EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Proof-of-principle demonstration of semi-quantum key distribution based on the Mirror protocol

Siyu Han[1], Yutao Huang[1], Shang Mi[1], Xiaojuan Qin[2], Jindong Wang[1]*, Yafei Yu[1], Zhengjun Wei[1] and Zhiming Zhang[1]

*Correspondence:
wangjindong@m.scnu.edu.cn
[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
Full list of author information is available at the end of the article

Abstract

Semi-quantum key distribution (SQKD) is used to establish a string of shared secret keys between a quantum party and a classical party. Here, we report the first proof-of-principle experimental demonstration of SQKD based on the Mirror protocol, which is the most experimentally feasible SQKD protocol, and equipped with time-phase encoding scheme employing the method of selective modulation. The experiment was performed at a repetition frequency of 62.5 MHz and a high raw key rate arrived at 69.8 kbps, and the average quantum bit error rate was found to be 4.56% and 2.78% for the "SWAP-x-Z" ($x \in \{01, 10\}$) and the "CTRL-X", respectively. The results demonstrate the feasibility of our system, and this study is helpful for future research on SQKD experiments.

Keywords: Semi-quantum key distribution; Classical operation; Time-phase encoding; Selective modulation

1 Introduction

Since the security of the classical communication is based on the algorithm strength, unconditional security of the communication cannot be guaranteed. Quantum information technology provides a variety of possible ways to achieve secure communication: quantum key distribution (QKD) [1], quantum secret sharing (QSS) [2, 3], quantum secure direct communication (QSDC) [4–13], quantum teleportation (QT) [14], quantum dense coding [15], etc. One of the characteristics of QKD is on the capability to detect eavesdropping on-site. Combined with "one time pad" [16], QKD can ensure unconditional security of communication theoretically. QSS is suitable for secure multi-party computing and key management. QSDC has become a hot topic in recent years due to its property of enabling secret messages to be transmitted directly without the need for keys. QT takes advantage of the property of quantum entanglement without the need to send solid particles into the channel, thus completely avoiding the risk of eavesdropping on quantum information. Quantum dense coding provides a higher capacity than its counterpart in classical domain and can be used in QKD and QSDC.

Among the various branches mentioned above, QKD is a very important technology that is currently the most developed and fastest to be incorporated into practical applications. For secure key distribution, is it possible that only one party is quantum, yet and the other has only classical capabilities? Of course the answer is“yes” [17–19], and this new kind of key distribution is called semi-quantum key distribution (SQKD).

In 2007, the concept of SQKD was introduced originally by Boyer et al. and the BKM07 protocol - “QKD with classical Bob” was presented [17]. Subsequently, “QKD with classical Alice” protocol [18, 19] as well as other SQKD protocols [20–24] have been proposed in succession, and new kinds of protocols were derived from crossover with other fields, such as semi-quantum secret sharing (SQSS) [25], semi-quantum secure direct communication (SQSDC) [26], semi-quantum private comparison (SQPC) [27] and so on. Some of these protocols (e.g., Single-State SQKD protocol) have been proven to be secure in the “perfect qubit scenario” [28–31]. For the SQKD protocols, there are two operations can be chosen by the classical party Alice: “CTRL” and “SIFT”. “CTRL” means to return the photon to the quantum party Bob undisturbed, while “SIFT” is commonly achieved as follows: Alice is required to measure the photon from Bob in the Z basis $\{|0\rangle, |1\rangle\}$ and re-transmit the photon to Bob according to the measurement results. However, given the current experimental technology, the re-generated photon cannot be the same as the original photon, thus the photons will be attacked by using the “tagged” method in the mock protocol presented in [17], and information will be leaked to Eve [32, 33]. Therefore, based on the Single-state SQKD protocol, Boyer et al. proposed the experimentally feasible Mirror protocol [34] to avoid the security vulnerability introduced by regenerating new photons. Nevertheless, the Mirror protocol is more complicated than other SQKD protocols, and the classical operations (CTRL, SWAP-10, SWAP-01 and SWAP-ALL) pose technical challenges to its experimental implementation. Before that, Gurevich used the time encoding scheme to partially implement the experiment based on the SQKD protocol [35]. However, as described by the author, the error rates of this system are relatively high: the quantum bit error rate of “CTRL-X” is 16.7%, and that of “SWAP-x-Z” ($x \in \{01, 10\}$) is 23.59%. Meanwhile, because of the incomplete implementation of the classical operations (i.e., the lack of SWAP-ALL), attacks can take place in the current implementation [36]. Strictly speaking, it is not a successful feasibility verification of the SQKD protocol.

Here, we have implemented the first proof-of-principle experimental demonstration of SQKD based on the Mirror protocol, which uses the time-phase encoding scheme with the method of selective modulation to avoid the security problem of regenerating new photons. Moreover, our experiment obtains a higher raw key rate and lower bit error rate. The method of selective modulation we presented may promote the research progress of theory and experiments in the semi-quantum field and open new ideas for future researchers.

The remainder of this paper is organized as follows. In Sect. 2, the Mirror protocol is briefly introduced. In Sect. 3, we propose the time-phase coding scheme based on the Mirror protocol, and then the experimental setup is described in detail in Sect. 4. The experimental results are showed and discussed in Sect. 5. We conclude in Sect. 6.

2 The Mirror protocol

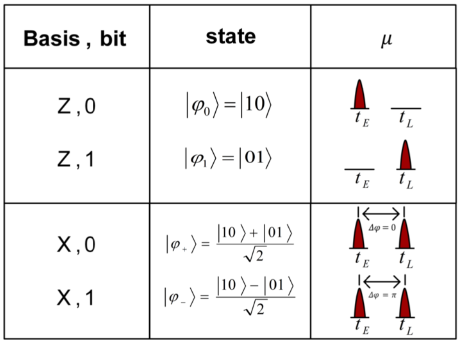
In the Mirror protocol, the operations of the classic party Alice change from the original operations “CTRL” and “SIFT” [18, 19] to four operations: (1) CTRL: Alice reflects the qubit to Bob directly; (2) SWAP-10: Alice measures photons in the $|1\rangle$ state and returns photons in the $|0\rangle$ state to Bob; (3) SWAP-01: Alice measures photons in the $|0\rangle$ state and return photons in the $|1\rangle$ state to Bob; (4) SWAP-ALL: Alice measures all photons, and does not return any photons to Bob.

The Mirror protocol is as follows: the sender Bob sends the quantum state $|+\rangle$ to Alice. Then, Alice randomly selects one of the operations "CTRL," "SWAP-ALL," "SWAP-01," "SWAP-10", and records whether it receives a "click". If Alice chooses "SWAP-01," no photon is detected with a one-half probability, and then the quantum state is projected into the state $|1\rangle$. If Alice chooses "SWAP-10," no photon is detected with a one-half probability, and then the quantum state is projected into the state $|0\rangle$.

Bob then randomly chooses Z basis $\{|0\rangle, |1\rangle\}$ or X basis $\{|+\rangle, |-\rangle\}$ to measure the qubit sent back from classical Alice. After N qubits are measured and sent, Alice declares her operation choices (CTRL, SWAP-x, or SWAP-ALL; she keeps x $\in \{01, 10\}$ in secret) and Bob announces his basis choices. For the combination chosen by both parties, if Bob chooses the Z basis, Alice chooses to "SWAP-x" (which is called "SWAP-x-Z"), and the photon is not detected, they will use the bits of this position as the raw keys. That is, Bob's measurement result is $|i\rangle$ ($i \in \{0, 1\}$), and the opposite result of Alice's measurement result is also $|i\rangle$. Hence, their shared secret key is coded as i. If Alice selects "CTRL" and Bob chooses measurement in X basis, this kind of operation will be called "CTRL-X". In this case, the position of the bits can be used to detect Eve's eavesdropping. Alice and Bob then check the bit error rate in "CTRL-X" and "SWAP-x-Z," and if the bit error rate is too high, the protocol will be aborted. Alice and Bob also check whether other errors exist (for example, they verify if Bob detects no photons in case Alice uses "SWAP-ALL"). Alice and Bob discard the other mismatched bits of "CTRL-Z" and "SWAP-x-X" because of the uncertainty in the measurement results. Finally, Alice and Bob perform error correction and privacy amplification on the code location "SWAP-x-Z," and both parties obtain the secret security keys.

3 Time phase coding scheme based on the Mirror protocol

A proof-of-principle experimental demonstration of SQKD based on the Mirror protocol is implemented by using time-phase encoding. The time-phase encoding rule is shown in Fig. 1 [37]. In this rule, the qubits in the Z basis and the X basis are composed of the two temporal modes, denoted as early (t_E) and late (t_L), and the phase difference of the



Basis , bit	state	μ
Z , 0	$\lvert\varphi_0\rangle = \lvert 10\rangle$	t_E t_L
Z , 1	$\lvert\varphi_1\rangle = \lvert 01\rangle$	t_E t_L
X , 0	$\lvert\varphi_+\rangle = \frac{\lvert 10\rangle + \lvert 01\rangle}{\sqrt{2}}$	$\Delta\varphi = 0$ t_E t_L
X , 1	$\lvert\varphi_-\rangle = \frac{\lvert 10\rangle - \lvert 01\rangle}{\sqrt{2}}$	$\Delta\varphi = \pi$ t_E t_L

Figure 1 Time-phase encoding of the states

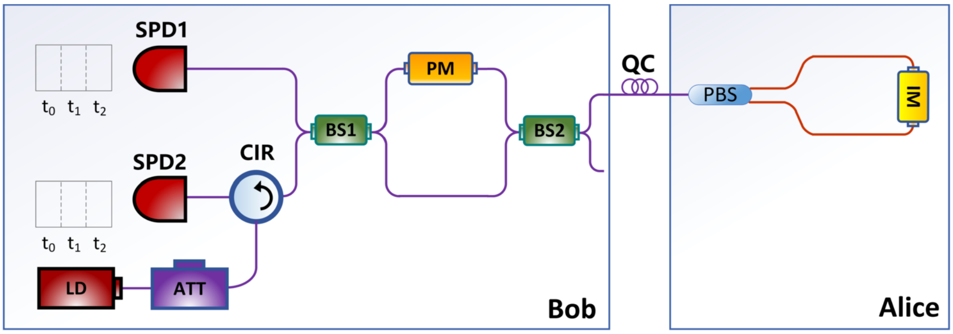


Figure 2 The scheme based on the Mirror protocol with time-phase encoding. LD: laser diode, ATT: attenuator, CIR: circulator, BS: beam splitter, PM: phase modulator, IM: intensity modulator, PBS: polarization beam splitter, QC: quantum channel, SPDs (SPD1 and SPD2): single photon detectors

two temporal modes. When the photons are located at the two different time windows, t_E and t_L, the Z basis is determined by the time window in which the photon resides, and the X basis is determined by the phase difference between the optical pulses in the two time windows. In the Z basis, if the photon is only located at the time window t_E, this situation represents $|\varphi_0\rangle$, which is encoded as "0". If it is only located in the time window t_L, this situation stands for $|\varphi_1\rangle$, which is encoded as "1". Considering the case where both photons are located on two time windows (t_E and t_L), we define it as the encoding under X basis. In the X basis, the state $|\varphi_+\rangle$ or $|\varphi_-\rangle$ is encoded as "0" or "1", depending on phase difference $\Delta\varphi = 0$ or π.

The scheme based on the Mirror protocol with time-phase encoding is as follows (see Fig. 2). The quantum Bob prepares the qubit state $|\varphi_+\rangle$ in the X basis by an unbalanced interferometer and then sends it to Alice through the quantum channel. For the qubit state $|\varphi_+\rangle$ from Bob, Alice randomly selects one of the classical operations: (1) CTRL: the intensity modulator (IM) is not operated. It also means to return $|\varphi_+\rangle$ directly; (2) SWAP-x: IM randomly modulates the intensity of one of the pulses to zero, to return the state $|\varphi_0\rangle$ or $|\varphi_1\rangle$ in the Z basis to Bob; (3) SWAP-ALL: IM modulates the intensity of both pulses to zero. Thus, Alice realizes the four classical operations by selective modulation.

When the qubit comes back to Bob again, Bob randomly measures it either in the Z or X basis. The Z basis measurement is a direct measurement of the arrival time of the photons, and the X basis is the measurement of the phase difference carried by the temporal modes. For the measurement results, the single-photon detectors (SPDs) may receive photons in the three time windows t_0, t_1, and t_2. The time pattern of the single-photon detector response is shown in Fig. 3. If the CTRL-X used for eavesdropping detection is selected by both communication parties, there is a corresponding constructive or destructive interference at the t_1 of SPD1 and SPD2. If the SWAP-x-Z used for distilling the key bits is selected, there are two cases: If SPD1 or SPD2 detects photons in the first time window t_0, the result is the "0" code in the Z basis; If SPD1 or SPD2 detects photons in the third time window t_2, the result is the "1" code in the Z basis. Finally, Bob announces the chosen basis and Alice declares "CTRL," "SWAP-x" or "SWAP-ALL" (she keeps x ∈ $\{01, 10\}$ secretly). Then, after error correction and privacy amplification, Alice and Bob both obtain the shared secure key.

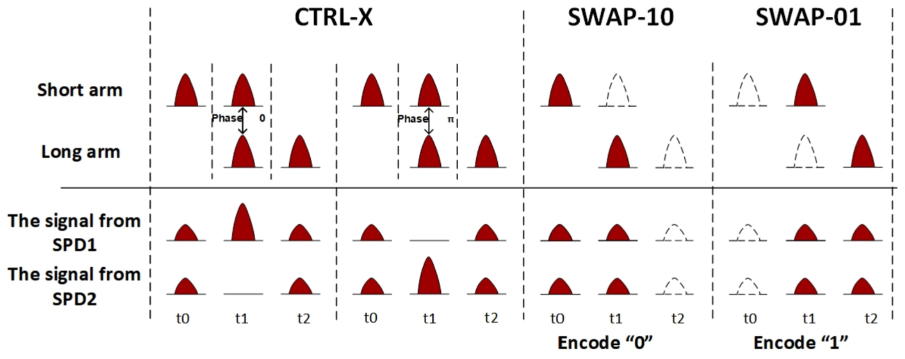


Figure 3 Time pattern of single photon detector response

4 Experimental setup

The experimental setup, which is based on the protocol and scheme mentioned in the previous section, is depicted in Fig. 4. At Bob's site, it is composed of three modules: laser source module, Mach-Zehnder Interferometer (MZI) module and detection module. And at Alice's site, there is the Sagnac loop module.

In the optical source module, the optical pulse is generated by a picosecond pulse laser (LD, manufactured by QuantumCTek, QCL-102). Its wavelength centers at 1550.15 nm, and the pulse width is 60 ps, with the system frequency of 62.5 MHz. Behind the LD, an isolator (ISO) is used to reduce the effect of reflected light. We then use a programmable attenuator (ATT) to reduce the average photon number of the optical pulse to the single-photon level. After leaving the ATT, the optical pulse enters the circulator (CIR) through the Port 1, and exits from the Port 2 into the MZI module.

The setup between two 50:50 beam splitter (BS1 and BS2) is the MZI module, which contains a short arm and a long arm. The short arm consists of a polarization-independent phase modulator (PM, manufactured by KANGGUAN, KG-PM-15-10G-PP-FP), which is driven by an electrical pulse generator (PG, manufactured by SIGLENT, SDG6052X-E) to load the phase for the second pulse in reverse transmission, and a polarization controller (PC1) that adjusts the polarization state of the backward optical pulse for PM to work in the single mode. In the long arm, there are a PC2 and a variable fiber optic attenuator (VOA). The role of the VOA is used to modify the optical attenuation of the long arm, so that the intensities of the optical pulses output from the two arms are equal. The detection module is composed of two single photon detectors (SPD1 connected to the Port 4 of BS1, SPD2 connected to the Port 3 of CIR).

At the classical site, the symmetric Sagnac loop, which is used to modulate optical pulses for classical operations, is constructed by a polarization-maintaining polarization beam splitter (PMPBS) and a polarization-maintaining IM (PMIM) [38]. PGs and SPDs are synchronized by an electrical delay generator (DG) at Bob's end.

In the SQKD experiment, the critical technical challenge is to completely implement the "CTRL-X", "SWAP-x" and "SWAP-ALL" operations. To solve this problem, we utilize the above-mentioned apparatus in combination with the method of selective modulation to continue characterizing the path of the optical pulse. Upon entering the MZI module, the optical pulse is split in two and the state $|\varphi_+\rangle$ with a time interval of $\Delta t = 5.86$ ns is prepared due to the presence of the arm length difference of $\Delta L = 119.8$ cm. For conve-

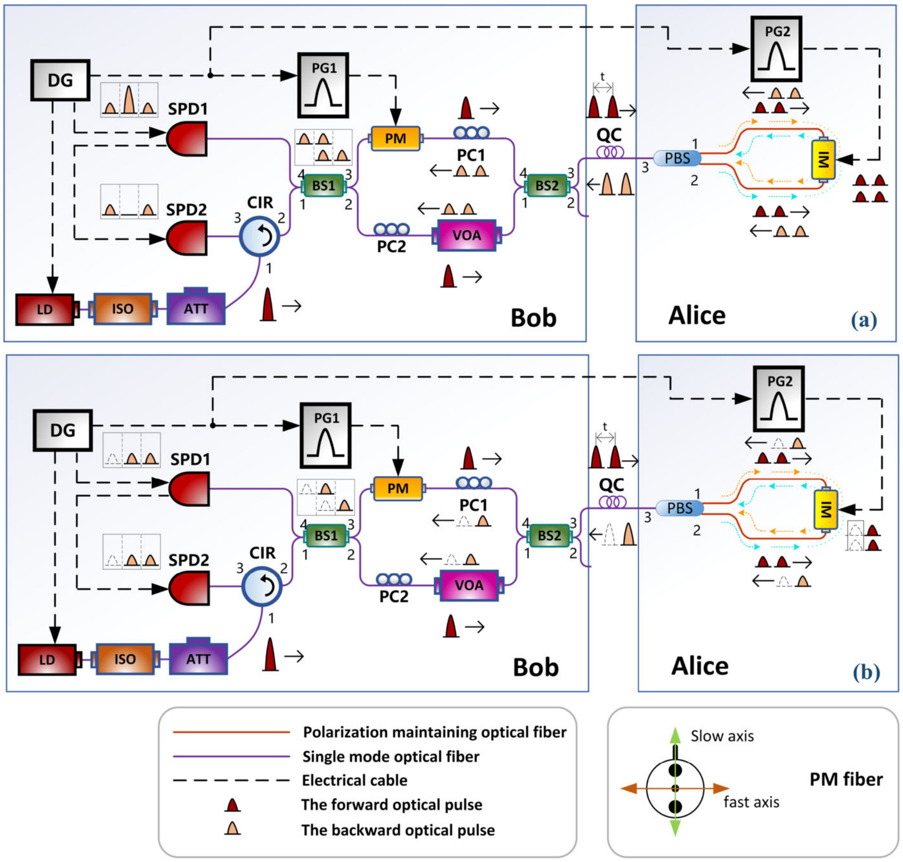

DG
PG1
PG2
SPD1
SPD2
CIR
PM
PC1
PC2
VOA
BS1
BS2
LD
ISO
ATT
QC
t
PBS
IM
Bob
Alice
(a)
(b)
1
2
3
4
Polarization maintaining optical fiber
Single mode optical fiber
Electrical cable
The forward optical pulse
The backward optical pulse
Slow axis
fast axis
PM fiber

Figure 4 (a) The forward and backward optical path of the "CTRL-X" operation. (b)The forward and backward optical path of the "SWAP-x-Z" (x ∈ {01, 10}) operation. ISO: isolator, PC: polarization controller, VOA: variable attenuator, PG: electrical pulse generator

nience of description, the optical pulses of the short and long arms are denoted as P_S and P_L, respectively. Subsequently, the optical pulses are sent to Alice via the quantum channel. After the classical operations are performed in the Sagnac loop, the optical pulses are returned to Bob via the quantum channel. Once again, they pass through the MZI module and eventually the response will occur at the SPDs.

Next, we describe in detail the implementation of the classical operations.

If Alice chooses "CTRL" operation, IM does nothing. The optical pulses (P_S and P_L) emitted from Alice are sent to Bob and are split into four pulses by BS2. Along the lines of the above representation, we record the four pulses as P_{S+S}, P_{L+L}, P_{S+L} and P_{L+S}. For example, a pulse that passes through the short arm of MZI in the forward propagation and the long arm of MZI in the backward propagation, is denoted as P_{S+L}. In the reverse optical path, PC1 adjusts the polarization of the optical pulses so that the PM works in the single mode. And the PM, which is driven by the PG1 with the repetition frequency of 62.5 MHz and the FWHM of 3.3 ns, modulate voltage 0 V or half-wave voltage $\mathrm{V}_\pi = 4.82V$ which loads the corresponding phase 0 or π on the P_{L+S} randomly. Meanwhile, by adjusting the polarization state of P_{S+L} with PC2 to the same as that of P_{L+S}, interference will occur on the second time window t_1 at BS1. The forward and backward optical path of the "CTRL-X" operation is illustrated in Fig. 4(a).

If Alice chooses “SWAP-10” (or “SWAP-01”) operation, the PG2, with the frequency of 62.5 MHz, the voltage of 6.3 V, the FWHM of 3.3 ns, and the corresponding delay of 13.8 ns (or 7.6 ns), drives IM to modulate optical pulses P_L (or P_S) reducing light intensity to be close to zero, where the extinction ratio of IM is 18.4 dB. In the backward propagation, the pulse P_S (or P_L) is then divided into two pulses by BS2. After the optical pulses are combined by BS1, SPD1 and SPD2 will have the same response probabilities. When SPD1 or SPD2 responds in the first time window t_0, the code “0” in the Z basis is obtained. When SPD1 or SPD2 responds in the third time window t_2, the code “1” in the Z basis is obtained. The forward and backward optical path of the “SWAP-01-Z” operation is illustrated in Fig. 4(b).

If Alice chooses “SWAP-ALL” operation, the PG2, with the pulse width of 7 ns, drives IM to modulate the both optical pulses P_S and P_L for reducing the intensity of light to zero and there are no photons returned to Bob.

5 Results and discussion

For the sake of the verification of experimental feasibility, we can evaluate the quantum bit error rates, which are obtained from the photon counts (within 10 mins) by the measurement of SPDs. In this proof-of-principle experiment, the employed SPDs are commercial InGaAs/InP detectors working in gated mode, with 300-ps-gate windows, 1.25-GHz repetition frequency, average dark count probability per gate of 1×10^{-6}, 50 ns dead time, and a detection efficiency of approximately 16.91%. For the “CTRL-X” operation, the PM modulates the phase difference between the two optical pulses to 0 or π so that the SPDs detect the interference signal in the second time window t_1 eventually, and the average interference contrast is 94.45% as shown in Fig. 5(a). Moreover, this position can be used to monitor noise and error rates. For “SWAP-10” and “SWAP-01”operations, IM modulates one of the two light pulses corresponding to the codes “0” and “1”, respectively. For“SWAP-ALL” operation, IM modulates both the pulses, so that no light pulses return. When the average number of photons per pulse is attenuated to $\mu = 0.1$, depending on the photon counts in different cases, we obtain the quantum bit error rate of “CTRL-X” which is 2.78%, and that of “SWAP-x-Z”which is 4.56%(see Fig. 5(b)). While the raw key rate is 69.8 kbps. It can be seen that, compared with the experiment of the SQKD protocol implemented by Gurevich [35], our experiment has better performance.

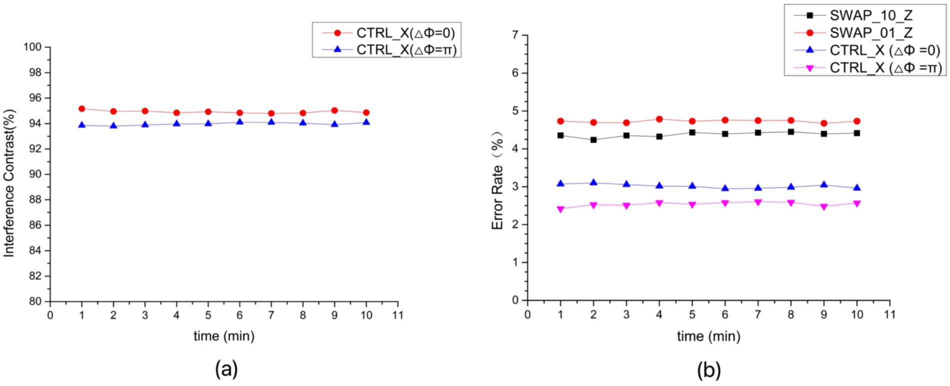


Figure 5 (a) Interference contrast corresponding to “CTRL-X” operation. (b) Error rate under different classical operations

The core of our experiment is adopting the method of selective modulation, which can take full advantage of the high-speed characteristics of the LiNbO3 intensity modulator to achieve high-speed switching among “SWAP-ALL,” “SWAP-10,” and “SWAP-01” operations. In future work, we intend to improve the secure key rate by increasing the repetition rate of the system and the detection efficiency of the SPDs. The quantum bit error rate can be reduced by increasing the extinction ratio of the IM and using lower-loss devices. Once the SQKD field breaks through in practical applications, experimental secure key rate evaluation based on weakly coherent states will be an important research topic, which is what our group will concentrate on for the next.

6 Conclusion

In conclusion, we performed the first proof-of-principle demonstration of semi-quantum key distribution based on the Mirror protocol, proving that the implementation of the Mirror protocol employing the method of selective modulation is feasible. Compared with the previous experimental version of the Mirror protocol, our experiment complements the “SWAP-ALL” classical operation, and avoids the “Full attack” and the “Weak attack”. In addition, our scheme dramatically reduces the quantum bit error rate. In this proof-of-principle experiment, we adopt the method of the selective modulation to avoid preparing identical photons. This research indicates that this method will be available for other experimental demonstration of SQKD protocols to drive the development of SQKD experiments.

In addition, it can be noted that the physical structure of QSDC [8] based on single photons has similarities with that of SQKD, such as the selection of control mode and encode mode, so our experimental approach may be applied to the implementation of QSDC based on single photons to improve its performance in the future as well.

Acknowledgements
The authors thank the Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials for provision of experimental platform. The authors also thank Dr. Zhantong Qi for discussions and suggestions.

Funding
National Science Foundation of China (61771205, 62071186); National Science Foundation of Guangdong Province (2015A030313388); Science and Technology Planning Projects of Guangdong Province (2015B010128012, 2017KZ010101).

Availability of data and materials
The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declarations

Competing interests
The authors declare that they have no competing interests.

Authors’ contributions
All authors read and approved the final manuscript.

Author details
[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, Tong Xin Road, Guangzhou 510091, China.

Received: 7 October 2021 Accepted: 9 December 2021 Published online: 20 December 2021

References

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11. https://doi.org/10.1016/j.tcs.2014.05.025.
2. Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A. 1999;59:1829. https://doi.org/10.1103/PhysRevA.59.1829.
3. Deng F-G, Zhou H-Y, Long G-L. Circular quantum secret sharing. J Phys A, Math Gen. 2006;39:14089. https://doi.org/10.1088/0305-4470/39/45/018.
4. Long G-L, Liu X-S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A. 2002;65:032302. https://doi.org/10.1103/PhysRevA.65.032302.
5. Deng F-G, Long G-L, Liu X-S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A. 2003;68:042317. https://doi.org/10.1103/PhysRevA.68.042317.
6. Deng F-G, Long G-L. Secure direct communication with a quantum one-time pad. Phys Rev A. 2004;69:052319. https://doi.org/10.1103/PhysRevA.69.052319.
7. Lin S, Wen Q-Y, Gao F, Zhu F-C. Quantum secure direct communication with χ-type entangled states. Phys Rev A. 2008;78:064304. https://doi.org/10.1103/PhysRevA.78.064304.
8. Hu J-Y, Yu B, Jing M-Y, Xiao L-T, Jia S-T, Qin G-Q, Long G-L. Experimental quantum secure direct communication with single photons. Light Sci Appl. 2016;5:e16144. https://doi.org/10.1038/lsa.2016.144.
9. Zhang W, Ding D-S, Sheng Y-B, Zhou L, Shi B-S, Quantum GG-C. Secure direct communication with quantum memory. Phys Rev Lett. 2017;118:220501. https://doi.org/10.1103/PhysRevLett.118.220501.
10. Zhu F, Zhang W, Sheng Y-B, Huang Y-D. Experimental long-distance quantum secure direct communication. Sci Bull. 2017;62:1519–24. https://doi.org/10.1016/j.scib.2017.10.023.
11. Zhou L, Sheng Y-B, Long G-L. Device-independent quantum secure direct communication against collective attacks. Sci Bull. 2020;65:12–20. https://doi.org/10.1016/j.scib.2019.10.025.
12. Sheng Y-B, Zhou L, Long G-L. One-step quantum secure direct communication. Sci Bull. 2021. https://doi.org/10.1016/j.scib.2021.11.002.
13. Qi Z-T, Li Y-H, Huang Y-W, Feng J, Zheng Y-L, Chen X-F. A 15-user quantum secure direct communication network. Light Sci Appl. 2021;10:183. https://doi.org/10.1038/s41377-021-00634-2.
14. Bennett CH, Gilles B, Crépeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett. 1993;70:1895. https://doi.org/10.1103/PhysRevLett.70.1895.
15. Bennett CH, Wiesner SJ. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys Rev Lett. 1992;62:2881. https://doi.org/10.1103/PhysRevLett.69.2881.
16. Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J. 1949;28:656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.
17. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. Phys Rev Lett. 2007;99:140501. https://doi.org/10.1103/PhysRevLett.99.140501.
18. Zou X, Qiu D, Li L, Wu L, Li L. Semiquantum-key distribution using less than four quantum states. Phys Rev A. 2009;79:052312. https://doi.org/10.1103/PhysRevA.79.052312.
19. Boyer M, Mor T. Comment on "Semiquantum-key distribution using less than four quantum states". Phys Rev A. 2011;83:046301. https://doi.org/10.1103/PhysRevA.83.046301.
20. Boyer M, Gelles R, Kenigsberg D, Mor T. Semiquantum key distribution. Phys Rev A. 2009;79:032341. https://doi.org/10.1103/PhysRevA.79.032341.
21. Boyer M, Gelles R, Kenigsberg D, Mor T. Quantum key distribution with limited classical Bob. Int J Quantum Inf. 2013;11:135005. https://doi.org/10.1142/S0219749913500056.
22. Yu K-F, Yang C-W, Liao C-H, Hwang T. Authenticated semi-quantum key distribution protocol using Bell states. Quantum Inf Process. 2014;13:1457–65. https://doi.org/10.1007/s11128-014-0740-z.
23. Krawec WO. Mediated semiquantum key distribution. Phys Rev A. 2015;91:032323. https://doi.org/10.1103/PhysRevA.91.032323.
24. Zou X, Qiu D, Zhang S, Mateus P. Semiquantum key distribution without invoking the classical party's measurement capability. Quantum Inf Process. 2015;14:2981–96. https://doi.org/10.1007/s11128-015-1015-z.
25. Li Q, Chan WH, Long D-Y. Semiquantum secret sharing using entangled states. Phys Rev A. 2010;82:022303. https://doi.org/10.1103/PhysRevA.82.022303.
26. Zou X-F, Qiu D-W. Three-step semiquantum secure direct communication protocol. Sci China, Phys Mech Astron. 2014;57:1696–702. https://doi.org/10.1007/s11433-014-5542-x.
27. Thapliyal K, Sharma RD, Pathak A. Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. Int J Theor Phys. 2018;16:1850047. https://doi.org/10.1142/S0219749918500478.
28. Krawec WO. Security proof of a semi-quantum key distribution protocol. In: IEEE ISIT. 2015. https://doi.org/10.1109/ISIT.2015.7282542.
29. Krawec WO. Security of a semi-quantum protocol where reflections contribute to the secret key. Quantum Inf Process. 2016;15:2067–90. https://doi.org/10.1007/s11128-016-1266-3.
30. Zhang W, Qiu D, Mateus P. Security of a single-state semi-quantum key distribution protocol. Quantum Inf Process. 2018;17:135. https://doi.org/10.1007/s11128-018-1904-z.
31. Krawec WO. Practical security of semi-quantum key distribution. Proc SPIE. 2018;10660:1066009. https://doi.org/10.1117/12.2303759.
32. Tan Y-G, Lu H, Cai Q-Y. Comment on "Quantum key distribution with classical Bob". Phys Rev Lett. 2009;102:098901. https://doi.org/10.1103/PhysRevLett.102.098901.
33. Boyer M, Kenigsberg D, Mor T. Boyer, Kenigsberg, and Mor reply. Phys Rev Lett. 2009;102:098902. https://doi.org/10.1103/PhysRevLett.102.098902.
34. Boyer M, Katz M, Liss R, Mor T. Experimentally feasible protocol for semiquantum key distribution. Phys Rev A. 2017;96:062335. https://doi.org/10.1103/PhysRevA.96.062335.
35. Gurevich P. Experimental Quantum Key Distribution with Classical Alice. Mastersthesis. 2013. http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-info.cgi/2013/MSC/MSC-2013-19.

36. Boyer M, Liss R, Mor T. Attacks against a simplified experimentally feasible semiquantum key distribution protocol. Entropy. 2018;20:536. https://doi.org/10.3390/e20070536.
37. Boaron A, Korzh B, Houlmann R, Boso G, Rusca D, Gray S, Li M-J, Nolan D, Martin A, Zbinden H. Simple 2.5 GHz time-bin quantum key distribution. Appl Phys Lett. 2018;112:171108. https://doi.org/10.1063/1.5027030.
38. Avesani M, Agnesi C, Stanco A, Vallone G, Villoresi P. Stable, low-error, and calibration-free polarization encoder for free-space quantum communication. Opt Lett. 2020;45:4706–9. https://doi.org/10.1364/OL.396412.