npj | quantum information

Article

Published in partnership with The University of New South Wales

https://doi.org/10.1038/s41534-025-01089-8

Implementation of carrier-grade quantum communication networks over 10000 km

Check for updates

Hao-Ze Chen[1,2,3], Ming-Han Li[1,2,3], Yu Zhou Wang[1], Zhen-Geng Zhao[2], Cheng Ye[1,2], Fei Long Li[1,2], Zhu Chen[2], Sheng-Long Han[2], Bao Tang[2], Ya Jun Miao[1,2] ✉ & Wei Qi[1,2] ✉

Quantum computing poses a serious threat to classical cryptographic algorithms based on computational complexity. Quantum key distribution (QKD), utilizing the principles of quantum mechanics, enables secure key exchange and has been proven to be an essential technology to resist the threat of quantum computing. China attaches great importance to the construction of QKD network to deal with this threat. In 2020, China established an integrated space-to-ground quantum communication network, which includes 32 backbone nodes and 4 metropolitan networks. Here we introduce China's latest progress in the deployment of QKD networks, called the China Quantum Communication Network (CN-QCN). CN-QCN is an operational, long-range, and trusted-relay-based QKD network spanning over 10,000 kilometers, incorporating 145 fiber backbone nodes, and 20 metropolitan networks, which cover 17 provinces and 80 cities. Moreover, the network has deployed 6 ground stations linked with Jinan-1 quantum microsatellite. CN-QCN has not only surpassed its predecessor in scale, but also made significant advancements in multi-type QKD hybrid networking and long-range quantum network operation and maintenance. We present the network architecture, QKD implementation, and long-term performance of CN-QCN in this paper. This work lays the foundation for widespread applications of QKD in China.

As a countermeasure against quantum computing threats, Quantum Key Distribution (QKD)[1], provides a robust solution by enabling distant parties to establish a shared secret key with information-theoretic security. Over the past four decades, QKD technology has made significant progress in achieving longer transmission distances, higher secure key rate, and improved practical security. The transmission distance has increased from an initial 32 cm^2 in laboratory experiments to over 1000 km[3,4]. On a separate front, secure key rates have also seen dramatic improvements, now exceeding 100 Mbps in high-performance setups[5]. Simultaneously, a comprehensive practical security protocol framework has been systematically established and implemented[6].

Many countries and regions around the world have launched field tests of QKD networks, including DAPRA's three-user network (2003)[7], the six-node SECOQC network in Austria (2008)[8], the Swiss QKD network featuring three-node key management functionality (2009)[9], the six-node mesh-type network in Tokyo (2010)[10], the three-node high-speed quantum metropolitan ring network in Cambridge (2019)[11], the 46-node quantum metropolitan network in Hefei (2021)[12], etc. For long-distance backbone QKD networks, China initiated the construction of the world's first long-distance quantum backbone network, the Beijing-Shanghai Backbone Network (BSBN), in 2013. The network was completed by 2017, spanning 2032 km and comprising 32 nodes. In 2020, BSBN established a satellite-to-ground link with the Micius satellite, creating the world's first integrated satellite-ground quantum secure communication network, spanning of 4600 km[13]. The European Union launched the OPENQKD project in June 2019 and constructed QKD network exceeding 1000 kilometers[14]. Base on OPENQKD project, the European Union began the construction of European Quantum Communication Infrastructure (EuroQCI), where MadQCI has been deployed using Software-Defined Networking (SDN) in Spain (2024)[15] and interconnection tests between remote QKD networks has been conducted in Berlin, Madrid, and Poznan (2024)[16].

To achieve more reliable, secure, and long-range key distribution, and to facilitate the transition of quantum networks from technology verification networks to carrier-grade networks, China has launched the national quantum communication network project (CN-QCN). Compared to BSBN, CN-QCN significantly expands its coverage by newly constructing 145 fiber backbone nodes, 6 ground station backbone nodes, 20 metropolitan networks, and an operations and maintenance (O&M) center, extending across 17 provinces and 80 cities. CN-QCN is interconnected with BSBN, and the combined fiber mileage of the two exceeds 12,000

[1]CAS Quantum Network Co., Ltd., Shanghai, China. [2]Anhui CAS Quantum Network Co., Ltd., Hefei, China. [3]These authors contributed equally: Hao-Ze Chen, Ming-Han Li. ✉e-mail: miaoyajun@qtict.com; qiwei@qtict.com

kilometers, making it the largest quantum network in the world to date. In this paper, we present the network topology and architecture of CN-QCN. Subsequently, we focus on the technical solutions and key generation performance of different types of QKD devices deployed in the backbone and metropolitan networks. Finally, we analyze the long-term operational status of CN-QCN.

Results

Network topology

CN-QCN consists of several backbone networks and metropolitan networks. Spanning across China's principal urban centers, the backbone network operates in coordination with BSBN to implement a distinctive "two-horizontal, two-vertical" topological framework that optimizes nationwide connectivity. Notably, Beijing, Jinan, Hefei, and Wuhan, as well as Shanghai, Hangzhou, Hefei, and Nanjing form two ring structures, enabling ring-topology protection within the QKD network. The backbone network comprises 145 fiber backbone nodes and 144 fiber links, with a total optical fiber length of approximately 10,103 km. The average distance between adjacent QKD nodes is about 70 km, with an average attenuation of 18.61 dB per link. Among the 145 backbone nodes, 41 are designated as backbone access nodes with metropolitan network access capabilities, while the remaining 104 nodes serve as relay nodes. As illustrated in Fig. 1, the green lines represent CN-QCN backbone links, the yellow lines indicate BSBN, and the red circles denote backbone access nodes, which are capable of interfacing with metropolitan networks and performing key relaying in multiple directions. The yellow dots represent trusted relay nodes located between backbone access nodes, each responsible for key forwarding to neighboring nodes.

Some backbone access nodes are connected to metropolitan networks. Metropolitan networks enable users within a metropolitan region to access the QKD network and establish cross-regional interconnections via the backbone. Depending on the city scale and user distribution, several access nodes are deployed in each metropolitan network. The metropolitan access nodes are interconnected using ring or chain topologies, while the links from access nodes to user nodes adopt a tree topology. Each user node can provide quantum keys to multiple end user systems. We have deployed QKD devices and optical switches at each metropolitan access node to enable time-division multiplexing (TDM) for different user nodes. Each optical switch supports switching for up to 24 user nodes. To date, metropolitan networks have been deployed in 20 cities including Beijing, Shanghai, Jinhua, Haikou, and Chongqing, comprising 36 access nodes which are able to support more than 800 user nodes. These access nodes can be upgraded and expanded according to user demands.

The backbone nodes in Beijing, Shanghai, Guangzhou, Chongqing, Hainan, and Xinjiang are equipped with satellite ground stations. Through the Jinan-1 quantum microsatellite, key relays are established to create KM links, thereby interconnecting the satellite-ground and fiber-based QKD infrastructures. The detailed information about the Jinan-1 quantum microsatellite can be found in ref. 17.

An operation and maintenance (O&M) center has been established for the entire QKD network. It performs real-time collection of QKD

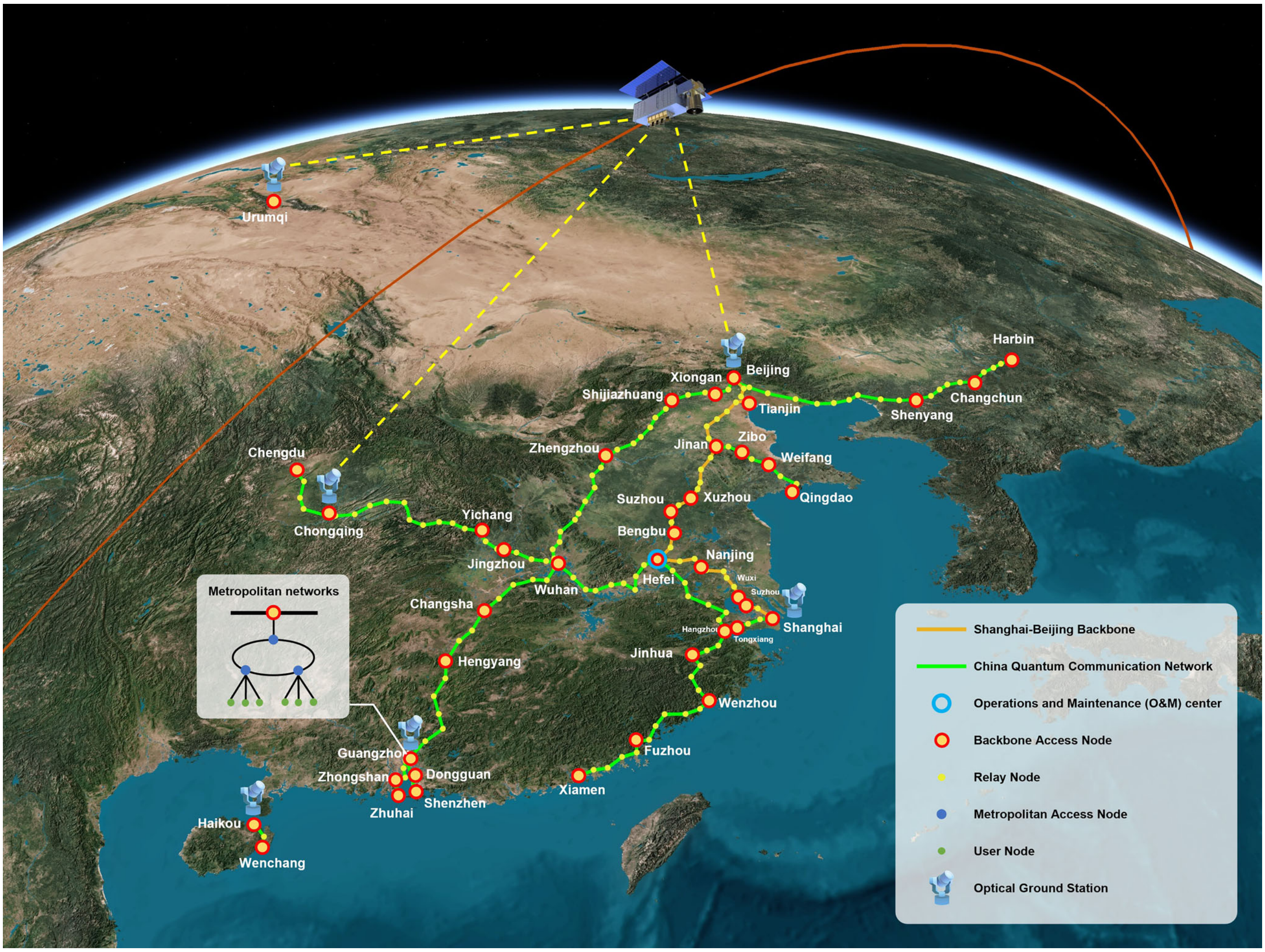

Fig. 1 | Network topology. The backbone network comprises CN-QCN (green lines) and BSBN (yellow lines). There are 145 backbone nodes, 41 (red circles) are backbone access nodes, while the remaining 104 nodes are relay nodes (yellow dots). The blue circle denotes the O&M center. In the metropolitan network, the blue dots indicate metropolitan access nodes, and green dots represent user nodes. The quantum microsatellite can connect to ground stations.

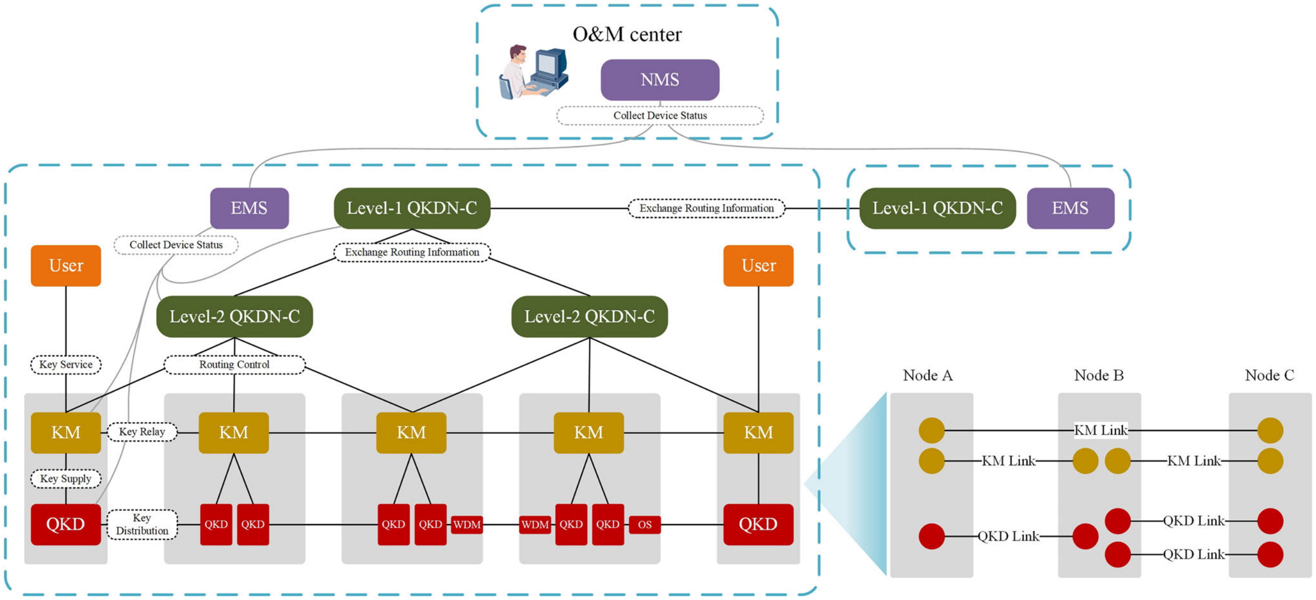

Fig. 2 | Functional architecture of the QKD network. The network consists of five layers: the quantum layer, the key management layer, the QKD network control layer, the QKD network management layer and the application layer. The quantum layer is responsible for key distribution between two adjacent nodes. The key management layer performs key relaying based on the One-Time-Pad scheme to complete an end-to-end key distribution. The QKD network control layer is responsible for key routing calculation and control. The QKD network management layer monitors the network status. The application layer uses the secure keys for encryption and authentication. Definitions of abbreviations, QKD: Quantum Key Distribution device; WDM: Wavelength division multiplexers; OS: Optical Switch; KM: Key Manager; QKDN-C: QKD Network Controller; EMS: Element Management System; NMS: Network Management System; User: End User System.

performance indicators such as secure key rate, quantum bit error rate, KM-Links status, etc. It also monitors the physical environment of equipment rooms and the operation status of classical communication systems, ensuring 24/7 maintenance services for the quantum network.

To ensure the long-term stability and security of CN-QCN, the network not only uses independent server room spaces and dark fiber resources, but also deploys exclusive equipment, including Optical Transport Network (OTN) devices, Network Time Protocol (NTP) servers, network security devices and so on. These measures ensure strict network isolation between CN-QCN and the Internet, preventing information leakage and cyber-attacks. We present deployment schematics for several representative nodes in Supplementary Note 1.

Network architecture

The functional architecture of CN-QCN comprises the quantum layer, key management layer, QKD network control layer, QKD network management layer, and application layer (Fig. 2), in accordance with the ITU-T Y.3802 recommendation Quantum Key Distribution Networks—Functional Architecture[18]. In the quantum layer, QKD-links utilize either the decoy-state BB84 protocol[19] or Gaussian-modulated continuous-variable (CV) QKD protocols[20,21] to generate QKD-keys between two adjacent nodes which are subsequently delivered to the key management layer. Wavelength division multiplexers (WDM) or optical switches (OS) are used for multiplexing quantum channels. The key management layer performs key relaying based on the One-Time-Pad scheme, establishing key management links (KM-Links) between two arbitrary nodes to enable end-to-end, networked key distribution and provide key services to end user systems. Notably, each KM-Link may utilize one or more underlying QKD-Links. These KM-Links can establish both direct connections between adjacent nodes and remote connections between non-adjacent nodes via predefined key relay paths. The QKD network control layer is responsible for key routing calculation and control. It gathers real-time data on the key quantity of each KM-link, computes the optimum key relay paths according to the demand of key services and dispatches key relay policies to the corresponding KM devices. The control layer adopts a hierarchical architecture: Level-1 QKD network controllers are in charge of inter-domain routing between backbone and metropolitan networks within a given region, while Level-2 QKDN controllers are responsible for intra-domain routing of one backbone or metropolitan network. If there is a need for key relaying between different regional networks, the corresponding Level-1 controllers should coordinate the routing processes. The QKD network management layer also follows a hierarchical deployment model. The element management system (EMS) in each region collects device status from local network elements and transmits the information via northbound interfaces to the centralized network management system (NMS) located at the O&M center. This facilitates real-time status monitoring of the entire network.

QKD implementation

In backbone networks, we have deployed four distinct high-speed QKD systems, all adhering to the decoy-state BB84 protocol. Three of these systems are polarization-encoding systems operating at a repetition frequency of 625 MHz (labeled as Types I, II, and III), and the other one is a phase-encoding system operating at a repetition frequency of 312.5 MHz (labeled as Type IV). Type I incorporates a single-laser scheme (for details, see Supplementary Fig. 2). In this scheme, the laser at the transmitter emits optical pulses that are modulated into decoy states by an intensity modulator, followed by a polarization encoding module to achieve modulation of four polarization states. At the receiver side, four InGaAs/InP single-photon detectors with a detection efficiency of 15% are utilized. Type II and Type III transmitters share the same structure, both employing a multi-laser scheme (as detailed in Supplementary Fig. 3), utilizing eight lasers to achieve modulation of four polarization states for signal and decoy states. At the receiver side, Type II implements four up-conversion single-photon detectors with a detection efficiency of 20%, whereas Type III utilizes four InGaAs/InP single-photon detectors with a detection efficiency of 10%. In the Type IV system (as illustrated in Supplementary Fig. 4), the transmitter primarily consists of two Sagnac interferometers and an asymmetric Mach-Zehnder interferometer, which together facilitate the intensity modulation and encoding of quantum states. The receiver employs a Faraday mirror-based Michelson interferometer for decoding, with a detection efficiency of 15%.

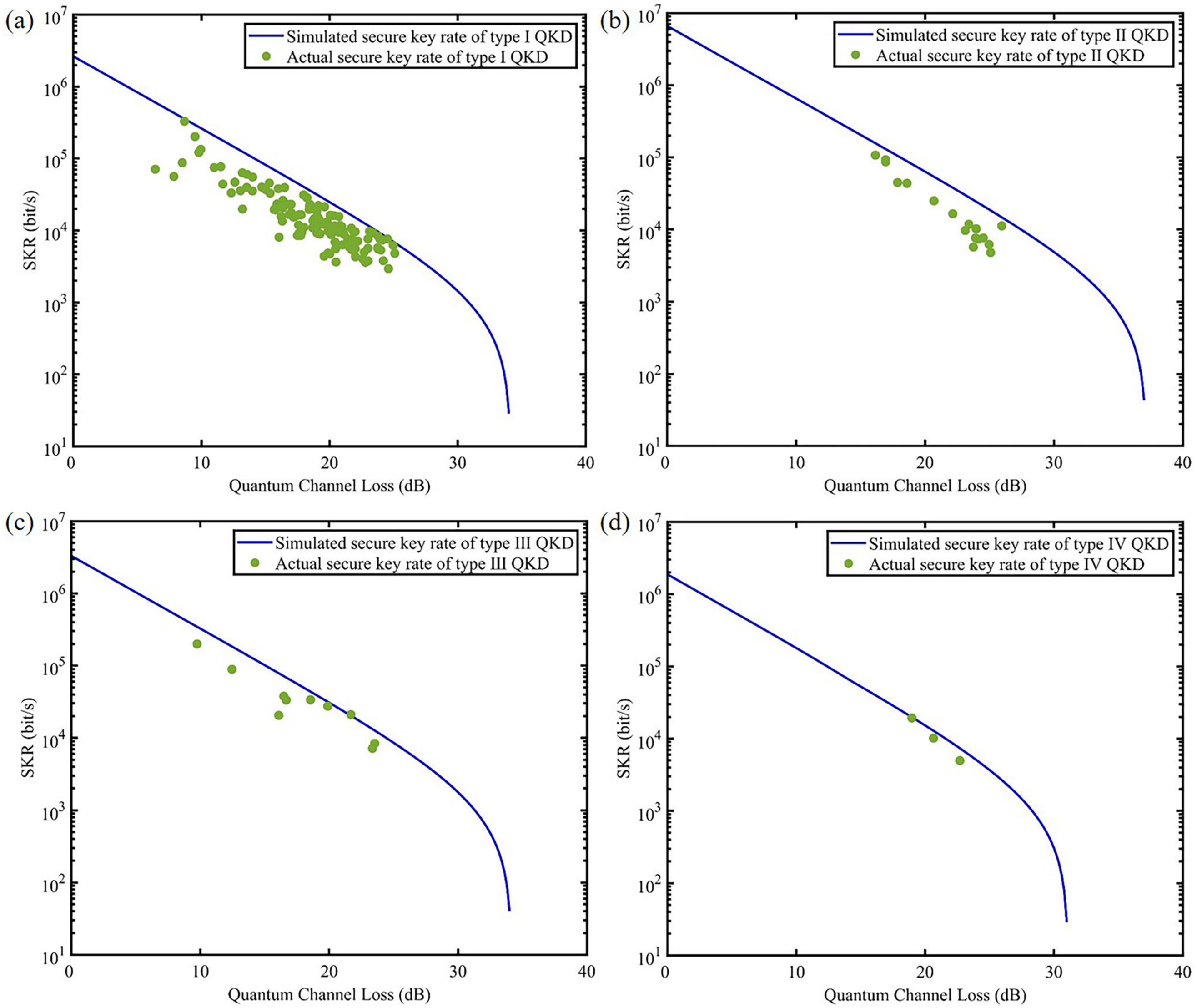

Fig. 3 | Relationship between the secure key rate (SKR) of single pairs at backbone network nodes and quantum channel loss. Panels (**a**–**d**) represent the system SKR for Types I, II, III, and IV, respectively. The blue lines indicate the simulated secure key rates, while the green dots represent the actual secure key rates generated by the QKD systems.

These QKD devices account for the primary quantum hacking strategies and have been designed with corresponding countermeasures. For instance, the decoy-state protocol has been implemented to counter photon-number-splitting attacks[22]; the transmitter of the QKD system is equipped with optical circulators to achieve high isolation, preventing Trojan-horse attacks[23] and laser seeding attacks[24]. The receiver is safeguarded against time-shift attacks[25] by precisely setting the detector delays. Also, an electrical monitor is included for real-time monitoring of the output current from the single-photon detectors, to counter detector blinding attacks[26]. Compared to multi-laser schemes, the single-laser scheme further prevents side-channel attacks that arise from the inability to maintain complete consistency in the attributes of laser wavelength, temporal characteristics and so on[27].

Although the same type of QKD systems follow identical technical standards, variations in the performance of components and operating environments can still lead to differences in the secure key rates. For instance, the intrinsic quantum bit error rate may vary from 0.5% to 2% in actual environments, the dark count rate for single-photon detectors generally ranges between 600 Hz and 1000 Hz, and the error correction efficiency typically ranges from 1.2 to 2. Furthermore, the methods for calculating the secure key rate exhibit slight differences among various types of devices. Supplementary Note 2 details the system architecture, typical parameters, and secure key rate calculation method for each QKD system types.

Figure 3 illustrates the relationship between the single-pair secure key rate and quantum channel loss in the backbone network. To avoid redundant statistics under identical conditions, the figure includes data from only one pair of QKD systems selected from multiple pairs of the same type of QKD systems deployed in the same fiber link. To accurately assess the discrepancies between the actual and theoretical secure key rates, we plotted the single-pair secure key rates for identical types of QKD systems on the same graph. Subsequently, we simulated the relationship between the secure key rate and channel loss using ideal system parameters, which include an intrinsic error rate of 0.5%, a dark count rate of 600 Hz, and an error correction efficiency of 1.2. The results indicate that the actual secure key rate is lower than the theoretical value, attributable to several factors: variations in device performance due to differences in manufacturing processes; in practical applications, QKD systems are affected by temperature fluctuations and fiber vibrations, leading to reduced quantum channel stability and increased error rates; synchronization light leakage increases the noise; and fluctuations in error rates limit the optimal parameter

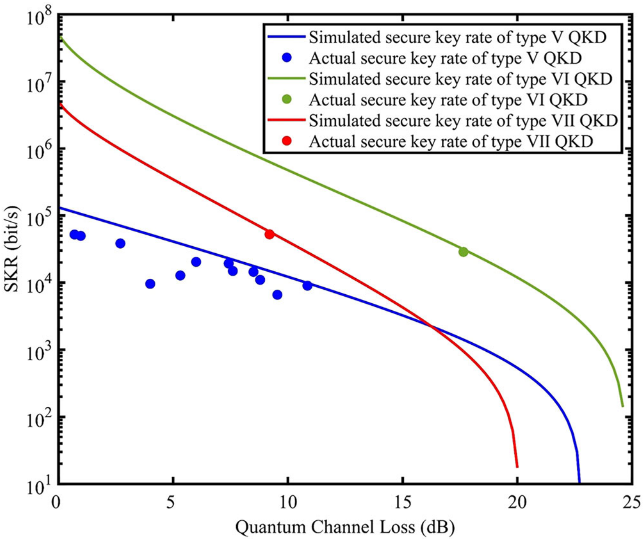

Fig. 4 | Relationship between the single pair secure key rate (SKR) at metropolitan network nodes and quantum channel loss. The blue, green, and red lines and dots correspond to the simulated and actual SKRs for QKD system types V, VI, and VII, respectively.

selection for error correction algorithms, thereby reducing the efficiency of error correction. Collectively, these factors contribute to the reduction in the actual secure key rate. Nonetheless, the trend of the actual secure key rate remains consistent with the theoretical simulation results, and QKD devices operate within the linear range where the secure key rate is linearly related to the channel transmittance.

In metropolitan networks, where fiber link loss is relatively low, we have deployed a low-speed QKD system based on the decoy-state BB84 protocol (labeled as Type V), as well as two types of CV-QKD devices based on Gaussian-modulated coherent states (labeled as Types VI and VII). Type V QKD systems utilize a single-laser scheme, featuring an optical structure similar to that of Type I, operating at a repetition frequency of 40 MHz, with an intrinsic error rate ranging from 0.5% to 2%, and a detection efficiency of 10%. Type VI CV-QKD systems employ a locally-generated local oscillator (LLO) scheme, wherein the transmitter employs IQ modulation technology with a modulation variance set to 4 and a repetition frequency of 125 MHz. At the receiver, after heterodyne detection of the quantum signal and LO, bit information is yielded, with a quantum efficiency of approximately 0.43 and an electrical noise variance of about 0.2 (SNU). Type VII systems adopt a transmitted local oscillator (TLO) scheme, with a modulation variance set to 4 and a modulation rate of 10 MHz. In contrast to the LLO scheme, the TLO scheme generates the LO and quantum signal light from the same laser, which are then time and polarization multiplexed using an isolate polar-

Fig. 5 | Backbone secure key rate performance. **a** Average secure key rates of all adjacent KM-Links along the Harbin-Shenzhen path in a period of 10 weeks, with the horizontal axis indicating the abbreviations of relay node locations in the backbone network. **b** Weekly average end-to-end secure key rates between Harbin and Beijing, Beijing and Wuhan, Wuhan and Guangzhou, Guangzhou, and Shenzhen.

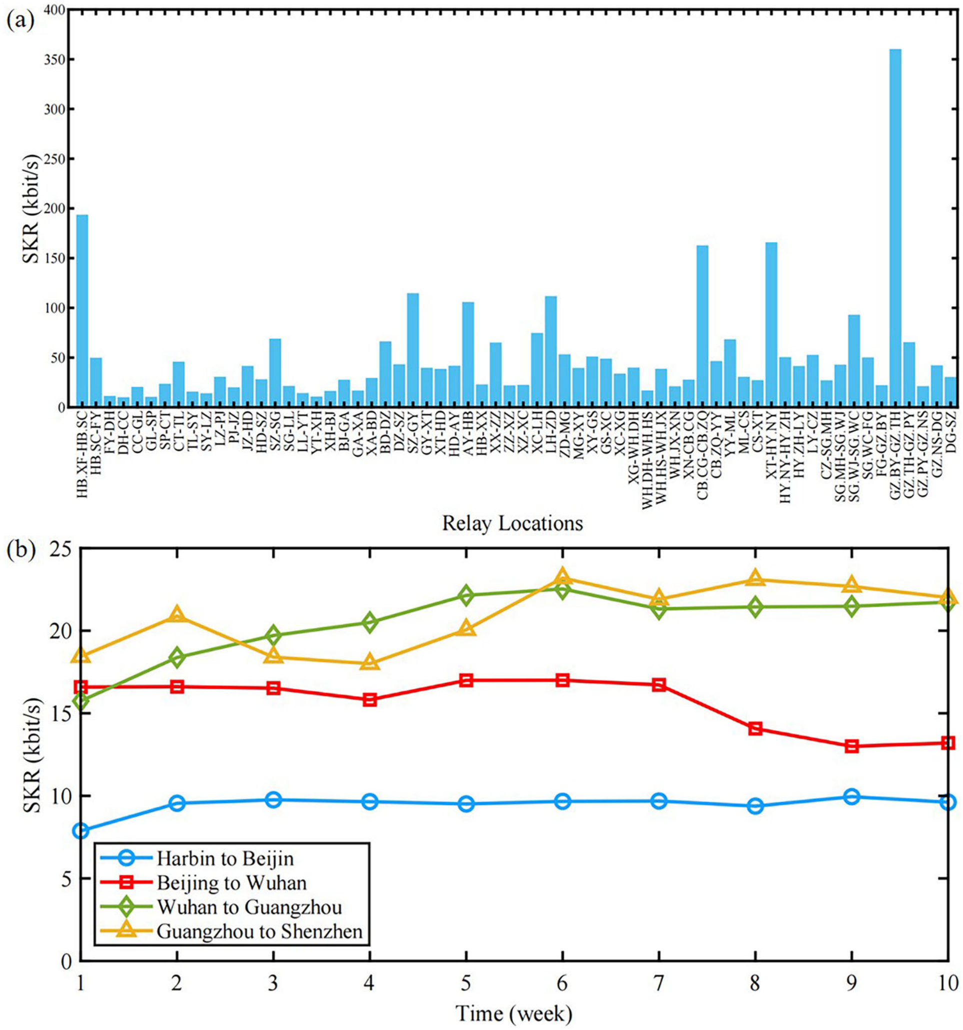

Table 1 | List of the durations when KM-Links failed to provide service (hours)

	Harbin-Beijing (3 KM-Link)	Beijing-Wuhan (4 KM-Link)	Wuhan-Guangzhou (3 KM-Link)	Guangzhou-Shenzhen (2 KM-Link)
Week 1	0.51	0	1.01	0
Week 2	0	0	0	0
Week 3	1.69	0	0	0
Week 4	0.09	0	0.96	0
Week 5	1.21	0	0	0
Week 6	0	0	0	0
Week 7	0.49	0	0	0
Week 8	0.51	0	0.91	0
Week 9	0.17	0	0	0
Week 10	0.46	0	0	0
SUM	5.13	0	2.88	0

ization beam splitter. At the receiver, a homodyne detection scheme is employed, with a quantum efficiency of 0.6 and an electrical noise variance of approximately 0.13. Details of the system structures for Types V, VI, and VII can be found in Supplementary Note 2. In Fig. 4, we present a comparison between the actual and simulated secure key rates for Types V, VI, and VII QKD systems within metropolitan networks.

Network reliability and security

To evaluate the secure key rate performance of the backbone network, we selected the backbone network from Harbin to Shenzhen and conducted statistics over a period of 10 weeks. As shown in Fig. 5a, we present the average secure key rates of all adjacent KM-Links between Harbin and Shenzhen over this period. Among the 64 KM-Links, the minimum secure key rate was 9.75 kbps, and the maximum was 359.89 kbps. Furthermore, we segmented the link from Harbin to Shenzhen into four segments: Harbin to Beijing, Beijing to Wuhan, Wuhan to Guangzhou, and Guangzhou to Shenzhen. For each segment, the end-to-end secure key rate is determined by the minimum secure key rate among all KM-Links between adjacent nodes. The average end-to-end secure key rates for the four segments were 9.75 kbps, 16.41 kbps, 20.73 kbps, and 20.85 kbps, respectively. We also calculated the weekly average end-to-end secure key rates for these segments and depicted their variations over this period, as illustrated in Fig. 5b. The experimental results demonstrate that all segments sustained consistent secure key rates throughout the extended operation period.

Moreover, we monitored the key service availability of 12 KM-Links between every backbone access node from Harbin to Shenzhen, as shown in Table 1. It records the service interruption durations for each of the four network segments on a weekly basis over the ten-week observation period. The results show that KM-Links from Beijing to Wuhan were always available due to the existence of redundant routing paths. In contrast, single-link topologies are more vulnerable to disruptions because of the interruption of any fiber link or the equipment failure of one node, for instance, the KM-Links from Harbin to Beijing and from Wuhan to Guangzhou. Therefore, ring-topology protection is particularly necessary for long-distance QKD backbones.

Besides, during the construction of CN-QCN, particular emphasis was placed on the overall security of the network to ensure compliance with general security standards. This is especially critical because layers above the quantum layer are no longer inherently protected by the principles of quantum mechanics. Compared to BSBN, CN-QCN incorporates more comprehensive technical safeguards and stricter management practices across five layers: physical environment, network communication, device software, application data, and security management. For example, stringent physical access control mechanisms were implemented to secure trusted relay nodes. These measures collectively enable CN-QCN to support large-scale applications in sectors such as government, finance, and energy.

Discussion

In summary, this paper presents a carrier-grade quantum communication network developed in China, comprising over 10,000 km of optical fiber links, which represents an important milestone in the development of the global quantum communication network. CN-QCN has not only surpassed BSBN in scale, but also made significant advancements in multi-type QKD hybrid networking and long-range quantum network operation and maintenance. We illustrate the topology and architecture of the network, and explain the actual deployment and the main business processes of the network. We focus on the technical solutions and key generation status of the 7 types of QKD devices deployed in the backbone and metropolitan networks. Finally, we examine the secure key rate and availability of the network during long-term operation, which demonstrates the stability and robustness of the network operation. We hold the view that CN-QCN will become an important information security infrastructure in China, laying the foundation for countering the threat of quantum computing. In the future, with the development of quantum measurement[28] and quantum relay[29] technologies, this network can also serve as a testbed and incubator for various quantum information technologies, paving the way for the development of the quantum internet.

Data availability

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

Received: 27 December 2024; Accepted: 26 July 2025;
Published online: 08 August 2025

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. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **5**, 3–28 (1992).
3. Liu, Y. et al. Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.* **130**, 210801 (2023).
4. Liu, Y. et al. 1002 km twin-field quantum key distribution with finite-key analysis. *Quantum Front.* **2**, 16 (2023).
5. Li, W. et al. High-rate quantum key distribution exceeding 110 Mb s–1. *Nat. Photon.* **17**, 416–421 (2023).
6. 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).
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. *N. J. Phys.* **11**, 075001 (2009).
9. Stucki, D. et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *N. J. Phys.* **13**, 123001 (2011).
10. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387 (2011).
11. Dynes, J. F. et al. Cambridge quantum network. *npj Quantum Inf.* **5**, 101 (2019).
12. Chen, T. Y. et al. Implementation of a 46-node quantum metropolitan area network. *npj Quantum Inf.* **7**, 134 (2021).
13. Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4600 kilometers. *Nature* **589**, 214–219 (2021).
14. European Union. CORDIS - EU research results. https://cordis.europa.eu/project/id/857156 (2024).

15. Martin, V. et al. MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities. *npj Quantum Inf.* **10**, 80 (2024).
16. Brauer, M. et al. Linking QKD Testbeds across Europe. *Entropy* **26**, 123 (2024).
17. Li, Y. et al. Microsatellite-based real-time quantum key distribution. *Nature* **640**, 47–54 (2025).
18. ITU-T Y.3802. Quantum key distribution networks – Functional architecture[S] (2020).
19. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
20. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
21. Weedbrook, C. et al. Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).
22. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330–1333 (2000).
23. Lucamarini, M. et al. Practical security bounds against the Trejan-Hose attack in quantum key distribution. *Phys. Rev. X* **5**, 031030-1-19 (2015).
24. Sun, S.-H. et al. Effect of source tampering in the security of quantum cryptography. *Phys. Rev. A* **92**, 022304 (2015).
25. 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).
26. Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686–689 (2010).
27. Gnanapandithan, A., Qian, L. & Lo, H.-K. Hidden multidimensional modulation side channels in quantum protocols. *Phys. Rev. Lett.* **134**, 130802 (2025).
28. Komar, P. et al. A quantum network of clocks. *Nat. Phys.* **10**, 582–587 (2014).
29. 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).

Acknowledgements

This work was supported by the National Development and Reform Commission and other relevant ministries, the Chinese Academy of Sciences, and the Hefei National Laboratory. This work was funded by National wide-area quantum secure communication network Project, “east data, west computing” Quantum-safe cloud Service Project, Innovation Program for Quantum Science and Technology (2021ZD0301300), and Soft Science Research Project of Shanghai (25692107800). We are grateful to QuantumCTek Co., Ltd. and XT Quantech Co., Ltd. for providing the parameters and optical structures of the QKD systems, as well as for the helpful discussions. The author also acknowledges Zi-Han Zhang and Gui-Zhong Zhang, for their contributions to the writing and illustration.

Author contributions

W.Q. and Y.J.M. conceived the research and supervised the project. H.-Z.C. and M.-H.L. designed the experiment and analyzed the data, these two authors contributed equally to this work. Y.Z.W., Z.-G.Z., C.Y., F.L.L. and B.T. collected the data and wrote the manuscript. Z.C. and S.-L.H. led the experimental implementation.

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/s41534-025-01089-8.

Correspondence and requests for materials should be addressed to Ya Jun Miao or Wei Qi.