Research Article | Vol. 26, No. 5 | 5 Mar 2018 | OPTICS EXPRESS 6010

Optics EXPRESS

Integrating quantum key distribution with classical communications in backbone fiber network

YINGQIU MAO,[1,2] BI-XIAO WANG,[1,2] CHUNXU ZHAO,[3] GUANGQUAN WANG,[3] RUICHUN WANG,[4] HONGHAI WANG,[4] FEI ZHOU,[5] JIMIN NIE,[6] QING CHEN,[7] YONG ZHAO,[7] QIANG ZHANG,[1,2] JUN ZHANG,[1,2] TENG-YUN CHEN,[1,2,*] AND JIAN-WEI PAN[1,2]

[1] *Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*
[2] *CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*
[3] *Network Technology Research Institute, China Unicom Network Communications Corporation Limited, Beijing 100048, China*
[4] *State Key Laboratory of Optical Fiber and Cable Manufacture Technology, Yangtze Optical Fibre and Cable Joint Stock Limited Company, Wuhan, Hubei 430073, China*
[5] *Jinan Institute of Quantum Technology, Shandong Academy of Information Technology, Jinan, Shandong 250101, China*
[6] *CAS Quantum Network Corporation Limited, Shanghai 201315, China*
[7] *QuantumCTek Corporation Limited, Hefei, Anhui 230088, China*
[*] *tychen@ustc.edu.cn*

Abstract: Quantum key distribution (QKD) provides information-theoretic security based on the laws of quantum mechanics. The desire to reduce costs and increase robustness in real-world applications has motivated the study of coexistence between QKD and intense classical data traffic in a single fiber. Previous works on coexistence in metropolitan areas have used wavelength-division multiplexing, however, coexistence in backbone fiber networks remains a great experimental challenge, as Tbps data of up to 20 dBm optical power is transferred, and much more noise is generated for QKD. Here we present for the first time, to the best of our knowledge, the integration of QKD with a commercial backbone network of 3.6 Tbps classical data at 21 dBm launch power over 66 km fiber. With 20 GHz pass-band filtering and large effective core area fibers, real-time secure key rates can reach 4.5 kbps and 5.1 kbps for co-propagation and counter-propagation at the maximum launch power, respectively. This demonstrates feasibility and represents an important step towards building a quantum network that coexists with the current backbone fiber infrastructure of classical communications.

© 2018 Optical Society of America under the terms of the OSA Open Access Publishing Agreement

OCIS codes: (270.5565) Quantum communications; (270.5568) Quantum cryptography; (270.5585) Quantum information and processing.

References and links

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145 (2002).
2. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, 1984), pp. 175–179.
3. H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Phys. Rev. Lett. **117**(19), 190501 (2016).
4. J. F. Dynes, W. W. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards, and A. J. Shields, "Ultra-high bandwidth quantum secured data transmission," Sci. Rep **6**, 35149 (2016).
5. R. J. Hughes, G. L. Morgan, and C. G. Peterson, "Quantum key distribution over a 48 km optical fibre network," J. Mod. Opt. **47**(2-3), 533–547 (2000).

#321313 https://doi.org/10.1364/OE.26.006010
Journal © 2018 Received 1 Feb 2018; accepted 11 Feb 2018; published 27 Feb 2018

Optics EXPRESS

6. C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," https://arXiv preprint quant-ph/0503058 (2005).
7. 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," Opt. Express **17**(8), 6540–6549 (2009).
8. 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. Lorünser, 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**(7), 075001 (2009).
9. 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**(11), 10387–10409 (2011).
10. 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. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," New J. Phys **13**(12), 123001 (2011).
11. J. Qiu, "Quantum communications leap out of the lab," Nature **508**(7497), 441–442 (2014).
12. S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express **22**(18), 21739–21756 (2014).
13. Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," Phys. Rev. X **6**(1), 011024 (2016).
14. R.-J. Essiambre, G. Kramer, P. J. Winzer, G. J. Foschini, and B. Goebel, "Capacity limits of optical fiber networks," J. Lightwave Technol **28**(4), 662–701 (2010).
15. P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," Electron. Lett **33**(3), 188–190 (1997).
16. 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**(10), 105001 (2009).
17. I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10 Gb/s WDM-PON," Opt. Express **18**(9), 9600–9612 (2010).
18. P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," New J. Phys **12**(6), 063027 (2010).
19. K. Patel, J. Dynes, I. Choi, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," Phys. Rev. X **2**(4), 041010 (2012).
20. 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**(5), 051123 (2014).
21. L.-J. Wang, L.-K. Chen, L. Ju, M.-L. Xu, Y. Zhao, K. Chen, Z.-B. Chen, T.-Y. Chen, and J.-W. Pan, "Experimental multiplexing of quantum key distribution with classical optical communication," Appl. Phys. Lett. **106**(8), 081108 (2015).
22. R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," New J. Phys **17**(4), 043027 (2015).
23. D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, "Continuous-variable quantum key distribution with 1 Mbps secure key rate," Opt. Express **23**(13), 17511–17519 (2015).
24. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, S. W.-B. Tam, Z. Yuan, and A. J. Shields, "Quantum secured gigabit optical access networks," Sci. Rep **5**, 18121 (2015).
25. M. S. Goodman, P. Toliver, R. J. Runser, T. E. Chapuran, J. Jackel, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, S. McNown, N. Nweke, J. T. Blake, L. Mercer, and H. Dardy, "Quantum cryptography for optical networks: a systems perspective," in *The 16th Annual Meeting of the IEEE Lasers and Electro-Optics Society, 2003. LEOS 2003* (IEEE, 2003), pp. 1040–1041 vol. 2.
26. D. Subacius, A. Zavriyev, and A. Trifonov, "Backscattering limitation for fiber-optic quantum key distribution systems," Appl. Phys. Lett. **86**(1), 011103 (2005).
27. B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," New J. Phys **12**(10), 103042 (2010).

Optics EXPRESS

28. S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, and G. Franzl, "Perspectives and limitations of QKD integration in metropolitan area networks," Opt. Express **23**(8), 10359–10373 (2015).
29. B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," Optica **4**(1), 163–167 (2017).
30. L.-J. Wang, K.-H. Zou, W. Sun, Y. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen, and J.-W. Pan, "Long-distance copropagation of quantum key distribution and terabit classical optical data channels," Phys. Rev. A **95**(1), 012301 (2017).
31. I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert, H. Griesser, M. Eiselt, C. Chunnilall, G. Lepert, A. Sinclair, J.-P. Elbers, A. Lord, and A. Shields, "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," Opt. Express **22**(19), 23121–23128 (2014).
32. X.-B. Wang, "Decoy-state quantum key distribution with large random errors of light intensity," Phys. Rev. A **75**(5), 052301 (2007).
33. X.-L. Liang, J.-H. Liu, Q. Wang, D.-B. Du, J. Ma, G. Jin, Z.-B. Chen, J. Zhang, and J.-W. Pan, "Fully integrated InGaAs/InP single-photon detector module with gigahertz sine wave gating," Rev. Sci. Instrum **83**(8), 083111 (2012).
34. J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, "Advances in InGaAs/InP single-photon detector systems for quantum communication," arXiv preprint arXiv:1501.06261 (2015).
35. T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, 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," Opt. Express **18**(26), 27217–27225 (2010).
36. H. Krawczyk, "LFSR-based hashing and authentication," in *Advances in Cryptology-CRYPTO'94* (Springer, 1994), pp. 129–139.
37. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**(23), 230503 (2005).
38. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**(23), 230504 (2005).
39. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**(1), 012326 (2005).
40. Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, and H.-W. Li, "Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources," Phys. Rev. A **94**(3), 032335 (2016).
41. G. P. Agrawal, *Nonlinear Fiber Optics* (Academic Press, 2007).
42. X. Yang, H. Li, W. Zhang, L. You, L. Zhang, X. Liu, Z. Wang, W. Peng, X. Xie, and M. Jiang, "Superconducting nanowire single photon detector with on-chip bandpass filter," Opt. Express **22**(13), 16267–16272 (2014).
43. P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," Nat. Commun **8**, 13984 (2017).

1. Introduction

Quantum key distribution (QKD) [1], based on the laws of quantum physics, provides proven unconditional security for data communication between remote users. Since its introduction in 1984 [2], experimental efforts have been made to achieve long distance and high key rate in optical fibers, such as the recent record demonstration of 404 km [3] and Mbits per second (Mbps) secure key generation [4]. So far, QKD has become one of the most mature and advanced quantum information technologies ready for use. To demonstrate its reliability and robustness over long periods of time, field experiments of QKD based secure communications for metropolitan networks and intercity links have been performed [5–13].

However, in order to protect ultra-weak QKD signals, all of the above achievements were performed in dark fibers with a wavelength set around 1550 nm. This implies dedicated fiber installations for quantum communication networks, which bears cost penalties in fiber leasing and maintenance, as well as limitations on the network scale. In fact, to reduce cost and increase fiber transmission efficiency, classical communications (CC) have already exploited methods such as time-division multiplexing (TDM) and wavelength-division multiplexing (WDM) to achieve data throughput of up to Terabits per second (Tbps) and ultra-long transmission distances [14]. Therefore, it is highly desired to integrate QKD with CC in existing fiber infrastructures and to expand the scalability of QKD networks.

The scheme of simultaneously transmitting QKD with conventional data was first introduced by Townsend in 1997 [15]. Using coarse wavelength-division multiplexing (CWDM), a QKD

Optics EXPRESS

channel at 1300 nm was multiplexed with a conventional 1.2 Gbps data channel at 1550 nm over 28 km installed fiber. Although no privacy amplification or yield of secret key was reported [15], it provided a blueprint for the coexistence works that followed. A series of QKD experiments integrating with various classical channels have been demonstrated [4, 16–24], and perspectives on the obstacles and approaches to share existing fiber infrastructures among quantum and classical channels have been discussed [25–28].

Currently, by using spectral and temporal controls, state-of-the-art developments have been made to realize co-propagation of QKD with one 100 Gbps dense wavelength-division multiplexing (DWDM) data channel in 150 km ultra-low loss fiber at −5 dBm launch power [29]. By setting QKD wavelength to 1310 nm and inserting DWDM filters with bandwidth of 100 GHz before QKD receivers to improve out-of-band noise rejection, co-propagation of QKD with classical traffic was recently demonstrated over 80 km fiber spools [30]. In that experiment, by assembling the CC system with high-performance affiliated equipment in the laboratory, data transmission at Tbps level was achieved at 11 dBm launch power. A field trial of simultaneous QKD transmission and four 10 Gbps encrypted data channels was implemented over 26 km installed fiber at −10 dBm launch power [31].

However, the integration of QKD with existing backbone network is different from the previous implementations. On the one hand, backbone networks use complex classical communication systems with extremely high-level stability, reliability, and redundancy. Therefore, in realistic backbone networks, launch power for Tbps level classical data reaches ~ 20 dBm, which results in significantly stronger Raman scattering to QKD than in Ref. [30]. Using the previous 100 GHz pass-band filtering, key generation will be difficult, and coexistence may not be achieved in realistic backbone networks. On the other hand, such field integration may suffer from environmental factors and social activities that are not encountered in laboratory demonstrations. To close the gap between laboratory demonstrations and practical applications, there are many great technical challenges to overcome for the integration of QKD with backbone fiber infrastructures.

In this work, we present for the first time, to the best of our knowledge, the coexistence of QKD and commercial backbone network of 3.6 Tbps classical data over 66 km fiber at the maximum launch power, i.e., 21 dBm. With a 20 GHz pass-band filter, we achieve co-propagation of QKD and 21 dBm classical data over standard single-mode fiber with 3.0 kbps secure key rate and 2.5% quantum bit error rate (QBER). Using low-loss fiber with large effective core area, secure key rates can be further increased to 4.5 kbps and 5.1 kbps for co-propagation and counter-propagation, respectively. Contributions of filter bandwidth, fiber loss, and fiber effective core area to the quantum signal-to-noise ratio (QSNR) and secure key rate are modeled and analyzed. The QKD stability and the coexistence effects on CC are also investigated.

2. Experiment

The field experiment is performed over a backbone loop network with a total installed fiber distance of 800 km and eight nodes spanning across Shandong province, China, deployed by China United Telecom (China Unicom), as shown in Fig. 1a. Considering fiber loss between the nodes and QKD system performance, we assign Alice to node Zhucheng (119°24′43″ N 36°3′00″ E) and Bob to node Huangshan (119°59′50″ N, 36°2′4″ E), which has in-between 66 km installed fiber deployed along highways, bridges, and tunnels. Meanwhile, the transmitter and receiver of CC are placed in the Jinan laboratory for performance analysis, while optical amplifiers (OA) are located in other stations, controlled by internet monitors for optical gain adjustments. We verify the performances of both QKD system and CC system on three types of fibers with different effective core areas (whereas the fibers connecting other nodes are all G654 fibers with an effective core area of 110 μm^2), whose specifications are listed in Table 1, with fiber links G652-1, G654-110-1, G654-130-1 for co-propagation and fiber links G652-2, G654-110-2, G654-130-2 for counter-propagation. All fibers on the backbone network follow

Optics EXPRESS

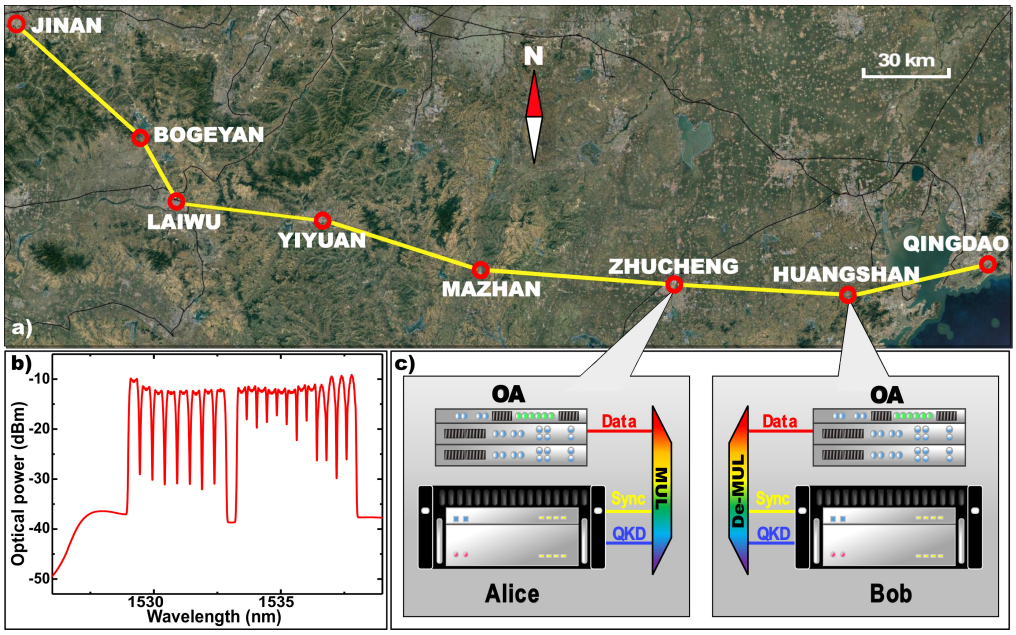

Fig. 1. a) Field configurations of the experiment. The single yellow line represents the deployed two fiber links between communication stations. b) Spectrum of the CC measured at Zhucheng. The 200 Gbps channels are shown as the root-raised cosine waveforms, while the 100 Gbps channels are shown as the Gaussian waveforms. c) Coexistence schematics of the experiment. The wavelengths of QKD, sync, and data signals are 1310 nm, 1490 nm, 1528 ~ 1538 nm, respectively.

the International Telecommunication Union standards. Since these G654 fibers possess larger effective core areas than the standard single-mode fiber, it can be used to lower optical effects at the fundamental light-matter interaction level in coexistence experiments and thus to enhance QKD performances.

Table 1. Field fibers specifications

Fiber type	Att (dB/km)		Total loss (dB)		Aeff
	1550nm	1310nm	1550nm	1310nm	μm^2
G652-1	0.197	0.337	13.01	22.21	80
G652-2	0.196	0.338	12.94	22.29	80
G654-110-1	0.184	0.300	12.13	19.83	110
G654-110-2	0.174	0.288	11.51	19.03	110
G654-130-1	0.210	0.347	13.84	22.88	130
G654-130-2	0.208	0.348	13.73	22.95	130

For classical data traffic, we adopt a commercial hybrid system from China Unicom (Alcatel-Lucent 1830PSS-64) with aggregate transmission rate of 3.6 Tbps, which is achieved by four line cards with 50 GHz bandwidth and four line cards with 62.5 GHz bandwidth. In each line card, the super-channel scheme is used, consisting of two sub-carriers that carry 200 Gbps polarization division multiplexing with 8-quadrature amplitude modulation format. In addition, four 100 Gbps line cards with quadrature phase shift keying modulation format are included in the CC system.

Optics EXPRESS

The CC spectrum is shown in Fig. 1b, including 20 channels covering about 1528 ~ 1538 nm. The total launch power can be tuned from 8 to 21 dBm, with optimal launch power is ~ 18 dBm. Utilizing pseudo-random binary sequence generated by a test instrument to serve as the classical data throughout the experiment and varying the launch power, the parameters of Q-factor and OSNR are measured. When the launch power is reduced down to a low level, e.g., 11 dBm as in [30], the bit error rate (BER) is close to the bound for forward error correction, which results in the failure of the data transmission of CC.

For QKD, we develop a polarization encoding, decoy-state BB84 protocol-based system. Signal pulses at 1310 nm are prepared at Alice's site with a repetition rate of 625 MHz. The pulse train is internally modulated to 70 ps width and further shaped to 1310 ± 0.036 nm at full width at half maximum (FWHM) with a 10 GHz fiber Bragg grating (FBG), which is used to compensate dispersion effects and to guarantee pulse registration within the detector effective gating width. The mean photon numbers of the signal state μ, decoy state ν, and vacuum state ω are 0.6, 0.2, 0 [32], respectively, with an emission ratio of $P_\mu : P_\nu : P_\omega = 6 : 1 : 1$, which are controlled by a physical random number generator implemented in a field programmable gate array (FPGA). Using two polarization beam splitters and a polarization controller, four nonorthogonal states are generated with output powers adjusted to single-photon level using a variable optical attenuator. The received photons at Bob's site are recorded by four InGaAs/InP single-photon detectors (SPDs) [33, 34], which operated at 1.25 GHz gating frequency with a detection efficiency of 11% and a dark count rate per gate of 3×10^{-7} in average. The detector effective gating width is set to ~180 ps to provide temporal filtering while maintaining maximum detection efficiency, and the detector dead time (t_{dead}) is 1 μs. Automatic polarization feedback system is implemented using two electric polarization controllers at Bob's site to adjust the extinction ratio between the orthogonal states [35]. Visibility reaches ~ 21.5 dB after feedback control, corresponding to a 0.7% optical misalignment error rate (e_d). Meanwhile, synchronized clock signal between Alice and Bob (Sync) at 1490 nm propagates along QKD signals with a repetition rate of 100 kHz and a received optical power of −53 dBm.

After the pulses are registered at Bob's detectors, a series of post-processing for real-time secure key extraction is performed. First, the public discussion channel between Alice and Bob is established through pre-stored QKD keys, which are periodically replaced with fresh keys. The keys are fed into Toeplitz Hash algorithms using linear feedback shift register to implement authentication [36]. Next, key sifting and basis sifting are executed, followed by error correction (EC) using Winnow codes with a correction efficiency of 1.2~1.5, and error verification (EV) using CRC-64 algorithm. Afterwards, privacy amplification (PA) is performed to eliminate information leakage to Eve during EC and EV. An estimated final key rate is calculated using standard decoy-state method [37–40] to determine a PA factor, defined as the ratio of the estimated final key rate to the corrected key rate after EV. With the PA factor, an exact Toeplitz matrix is constructed to extract final secure keys from the corrected keys. Considering the real-time key extraction period, the block size for parameter estimation is set to 500 kbits to guarantee the freshness of final keys. Also, considering statistical fluctuations, 7 standard deviations are used to guarantee the security of final keys. Further, by evaluating QBER using the decoy-state method, a strict upper bound is set to 4% for redundancy control, which corresponds to a QSNR lower bound of ~11 dB, to guarantee stable key generation.

To achieve coexistence, WDM filters are applied, forming a multiplexing module (MUL) at Alice and a de-multiplexing module (De-MUL) at Bob, see Fig. 1c. The insertion losses at 1550 nm and 1310 nm are respectively 0.86 dB and 0.30 dB for MUL, while 0.87 dB and 2.50 dB for De-MUL. The isolation of 1310 nm from 1550 nm at MUL is 50 dB, while that of 1550 nm from 1310 nm at De-MUL is 120 dB. Combining with a circulator, a temperature-compensated FBG with a reflection band of 1310 ± 0.087 nm at FWHM forms a 20 GHz filter in De-MUL. The crosstalk between QKD and CC channels is measured, with a noise level of ~ 60 counts per

Optics EXPRESS

second (cps), which is much lower than the dark count rates of the SPDs and thus negligible in the experiment.

When QKD is integrated with CC, the strong CC signals may cause severe impairments on the weak QKD signals through fundamental light-matter interactions. Possible sources of noise in the QKD wavelength from CC channels include four-wave mixing, Brillouin scattering, and Raman scattering. By allocating the QKD wavelength to 1310 nm, a ~ 200 nm gap is set between the QKD and CC signals, so the noise photons caused by four-wave mixing in the QKD channel is negligible. In addition, because of its low bandwidth (~ 10 GHz), Brillouin scattering from the CC channels do not affect QKD. In contrast, Raman scattering lead to large spectral shifts from the CC channel wavelengths, with an intensity maximum at a shift of ~ 13 THz and maximum offset parameter to more than 50 THz [28]. Stimulated Raman scattering has a threshold of ~ 600 mW for 20 km single-mode fiber at 50 μm^2 effective core area [41], so considering the fiber length and CC launch powers of our experiment, this effect from CC channels in the QKD channel is negligible. Therefore, in this experiment, the photons generated by spontaneous Raman scattering (SRS) from the CC channels is the only optical scattering noise in the QKD channel. Furthermore, with the 20 GHz filter, SRS photons can be further reduced and hence the QSNR is enhanced, which suggests the coexistence possibility with CC at the maximum launch power, despite the fact that the 20 GHz filter has an insertion loss of 1.9 dB compared to that of 0.5 dB for 100 GHz filter in Ref. [30].

3. Results and discussion

By adjusting the launch power of CC from 8 to 21 dBm, we measure the secure key rate and QBER of QKD, as shown in Figs. 2a and b. For G652 fiber, 3.0 kbps secure key rate is achieved

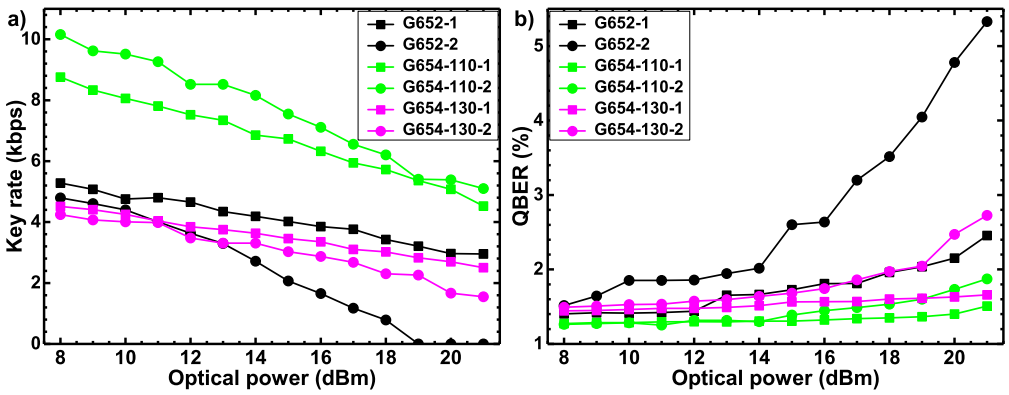

Fig. 2. Secure key rate (a) and QBER (b) of QKD as a function of CC optical power. Solid squares: co-propagation; solid circles: counter-propagation.

at the maximum launch power for co-propagation. For counter-propagation, secure key rates significantly drop given the launch power higher than 18 dBm. This is due to the fact that much more SRS photons are created than in the case of co-propagation [16, 17, 26], corresponding to a lower QSNR, given the same length of fiber and launch power. At 19 dBm, QBER reaches 4.0% and no secure keys are generated, as shown in Figs. 2a and b. These results indicate the possibility of coexistence between QKD and classical backbone network in standard single-mode fiber, both for co-propagation at the maximum launch power and for counter-propagation by slightly decreasing the launch power.

The best QKD performance is achieved in G654-110 fiber. At the maximum launch power, key rates reach 4.5 kbps and 5.1 kbps for co-propagation and counter-propagation, respectively.

Optics EXPRESS

The higher key rate in counter-propagation is due to the relatively lower fiber attenuation of G654-110-2 fiber, see Table 1. For G654-130 fiber, the created SRS photons are much less than that in G652 fiber, as shown in Fig. 3. However, due to the characteristic of higher fiber attenuation, the key rate for co-propagation is lower than G652 fiber. For counter-propagation, given a launch power larger than 13 dBm, contributions due to SRS in G652 fiber is much more significant than fiber attenuations, which results in a lower QSNR than G654-130 fiber.

Further, we model the key rates using different fibers. Considering fiber attenuation and the SRS of different effective core areas, the QSNR is defined as

$$\mathrm{QSNR} = 10log_{10}(\frac{N_{\mathrm{actual}}(1 - P_{\mathrm{after}} - e_d)}{N_{\mathrm{SRS}} + N_{\mathrm{dark}} + N_{\mathrm{after}}}),$$

where N_{actual} is the actual QKD signal count rate, N_{SRS} is the SRS photon count rate, N_{dark} is the detector dark count rate, P_{after} is the detector afterpulse probability ($\sim 0.5\%$ in our experiment), and N_{after} is the afterpulse count rate, calculated by $N_{\mathrm{after}} = N_{\mathrm{actual}} \cdot P_{\mathrm{after}}$. Due to the detector dead time, $N_{\mathrm{actual}} = N_\mu/(1+\frac{N_\mu \cdot t_{\mathrm{dead}}}{4})$, where N_μ is the QKD signal count rate that would be obtained if dead time was negligible. N_μ and N_{SRS} are calculated, while N_{actual}, N_{dark}, and t_{dead} are measured.

Table 2. Simulation results of QSNR and secure key rate in different cases. The attenuation coefficients of standard fiber and low-loss fiber are 0.337 dB/km at 1310 nm and 0.197 dB/km at 1550 nm, and 0.288 dB/km at 1310 nm, 0.174 dB/km at 1550 nm, respectively.

Aeff (μm^2)	Co-propagation		Counter-propagation	
	QSNR (dB)	Key rate (kbps)	QSNR (dB)	Key rate (kbps)
20 GHz filtering, low-loss fiber				
80	50.5	5.5	18.3	3.2
110	65.8	5.9	29.5	4.9
130	71.1	6.0	34.5	5.2
20 GHz filtering, standard fiber				
80	36	2.2	10.0	–
110	45.8	2.3	16.6	1.2
130	49.2	2.4	19.8	1.5
100 GHz filtering, low-loss fiber				
80	14.0	1.8	2.8	–
110	23.5	3.6	5.8	–
130	28.1	4.1	7.5	–
100 GHz filtering, standard fiber				
80	10.4	–	1.0	–
110	17.5	1.1	2.7	–
130	20.8	1.4	3.6	–

We then calculate N_{SRS}, following the methods in Refs. [16, 17] to obtain the SRS coefficient ($\beta_{20\,\mathrm{GHz}}$) of the three fibers. By averaging the results in Fig. 3 with different launch powers, for both co-propagation and counter-propagation, we calculate the values of $\beta_{20\,\mathrm{GHz}}$ as 18, 10, and 8 $^{\mathrm{cps}}/_{\mathrm{dBm\cdot km}}$ for G652, G654-110, and G654-130, respectively.

Following the above model, we evaluate the contributions of the major factors, i.e., filter bandwidth, fiber attenuation, and fiber effective core area, to the key rate of QKD coexisting with 21 dBm launch power over 66 km transmission distance. The simulated results are shown in Table 2, from which one can find out three facts. First, narrow pass-band filtering in such coexistence experiment is necessary. As shown in Table 2, using 100 GHz filtering, the QSNR values for counter-propagation in three fibers are below 8 dB, without generating secure keys. In particular, no keys are generated for both co-propagation and counter-propagation in standard fiber with 100

Optics EXPRESS

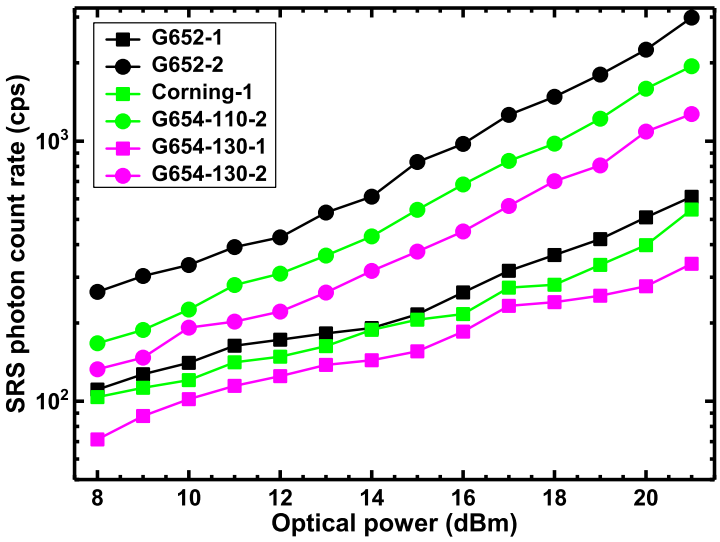

Fig. 3. Photon count rate generated by SRS. By sending classical signals through the 66 km field fiber along either the same direction of QKD signals (co-propagation, solid squares) or the opposite direction (counter-propagation, solid circles), photons are recorded by the SPDs. During this process, no QKD signals are transmitted. At each point, four SPD count rates are averaged. For co-propagation and counter-propagation, G654-130 fiber exhibits the lowest SRS photon count rates, with ~ 60% reduction compared with the G652 fiber.

GHz filtering. This means QKD cannot be integrated with backbone network using the same coexistence scheme of Ref. [30]. Second, using low-loss fiber, the QSNR is enhanced by 15.4 dB in average, and the key rate can be increased twice at least. Third, since large effective core area reduces the optical power density of the CC, the QSNR can be improved, which brings moderate increase in key rate. By combining 20 GHz filtering, low-loss fiber with 130 μm^2 effective core area, the highest secure key rates of QKD for co-propagation and counter-propagation may reach 6.0 kbps and 5.2 kbps, respectively.

In the experiment, we have demonstrated integrating QKD with 3.6 Tbps classical data over 66 km installed fiber. Further results for longer transmission distances using G654-110-2 fiber at the maximum launch power are simulated, as shown in Fig. 4. At 70 km and 80 km, secure key rates are respectively 4.4 kbps and 1.9 kbps for co-propagation , and 4.0 kbps and 1.5 kbps for counter-propagation. Even at 90 km, secure key rate may still reach 0.7 kbps for co-propagation. This suggests that even integrating with CC at a typical span distance of 80 to 100 km secure key rate of QKD is still sufficient for one-time pad voice and text encryptions. Using superconducting nanowire single-photon detectors (SNSPDs) instead of InGaAs/InP SPDs used in the experiment, the secure key rate can be substantially increased. We perform the theoretical calculations of key rate for co-propagation and counter-propagation at 21 dBm launch power in G654-110-2 fiber, using the calibrated parameters of the SNSPDs in our laboratory [42], i.e., 45% detection efficiency at 1310 nm and 30 cps dark count rate. The key rate is calculated following the decoy-state approach in Ref. [39]. As shown in Fig. 4, when the SNSPDs are used, the key rates for co-propagation and counter-propagation can be significantly increased to 32.7 kbps and 32.3 kbps at 66 km, respectively, while the maximum coexistence distances reach 145 km and 130 km for co-propagation and counter-propagation, respectively.

We further investigate the stability of QKD coexisting with CC systems. Due to the limited usage time in the backbone communication stations, we perform co-propagation measurement in three fibers for 3 hours each, with ~ 18 dBm launch power. The average key rates are 6.2

Optics EXPRESS

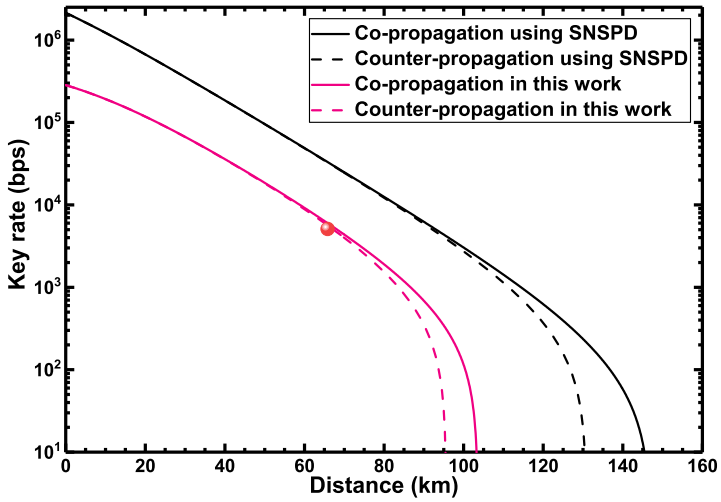

Fig. 4. Calculated secure key rates of QKD as a function of distance for co-propagation (solid lines) and counter-propagation (dashed lines) with 21 dBm launch power in G654-110-2 fiber. The red lines represent the results with the QKD system in the experiment, while the black lines represent the results using SNSPDs instead of InGaAs/InP SPDs for the QKD system. The solid red dot represents the measured result in the experiment.

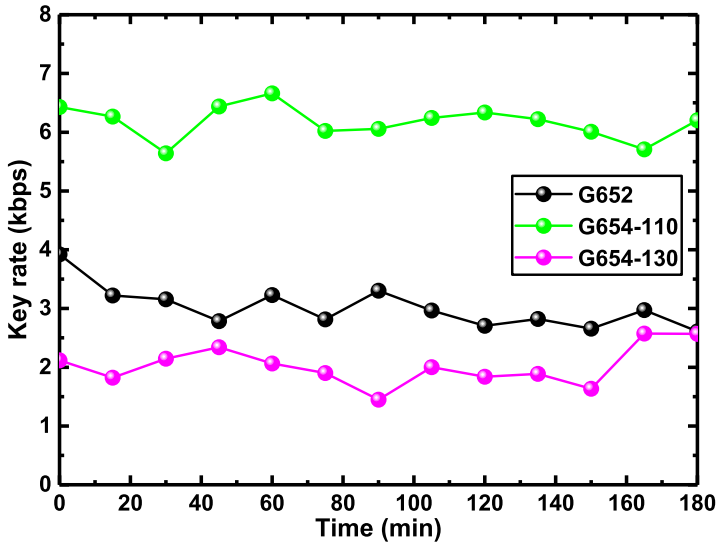

Fig. 5. The stability test of secure key rate in three fibers.

kbps, 3.0 kbps, and 2.0 kbps for G654-110, G652, and G654-130 fibers, respectively, as shown in Fig. 5. Despite the effects from social activities such as traffic, electricity, and constructions, the stability test results indicate that our QKD systems can be reliably integrated with the CC systems of backbone networks.

Finally, we measure the CC performance changes in the presence of QKD. The measured results in G654-110 fiber are plotted in Figs. 6a and b, which show that the inclusion of QKD brings negligible variations on OSNR of CC system. Nevertheless, due to insertion losses of WDM modules, CC launch power is lowered and the optical effects between adjacent CC channels

Optics EXPRESS

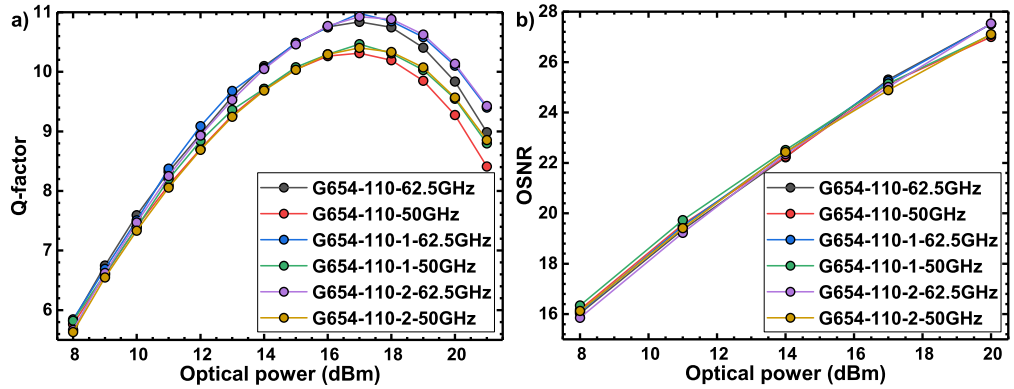

Fig. 6. Q-factor (a) and OSNR (b) of CC system as the function of optical power in G654-110 fiber by applying 62.5 GHz and 50 GHz bandwidth carriers, respectively. G654-110: no co-existence; G654-110-1: co-propagation; G654-110-2: counter-propagation.

during data transmission are reduced, which induces a slight increase of Q-factor, particularly with launch powers higher than 16 dBm, as shown in Fig. 6a.

4. Conclusion

In summary, we have achieved for the first time, to the best of our knowledge, the coexistence of QKD with a commercial backbone network of 3.6 Tbps classical data at the maximum launch power over 66 km fiber. The key factors affecting the coexistence performance such as filter bandwidth, fiber attenuation, and fiber effective core area are modeled and analyzed. Our work validates the feasibility to build a quantum network coexisting with current backbone fiber infrastructures of classical communications. Utilizing superconducting nanowire single-photon detectors and increasing the repetition rate of the QKD system, the secure key rate and coexistence distance can be further improved. Meanwhile, in the presence of untrusted network nodes and detection attacks, measurement-device-independent QKD [13] provides an effective approach and its coexistence with CC deserves future investigations. Using silicon photonics technologies, low-cost, chip-based QKD devices [43] may be fully integrated inside CC modules, offering wide accessibility and large-scale application.

In this work, the effects of transient problems caused by the dropping or adding data channels are not included, and the spectral bandwidth of the classical channels does not cover all the C+L-bands. Such interesting topics deserve future investigations.

Funding

National Key R&D Program of China (2017YFA0303900, 2017YFA0304004); Anhui Provincial Natural Science Foundation (Grant No. 1508085J02); Priority R&D Plan Project (2015GGX101035).

Acknowledgments

We thank L.-J. Wang, Y.-L. Tang for useful discussions, and H. Yu for assistance in classical communication system tests.

202.38.88.155 {ts '2018-02-27 20:52:56'}