# Security analysis against the Trojan horse attack on practical polarization-encoding quantum key distribution systems

Tingting Luo,[1] Qiang Liu,[2,*] Xiaoran Sun,[1] Chunfeng Huang,[1] Ye Chen,[1] Zhenrong Zhang,[2,†] and Kejin Wei[1,‡]

[1]*Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning 530004, China*

[2]*Guangxi Key Laboratory of Multimedia Communications and Network Technology, School of Computer, Electronics and Information, Guangxi University, Nanning 530004, China*

(Received 6 July 2023; revised 22 December 2023; accepted 8 March 2024; published 3 April 2024)

Quantum key distribution (QKD), which theoretically provides unconditional secure communication, has developed rapidly in the past decades. However, the practical QKD systems still have vulnerabilities due to device imperfections. Polarization-encoding systems are one of the most important branches in the field of QKD. To date, a variety of polarization-encoding schemes have been proposed to meet the requirements of high speed and robust modulation, but the security analysis of these schemes is often ignored. In this paper, we experimentally and theoretically evaluated the security of three typical polarization encoders against the Trojan horse attack (THA), which is recognized as one of the critical quantum attacks. We built a system to implement the THA and collected the reflection from QKD configuration with different encoders. According to the experimental results, we further analyzed the secure key rate and the resistance against THAs of the system while BB84 or measurement-device-independent QKD was applied. Our paper plays an important guiding role in the design of polarization encoders and the construction of secure QKD systems with realistic devices.

DOI: 10.1103/PhysRevA.109.042608

## I. INTRODUCTION

Guaranteed by the principle of quantum mechanics, unconditional security can be theoretically realized in quantum key distribution (QKD). Since the first proposal of the BB84 protocol [1], QKD has rapidly developed in both theory [2–7] and experiments [8–14]. However, due to device imperfections, there are still realistic vulnerabilities in practical QKD systems. Aimed at these vulnerabilities, a number of attacks have been proposed [15–28].

The Trojan horse attack (THA) [29,30] is one of the critical source attacks [24,31,32] that can seriously threaten the security of practical QKD systems. In a THA, an eavesdropper (usually named Eve) can inject strong Trojan horse optical pulses via the communication channel into the transmitter (usually named Alice). Part of the Trojan horse photons will be modulated along with the information to be transmitted by the encoder and then reflected back into the channel. Hence, Eve can eavesdrop the key information by analyzing the encoded reflection. THA has been proven feasible for most practical components in QKD systems [33,34], even in small-scale chip-based devices [35]. THAs were reported to pose significant harm to the earliest versions of commercial QKD systems [36]. Moreover, it has been confirmed that Eve could not only eavesdrop the encoded information [36] but also might tamper with some parameters of the encoded signal from Alice [37] in a THA or other strong light attacks. To date, the THA has attracted much attention and a large number of studies on THA have been carried out [38–46].

Nowadays, polarization-encoding QKD is one of the most widely used schemes, which has been proven to exhibit excellent immunity to environmental noise in optical fibers [47–49] and in chip-based [14,50–52], free-space [53–55], and underwater channels [56–58]. A key to polarization-encoding QKD systems is to achieve high-speed and stable polarization modulation. For this purpose, several research groups have proposed a variety of polarization-encoding schemes [48,59–64], such as polarization modulation based on the Mach-Zehnder interferometer (MZI) [60], Faraday mirror (FM) [61], and Sagnac interferometer [48,64]. A natural question is arising: How robust are the given polarization-encoding schemes against a THA?

In this paper, we assess the resistance of three recently reported polarization-encoding schemes against THAs. The reflections of the optics used in these systems are calibrated, and the associated information leakage is estimated. Based on the experimental results, we theoretically analyze the secure key rate (SKR) of these polarization-encoding systems when the BB84 or measurement-device-independent QKD (MDI-QKD) schemes are applied. Our paper paves the way for new designs of polarization-encoding schemes and the construction of realistic safe QKD systems.

The outline of this paper is as follows: In Sec. II A, we describe the experimental setup for polarization-encoding configurations and the THA testing. The experimental results are explained in Sec. II B. The analysis method and results for the SKR of BB84-QKD and MDI-QKD systems with polarization encoders are illustrated in Sec. III. Then we conclude our paper in Sec. IV.

*q.liu@gxu.edu.cn
†zzr76@gxu.edu.cn
‡kjwei@gxu.edu.cn

 

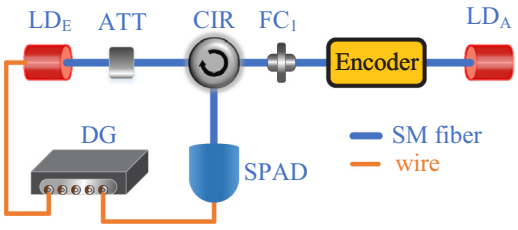


FIG. 1. Schematic diagram of the time domain reflection setup. Encoder: the encoders under test. The specific composition of the three different encoders studied will be shown in Figs. 2(a), 3(a), and 4(a), respectively. LD$_E$, laser diode at Eve; LD$_A$, laser diode at Alice; ATT, optical attenuator; FC$_1$, FC/APC fiber connector; CIR, circulator; SPAD, InGaAs-based time-gated infrared single-photon avalanche detector; DG, digital time delay generator; SM fiber, single-mode fiber.

## II. EXPERIMENT

### A. Experimental setup

In order to investigate the resistance of different polarization-encoding schemes against THAs, we experimentally reproduced three reported quantum polarization encoders [48,60,61] via reverse engineering, and built an optical time domain reflection system. This system consists of a laser, an InGaAs-based time-gated infrared single-photon avalanche detector (SPAD), a circulator (CIR), and a digital delay generator (DG) (Fig. 1). Eve's laser (WT-LD200-DL, Qasky) provides laser pulses (wavelength 1550 nm, frequency 1 MHz, pulse width 200 ps) as the Trojan horse pulses (THPs). Eve was connected to the output of Alice via a CIR. The THPs were injected into Alice and part of these pulses were reflected by the end faces of fiber connectors (FCs) or optical components in Alice's encoder. The reflection was modulated along with key information in the encoder and then propagated back to the channel. The SPAD (WT-SPD300, Qasky) was used to collect this reflection, and a DG (DG645, Stanford Research Systems) was used to control the time delay between launched THPs and received reflection. To acquire information about the transmitted state, Eve probed the phase modulator (PM) or the intensity modulator (IM), measuring the reflected signals and determining the introduced phase difference or intensity difference. With this configuration, we can determine each encoder's reflectivity and define the amount of information that Eve may eavesdrop.

The three quantum polarization encoders reproduced in our experiments are introduced as follows: The first encoder scheme [60] (named encoder *A*) in our paper was based on a balanced MZI configuration as shown in Fig. 2(a). We re-engineered the telecom all-fiber modulation system reported in Ref. [60] but replaced the sum-frequency generation process with a commercial laser (WT-LD200-DL, Qasky). The output from Alice's laser was first aligned to the polarization-maintaining IM working axis by using a polarization controller (PC$_2$). These intensity-controllable laser pulses out of the IM then entered the MZI polarization-maintaining module, which contains two polarization beam splitters (PBSs) and two PMs. By tuning the voltage applied to PM$_1$ and PM$_2$, a phase difference could be modulated in

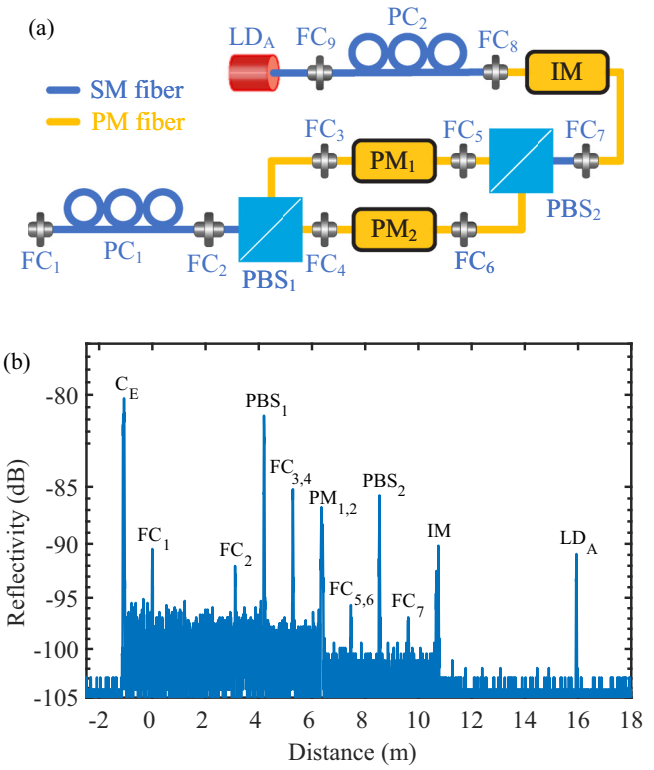


FIG. 2. Experimental setup and test result of encoder *A*. (a) Schematic diagram of the polarization encoder *A* setup. LD$_A$, laser diode at Alice; FC$_i$, FC/APC fiber connector; PC$_i$, polarization controller; IM, intensity modulator; PBS$_i$, polarization beam splitter; PM$_i$, phase modulator. SM fiber, single-mode fiber. PM fiber, polarization-maintaining fiber. (b) Reflections of THAs on encoder *A*. The distance is measured from the fiber connector FC$_1$ placed at the end of Alice. The corresponding source is marked above each reflection peak. C$_E$, circulator at Eve's setup; FC$_{3,4}$ indicates that the peak is the superposition of FC$_3$'s and FC$_4$'s reflection peaks, as are PM$_{1,2}$ and FC$_{5,6}$.

the laser pulses. At the output of the encoder, the PC$_1$ is used to transform the generated state from the circular-diagonal polarization plane to the linear polarization plane.

The second encoder scheme [61] (named encoder *B*) in our paper was an intrinsically stable polarization-modulated unit (PMU) based on three FMs [Fig. 3(a)]. The laser pulses were modulated by IM to generate decoy states and signal states, then transmitted to PBS via CIR. The intensity-modulated laser beam was divided into two orthogonal polarizations at the PBS. We imitate the method in Ref. [61] by specifying that the PBS reflects the vertically polarized pulse (V pulse) and transmits the horizontally polarized pulse (H pulse). These two orthogonal polarization pulses travel in distinct directions between the three FMs before recombining at the PBS to output in opposite directions. Phase differences were introduced to two orthogonal polarization states at PM, and FMs played the role of reversing polarization states. Polarization modulation was completed by using PM and FMs. Polarization-maintaining fibers were unnecessary in the PMU and all optical components were connected by single-mode fibers.

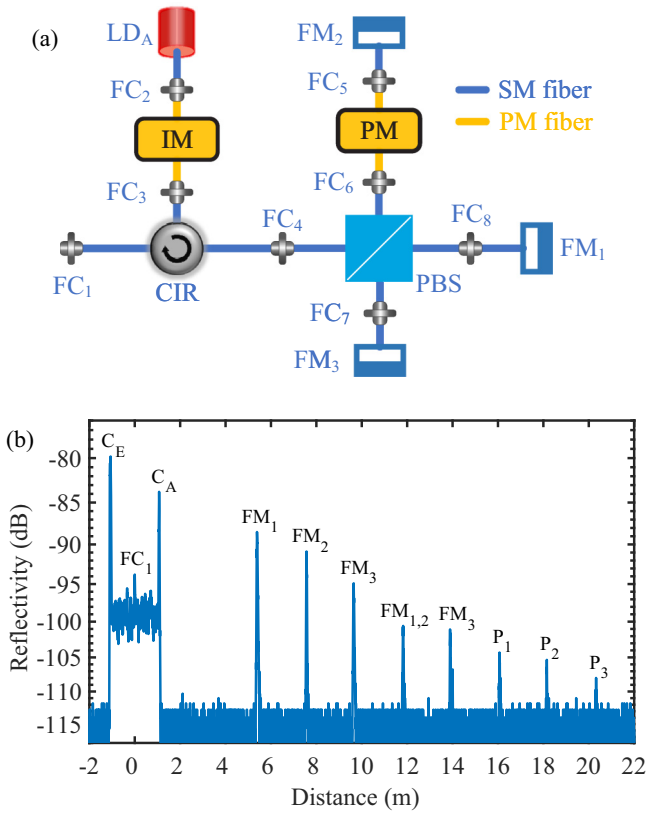


FIG. 3. Experimental setup and test result of encoder *B*. (a) Schematic diagram of the polarization encoder *B* setup. $LD_A$, laser at Alice; $FC_i$, FC/APC fiber connector; IM, intensity modulator; CIR, circulator; $FM_i$, Faraday mirror; PM, phase modulator; PBS, polarization beam splitter; SM fiber, single-mode fiber; PM fiber, polarization-maintaining fiber. (b) Reflections of THAs on encoder *B*. The distance is measured from the fiber connector $FC_1$ placed at the end of Alice. $C_E$, circulator at Eve's setup; $C_A$, circulator at Alice's setup; $FM_{1,2}$, superposition of the vertical reflections from $FM_1$ and horizontal reflections from $FM_2$; $P_i$, superposition of undesired reflections from different optical paths. These undesired reflections originate from nonflipped light caused by FM imperfections.

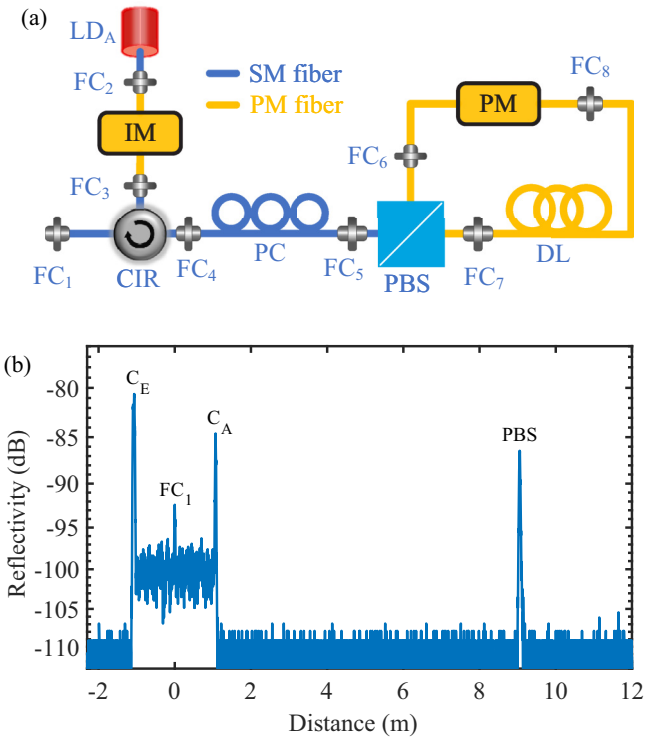


FIG. 4. Experimental setup and test result of encoder *C*. (a) Schematic diagram of the polarization encoder *C* setup. $LD_A$, laser at Alice; $FC_1$, FC/APC fiber connector; IM, intensity modulator; CIR, circulator; PC, polarization controller; PBS, polarization beam splitter; PM, phase modulator; SM fiber, single-mode fiber; PM fiber, polarization-maintaining fiber. (b) Reflections of THAs on encoder *C*. The distance is measured from the fiber connector $FC_1$ placed at the end of Alice. $C_E$, circulator at Eve's setup; $C_A$, circulator at Alice's setup.

The third polarization encoder scheme [48] (named encoder *C*) in our paper was termed POGNAC (polarization plus Sagnac), and it was based on a self-compensating Sagnac interferometer [Fig. 4(a)]. The laser beam was adjusted to 45° linear polarization by using a PC, then divided into horizontal and vertical linear polarization by a PBS, which marked the beginning and end of the Sagnac ring. These two polarization states propagated along opposite directions in the Sagnac interferometer, and their phases were modulated by the PM successively. After phase modulation, two new orthogonal polarization states were recombined at the PBS. This scheme shows a high degree of stability and simplicity and a low intrinsic quantum bit error rate (QBER). Thus, it can be a prime candidate for applications in optical fiber, free-space, and satellite-based QKD.

Note that the CIRs used in the experiment are commercially available from Optimizer Technology (Shenzhen) [65]. The IMs (center wavelength 1550 nm, extinction ratio 23 dB, half-wave voltage 4 V at 1 kHz) and PMs (center wavelength 1550 nm, half-wave voltage 3.8 V at 50 MHz) used in our experiment are commercially available from Beijing Conquer Century Photoelectric Technology [66]. All the pigtails of the modulators in our experimental setups are panda polarization-maintaining fibers (PM-1550 Panda Fiber). The single-mode fibers used in our setup are standard single-mode fibers (SMF-28), and all the component pigtails are connected by using ferrule connectors with angled physical contact (FC/APC).

Furthermore, in our experiment, we eliminated the attenuator at the exit of the above encoders to mitigate the experimental dependency on the instrumentation. In principle, as long as higher-power lasers and more efficient detectors are employed, the inclusion of attenuators at additional ports would not preclude the attainment of equivalent test outcomes.

### B. Results

The experimental results of THAs on the three encoders are shown in Figs. 2(b), 3(b), and 4(b) respectively. The height of each reflecting peak in the pictures corresponds to the reflectivity of various devices, and complete reflectivity data of each peak are provided in Appendix A. By comparing the time differences of reflection peaks with the distances in the actual

TABLE I. Experimental parameters and reflectivity of each encoder. $P_E$, intensity of the THP via Eve; $N_E$, number of single photons per second of Eve's output; $N_R$, photons reflected per second in total; $R^{\mathrm{IM}}$, reflectivity of the IM; $R^{\mathrm{PM}}$, reflectivity of the PM; $R$, total reflectivity. The reflectivity of IM in encoder $B$ or $C$ is not displayed because the leaky peak of the IM in encoder $B$ or $C$ is absent.

| Encoders | Encoder $A$ | Encoder $B$ | Encoder $C$ |
|---|---|---|---|
| $P_E$ (dB m) | $-40.003$ | $-30.143$ | $-35.023$ |
| $N_E$ ($s^{-1}$) | $7.789 \times 10^{11}$ | $7.542 \times 10^{12}$ | $2.452 \times 10^{12}$ |
| $N_R$ ($s^{-1}$) | 13500 | 21140 | 5570 |
| $R^{\mathrm{IM}}$ (dB) | $-90.164$ | | |
| $R^{\mathrm{PM}}$ (dB) | $-68.304$ | $-75.524$ | $-76.436$ |
| $R$ (dB) | $-67.612$ | $-75.524$ | $-76.436$ |

optical paths, we calculated the sources of reflection peaks to determine the main components that caused information leakage in each module. The overall information leakage of each encoder was also evaluated.

Figure 2(b) shows the experimental result of THA on encoder $A$. From left to right, the first peak indicates the reflection from the CIR at Eve's end. The second peak represents the reflection from $FC_1$, which is the fiber connector linking Eve and Alice. The reflection includes the intensity from input surfaces of fiber. The third peak is the reflection from $FC_2$ via $PC_1$. The fourth one represents reflection from $PBS_1$. The next three peaks are a superposition of reflection from $FC_3$ and $FC_4$, $PM_1$ and $PM_2$, and $FC_5$ and $FC_6$, followed by peaks of reflection from $PBS_2$, $FC_7$, and IM. The last peak indicates the reflection from the laser at Alice. It is worth noting that the reflections from all the components in the encoder can be detected, meaning that the polarization coding and intensity coding information are leaked.

Figure 3(b) shows the experimental result of THA on encoder $B$. The first two peaks are reflections from Eve's setup, which correspond to Eve's CIR and the $FC_1$ at the exit of Alice, respectively. The third peak is the reflection from the end face of Alice's CIR. According to the optical path analysis in Ref. [61], the fourth peak marked as $FM_1$ indicates the horizontal output reflected from $FM_1$. Similarly, the fifth (sixth) peak represents the vertical (horizontal) reflections from $FM_2$ ($FM_3$) as noted. $FM_{1,2}$ implies the superposition of vertical reflections from $FM_1$ and horizontal reflections from $FM_2$. Different from the sixth peak, the eighth peak denotes the total vertical reflection from $FM_3$. Due to the imperfection of the FMs, a small portion of H pulses (V pulses) cannot be reversed to V pulses (H pulses), resulting in undesired mixed outputs $P_1$, $P_2$, and $P_3$ from distinct beam paths. If the output power of Eve is increased, a series of equidistant reflection peaks can be observed. These peaks result from the repeated reflections between FMs and ports of the PBS, appearing behind $P_3$. It is important to note that the series of peaks after $C_A$ (i.e., the third peak) may all contain polarization-encoding information.

Figure 4(b) shows the experimental result of THA on encoder $C$. The first three peaks represent the reflections from Eve's CIR, the FC connecting Eve and Alice, and Alice's CIR in turn. The last peak is the reflection from the PBS in the POGNAC ring, which contains Alice's polarization-encoding information.

It is worth noting that a distinct difference among the three encoders is that the peak of the IM cannot be observed in encoder $B$ [Fig. 3(b)] and encoder $C$ [Fig. 4(b)]. This is due to Eve injecting THPs from port 3 of the CIR to the Alice side, and there is no coupling between port 3 and port 1 inside the CIR. Consequently, after transmission from port 3 to port 1 of the CIR, the intensity of the THPs is significantly weakened. Moreover, all encoders are interconnected using fiber connectors. In commercial systems, fiber fusion is employed instead of connectors, resulting in minimal reflection. This would not impact the results as the primary source of reflection is from other optical components, excluding connectors.

## III. SIMULATION

### A. Estimating the reflectivity

Based on the experimental results of reflections from optical components in the beam path, we calculate the total reflectivity and corresponding information leakage of each encoder. Table I shows the calculation data of encoders, and we take the data of encoder $A$ as an example to briefly explain the data processing. To determine the reflectivity of each module, we need to count the number of photons sent by Eve and calculate the number of photons reflected by the module that may cause information leakage. The corresponding number of single photons per second of Eve's laser output was

$$N_E = \frac{P_E}{E_1} = \frac{P_E}{hc/\lambda}, \tag{1}$$

where the intensity of incident light from Eve is $P_E = -40.003$ dBm, $E_1$ is the single-photon energy at 1550nm, $h = 6.6 \times 10^{-34}$ J is the Planck constant, and $c = 3 \times 10^8$ m/s is the light speed. So we can get that the corresponding number of single photons per second of Eve's laser output is $7.789 \times 10^{11}$/s. To obtain the total number of reflected photons of encoder $A$, we count all the reflection peaks that might lead to information leakage [peaks after $FC_1$ in Fig. 2(b)] and calculate the total number of photons leaked per second as $N_R = 1.35 \times 10^4$/s. Therefore, the total reflectivity of encoder $A$ is

$$R_A = \frac{N_R}{N_E \times \eta_E}, \tag{2}$$

where $\eta_E = 10\%$ denotes the detection efficiency of Eve's SPAD. By inputting the data in Table I, we get $R_A = R_A^{\mathrm{IM}} + R_A^{\mathrm{PM}} = 1.733 \times 10^{-7}$ (i.e., $-67.612$ dB), where the superscripts IM and PM denote the reflectivity from IM and PM, receptively, where $R_A^{\mathrm{IM}} = 9.629 \times 10^{-10}$ (i.e., $-90.164$ dB) and $R_A^{\mathrm{PM}} = 1.478 \times 10^{-7}$ (i.e., $-68.304$ dB).

Following the definition of $\mu_{\mathrm{out}}$, which represents the mean photon number of the THPs retrieved by Eve and is utilized to estimate the maximum information leakage against THA [38], we obtain

$$\mu_{\mathrm{out}} = \frac{\mu_e \gamma}{f}, \tag{3}$$

where $\mu_e = 10^{20}$/s represents the laser-induced damage threshold of optical devices [38]. Here, $f$ is the clock rate of

TABLE II. Leaking mean photon number of each encoder in the simulation of BB84-QKD and MDI-QKD. We set the $\mu_{\text{out}}$ of the IM in encoders $B$ and $C$ to zero since the reflection peaks of the IM in those encoders were not observed in our experiments.

| | BB84-QKD | | MDI-QKD | |
|---|---|---|---|---|
| $\mu_{\text{out}}$ | $\mu_{\text{out}}^{\text{IM}}$ | $\mu_{\text{out}}^{\text{PM}}$ | $\mu_{\text{out}}^{\text{IM}}$ | $\mu_{\text{out}}^{\text{PM}}$ |
| Encoder $A$ | $1.926 \times 10^{-9}$ | $2.956 \times 10^{-7}$ | $7.704 \times 10^{-14}$ | $1.182 \times 10^{-11}$ |
| Encoder $B$ | | $5.606 \times 10^{-8}$ | | $2.242 \times 10^{-12}$ |
| Encoder $C$ | | $4.544 \times 10^{-8}$ | | $1.818 \times 10^{-12}$ |

Alice's encoder, and $\gamma$ is defined as

$$\gamma = \beta \times R_A. \tag{4}$$

Here, $\beta$ is denoted as an additional isolation factor that comprehensively considers the optical filter, attenuator, and isolator. $R_A$ represents the total reflection of encoder $A$.

In the simulation of BB84-QKD, we set $f$ to 50 MHz [49]. The additional isolation at Alice is −120 dB. Consequently, we obtained the leaked information from the IM and PM of encoder $A$ as $\mu_{\text{out}}^{\text{IM}} = 1.926 \times 10^{-9}$ and $\mu_{\text{out}}^{\text{PM}} = 2.956 \times 10^{-7}$. Similarly, in the simulation of MDI-QKD, with the system clock rate $f$ set to 1.25 GHz [35] and the same additional isolation at Alice being −150 dB, we obtained the leaked information from the IM and PM of encoder $A$ as $\mu_{\text{out}}^{\text{IM}} = 7.704 \times 10^{-14}$ and $\mu_{\text{out}}^{\text{PM}} = 1.182 \times 10^{-11}$.

Using the same method, we obtained the leaking mean photon $\mu_{\text{out}}$ for encoder $B$ and $C$ by processing the data in Table I, which are summarized in Table II.

Here, the additional isolation at Alice used in the calculations for the three different encoders was set to the same (i.e., −120 dB) in BB84-QKD and -150 dB in MDI-QKD, so that we can compare the resistance of three encoders against THAs.

Additionally, as shown in Table I, the intensities of THPs used in experiments with three different encoders were distinct in order to show complete reflection peaks. But they are required to be lower than the upper bound of the Trojan injected pulse, which is determined by the laser-induced damage threshold (≈4.6 W) [32]. The reflectivity is a ratio that is independent of the incident laser intensity; thus, the intensity differences in experiments of diverse encoders caused no change in results. Since the components (such as CIRs) that provide isolation at Alice's output might be damaged by intense THPs, these components should not be considered as the effective isolation required to resist THAs [32]. Therefore, only the reflections on the right-hand side of the $C_A$ peaks were taken into account when calculating the total reflectivity of encoder $B$ or $C$.

Obviously, the results of data processing indicate that the reflectivity and information leakages of encoder $A$ are larger than those of encoder $B$ or $C$, indicating that encoder $B$ and $C$ own better resistance against THAs.

It is worth mentioning that the purpose of adding isolation at Alice was to distinguish the resistance of each encoder against a THA rather than make the key rate of the system closer to that under a nonattack situation. Based on the $\mu_{\text{out}}$ mentioned above, we analyze the SKR of QKD systems with the three polarization encoders when BB84-QKD or MDI-QKD was applied. The SKR intuitively represents the resistance of different coding schemes against THAs.

TABLE III. Simulation parameters of BB84-QKD. $f$, frequency of the system in BB84-QKD simulation; $\eta_B$, detector efficiency; $P_{\text{dc}}$, background rate; $f_{\text{EC}}$, error-correction efficiency; $e_0$, total error rate; $\varepsilon_{\text{sec}}$, secrecy parameter; $\varepsilon_{\text{cor}}$, correctness parameter; $N$, total pulses sent by Alice.

| $f$ | $\eta_B$ | $P_{\text{dc}}$ | $f_{\text{EC}}$ | $e_0$ | $\varepsilon_{\text{sec}}$ | $\varepsilon_{\text{cor}}$ | $N$ |
|---|---|---|---|---|---|---|---|
| $5 \times 10^7$ | 0.1 | $6 \times 10^{-7}$ | 1.16 | 0.01 | $10^{-9}$ | $10^{-15}$ | $10^{13}$ |

### B. BB84

To simulate the SKRs of the three encoders while the BB84 protocol is applied, we employ the SKR analysis of the finite keys BB84-QKD protocol with two decoy states proposed in Ref. [67], combining with the security bounds against THA in Ref. [38]. According to Ref. [67], the length of the final secure key is given by

$$l \geqslant s_{z,0}^{-} + s_{z,1}^{-}\left[1 - h\left(e_{z,1}^{t}\right)\right] - \lambda_{\text{EC}} - 6\log_2\frac{21}{\varepsilon_{\text{sec}}} - \log_2\frac{2}{\varepsilon_{\text{cor}}} \tag{5}$$

where $s_{z,1}^{-}$ ($s_{z,0}^{-}$) is the lower bound of the number of Alice sent single-photon (vacuum) pulses in the $z$ basis; $e_{z,1}^{t}$ is the phase error rate when THA is taken into account. $\lambda_{\text{EC}}$ is the number of announced bits when Alice and Bob perform an error-correction step. $\varepsilon_{\text{sec}}$ and $\varepsilon_{\text{cor}}$ are the secrecy and correctness parameters, respectively. And $h(x)$ is the binary Shannon entropy function, given by

$$h(x) = -x\log_2(x) - (1-x)\log_2(1-x). \tag{6}$$

The calculating details will be given in Appendix B 1. The experimental parameters in the simulation are listed in Table III. Using the genetic algorithm [68], we numerically optimized the SKR over the free simulation parameters $\{\mu,\ \nu,\ p_\mu,\ p_\nu,\ q_z\}$, where $\mu$ and $\nu$ are the intensity of signal and decoy state, respectively; $p_\mu$ ($p_\nu$) is the probability of $\mu$ ($\nu$) sent by Alice; $q_z$ is the probability of Alice choosing the $z$ basis.

Figure 5 shows the SKRs of the three encoders while the BB84-QKD protocol is applied. The SKRs are plotted as a function of the signal transmission distance. The SKR of the QKD system with encoder $A$ drops quicker than that of the system with encoder $B$ or $C$ as the transmission distance increases. At a specified SKR, such as SKR $= 10^{-5}$ bit/pulse, the furthest supporting distance of the system with encoder $A$ is about 71.1 km, while those of encoder $B$ and $C$ can reach 146.9 and 147.1 km separately. The reason for these phenomena is mainly because the system with encoder $B$ or $C$ has a CIR, which provides isolation at the Alice output. The curve labeled with $\mu_{\text{out}} = 0$, which indicates the situation without THA and information leakage, is given as a reference. With the addition of 120-dB isolation, the SKRs of the encoder $B$ and $C$ are nearly comparable to $\mu_{\text{out}} = 0$ (i.e., without THA) within 145 km, the SKR of encoder $A$ starts decreasing

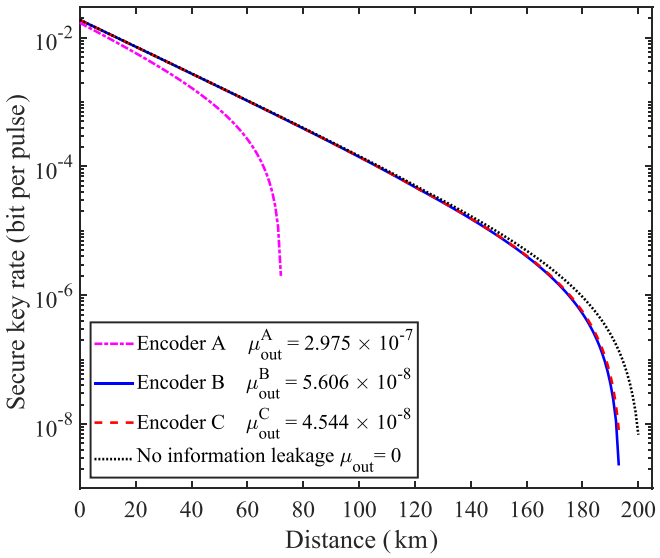


FIG. 5. The SKRs of BB84-QKD systems with encoder $A$, $B$, and $C$, corresponding to the magenta dash-dotted line, the blue solid line, and the red dashed line, respectively. The corresponding $\mu_{\text{out}}$ of each encoder is $\mu_{\text{out}}^{A} = 2.975 \times 10^{-7}$, $\mu_{\text{out}}^{B} = 5.606 \times 10^{-8}$, and $\mu_{\text{out}}^{C} = 4.544 \times 10^{-8}$. The curve labeled with $\mu_{\text{out}} = 0$ indicates the situation without THA and information leakage, corresponding to the black dotted line.

significantly once the distance exceeds 60 km. Furthermore, at distances of less than 180 km, the SKRs of encoders $B$ and $C$ almost overlap. Obviously, encoder $C$ has a better ability to resist THA than encoder $B$ and $A$ when applied to BB84-QKD, and $A$ has a weaker ability to resist THA than $B$ and $C$. The SKR of encoder $B$ starts to decrease at 138 km, which means encoder $C$ has better resistance than encoder $B$ against THA.

### C. MDI-QKD

The SKRs of MDI-QKD systems with encoder $A$, $B$, or $C$ were calculated by employing the analysis of finite length SKR reported by Tan *et al.* [35]. The actual security bounds [38], information leakage caused by the IM and PM [39], as well as the finite length analysis [44] were comprehensively considered in the calculation. According to Ref. [69], the SKR is given by

$$R = p_{s_A} p_{s_B} \left\{ (s_A e^{-s_A})(s_B e^{-s_B}) Y_{11}^{x,l} \left[1 - h\left(e_{11}^{x,t}\right)\right] - f_{\text{EC}} Q_z^{ss} h\left(E_z^{ss}\right) \right\} \tag{7}$$

where $s_A$ ($s_B$) is the intensity of the signal states sent by Alice (Bob), and $p_{s_A}$ ($p_{s_B}$) is the probability of Alice (Bob) choosing them; $Y_{11}^{x,l}$ is the lower bound of the single-photon yield in the $x$ basis; $e_{11}^{x,t}$ is the error rate when THA is taken into account; $f_{\text{EC}}$ is the error correction efficiency; $Q_z^{ss}$ ($E_z^{ss}$) is the gain (QBER) in the $z$ basis, which can be obtained directly in the experiment; $h(x)$ is the binary Shannon entropy function. The calculating details will be given in Appendix B 2. The simulation parameters are listed in Table IV. We use the genetic algorithm [68] to numerically optimize the intensity of signal state $s$ and the decoy state ($\mu$, $\nu$), as well as the probability that Alice chose them ($p_s$, $p_\mu$, $p_\nu$).

TABLE IV. Simulation parameters of MDI-QKD. $f$, frequency of the MDI-QKD system in simulation; $\eta_B$, detector efficiency; $P_{\text{dc}}$, background rate; $f_{\text{EC}}$, error-correction efficiency; $e_0$, error rate of the dark rate; $e_d$, total misalignment error; $N$, total pulse pairs sent by Alice and Bob.

| $f$ | $\eta_B$ | $P_{\text{dc}}$ | $f_{\text{EC}}$ | $e_0$ | $e_d$ | $N$ |
|---|---|---|---|---|---|---|
| $1.25 \times 10^9$ | 0.495 | $8 \times 10^{-8}$ | 1.16 | 0.5 | 0.02 | $10^{13}$ |

Figure 6 shows the SKRs of MDI-QKD systems with encoder $A$, $B$, or $C$, respectively. Similar to the BB84 systems discussed above, the SKR of the MDI-QKD system with encoder $A$ drops quicker than that of the other two. At a given SKR $= 10^{-6}$ bit/pulse, the signal transmission distance of the system with encoder $A$ is 59.3 km while that of the systems with encoder $B$ or $C$ is 125.4 and 125.5 km respectively. With the addition of 150-dB isolation, the SKRs of the encoder $B$ and $C$ are nearly comparable to $\mu_{\text{out}} = 0$ (i.e., without THA) within 140 km. The SKR of encoder $A$ falls more quickly when the distance exceeds 55 km. Encoders $B$ and $C$ almost overlap in SKR at distances under 160 km. The SKR of the MDI-QKD system with encoder $B$ or $C$ can maintain a longer distance thanks to the additional isolation at the Alice output.

For a comparative analysis of the security levels of encoders, we present the simulated SKR corresponding to different $\mu_{\text{out}}$ in both the BB84-QKD and MDI-QKD protocols. Additionally, we mark the different $\mu_{\text{out}}$ of the three encoders at a transmission distance of 100 km. Here, we assume the amount of leakage from the IM is zero to more closely match the realistic $\mu_{\text{out}}$ of the three encoders. The results are shown in Figs. 7(a) and 7(b). It can be seen that when $\mu_{\text{out}}$ reaches the level of $10^{-7}$ in BB84 and $10^{-12}$ in

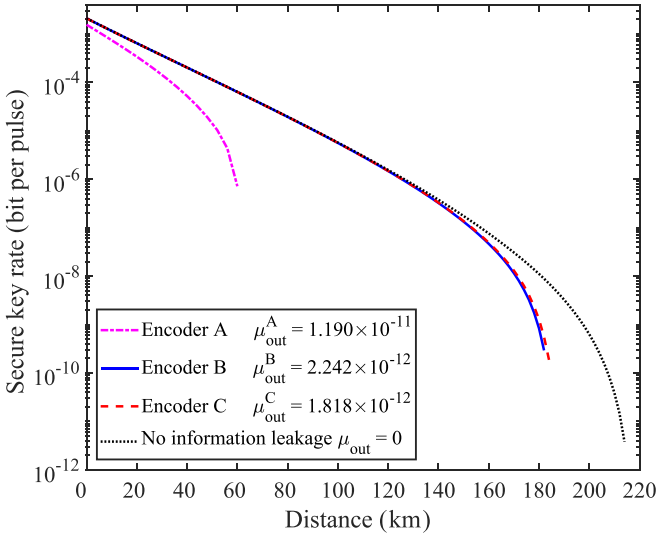


FIG. 6. The SKRs of MDI-QKD systems with encoder $A$, $B$, and $C$, corresponding to the magenta dash-dotted line, the blue solid line, and the red dashed line, respectively. The corresponding $\mu_{\text{out}}$ of each encoder is $\mu_{\text{out}}^{A} = 1.190 \times 10^{-11}$, $\mu_{\text{out}}^{B} = 2.242 \times 10^{-12}$, and $\mu_{\text{out}}^{C} = 1.818 \times 10^{-12}$. The curve labeled with $\mu_{\text{out}} = 0$ indicates the situation without THA and information leakage, corresponding to the black dotted line.

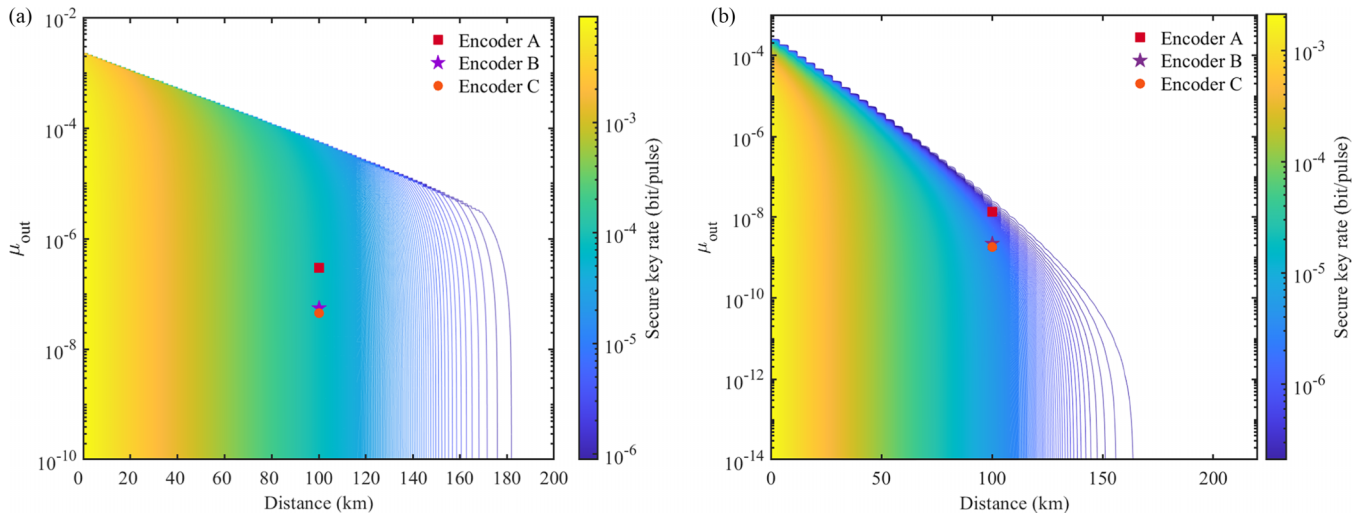


FIG. 7. (a) The SKR for the BB84-QKD protocol under the THA with various values of $\mu_{out}$. The red square marks the corresponding $\mu_{out}$ and SKR of encoder $A$ at 100 km, and the purple star and orange circle represent encoder $B$ and $C$, respectively. (b) The SKR for the MDI-QKD protocol under the THA corresponding to various values of $\mu_{out}$. The red square, purple star, and orange circle mark the corresponding $\mu_{out}$ and SKR at 100 km of encoder $A$, $B$, and $C$, respectively.

MDI-QKD, the SKR almost perfectly overlaps with that without THA. Furthermore, the tested encoder is secure against THA with additional isolation.

## IV. CONCLUSION AND DISCUSSION

We experimentally and theoretically evaluated the resistance of three polarization encoders in QKD systems against THAs. We estimate quantitative security bounds based on the experimental parameters, accounting for finite-size effects. Specifically, we simulate SKRs of QKD systems with different encoders under BB84-QKD or MDI-QKD protocols to evaluate their security against THAs.

Simulation results demonstrated that systems with encoder $B$ or $C$ performed better than systems with encoder $A$ thanks to a CIR that provided about 55-dB isolation at Alice output. Our experimental results demonstrated that an additional isolator or CIR at the Alice output end could effectively reduce the reflection intensity of THPs so as to reduce the information leakage. Our research serves as a reference for designing and constructing secure polarization coding schemes for QKD manufacturers. It also supplements standardization in testing and security evaluation of QKD modules, thereby reducing the risk of security failures during operation.

In the future, finite-length analysis proposed in Ref. [45] will be employed to calculate the system SKR in our paper. The information leakage caused by IMs or PMs will also be estimated separately for more details.

## ACKNOWLEDGMENTS

This study was supported by the National Natural Science Foundation of China (Grants No. 62171144, No. 11905065, and No. 62365001), the Guangxi Science Foundation (Grants No. 2021GXNSFAA220011 and No. 2021AC19384), the Open Fund of IPOC (BUPT) (Grant No. IPOC2021A02), and the Innovation Project of Guangxi Graduate Education (Grant No. YCSW2022040).

## APPENDIX A: DETAILS OF EXPERIMENTAL DATA

Here, we list the corresponding data of reflection peaks in each encoder, which are plotted in Figs. 2(b), 3(b), and 4(b), respectively. The details are shown in Table V.

## APPENDIX B: DETAILS OF THE SIMULATION

### 1. BB84

According to Ref. [67], the length of the final secure key is given by

$$l \geqslant s^{-}_{z,0} + s^{-}_{z,1}\left[1 - h\left(e^{t}_{z,1}\right)\right] - \lambda_{\mathrm{EC}} - 6\log_2\frac{21}{\varepsilon_{\mathrm{sec}}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}} \tag{B1}$$

where $s^{-}_{z,1}$ ($s^{-}_{z,0}$) is the lower bound of the number of Alice sent single-photon (vacuum) pulses in the $z$ basis and $e^{t}_{z,1}$ is the phase error rate when THA is taken into account. $\lambda_{\mathrm{EC}}$ is the number of announced bits when Alice and Bob perform an error-correction step. $\varepsilon_{\mathrm{sec}}$ and $\varepsilon_{\mathrm{cor}}$ are the secrecy and correctness parameters, respectively. And $h(x)$ is the binary Shannon entropy function, given by

$$h(x) = -x\log_2(x) - (1-x)\log_2(1-x). \tag{B2}$$

Next, we simply calculate each term in Eq. (B1). In the asymptotic limit, for all intensities $j \in \{\mu, \nu_1, \nu_2\}$, the total number of detections in specific basis $b \in \{x, z\}$ is given by

$$n^{*}_{b,j} = \sum_{n=0}^{\infty} p_{j|n} s_{b,n} \tag{B3}$$

and the conditional probability is given by $p_{j|n} = \frac{p_j}{\tau_n}\frac{e^{-j}j^n}{n!}$, where $\tau_n = \sum_j p_j e^{-j} j^n/n!$ is the total probability of $n$-photon states that Alice prepared.

TABLE V. Corresponding data of reflection peaks of each encoder.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Peaks of encoder $A$ | $C_E$ | $FC_1$ | $FC_2$ | $PBS_1$ | $FC_{3,4}$ | $PM_{1,2}$ | $FC_{5,6}$ | $PBS_2$ | $FC_7$ | IM | $LD_A$ |
| Reflectivity (dB) | −80.282 | −90.464 | −92.013 | −81.689 | −85.204 | −86.766 | −95.693 | −85.734 | −96.874 | −90.164 | −90.921 |
| Peaks of encoder $B$ | $C_E$ | $FC_1$ | $C_A$ | $FM_1$ | $FM_2$ | $FM_3$ | $FM_{1,2}$ | $FM_3$ | $P_1$ | $P_2$ | $P_3$ |
| Reflectivity (dB) | −79.825 | −93.819 | −83.766 | −88.485 | −90.893 | −94.901 | −100.579 | −101.066 | −104.303 | −105.351 | −107.983 |
| Peaks of encoder $C$ | $C_E$ | $FC_1$ | $C_A$ | PBS | | | | | | | |
| Reflectivity (dB) | −80.616 | −92.372 | −84.616 | −86.437 | | | | | | | |

When the finite key size is considered, Hoeffding's inequality [70] can be employed to bound the fluctuation, so we can get that

$$|n^*_{b,j} - n_{b,j}| \leqslant \delta(n_b, \varepsilon_1), \tag{B4}$$

where Hoeffding's inequality is defined as $\delta(n_b, \varepsilon_1) := \sqrt{n_b/2ln(1/\varepsilon_1)}$. The inequality above holds when the probability is at least $1 - 2\varepsilon_1$.

According to the above inequality, we have the upper bound and lower bound of $n^*_{b,j}$ as follows:

$$\begin{aligned} n^*_{b,j} &\leqslant n_{b,j} + \delta(n_{b,j}, \varepsilon_1) = n^+_{b,j}, \\ n^*_{b,j} &\geqslant n_{b,j} - \delta(n_{b,j}, \varepsilon_1) = n^-_{b,j}. \end{aligned} \tag{B5}$$

Similarly, the expected number of errors and the observed number of errors have the same relation. In the asymptotic case, for all intensities, we have

$$m^*_{b,j} = \sum_{n=0}^{\infty} p_{j|n} v_{b,n}, \tag{B6}$$

where $v_{b,n}$ is the number of errors detected by Bob with $n$-photon events. By employing Hoeffding's inequality [70], we can get

$$|m^*_{b,j} - m_{b,j}| \leqslant \delta(m_b, \varepsilon_2), \tag{B7}$$

with a probability of at least $1 - 2\varepsilon_2$. By solving inequality (B7), we thus know the upper bound and lower bound of $m^*_{b,j}$:

$$\begin{aligned} m^*_{b,j} &\leqslant m_{b,j} + \delta(m_b, \varepsilon_2) = m^+_{b,j}, \\ m^*_{b,j} &\geqslant m_{b,j} - \delta(m_b, \varepsilon_2) = m^-_{b,j}. \end{aligned} \tag{B8}$$

According to the method proposed in Ref. [67], we have the lower bound of the vacuum counts in the $z$ basis as follows:

$$s_{z,0} \geqslant s^-_{z,0} := \frac{\tau_0}{(\nu_1 - \nu_2)} \left( \frac{\nu_1 e^{\nu_2} n^-_{z,\nu_2}}{p_{\nu_2}} - \frac{\nu_2 e^{\nu_1} n^+_{z,\nu_1}}{p_{\nu_1}} \right). \tag{B9}$$

The single-photon events, which make a main contribution to the secret key, satisfy the following formula [67]:

$$\begin{aligned} s_{z,1} \geqslant s^-_{z,1} := {} & \frac{\mu \tau_1}{\mu(\nu_1 - \nu_2) - \nu_1^2 + \nu_2^2} \\ & \times \left[ \frac{e^{\nu_1} n^-_{z,\nu_1}}{p_{\nu_1}} - \frac{e^{\nu_2} n^+_{z,\nu_2}}{p_{\nu_2}} + \frac{\nu_1^2 - \nu_2^2}{\mu^2} \left( \frac{s_{z,0}}{\tau_0} - \frac{e^{\mu} n^+_{z,\mu}}{p_{\mu}} \right) \right]. \end{aligned} \tag{B10}$$

The upper bound on the number of single-photon phase errors in the $z$ basis can be estimated by the bit errors in the $x$ basis as [67]

$$e^+_{z,1} := \frac{c_{z,1}}{s_{z,1}} \leqslant \frac{v_{x,1}}{s_{x,1}} + \gamma \left( \varepsilon_{\text{sec}}, \frac{v_{x,1}}{s_{x,1}}, s_{x,1}, s_{z,1} \right), \tag{B11}$$

where

$$\gamma(a, b, c, d) = \sqrt{\frac{(c+d)(1-b)b}{cd \log 2} \log_2 \left( \frac{c+d}{cd(1-b)b} \frac{21^2}{a^2} \right)} \tag{B12}$$

and

$$v_{x,1} \leqslant \frac{\tau_1}{\nu_1 - \nu_2} \left( \frac{e^{\nu_1} m^+_{x,\nu_1}}{p_{\nu_1}} - \frac{e^{\nu_2} m^-_{x,\nu_2}}{p_{\nu_2}} \right). \tag{B13}$$

Here, we consider the impact of THA on the number of single-photon errors $e^+_{z,1}$:

$$\begin{aligned} e^t_{z,1} = {} & e^+_{z,1} + 4\Delta'(1-\Delta')(1 - 2e^+_{z,1}) \\ & + 4(1 - 2\Delta')\sqrt{\Delta'(1-\Delta')e^+_{z,1}(1 - e^+_{z,1})}, \\ \Delta = {} & \frac{1 - \exp(-\mu_{\text{out}}) \cos(\mu_{\text{out}})}{2}, \\ \Delta' = {} & \frac{\Delta}{Y^l_1}. \end{aligned} \tag{B14}$$

We use the trace-distance argument to determine the deviations introduced by THA, and the trace distance $D_{jj'}$ can be expressed as

$$\begin{aligned} \left| Y^j_n - Y^{j'}_n \right| &\leqslant D_{jj'}, \\ \left| Y^j_n e^j_n - Y^{j'}_n e^{j'}_n \right| &\leqslant D_{jj'}, \end{aligned} \tag{B15}$$

where $j, j' \in \{\mu, \nu_1, \nu_2\}$ are the intensities selected by Alice, and $Y_n$ and $e_n$ are the yield and the error rate of $n$-photon signals under the THA, respectively. The lower bound of $Y_1$ is given by [71]

$$\begin{aligned} Y_1 \geqslant Y^l_1 = {} & \frac{\mu}{\mu(\nu_1 - \nu_2) - \nu_1^2 + \nu_2^2} \\ & \times \left[ Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} \left( Q_\mu e^\mu - Y^l_0 \right) \right], \end{aligned} \tag{B16}$$

where $Q_\mu$, $Q_{\nu_1}$, and $Q_{\nu_2}$ are the gains for signal states and decoy states, respectively. $Y^l_0$ is the lower bound of single-photon gain, which is given by

$$Y^l_0 = \max \left\{ \frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, 0 \right\}. \tag{B17}$$

### 2. MDI-QKD

According to Ref. [69], the SKR is given by

$$R = p_{s_A} p_{s_B} \{(s_A e^{-s_A})(s_B e^{-s_B}) Y_{11}^{x,l} [1 - h(e_{11}^{x,t})] - f_{\mathrm{EC}} Q_z^{ss} h(E_z^{ss})\}, \tag{B18}$$

where $s_A$ ($s_B$) is the intensity of the signal states sent by Alice (Bob), and $p_{s_A}$ ($p_{s_B}$) is the probability of Alice (Bob) choosing them; $Y_{11}^{x,l}$ is the lower bound of the single-photon yield in the $x$ basis; $e_{11}^{x,t}$ is the error rate when THA is taken into account; $f_{\mathrm{EC}}$ is the error correction efficiency; $Q_z^{ss}$ ($E_z^{ss}$) is the gain (QBER) in the $z$ basis, which can be obtained directly in the experiment; $h(x)$ is the binary Shannon entropy function.

In the estimation of the MDI-QKD channel model, the gains and QBERs in the $x$ and $z$ basis can be expressed as

$$\begin{aligned} Q_z^{\mu\nu} &= Q_c + Q_e, \\ Q_x^{\mu\nu} &= 2y^2[1 + 2y^2 - 4yI_0(x) + I_0(2x)], \\ E_x^{\mu\nu} Q_x^{\mu\nu} &= e_0 Q_x^{\mu\nu} - 2(e_0 - e_d)y^2[I_0(2x) - 1], \\ E_z^{\mu\nu} Q_z^{\mu\nu} &= e_d Q_c + (1 - e_d) Q_e, \end{aligned} \tag{B19}$$

where $\mu$ and $\nu$ are the intensities of signal and decoy states sent by Alice and Bob; $I_0(x)$ is the modified Bessel function of the first kind; $e_d$ is the total misalignment error; $e_0$ is the error rate of the dark count; and

$$\begin{aligned} Q_c &= 2(1 - p_d)^2 e^{-\mu'/2}[1 - (1 - p_d)e^{-\eta_a \mu/2}] \\ &\quad \times [1 - (1 - p_d)e^{-\eta_b \nu/2}], \\ Q_e &= 2p_d(1 - p_d)^2 e^{-\mu'/2}[I_0(2x) - (1 - p_d)e^{-\mu'/2}], \end{aligned} \tag{B20}$$

and

$$\begin{aligned} x &= \sqrt{\eta_a \mu \eta_b \nu}/2, \\ y &= (1 - p_d)e^{-\mu'/4}, \\ \mu' &= \eta_a \mu + \eta_b \nu, \end{aligned} \tag{B21}$$

where $\eta_a$ ($\eta_b$) is the total efficiency that Alice (Bob) transmitted the quantum states.

The gains and QBERs can be expressed as

$$\begin{aligned} Q_b^{jk} &= \frac{n_b^{jk}}{N p_j p_k p_b} = \sum_{n,m=0}^{\infty} (p_n^j p_m^k Y_{nm}^b), \\ Q_b^{jk} E_b^{jk} &= \frac{m_b^{jk}}{N p_j p_k p_b} = \sum_{n,m=0}^{\infty} (p_n^j p_m^k Y_{nm}^b e_{nm}^b), \end{aligned} \tag{B22}$$

where $p_j$ ($p_k$) is the probability of Alice or Bob selecting the intensity $j$ ($k$); $p_b$ is the probability of Alice and Bob choosing the $b$ basis ($b \in \{x, z\}$); $N$ is the total number of pulse pairs sent by Alice and Bob; $n_b^{jk}$ and $m_b^{jk}$ are the observed and error counts, respectively; $p_n^j$ ($p_m^k$) denotes the probability that Alice or Bob send an $n$-photon (m-photon) pulse with intensity $j$ ($k$); $Y_{nm}^b$ ($e_{nm}^b$) donates the yield (error rate) when Alice sends an $n$-photon pulse and Bob sends an $m$-photon one.

We can use the trace-distance argument to determine the deviations introduced by THA, and the trace distance $D_b^{jk,gh}$ can be expressed as

$$\begin{aligned} \left| Y_{nm}^{jk,b} - Y_{nm}^{gh,b} \right| &\leqslant D_b^{jk,gh}, \\ \left| e_{nm}^{jk,b} Y_{nm}^{jk,b} - e_{nm}^{gh,b} Y_{nm}^{gh,b} \right| &\leqslant D_b^{jk,gh}, \end{aligned} \tag{B23}$$

where $j, k, g, h \in \{\mu, \nu, \omega\}$. By solving the inequalities above, we have

$$\begin{aligned} \overline{Q_b^{jk}} &= Q_b^{jk} + \sigma \sqrt{\frac{Q_b^{jk}}{N p_j p_k p_b}} + D_b^{jk,gh}, \\ \underline{Q_b^{jk}} &= Q_b^{jk} - \sigma \sqrt{\frac{Q_b^{jk}}{N p_j p_k p_b}} - D_b^{jk,gh}, \\ \overline{T_b^{jk}} &= T_b^{jk} + \sigma \sqrt{\frac{T_b^{jk}}{N p_j p_k p_b}} + D_b^{jk,gh}, \\ \underline{T_b^{jk}} &= T_b^{jk} - \sigma \sqrt{\frac{T_b^{jk}}{N p_j p_k p_b}} - D_b^{jk,gh}, \end{aligned} \tag{B24}$$

where ${T_b}^{jk} = Q_b^{jk} E_b^{jk}$, and $\sigma$ is the standard deviation for statistical fluctuation analysis.

Based on the estimation method proposed in Ref. [72], the major task of the SKR analysis is to tightly estimate the lower bound of $Y_{11}^x$ and the upper bound of $e_{11}^x$, which are shown in Eqs. (B25) and (B27), respectively:

$$Y_{11}^{x,l} = \frac{(\mu^2 - \omega^2)(\mu - \omega)\underline{Q^{M_1}} - (\nu^2 - \omega^2)(\nu - \omega)\overline{Q^{M_2}}}{(\mu - \omega)^2(\nu - \omega)^2(\mu - \nu)}, \tag{B25}$$

where

$$\begin{aligned} \underline{Q^{M_1}} &= e^{2\nu} \underline{Q_x}^{\nu\nu} - e^{\nu+\omega} \overline{Q_x^{\nu\omega}} - e^{\omega+\nu} \overline{Q_x^{\omega\nu}} + e^{2\omega} \underline{Q_x^{\omega\omega}}, \\ \overline{Q^{M_2}} &= e^{2\mu} \overline{Q_x^{\mu\mu}} - e^{\mu+\omega} \underline{Q_x^{\mu\omega}} - e^{\omega+\mu} \underline{Q_x^{\omega\mu}} + e^{2\omega} \overline{Q_x^{\omega\omega}}, \end{aligned} \tag{B26}$$

and

$$e_{11}^{x,u} = \frac{e^{2\nu} \overline{T_x^{\nu\nu}} + e^{2\omega} \overline{T_x^{\omega\omega}} - e^{\nu+\omega} \underline{T_x^{\nu\omega}} - e^{\omega+\nu} \underline{T_x^{\omega\nu}}}{(\nu - \omega)^2 Y_{11}^{x,l}}. \tag{B27}$$

Base on Ref. [15], we have the following relation:

$$\begin{aligned} e_{11}^{x,t} &= e_{11}^{x,u} + 4\Delta'(1 - \Delta')(1 - 2e_{11}^{x,u}) \\ &\quad + 4(1 - 2\Delta')\sqrt{\Delta'(1 - \Delta')e_{11}^{x,u}(1 - e_{11}^{x,u})}, \end{aligned} \tag{B28}$$

where

$$\begin{aligned} \Delta &= \frac{1 - \exp(-2\mu_{\mathrm{out}}) \cos^2(\mu_{\mathrm{out}})}{2}, \\ \Delta' &= \frac{\Delta}{Y_{11}^{x,l}}. \end{aligned} \tag{B29}$$

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) **557**, 400 (2018).

[3] M. Curty, K. Azuma, and H.-K. Lo, npj Quantum Inf. **5**, 64 (2019).

[4] P. Zeng, H. Zhou, W. Wu, and X. Ma, Nat. Commun. **13**, 3903 (2022).

[5] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, PRX Quantum **3**, 020315 (2022).

[6] W. Wang, R. Wang, C. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, and H.-K. Lo, Phys. Rev. Lett. **130**, 220801 (2023).

[7] F. Grünenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hänggi, N. Bosshard, F. Bussières, and H. Zbinden, Nat. Photon. **17**, 422 (2023).

[8] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Appl. Phys. Lett. **117**, 144003 (2020).

[9] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Nat. Photon. **15**, 570 (2021).

[10] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, Nat. Photon. **15**, 530 (2021).

[11] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nat. Photon. **16**, 154 (2022).

[12] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, Z. Zhou, Z.-H. Wang, J. Teng, G.-C. Guo, and Z.-F. Han, Optica **9**, 812 (2022).

[13] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **130**, 210801 (2023).

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

[15] H.-K. Lo and J. Preskill, Quantum. Inf. Comput. **7**, 431 (2006).

[16] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).

[17] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).

[18] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, Phys. Rev. A **94**, 030302(R) (2016).

[19] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Opt. Express **26**, 21020 (2018).

[20] K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, npj Quantum Inf. **4**, 8 (2018).

[21] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. Appl. **10**, 064062 (2018).

[22] K. Wei, W. Zhang, Y.-L. Tang, L. You, and F. Xu, Phys. Rev. A **100**, 022325 (2019).

[23] P. Chaiwongkhot, K. B. Kuntz, Y. Zhang, A. Huang, J.-P. Bourgoin, S. Sajeed, N. Lütkenhaus, T. Jennewein, and V. Makarov, Phys. Rev. A **99**, 062315 (2019).

[24] A. Huang, A. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Phys. Rev. Appl. **12**, 064043 (2019).

[25] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Optica **6**, 1178 (2019).

[26] X.-L. Pang, A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, and X.-M. Jin, Phys. Rev. Appl. **13**, 034008 (2020).

[27] P. Ye, W. Chen, G.-W. Zhang, F.-Y. Lu, F.-X. Wang, G.-Z. Huang, S. Wang, D.-Y. He, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. Appl. **19**, 054052 (2023).

[28] F.-Y. Lu, P. Ye, Z.-H. Wang, S. Wang, Z.-Q. Yin, R. Wang, X.-J. Huang, W. Chen, D.-Y. He, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, Optica **10**, 520 (2023).

[29] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).

[30] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

[31] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, Phys. Rev. Appl. **13**, 034017 (2020).

[32] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, PRX Quantum **3**, 040307 (2022).

[33] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, IEEE J. Sel. Top. Quantum Electron. **21**, 168 (2015).

[34] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, Sci. Rep. **7**, 8403 (2017).

[35] H. Tan, W. Li, L. Zhang, K. Wei, and F. Xu, Phys. Rev. Appl. **15**, 064038 (2021).

[36] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 123030 (2014).

[37] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, Phys. Rev. A **92**, 022304 (2015).

[38] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Phys. Rev. X **5**, 031030 (2015).

[39] K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).

[40] S. E. Vinay and P. Kok, Phys. Rev. A **97**, 042335 (2018).

[41] W. Wang, K. Tamaki, and M. Curty, New J. Phys. **20**, 083027 (2018).

[42] M. Pereira, M. Curty, and K. Tamaki, npj Quantum Inf. **5**, 62 (2019).

[43] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, Phys. Rev. A **99**, 062332 (2019).

[44] W. Wang, K. Tamaki, and M. Curty, Sci. Rep. **11**, 1678 (2021).

[45] Á. Navarrete and M. Curty, Quantum Sci. Technol. **7**, 035021 (2022).

[46] H.-J. Ding, J.-Y. Liu, X.-Y. Zhou, C.-H. Zhang, J. Li, and Q. Wang, Phys. Rev. Appl. **19**, 044022 (2023).

[47] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Opt. Express **18**, 8587 (2010).

[48] C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, Opt. Lett. **44**, 2398 (2019).

[49] D. Ma, X. Liu, C. Huang, H. Chen, H. Lin, and K. Wei, Opt. Lett. **46**, 2152 (2021).

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

[51] K. Wei, X. Hu, Y. Du, X. Hua, Z. Zhao, Y. Chen, C. Huang, and X. Xiao, Photon. Res. **11**, 1364 (2023).
[52] Y. Du, X. Zhu, X. Hua, Z. Zhao, X. Hu, Y. Qian, X. Xiao, and K. Wei, Chip **2**, 100039 (2023).
[53] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou *et al.*, Nature (London) **549**, 43 (2017).
[54] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu *et al.*, Phys. Rev. Lett. **120**, 030501 (2018).
[55] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, npj Quantum Inf. **7**, 93 (2021).
[56] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. w. Boyd, and E. Karimi, Opt. Express **26**, 22563 (2018).
[57] C.-Q. Hu, Z.-Q. Yan, J. Gao, Z.-Q. Jiao, Z.-M. Li, W.-G. Shen, Y. Chen, R.-J. Ren, L.-F. Qiao, A.-L. Yang, H. Tang, and X.-M. Jin, Photon. Res. **7**, A40 (2019).
[58] Z. Feng, S. Li, and Z. Xu, Opt. Express **29**, 8725 (2021).
[59] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, New J. Phys. **11**, 095001 (2009).
[60] Z. Yan, E. Meyer-Scott, J.-P. Bourgoin, B. L. Higgins, N. Gigov, A. MacDonald, H. Hubel, and T. Jennewein, J. Light. Technol. **31**, 1399 (2013).
[61] J. Wang, X. Qin, Y. Jiang, X. Wang, L. Chen, F. Zhao, Z. Wei, and Z. Zhang, Opt. Express **24**, 8302 (2016).
[62] A. Duplinskiy, V. Ustimchik, A. Kanapin, V. Kurochkin, and Y. Kurochkin, Opt. Express **25**, 28886 (2017).
[63] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Appl. Phys. Lett. **112**, 051108 (2018).
[64] Y. Li, Y.-H. Li, H.-B. Xie, Z.-P. Li, X. Jiang, W.-Q. Cai, J.-G. Ren, J. Yin, S.-K. Liao, and C.-Z. Peng, Opt. Lett. **44**, 5262 (2019).
[65] https://www.optizonetech.com/.
[66] http://www.conquer-oc.com/.
[67] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014).
[68] Z. Li and K. Wei, Quantum Eng. **2022**, 9717591 (2022).
[69] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[70] W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).
[71] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[72] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013).