

Field and long-term demonstration of a wide area quantum key distribution network

Shuang Wang,^{1,2} Wei Chen,^{1,2,5} Zhen-Qiang Yin,^{1,2,6} Hong-Wei Li,^{1,2,3}
De-Yong He,^{1,2} Yu-Hu Li,³ Zheng Zhou,^{1,2} Xiao-Tian Song,^{1,2} Fang-Yi
Li,^{1,2} Dong Wang,^{1,2} Hua Chen,^{1,2} Yun-Guang Han,^{1,2} Jing-Zheng
Huang,^{1,2} Jun-Fu Guo,⁴ Peng-Lei Hao,⁴ Mo Li,^{1,2} Chun-Mei Zhang,^{1,2}
Dong Liu,^{1,2} Wen-Ye Liang,^{1,2} Chun-Hua Miao,⁴ Ping Wu,⁴
Guang-Can Guo,^{1,2} and Zheng-Fu Han^{1,2,7}

¹Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, China

²Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, CAS, Hefei 230026, China

³Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230026, China;

⁴Anhui Asky Quantum Technology Co.,Ltd. , Wuhu 241002, China

⁵kooky@mail.ustc.edu.cn

⁶yinzheqi@mail.ustc.edu.cn

⁷zghan@ustc.edu.cn

Abstract: A wide area quantum key distribution (QKD) network deployed on communication infrastructures provided by China Mobile Ltd. is demonstrated. Three cities and two metropolitan area QKD networks were linked up to form the Hefei-Chaohu-Wuhu wide area QKD network with over 150 kilometers coverage area, in which Hefei metropolitan area QKD network was a typical full-mesh core network to offer all-to-all interconnections, and Wuhu metropolitan area QKD network was a representative quantum access network with point-to-multipoint configuration. The whole wide area QKD network ran for more than 5000 hours, from 21 December 2011 to 19 July 2012, and part of the network stopped until last December. To adapt to the complex and volatile field environment, the Faraday-Michelson QKD system with several stability measures was adopted when we designed QKD devices. Through standardized design of QKD devices, resolution of symmetry problem of QKD devices, and seamless switching in dynamic QKD network, we realized the effective integration between point-to-point QKD techniques and networking schemes.

© 2014 Optical Society of America

OCIS codes: (270.5568) Quantum cryptography; (060.5565) Quantum communications.

References and links

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145 (2002).
2. V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**, 1301 (2009).
3. A. Müller, H. Zbinden, and N. Gisin, "Underwater quantum coding," *Nature*, **378**, 449-449 (1995).
4. R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, and C. Simmons, "Quantum cryptography over underground optical fibers," *Lecture Notes in Computer Science*, **1109**, 329-342 (1996).

5. P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electron. Lett.* **33**, 188-190 (1997).
6. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.* **81**, 3283-3286 (1998).
7. R. J. Hughes, G. L. Morgan, and C. G. Peterson, "Quantum key distribution over a 48 km optical fibre network," *J. Mod. Opt.* **47**, 533-547 (2000).
8. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New J. Phys.* **4**, 41.1-41.8 (2002).
9. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "Quantum cryptography: A step towards global key distribution," *Nature* **419**, 450-450 (2002).
10. Z. L. Yuan and A. J. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre," *Opt. Express* **13**, 660-665 (2005).
11. X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, "Faraday-Michelson system for quantum cryptography," *Opt. Lett.* **30**, 2632 (2005).
12. J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields, "Stability of high bit rate quantum key distribution on installed fiber," *Opt. Express*, **20**, 16339-16347 (2012).
13. P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alleaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, "Field test of classical symmetric encryption with continuous variables quantum key distribution," *Opt. Express*, **20**, 14030-14041 (2012).
14. T. Langer and G. Lenhart, "Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD," *New J. Phys.* **11**, 055051 (2009).
15. G. Lenhart, "QKD standardization at ETSI," *AIP Conference Proceedings*, **1469**, 50-57 (2012).
16. A. Shields and Y. L. Yuan, "Key to the quantum industry," *Physics World*, **12**, 24-29 (2007).
17. P. D. Townsend, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, "Design of quantum cryptography systems for passive optical networks," *Electron Lett.* **30**, 1875 (1994).
18. P. D. Townsend, "Quantum cryptography on multi-user optical fibre networks," *Nature*. **385**, 47 (1997).
19. T. Nishioka, H. Ishizuka, T. Hasegawa, and J. Abe, "Circular type quantum key distribution," *IEEE Photon. Technol. Lett.* **53**, 1310-1314 (2002).
20. G. Brassard, F. Bussi eres, N. Godbout, and S. Lacroix, "Multi-user quantum key distribution using wavelength division multiplexing," *Proc. SPIE* **5260**, 149 (2003).
21. P. Toliver, R.J. Runser, T.E. Chapuran, J.L. Jackel, T.C. Banwell, M.S. Goodman, R.J. Hughes, C.G. Peterson, D. Derkacs, J.E. Nordholt, L. Mercer, S. McNown, A. Goldman, J. Blake, "Experimental investigation of quantum key distribution through transparent optical switch elements," *IEEE Photon. Technol. Lett.* **15**, 1669-1671 (2003).
22. P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, "Comparison of four multi-user quantum key distribution schemes over passive optical networks," *J. Lightwave Technol.* **23**, 268 (2005).
23. L. J. Ma, H. Xu and X. Tang, "Polarization recovery and auto-compensation in quantum key distribution network," *Proc. SPIE*, **6305**, 630513 (2006).
24. T. Zhang, X. F. Mo, Z. F. Han, and G. C. Guo, "Extensible router for a quantum key distribution network," *Phys. Lett. A* **372**, 3957 (2008).
25. M. Dianati, R. Alleaume, M. Gagnaire, and X. M. Shen, "Architecture and protocols of the future European quantum key distribution network," *Security and Communication Networks* **1**, 57-74 (2008).
26. R. Alleaume, F. Roueff, E. Diamanti, and N. Lutkenhaus, "Topological optimization of quantum key distribution networks," *New J. Phys.* **11**, 075002 (2009).
27. S. Wang, W. Chen, Z. Q. Yin, Y. Zhang, T. Zhang, H. W. Li, F. X. Xu, Z. Zhou, Y. Yang, D. J. Huang, L. J. Zhang, F. Y. Li, D. Liu, Y. G. Wang, G. C. Guo, and Z. F. Han, "Field test of wavelength-saving quantum key distribution network," *Opt. Lett.* **35**, 2454 (2010).
28. E. Donkor, "Experimental auto-compensating multi-user quantum key distribution network using a wavelength-addressed bus line architecture," *Proc. of SPIE* **8397**, 839704 (2012).
29. M. Razavi, "Multiple-access quantum key distribution networks," *IEEE Trans. Commun.* **60**, 3071-3079 (2012).
30. B. Fr ohlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, "A quantum access network," *Nature*, **501**, 69-72 (2013).
31. A. Ciurana, J. Mart inez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Mart ın, "Quantum metropolitan optical network based on wavelength division multiplexing," *Opt. Express*, **22**, 1576-1592 (2014).
32. C. Elliott, "Building the quantum network," *New J. Phys.* **4**, 46.1 (2002).
33. C. Elliott, "Current status of the DARPA quantum network," in *Quantum Information and Computation III*, *Proc. SPIE* **5815**, 138-149 (2005).
34. W. Chen, Z. F. Han, T. Zhang, H. Wen, Z. Q. Yin, F. X. Xu, Q. L. Wu, Y. Liu, Y. Zhang, X. F. Mo, Y. Z. Gui, G. Wei, and G. C. Guo, "Field experiment on a "Star Type" metropolitan quantum key distribution network," *IEEE Photonics Tech. Lett.* **21**, 575 (2009).
35. A. Poppe, M. Peev, and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna," *Int. J. Quantum Inf.* **6**, 209 (2008).

36. M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J.F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorinser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A.W. Sharpe, A.J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.* **11**, 075001 (2009).
37. F. X. Xu, W. Chen, S. Wang, Z. Q. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. B. Zhao, H. W. Li, D. Liu, Z. F. Han, and G. C. Guo, "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chinese Sci. Bull.* **54**, 2991 (2009).
38. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the tokyo QKD network," *Opt. Express*, **19**, 10387-10409 (2011).
39. A. Mirza and F. Petruccione, "Realizing long-term quantum cryptography," *J. Opt. Soc. Am. B*, **27**, A185-188 (2010).
40. D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J. -B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Vörol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New J. Phys.* **13**, 123001 (2011).
41. T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy, "Optical networking for quantum key distribution and quantum communications," *New J. Phys.* **11**, 105001 (2009).
42. T. Y. Chen, H. Liang, Y. Liu, W. Q. Cai, L. Ju, W. Y. Liu, J. Wang, H. Yin, K. Chen, Z. B. Chen, C. Z. Peng, and J. W. Pan, "Field test of a practical secure communication network with decoy-state quantum cryptography," *Optics Express*, **17**, 6540-6549 (2009).
43. T. Y. Chen, J. Wang, H. Liang, W. Y. Liu, Y. Liu, X. Jiang, Y. Wang, W. Q. Cai, L. Ju, L. K. Chen, L. J. Wang, Y. Gao, K. Chen, C. Z. Peng, Z. B. Chen, and J. W. Pan, "Metropolitan all-pass and inter-city quantum communication network," *Optics Express*, **18**, 27217-27225 (2010).
44. D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin, "QKD in Standard Optical Telecommunications Networks," *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, **36**, 142-149 (2010).
45. K. A. Patel, J.F. Dynes, I. Choi, A.W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber," *Phys. Rev. X* **2**, 041010 (2012).
46. http://en.wikipedia.org/wiki/Inter-city_rail.
47. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New J. Phys.* **11**, 075003 (2009).
48. S. Wang, W. Chen, J. F. Guo, Z.Q. Yin, H. W. Li, Z. Zhou, G.C. Guo, and Z.F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Opt. Lett.* **37**, 1008-1010 (2012).
49. L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature* **414**, 413-418 (2001).
50. S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," *Nature Photon.* **7**, 382-386 (2013).
51. A. Tanaka, M. Fujiwara, K. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, "High-Speed Quantum Key Distribution System for 1-Mbps Real-Time Key Generation," *IEEE J. Quantum Electron.* **48**, 542-550 (2012).
52. K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.* **104**, 051123 (2014).
53. R. Ursin and R. Hughes, "Quantum information: sharing quantum secrets," *Nature* **501**, 37-38 (2013).
54. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE, 1984)*, p.175-179.
55. W. Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Phys. Rev. Lett.* **91**, 057901 (2003).
56. X. B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.* **94**, 230503 (2005).
57. H. K. Lo, X. F. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.* **94**, 230504 (2005).
58. V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryp-

- tosystems,” *Phys. Rev. A* **74**, 022313 (2006).
59. B. Qi, C. F. Fung, H. K. Lo, and X. F. Ma, “Time-shift attack in practical quantum cryptosystems,” *Quant. Inf. Comp.* **7**, 73-82 (2007).
 60. <http://www.hongsi-ic.com>.
 61. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nature Photon.* **4**, 686-689 (2010).
 62. Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Avoiding the blinding attack in QKD,” *Nature Photon.* **4**, 800-801 (2010).
 63. Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography,” *Appl. Phys. Lett.* **98**, 231104 (2011).
 64. A. Acín, N. Gisin, and L. Masanes, “From Bell’s theorem to secure quantum key distribution,” *Phys. Rev. Lett.* **97**, 120405 (2006).
 65. H. K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” *Phys. Rev. Lett.* **108**, 130503 (2013).
 66. M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, “Photon level crosstalk between parallel fibers installed in urban area,” *Opt. Express*, **18**, 22199-22207 (2010).
-

1. Introduction

The principle of a quantum key distribution (QKD) system is to share secure keys between two remote users. Different from the ways employing mathematical techniques to avoid eavesdroppers, the unconditional security of QKD originates from quantum physics, and has been theoretically proved [1, 2]. Since Muller et al. successfully implemented the first QKD experiment over 23 km installed optical fiber under Lake Geneva [3], several groups have demonstrated their QKD experiments in field environments [4–13]. QKD has moved far beyond laboratory experiments. Commercial QKD systems are available from some companies, and moreover, European Telecommunication Standards Institute has published standards for QKD to fulfill urgent market needs [14, 15].

As an important milestone, quantum network, or more precisely QKD network, was proposed to extend QKD from point-to-point configuration to multi-user and large-scale scenario [16]. Based on the passive beam splitter, Townsend et al. presented and realized the first QKD network [17, 18]. And since then, researchers have devised and developed an impressive collection of network architectures for QKD [19–31]. Combined with increasingly mature QKD devices, these developments enabled QKD networks to be deployed over real-world telecommunication networks. Under US Defense Advanced Research Projects Agency (DARPA), researchers from BBN Technologies, Boston University and Harvard University built the world’s first QKD network across a metropolitan area – DARPA quantum network [32, 33]. Then, based on the quantum router structure [24], our group from University of Science and Technology of China realized the second field QKD network in the commercial telecommunication fiber network in Beijing in March 2007 [34]. The SEcure COmmunication based on Quantum Cryptography (SECOQC) network in Vienna integrated 6 different QKD systems together through trusted repeaters [35, 36]. Also, “Q-Government network” built by our group was a field trial of application of quantum keys [37]. In 2010, the most high-speed QKD network was presented in Tokyo, where the live video conferencing using one-time-pad (OTP) encryption was successfully demonstrated [38]. Long-term performance of QKD networks have also been tested [39, 40], in which SwissQuantum network [40] ran for more than one-and-a-half year. And, other QKD networks were also deployed in the field environment [41–44].

In order to furthest extend the applicability of QKD technologies, QKD networks leverage available fiber networks, and take advantage of the technologies, components and topologies for conventional fiber communications [41]. Figure 1 illustrates the schematic overview of one QKD network, which is a wide area QKD network, and for the sake of simple illustration, only four cities are included. The wide area QKD network is composed of metropolitan area QKD networks and intercity backbone QKD network which consists of long-haul intercity QKD links

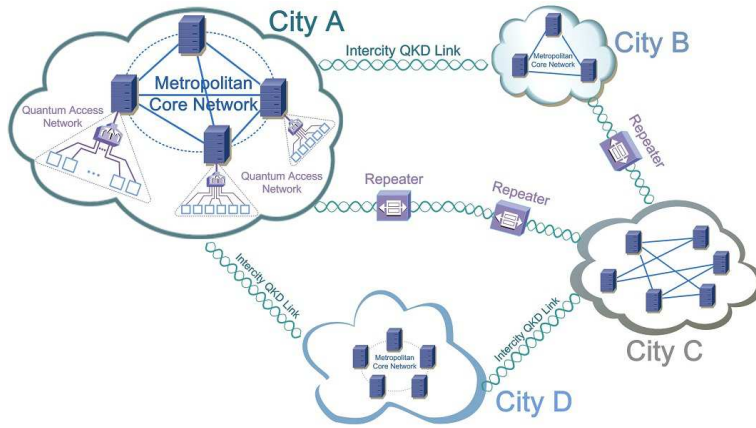


Fig. 1. Schematic overview of a wide area QKD network.

among metropolitan area QKD networks. The metropolitan area networks usually span several tens of kilometers [31], such as the typical range of smart cities is 30-80 km [45], while distances of intercity links at least exceed 50 km [46]. Although the transmission distance of QKD systems is already over 250 km [47, 48], quantum techniques including trusted repeater, quantum repeater [49], and ground-to-satellite communication [50] would be used in the intercity link to extend the distance scale, and multiplex techniques [51, 52] would also be employed to increase the key rate. The tradeoff between key rates and relay distances is one of the key issues should be considered before intercity QKD links are deployed. In each city, the metropolitan area QKD network comprises metropolitan core networks and quantum access networks. The metropolitan core network is the core part of the metropolitan area QKD network, which usually has a mesh configuration to provide all-to-all interconnections among the network nodes, the interconnectivity should be taken into account when we plan the core network. The quantum access network encompasses connections that extend from one node in the metropolitan core network to multiple end-users, and provides the last-mile QKD service for subscribers [30, 53]. Therefore, quantum access network usually follows point-to-multipoint topology and covers a few tens of kilometers [31]. And, subscribers belonged to different quantum access networks are connected through the metropolitan core network.

In this paper, we present a wide area QKD network demonstrated in the field environment. The network was installed in the Anhui provincial telecommunication fiber network of China Mobile Ltd., with over 150 kilometers coverage area. Three cities and two metropolitan area QKD networks were linked up by intercity QKD links to form the wide area QKD network, in which one metropolitan area QKD network was a typical full-mesh core network based on the QKD router and switch techniques to offer all-to-all interconnections, and the other one was a simulative quantum access network using the $1 \times N$ switch to realize the point-to-multipoint configuration. The whole wide area QKD network ran for more than 5000 hours, from 21 December 2011 to 19 July 2012, and part of the network stopped until last December. To adapt to the complex and volatile network environment, standardized design of QKD devices and several networking techniques were tried when the wide area QKD network was field deployed. And, we also developed and tested two typical applications of quantum keys on this QKD network.

Compared with previous QKD networks [32–44], the Hefei-Chaohu-Wuhu QKD network is not only the first wide area QKD network, but also shows significant improvements on the

QKD networking scheme and technology. In the respect of networking scheme, for the core QKD network, we designed and implemented the novel all-to-all scheme based on the combination of passive and active optical elements, and for the quantum access network, we proposed and implemented the practical point-to-multipoint scheme based on the optical switch. Beyond novelty, these networking schemes make the QKD network more reliable, flexible and reconfigurable. In the respect of networking technology, we have successfully resolved two crucial issues – the symmetry of QKD devices and seamless switching among different links. These successes further enhance the competitiveness of QKD network in the field environment.

2. Overview of the Hefei-Chaohu-Wuhu wide area QKD network

The Geographic distribution of the wide area QKD network is presented in Fig. 2, Hefei, Chaohu, and Wuhu are three connected cities in the network. The Hefei-Chaohu-Wuhu wide area QKD network consists of three parts: (1) Hefei metropolitan area QKD network, which has 5 nodes, one node is in Wan-Tong Post and Telecommunication (WTPT) Co. Ltd., the other 4 nodes are all in the campuses of University of Science and Technology of China (USTC), both Library (Lib) and Key Laboratory of Quantum Information (KLQI) are located in the East Campus, other two nodes respectively locate in the North Campus (NC) and West Campus (WC), and these 4 nodes compose the Quantum Campus Network of USTC (QCN-USTC); (2) Wuhu metropolitan area QKD network, which has 3 nodes that are located in the Telecom Room (TR) of China Mobile, Wuhu Branch (WHB) of China Mobile, and Asky Quantum Technology Co. Ltd. (Qasky); (3) Hefei-Chaohu-Wuhu (HCW) intercity QKD link, which combines Hefei and Wuhu metropolitan area QKD networks together through the trusted intermediate node lies in the Chaohu Branch (CHB) of China Mobile. 6 nodes are located in the north of Changjiang river, and the other 3 nodes are located in the south of Changjiang river, hence the HCW wide area QKD network is the first QKD network across the Changjiang river.

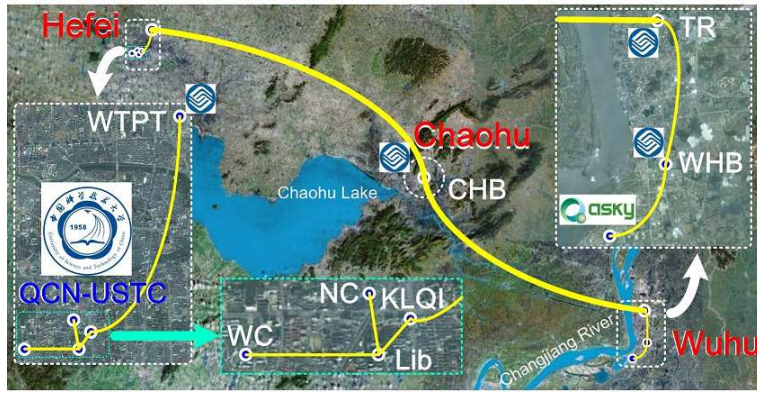


Fig. 2. Geographic distribution of the Hefei-Chaohu-Wuhu wide area QKD network, which connects three cities – Hefei, Chaohu, and Wuhu.

There are 8 optical fiber links among 9 nodes in the wide area QKD network, as the yellow lines in Fig. 2. All the 8 optical fiber links are characterized as table 1. The total length of the installed fiber is almost 200 km, of which the intercity fiber length exceeds 150 km.

Figure 3 shows the topology of the whole wide area QKD network. Two kinds of networking schemes [38, 40] were adopted in the wide area QKD network. One is based on trusted intermediate nodes, there were three trusted intermediate nodes in the three parts of the whole QKD network respectively: WTPT in the Hefei metropolitan area network, TR in the Wuhu

Table 1. Characteristics of fiber links in the Hefei-Chaohu-Wuhu wide area QKD network.

	Optical fiber link	Length of fiber(km)	Optical loss(dB)
Hefei metro network	WTPT-USCT(KLQI)	16.9	-6.1
	KLQI-Lib	0.9	-1.2
	QCN-USTC	1.2	-0.6
	WC-Lib	1.9	-0.5
HCW-intercity link	Hefei-Chaohu	85.1	-18.4
	Chaohu-Wuhu	69.7	-14.1
Wuhu metro network	TR-WHB	14.3	-5.0
	WHB-Qasky	9.0	-7.1

metropolitan area network, and CHB in the HCW-intercity link. The other one is based on additional optical components, in which the fiber was shared among multiple nodes, both Hefei and Wuhu metropolitan area QKD networks were realized in this way. The Hefei metropolitan area network is full-mesh, each network node has direct link with all the other nodes in this network. And, the Wuhu metropolitan area QKD network is a time division multiplexing type, only one point-to-point (P2P) QKD link exists at each time. Here, the full-mesh Hefei metropolitan area QKD network is one typical metropolitan core network to offer all-to-all interconnections, while the Wuhu metropolitan area QKD network is used to simulate a quantum access network.

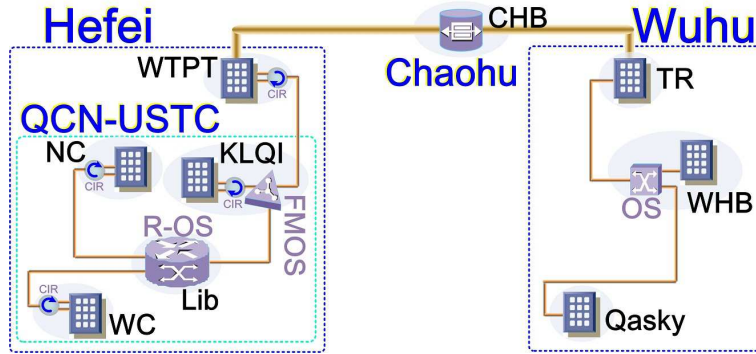


Fig. 3. Topology of the wide area QKD network. CIR: optical circulator, OS: optical switch, FMOS: full-mesh optical switch, R-OS stands for the combination of the QKD router and optical switch.

3. P2P QKD devices in the wide area QKD network

In the HCW wide area QKD network, a total of 13 QKD devices were employed to support the two metropolitan area QKD networks and intercity QKD links. To manufacture and maintain these QKD devices, it would require a large amount of work. Therefore, standardized design of QKD devices was tried before deployment of the wide area QKD network, especially for the symmetry among QKD devices which will be discussed later. All P2P QKD devices adopted the Faraday-Michelson interferometer (FMI) system [11] to implement phase coding BB84 protocol [54] with the decoy state method [55–57]. And, all parts of each QKD devices were housed in a standardized 3.5U rack mount case ($15.6 \times 44 \times 40$, H×W×D, cm), in which the optics, associated electronics, the single photon detector, and one computer with a displayer

and a keyboard were all included. We designed two types of P2P QKD devices: one is the divided type, in which the QKD-Transmitter and the QKD-Receiver were separated in two cases respectively; the other was the integral type, named QKD-Transceiver, in which the QKD-Transmitter and the QKD-Receiver were integrated together in one case with an optical switch.

3.1. The divided type – QKD-Transmitter and QKD-Receiver

Figure 4 outlines the divided type QKD device. Both sync and quantum signals are transmitted through the same fiber channel.

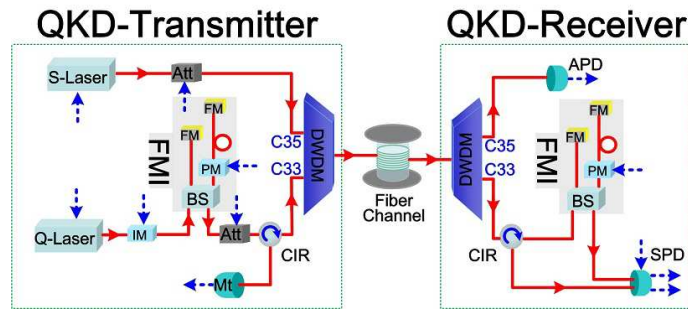


Fig. 4. Schematic of the divided QKD device.

In the QKD-Transmitter, the sync signal of 1549.32 nm (channel C33 of the ITU grid) wavelength is produced by the sync laser (S-Laser), and attenuated before entering the dense wavelength division multiplexing (DWDM). The quantum laser (Q-Laser) generates the 1550.92 nm (channel C35 of the ITU grid) pulse train with 20 MHz repetition rate and 600 ps pulse width. These quantum pulses are first prepared in decoy states by an intensity modulator (IM), then phase-encoded through the phase modulator (PM) in the Faraday-Michelson interferometer (FMI), and finally attenuated to single-photon level using an attenuator (Att). The 3-port optical circulator (CIR) and monitor (Mt) are added to prevent and detect possible Trojan-horse photons from the channel.

In the QKD-Receiver, DWDM is used to demultiplex the received sync and quantum pulses. The sync pulses is detected by a normal avalanche photodiode (APD) to keep the QKD-Receiver and QKD-Transmitter in synchronicity. After passing through CIR, phase-encoded quantum pulses are first phase-decoded by PM in the paired FMI, and then detected by the single photon detector (SPD). The InGaAs/InP APDs belonged to SPD is cooled down to -50°C , and works in Geiger mode with a gate width of less than 1 ns.

3.2. The integral type – QKD-Transceiver

Figure 5 shows the integral type QKD system that is named QKD-Transceiver. It consists of a QKD-Transmitter, a 2×2 optical switch (OS), and a QKD-Receiver. The 2×2 OS has two states: in the “cross” state (solid lines of OS in Figure 5) the QKD-Transmitter part communicates with remote QKD-Receiver, and the QKD-Receiver part communicates with remote QKD-Transmitter respectively to share secure keys; in the “bar” state (dash lines of OS in Figure 5) the QKD-Transmitter and the QKD-Receiver parts communicate with each other to calibrate parameters such as half-wave voltages and delay times, and the QKD-Transceiver is skipped in the network. Incidentally, the QKD-Transceiver might be a good form of the trusted repeater.

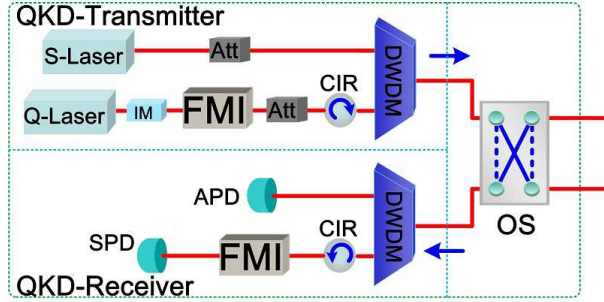


Fig. 5. Schematic of the QKD-Transceiver.

3.3. The security consideration of QKD devices

Practical security is a key consideration when QKD devices are built up. Many quantum hacking strategies based on imperfections of practical devices have been proposed, and some of them have been experimentally implemented successfully. For P2P QKD devices in HCW wide area QKD network, some proposed hacking strategies were considered, and corresponding countermeasures have been added into the QKD system as follows.

The decoy state method [55–57] was combined with BB84 protocol in the QKD device to exclude the PNS attack [2]. As a benefit, this method can dramatically increase the secure key rate. The decoy state method is implemented as follows: IM in the QKD-Transmitter is used to create the signal pulses of 0.65 (or 0.7) photons per pulse and the decoy pulses of 0.1 photons per pulse, the vacuum pulses are generated by not triggering Q-laser, and the ratio among the signal pulses, decoy pulses and vacuum pulses is 14:1:1.

Four phases ($\{0, \pi\}, \{\frac{\pi}{2}, \frac{3\pi}{2}\}$) modulation scheme was implemented in the QKD-Receiver to neutralize the fake state attack [58] and time-shift attack [59] which utilize the detection efficiency mismatch in the time domain. To restrain costs, only one InGaAs/InP APD was used in SPD for most QKD-Receivers, in which the four phases modulation is necessary.

Real-time physical random number generators (RNG) provided QKD devices with random bits. Quantum RNG is a critical component of QKD devices, but the commercial products such as Quantis from id Quantique is still difficult to meet the speed demand for QKD devices. As a compromise between speed and security, 20 Mbps physical RNG (WNG-8 from Beijing Hongsu Electronic Tech. Co. Ltd. [60]) based on thermal noise was adopted in our QKD devices. 6 pieces of such RNG were used in the QKD-Transmitter for random decoy state preparation (4×20 Mbps) and phase modulation (2×20 Mbps), and 2 pieces were used in the QKD-Receiver for phase demodulation.

The SPD component of QKD devices was transformed to avoid being controlled by bright light [61–63], and monitoring technologies was employed to detect bright light that sneaks into the QKD device. In addition to monitoring the photocurrent, the normal APD for sync signal detection was also an auxiliary monitor, because the isolation between C33 and C35 of DWDM is limited, usually -35 dB. And, for QKD-Receivers with only one APD in SPD, the output of FMI without connecting SPD was also monitored by normal APD.

Although practical security of QKD devices has been considered in this network, techniques such as device-independent QKD [64] or measurement-device-independent QKD [65] might be used in the future to further enhance the practical security.

4. Detailed layout of the HCW wide area QKD network

The QKD network is not a simple combination of QKD devices, but an effective integration between QKD devices and networking schemes (or techniques). In the HCW wide area QKD network, Hefei metropolitan part was based on QKD router and switch techniques to realize the full-mesh structure with 6 QKD devices, Wuhu metropolitan part used the $1 \times N$ switch to realize the point-to-multipoint configuration with $N+1$ QKD devices, and HCW-intercity link connected these two metropolitan part together through the trusted repeater technology. In particular, multiplexing are very useful techniques that share optical fiber channels and QKD devices to realize reliable, cost-competitive and reconfigurable QKD networks. We have resolved two key problems of multiplexing techniques - the symmetry of QKD devices and seamless switching in the HCW wide area QKD network.

4.1. Full-mesh Hefei metropolitan area QKD network

The Hefei metropolitan area QKD network is a full-mesh network with 4 QKD nodes as shown in Fig. 6. Each QKD node in the network had direct physical links to all the other nodes, although there were only 4 installed fiber channels. To share the limited fiber channel resource, we adopted QKD router and switch techniques, specifically, the wavelength-saving real-time full-mesh (RTFM) QKD router [27], and the time division multiplexing full-mesh optical switch (FMOS). Here, the router and switch served as optical components that were responsible for dynamically routing and blocking in the QKD network.

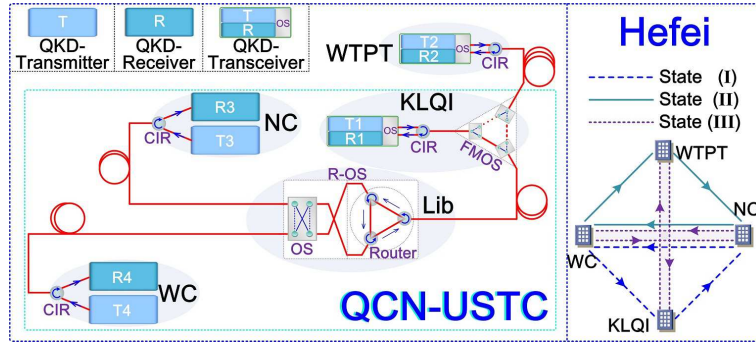


Fig. 6. Structure of full-mesh Hefei metropolitan area QKD network.

The structure of wavelength-saving RTFM router was propose in reference [27]. With N wavelengths, the wavelength-saving RTFM router can support a RTFM QKD network with $2N + 1$ QKD nodes, in which every two nodes share secure keys directly at the same time, and each node only has one fiber connecting with the router. Here, 3 CIRs were used to compose the simplest form of this router (see the router part of the R-OS in Fig. 6). Using single wavelength, this router can support a RTFM QKD network with 3 nodes, and every 2 nodes can share secure keys directly at the same time.

The structure of time division multiplexing FMOS is very similar with normal RTFM QKD router consisting of WDMs [24], each N wavelengths WDM is replace by a $1 \times N$ OS. Using FMOS with $N + 1$ ports, no more than $(N + 1)/2$ pair nodes can share secure keys directly at the same time, but every two nodes can distribute secure keys with each other by the time division multiplexing method. Here, three 1×2 optical switches were used to compose the simplest form of time division multiplexing FMOS (see the FMOS in Fig. 6). The FMOS can also support a full-mesh QKD network with 3 nodes, but only two nodes are connected at every time.

By combing the QKD router and FMOS as above, the full-mesh Hefei metropolitan area QKD network had three states (as shown in the right part of Fig. 6) corresponding to the three connection statuses of FMOS respectively.

State (I) – KLQI, NC and WC comprised the RTFM QKD network: the 2×2 optical switch was in the “cross” state, and the QKD-Transceiver at WTPT worked in the self-calibration mode, the quantum signals were from T1 to R3, from T3 to R4, from T4 to R1, and from T2 to R2, respectively.

State (II) – WTPT, NC and WC comprised the RTFM QKD network: the 2×2 optical switch was still in the “cross” state, and the QKD-Transceiver at KLQI worked in the self-calibration mode, the quantum signals were from T2 to R3, from T3 to R4, from T4 to R2, and from T1 to R1, respectively.

State (III) – KLQI and WTPT, NC and WC had duplex QKD links between each other: the 2×2 optical switch was in the “bar” state, and the quantum signals were from T1 to R2, from T2 to R1, from T3 to R4, and from T4 to R3, respectively.

Through controlling FMOS in the KLQI and 2×2 OS in the Lib, Hefei metropolitan area QKD network was in one of aforesaid tree states. There were 8 different direct QKD links in this QKD network, it was enough to support a full-mesh metropolitan core network with 4 QKD nodes.

4.2. Point-to-multipoint Wuhu metropolitan area QKD network

Wuhu metropolitan area QKD network is a quantum access network with three QKD nodes which are connected by a simple 1×2 optical switch with 1 output and 2 input ports. It is a typical point-to-multipoint access network with time division multiplexing, only one end node accesses QKD link at each time. As shown in Fig. 7, two QKD-Transmitters T7 and T8, which were respectively placed in WHB and Qasky, transmitted signals to the 2 input ports of the optical switch at different times, and one QKD-Receiver R7 which located in TR received signal from the output port of the optical switch. At each time, QKD-Receiver R7 only communicated with the QKD-Transmitters T7 or T8.

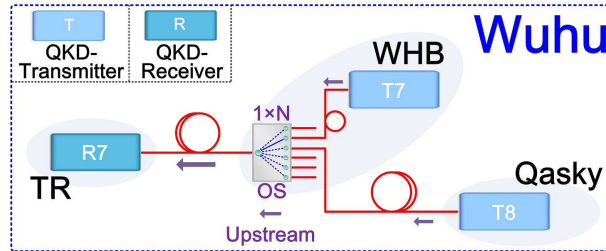


Fig. 7. Structure of point-to-multipoint Wuhu metropolitan area QKD network.

Replacing the 1×2 optical switch with $1 \times N$ one, this quantum access network could support N access nodes, with N QKD-Transmitters and only one QKD-Receiver. Since the QKD-Receiver requires SPDs, which are often expensive, difficult to operate [30], and bulky, the recommendable way is the upstream implementation, one QKD-Receiver receives signals from multiple QKD-Transmitters in the point-to-multipoint configuration. Beam splitter, WDM and optical switch are three optical components conveniently providing point-to-multipoint connections. Beam splitter has a high insertion loss about $-10 \lg N$ dB, WDM needs different laser sources, therefore, optical switch might be a compromise between beam splitter and WDM, but it requires a auxiliary system to offer power supply and remote control.

4.3. HCW-intercity QKD link

HCW-intercity QKD link connects Hefei and Wuhu cites, the distance and channel loss between which exceed 150 km and -32 dB respectively. In order to obtain practicable key rate, Chaohu city, which is located between Hefei and Wuhu, was chosen as the trusted intermediate node. Through the HCW-intercity QKD link, any node in Hefei metropolitan area QKD network could share secure keys with any node in Wuhu metropolitan area QKD network using the hop-by-hop fashion [26]. The optical loss of fiber channel between Hefei and Chaohu was -18.4 dB, but the loss between Chaohu and Wuhu was only -14.1 dB. Therefore, the best-matched QKD-Transmitter T5 and QKD-Receiver R5 were picked out to share secure keys between node WTPT in Hefei and node CHB in Chaohu, and the best two APDs were selected to compose SPD in R5. While, the second best-matched QKD-Transmitter T6 and QKD-Receiver R6 were used to share secure keys between node CHB in Chaohu and node TR in Wuhu, but only one APD was used in R6, the same as all the other QKD-Receivers. The Chaohu to Wuhu link is the first QKD link across the Changjiang river.

4.4. Symmetry of QKD devices

Symmetry of QKD devices is a pivotal issue for QKD networks, especially for the multiplexing type, in which one QKD device needs to communicate with multiple QKD devices. As to this specific wide area QKD network, in the Hefei metropolitan part, the QKD-Transmitter T1 needs to communicate with three different QKD-Receivers R3, R1, and R2 in the aforesaid three states, R3 needs to communicate with T1, T2, and T4, etc.; in the Wuhu metropolitan part, the same QKD-Receiver R7 has to communicate with two different QKD-Transmitters T7 and T8 in the time division multiplexing way. For these one-way phase coding QKD devices, the core symmetry problem is the matching requirements of every unbalanced interferometers - FMIs. Therefore, we have developed the method to fabricate FMIs, of which properties were almost the same. And, symmetry of QKD devices is finally characterized by measuring the quantum bit error rate (QBER) in back-to-back transmission. The measured results are given in table 2. From this table, QBERs of QKD-Transmitters (T1, T2, T3, T4) and QKD-Receivers (R1, R2, R3, R4) are all below 1.20%, and we may draw a conclusion that the symmetry problem of QKD devices has been largely resolved. If one QKD device in the network breaks, we only need to replace the broken one rather than paired devices, and if one new QKD node want to join the quantum access network, we just need one QKD-Transmitter, it makes the QKD technology more cost-competitive in the network respect.

Table 2. Symmetry characteristic of QKD devices

QBER	R1	R2	R3	R4
T1	0.97%	0.85%	0.70%	1.12%
T2	0.48%	1.02%	0.53%	1.07%
T3	0.86%	0.91%	1.09%	0.78%
T4	0.56%	0.62%	0.49%	0.67%

4.5. Seamless switching in QKD networks

Seamless switching is helpful to improve performances of dynamic QKD networks that have several states to switch back and forth, for example, QKD-Receiver R7 in Wuhu metropolitan area QKD network has to switch between two states to dynamically distribute keys with QKD-Transmitters T7 or T8. In QKD networks, the switching process includes not only changing the status of optical switching equipments, but also establishing a new QKD link or several

new QKD links. Although the switching is dynamic, the states before and after switching are deterministic, which means the QKD device knows in advance who it will communicate with. Therefore, QKD devices could store configuration parameters that need to communicate with other possible devices when the dynamic QKD network is deployed, then establishment of new QKD links is simplified to retrieve configuration parameters. And as mentioned above, the phase coding system based on unbalanced FMI was adopted, and the sync and quantum signals were multiplexed in the same fiber with 1.6 nm wavelength interval, these measures make the stored configuration parameters very stable for establishing new QKD links. In Hefei and Wuhu metropolitan area QKD networks, establishing new QKD links were proceeded simultaneously with changing the status of optical switches. For this reason, the switching process was very quick, and could be regarded as seamless. We designed two seamless switching modes here, the preemptive mode and automatic mode. If there were some special requirements, the preemptive switching mode worked, and the QKD network switched to and kept in the required state. At other times, the QKD network was in the automatic switching mode, and automatically switched to different states at set intervals to periodically update secure keys.

5. Long-term performance with the field environment

The field test assesses both performance and reliability of QKD networks in the actual operation environment. The field environments of the HCW wide area QKD network were relatively complicated: the optical fiber channels included the metropolitan area optical networks and intercity links, and operation environments of QKD nodes involved the telecom room, the laboratory, the normal room, and even the makeshift kitchen. Further, this whole QKD network ran for more than 5000 hours, from 21 December 2011 to 19 July 2012, and the the QCN-USTC part stopped until last December. For this long term, the field environment has changed a lot. For QKD networks, reliability is as essential as overall secure key rate. This effects not only the design of QKD devices, but also the topology of the QKD network. Therefore, the phase coding system based on FMI was adopted against fluctuations on the fiber channel, and the complex full-mesh topology was implemented in Hefei metropolitan core network to offer high flexibility and interconnectivity.

5.1. The field fiber channels and measures of crosstalk reduction

In the HCW wide area QKD network, most of the installed optical fiber channels were commercial fibers provided by China Mobile Ltd., and all fibers were standard telecom fiber (ITU-T G.652). From measurement results of the optical time domain reflector (Yokogawa, AQ7275), the fiber channels in intercity backbone links were very good - with no reflective events and 0.21 dB/km average loss coefficient, while, the fiber channels in metropolitan area were not good - with many reflective events and 0.46 dB/km average loss coefficient. In metropolitan area optical network, many splicing points and connectors combined numerous short fibers together, and reflective events from some splicing points and connectors with bad return loss made signals (including quantum and sync signals) in the channel influence each other, especially when several QKD links shared the same channel at the same time.

We improved the crosstalk suppression at the device level. To minimize the reflective noise on the quantum signals, nonadjacent channels of DWDM were chosen to transmit quantum and sync signals respectively, and between which time delay module was added. The field fiber channels were parallel with other commercial fibers in which high power optical streams were transmitted in the same multi-core cable, and these parallel fibers would leak photons into quantum channels [66], which made field fiber channels not dark any more. Different from forgoing reflective noise that could be considered as point events, the leakage photons would be continuous noise in the time and spectrum domain. However, this leakage noise could be

greatly reduced by the DWDM and the time gate of the SPD, which could be regarded as a spectral filter and a temporal bandpass respectively.

5.2. The operation environments of QKD devices

The performance of QKD devices is not only affected by the fiber channel, but also by the operation environments, which include environment temperature, humidity, pressure, dust, and ambient vibration. Figure 8 shows photographs of five QKD nodes in HCW wide area QKD network, WTPT and CHB nodes in the intercity QKD link, WHB node in Wuhu metropolitan area QKD network, WC and NC nodes in the QCN-USTC part of Hefei metropolitan QKD network. The operation environments of QKD devices can be divided into four types: the telecom room, the simple switching room, the office room, and the makeshift room.

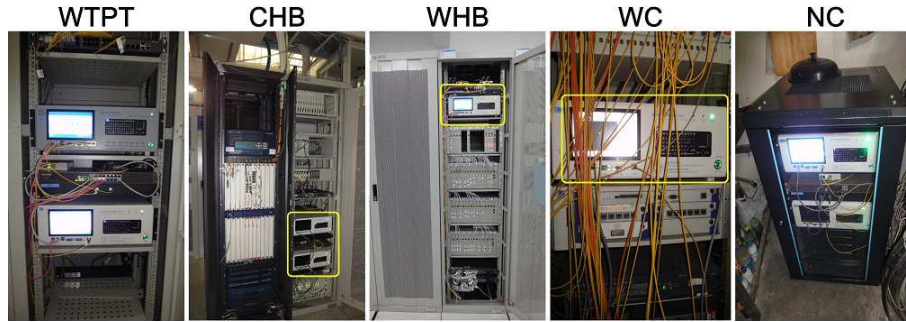


Fig. 8. Photographs of some nodes, including the surrounding environments and QKD devices.

Nodes WTPT, CHB, TR, and WHB were in the telecom rooms provided by China Mobile Ltd.. These telecom rooms have precision air conditioning systems, which control the temperature, humidity, and dust within tight tolerances. And, the telecom room has relatively strong physical security, anyone who wants to enter the room needs to be authenticated, and video cameras always monitor the room. These good environmental conditions were beneficial to long-term stable operation of QKD systems. However, the vibration and acoustic noise (e.g. nearby fans and humming equipment) in the telecom room are unneglectable and sustained, which requires the QKD devices able to resist a certain intensity of vibration.

Nodes WC and Lib were in the simple switching rooms of USTC. These simple rooms are relatively separate and only equipped with a household air conditioning for cooling. The temperature and humidity of these simple rooms are controlled within loose tolerances, and there is a lot of dust and also vibration from fans of nearby equipments.

Nodes KLQI and Qasky were in the office rooms, or normal laboratories rooms. These offices have a central air conditioning system to make people comfortable, so the temperature and humidity are $18\text{ }^{\circ}\text{C} \sim 28\text{ }^{\circ}\text{C}$ and $30\% \sim 60\%$ respectively when staff are in the office, but the central air conditioning system and lights are shut down when staff are off duty. There are twice temperature variation process on weekdays at least, especially in the winter and summer. In addition, vibration from staff activity should also be considered.

Nodes NC was in the makeshift kitchen of the doorkeepers, which was the harshest operation environment in the network. There are a gas cooker, a small exhaust fan, and other things to cook Chinese food. The kitchen become a hot, noisy, and smoky place when doorkeepers make the lunch and supper. Therefore the QKD-Transmitter T3 and QKD-Receiver R3 were put into a telecom cabinet to keep away from the lampblack. Since there is no air conditioning, the winter temperature falls to minus $5\text{ }^{\circ}\text{C}$, while the summer temperature gets up to $32\text{ }^{\circ}\text{C}$, and

even higher when cooking lunch in summer, which requires large operating temperature range for QKD devices, especially for the SPD part.

5.3. *The influence from weather and measures for QKD*

Weather is a crucial factor for the long-term operation of a wide area QKD network. During the operation term, weather would vary greatly. The influence from weather included on the QKD devices and the fiber channels. Changes of fiber channel properties would indirectly affect the stability and performance of QKD devices, and some measures were adopted to automatically compensate influence from the weather.

The variation of the weather would directly affect the operation status of QKD devices, especially for those in the nodes without air conditioning systems. Although several temperature control modules should be adopted to improve the stability of QKD devices, the ambient temperature and humidity are still important factors. In this network, the greatest challenge is to keep the working temperature of the SPD at $-50\text{ }^{\circ}\text{C}$. Most SPDs could work normally, only the SPD of QKD-Receiver R3 in NC node stopped working on the afternoon of June 8th, and resumed in the evening. Although the limited operating temperature of the SPD was about $35\text{ }^{\circ}\text{C}$, the ambient temperature and humidity, and also the cooking activity made the environment very tough for the cooling module belonged to the SPD part. In order to keep the working state of R3 in the whole summer, the working temperature of its SPD part was changed from $-50\text{ }^{\circ}\text{C}$ to $-40\text{ }^{\circ}\text{C}$ (the same as researchers did in the SwissQuantum QKD network [40]). After being reset the working temperature, the detection efficiency of the SPD was adjusted the same as before, but the dark count rate doubled.

The change of the weather would vary the birefringence, optical path length (or time delay), and loss of fiber channels, which are the main differences from the laboratory experiments. Moreover, these variations accumulate with distance. The operation stability of QKD devices would be greatly affected by variations of birefringence and optical path length of fiber channels. Instead of adding stabilization mechanism, we adopted two measures to automatically compensate these two types of variations of channels respectively. By using phase coding system based on FMI, QKD devices were insensitive to the polarization disturbance of channels [11]. The other measure was multiplexing quantum and sync signals in the same fiber with only 1.6 nm wavelength interval to compensate changes in optical path length, which led to drift of synchronization between the QKD-Transmitter and QKD-Receiver. Even with $50\text{ }^{\circ}\text{C}$ temperature change, the drift of synchronization in Hefei-Chaohu fiber channel was much less than 1 ps, which was negligible. The results from theoretical analysis and experiments show the effectiveness of these two measures. However, variations of loss of fiber channels are unavoidable, and their influences could not be compensated since intensity of each quantum signal from QKD-Transmitters is fixed.

5.4. *Other influence factors*

In addition to the weather, there were also some external factors influencing the performance of the long-term QKD network: (1) Fiber cable breaking by the road construction. One road near Node Qasky was under construction in the meantime. The fiber cable from Node WHB to Node Qasky was broken three times during the network operation phase, which made Node Qasky to be isolated from the whole network. (2) Power outage. All QKD devices in the wide area QKD network could operate from the single-phase AC power source. However, the stable power source in the telecom room is 48 V DC power. At the beginning, the lighting AC source (220V, 50Hz) in the wall was used in Node WTPT. Only ten days after running the whole QKD network, there was a power outage, which made the wide area network to be split into two independent metropolitan network. Considering the stability of the power source, one DC-AC

inverter was used to transfer the stable 48 V DC power to 220 V, 50 Hz AC power in Node WTPT. (3) Computer crash. (4) Halt of the controlling system.

5.5. Long-term performance of QKD links

After obtaining characteristics of the eight optical fiber links in the wide area network, we first built the whole QKD network in the laboratory. The test run lasted for one week, and then all devices were carried to the corresponding field Nodes. The whole wide area QKD network was completed on 20 December 2011. Starting from the next day and stopping on 19 July 2012, the field test of the whole wide area QKD network lasted more than 5000 hours, and the test of the QCN-USTC part stopped until last December.

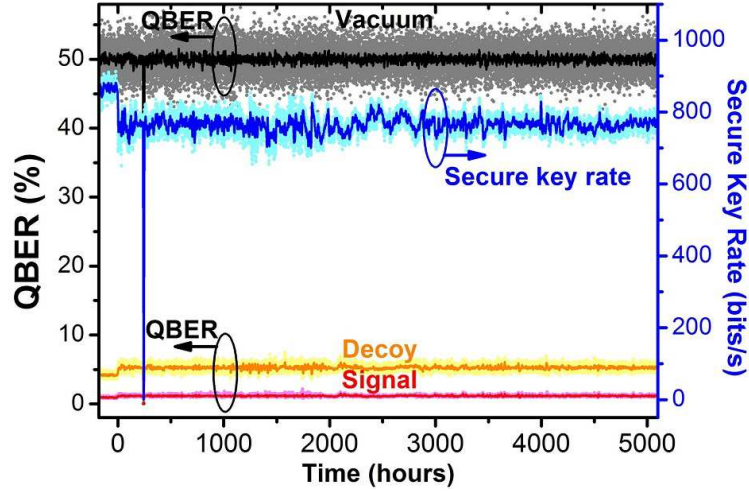


Fig. 9. QBER and secure key rate varied with time for the Hefei-Chaohu QKD link.

The QBERs of the signal, decoy, and vacuum states were recorded during the laboratory examination and the field test period (For the Hefei-Chaohu QKD link see Fig. 9, the magenta, yellow, and dark gray dots stand for the QBERs of the signal, decoy, and vacuum states, respectively.). And, the secure key rate was also recorded during the whole period (For the Hefei-Chaohu QKD link see Fig. 9, the cyan dot stands for the secure key rate). In Fig. 9, the laboratory examination stage of the whole QKD network lasted about one week, started from hour -168.6 and stopped at hour 0. The field test stage of the whole network started from hour 0 and stopped at hour 5093.9. And there was an interruption lasted for about 8 hours, because of the power outage in Node WTPT, during which time the QBERs and secure key rate reduced to zero.

There were obvious changes between the laboratory examination stage and the field test period for the Hefei-Chaohu QKD link, although the losses of the fiber channels in this two stage were almost the same. In the laboratory, the QBERs of the signal state and decoy state between T5 and R5 were respectively 0.94% and 4.18%, and the average secure key rate was 0.87 kbps. While, in the field circumstance, the QBERs of the signal state and decoy state increased up to 1.16% and 5.26%, and the secure key rate reduced to 0.77 kbps. These changes come from the background noise of the fiber channel and the surrounding environments of the QKD devices T5 and R5. The background noise was mainly the leaky photons from other parallel fibers in the same multi-core cable. The yield of the vacuum state was about 4×10^{-6} in the laboratory examination stage, but increased to 5×10^{-6} in the field test period. This presented background

noise cause about 0.1% increase of the QBER of the signal state. The QKD devices T5 and R5 were placed in the telecom rooms of China Mobile Ltd., where the vibration and acoustic noise were not ignorable. Even though the FMI was polarization independent and vibration isolation was considered when we designed QKD devices, the surrounding environments cause about 0.1% increase of the QBER of the signal state.

The fluctuations of QBERs and the secure key rate are observed in Fig. 9. We have also noticed that, the ranges of fluctuations during the field test period was obvious large than the ones during the laboratory examination stage. In the laboratory, these fluctuations mainly originated from the statistical fluctuation and detection probability fluctuation. But, when the QKD devices were tested in the field, the fluctuations of QBERs and key rates also come from the variations of fiber loss.

The secure key rates of each QKD links in the network are shown in table 3. The performance of the wide area QKD network was limited by the intercity QKD link, which has lower secure key rate due to longer channel. For example, in Hefei metropolitan area QKD network, the NC-WC QKD link has 29.54 kbps secure key rate in state (III), while the secure key rate of Hefei-Chaohu QKD link reduces to 0.77 kbps. We expect to increase the performance (especially the secure key rate) of the QKD network in near future with improvements of hardware and software.

Table 3. Secure key rates of each links in the Hefei-Chaohu-Wuhu wide area QKD network.

	QKD link	QKD devices	Secure key rate(kbps)
Hefei metro network	KLQI→NC	T1→R3	7.27
	NC→WC	T3→R4	8.33
	WC→KLQI	T4→R1	6.86
	WTPT→NC	T2→R3	1.05
	NC→WC	T3→R4	8.33
	WC→WTPT	T4→R2	1.02
	KLQI→WTPT	T1→R2	2.67
	WTPT→KLQI	T2→R1	2.42
	NC→WC	T3→R4	13.39
	WC→NC	T4→R3	16.15
HCW-intercity link	Hefei→Chaohu	T5→R5	0.77
	Chaohu→Wuhu	T6→R6	0.80
Wuhu metro network	WHB→TR	T7→R7	6.07
	Qasky→TR	T8→R7	0.96

6. Performance of the encryption applications

Just as Stucki et al. said in reference [40], the test of the performance of the encryption application was not the primary goal of the field QKD network. However, the encryption applications are the motive force of development of quantum cryptography, and the integrated technology of QKD device (the quick and secure key refresh server) and encryptor should be developed. Take the Thales Mistral products for example, the encryptors could not deal with a key renewal period lower than 3 seconds [13]. Here, two typical applications of the quantum keys from our QKD devices were developed and tested on this wide area QKD network.

The first one was the one-time pad encryption medium for the public switch telephone network (PSTN). This encryption medium was added between PSTN and traditional terminals, such as the conventional telephone and fax machine. It's very convenient for subscribers who

do not need to change their original telephone and fax machines, even their operative habits, the encryption medium was completely transparent in normal circumstance without security requirements. The keys used for one-time pad encrypted voice data came from the QKD server in two ways, one was real-time transport, which was tested on the QCN-USTC, the other one was downloading and storing in a secure digital (SD) card, which was tested on the link between KLQI in Hefei and Qasky in Wuhu.

The second one was the symmetric encryption virtual private network (VPN) security gateway for public networks. This VPN gateway integrated the QKD technology and the existing classical IPsec protocol together, and was completely compatible with conventional hardware and software in the Internet. The 256-bit advanced encryption standard (AES) encryption was employed to guarantee the security. The secret seed keys for AES derived from and refreshed by the QKD server. In this wide area QKD network, the VPN security gate was tested among subscribers in Hefei and subscribers in Wuhu. The seed key refresh rate for the VPN gateway was limited by the intercity QKD link, which could only support the rate about 3 256-bit keys per second. Network applications like the file transfer, internet telephone, video chat, and multimedia-based tripartite conference were tested.

7. Conclusions

We have shown that the dynamic QKD network can be field installed and run steadily in wide area for long term. Through sharing communication infrastructures from China Mobile Ltd., the Hefei-Chaohu-Wuhu wide area QKD network provided a secure and stable key distribution platform for subscribers in two cities (Hefei and Wuhu) that are over 150 kilometers apart. Four QKD nodes in Hefei city were combined together by two dynamic routing components to form a typical full-mesh metropolitan core network, in which there were up to eight different direct QKD links only by multiplexing four fiber channels. In Wuhu city, the point-to-multipoint metropolitan network was composed by three QKD nodes and one 1×2 switch to simulate a quantum access network. These two typical QKD networks and HCW-intercity QKD link ran for more than 5000 hours, and even the QCN-USTC part for about two years, the stable operation of the Hefei-Chaohu-Wuhu wide area QKD network has proven the reliability and robustness to the field environment of QKD networks. We have successfully field tested the wide area QKD network prototype, and also realized the effective integration between P2P QKD techniques and networking schemes, owing to the following developments: (1) Standardized design of QKD devices to facilitate establishment and maintenance of QKD networks; (2) Resolution of symmetry problem of QKD devices to clear obstacles in the way towards cost-effective technology for QKD (especially for one-way phase coding system), and also convenient to dynamically add new QKD nodes; (3) Seamless switching in dynamic QKD network based on stable QKD systems and networking techniques. In short, results from Hefei-Chaohu-Wuhu wide area QKD network demonstrate that QKD technology actually has the potential to be widely deployed.

Acknowledgments

We thank China Mobile Ltd. and Network Information Center of University of Science and Technology of China for providing communication infrastructures. This work was supported by the National Natural Science Foundation of China (Grant No.61101137, No.61201239, No.61205118, and No.11304397), National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200), and National High Technology Research and Development Program of China (863 program) (Grant No. 2009AA01A349).