




# Quantum State Preparation for Quantum Key Distribution Using PLC Module

Dan Wu , Shaokang Chen , Pengwei Cui, Junchi Ma, Wei Chen , Jiashun Zhang, Yue Wang, Jianguang Li, and Junming An

**Abstract**—Quantum Key Distribution (QKD) is gaining significant interest due to its theoretical guarantee of unconditional security. Integrated optics offers distinct advantages compared to bulk optics, including high stability, flexibility, controllability, and robustness. We develop a planar lightwave circuit (PLC) silica asymmetric Mach-Zehnder interferometer (AMZI) module with temperature system at an accuracy of 0.1 °C including an AMZI chip with a 400ps delay and a single-chip microcomputer. The silica AMZI module is used to encode at Alice, and the same low loss AMZI module is used to decode at Bob at a clock repetition rate of 156 MHz. Two intensity states Z-basis ( $|0\rangle, |1\rangle$ ) and two phase states X-basis ( $|+\rangle, |-\rangle$ ) are prepared at Alice and detected at Bob successfully. The extinction ratio of  $|0\rangle$  and  $|1\rangle$  between first-slot and third-slot are about 17 dB. And the interference visibility of  $|+\rangle, |-\rangle$  between interference max and min of second-slot are about 88%. The estimated secret key rate and the quantum bit error rate (QBER) using a simulation model for a transmission distance of 20 km is 16.3 kbps and 0.0384, respectively.

**Index Terms**—Asymmetric Mach-Zehnder interferometer module, extinction ratio, interference visibility, key rate, planar lightwave circuit, quantum key distribution.

## I. INTRODUCTION

SECURE communication has grown in significance and is deeply ingrained in our daily lives, including the daily interactions we have over the internet, the financial transactions made via bank transfers and national security involving sensitive information. But the emergence of quantum computing has posed a significant threat to the security of conventional

Manuscript received 28 September 2023; accepted 2 October 2023. Date of publication 5 October 2023; date of current version 23 October 2023. This work was supported in part by the Innovation Program for Quantum Science and Technology under Grant 2021ZD0300701, in part by the Strategic Priority Research Program of Chinese Academy of Sciences under Grant XDB43000000, and in part by the National Key R&D Program of China under Grant 2018YFA0306403. (Corresponding authors: Jiashun Zhang; Junming An.)

Dan Wu, Pengwei Cui, Junchi Ma, and Junming An are with the State Key Laboratory on Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing 100083, China, also with the Center of Materials Science and Optoelectronics Engineering, University of Chinese Academy of Sciences, Beijing 100049, China, and also with the College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing 100049, China (e-mail: wudan@semi.ac.cn; cuipengwei@semi.ac.cn; majunchi@semi.ac.cn; junming@semi.ac.cn).

Shaokang Chen, Jiashun Zhang, Yue Wang, and Jianguang Li are with the State Key Laboratory on Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing 100083, China (e-mail: skchen@semi.ac.cn; zhangjiashun@semi.ac.cn; wy1022@semi.ac.cn; lijg@semi.ac.cn).

Wei Chen is with the Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China (e-mail: weich@ustc.edu.cn).  
Digital Object Identifier 10.1109/JPHOT.2023.3322150

cryptographic techniques. In 2022, Xu et al. pointed out that once large-scale quantum computer is constructed, conventional cryptography will fall apart. The reason is that quantum computers have powerful parallel computing capabilities that traditional computers cannot match. The fundamental unit of a quantum computer is the quantum bit, which can exist in multiple states simultaneously, unlike the binary states of 0 or 1 in classical computers. And primitive small-scale quantum computers have been built to date [1]. In 2022, Xanadu achieved a 216-photon Gaussian boson sampling experiment using their latest programmable photonic quantum computer Borealis and IBM launched the world's first 433-qubit superconducting quantum computing chip Osprey [2]. In response to the information security threats, quantum key distribution (QKD), which theoretically ensures unconditional secure communication based on the principles of quantum mechanics, has gained increasing attention. C. H. Bennett and G. Brassard proposed the important QKD protocol, now known as BB84, and the information is encoded on polarization of pulses [3]. However, polarization states are not suitable for long-distance fiber transmission due to issues such as birefringence, polarization mode dispersion, and polarization-dependent losses. Therefore, the use of polarization states is primarily limited to free-space transmission. Due to the difficulty of stable transmission of quantum states using polarization encoding in optical fibers, BB84 time-bin encoding has been rapidly developed. Time-bin states can be directly generated using fast optical modulators and transmitted over long distances in both fiber optic and free-space environments [4]. The approach allows communicate between Alice and Bob using a pair of quantum states encoded on the relative phase or intensity that are corresponding to different basis in public channels.

Traditional BB84 system relied on fiber or discrete components and indeed required significant space on an optical platform that have limited scalability and integration compatibility [5], [6]. Over the years, numerous research on integrated optical systems have been conducted. Silica planar lightwave circuits (PLC) have been firstly used for double pulse photons generation at Alice and passive interferometers at Bob [7], [8], [9], [10], [11]. And QKD experiments with different encoding methods have been recently demonstrated using transmitter fabricated in indium phosphide (InP) [12], [13], [14], Si photonic (SiP) [15], [16], [17], [18], [19] and receiver fabricated silicon nitride (SiN) [14], [20] integrated photonic platforms. The main available

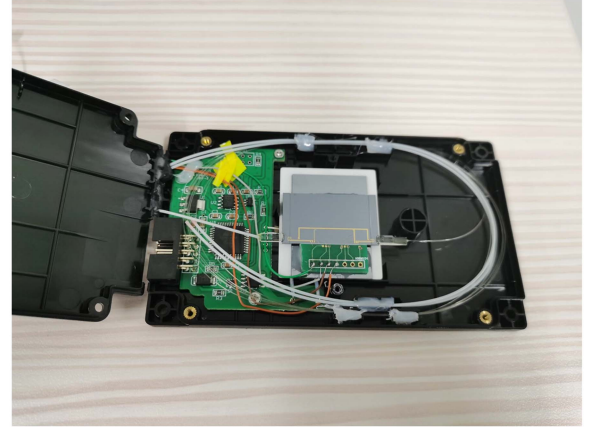
TABLE I  
MAIN INTEGRATED PHOTONICS PLATFORM [21]

Metric	Indium Phosphide	Silicon	Silicon nitride	Lithium niobate	Silica
COMS-compatible	●	●●●●●	●●●●●	●	●
All-in-one	●●●●●	●●●●	●●●	●	●
Low loss	●●●	●●●	●●●●●	●●●	●●●●●
Small size	●●●●	●●●●●	●●●●	●●	●
Polarization independent	●●●	●	●●●	●	●●●●●
RF modulation	●●●●●	●●●●	●	●●●●●	●

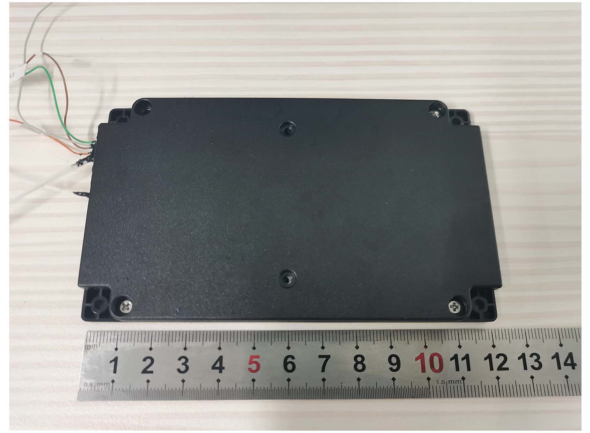
integrated photonics platform such as InP, Si, SiN, lithium niobate ( $\text{LiNbO}_3$ ) and  $\text{SiO}_2$  for quantum communication is shown in Table I [21]. Compared with other integrated photonics platform, silica waveguide chips have low loss and easy couple with fiber. So, the popular BB84 approach is that a silica asymmetric Mach-Zehnder interferometer (AMZI) connected with  $\text{LiNbO}_3$  modulator are used at Alice for encoding and the same silica AMZI at Bob is needed for decoding.

The silica PLC chips are temperature-sensitive and the full-wave temperature is only about  $2.0^\circ\text{C}$  for 400 ps delay [22]. Moreover, the thermo-optic phase modulators (TOPMs) on silica PLC chips are used to make the double pulses have balanced amplitude and adjust the relative phase of the two-pulses based on the thermo-optic effect. Therefore, maintaining the chip's operating temperature stable is crucial for the experiment. In previous PLC-based QKD system, temperature stabilization is achieved using a temperature control system external to the chip [22], [23], [24], [25]. This does not promote the enhancement of system stability and robustness.

In this article, we demonstrated QKD encoders and decoders based on a silica PLC AMZI module. Different from other design, the AMZI module is including a temperature control system with a range of  $45.0^\circ\text{C}$ – $80.0^\circ\text{C}$ . The microcontroller in the module can be programmed to achieve a temperature control accuracy of  $0.1^\circ\text{C}$ . The size of the AMZI module is  $120 \times 70 \times 10 \text{ mm}^3$ . Compared to bulk solutions, such as Stanford Research System LDC500, Chorma TEC Controllers 54100 series, et al., our co-packaged microcontroller offers a narrower temperature range, slightly lower precision, but a smaller footprint, which enhances integration and system flexibility. And considering our experimental requirements, the accuracy and the temperature range provided by our microcontroller is sufficient. Two intensity state  $|0\rangle$ ,  $|1\rangle$  and two phase state  $|+\rangle$ ,  $|-\rangle$  of BB84 time-bin encoding are prepared using the AMZI module at Alice and detected at Bob successfully. The secure key rate is obtained using a simulation model [26] about 16.3 kbps over a 20 km single-mode fiber (SMF) at a clock repetition rate of 156 MHz. After improving device performance and optimizing the process, the secure key rate will reach 370.1 kbps over a 20 km SMF.



(a)



(b)

Fig. 1. Photo of the AMZI module (a)Outside. (b)Inside.

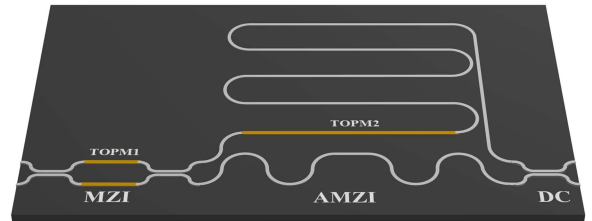


Fig. 2. Structure diagram of the AMZI chip.

## II. DESIGN AND FABRICATION

We designed and fabricate two AMZI modules, as shown in Fig. 1. The main structure of the module includes an AMZI chip, a single-chip microcomputer and a semiconductor ceramic plate. Two AMZI modules used at Alice and Bob are identical structure.

The AMZI chip is fabricated using the silica-based PLC technology. Fig. 2 shows the schematic diagram of the device. The waveguide core geometry is designed to be  $4 \mu\text{m} \times 4 \mu\text{m}$  with refractive index difference 2.0%, which can optimize coupling loss to single-mode fibers at around 1550 nm. The chip

comprises three parts, including a  $2 \times 2$  Mach-Zehnder interferometer (MZI), an AMZI with a 400 ps delay and a directional coupler (DC) with a 50:50 splitting ratio. The thermo-optic phase modulator (TOPM) in one arm of MZI and AMZI is used to set the optimum operating point for data decoding using the thermo-optic effect. The  $2 \times 2$  MZI is to adjust the power ratio of the two arms in the AMZI, which can make the output double pulses have balanced amplitude by the TOPM1. The AMZI not only is to generate double pulses, but also is to adjust the phase difference between the double pulses by the TOPM2.

The manufacturing process of the AMZI chips is as follows. First, 1050 °C thermal oxidation is used to form 16  $\mu\text{m}$  thick under-cladding, Plasma Enhanced Chemical Vapor Deposition (PECVD) is used to form 6  $\mu\text{m}$ -thick  $\text{GeO}_2\text{-SiO}_2$  core, contact exposure photolithography and Inductively Coupled Plasma (ICP) etching are used to fulfill pattern transfer. Then PECVD is used to form 20  $\mu\text{m}$ -thick BPSG upper cladding, at last thin film heaters are deposited by means of magnetron sputtering.

Next we package the chip with temperature control system. The chip is connected to the printed circuit board (PCB) with gold wires. And fiber arrays are coupled to the chip outputs using UV glue located in ultraviolet light for 5 minutes and drying box for 8 hours at 85 °C. This whole is glued on top of the semiconductor ceramic plate.

The single-chip microcomputer is driven by the power supply port at a 5V direct current (DC) voltage and used to change temperature by a thermistor. The modelling is programmed using Python. The temperature point can be set and read on computer. The current temperature can be read in real-time. The thermistor and a thermoelectric cooler (TEC) controlled with a range of 45.0 °C–80.0 °C and an accuracy of 0.1 °C are attached to the back of the semiconductor ceramic plate. And the size of the AMZI module is  $120 \times 70 \times 10 \text{ mm}^3$ . Without altering the phase, the excess loss of the two module is  $-4.2 \text{ dB}$  and  $-3.9 \text{ dB}$ , respectively. The silica PLC is polarization insensitive at a particular temperature point, as mentioned in references [22].

The long-term operation performance of the PLC module is crucial for practical QKD systems. When the module temperature and room temperature is set to 63.9 °C and 25 °C, the optical power at the output is observed for one hour, as shown in Fig. 3. Then room temperature is set to 15 °C and 10 °C at 15:50 and 16:10. In addition, the maximum wind force is activated at 16:20. Under extreme temperature and wind force changes, the optical power fluctuates about 1dBm within 4 minutes and 6 minutes. In summary, the PLC module keep stable when external environment remains unchanged; the module re-stabilizes in approximately 5 minutes when the external environment changes.

### III. EXPERIMENTAL SETUPS

In BB84 QKD system, phase-time qubit is often used, where information is encoded on amplitudes and/or relative phase of coherent double-pulses. In order to manipulate and detect photo pulse synchronously, pulse laser, programmed pulse generator (PPG) and single photon detector are synchronous by PPG's clock source. The intensity or relative phase of double pulses

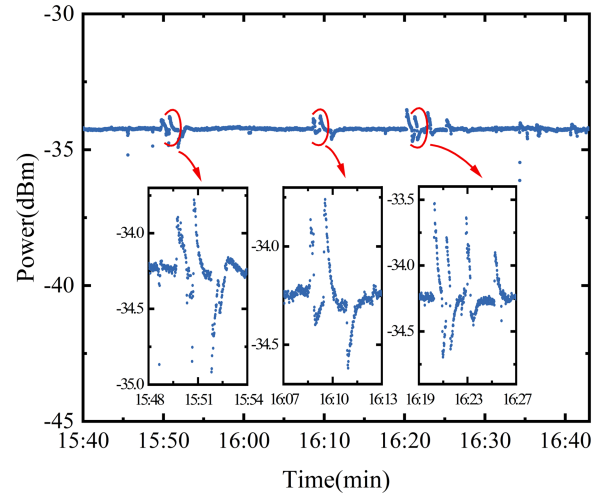


Fig. 3. PLC module stability under extreme temperature and wind force changes. The inset shows the details of the curve fluctuations.

generated by delay line in  $\text{SiO}_2$  AMZI are encoded by PPG at Alice station, and passively decoded by the other AMZI with same delay time at Bob station. The detail experiment is as following.

Typical encoder and decoder schemes are given in Fig. 4. At Alice's station, pulses from a laser diode (LD) of 1550 nm wavelength, 50 ps width and 156 MHz repetition is coupled into silica PLC AMZI module and converted to a pair of coherent double-pulses, which the time delay was set to 400 ps in order to maximally separate time-bin pulses. Then, the double-pulse entered into an optical fiber delay line (OFD),  $\text{LiNbO}_3$  phase modulator (PM) and intensity modulator (IM) in serial. The modulated codes are generated by PPG, amplified furtherly by radio frequency (RF) amplifier and applied to  $\text{LiNbO}_3$  modulator.

Then mean photons per state pulse are attenuated to less than 0.1 after varied optical attenuator (VOA). Four phase-time encoding states are shown as Fig. 5. The single pulse generated by the pulse laser is transformed into a dual pulse by the PLC module at Alice, as shown in Fig. 5(a) and (b). The intensity modulator modulates the dual pulse based on two codes generated by PPG, encoding two orthogonal states  $|0\rangle$  and  $|1\rangle$  in time-basis (Z basis), as shown in Fig. 5(c). The matching of the optical signal and the radio frequency signal is achieved by changing the delay of the optical signal using an OFD. The phase modulator also performs phase modulation on the dual pulse based on the signal generated by PPG, encoding the other two orthogonal states phase states  $0$  ( $|+\rangle$ ) and  $\pi$  ( $|-\rangle$ ) in phase-basis (X basis), as shown in Fig. 5(d). The relative phase of the two pulses is determined by scanning the amplitude of the signal.

At Bob's station, the same optical circuit as Alice's PLC-based AMZI module are used, which is a fully passive receiver without any optical modulators, followed by two single photon detectors (SPD). The dual pulse after intensity modulation and phase modulation pass through the other PLC module at Bob, as

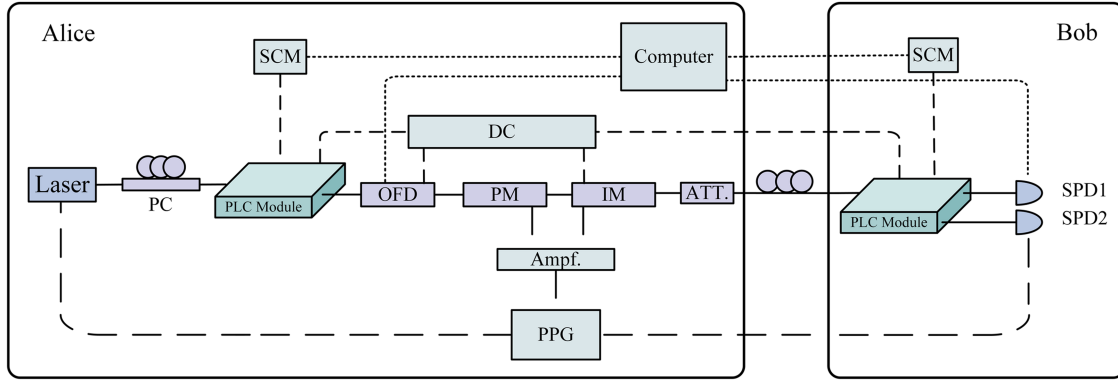


Fig. 4. Schematic of quantum state preparation for BB84. PPG, programmed pulse generator; PC, polarization controller; OFD, optical fiber delay line; SCM, single-chip microcomputer; DC, direct current source; Ampf., amplifier; PM, LiNbO<sub>3</sub> phase modulator; IM, LiNbO<sub>3</sub> intensity modulator; ATT., attenuator; SPD, single-photon detector. Solid line, long line, short line and dotted line indicate optical signal, RF signal, DC signal and USB signal, respectively.

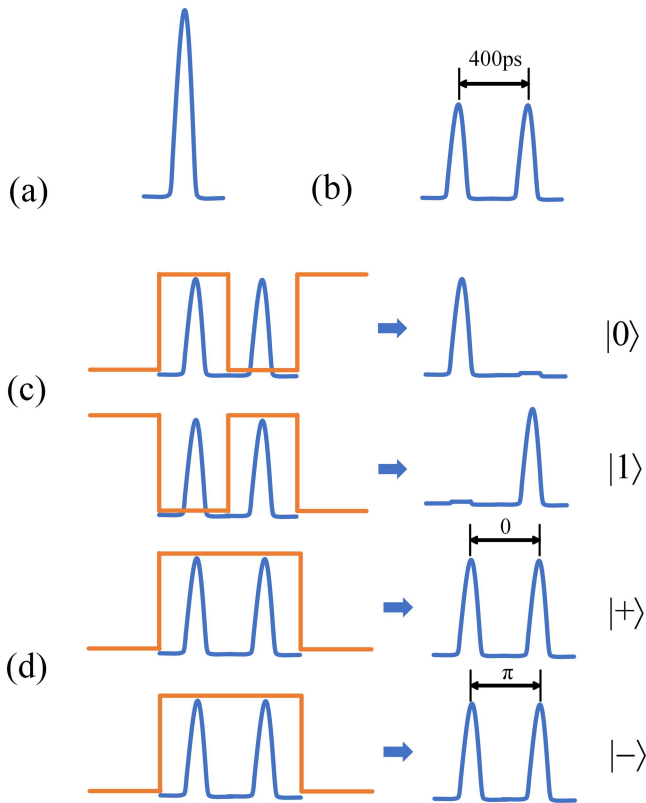


Fig. 5. Four states of BB84 phase-time encoding at Alice. (a) A pulse from pulse laser. (b) The dual pulse generated by the module. (c) The schematic diagram illustrates the intensity modulation of the dual pulse by the intensity modulator according to the codes generated by PPG. (d) The schematic diagram illustrates the intensity modulation of the dual pulse by the intensity modulator according to the codes generated by PPG. The yellow line indicates modulated codes from PPG.

shown in Fig. 6(a) and (b). Interference occurs in the second slot, where the time basis quantum states focus on the information of the first and third slots, while the phase basis quantum states focus on the second slot. The passive receiver scheme greatly simplifies the Bob construction, and also eliminates optical loss due to the modulator. The BB84 state,  $|0\rangle$ ,  $|1\rangle$ ,  $|+\rangle$ ,  $|-\rangle$ , are decoded by single photon detectors, as shown in Fig. 5.

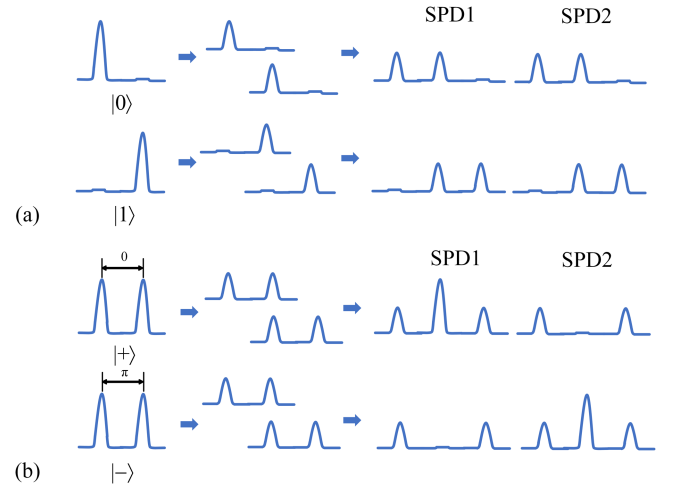


Fig. 6. Four states of BB84 phase-time decoding at Bob. (a) and (b) the dual pulse after intensity modulation and phase modulation pass through the other PLC module at Bob, generating interference peaks, respectively.

As mentioned in reference [22], operation temperature of both SiO<sub>2</sub> AMZI are controlled by temperature control system in order to obtain optimal interference visibility. The delay time should be greater than or equal to the gate width of detector, otherwise it would be challenging to distinguish the two-pulse. Considering the 400 ps-gate width of detector, we select 400 ps-delay chips to perform the following experiment. We investigate the polarization characteristics of chips for Alice and Bob separately. The InGaAs SPDs are used to record photon number per second. The jitter, detection efficiency and dark count rate is 50 ps, 8.42% and  $1 \times 10^{-5}$ /gate, respectively. The interference visibility is a function of temperature, as well as a function of the phase difference  $\Delta\varphi$  between TE and TM modes. When  $\Delta\varphi = 2N\pi$  ( $N$  is an integer), the TE and TM modes are in phase and the corresponding visibility is maximum. Therefore, we observe that TE and TM modes are in phase for Alice chip in the vicinity of 47.5 °C, while for Bob chip in the vicinity of 63.9 °C. Despite of the same design of chips, this temperature difference is notable and could be introduced by several factors

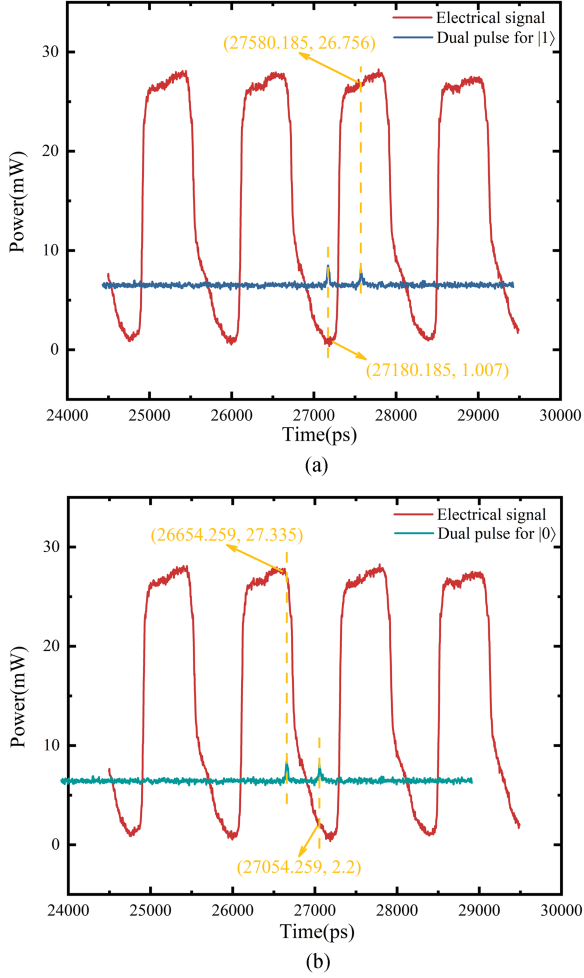


Fig. 7. Match electrical signal and optical signal for time-basis (Z basis) encoding. (a) Dual pulsed for state  $|1\rangle$  with 400 ps (blue line) and programed code generated by PPG (red line). (b) Dual pulsed for state  $|0\rangle$  with 400 ps (green line) and programed code generated by PPG (red line).

from the fabrication process, one of which could be that they are made from different silicon wafers.

#### IV. RESULT

##### A. Time Basis $|0\rangle$ and $|1\rangle$ Preparation and Detection

Regarding to time basis  $|0\rangle$  and  $|1\rangle$  (Z basis),  $\text{LiNbO}_3$  IM is used to modulate the double pulses. Fig. 7 are classic multi-photon profile recorded at high-speed oscilloscope. We need to remain first pulse and second pulse of double pulses, and eliminate second pulse and first pulse of double pulses, respectively. As shown in Fig. 7(a) blue line, double pulses with 400ps delay time are generated by  $\text{SiO}_2$  AMZI, and the period of double pulses is as the same as that of pulse laser 156 MHz. According to the delay time and period of double pulses, electrical signal are programed using PPG and the period of the low and high level signal is 600 ps. When quantum state  $|1\rangle$  of Z basis is encoded, the second pulse (or right pulse) is remained and the first pulse (or left pulse) is eliminated. So, the low and high level signal encoded by PPG are corresponding to the first pulse and

the second pulse, respectively. The matching of two signals is achieved by adjusting the OFD to move the optical signal. After matching the period between the double pulses and electrical signal, the amplified PPG encoding signals by RF amplifier are applied to  $\text{LiNbO}_3$  IM. Then the signal voltage is scanned, and when the voltage is 0.4V the first pulse is remained successfully, as shown in Fig. 8(a), where the red and green/blue lines are the stated with and without encoded by PPG, respectively.

The generation of quantum state  $|0\rangle$  also uses OFD, similar to the process described above. The delay is scanned to maximize the extinction ratio of the state  $|0\rangle$ . The matching between the electrical signal and the optical signal is depicted in Fig. 7(b), and the modulation range of  $|0\rangle$  is slightly smaller than that of  $|1\rangle$ . Therefore, the intensity of  $|0\rangle$  is slightly lower than that of  $|1\rangle$ , which agrees with the test results shown in Fig. 8(a).

The encoded single pulse is recorded by single photon detector. Where  $|0\rangle$  and  $|1\rangle$  state pulses are encoded at Alice as shown in Fig. 8(a), corresponding to only first time-slot pulse and second time-slot pulse, respectively. The peak accumulated photons per second are 3166979 and 3248223, we can infer that the mean photons are less 0.1 per pulse at frequency 156 MHz of pulse laser, which ensures that there is single output at Alice station. The decoded pulses are recorded shown as Fig. 8(b) and (c). As quantum state  $|0\rangle$  and  $|1\rangle$  time basis (Z basis), the concerned information are first-slot and third-slot, respectively.

For  $|0\rangle$  time basis, the accumulated photons per second in first-slot are 59913 and 43815 for SPD1 and SPD2, respectively. The accumulated photons per second in third-slot are 1492 and 763. For  $|1\rangle$  time basis, the accumulated photons per second in third-slot are 85224 and 49939 for SPD1 and SPD2, respectively. The accumulated photons per second in first-slot are 1554 and 734. It can be inferred that the extinction ratio of counts between first-slot and third-slot for  $|0\rangle$  and  $|1\rangle$  are 16.63 dB and 17.71 dB, respectively.

For  $|1\rangle$  time basis, SPD1 detects significantly more photons compared to SPD2. This is due to polarization sensitivity of system caused by the  $\text{LiNbO}_3$  IM and  $\text{LiNbO}_3$  PM. In the next experimental, we will attempt to reduce the polarization sensitivity of the system, such as using polarization-maintaining fiber to replace the current fiber.

The pulse widths measured using the oscilloscope and SPD are different, as shown in Figs. 7 and 8, being 50ps and 250ps respectively. And the oscilloscope has a sampling bandwidth of 40GS/s. The main reason for the difference is the time jitter of the SPDs.

##### B. Phase Basis $|+\rangle$ and $|-\rangle$ Preparation and Detection

Regarding to two phase basis  $|+\rangle$  and  $|-\rangle$  (X basis), the related phases between double pluses are modulated as 0 and  $\pi$  by  $\text{LiNbO}_3$  PM, respectively. The relative phase of the two pulses is determined by scanning the signal amplitude generated by the PPG applied to the PM. The output three time-slot pulse signals are fiber coupled and measured with InGaAs SPADs. The phase decoding AMZI overlaps successive time-bins creating three possible time-slots. Phase information is interfered in the middle time-slot allowing measurements the  $|+\rangle$  and  $|-\rangle$  basis.

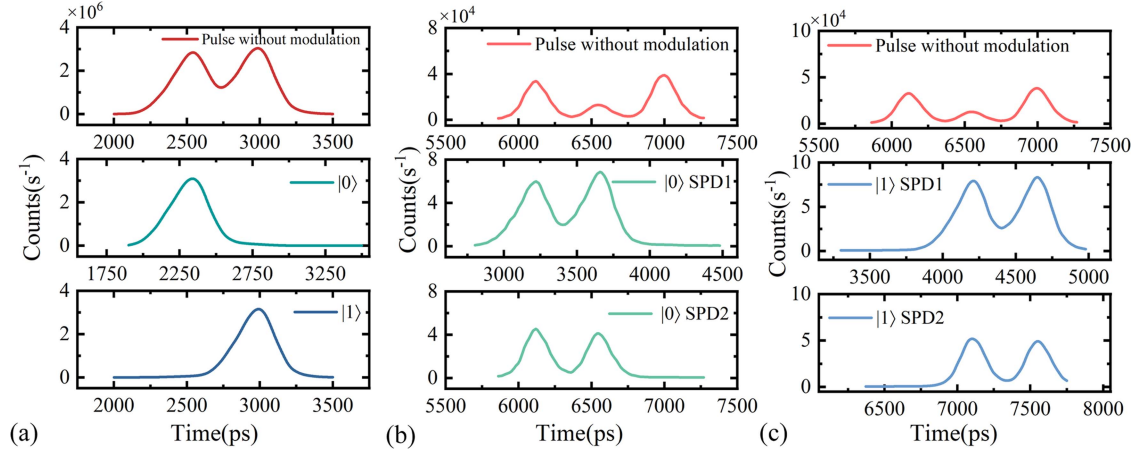


Fig. 8.  $|0\rangle$  and  $|1\rangle$  (Z basis) quantum state encoding and decoding profile. (a) Output at Alice. (b) Output1 at Bob. (c) Output2 at Bob.

The output accumulated photons of middle time slot per second varies with PPG voltage. It can be seen that the related phase between double pulses is 0 or  $\pi$  when the voltage of PPG are 0.1 V and 0.4 V, respectively.

So, we select PPG voltage 0.1 V and 0.4 V to apply to LiNbO3 PM through RF amplifier. The detected photon counts of three time-slot are shown Fig. 9. Fig. 9 shows the interference diagrams at the two voltages relative phases is 0 and  $\pi$ , corresponding to maximum interference and minimum interference, respectively. When the voltage is 0.1 V, corresponding to 0 related phase, quantum state  $|+\rangle$  is prepared, the counts per second in the second slot are 101845 and 6224 at output1 and output2, respectively. When the voltage is 0.4 V, corresponding to  $\pi$  related phase, quantum state  $|-\rangle$  is prepared, the counts per second in the second slot are 6440 and 109977 at output1 and output2, respectively. And the width of the middle slots is 50 ps but the reason for the larger size in Fig. 9 is the low resolution of the SPDs. The interference visibility,  $V = (\text{Max}-\text{Min})/(\text{Max}+\text{Min})$ , is 88.48% and 88.94% at quantum states  $|+\rangle$  and  $|-\rangle$ , respectively.

The accumulated photons per second in the first-slot recorded by SPD1 is close to that in the third-slot, but this is not the case for SPD2. Moreover, it is not possible to adjust TOPM1 on DC of AMZI at Bob to make the photons balance in the two slots for SPD1 and SPD2. This leads to low interference visibility. The reason comes from that the DC after AMZI at Bob is not perfectly 3 dB. The following content will explain in detail by calculating the ratio of the photons in the first-slot and third-slot for SPD2 when the photons in first-slot and third-slot are equal for SPD1. First, the photon passing through the long arm of two AMZI and the short arm are  $N_l$  and  $N_s$ , respectively. For the quantum state  $|+\rangle$ , when the splitting ratio of the DC after AMZI is 60:40, the photon number per second in first-slot and third-slot for SPD1 is  $60\%N_l$  and  $40\%N_s$ , while the photon number per second in first-slot and third-slot for SPD2 is  $40\%N_l$  and  $60\%N_s$ . By readjusting the TOPM1 on DC of AMZI at Bob to ensure that the photon in the two slots of SPD1 are equal, so  $60\%N_l = 40\%N_s$  and  $N_s : N_l = 60:40$  can be obtained. Therefore, the

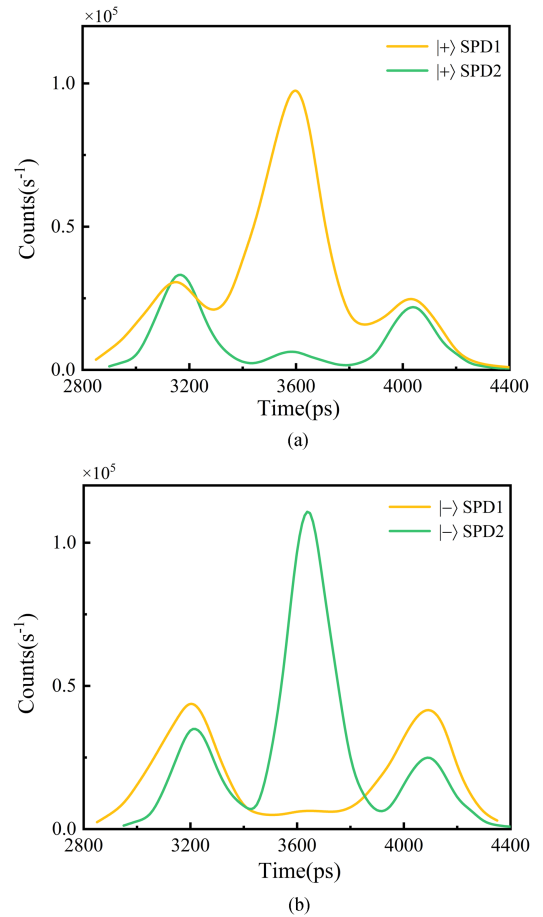


Fig. 9. Phase 0 ( $|+\rangle$ ) and  $\pi$  ( $|-\rangle$ ) accelerated counts per second of three time slot. (a) Phase = 0 at  $V = 0.1\text{V}$ . (b) Phase =  $\pi$  at  $V = 0.4\text{V}$ .

photons per second in first-slot and third-slot for SPD2 is 32:72. It follows that when the photons in first-slot and in third-slot for SPD1 is in equilibrium, the photons balance for SPD2 becomes worse, which well explains the experimental results in Fig. 9(a) and (b).

The aforementioned principle applies equally to the difference of extinction ratios for quantum states  $|0\rangle$  and  $|1\rangle$  in Fig. 8(b) and (c). The photons of state  $|0\rangle$  in the first-slot and the second-slot is significantly more different than state  $|1\rangle$  for SPD1 and SPD2, as shown in Fig. 8(b) and (c). Therefore, the extinction ratio of state  $|0\rangle$  is lower.

### C. Asymptotic Secure Key Analysis

The absence of codes in the experiment are not randomized, therefore we use a security proof to analyze the key rate per pulse [26]. Firstly, the raw key generation rate  $R$  is given by [11]

$$R = \frac{1}{2}F \left[ \mu 10^{\frac{(\alpha + \gamma_{Bob})}{10}} \eta + P_d \right] \quad (1)$$

where  $F = 156$  MHz is a repetition frequency of optical pulses,  $\mu$  is an average photo number,  $\alpha = 0.2$  dB/km is the loss coefficient of single mode fiber,  $l$  is the fiber length,  $\gamma_{Bob}$  is the loss of Z basis,  $\eta = 0.0842$  is the efficiency of SPD (measured) and  $P_d = 1.0 \times 10^{-5}$  is a dark count rate. Then the achieved key rate per pulse is described as [16]

$$K_{BB84} = \frac{1}{2}R[1 - f(\varepsilon)H_2(\varepsilon) - H_2(\varepsilon_{ph})] \quad (2)$$

where the binary Shannon entropy gives

$$H_2(\varepsilon) = -\varepsilon \log_2(\varepsilon) - (1-\varepsilon) \log_2(1-\varepsilon) \quad (3)$$

$\varepsilon$  is the quantum bit error rate (QBER) observed in the test and  $f(\varepsilon) = 1.22$  parametrizes the inefficiency of the error correction used to perform key reconciliation. And  $\varepsilon_{ph}$  is a function of  $\varepsilon$  given by

$$\begin{aligned} \varepsilon_{ph} = & \varepsilon + 4\Delta'(1 - \Delta')(1 - 2\varepsilon) \\ & + 4(1 - 2\Delta')\sqrt{\Delta'(1 - \Delta')\varepsilon(1 - \varepsilon)} \end{aligned} \quad (4)$$

where

$$\Delta' = \Delta/R_0 = \frac{1}{2R_0} (1 - e^{-\mu/2} (\cos(\mu/2) + \sin(\mu/2))) \quad (5)$$

And  $R_0$  refers to the  $R$  at 0 km. The following equation is used to calculate the  $\varepsilon$ :

$$\varepsilon = QBER_{opt} + QBER_{det} \quad (6)$$

The first one can be considered as a measured of the optical quality of the set up and given by

$$\begin{aligned} QBER_{opt} = & \frac{1}{2}QBER_{phase} + \frac{1}{2}QBER_{time} \\ = & \frac{1}{2} \cdot \frac{1 - V}{2} + \frac{1}{2} \cdot \frac{1}{10^{ER/10} + 1} \end{aligned} \quad (7)$$

where  $V$  is the measured interference visibility and  $ER$  is the time-bin extinction ratio. The second one depends entirely on the ratio of the dark-count rate to the quantum efficiency, which is given by

$$QBER_{det} = \frac{p_{dark}n}{2 \cdot 10^{(\alpha + \gamma_{Bob}/10)} \eta \mu} \quad (8)$$

where  $p_{dark} = 3 \times 10^{-6}$ /gate is the probability of recoding a dark count per time gate and per detector and  $n = 2$  is the number of

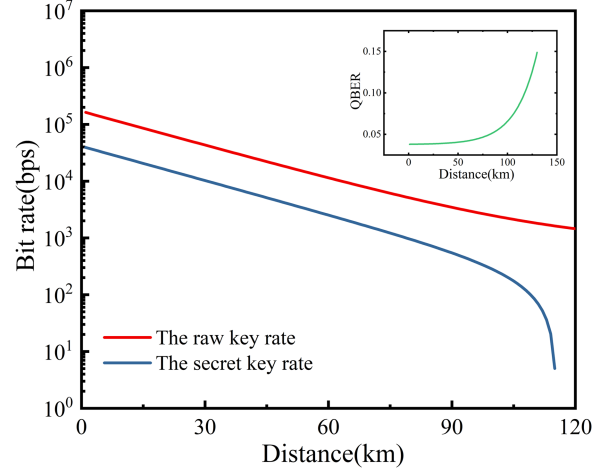


Fig. 10. Estimated asymptotic secret key rate and QBER.

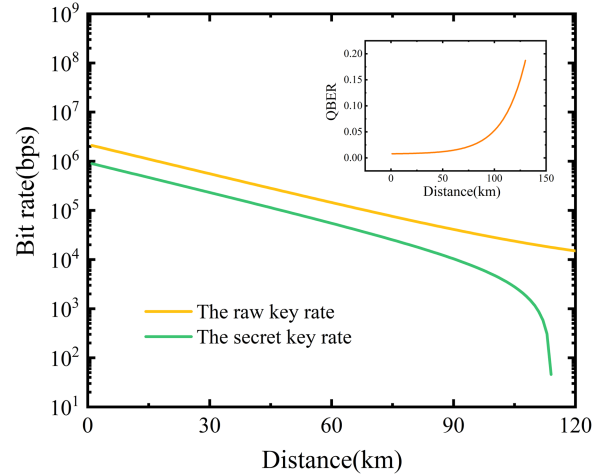


Fig. 11. Estimated asymptotic secret key rate and QBER after improving the system repetition frequency, chip loss and extinction ratio and interference visibility.

detectors. Based on the measurement results we have simulated the raw key rate  $R$ , secret key rate  $K_{BB84}$  and  $QBER$  as a function of transmission distance, as shown in Fig. 10. The raw key rate, secret key rate and the  $QBER$  for a transmission distance of 20 km is 68.1 kbps, 16.3 kbps and 0.0384, respectively.

Our current laboratory setup is constrained by a system repetition frequency of 156 MHz and a detection efficiency of single photon detector of 8.42%. These limitations reduce both the raw key rate and the secret key rate. In addition, the loss of AMZI (Mach-Zehnder Interferometer) chip at Bob's end substantially affects the key rate. To address this, we are actively working on enhancing the coupling efficiency and minimizing the loss. This will involve a detailed review and improvement of the design and manufacturing process of the chip. Furthermore, the design of the DC structure is refined because the imperfect 3 dB DC reduces the extinction ratio and interference visibility of the quantum state. This includes adjusting parameters like the length and gap of the DC to optimize its performance. By improving the extinction ratio and interference visibility, we expect to see a significant enhancement in the system's overall efficiency.

According to the current manufacturing level and equipment, the system repetition frequency can reach 1.25 GHz, and the loss can be as low as 4 dB. In the same time, when the DC is perfect 3 dB, the extinction ratio and interference visibility will be up to 20 dB and 99%. Under these conditions, we estimated the raw key rate, secret key rate and the QBER for a transmission distance of 20 km is 879.6 kbps, 370.1 kbps and 0.00858, respectively. The results are shown in the Fig. 11.

## V. CONCLUSION

We demonstrated the PLC AMZI module with temperature control system at an accuracy of 0.1 °C is used at Alice for double pulses generation, at Bob for passive decoding at a clock repetition frequency of 156 MHz. It suggests that this module possesses significant practical and commercial worth. LiNbO3 IM and PM are used as time-basis generation and phase-basis generation at Alice, respectively. The quantum states  $|0\rangle$ ,  $|1\rangle$ ,  $|+\rangle$ ,  $|-\rangle$  are prepared successfully. The extinction ratio of  $|0\rangle$  and  $|1\rangle$  are 16.63 dB and 17.71 dB, respectively. The interference visibility of  $|+\rangle$  and  $|-\rangle$  is 88.48% and 88.94%, respectively. The asymptotic estimated secret key rate and the QBER for a transmission distance of 20 km is 16.3 kbps and 0.0384, respectively. The key rate can be improved by increasing the repetition frequency of the system, the loss of AMZI chip at Bob, the extinction ratio of the time basis and the interference visibility of the phase basis in the next experiments. We believe that these changes will lead to a substantial improvement in both the raw and secret key rates, thereby boosting the overall performance of our system.

## ACKNOWLEDGMENT

The authors would like to thank Jin You for their help in module fabrication.

## REFERENCES

- [1] F. Xu et al., "Secure quantum key distribution with realistic devices," *Rev. Modern Phys.*, vol. 92, no. 2, May 2020, Art. no. 025002, doi: [10.1103/RevModPhys.92.025002](https://doi.org/10.1103/RevModPhys.92.025002).
- [2] L. S. Madsen et al., "Quantum computational advantage with a programmable photonic processor," *Nature*, vol. 606, no. 7912, pp. 75–81, Jun. 2022, doi: [10.1038/s41586-022-04725-x](https://doi.org/10.1038/s41586-022-04725-x).
- [3] C. H. Bennett et al., "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, Jan. 1992, doi: [10.1007/BF00191318](https://doi.org/10.1007/BF00191318).
- [4] F. Bouchard et al., "Quantum communication with ultrafast time-bin qubits," *PRX Quantum*, vol. 3, no. 1, Feb. 2022, Art. no. 010332, doi: [10.1103/PRXQuantum.3.010332](https://doi.org/10.1103/PRXQuantum.3.010332).
- [5] C. Gobby et al., "Quantum key distribution over 122km of standard telecom fiber," *Appl. Phys. Lett.*, vol. 89, no. 19, pp. 3762–3764, 2004, doi: [10.1063/1.1738173](https://doi.org/10.1063/1.1738173).
- [6] L. Achatz et al., "Simultaneous transmission of hyper-entanglement in three degrees of freedom through a multicore fiber," *NPJ Quantum Inf.*, vol. 9, no. 1, May 2023, Art. no. 45, doi: [10.1038/s41534-023-00700-0](https://doi.org/10.1038/s41534-023-00700-0).
- [7] G. Bonfrate et al., "Asymmetric Mach-Zehnder germano-silicate channel waveguide interferometers for quantum cryptography systems," *Electron. Lett.*, vol. 37, no. 13, pp. 846–847, Jun. 2001, doi: [10.1049/el:20010508](https://doi.org/10.1049/el:20010508).
- [8] Y. Nambu et al., "BB84 quantum key distribution system based on silica-based planar lightwave circuits," *Japanese J. Appl. Phys.*, vol. 43, no. 8B, pp. L1109–L1110, Jul. 2004, doi: [10.1143/JJAP.43.L1109](https://doi.org/10.1143/JJAP.43.L1109).
- [9] A. Tanaka et al., "Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization," *Opt. Exp.*, vol. 16, no. 15, pp. 11354–11360, Jul. 2008, doi: [10.1364/OE.16.011354](https://doi.org/10.1364/OE.16.011354).
- [10] Y. Nambu et al., "Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit," *J. Modern Opt.*, vol. 55, no. 12, pp. 1953–1970, Jul. 2008, doi: [10.1080/09500340801942414](https://doi.org/10.1080/09500340801942414).
- [11] A. Tanaka et al., "High-speed quantum key distribution system for 1-Mbps real-time key generation," *IEEE J. Quantum Electron.*, vol. 48, no. 4, pp. 542–550, Apr. 2012, doi: [10.1109/JQE.2012.2187327](https://doi.org/10.1109/JQE.2012.2187327).
- [12] A. Trenti et al., "On-chip quantum communication devices," *J. Lightw. Technol.*, vol. 40, no. 23, pp. 7485–7497, Dec. 2022, doi: [10.1109/JLT.2022.3201389](https://doi.org/10.1109/JLT.2022.3201389).
- [13] B. Zhang et al., "High performance InGaAs/InP single-photon avalanche diode using DBR-metal reflector and backside micro-lens," *J. Lightw. Technol.*, vol. 40, no. 12, pp. 3832–3838, Jun. 2022, doi: [10.1109/JLT.2022.3153455](https://doi.org/10.1109/JLT.2022.3153455).
- [14] P. Sibson et al., "Chip-based quantum key distribution," *Nature Commun.*, vol. 8, no. 1, Feb. 2017, Art. no. 13984, doi: [10.1038/ncomms13984](https://doi.org/10.1038/ncomms13984).
- [15] J. W. Silverstone, D. Bonneau, J. L. O'Brien, and M. G. Thompson, "Silicon quantum photonics," *IEEE J. Sel. Top. Quantum Electron.*, vol. 22, no. 6, pp. 390–402, Nov./Dec. 2016, doi: [10.1109/JSTQE.2016.2573218](https://doi.org/10.1109/JSTQE.2016.2573218).
- [16] P. Sibson et al., "Integrated silicon photonics for high-speed quantum key distribution," *Optica*, vol. 4, no. 2, pp. 172–177, Feb. 2017, doi: [10.1364/OPTICA.4.000172](https://doi.org/10.1364/OPTICA.4.000172).
- [17] W. Geng et al., "Stable quantum key distribution using a silicon photonic transceiver," *Opt. Exp.*, vol. 27, no. 20, pp. 29045–29054, Sep. 2019, doi: [10.1364/OE.27.029045](https://doi.org/10.1364/OE.27.029045).
- [18] K. Wei et al., "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," *Phys. Rev. X*, vol. 10, no. 3, Aug. 2020, Art. no. 031030, doi: [10.1103/PhysRevX.10.031030](https://doi.org/10.1103/PhysRevX.10.031030).
- [19] R. Sax et al., "High-speed integrated QKD system," *Photon. Res.*, vol. 11, no. 6, pp. 1007–1014, Jun. 2023, doi: [10.1364/PRJ.481475](https://doi.org/10.1364/PRJ.481475).
- [20] E. Murray et al., "Quantum photonics hybrid integration platform," *Appl. Phys. Lett.*, vol. 107, no. 17, Oct. 2015, Art. no. 171108, doi: [10.1063/1.4935029](https://doi.org/10.1063/1.4935029).
- [21] A. Orioux et al., "Recent advances on integrated quantum communications," *J. Opt.*, vol. 18, no. 8, Jul. 2016, Art. no. 083002, doi: [10.1088/2040-8978/18/8/083002](https://doi.org/10.1088/2040-8978/18/8/083002).
- [22] X. Li et al., "Interference at the single-photon level based on silica photonics robust against channel disturbance," *Photon. Res.*, vol. 9, no. 2, pp. 222–228, Feb. 2021, doi: [10.1364/PRJ.406123](https://doi.org/10.1364/PRJ.406123).
- [23] M. Ren et al., "Single-photon interference using silica-based AMZI with phase modulation," *Opt. Laser Technol.*, vol. 122, Feb. 2020, Art. no. 105837, doi: [10.1016/j.optlastec.2019.105837](https://doi.org/10.1016/j.optlastec.2019.105837).
- [24] G. Zhang et al., "Polarization-insensitive interferometer based on a hybrid integrated planar light-wave circuit," *Photon. Res.*, vol. 9, no. 11, pp. 2176–2181, Nov. 2021, doi: [10.1364/PRJ.432327](https://doi.org/10.1364/PRJ.432327).
- [25] G. Zhang et al., "Polarization-insensitive quantum key distribution using planar lightwave circuit chips," *Sci. China Inf. Sci.*, vol. 65, no. 10, Aug. 2022, Art. no. 200506, doi: [10.1007/s11432-022-3514-3](https://doi.org/10.1007/s11432-022-3514-3).
- [26] H. K. Lo et al., "Security of quantum key distribution using weak coherent states with nonrandom phases," *Quantum Inf. Computation*, vol. 7, no. 5-6, pp. 431–458, Jan. 2007, doi: [10.48550/arXiv.quant-ph/0610203](https://doi.org/10.48550/arXiv.quant-ph/0610203).