Metropolitan all-pass and inter-city quantum communication network

Teng-Yun Chen,[1,2] **Jian Wang,**[1,2] **Hao Liang,**[1] **Wei-Yue Liu,**[2,3] **Yang Liu,**[1,2] **Xiao Jiang,**[1,2] **Yuan Wang,**[1] **Xu Wan,**[1] **Wen-Qi Cai,**[1] **Lei Ju,**[1,2] **Luo-Kan Chen,**[1,2] **Liu-Jun Wang,**[1] **Yuan Gao,**[1] **Kai Chen,**[1,4] **Cheng-Zhi Peng,**[1,5] **Zeng-Bing Chen,**[1,6] **and Jian-Wei Pan**[1,7]

[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]*Anhui Quantum Communication Technology Co., Ltd., Hefei, Anhui 230088, China*
[3]*School of Information Science and Engineering, Ningbo University, Ningbo, Zhejiang 315211, China*
[4]*kaichen@ustc.edu.cn*
[5]*pcz@ustc.edu.cn*
[6]*zbchen@ustc.edu.cn*
[7]*pan@ustc.edu.cn*

Abstract: We have demonstrated a metropolitan all-pass quantum communication network in field fiber for four nodes. Any two nodes of them can be connected in the network to perform quantum key distribution (QKD). An optical switching module is presented that enables arbitrary 2-connectivity among output ports. Integrated QKD terminals are worked out, which can operate either as a transmitter, a receiver, or even both at the same time. Furthermore, an additional link in another city of 60 km fiber (up to 130 km) is seamless integrated into this network based on a trusted relay architecture. On all the links, we have implemented protocol of decoy state scheme. All of necessary electrical hardware, synchronization, feedback control, network software, execution of QKD protocols are made by tailored designing, which allow a completely automatical and stable running. Our system has been put into operation in Hefei in August 2009, and publicly demonstrated during an evaluation conference on quantum network organized by the Chinese Academy of Sciences on August 29, 2009. Real-time voice telephone with one-time pad encoding between any two of the five nodes (four all-pass nodes plus one additional node through relay) is successfully established in the network within 60km.

OCIS codes: (270.0270) Quantum optics; (060.0060) Fiber optics and optical communications; (060.5565) Quantum communications.

References and links

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conferenceon Computers, Systems and Signal Processing,* (Bangalore, India, 1984), pp. 175–179.
2. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug and play' systems for quantum cryptography," Appl. Phys. Lett. **70,** 793–795 (1997).
3. T. Nishioka, H. Ishizuka, T. Hasegawa, and J. Abe, "'Circular type' quantum key distribution," IEEE Photon. Technol. Lett. **14,** 576–578 (2002).
4. F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," Nature **421,** 238–241 (2003).

#133167 - $15.00 USD Received 9 Aug 2010; revised 8 Nov 2010; accepted 6 Dec 2010; published 10 Dec 2010

5. C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Appl. Phys. Lett. **84,** 3762–3764 (2004).
6. C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," Phys. Rev. Lett. **94,** 150501 (2005).
7. T. Honjo, K. Inoue, A. Sahara, E. Yamazaki, and H. Takahashi, "Quantum key distribution experiment through a PLC matrix switch," Opt. Commun. **263,** 120–123 (2006).
8. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," Nat. Photonics **1,** 343–348 (2007).
9. Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, and Y. Yamamoto, "Megabits secure key rate quantum key distribution," N. J. Phys. **11,** 045010 (2009).
10. SECOQC White Paper on Quantum Key Distribution and Cryptography, http://www.secoqc.net/downloads/secoqc_crypto_wp.pdf, accessed Feb. 2009.
11. 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**, 6540–6549 (2009).
12. C. Elliott, "Building the quantum network," N. J. Phys. **4,** 46 (2002).
13. C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA Quantum Network," in *Quantum Information and Computation III*, E. J. Donkor, A. R. Pirich, and H. E. Brandt, eds., Proc. SPIE **5815,** 138–149 (2005).
14. X. Tang, L.-J. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. Bienfang, D. Su, R. F. Boisvert, C. Clark, and C. Williams, "Demonstration of an active quantum key distribution network," in *Quantum Communications and Quantum Imaging IV*, R. E. Meyers, Y.-H. Shih, K. S. Deacon, eds., Proc. SPIE **6305,** 630506 (2006).
15. S. J. D. Phoenix, S. M. Barnett, P. D. Townsend, and K. J. Blow, "Multi-user quantum cryptography on optical networks," J. Mod. Opt. **72,** 1155–1163 (1995).
16. P. D. Townsend, "Quantum cryptography on multi-user optical fibre networks," Nature **385,** 47–49 (1997).
17. 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).
18. 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 Photon. Technol. Lett. **21**, 575–577 (2009).
19. A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, Y. Nambu, and A. Tomita, "Recent Progress in Quantum Key Distribution Network Technologies," European Conf. on Communication (ECOC 06) Th2.6.2 (2006).
20. 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," N. J. Phys. **11,** 105001 (2009).
21. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbits secure key rate," Opt. Express **17**, 6540–6549 (2009).
22. W. Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91,** 057901 (2003).
23. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94,** 230503 (2005).
24. H.-K. Lo, X.-F. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94,** 230504 (2005).
25. X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," Phys. Rev. A **72,** 012322 (2005).
26. X.-F. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72,** 012326 (2005).
27. Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, "Decoy-state quantum key distribution with polarized photons over 200 km," Opt. Express **18**, 8587–8594 (2010).
28. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. **5,** 325–360 (2004).
29. G. Brassard, L. Salvail, *Advances in Cryptology EUROCRYPT'93*, Vol. 765 of *Lecture Notes in Computer Science*, (Springer, Berlin, 1994), pp. 410–423.

1. Introduction

It has been nearly 3 decades since proposal of quantum key distribution (QKD) [1]. There are significant theoretical developments and experimental schemes demonstrated, to name a

#133167 - $15.00 USD Received 9 Aug 2010; revised 8 Nov 2010; accepted 6 Dec 2010; published 10 Dec 2010

few of them, see, e.g., [2–9], which enables rapid developments for point to point (PTP) key establishment. Compared with classical optical communications, it is very critical to realize secure connections beyond PTP links by employing QKD, which would offer very promising network applications.

Currently there are mainly two topology structures to expand existing QKD links. One is to use so-called trusted relay architecture. Another one is to implement a transparent network architecture, similar to the case of classical optical network. By using trusted relay, one can increase communication distance for QKD arbitrarily. Also different type of QKD links are compatible in such architecture. However, one should ensure privacy for the relay sites to guarantee security for the whole network. The European SECOQC (Secure Communication based on Quantum Cryptography) quantum network [10] has utilized this kind of paradigm. We have also demonstrated a 3-node communication network based on a trusted relay with each adjacent link of about 20km [11]. By employing optical switching techniques, on the other hand, one can achieve low network complexity for constructing transparent connections. Unfortunately, the application of switching solely can not increase communication distance and key generation rate for QKD. A practical way is to combine additional trust relays to construct a hybrid scalable network. There are many ways to maintain transparent network implementations, such as via optical switching [12–14], passive optical splitting [15, 16], or wavelength-division multiplexing (WDM) [17, 18]. By using beam splitters, one cannot choose connections freely in a passive network, whereas in a WDM-type network, the transmitter has to prepare in advance laser diodes for operating in corresponding wavelength and choosing communications sites. Optical switching has been extensively used such as in the DARPA network [12, 13], the 3-node NIST network [14], in [19] together with a relay, and in [20] for a dynamically reconfigured network. Recent progress in [21] has achieved secure key in a level of Mbits/s for 20 km fiber PTP link, which would promise high-speed metropolitan QKD in the future.

We have complemented and improved performance of QKD network over existing demonstrations in several aspects. This mainly includes all-pass optical switching, novel QKD terminals, 60$\sim$130 km inter-city links, with the help of scalable hybrid network topology. The earlier demonstrations for optical switching network used single optical switch [13, 14] and achieved only one-way connection for some of communication parties. We have managed to design an optical switching equipment that enables 2-connectivity for any input and output ports. Therefore arbitrary interconnection can be created between any two of input and output ports. An all-pass metropolitan QKD network with star-type topology is then accomplished in Hefei city of China. The QKD communications are carried out for any two nodes based on polarization coding. Real-time voice encryption and decryptions are successfully demonstrated through one-time pad coding. Besides, each of the nodes could work as a transmitter or a receiver, or even as both altogether in field experiment. Our design thus offers a potential for duplex communication for the node terminals. Moreover, with such switching equipments and terminals, it is straightforward to construct a network with routing function for quantum signals, similar to the case of classical communications. In our case, the distribution of quantum channel is automatically decided base on communication request, loss of the backbone network, busy or on-off status for fibers. An additional node in Feixi county that is about 60 km fiber distance far from relay node at USTC site in Hefei city, is further added to achieve an inter-city QKD network. With help of trusted relay architecture, we have again established real-time voice communication between this node and any node from the metropolitan network. The network's robustness is verified for this 5-node hybrid structure, by moving further the additional node to Tongcheng city that is about 130 km for fiber distance far from USTC site (the actual distance is about 100km). It works well to communicate with any node from metropolitan network. The network deployment took place in August 2009, and was publicly demonstrated during an

#133167 - $15.00 USD Received 9 Aug 2010; revised 8 Nov 2010; accepted 6 Dec 2010; published 10 Dec 2010

evaluation conference on quantum network organized by the Chinese Academy of Sciences on August 29, 2009. Our hybrid network has realized all necessary functions for a practical QKD network by developing and integrating several key modules including active optical switching for connecting any two ports, hybrid network architecture by integrating optical switching and trusted relay, tailored QKD network processing and control software, automated distribution for quantum channels, intercorporate communication functions of transmitter and receiver for QKD terminals in every node of all-pass network, guaranteed security by employing decoy state schemes [22–26]. Thus we hope that our demonstration could provide a critical step towards practical QKD network in a large scale.

2. Optical switching and network architecture

In order to achieve an all-pass network in a metropolitan network, one of the key ingredient is an equipment that allows arbitrary interconnecting for fibers connecting with different communication parties. The earlier uses for optical switching network [13,14] has not yet operated with this function. In the demonstration, we have managed to produce an 8-port optical switching equipment that allows interconnecting of any two ports. A star-type network is accomplished by connecting every node to our optical switching equipment. Compared with other types of network, there is no special requirements for all-pass network with optical switches. Particularly, this network offers distribution of quantum channel with relatively low loss and enjoying the advantage of easy controlling with classical network commands. We use the mechanical optical switches, which provides high degree of isolations among different ports without direct connections. Moreover, there is no induced additional noise when all the ports work at the same time. Furthermore, this kind of optical switching techniques provides standard single mode fiber channel, which enables hybrid connections for different schemes of QKD and holds potential performance improvement if combined with multiple transmitters and receivers through WDM in every node.

It is neither proved nor quantified for unconditional security through trusted relay architecture up to now. We remark that trusted relay architecture is however a very practical architecture, which could in principle extend range of secure distance for QKD in a large scale. Once the relay nodes are secure, any other nodes can communicate securely with the help of relay nodes. In addition, the relay node provide an interface allowing interoperability of heterogeneous QKD devices, which expand practical applications of QKD network. We have set up a star-type network based on a trusted relay in USTC site, as shown in Fig. 1. If combined with multi-level optical switching and multiple trusted relays, this network topology is scalable to arbitrarily expand to be a complex network with additional QKD devices. We have set up two types of QKD terminals. The terminals connected to the optical switching module are those equipped with functions of being both transmitter and receiver. It should be remarked that there is one circle link of 10 km goes back USTC through underground optic fiber cable, to simulate a separately remote node USTC'. The USTC' node connected to optical switching has acted as a trusted relay, one part of which has been equipped with such a terminal. Another part of USTC' node is treated as a receiver, and uses high speed system that we have developed in [27] without amplification of synchronized signal in between link. All the nodes are running with the standard BB84 protocols based on decoy state schemes [22–26]. The performances are tested and verified for all of possible connections among the 5 nodes.

3. QKD terminal devices for network applications

As shown in Fig. 1, the star-type network provides quantum channels for any two nodes among the 4 nodes in the metropolitan area of Hefei city. To run the network, one has to update the normal PTP QKD links to cover all the nodes. Considering the fact that the arbitrary connection

#133167 - $15.00 USD Received 9 Aug 2010; revised 8 Nov 2010; accepted 6 Dec 2010; published 10 Dec 2010

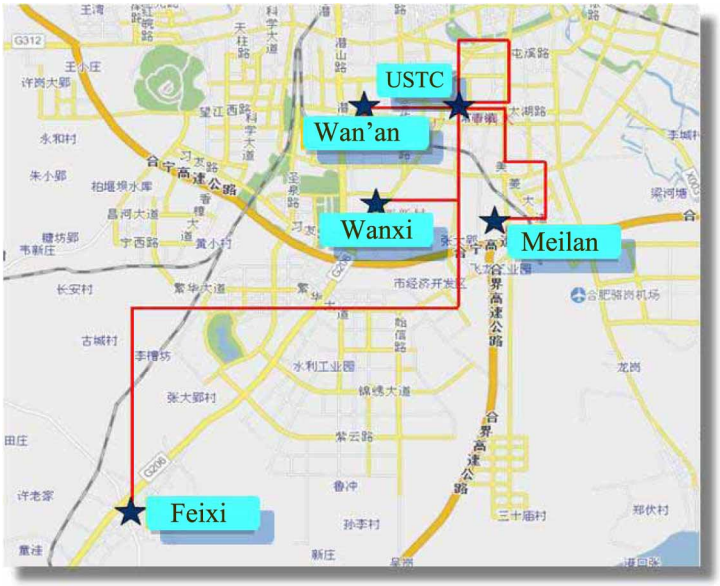

Fig. 1. Metropolitan all-pass quantum communication network constitutes 4 nodes including USTC', Wan'an, Meilan, and Wanxi. A circle link of 10 km goes back USTC through underground optic fiber cable, which is used to simulate a separately remote node USTC'. An additional node in Feixi county (finally moved to Tongcheng city) that is about 60 km fiber distance (130 km fiber distance) far from USTC' site in Hefei city, is further connected to achieve an inter-city QKD network, when the USTC' node serves as a trusted relay.

should be possible for any two of the nodes, we have made a integrated design for terminals that could work either a transmitter or a receiver.

We make use of weak coherent states coming from laser diodes as optical source. Decoy state scheme is implemented for all the links, to extend significantly secure distance and improve key generation rate with proved security. The main idea for decoy scheme is to insert randomly decoy states with different intensity from the signal state during the transmission process. In the receiver side, through detection rates and quantum bit error rates for both the signal states and the decoy states, one can analyze to derive maximum possible information leaked to eavesdropper. Thus two communications sides could then generate secure keys after error corrections and privacy amplification process.

A schematic view of QKD terminal in every terminal of metropolitan network is illustrated in Fig. 2. In order to maintain a relatively high key generation rate, we set the photon number intensity to be $0.6 : 0.2 : 0$/pulse for signal states, decoy states and vacuum states, respectively. The occupancy proportion is set as $6 : 1 : 1$. When the terminal serves a transmitter, the optical pulses are modulated randomly with intensity ratios of 3:1:0 with two cascaded intensity modulators after 1550 nm laser diodes to generate the three kinds of states. Four types of polarized states of $H/V/+/-$ are prepared also at this stage after two cascaded beamsplitters (BS) to represent horizontal, vertical $+45^\circ$ and -45° polarization states. With additional attenuations, the pulses are outputted to field fiber after adjusting the average photon number intensity to be 0.6/pulse for signal states. In the receiver side, standard BB84 detection scheme is applied. When the terminal serve as a receiver, in the detection part the input optical pulses are divided by a beamsplitter (BS) into two arms corresponding to H/V and $+/-$ basis detection unit, re-

#133167 - $15.00 USD Received 9 Aug 2010; revised 8 Nov 2010; accepted 6 Dec 2010; published 10 Dec 2010

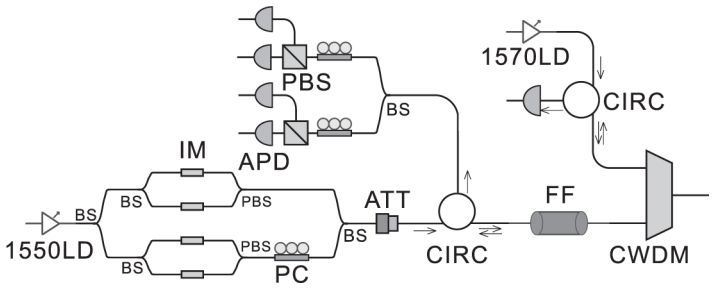

Fig. 2. Schematic view of a QKD device terminal in the experimental setup. When the device serves as a transmitter, four polarizing states are generated by a 1550 nm laser diode after two cascaded BS with additional intensity modulation, before combined by another output BS. Signal and decoy states are also controlled at this stage by random choice. After suitable attenuation, the optical pulses go through a circulator before combining in a CWDM with synchronization pulse. When the terminal serves as a receiver, the optical pulses enter at CWDM, and then decode quantum signals out, for going through circulator at the detection part. Synchronization signal goes along another circulator for clock signal detection. Here, LD: Laser Diode; IM: Intensity Modulator; PBS: Polarization Beam Splitter; PC: Polarization Controller; ATT: Attenuator; CIRC: Circulator; FF: Fiber Filter; CWDM: Coarse Wavelength-division multiplexing.

spectively. In each arm, there is a polarization controller that will actively compensate possible polarization displacement in fiber channel. The polarization beamsplitters (PBS) are then for choosing H/V or $+/-$ measurement basis before the pulses entering detectors.

To incorporating the transmitter function in the same terminal, we have used fiber circulator to isolate the input pulses from field fiber, and the output pulses from the optical source. Whenever the terminal plays a role of transmitter, pulses from laser diode will go through the circulator to outer fiber. Whenever the terminal works as a receiver, the input pulses from outer fiber goes over the circulator and then arrives at detectors. To avoid strong reflection caused by Rayleigh backward scattering for light other than quantum signals in WDM output ports, we have added a narrowband ($\sim$ 100GHz) fiber filter after the circulator with central wavelength of 1510.12 nm. This improvement could dramatically reduce unwanted disturbance caused by noisy light (mainly from synchronization light), and thus contribute low quantum bit error rate (QBER). Moreover the setting will result in a high visibility for outputs of polarizing quantum states. As the detectors are working in gate mode, they require external trigger signals. We have therefore use strong optical pulses as synchronization signal, which allow detections by normal photoelectrical diodes. Whenever there is a quantum pulse is emitted, there is a synchronization pulse from synchronization laser of 200 nw, to tag timing information. For purpose of reducing cost for using fiber, we have managed to use 1570 nm optical pulses as synchronization signal. Together with quantum optical pulses, they are combined into a coarse wavelength division multiplexing module for outputting in field fiber. Another advantage is that the light with wavelength 1570 nm contributes relatively small anti-Stokes scattering for light of 1550 nm, which reflects very low disturbance for quantum signals.

4. Performance in field fiber

Our QKD network is based on installed field fibers of China Netcom Group Corp Ltd. All of the four nodes are connected to the optical switching module at laboratory situated in USTC. The fifth node in Feixi county that is 60 km fiber distance far from USTC' is connected to all-pass

#133167 - $15.00 USD Received 9 Aug 2010; revised 8 Nov 2010; accepted 6 Dec 2010; published 10 Dec 2010

metropolitan network in Hefei city, with USTC' site acting as a trusted relay. The specification parameter for all the links are shown in Table 1.

Table 1. Measured specifications for QKD network

link	Circle link USTC	Wan'an	Meilan	Wanxi	Feixi
Distance	10.047 km	8.447 km	9.904 km	8.417km	60km
Fiber loss	2.82 dB	2.65 dB	2.86 dB	2.75 dB	17 dB

The measured fiber losses among different links do not include loss coming from optical switch, whose value is typically around 0.9 dB$\sim$1.2 dB. The CWDM and FF contribute a loss less than 0.8 dB, and can achieve isolation of about 70 dB between classical communication and quantum signals.. All of the four nodes including USTC', Wan'an, Wanxi and Meilan utilize integrated QKD terminals with functions of transmitter and receiver. The repetition rate of 4 MHz is used for the laser source at these nodes. As mentioned before, the average photon number is 0.6 and 0.2, for sinal states and decoy states, respectively. The receivers use single photon detectors of InGaAs type with two id201 detectors from id Quantique and two detectors produce by East China Normal University. The detectors' efficiency is about 10% for all of four detectors in each node. The random numbers we used for 4 MHz system are produced by modules from id Quantique, while the high-speed system of 320 MHz in Feixi-USTC' link are using pseudo-random numbers. Once powered on, our system can automatically execute whole adjusting and feedback process, wait connecting request from any nodes, and choose their corresponding working modes. We find that the systems can work perfectly with current commercially available underground fiber cables. After extensive monitoring and tests, the system has proven very robust and stable, with a consistent key generation rate for a period of 24h.

For the whole network links, we have measured and derived all the relevant parameters, as listed in Table 2. Here we use post data processing method followed from results of [28] and [22–26]. The key generation rate that can be achieved is as follows

$$R \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1-H_2(e_1)]\}, \tag{1}$$

where the subscript μ is the average photon number per signal in signal states. For convenience, we denote ν the average photon number per pulse for decoy state. Q_μ and E_μ are the measured gain and the QBER for signal states, respectively; q is an efficiency factor for the protocol. Q_1 and e_1 are the unknown gain and the error rate of the true single photon state in signal states. The decoy state method can estimate the lower bound of Q_1 denoting as Q_1^L, and the upper bound of e_1 denoting as e_1^U, and then one can achieve maximum possible secure key rate. The $H_2(x)$ is the binary entropy function: $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$, while the factor $f(x)$ is for considering an efficiency of the bi-directional error correction [29].

We follow here the method developed in [28] and [22–26] to estimate good bounds for Q_1 and e_1. After experimentally measuring all the relevant parameters as listed in Table 2, we can input the following bounds for calculating final key generation rate [26]

$$Q_1 \geq Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}(Q_\nu^L e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - Y_0^U \frac{\mu^2-\nu^2}{\mu^2}), \tag{2}$$

$$e_1 \leq e_1^U = \frac{E_\mu Q_\mu - Y_0^L e^{-\mu}/2}{Q_1^L}, \tag{3}$$

#133167 - $15.00 USD Received 9 Aug 2010; revised 8 Nov 2010; accepted 6 Dec 2010; published 10 Dec 2010

Table 2. Measured and derived specifications for quantum network based on decoy states

Para.	Meilan-USTC'	USTC'-Meilan	USTC'-Wanxi	Wanxi-USTC'	Wanxi-Wan'an
Sifted R	11.0k	9.74k	10.0k	8.02k	8.00k
Final R	1.45k	1.20k	1.95k	1.45k	1.30k
E_μ	1.58%	1.47%	1.51%	1.53%	1.35%
E_ν	4.00%	4.10%	4.99%	4.99%	4.41%
Q_μ	8.21×10^{-3}	5.81×10^{-3}	7.25×10^{-3}	5.83×10^{-3}	7.15×10^{-3}
Q_ν	2.71×10^{-3}	1.90×10^{-3}	2.32×10^{-3}	1.91×10^{-3}	2.20×10^{-3}
Y_0	2.03×10^{-4}	1.38×10^{-4}	2.04×10^{-4}	1.70×10^{-4}	1.78×10^{-4}

Para.	Wan'an-USTC'	Meilan-Wanxi	Meilan-Wan'an	USTC'-Wan'an	Wanxi-Meilan
Sifted R	8.33k	8.54k	9.39k	8.17k	7.97k
Final R	1.40k	1.43k	2.54k	1.82k	1.75k
E_μ	1.67%	1.70%	1.28%	1.43%	1.68%
E_ν	5.40%	4.43%	3.48%	2.79%	4.28%
Q_μ	5.80×10^{-3}	6.79×10^{-3}	6.86×10^{-3}	7.33×10^{-3}	6.23×10^{-3}
Q_ν	1.90×10^{-3}	2.30×10^{-3}	2.29×10^{-3}	2.48×10^{-3}	2.21×10^{-3}
Y_0	1.75×10^{-4}	1.86×10^{-4}	1.19×10^{-4}	1.33×10^{-4}	1.58×10^{-4}

Para.	Wan'an-Meilan	Wan'an-Wanxi	Feixi-USTC'
Sifted R	7.33k	8.39k	18.0k
Final R	1.40k	1.21k	4.50k
E_μ	1.60%	1.56%	1.13%
E_ν	5.16%	4.97%	1.71%
Q_μ	6.43×10^{-3}	5.68×10^{-3}	1.64×10^{-4}
Q_ν	2.16×10^{-3}	1.91×10^{-3}	6.60×10^{-5}
Y_0	1.77×10^{-4}	1.74×10^{-4}	1.13×10^{-6}

in which

$$\begin{aligned} Q_\nu^L &= Q_\nu(1-\frac{10}{\sqrt{N_\nu Q_\nu}}), \\ Y_0^L &= Y_0(1-\frac{10}{\sqrt{N_0 Y_0}}), \\ Y_0^U &= Y_0(1+\frac{10}{\sqrt{N_0 Y_0}}), \end{aligned}$$

Here N_ν, and N_0 are numbers of pulses used as decoy state and vacuum state, respectively, while Q_ν is the measured gain for the decoy states. The measured counting rate for vacuum decoy state is denoted by Y_0.

From Table 2, we see a final key rate of more than 1.2 kbps whenever QBER is less than 2%, for a typical running of 400 s for our system. This has already excluded 1/5 period consuming for adaptive feedback control. We have estimated the bounds for Q_1^L and e_1^U by considering the statistical fluctuations for vacuum states, gains for signal states and decoy states within 10 standard deviations, which ensure the final keys rates promises a confidence interval of about $1-1.5\times10^{-23}$. Although the distance is relatively long for Feixi-USTC' link, we obtain highly fast key rates of 4.5 kbps. This is mainly due to several essential elements that we have

#133167 - $15.00 USD Received 9 Aug 2010; revised 8 Nov 2010; accepted 6 Dec 2010; published 10 Dec 2010

maintained. We have managed to achieve 320 MHz high repetition rate for optical source. With the help of superconduction detectors, extremely low dark counts or counts from unwanted light is anticipated. It is therefore attained for high detection counting rate of about 10 kbps for each arm, and low QBER of typically less than 1%. Based on these resource of secure keys, we have finally tested in application layer to realize voice communication with one-time pad. The voice communication is not only implemented in all of the four nodes in the metropolitan network, each of which has also successfully created secretly audio communication with Feixi node. We have attempted to move the system in Feixi node to Tongcheng city that is about 130 km from USTC', with an approximate fiber loss of 29 dB for transmission. Again we have demonstrated successful operation of QKD, by using broadband wireless network from China Telecom as classical communication channel. A final key rate around 0.2 kbps and QBER of less than 2 % are achieved. We remark that authentication of classical communication is not yet implemented in our system, which is an important ingredient for QKD network and will be covered in our future work.

5. Conclusions and perspectives

We have demonstrated an all-pass quantum communication network in field environment. Hybrid network architecture is illustrated to construct an inter-city network by combining the metropolitan quantum network and a trusted relay, which is capable of extending reach of network nodes arbitrarily. All of necessary functions and equipments are realized, including seamless integrating of all-pass optical switching, trusted relay, decoy state protocol, tailored QKD network hardware, and software control etc. Integrated QKD terminals are developed, which can operate both as a transmitter or a receiver with automated switching. The designed terminals are in fact possible to be used as both transmitter and receiver at the same time, which will double key generation rate with suitable software and electrical control hardware. The hybrid architecture by using of all-pass structure and trusted relay would enables a scalable network for arbitrary distance. The results reported in this paper would help to make a significant step for a practical QKD network in widespread implementation and associated applications.

Acknowledgments

We are grateful to Xiang-Bin Wang for his very valuable discussion. We acknowledge the financial support from the CAS, the National Fundamental Research Program of China under Grant No.2006CB921900, the National High Technology Research and Development Program (863 Program) of China, the NNSFC and the Fundamental Research Funds for the Central Universities.

#133167 - $15.00 USD Received 9 Aug 2010; revised 8 Nov 2010; accepted 6 Dec 2010; published 10 Dec 2010