat. Phys.* **3**, 481 (2007).
4. Takesue, H. et al. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nat. Photonics* **1**, 343 (2007).
5. Nauerth, S. et al. Air-to-ground quantum communication. *Nat. Photonics* **7**, 382 (2013).
6. Wang, J.-Y. et al. Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. *Nat. Photonics* **7**, 387 (2013).
7. Elliott, C. et al. Current status of the DARPA quantum network. In *Quantum Information and Computation III* Vol. 5815, 138–150 (International Society for Optics and Photonics, 2005).
8. Peev, M. et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001 (2009).
9. Stucki, D. et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **13**, 123001 (2011).
10. Wang, S. et al. Field test of wavelength-saving quantum key distribution network. *Opt. Lett.* **35**, 2454 (2010).
11. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387 (2011).
12. Chen, T.-Y. et al. Field test of a practical secure communication network with decoy-state quantum cryptography. *Opt. Express* **17**, 6540 (2009).
13. Chen, T.-Y. et al. Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **18**, 27217 (2010).
14. Liao, S.-K. et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501 (2018).
15. Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 1 (2021).
16. 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).
17. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
18. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
19. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
20. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
21. Buttler, W. T. et al. Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A* **67**, 052303 (2003).
22. Krawczyk, H. New hash functions for message authentication. In *International Conference on the Theory and Applications of Cryptographic Techniques* 301–310 (Springer, 1995).
23. Krawczyk, H., Bellare, M. & Canetti, R. *HMAC: Keyed-Hashing for Message Authentication* (RFC Editor, 1997).
24. Fung, C.-H. F., Ma, X. & Chau, H. F. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **81**, 012318 (2010).
25. Gottesman, D., Lo, H.-K., Lutkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. In *Proc. International Symposium on Information Theory, ISIT 2004* 136 (IEEE, 2004).
26. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949).
27. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
28. Tang, Y.-L. et al. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X* **6**, 011024 (2016).

ACKNOWLEDGEMENTS

The authors acknowledge insightful discussions with Z. Zhang. This work was supported by the National Key Research and Development Program of China (2017YFA0303903), Anhui Initiative in Quantum Information Technologies, and the Chinese Academy of Sciences. The authors also acknowledge support from the Anhui Provincial Government, the Hefei City Government, the Hefei Broadcast & TV Broad Band Network Ltd.

AUTHOR CONTRIBUTIONS

J.-W.P. conceived the research and supervised the project. T.-Y.C. and J.-W.P. designed the experiment. T.-Y.C. led the experimental implementation. X.J. developed the single-photon detectors. S.-B.T., J.W., H.-F.Z. and K.C. realized the control and data post-processing systems for QKD. L.Z. realized the key management system. L.-K.C. and H.L. designed and realized the quantum-encrypted telephone. W.-Y.L. designed the QKD data post-processing algorithms. H.L. designed the electrical circuits for the QKD source. X.-G.L. designed the QKD overall system and structure, as well as system manufacture. X.Y., H.Z. and X.M. analysed the security of the system. X.Y., H.Z., Y.M., L.-J.W., Q.Z., X.M., T.-Y.C. and J.-W.P. wrote the manuscript. Y.L. participated in the design for the network experiment. S.-B.F., Q.C. and Y.Z. coordinated all the external resources for the experiment. L.L. and N.-L.L. managed the project. C.-Z.P. provided technical support.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-021-00474-3.

Correspondence and requests for materials should be addressed to T.-Y.C.