

Multi-protocol quantum key distribution decoding chip

Chun-Xue Zhang(张春雪), Jian-Guang Li(李建光), Yue Wang(王玥), Wei Chen(陈巍), Jia-Shun Zhang(张家顺), and Jun-Ming An(安俊明)

Citation: Chin. Phys. B, 2025, 34 (**5**): 050303. DOI: 10.1088/1674-1056/adb686
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Free-space discrete-variable quantum key distribution in a mountainous environment

Xing-Ran Chen(陈星燃), Jian-Hong Shi(史建红), and Hai-Long Zhang(张海龙)
Chin. Phys. B, 2025, 34 (**5**): 050301. DOI: 10.1088/1674-1056/adbd25

Effect of pseudo-random number on the security of quantum key distribution protocol

Xiao-Liang Yang(杨晓亮), Yu-Qing Li(李毓擎), and Hong-Wei Li(李宏伟)
Chin. Phys. B, 2025, 34 (**2**): 020301. DOI: 10.1088/1674-1056/ad99c9

Multi-protocol relay chaining for large-scale quantum key distribution networks

Yuan Cao(曹原), Xiaosong Yu(郁小松), Yongli Zhao(赵永利), Chunhui Zhang(张春辉), Xingyu Zhou(周星宇), Jie Zhang(张杰), and Qin Wang(王琴)
Chin. Phys. B, 2025, 34 (**1**): 010310. DOI: 10.1088/1674-1056/ad9018

Security analysis of satellite-to-ground reference-frame-independent quantum key distribution with beam wandering

Chun Zhou(周淳), Yan-Mei Zhao(赵燕美), Xiao-Liang Yang(杨晓亮), Yi-Fei Lu(陆宜飞), Yu Zhou(周雨), Xiao-Lei Jiang(姜晓磊), Hai-Tao Wang(汪海涛), Yang Wang(汪洋), Jia-Ji Li(李家骥), Mu-Sheng Jiang(江木生), Xiang Wang(汪翔), Hai-Long Zhang(张海龙), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2024, 33 (**8**): 080306. DOI: 10.1088/1674-1056/ad51f6

A new quantum key distribution resource allocation and routing optimization scheme

Lin Bi(毕琳), Xiaotong Yuan(袁晓同), Weijie Wu(吴炜杰), and Shengxi Lin(林升熙)
Chin. Phys. B, 2024, 33 (**3**): 030309. DOI: 10.1088/1674-1056/ad2503

SPECIAL TOPIC — Quantum communication and quantum network

Multi-protocol quantum key distribution decoding chip

Chun-Xue Zhang(张春雪)[1,3], Jian-Guang Li(李建光)[1], Yue Wang(王玥)[1], Wei Chen(陈巍)[4], Jia-Shun Zhang(张家顺)[1,2,3,†], and Jun-Ming An(安俊明)[1,2,3,‡]

[1] *Key Laboratory of Optoelectronic Materials and Devices, Institute of Semiconductors, Chinese Academy of Sciences, Beijing* 100083, *China*
[2] *Center of Materials Science and Optoelectronics Engineering, University of Chinese Academy of Sciences, Beijing* 100049, *China*
[3] *College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing* 100049, *China*
[4] *Hefei National Laboratory, University of Science and Technology of China, Hefei* 230088, *China*

(Received 5 December 2024; revised manuscript received 12 February 2025; accepted manuscript online 17 February 2025)

Quantum key distribution (QKD) is a method for secure communication that utilizes quantum mechanics principles to distribute cryptographic keys between parties. Integrated photonics offer benefits such as compactness, scalability, energy efficiency and the potential for extensive integration. We have achieved BB84 phase encoding and decoding, time-bin phase QKD, and the coherent one-way (COW) protocol on a planar lightwave circuit (PLC) platform. At the optimal temperature, our chip successfully prepared quantum states, performed decoding and calculated the secure key rate of the time-bin phase-decoding QKD to be 80.46 kbps over a 20 km transmission with a quantum bit error rate (QBER) of 4.23%. The secure key rate of the COW protocol was 18.18 kbps, with a phase error rate of 3.627% and a time error rate of 0.377%. The uniqueness of this technology lies in its combination of high integration and protocol flexibility, providing an innovative solution for the development of future quantum communication networks.

Keywords: quantum key distribution (QKD), secure key rate, decoding chip, quantum bit error rate

PACS: 03.67.Dd, 42.82.Et, 42.82.Bq, 03.67.Hk

DOI: 10.1088/1674-1056/adb686 **CSTR:** 32038.14.CPB.adb686

1. Introduction

Quantum key distribution (QKD) stands as a cornerstone within the realm of quantum information science, leveraging the fundamental principles of quantum mechanics to realize secure communication.[1] The concept of QKD was first proposed by Charles H. Bennett and Gilles Brassard in 1984 and is known as the BB84 protocol.[2] In this protocol, Alice initially encodes a series of photons. Bob, choosing a measurement basis, decodes these photons. The protocol incorporates a critical security measure: the calculation of the quantum bit error rate (QBER) and the key rate, which allows Alice and Bob to detect the presence of any eavesdropper. This process effectively ensures the confidentiality of the transmitted information, making QKD a cornerstone of secure communication systems.[3]

Traditional bulk optical components encounter substantial hurdles in constructing sophisticated interference structures and achieving large-scale integration.[4–9] To surmount these limitations, an effective strategy involves embracing integrated photonic devices on a chip.[10–17] These integrated photonic devices confer benefits like compact size and straightforward integration. They can integrate a large number of optical components, such as waveguides, splitters, modulators, etc., on the same chip, thus achieving complex optical functions.[18] The first QKD experiment using a waveguide interferometer was reported in 2004.[19] Photonic integrated circuits are harmonious with CMOS technology, thereby potentially reducing costs, enhancing efficiency, and augmenting both reliability and scalability, making them a promising solution for large-scale quantum communication systems.[20]

Researchers have studied the key technologies of QKD based on different photonic integrated platforms, such as silicon dioxide planar lightwave circuits (PLCs),[21–23] silicon-on-insulators[24–30] and InP,[31,32] and achieved significant results. Chips crafted from silica waveguides showcase minimal coupling loss when interfaced with optical fibers and exhibit low transmission loss within the waveguides themselves, rendering them highly suitable for fabricating low-loss quantum asymmetric Mach–Zehnder interferometers (AMZIs). As a result, silica-based platforms have become the preferred choice for producing passive photonic chips, which motivated our selection of the PLC platform for this study.[33]

In this paper, we present a decoding chip that can work with various quantum protocols, based on a silica PLC platform with a 2.0% index contrast. Within this chip, we employ variable optical splitters (VOSs) for selecting different protocols and balancing the optical power entering the two arms of the AMZI with a 400 ps delay. This innovative approach facil-

†Corresponding author. E-mail: zhangjiashun@semi.ac.cn
‡Corresponding author. E-mail: junming@semi.ac.cn

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

itates dynamic adjustment of the interferometer's input conditions, allowing the system to adapt to diverse quantum communication protocols and optimize performance according to their specific requirements. By finely tuning the distribution of light between the AMZI's paths, we can ensure optimal interference conditions. This flexibility enhances the chip's versatility, making it suitable for a wide range of applications in QKD and other quantum information processing tasks. This multi-protocol decoding chip is suitable for the BB84 phase encoding and decoding protocol,[34] time-bin phase encoding and decoding QKD,[35] and the coherent one-way (COW) protocol.[36] This innovative design integrates multiple quantum communication protocols into a single chip, providing quantum communication systems with a high degree of flexibility and performance advantages. We also conducted a detailed calculation of the secure key rates of the developed silicon dioxide multi-protocol decoding chip under different protocols. By optimizing the working temperature and experimental steps, we successfully calculated the secure key rates, providing crucial support for the security and efficiency of quantum communication systems. By implementing multiple protocols on a single chip, our decoding chip not only meets the diverse needs of quantum communication but also significantly reduces system complexity and costs. The uniqueness of this technology lies in its combination of high integration and protocol flexibility, providing an innovative solution for the development of future quantum communication networks.

2. Setup

Figures 1(a) and 1(b) depict the schematic diagrams of the chip, while Fig. 1(c) shows the physical layout of the chip after coupling wire bonding, and Fig. 1(d) shows decoding chip layout. Our decoding chip has a length of 3 cm, a width of 1.2 cm and the delay line length is 8.244 cm. The chips were fabricated on a silica PLC platform with a refractive index contrast of 2.0%. The VOS has a waveguide separation of 100 μm, and the bending radii are set to 2.4 mm. In the coupling region, the gap between the waveguides is 2 μm, with a coupling length of 370 μm. The modulated arm, which plays a crucial role in signal modulation, has a length of 2000 μm. Additionally, the chip incorporates a directional coupler with a 50:50 splitting ratio, providing balanced power division between the waveguides.

In phase encoding and decoding, the quantum state $|\varphi\rangle = |0\rangle + e^{i\Delta\phi}|1\rangle$ is represented as the superposition state of a single photon appearing in the first and second time slots. Here, $\Delta\phi$ denotes the phase difference between these two time slots. 0 and π form a set of orthogonal bases, referred to as the X basis; $\pi/2$ and $3\pi/2$ form another set of orthogonal bases, referred to as the Y basis. Figure 2(a) depicts the journey of single photon as it traverses the devices operated by Alice and Bob, culminating in the creation of three distinct temporal intervals at the endpoint. SPD1 is connected to out1 of the decoding chip, and SPD2 is connected to out2 of the decoding chip. SPD refers to the single-photon detectors used in our experiment. Within the central interval, an interference pattern emerges, characterized by constructive interference at detector SPD1, while detector SPD2 exhibits a pattern of destructive interference.

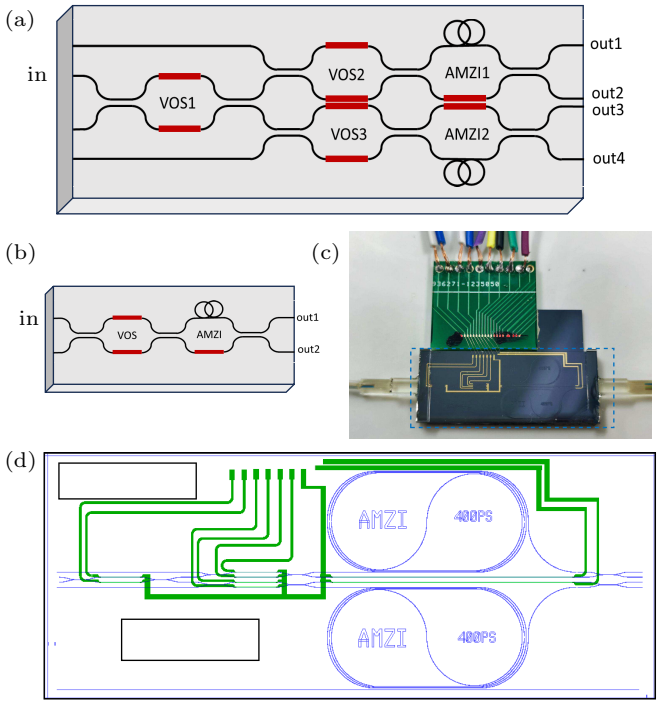


Fig. 1. Chip schematic. VOS, variable optical beam splitter. AMZI, asymmetric Mach–Zehnder interferometer. Light enters from 'in' and outputs from 'out'. The red area represents the heated electrode. (a) Decoding chip schematic. (b) Encoding chip schematic. (c) The physical layout of the chip post coupling wire bonding is depicted, providing a tangible representation of the device's structure and interconnections. (d) Decoding chip layout.

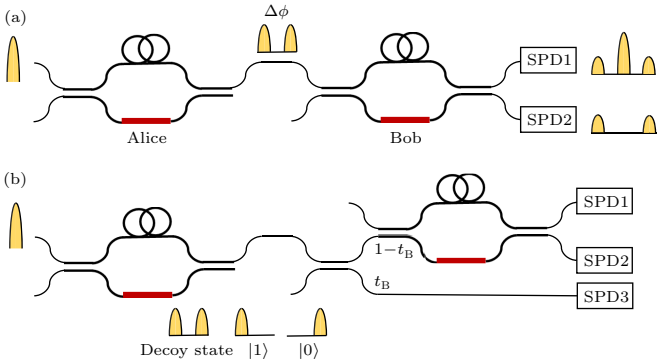


Fig. 2. Encoding and decoding process. The yellow area represents the light pulse. (a) BB84 phase encoding and decoding protocol process. (b) COW protocol encoding and decoding process.

For the COW protocol, Alice prepares three quantum states, $|0\rangle$, $|1\rangle$, and a decoy state, as shown in Fig. 2(b). The prepared quantum states passively enter a part through an unbalanced beamsplitter (with a transmittance rate close to 1). The detector SPD3 generates a key discrimination through the

response time. The remaining small part of the energy enters the part with AMZI, that is, the coherence detection module, to implement the security analysis of the system. In our decoding chip design, the light pulse is directed through VOS1, which is finely tuned to ensure that the majority of the light is channeled into VOS3. Subsequently, both VOS3 and AMZI2 are meticulously adjusted to facilitate the light's emission predominantly from one arm, while a minor fraction of the light is diverted into VOS2. This subset of light then interacts with AMZI1 through interference.

For the BB84 phase QKD, the encoding and decoding process is similar to that in Fig. 2(a). Bob's apparatus generates three temporal slots; however, only photons arriving in the central slot are utilized for key generation, leaving those in the first and third slots unused. To enhance the efficiency of photon utilization and thus increase the encoding rate, an advanced iteration of the BB84 protocol incorporating time-phase encoding has been developed. This method introduces an additional quantum state basis, known as the Z basis, defined by the timing of photon arrival: photons in the first slot represent the quantum state $|0\rangle$, while those in the second slot represent $|1\rangle$. These states are orthogonal. Furthermore, this model incorporates the phase basis (X basis) quantum states discussed previously, with quantum states having relative phases $\Delta\phi$ of 0 and π, represented as $|+\rangle$ and $|-\rangle$, respectively. Collectively, these four quantum states form the cornerstone of the sophisticated phase-time encoding strategy. Figure 3 shows the schematic diagram of the four quantum states and the detector responses. Alice prepares four quantum states. For the X basis, the pulse pairs pass through VOS1 and are guided to VOS2. VOS2 adjusts the balance of the pulse pairs, which then pass through AMZI1 to select the X basis. At out1 and out2, the results of the second time slot with destructive and subtractive interference are obtained, respectively. For the Z basis, the light pulses pass through VOS1 and are guided to VOS3. VOS3 adjusts the balance of the pulse pair, which then passes through AMZI2. At out3 and out4, the double pulse pair is obtained, respectively.

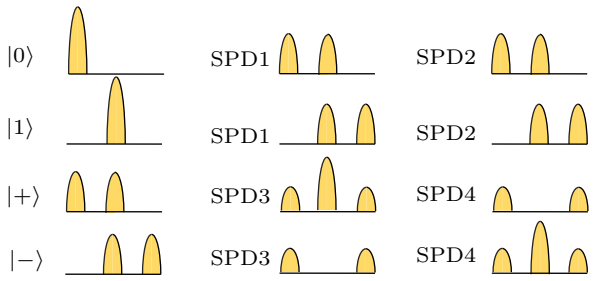


Fig. 3. The state changes of time-bin light pulses during the encoding and decoding process.

2.1. Temperature

First, we need to identify the optimal operating temperature for the encoding and decoding chips to ensure they function at their best temperature point. The pulses within the waveguide are decomposed into two components: the transverse electric (TE) mode and the transverse magnetic (TM) mode, with their electric vectors oriented parallel and perpendicular to the substrate plane, respectively. When interference occurs in the overlapping region, the number of interfering photons can be represented as follows:

$$N = N_{\mathrm{s}}^{\mathrm{TE}} + N_{\mathrm{l}}^{\mathrm{TE}} + 2\sqrt{N_{\mathrm{s}}^{\mathrm{TE}} N_{\mathrm{l}}^{\mathrm{TE}}}\cos\left(\Delta\phi^{\mathrm{TE}}\right) + N_{\mathrm{s}}^{\mathrm{TM}} + N_{\mathrm{l}}^{\mathrm{TM}} + 2\sqrt{N_{\mathrm{s}}^{\mathrm{TM}} N_{\mathrm{l}}^{\mathrm{TM}}}\cos\left(\Delta\phi^{\mathrm{TM}}\right). \tag{1}$$

The quantities $N_{\mathrm{s}}^{\mathrm{TE}}$ and $N_{\mathrm{s}}^{\mathrm{TM}}$ represent the number of TE and TM mode photons passing through the short arm, respectively, while $N_{\mathrm{l}}^{\mathrm{TE}}$ and $N_{\mathrm{l}}^{\mathrm{TM}}$ denote the number of TE and TM mode photons traversing the long arm, respectively. The phase delays for the TE and TM modes in the two arms are given by

$$\Delta\phi^{\mathrm{TE}} = \frac{2\pi}{\lambda_0} n^{\mathrm{TE}} \Delta L + \phi\left(V^2\right), \tag{2}$$

$$\Delta\phi^{\mathrm{TM}} = \frac{2\pi}{\lambda_0} n^{\mathrm{TM}} \Delta L + \phi\left(V^2\right), \tag{3}$$

where ΔL is the arm length difference, and λ_0 is the wavelength in vacuum. The first term represents the phase difference introduced by the thermo-optic effect, where n^{TE} and n^{TM} are the modal refractive indices for the TE and TM modes, respectively, in the silicon dioxide waveguide. Within a temperature range of 15 °C to 55 °C, these indices can be approximated as linear functions of temperature T. The second term accounts for the phase difference induced by voltage variations. V is the voltage applied to the heating electrodes. By optimizing the waveguide structure to nullify its geometric birefringence and implementing overall temperature control at the base, the temperature field's effect from the heating electrode on the stress-induced birefringence between the base and the silicon dioxide cladding film is minimal. Consequently, it is reasonable to approximate that $n^{\mathrm{TE}} = n^{\mathrm{TM}}$, rendering the phase shifts $\phi\left(V^2\right)$ for the TE and TM modes approximately equal. Therefore, we define the modal phase mismatch between TE and TM modes as

$$\Delta\phi = \Delta\phi^{\mathrm{TE}} - \Delta\phi^{\mathrm{TM}} = \frac{2\pi\Delta n \Delta L}{\lambda_0}, \tag{4}$$

where $\Delta n = n^{\mathrm{TE}} - n^{\mathrm{TM}}$ represents the modal birefringence; this birefringence is primarily attributed to stress-induced birefringence resulting from changes in the waveguide temperature. By adjusting the voltage of the thermo-optic phase shifter on the VOS, we can achieve equality between the number of TE mode photons passing through the short and long arms ($N_{\mathrm{s}}^{\mathrm{TE}} = N_{\mathrm{l}}^{\mathrm{TE}}$) or the number of TM mode photons ($N_{\mathrm{s}}^{\mathrm{TM}} = N_{\mathrm{l}}^{\mathrm{TM}}$). For simplicity, we assume that the photon numbers for both TE and TM modes reach equilibrium simultaneously, which means

$$N_{\mathrm{s}}^{\mathrm{TE}} = N_{\mathrm{l}}^{\mathrm{TE}} = \frac{N_1}{2}, \quad N_{\mathrm{s}}^{\mathrm{TM}} = N_{\mathrm{l}}^{\mathrm{TM}} = \frac{N_2}{2}, \tag{5}$$

where N_1 and N_2 are the number of photons in the upper and lower arms of the AZMI, respectively. By formula (4), $\Delta\phi^{\mathrm{TE}}$ can be expressed as

$$\Delta\phi^{\mathrm{TE}} = \Delta\phi^{\mathrm{TM}} + \Delta\phi. \tag{6}$$

In summary,

$$N = N_1 + N_2 + 2\sqrt{N_1 N_2}\cos\left(a\frac{2\pi}{\lambda_0}\Delta L\cdot T + b\cdot V^2 + c\right) \times \cos\left(d\cdot T + e\right). \tag{7}$$

The interference visibility V_{is} can be derived as follows:

$$V_{\mathrm{is}} = \frac{N_{\max} - N_{\min}}{N_{\max} + N_{\min}} = 2\frac{\sqrt{N_1 N_2}}{N_1 + N_2}\left|\cos\frac{\Delta\phi}{2}\right| = 2\frac{\sqrt{N_1 N_2}}{N_1 + N_2}\left|\cos(d\cdot T + e)\right|. \tag{8}$$

From the above equation, it can be concluded that when $\Delta\phi = 2N\pi$ (where N is an integer), the TE and TM modes are in phase and V_{is} is maximized. When $\Delta\phi = (2N+1)\pi$, the TE and TM modes are out of phase and V_{is} is minimized. Furthermore, we can adjust the temperature of the chip to optimize V_{is}.

We use the pulse self-interference method[37] to study the polarization characteristics of the chip. The pulses with a repetition frequency of 50 MHz and a pulse width of 1 ns are attenuated by the attenuator to the single photon level and then input to the multi-protocol decoding chip. A detector is connected at out1, as shown in Fig. 4(a). We scan the thermoelectric cooler temperature from 15 °C to 55 °C with a step of 0.1 °C and obtain the curves of the photon counts of TE and TM modes as a function of temperature, as shown in Fig. 5.

When T is 41.7 °C, the TM and TE curves are in phase, and the interference visibility is the highest. Therefore, the appropriate operating temperature point for our decoding chip is 41.7 °C.

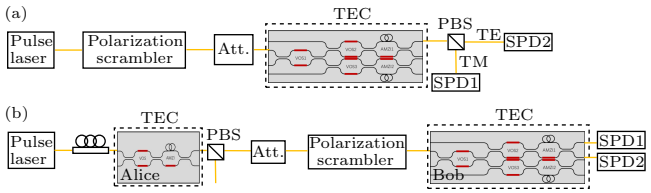


Fig. 4. Diagram of the principle of optimal temperature point experiment. (a) Experimental setup designed to analyze the polarization characteristics of the AMZI. The system components include a variable optical attenuator (Att.), a temperature controller (TEC) and a polarization beam splitter (PBS). (b) Confirming the optimal temperature point for the encoder and decoder chip connection.

The phase-matching temperature of the encoding chip we used is 50 °C. We controlled the encoding chip with a circuit board at 50 °C and the decoding chip at 41.7 °C. We connect the encoding and decoding chips together. As shown in Fig. 4(b), a 50 MHz repetition rate, 50 ps pulse width light pulse is incident on the polarization controller PC and encoded by Alice. The pulse enters one arm of the PBS and is attenuated to the single photon level by a variable optical attenuator before entering Bob for decoding.

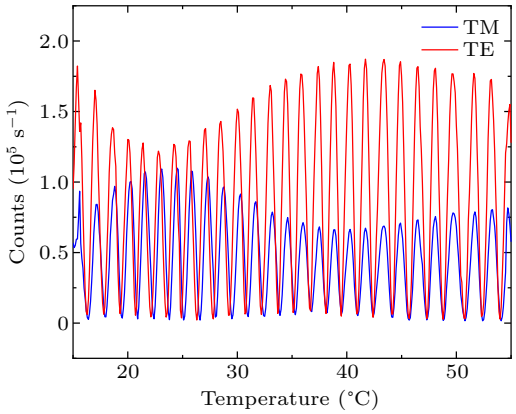


Fig. 5. The change in the number of photons in the TE and TM modes with temperature.

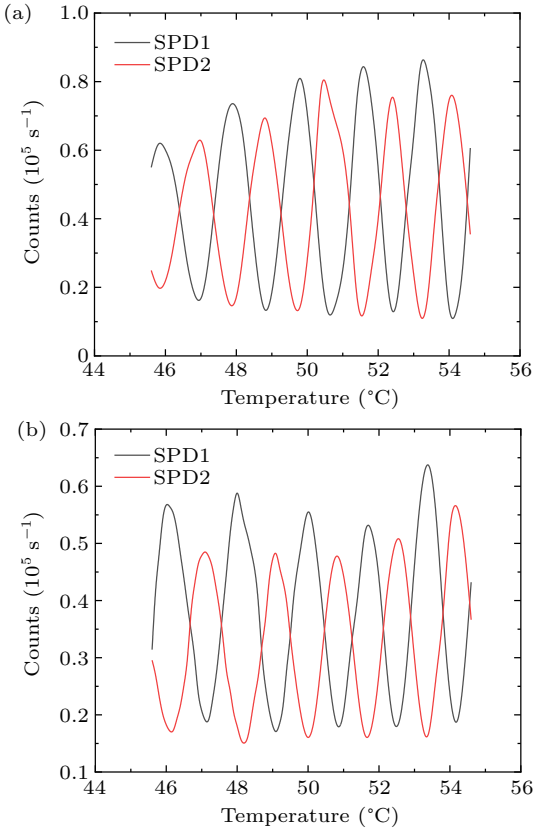


Fig. 6. Detector's second time slot interference photon count versus temperature curve. (a) With the encoding chip fixed, the photon count of the detector changes as the decoding chip is scanned. (b) With the decoding chip fixed, the photon count of the detector changes as the encoding chip is scanned.

In the experiment, we initially set the temperature of Alice to 50 °C and then adjusted Bob's temperature within the range of 45.6 °C to 54.6 °C. Through this process, we obtained Fig. 6(a), which showed that the visibility of interference reached its maximum when Bob's temperature was at 53.2 °C. Further, by fixing Bob's temperature at 53.2 °C and

adjusting Alice's temperature, we obtained Fig. 6(b). The results indicated that the visibility of interference also reached its maximum when Alice's temperature was at 53.4 °C. Therefore, we can conclude that the maximum visibility of interference for the encoding chip occurs at 53.4 °C, while for the decoding chip, the maximum visibility of interference temperature point is at 53.2 °C.

2.2. Preparation of the quantum state

We proceed with the preparation of the quantum state. As shown in Fig. 7, in this system, a pulse laser is used to generate a sequence of light pulses with a wavelength of 1550 nm and a pulse width of 50 ps. The SPD is composed of an InGaAs/InP avalanche photodiode detector (APD) and a counting module. It uses a narrow gate pulse mode to detect single photons triggered by an external clock and communicates with the computer via a serial port. The PPG clock signal synchronizes the pulse laser and SPD. Due to the bandwidth limitations of our detector, the system repetition rate is set to 156 MHz. Our decoding and encoding chips are placed at the optimal temperature points shown above by TEC. A coded signal is written, amplified by Ampf., and then drives the phase modulator (PM) and intensity modulator (IM). The signals generated by the PPG modulate the double pulses through the modulator, as shown in Fig. 8.

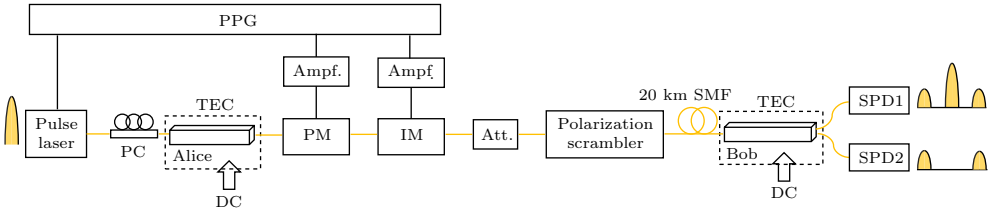


Fig. 7. The preparation of quantum states. DC, direct current voltage source; PPG, pulse pattern generator; Ampf., radio frequency amplifier; PM, $LiNbO_3$ phase modulator; IM, $LiNbO_3$ intensity modulator.

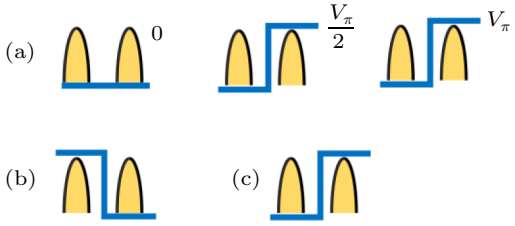


Fig. 8. Phase basis and time basis encoding. The blue line is the code generated by the PPG, and the yellow is the optical pulse pair. (a) It is encoded with 0, $\pi/2$, π phase. (b) Encoded with $|0\rangle$ quantum state. (c) Encoded with $|1\rangle$ quantum state.

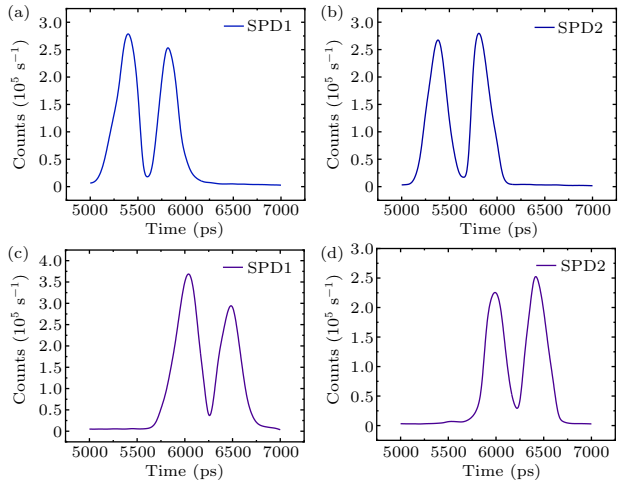


Fig. 9. The change in photon count of the detectors. (a) The change in photon count of SPD1 detecting quantum state $|0\rangle$. (b) The change in photon count of SPD2 detecting quantum state $|0\rangle$. (c) The change in photon count of SPD1 detecting quantum state $|1\rangle$. (d) The change in photon count of SPD2 detecting quantum state $|1\rangle$.

Quantum states $|0\rangle$ and $|1\rangle$ are encoded by the IM. For the quantum state $|0\rangle$, only the optical pulse in the first time slot is retained, while for the quantum state $|1\rangle$, only the optical pulse in the second time slot is retained. A single pulse, after passing through the decoding chip's delay line, is split into two pulses: one in the 1,2 time slot and the other in the 2,3 time slot. The photon number distribution of quantum states $|0\rangle$ and $|1\rangle$ in two SPD detectors is shown in Fig. 9. For $|0\rangle$, the number of photons in the first slot of SPD1 is 28813, and the number of photons in the third slot is 787; the number of photons in the first slot of SPD2 is 27493, and the number of photons in the third slot is 366. The extinction ratio is 16.9 dB. For $|1\rangle$, the number of photons in the third slot of SPD1 is 30493, and the number of photons in the first slot is 588; the number of photons in the third slot of SPD2 is 26328, and the number of photons in the first slot is 643. The extinction ratio is 16.5 dB.

For phase-encoded quantum states, the graph below shows the photon count detected by SPD as a function of PPG voltage. As shown in Fig. 10, when the PPG voltage is set to 0.1 Vpp and 0.75 Vpp, corresponding to relative phases of 0 and π respectively, and at 0.4 Vpp, there are optical pulse pairs with a phase difference of $\pi/2$. Due to saturation of the PPG and amplifier inputs, we cannot generate optical pulse pairs with a phase difference of $3\pi/2$. Although our encoding end cannot encode a $3\pi/2$ phase due to equipment limitations, our multi-protocol decoding chip is theoretically capable of decoding a $3\pi/2$ phase. Therefore, while we did not calculate the key rate for the BB84 phase encoding and decoding protocol, this does not affect the performance of our decoding chip under other protocols. Our decoding chip still demonstrates superior flexibility and performance, providing crucial support for the development of quantum communication systems. At 0.1 Vpp, the photon count for SPD1 is 105030, and for SPD2

is 8241, resulting in an interference visibility of 85.4%. At 0.75 Vpp, the photon count for SPD1 is 7198, and for SPD2 is 148846, with an interference visibility of 90.3%.

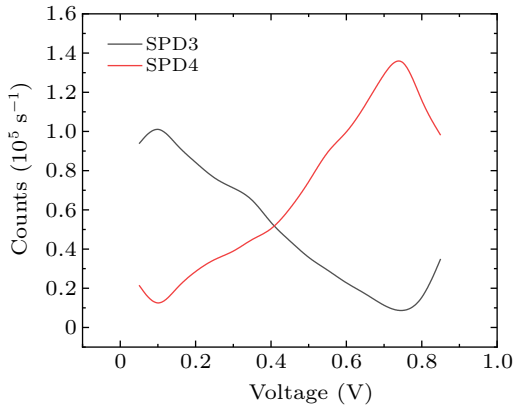


Fig. 10. The variation of photon count with PPG voltage.

3. Results

Finally, we calculate the key rate of different protocols. Our experiment does not utilize decoy states, so we have adopted a security proof[38,39] to analyze the key rate per pulse without decoy states, as shown by the following formula:

$$K_{\mathrm{BB84}} = \frac{1}{2} R \left[1 - f(\varepsilon) H_2(\varepsilon) - H_2\left(\varepsilon_{\mathrm{ph}}\right)\right], \tag{9}$$

where R is the proportion of pulses detected by the decoding end, as shown by the following formula:

$$R = \frac{\text{raw key rate}}{\text{repetition rate}} = \mu t_{\mathrm{link}} \eta, \tag{10}$$

wherein the repetition frequency is 156 MHz, μ is the average number of photons emitted by the encoding end, η is the detection efficiency of the SPD, and t_{link} is the probability of photons reaching the detector. We set $\mu = 0.1$ and η is 10%. The following formula is the expression for t_{link}:

$$t_{\mathrm{link}} = 10^{(-\alpha L - IL_{\mathrm{Bob}})/10}. \tag{11}$$

Bob's additional loss is 2.28 dB; that is, $IL_{\mathrm{Bob}} = 2.28$ dB. α is the loss coefficient of single mode fiber, which is 0.2 dB/km, and L is the length of the fiber.

The ε is the QBER. $f(\varepsilon)$ is the error correction inefficiency factor, used to perform key reconciliation, usually greater than or equal to 1. In this case, $f(\varepsilon) = 1.22$. The term $f(\varepsilon) H_2(\varepsilon)$ represents the cost of error correction and $H_2(\varepsilon)$ is the binary Shannon entropy, as shown in the following formula:

$$H_2(\varepsilon) = -\varepsilon \log_2(\varepsilon) - (1-\varepsilon)\log_2(1-\varepsilon). \tag{12}$$

The photon error rate $\varepsilon_{\mathrm{ph}}$ is related to ε as shown below:

$$\begin{aligned} \varepsilon_{\mathrm{ph}} = {} & \varepsilon + 4\Delta'\left(1-\Delta'\right)(1-2\varepsilon) \\ & + 4\left(1-2\Delta'\right)\sqrt{\Delta'(1-\Delta')\,\varepsilon(1-\varepsilon)} \end{aligned} \tag{13}$$

with

$$\Delta' = \frac{\Delta}{R_0} = \frac{1}{2R_0}\left(1 - \mathrm{e}^{-\mu/2}\left(\cos\left(\frac{\mu}{2}\right) + \sin\left(\frac{\mu}{2}\right)\right)\right). \tag{14}$$

Here, R_0 is the R when L is 0 km. To find ε, we need to use the equation

$$\varepsilon = \mathrm{QBER}_{\mathrm{opt}} + \mathrm{QBER}_{\mathrm{det}}. \tag{15}$$

$\mathrm{QBER}_{\mathrm{opt}}$ is the part of the error rate that reflects the errors caused by the imperfections of the optical system. $\mathrm{QBER}_{\mathrm{phase}}$ is related to issues with the phase of the quantum state and $\mathrm{QBER}_{\mathrm{time}}$ is associated with problems in the time-bin encoding of the state.

$$\begin{aligned} \mathrm{QBER}_{\mathrm{opt}} &= \frac{1}{2}\mathrm{QBER}_{\mathrm{phase}} + \frac{1}{2}\mathrm{QBER}_{\mathrm{time}} \\ &= \frac{1}{2}\cdot\frac{1-V_{\mathrm{is}}}{2} + \frac{1}{2}\cdot\frac{1}{10^{ER/10}+1}, \end{aligned} \tag{16}$$

where V_{is} is the interference visibility we know from our experiment and ER is the extinction ratio. $\mathrm{QBER}_{\mathrm{det}}$ is the part of the error rate caused by the imperfections of the detection system, such as detector noise, detector efficiency inconsistency, detector dead time, etc. $\mathrm{QBER}_{\mathrm{det}}$ is given by

$$\mathrm{QBER}_{\mathrm{det}} = \frac{p_{\mathrm{dark}} n}{2 \cdot t_{\mathrm{link}} \eta \mu}, \tag{17}$$

where p_{dark} is the probability of recording a dark count per time gate and per detector. In our experiment, $p_{\mathrm{dark}} = 3 \times 10^{-6}$ gate^{-1}. $n = 2$ is the number of detectors.

The key rate of the COW protocol is provided by references.[40,41] Our raw key rate, secret key rate and QBER are depicted in Fig. 11. At 20 km, the raw key rate of the time-bin phase-encoding QKD is 184.5 kbps, with a secret key rate of 80.46 kbps and a QBER of 0.0423. The secret key rate of the COW protocol is 18.18 kbps, with a phase error rate of 0.03627 and a time error rate of 0.00377. Compared to the chip described in Ref. [42], our chip demonstrates superior performance. While its key rate may not be exceptionally high in single-protocol scenarios, it offers significant advantages in terms of reducing overall system complexity, scalability and adaptability, making it a promising solution for future quantum key distribution systems. Our suboptimal key rates can be attributed to several factors. Firstly, significant chip losses are observed, potentially due to inefficient light transmission within the chip. At 0 km, when the chip loss is 2 dB, 2.5 dB and 3 dB, the raw key rate decreases by approximately 100 kbps for every 0.5 dB increase in chip loss, based on the

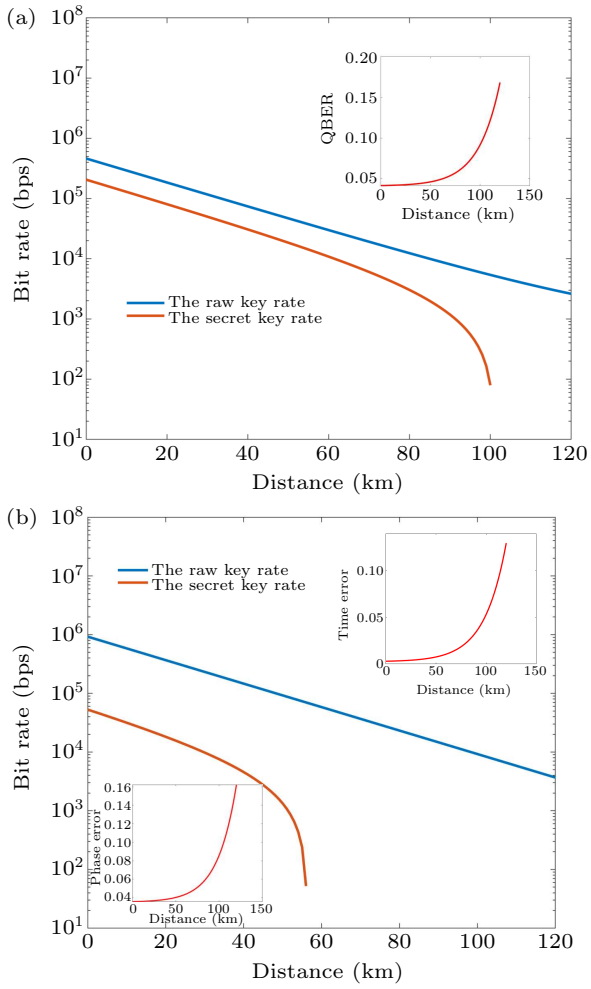


Fig. 11. The change of bit rate with distance. (a) The bit rate of the time-bin phase-encoding QKD as a function of distance. (b) The bit rate of the COW protocol as a function of distance.

experimental data. Secondly, our detector efficiency remains low, leading to a reduced probability of accurately detecting transmitted photons. We simulated the effect of varying detector efficiencies (10%, 20% and 30%) on the raw key rate. Our results show that for every 10% increase in detector efficiency, the raw key rate increases by approximately 900 kbps. Thirdly, narrow detector gate widths impose limitations that hinder our ability to achieve higher repetition rates. When simulating the effect of repetition rate variations, we found that the relationship between repetition rate and raw key rate is multiplicative. An increase in repetition rate leads to a corresponding multiplicative increase in the raw key rate, demonstrating the critical role of higher repetition rates in improving the overall key generation efficiency. Moreover, manufacturing defects in the integrated silicon chip, particularly the incomplete achievement of 3 dB splitting during fabrication, have contributed to our relatively high QBER. Lastly, environmental interference further exacerbates these challenges, impacting signal stability and quality. Temperature variations can cause changes in the refractive index of optical fibers, affecting the propagation speed, transmission loss and phase velocity of light. Particularly in long-distance QKD experiments, temperature fluctuations may lead to minor structural changes in the fiber (such as expansion or contraction), which in turn can shift the propagation mode of the light. These changes may alter the phase difference of the signal, increasing decoherence and ultimately affecting the QBER in the QKD experiment.

4. Conclusion

In conclusion, we have designed chips that satisfy the BB84 phase-decoding protocol, the time-bin phase-decoding protocol and the COW protocol. We have identified the optimal temperatures for the operation of both decoding and encoding chips. Additionally, we have calculated the secret key rates for the time-bin phase-decoding QKD and COW protocol. The secret key rate for the time-bin phase-decoding QKD is 80.46 kbps with a quantum bit error rate of 4.23%, while for the COW protocol, it is 18.18 kbps with a phase error rate of 3.627% and a time error rate of 0. 377%. With enhancements to our testing equipment, refined manufacturing processes and bolstered environmental controls, we anticipate a marked increase in the key rates.

Acknowledgments

Project supported by the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300701), the National Key Research and Development Program of China (Grant No. 2018YFA0306403), and the Strategic Priority Research Program of Chinese Academy of Sciences (Grant No. XDB43000000).

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Bennett C H, Bessette F, Brassard G, Salvail L and Solin J 1992 *J. Cryptol.* **5** 3
[3] Lo H K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595
[4] Grünenfelder F, Boaron A, Resta G V, Perrenoud M, Rusca D, Barreiro C, Houlmann R, Sax R, Stasi L, El-Khoury S, Hänggi E, Bosshard N, Bussières F and Zbinden H 2023 *Nat. Photon.* **17** 422
[5] Liu Y, Zhang W J, Jiang C, Chen J P, Zhang C, Pan W X, Ma D, Dong H, Xiong J M, Zhang C J, Li H, Wang R C, Wu J, Chen T Y, You L X, Wang X B, Zhang Q and Pan J W 2023 *Phys. Rev. Lett.* **130** 210801
[6] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, Ye P, Zhou Y, Fan-Yuan G J, Wang F X, Chen W, Zhu Y G, Morozov P V, Divochiy A V, Zhou Z, Guo G C and Han Z F 2022 *Nat. Photon.* **16** 154
[7] Huang C F, Chen Y, Luo T T, He W J, Liu X, Zhang Z R and Wei K J 2024 *Sci. China Phys. Mech. Astron.* **67** 240312
[8] Wang W Y, Wang R, Hu C Q, Zapatero V, Qian L, Qi B, Curty M and Lo H K 2023 *Phys. Rev. Lett.* **130** 220801
[9] Liu X, Luo D, Luo Z C, Li S Z, Zhang Z R and Wei K J 2024 *Phys. Rev. Appl.* **22** 064018
[10] Liu Q, Huang Y M, Du Y Q, Zhao Z G, Geng M M, Zhang Z R and Wei K J 2022 *Entropy* **24** 1334
[11] Sax R, Boaron A, Boso G, Atzeni S, Crespi A, Grünenfelder F, Rusca D, Al-Saadi A, Bronzi D, Kupijai S, Rhee H, Osellame R and Zbinden H 2023 *Photon. Res.* **11** 1007
[12] Du H, Paraiso T K, Pittaluga M, Lo Y S, Dolphin J A and Shields A J 2024 *Optica* **11** 1385

[13] Du Y Q, Zhu X, Hua X, Zhao Z G, Hu X, Qian Y, Xiao X and Wei K J 2023 *Chip* **2** 100039

[14] Wei K J, Hu X, Du Y Q, Hua X, Zhao Z G, Ye Chen, Huang C F and Xiao X 2023 *Photon. Res.* **11** 1364

[15] Paraïso T K, Roger T, Marangon D G, Marco I D, Sanzaro M, Woodward R I, Dynes J F, Yuan Z L and Shields A J 2021 *Nat. Photon.* **15** 850

[16] Zhu C X, Chen Z Y, Li Y, Wang X Z, Wang C Z, Zhu Y L, Liang F T, Cai W Q, Jin G, Liao S K and Peng C Z 2022 *Phys. Rev. Appl.* **17** 064034

[17] Zhang C X, Wu D, Cui P W, Ma J C, Wang Y and An J M 2023 *Chin. Phys. B* **32** 124207

[18] Zhang Q Y, Xu P and Zhu S N 2018 *Chin. Phys. B* **27** 054207

[19] Honjo T, Inoue K and Takahashi H 2004 *Opt. Lett.* **29** 2797

[20] Harris N C, Bunandar D, Pant M, Steinbrecher G R, Mower J, Prabhu M, Baehr-Jones T, Hochberg M and Englund D 2016 *Nanophotonics* **5** 456

[21] Nambu Y, Yoshino K and Tomita A 2008 *J. Mod. Opt.* **55** 1953

[22] Zhang G W, Ding Y Y, Chen W, Wang F X, Ye P, Huang G Z, Wang S, Yin Z Q, An J M, Guo G C and Han Z F 2021 *Photon. Res.* **9** 2176

[23] Zhang G W, Chen W, Fan-Yuan G J, Zhang L, Wang F X, Wang S, Yin Z Q, He D Y, Liu Wen, An J M, Guo G C and Han Z F 2022 *Sci. China Inf. Sci.* **65** 200506

[24] Ma C X, Sacher W D, Tang Z Y, Mikkelsen Jared C, Yang Y, Xu F H, Thiessen T, Lo H K and Poon J K S 2016 *Optica* **3** 1274

[25] Sibson P, Kennard J E, Stanisic S, Erven C, O'Brien J L and Thompson M G 2017 *Optica* **4** 172

[26] Cai H, Long C M, DeRose C T, Boynton N, Urayama J J, Camacho R, Pomerene A, Starbuck A L, Trotter D C, Davids P S and Lentine A L 2017 *Opt. Express* **25** 12282

[27] Geng W, Zhang C, Zheng Y, He J, Zhou C and Kong Y 2019 *Opt. Express* **27** 29045

[28] Wei K, Li W, Tan H, Li Y, Min H, Zhang W J, Li H, You L X, Wang Z, Jiang X, Chen T Y, Liao S K, Peng C Z, Xu F H and Pan J W 2020 *Phys. Rev. X* **10** 031030

[29] Cao L, Luo W, Wang Y X, Zou J, Yan R D, Cai H, Zhang Y, Hu X L, Jiang C, Fan W J, Zhou X Q, Dong B, Luo X S, Lo G Q, Wang Y X, Xu Z W, Sun S H, Wang X B, Hao Y L, Jin Y F, Kwong D L, Kwek L C and Liu A Q 2020 *Phys. Rev. Applied* **14** 011001

[30] Li W, Zhang L K, Tan H, Lu Y, Liao S K, Huang J, Li H, Wang Z, Mao H K, Yan B, Li Q, Liu Y, Zhang Q, Peng C Z, You L X, Xu F H and Pan J W 2023 *Nat. Photon.* **17** 416

[31] Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner M G, Natarajan C M, Hadfield R H, O'Brien J L and Thompson M G 2017 *Nat. Commun.* **8** 13984

[32] Dolphin J A, Paraïso T K, Du H, Woodward R I, Marangon D G and Shields A J 2023 *npj Quantum Inf.* **9** 84

[33] Maker A J and Armani A M 2011 *Opt. Lett.* **36** 3729

[34] Nambu Y, Hatanaka T and Nakamura K 2004 *Jpn. J. Appl. Phys.* **43** L1109

[35] Tanaka A, Fujiwara M, Nam S W, Nambu Y, Takahashi S, Maeda W, Yoshino K I, Miki S, Baek B, Wang Z, Tajima A, Sasaki M and Tomita A 2008 *Opt. Express* **16** 11354

[36] Korzh B, Walenta N, Houlmann R and Zbinden H 2013 *Opt. Express* **21** 19579

[37] Li X, Ren M Z, Zhang J S, Wang L L, Chen W, Wang Y, Yin X Y, Wu Y D and An J M 2021 *Photon. Res.* **9** 222

[38] Lo H K and Preskill J 2007 *Quantum Info. Comput.* **7** 431

[39] Li X, Wang L L, Zhang J, Chen W, Wang Y, Wu Y D and An J M 2022 *Chin. Phys. B* **31** 064212

[40] Branciard C, Gisin N and Scarani V 2008 *New J. Phys.* **10** 013031

[41] Li X, Wang L L, Zhang J S, Chen W, Wang Y, Wu D and An J M 2022 *Chin. Phys. B* **31** 010304

[42] Wu D, Chen S K, Cui P W, Ma J C, Chen W, Zhang J S, Wang Y, Li J G and An J M 2023 *IEEE Photonics J.* **15** 1