CHINESE OPTICS LETTERS

Vol. 20, No. 12 | December 2022

Phase modulation polarization encoding module applied to one-to-many QKD network based on wavelength division multiplexing

Yi Zhang (张 毅)[1], Xiaojuan Qin (秦晓娟)[2], Jindong Wang (王金东)[1*], Yafei Yu (於亚飞)[1], Zhengjun Wei (魏正军)[1], and Zhiming Zhang (张智明)[1]

[1] Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China

[2] Guangdong Polytechnic Institute, Guangzhou 510091, China

***Corresponding author:** wangjindong@m.scnu.edu.cn

Received March 1, 2022 | Accepted June 27, 2022 | Posted Online August 15, 2022

The quantum key distribution (QKD) network is a promising solution for secure communications. In this paper, we proposed a polarization-independent phase-modulated polarization encoding module, and it can be combined with a dense wavelength division multiplexer (DWDM) to achieve multi-user QKD. We experimentally test the encoding module with a repetition rate of 62.5 MHz, and its average quantum bit error rate (QBER) is as low as 0.4%. Finally, we implement a principle verification test for simultaneous QKD for 1 to 2 users in 100 min, and the average QBER of two users under the transmission distance of 1 km and 5 km is kept below 0.8%. Due to the use of polarization encoding, the module can also realize scalable network architecture in free-space QKD systems in the future.

Keywords: quantum key distribution; polarization encoding; wavelength division multiplexing; quantum networks.
DOI: 10.3788/COL202220.122701

1. Introduction

Quantum key distribution (QKD) allows two remote parties, commonly known as Alice and Bob, to share a secure encryption key by exchanging qubits encoded into a single photon[1–3]. Since the first QKD protocol was proposed in 1984[4], QKD has been successfully demonstrated in many systems and protocols[5–25], the more famous of which are the decoy state protocol[14], measurement-device-independent (MDI) QKD[15–18], continuous variable (CV) QKD[19–21], and two-field (TF) QKD[22–25]. In order to ensure secure communication with many different parties, various QKD networks have been proposed[26–35]. There are mainly QKD networks based on optical devices[27–29,31–33,35], QKD networks based on trusted relays[30,36], and QKD networks based on quantum repeaters[37,38]. The QKD networks based on quantum repeaters may be one of the best solutions for long-distance transmission in the future, but unfortunately they are still at the research stage and do not have the capability of practical implementation for the time being. The QKD networks based on trusted relays rely on the absolute trust of the relay nodes, and, if one node in the network system is hijacked, the security of the whole system will not be guaranteed. In addition, even if the relay nodes can ensure security, the QKD network is subject to attacks against the measurement end. To solve this problem, MDI-QKD has been proposed[15], where legitimate users send their coded signals to an untrusted third party for interference and detection. Due to the existence of a non-trusted third party, MDI-QKD makes it easier to form a star-type quantum communication network. Currently, MDI-QKD networks have been implemented in metropolitan area networks[26]. The QKD networks based on optical devices do not require trusted intermediate nodes, and furthermore, optical devices are easy to install and maintain, which has become the most common form of a local QKD network today.

In 1997, Townsend proposed a QKD network solution using a passive optical beam splitter (BS)[27], but in this scheme the quantum key rate for each node will reduce with the increase of the number of users. Hence, the optical switch scheme was proposed[33], however, the optical switch will have a rate limit, and QKD cannot be performed simultaneously by multiple users. To solve these problems, wavelength division multiplexer (WDM)-based QKD network solutions have been proposed in large numbers[32,33]. Of all the network architectures mentioned above, the one-to-many network architecture is very useful in large-scale quantum networks to connect a large number of end users[39]. Since the plug-and-play system can achieve

self-compensation of phase drift and polarization[5,40,41], the current one-to-many network architecture mostly uses the plug-and-play system with phase encoding. However, the phase modulator (PM) in the one-to-many QKD system based on WDM cannot modulate optical pulses with different wavelengths quickly and accurately, which will result in a higher quantum bit error rate (QBER)[39]. But, this problem can be avoided by polarization encoding. Unfortunately, there is no solution to realize the expansion of the QKD network at low cost based on polarization encoding.

Therefore, this paper proposed a polarization-independent phase-modulated polarization encoding module, which can increase the number of users by using dense WDM (DWDM) based on a point-to-point structure. Since only the two-way system is used at the encoding side, the encoding process can automatically compensate for the birefringence, polarization-related loss, and phase shift in the fiber[5,40,41]. QKD in free space requires a set of devices that can transmit and track scan probes[42,43]. Our scheme can increase the number of Alice users by sharing only one transmitter at low cost; combined with time division multiplexing (TDM)[35], we can realize QKD between all users in one region and Bob in another region. Firstly, we implement the principle verification experiment on the encoding module at the repetition rate of 62.5 MHz, and the average QBER remains at 0.4% over 100 min. Subsequently, based on this module, we choose DWDM combined with TDM to implement a one-to-two QKD network test experiment. Under the transmission distance of 1 km, the average QBER of two users is 0.57% and 0.55%, respectively, and, under the transmission distance of 5 km, the average QBER of two users is 0.68% and 0.70%, respectively.

2. Principle of Polarization-Independent Phase-Modulated Polarization Encoding Module

Polarization encoding is essentially differential phase encoding between two orthogonal polarization components. Most encoders today are designed on this principle, and our encoding module is no exception. The encoding module at Alice's node is shown in Fig. 1. We use the BB84 four-state protocol to implement our scheme, and the Dirac symbols of these four states are $|D\rangle(\frac{\sqrt{2}}{2}(|H\rangle+|V\rangle))$, $|A\rangle(\frac{\sqrt{2}}{2}(|H\rangle-|V\rangle))$, $|R\rangle(\frac{\sqrt{2}}{2}(|H\rangle+i|V\rangle))$, and $|L\rangle(\frac{\sqrt{2}}{2}(|H\rangle-i|V\rangle))$. The laser sends out an optical pulse, which passes through the isolator, polarization controller (PC), circulator, and into the polarization BS (PBS). The PC ensures that the polarization state of the optical pulse input to PBS1 is 45° $[|\phi\rangle=\frac{\sqrt{2}}{2}(|H\rangle+|V\rangle)]$; then, from PBS1, the optical pulse generates two orthogonal components of $|H\rangle$ and $|V\rangle$ with equal probability. Component $|H\rangle$ passes through a polarization maintaining fiber with a delay line, which we will refer to as L1. The component $|V\rangle$ is reflected through the other way of the polarization maintaining fiber, which we will call L2. Due to the existence of a delay line, the two component pulses will have a delay of 5 ns. After they pass through PBS2, they will

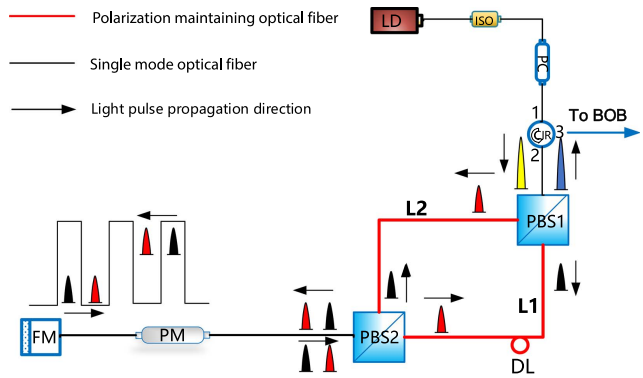

Fig. 1. Polarization-independent phase-modulated polarization encoding module. LD, laser diode; ISO, isolator; PC, polarization controller; CIR, circulator; PBS, polarization beam splitter; DL, delay line; PM, phase modulator; FM, Faraday mirror.

be transmitted to the same single-mode fiber (SMF) and arrive at the PM. The polarization state of the optical pulse arriving at the PM cannot be maintained, so we use the polarization-independent PM. As shown in black in Fig. 1, this PM modulates one of the two single-photon pulses, and we apply the same voltage to its forward and backward transmitted pulses. Another single-photon pulse, such as the red in Fig. 1, will never be modulated. The component $|H\rangle$, reflected by the Faraday mirror (FM), becomes the polarization state of $|V\rangle$, and it is reflected by PBS2 to the path of L2. The component $|V\rangle$, reflected by the FM, becomes the polarization state of $|H\rangle$, and it is reflected by PBS2 to the path of L1. Both components reaching PBS1 at the same time superimpose a new polarization state emitted through the circulator 3 port.

We now theoretically deduce the stability of the module encoding. The forward and reverse operators for SMF1 between PBS2 and PM are given here first[44,45]:

$$\widehat{P_{s1}}=A_1|H\rangle\langle H|+B_1|H\rangle\langle V|+B_1|V\rangle\langle H|+D_1|V\rangle\langle V|, \quad (1)$$

$$\widehat{P_{s1}}'=A_1|H\rangle\langle H|-B_1|H\rangle\langle V|-B_1|V\rangle\langle H|+D_1|V\rangle\langle V|. \quad (2)$$

Similarly, for SMF2 between the FM and PM, it has the operator

$$\widehat{P_{s2}}=A_2|H\rangle\langle H|+B_2|H\rangle\langle V|+B_2|V\rangle\langle H|+D_2|V\rangle\langle V|, \quad (3)$$

$$\widehat{P_{s2}}'=A_2|H\rangle\langle H|-B_2|H\rangle\langle V|-B_2|V\rangle\langle H|+D_2|V\rangle\langle V|. \quad (4)$$

In the above equations, $A=e^{i\frac{\sigma}{2}}\cos^2\theta+e^{-i\frac{\sigma}{2}}\sin^2\theta$, $B=i\sin 2\theta\sin\frac{\sigma}{2}$, $D=e^{i\frac{\sigma}{2}}\sin^2\theta+e^{-i\frac{\sigma}{2}}\cos^2\theta$, where σ and θ are the phase and angle between the two eigenmodes. Among them, A, B, and D satisfy the condition $A_1D_1-B_1^2=1$, $A_2D_2-B_2^2=1$.

We ensure that the polarization state of the optical pulse entering PBS1 is

$$|\phi_1\rangle = \frac{\sqrt{2}}{2}(|H\rangle + |V\rangle). \tag{5}$$

After passing through PBS1, the polarization of the optical pulse is divided with equal probability into two components of $|H\rangle$ and $|V\rangle$. We first discuss the state evolution of component $|H\rangle$, which will first pass through the path of L1 and then reach PBS2. The polarization state is

$$|\phi_2\rangle = e^{i\varphi_{\mathrm{PMF}_1}}|H\rangle, \tag{6}$$

where φ_{PMF_1} is the phase shift produced by the path of L1. After passing through PBS2, the optical pulse enters SMF1 and reaches the PM. Due to the birefringence effect of the SMF, the polarization state of the optical pulse is

$$|\phi_3\rangle = \widehat{P_{s1}}|\phi_2\rangle = e^{i\varphi_{\mathrm{PMF}_1}}(A_1|H\rangle + B_1|V\rangle). \tag{7}$$

We load the electric pulse signal propagating synchronously with the component onto the polarization-independent PM, and the first modulation is performed here,

$$|\phi_4\rangle = e^{i\varphi_{\mathrm{PMF}_1}}(e^{i\varphi_e}A_1|H\rangle + e^{i\varphi_o}B_1|V\rangle), \tag{8}$$

where φ_e and φ_o denote the phase shift introduced by the TE mode and the TM mode of the PM waveguide when applying control voltage pulses to the PM, respectively. The polarization-independent PM has different modulation efficiencies for o light and e light, thus, we have $\varphi_e \neq \varphi_o$.

The light pulse then passes through SMF2, so the polarization state of the light pulse before reaching the FM is

$$\begin{aligned}|\phi_5\rangle &= \widehat{P_{s2}}|\phi_4\rangle \\ &= e^{i\varphi_{\mathrm{PMF}_1}}(e^{i\varphi_e}A_1A_2|H\rangle + e^{i\varphi_e}A_1B_2|V\rangle \\ &\quad + e^{i\varphi_o}B_1B_2|H\rangle + e^{i\varphi_o}B_1D_2|V\rangle).\end{aligned} \tag{9}$$

The FM operator is

$$\widehat{P_{\mathrm{FM}}} = |H\rangle\langle V| + |V\rangle\langle H|. \tag{10}$$

Therefore, when the light pulse returns from the FM and passes SMF2 again to the PM, its polarization state is

$$|\phi_6\rangle = \widehat{P_{s2}}'\widehat{P_{\mathrm{FM}}}|\phi_5\rangle = e^{i\varphi_{\mathrm{PMF}_1}}(e^{i\varphi_o}B_1|H\rangle + e^{i\varphi_e}A_1|V\rangle). \tag{11}$$

At this point the light pulse reaches the PM again, and we load it with the same voltage for modulation,

$$\begin{aligned}|\phi_7\rangle &= e^{i\varphi_{\mathrm{PMF}_1}}(e^{i\varphi e}e^{i\varphi_o}B_1|H\rangle + e^{i\varphi_o}e^{i\varphi_e}A_1|V\rangle) \\ &= e^{i\varphi_{\mathrm{PMF}_1}}e^{i(\varphi_e+\varphi_o)}(B_1|H\rangle + A_1|V\rangle).\end{aligned} \tag{12}$$

Finally, the light pulse will return to PBS2 through SMF1,

$$\begin{aligned}|\phi_8\rangle &= \widehat{P_{s1}}'|\phi_7\rangle \\ &= e^{i\varphi_{\mathrm{PMF}_1}}e^{i(\varphi_e+\varphi_o)}((A_1B_1 - A_1B_1)|H\rangle + (A_1D_1 - B_1^2|V\rangle)) \\ &= e^{i\varphi_{\mathrm{PMF}_1}}e^{i(\varphi_e+\varphi_o)}|V\rangle.\end{aligned} \tag{13}$$

Then, the optical pulse will be transmitted from PBS2 to PBS1 through path L2, and its polarization state is

$$|\phi_9\rangle = e^{i(\varphi_{\mathrm{PMF}_2}+\varphi_{\mathrm{PMF}_1})}e^{i(\varphi_e+\varphi_o)}|V\rangle, \tag{14}$$

where φ_{PMF_2} is the phase shift generated by the path of L2.

Similarly, the other component $|V\rangle$ is first reflected from PBS1 and then passes through the path of L2 to PBS2 with the polarization state

$$|\phi_2'\rangle = e^{i\varphi_{\mathrm{PMF}_2}}|V\rangle. \tag{15}$$

After passing through PBS2, it will reach the PM through the SMF and then be reflected back by the FM. Since the optical pulse is not modulated in the whole process, the polarization state after returning to PBS2 is

$$|\phi_3'\rangle = e^{i\varphi_{\mathrm{PMF}_2}}|H\rangle. \tag{16}$$

The optical pulse will be transmitted from PBS2 to PBS1 through the path of L2, and its polarization state is

$$|\phi_4'\rangle = e^{i(\varphi_{\mathrm{PMF}_2}+\varphi_{\mathrm{PMF}_1})}|H\rangle. \tag{17}$$

The initial two components then travel the same distance through the fiber and reach PBS1 at the same time, and the final polarization state is

$$\begin{aligned}|\phi\rangle &= \frac{\sqrt{2}}{2}(|\phi_9\rangle + |\phi_4'\rangle) \\ &= \frac{\sqrt{2}}{2}(e^{i(\varphi_{\mathrm{PMF}_2}+\varphi_{\mathrm{PMF}_1})}e^{i(\varphi_e+\varphi_o)}|V\rangle + e^{i(\varphi_{\mathrm{PMF}_2}+\varphi_{\mathrm{PMF}_1})}|H\rangle) \\ &= \frac{\sqrt{2}}{2}e^{i(\varphi_{\mathrm{PMF}_2}+\varphi_{\mathrm{PMF}_1})}(e^{i(\varphi_e+\varphi_o)}|V\rangle + |H\rangle).\end{aligned} \tag{18}$$

The phase shift of $\varphi_{\mathrm{PMF}_2} + \varphi_{\mathrm{PMF}_1}$ caused by the polarization maintaining fiber is constant, that is, the final polarization state is determined by the phase shift of $\varphi_e + \varphi_o$ produced by the polarization-independent PM.

3. Experimental Setup

3.1. Point-to-point QKD based on encoding module

The four-state feasibility test experiment is carried out on the encoding module, and the experimental setting is shown in Fig. 2. We use the digital generator (DG) as a synchronous trigger source to trigger the laser diode (LD), electrical pulse generator (EPG-210, manufactured by Alnair Labs), and single-photon detectors (SPDs, manufactured by QuantumCTek), respectively. The laser generates optical pulses with a temporal

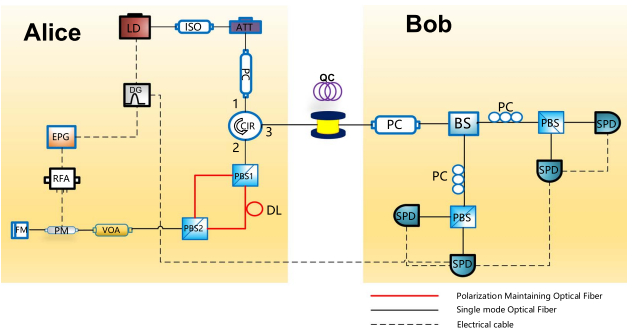

Fig. 2. Point-to-point QKD based on encoding module. LD, laser diode; ISO, isolator; PC, polarization controller; CIR, circulator; PBS, polarization beam splitter; PM, phase modulator; FM, Faraday mirror; VOA, variable optical attenuator; DG, digital generator; EPG, electrical pulse generator; DL, delay line; RFA, radio-frequency amplifier; QC: quantum channel; BS, optical beam splitter; SPD, single-photon detector.

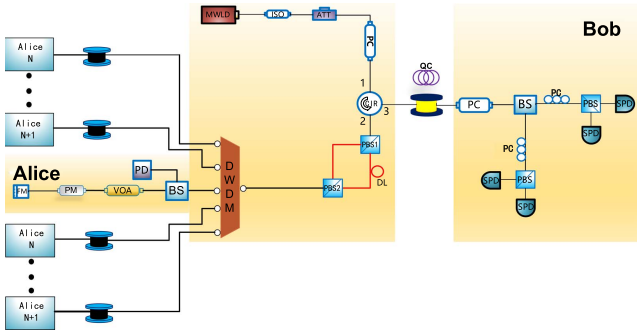

Fig. 3. Multi-user QKD networks based on point-to-point structure using DWDM. MWLD, multi-wavelength laser diode; ISO, isolator; PC, polarization controller; CIR, circulator; PBS, polarization beam splitter; DWDM, dense wavelength division multiplexer; PM: phase modulator; PD, photo diode; FM: Faraday mirror; VOA, variable optical attenuator; DL, delay line; QC: quantum channel; BS, beam splitter; SPD, single-photon detector.

width of approximately 50 ps (FWHM) at a repetition rate of 62.5 MHz. The isolator behind the laser can effectively isolate the light reflected from the fiber and avoid the impact of reflected light on the performance of the laser. The optical attenuator (ATT) serves to attenuate the optical pulses and reduce the Rayleigh scattering effect due to the two-way system. The PC ensures that the optical pulse is incident at 45° to PBS1, and the circulator ensures that the optical pulse is encoded by Alice and sent to Bob for detection. The variable optical ATT (VOA) serves to attenuate the optical pulse reflected back from the FM to the single-photon level. Since the rated voltage of the EPG is not enough, we must use a radio frequency amplifier (RFA, manufactured by Photline Technologies) to linearly amplify the voltage so that the voltage loaded on the PM can meet the modulation of four states. The conventional BB84 four-state protocol detection device is used at the Bob end, and the SPDs employed are commercial InGaAs/InP detectors working in gated mode; they have 300 ps gate windows, with an average dark count probability per gate of 10^{-6} and a detection efficiency of about 16%.

3.2. Multi-user QKD networks based on point-to-point structure using DWDM

Here, we will use a DWDM to extend the user based on a point-to-point structure, as shown in Fig. 3. The pale yellow areas represent one of the Alice users with a multi-wavelength laser source, and the area where the laser source is located acts as the transmitter for all Alice users. Since our encoding module is based on a two-way system, we can send optical pulses to multiple Alices through a multi-wavelength laser. After being modulated by the user, the optical pulses return to form a single-photon pulse with information, which is then sent to Bob. In this experiment, the polarization state is affected by the SMF, so only the optical fiber reel is used at the encoding node, while the quantum channel (QC) uses an optical ATT for equivalent substitution. The light blue area in Fig. 3 represents the equipment of each user on the encoding side, which is composed of a PM, an FM, a 1:99 BS, and a photo diode (PD). The PD is used to detect optical power to prevent Trojan horse attacks. In terms of increasing users at low cost, our system will have very significant advantages. We used a dual picosecond pulsed laser as the laser source, using DWDM channels CH34 (wavelength 1550.13 nm) and CH35 (wavelength 1549.34 nm) as the two Alice user channels, and implement simultaneous QKD experiments at the 1 km and 5 km optical fiber reel by combining TDM. As we want to ensure that simultaneous QKD for two users can be achieved, the optical pulses of the two users must be staggered in the time domain by designing the fiber length so that they are detected by SPDs. Only the optical path is plotted in the figure, and we omitted the synchronization signal circuit diagram.

4. Results and Discussion

In Section 3.1 on point-to-point QKD based on the encoding module, we tested the stability of the four polarization states of the encoding module, with an average QBER of 0.4% in the system. The results are shown in Fig. 4. When modulating the four

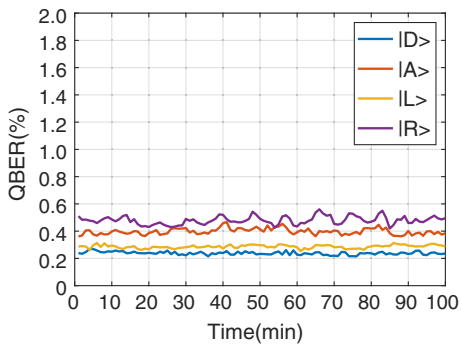

Fig. 4. QBER of the four polarization states tested under polarization-independent phase modulation over 100 min.

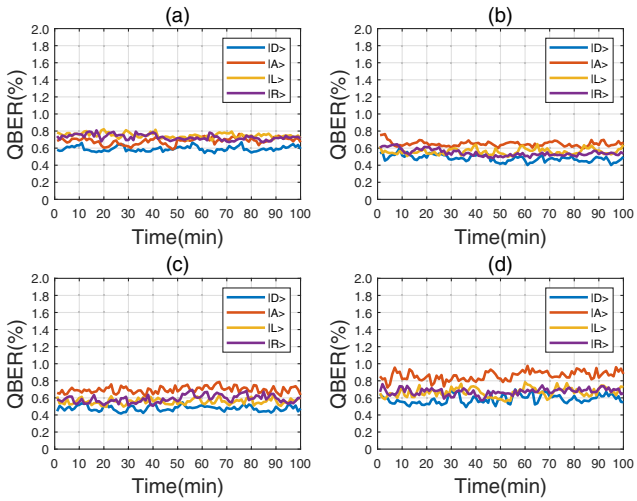

Fig. 5. (a) QBER of CH34 over 100 min at 1 km; (b) QBER of CH35 over 100 min at 1 km; (c) QBER of CH34 over 100 min at 5 km; (d) QBER of CH35 over 100 min at 5 km.

polarization states, the voltage values applied to the PM are different. The average QBER of $|D\rangle$, $|A\rangle$, $|L\rangle$, and $|R\rangle$ are 0.24%, 0.40%, 0.29%, and 0.48%, respectively.

After that, we chose to test the one-to-two QKD network experiment on the basis of the point-to-point structure.

From the Fig. 5, we can see that there is not much difference in the QBER fluctuation between the two transmission distances at 1 km and 5 km. Of course, the QBER of CH35 is higher at the transmission distance of 5 km, which is caused by different modulation voltages and different optical fiber reels. In the whole experimental system, the average QBER of all users under the transmission distance of 1 km and 5 km is kept below 0.8%. If we take 1 km or 5 km transmission distance as the coverage radius, we can use DWDM to connect a large number of users to our system. Bob can realize TDM by setting the time division at the SPD according to the arrival time of the quantum key signal on each channel, thus enabling simultaneous communication between all coverage areas and the Bobs at the other areas.

5. Conclusion

In this paper, we proposed a polarization-independent phase-modulated polarization encoding module; based on this module, one-to-many QKD networks can be realized by using DWDM. We performed a theoretical derivation of the encoding process of the module and then tested the stability of the four polarization states of the modulation. We obtained that the average QBER of the four states remained below 0.4%. Then, we implemented the QKD test experiment of two Alices and one Bob. Within 100 min, the average QBERs of two Alices under the 1 km optical fiber reel are 0.57% and 0.55%, respectively, while the average QBERs under the 5 km optical fiber reel are 0.68% and 0.70%, respectively. The experimental results show that the module can realize stable encoding in a short distance when applied to multi-user systems. The use of polarization encoding not only avoids the noise problem in the plug-and-play phase encoding network system, but also avoids the problem that the PM cannot modulate the optical pulse of different wavelengths quickly and accurately. More importantly, the system shares a common transmitter for all users, and it can be applied to a flexible and scalable network architecture based on point-to-point free-space QKD. Our group will add the decoy state protocol to this scheme for further experiments in a free-space QC in the future. The module has broad application prospects and provides more solutions for local QKD networks.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (Nos. 61771205 and 62071186), Natural Science Foundation of Guangdong Province (No. 2015A030313388), Science and Technology Planning Project of Guangdong Province (Nos. 2015B010128012 and 2017KZ010101), and Key Laboratory Foundation of Guangdong Province, China (No. 2020B1212060066).

References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145 (2002).
2. V. Scarani, H. B. 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. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661 (1991).
4. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Theor. Comput. Sci. **7**, 560 (2014).
5. 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 (1997).
6. C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Appl. Phys. Lett. **84**, 3762 (2004).
7. 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).
8. Y.-P. Yuan, C. Du, Q.-Q. Shen, J.-D. Wang, Y.-F. Yu, Z.-J. Wei, Z.-X. Chen, and Z.-M. Zhang, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution based on intrinsically stable polarization-modulated units," Opt. Express **28**, 10772 (2020).
9. N.-N. Yu, Z.-Y. Dong, J.-D. Wang, Z.-J. Wei, and Z.-M. Zhang, "Impact of spontaneous Raman scattering on quantum channel wavelength-multiplexed with classical channel in time domain," Chin. Opt. Lett. **12**, 102073 (2014).
10. Y. Xue, W. Chen, S. Wang, Z.-Q. Yin, L. Shi, and Z.-F. Han, "Airborne quantum key distribution: a review [Invited]," Chin. Opt. Lett. **19**, 122702 (2021).
11. J.-P. Wang, Z.-H. Li, Z.-Q. Sun, T.-Q. Dou, W.-X. Qu, F. Zhou, Y.-X. Han, Y.-Q. Huang, and H.-Q. Ma, "Loss-tolerant measurement device independent quantum key distribution with reference frame misalignment," Chin. Opt. Lett. **20**, 092701 (2022).
12. G.-Y. Zhu, L. Xiao, B.-Z. Huo, and P. Xue, "Photonic discrete-time quantum walks [Invited]," Chin. Opt. Lett. **18**, 052701 (2020).
13. P.-Y. Zhang, L.-L. Lu, F.-C. Qu, X.-H. Jiang, X.-D. Zheng, Y.-J. Lu, S.-N. Zhu, and X.-S. Ma, "High-quality quantum process tomography of time-bin qubit's transmission over a metropolitan fiber network and its application," Chin. Opt. Lett. **18**, 082701 (2020).
14. H.-K. Lo, X.-F. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).

15. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2018).
16. X.-D. Zheng, P.-Y. Zhang, R.-Y. Ge, L.-L. Lu, G.-L. He, Q. Chen, F.-C. Qu, L.-B. Zhang, X.-L. Cai, Y.-Q. Lu, S.-N. Zhu, P.-H. Wu, and X.-S. Ma, "Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution," Adv. Photonics **3**, 055002 (2021).
17. C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, "Phase-reference-free experiment of measurement-device-independent quantum key distribution," Phys. Rev. Lett. **115**, 160502 (2015).
18. H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y.-Q. 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**, 190501 (2016).
19. S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," Nat. Photonics **9**, 397 (2015).
20. Y.-C. Zhang, Z.-Y. Chen, S. Pirandola, X.-Y. Wang, C. Zhou, B.-J. Chu, Y.-J. Zhao, B.-J. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Phys. Rev. Lett. **125**, 010502 (2020).
21. W.-B. Liu, C.-L. Li, Y.-M. Xie, C.-X. Weng, J. Gu, X.-Y. Cao, Y.-S. Lu, B.-H. Li, H.-L. Yin, and Z.-B. Chen, "Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance," PRX. Quantum. **2**, 040334 (2021).
22. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400 (2018).
23. H.-L. Yin and Y. Fu, "Measurement-device-independent twin-field quantum key distribution," Sci. Rep. **9**, 3045 (2019).
24. J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," Nat. Photonics **15**, 570 (2021).
25. S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. F. Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution over 830-km fibre," Nat. Photonics **16**, 154 (2022).
26. 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.-F. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," Phys. Rev. X. **16**, 011024 (2016).
27. P. Townsend, "Quantum cryptography on multiuser optical fibre networks," Nature **385**, 47 (1997).
28. E. Donkor, "Experimental auto-compensating multi-user quantum key distribution network using a wavelength-addressed bus line architecture," Proc. SPIE **8397**, 839704 (2012).
29. 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. Light. Technol. **23**, 268 (2005).
30. 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 (2009).
31. 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 (2011).
32. G. Brassard, F. Bussieres, N. Godbout, and S. Lacroix, "Multiuser quantum key distribution using wavelength division multiplexing," Proc. SPIE **5260**, 149 (2003).
33. J. Bogdanski, J. Ahrens, and M. Bouennane, "Sagnac quantum key distribution over telecom fiber networks," Opt. Commun. **282**, 1231 (2009).
34. 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).
35. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, "A quantum access network," Nature **501**, 69 (2013).
36. S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N. L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett. **120**, 030501 (2018).
37. H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," Phys. Rev. Lett. **81**, 5932 (1998).
38. Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J.-W. Pan, "Experimental demonstration of a BDCZ quantum repeater node," Nature **454**, 1098 (2008).
39. B. K. Park, M. K. Woo, Y. S. Kim, Y. W. Cho, S. Moon, and S. W. Han, "User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a $1 \times N$ quantum key distribution network system," Photon. Res. **8**, 296 (2020).
40. D. S. Bethune and W. P. Risk, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light," IEEE J. Quantum Electron. **36**, 340 (2010).
41. J.-D. Wang, X.-J. Qin, Y.-Z. Jiang, X-J. Wang, L.-W. Chen, F. Zhao, Z.-J. Wei, and Z.-M. Zhang, "Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units," Opt. Express **24**, 8302 (2016).
42. 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 (1998).
43. P. V. Trinh, T. V. Pham, H. V. Nguyen, S. X. Ng, and A. T. Pham, "Performance of free-space QKD systems using SIM/BPSK and dual-threshold/direct-detection," in *IEEE Globecom Workshops* (2016), p. 8302.
44. M. Martinelli, "A universal compensator for polarization changes induced by birefringence on a retracing beam," Opt. Commun. **72**, 341 (1989).
45. J. Liñares, G. M. Carral, X. Prieto-Blanco, and D. Balado, "Autocompensating measurement-device-independent quantum cryptography in space division multiplexing optical fibers," J. Eur. Opt. Soc. **17**, 19 (2021).