applied sciences

MDPI

Article

Practical Analysis of Sending or Not-Sending Twin-Field Quantum Key Distribution with Frequency Side Channels

Yi-Fei Lu [1,2], Mu-Sheng Jiang [1,2,*], Yang Wang [1,2,3], Xiao-Xu Zhang [1,2], Fan Liu [1,2], Chun Zhou [1,2], Hong-Wei Li [1,2], Shi-Biao Tang [4], Jia-Yong Wang [5] and Wan-Su Bao [1,2,*]

1 Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450001, China; lyf@qiclab.cn (Y.-F.L.); wy@qiclab.cn (Y.W.); zxx@qiclab.cn (X.-X.Z.); lf@qiclab.cn (F.L.); zc@qiclab.cn (C.Z.); lhw@qiclab.cn (H.-W.L.)
2 Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
3 National Laboratory of Solid State Microstructures, School of Physics and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China
4 QuantumCTek Co., Ltd., Hefei 230088, China; tangsb@ustc.edu.cn
5 CAS Quantum Network Co., Ltd., Shanghai 201315, China; wangjiayong@qtict.com
* Correspondence: jms@qiclab.cn (M.-S.J.); bws@qiclab.cn (W.-S.B.)

Abstract: The twin-field quantum key distribution (TF-QKD) and its variants can overcome the fundamental rate-distance limit of QKD. However, their physical implementations with the side channels remain the subject of further research. We test the side channel of a type of external intensity modulation that applies a Mach–Zehnder-type electro-optical intensity modulator, which shows the distinguishability of the signal and decoy states in the frequency domain. Based on this security loophole, we propose a side-channel attack, named the passive frequency-shift attack, on the imperfect implementation of the sending or not-sending (SNS) TF-QKD protocol. We analyze the performance of the SNS protocol with the actively odd-parity pairing (AOPP) method under the side-channel attack by giving the formula of the upper bound of the real secret key rate and comparing it with the lower bound of the secret key rate under Alice and Bob's estimation. The simulation results quantitatively show the effectiveness of the attack on the imperfect devices at a long distance. Our results emphasize the importance of practical security at the light source and might provide a valuable reference for device selection in the practical implementation of the SNS protocol.

Keywords: twin-field; practical security; decoy-state method

Citation: Lu, Y.-F.; Jiang, M.-S.; Wang, Y.; Zhang, X.-X.; Liu, F.; Zhou, C.; Li, H.-W.; Tang, S.-B.; Wang, J.-Y.; Bao, W.-S. Practical Analysis of Sending or Not-Sending Twin-Field Quantum Key Distribution with Frequency Side Channels. *Appl. Sci.* **2021**, *11*, 9560. https://doi.org/10.3390/app11209560

Academic Editor: Nikola Paunković

Received: 26 August 2021
Accepted: 9 October 2021
Published: 14 October 2021

1. Introduction

Quantum key distribution (QKD) promises to share the secret key bits with its security guaranteed by the laws of quantum physics [1–3]. Combined with the one-time pad, Alice and Bob can achieve unconditionally secure private communication. However, there are inevitable imperfections in the practical QKD systems which can be exploited by Eve and compromise the practical security. With the development of QKD, the proposal of the measurement-device-independent (MDI) QKD [4] and the decoy-state method [5–7] have greatly improved the practicality, performance, and practical security.

However, the secret key rate and distance are two implementation bottlenecks of point-to-point QKD. For example, the TGW bound [8] and PLOB bound [9] determine the repeaterless secret key capacity. To overcome this limit of repeaterless QKD, Lucamarini et al. [10] proposed the twin-field QKD (TF-QKD) protocol whose secret key rate scales with the square root of the channel transmittance by using the single-photon interference. However, the security is not completed as a security loophole is caused by the later announcement of the phase information [11]. Then, many variants of TF-QKD [11–17] have been proposed to deal with this security loophole and each has its own advantages. To accelerate the application of the TF-QKD protocols, many effects have been considered and analyzed, including the finite-key

effects [18–21], the asymmetric effects [22–24], the discrete phase randomization [25,26], the optimization of the protocol [27–29], and the practical issues [30,31]. Meanwhile, several experiments of the TF-QKD have been carried out in the laboratory and field, demonstrating its ability to break the limit of repeaterless QKD [32–39].

However, the physical implementations of the TF-QKD protocols with the side channels remain to be further researched at present. Ideally, it is assumed that the sending devices are placed in a protected laboratory, and can prepare and encode quantum states correctly without information leakage. Unfortunately, these conditions may be not satisfied in the practical systems due to the imperfect devices [40–43] or Eve's disturbance [44–50]. In those QKD protocols with the practical light source, the decoy-state method is vital and used to monitor the channel eavesdropping [51] in which the security is based on the fact that Eve cannot distinguish between the signal and decoy states. However, the indistinguishability of the signal and decoy states may be violated due to the imperfections of the real apparatuses or Eve's disturbance. For instance, the probability distributions of the signal and decoy states do not overlap in the time domain completely with the pump-current modulation [42]. In the frequency domain, Eve could apply the wavelength-selected photon-number-splitting attack [52] or the frequency shift attack [53] actively to distinguish the signal and decoy states in the "plug-and-play" systems. However, the frequency shift attack needs to perform time shift on the signal pulses actively which is only applicable to the "plug-and-play" systems. In addition, it only analyzes the frequency shift in the ideal case. Therefore, to exploit the negative effects of the frequency side channels clearly, we consider the most general case of side channels caused only by the imperfect devices and test it experimentally. As the decoy-state method is used in the TF-QKD protocols, it is of significance to analyze its practical security in this aspect. More specifically, we concentrate on the sending or not-sending (SNS) TF-QKD protocol [11] with the actively odd-parity pairing (AOPP) method [29] and propose a side-channel attack, named the passive frequency-shift attack, which could take advantage of the most general side channels in the frequency domain.

The paper is arranged as follows. In Section 2, we recap the frequency shift of intensity modulators (IMs) and test experimentally the spectral distribution of the signal pulses with the external modulation method, which shows a side channel in the frequency domain. In Section 3, we propose the side-channel attack on imperfect implementation of the SNS protocol with AOPP that applies the imperfect IM. We analyze the adverse impact of the side channels by giving the formula of the upper bound of the secret key rate and comparing it with the lower bound of the secret key rate under Alice and Bob's estimation. In Section 4, we present our simulation results with the finite-key effects. Last, we give some discussion about the countermeasure of the side channels in Section 5 and conclude in Section 6.

2. Frequency Shift of Intensity Modulators

In this section, we will recap the frequency shift of the IMs and test experimentally to show a side channel in the frequency domain.

There are several kinds of IMs such as the Mach–Zehnder type electro-optical intensity modulators (EOIMs), electro-absorption modulators (EAMs), and acousto-optical modulators (AOMs). EOIMs, especially $LiNbO_3$-based devices, possess excellent performance of wavelength-independent modulation characteristics, excellent extinction performance (typically 20 dB), and low insertion losses (typically 5 dB) [54].

$LiNbO_3$-based EOIMs work using the principle of interference, which is controlled by modulating the optical phase. The incoming light is coupled into a waveguide and then split into two paths of a Mach–Zehnder interferometer equally, which finally interfere at an output coupler. The two arms made of lithium-niobate will induce a phase change when the modulation voltages are applied. Accordingly, the intensity and phase of the output light will be modulated after interference depending on the applied modulation voltages.

Assuming voltages $V_1(t)$ and $V_2(t)$ are applied to the two arms separately with the input field of intensity E_0 and frequency ω_0, the output field can be written as [52]

$$E_{\text{out}}(t) = E_0 \cos[\Delta\varphi(t)] e^{i[\omega_0 t + \varphi(t)]}, \tag{1}$$

where $\Delta\varphi(t) = [\gamma V_1(t) + \varphi_1 - \gamma V_2(t) - \varphi_2]/2$, $\varphi(t) = [\gamma V_1(t) + \varphi_1 + \gamma V_2(t) + \varphi_2]/2$. Here, $\gamma = \pi/V_\pi$ is the voltage-to-phase conversion coefficient for two arms, and φ_1 and φ_2 are the static phases which we will omit for simplicity. Here, V_π is the half-wave voltage that is required to change the phase in one modulator arm by π radians. The output intensity is given by

$$P_{\text{out}}(t) = |E_{\text{out}}(t)|^2 = \frac{P_0}{2}[1 + \cos[\gamma V(t)]], \tag{2}$$

where $V(t) = V_1(t) - V_2(t)$. Here, P_0 is the input optical power. The phase is maintained and the intensity is determined by Equation (2) on the condition that the two modulator arms are driven by the same amount, but in opposite directions (i.e., $V_1(t) = -V_2(t)$), which is known as the balanced driving or a push–pull operation. When $V(t)$ is constant we will get pure intensity modulation without a frequency shift. However, once $V(t)$ is not a constant anymore, something unexpected arises in the output field. For example, if $V_1(t) = -V_2(t) = V_0 + kt$, the output field can be expressed as [52]

$$E_{\text{out}} = \frac{E_0}{2}\left[e^{i[(\omega_0+\gamma k)t + \gamma V_0]} + e^{i[(\omega_0-\gamma k)t + \gamma V_0]}\right]. \tag{3}$$

From Equation (3), we can see a frequency shift of the light pulses with $\pm\omega_m = \pm\gamma k$ compared with the original frequency ω_0. The frequency shift of the output field becomes more confusing when the modulation voltages are more complicated. To analyze the spectrum of the output field, the fast Fourier transform method can be used.

To evaluate the frequency shift of different intensity pulses, we tested it experimentally. The 33-MHz optical pulses with 1 ns pulse width were produced by a CW laser, modulated by an IM, and measured by an optical-spectrum analyzer. The IM was driven by an arbitrary waveform generator with an electric signal amplified by an electric amplifier. The measurement was taken before the fixed attenuation where the photon number follows the same distribution with the emitting pulses at the single-photon level. Figure 1a illustrates the wavelength spectrum of three signal pulses, where the intensity ratio is taken from the SNS experiment [36] as 0.1: 0.384: 0.447 ($\mu_a = 0.1$, $\mu_b = 0.384$, $\mu_z = 0.447$), and the original continuous light. The normalized intensity probability distributions are shown in Figure 1b to distinguish the difference. In addition, Figure 2 shows the modulation voltages corresponding to these signal pulses.

Obviously, the states modulated by the IM with different intensities do not overlap completely in the frequency domain. The distinction will be more evident when increasing the repetition rate and narrowing the pulse width to increase the key distribution rate. Therefore, we tested it using the same method and obtained the normalized intensity distribution of 33-MHz optical pulses with 300 and 100 ps pulse widths, which is shown in Figure 3a,b, respectively.

From Figures 1b and 3a,b, we can see that the distinction of the signal states (also the strong-decoy states) and the weak-decoy states is evident. This is because the amplitude of the modulation voltages of the signal and strong-decoy states are higher, which will induce a greater frequency shift. Thus, the peaks of the signal and strong-decoy states are lower than that of the weak-decoy states. There are also slight differences between the signal and strong-decoy states. On this foundation, Eve could take advantage of this side channel to distinguish different states, which will threaten the decoy-state method.

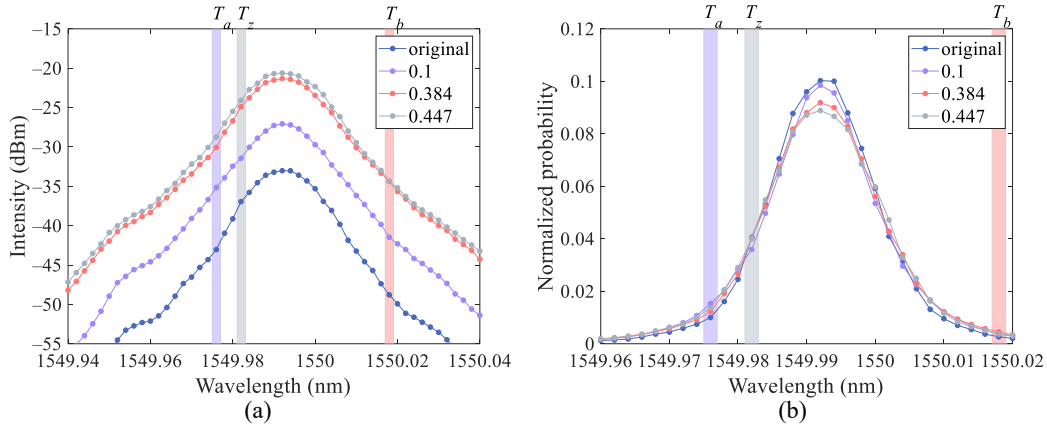

Figure 1. (**a**) The wavelength spectrum of the 1 ns signal pulses with intensity ratio as 0.1: 0.384: 0.447 ($\mu_a = 0.1$, $\mu_b = 0.384$, $\mu_z = 0.447$) and the original continuous light between 1549.94 nm and 1550.04 nm. (**b**) The normalized intensity distribution of these 1 ns signal pulses in the frequency domain. Three internals T_a, T_b, T_z with central wavelength 1549.976 nm, 1550.018 nm, 1549.982 nm and radius 0.001 nm are set to distinguish these signal pulses.

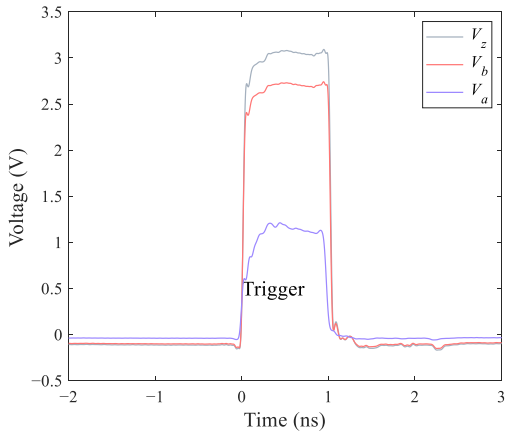

Figure 2. The 33 MHz modulation voltages with 3.34% duty ratio V_z, V_b and V_a, which correspond to the coherent states with intensities μ_z, μ_b and μ_a.

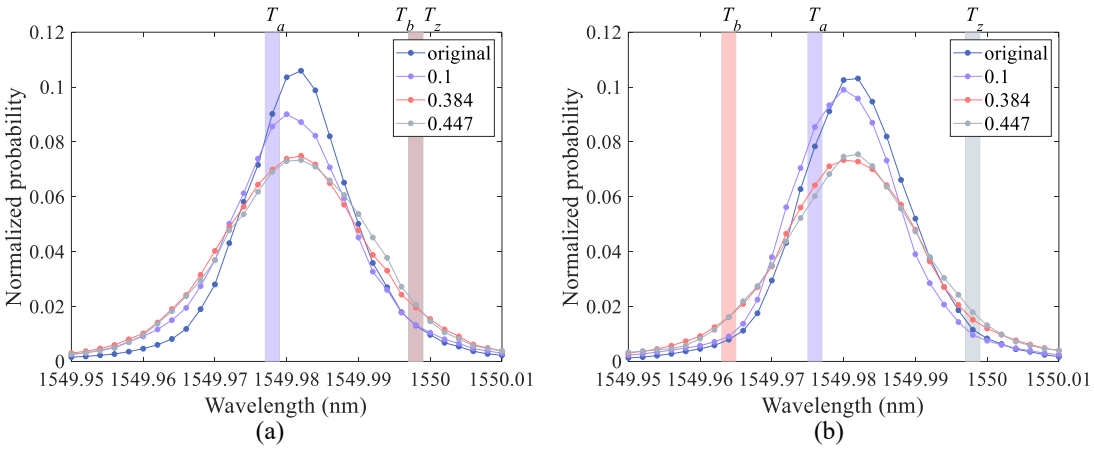

Figure 3. (**a**) The normalized intensity distribution of the 300 ps signal pulses with intensity ratio as 0.1: 0.384: 0.447 ($\mu_a = 0.1$, $\mu_b = 0.384$, $\mu_z = 0.447$) and the original continuous light between 1549.95 nm and 1550.01 nm. Three internals T_a, T_b, T_z with central wavelengths of 1549.978 nm, 1549.998 nm and 1549.998 nm and radius 0.001 nm are set to distinguish signal pulses. Here, internals T_b and T_z are overlapped. (**b**) The normalized intensity distribution of the 100 ps signal pulses with intensity ratio as 0.1: 0.384: 0.447 ($\mu_a = 0.1$, $\mu_b = 0.384$, $\mu_z = 0.447$) and the original continuous light between 1549.95 nm and 1550.01 nm. Three internals T_a, T_b and T_z with central wavelengths of 1549.976 nm, 1549.964 nm and and 1549.998 nm and radius 0.001 nm are set to distinguish these signal pulses.

3. Passive Frequency-Shift Attack on Imperfect Implementation of SNS

In this section, we propose a side-channel attack, named the passive frequency-shift attack, on the imperfect implementation of the SNS protocol with AOPP by exploiting the side channels in the frequency domain. The four-intensity decoy-state SNS protocol with AOPP is reviewed in the Appendix A.

In those TF-QKD protocols that need the post-phase compensation method, such as the SNS TF-QKD [11] and phase-matching (PM) TF-QKD [12], the signal and reference pulses should be produced with a stable CW laser source and modulated with the external modulation method to estimate and compensate for the phase noise. In the four-intensity decoy-state SNS TF-QKD protocol, Alice and Bob need to modulate the continuous light to five kinds of pulses with different intensities. The maximum-intensity pulses are used as the phase reference pulses, the minimums as the vacuum states, and others as the signal states, weak- and strong-decoy states. In the practical SNS systems [35,36], three IMs are used to modulate these five different pulses. The first IM modulates the continuous light to five pulses of different intensities and the second IM modulates the intensity to the designed ratio. The last IM only modulates the signal pulse width to a fixed width which can eliminate the side channels caused by the first two IMs. In this paper, we consider the simplified SNS systems where only one IM is applied to modulate the signal pulses. In this way, the side channels caused by the IM are exposed to Eve totally. We use this to verify the side channels of the IMs, prove their harmfulness, and present a reference for the device selection in the practical implementation.

Suppose Eve intercepts all of the signal pulses at Alice and Bob's output ports where the signal pulses have not been attenuated by the channels, and then distinguishes the signal and decoy states with a wavelength-division multiplexer (WDM) and three single-photon detectors (SPDs), which is illustrated in Figure 4. To distinguish the states with intensity μ_α, Eve sets internals T_α with $\alpha \in \{z, a, b\}$, according to the wavelength spectrum of different states. Suppose the four ports of WDM 1, 2, 3, and 4 can export photons with frequency located in T_z, T_a, T_b, and others. The light-path selector S1 (S2) is controlled by SPD1 (SPD1 and SPD2). Denote it as 1 or 0 when the SPD (i.e., SPD1, SPD2, or SPD3) clicks or not, and 1 or 0 when the light-path selector (i.e., S1 or S2) selects the up or down path. We set

$$\begin{aligned} \mathrm{S1} &= \overline{\mathrm{SPD1}}, \\ \mathrm{S2} &= \mathrm{SPD1} \vee \mathrm{SPD2}. \end{aligned} \tag{4}$$

Note that only one SPD at most will click under this principle. According to the response of the SPDs, set the total transmittance as η_1, η_2, η_3 or η_v when SPD1, SPD2, SPD3, or none click, respectively.

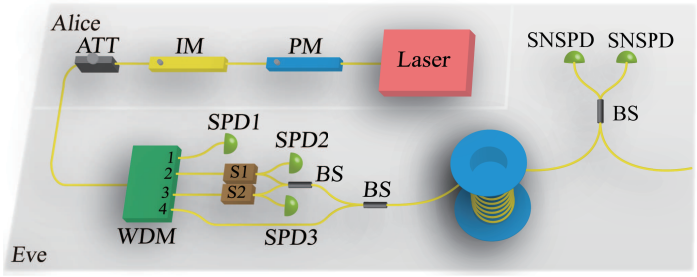

Figure 4. Schematic of the passive frequency-shift attack harnessing the side channels caused by the IM. PM: phase modulator, IM: intensity modulator, ATT: attenuator, WDM: wavelength-division multiplexer, SPD: single-photon detector, S: light-path selector, BS: beam splitter, SNSPD: superconducting-nanowire single-photon detectors. The light-path selector S1 (S2) is controlled by SPD1 (SPD1 and SPD2), and Bob's device is the same as Alice's.

In this process, Eve can get partial raw-key bits after Alice (Bob) announces the signal and decoy windows. It can be understood in this way that Eve can conclude the key bit as 1 (0) for Alice (Bob) when SPD1 $\vee$ SPD2 $\vee$ SPD3 $= 1$ in a Z window. There is no bit-flip error between Alice (Bob) and Eve because Eve can intercept photons at output ports without stray photons. Only the raw bits can be used to distill the secret bits in Z windows when SPD1 $\vee$ SPD2 $\vee$ SPD3 $= 0$ on both sides. Once Eve detects photons successfully on one side, Eve's bit is either the same or a bit-flip error with the other side, which will be revealed in the error-correction step (and the pre-error correction step when the AOPP method is performed). However, the bits are balanced (i.e., random for Eve) in one-detector heralded events with SPD1 $\vee$ SPD2 $\vee$ SPD3 $= 0$, which means the raw bits are unknown to Eve in these windows. Although Eve cannot distinguish the decoy and signal states without errors, the decoy-state method may not estimate the lower bound of the secret key rate correctly when the transmittances of the signal and decoy states differ. When the actual secret key rate is lower than the estimated one, the final secret string is partially insecure.

We emphasize that this side-channel attack will not introduce unnecessary errors, as the beam splitting and measurement by Eve can be viewed as a loss without phase noise. What is more, Eve could control errors completely except the inherent errors of the protocol through channels, superconducting-nanowire single-photon detectors (SNSPDs), and classic information he announces. In the following, we will analyze the effect of this passive frequency-shift attack.

Consider the most general case, assume the envelope of the wavelength spectrum can be written as $f_i(\lambda)$, where $i \in \{z, a, b, v\}$ and $f_v(\lambda) \equiv 0$ for vacuum states. When the wavelength spectrum of the signal and decoy states do not overlap completely, Eve can distinguish these states with errors by setting the internals T_α. The proportion of state μ_i in internals T_α can be shown as

$$r_{i|\alpha} = \frac{\int_{T_\alpha} f_i(\lambda) d\lambda}{\int_{-\infty}^{\infty} f_i(\lambda) d\lambda}. \tag{5}$$

The states of intensity μ_i would be transformed with one of four different transmittances $\eta_{i,k}$ ($k \in \{1, 2, 3, v\}$) when SPD$_k$ clicks (SPD$_v$ corresponds to no SPD click), where

$$\begin{aligned} \eta_{i,1} &= \eta_z(1 - r_{i|z}), \\ \eta_{i,2} &= \eta_a(1 - r_{i|z} - r_{i|a}), \\ \eta_{i,3} &= \eta_b(1 - r_{i|z} - r_{i|a} - r_{i|b}), \\ \eta_{i,v} &= \eta_k(1 - r_{i|z} - r_{i|a} - r_{i|b}). \end{aligned} \tag{6}$$

The total transmittance $\eta_{i,k}$ can be controlled by Eve completely, which means that Eve is allowed to use a lower-loss or even lossless channel and perfect detectors with 100% detection efficiency and no dark count. In addition, Eve could select the internals T_α freely to obtain satisfactory results. For the states with intensity μ_i, the probability of being transmitted with $\eta_{i,k}$ can be shown as

$$\begin{aligned} p_{i,z} &= (1 - e^{-\mu_{i|z}}), \\ p_{i,a} &= e^{-\mu_{i|z}}(1 - e^{-\mu_{i|a}}), \\ p_{i,b} &= e^{-\mu_{i|z}} e^{-\mu_{i|a}}(1 - e^{-\mu_{i|b}}), \\ p_{i,v} &= e^{-\mu_{i|z}} e^{-\mu_{i|a}} e^{-\mu_{i|b}}, \end{aligned} \tag{7}$$

where $\mu_{i|\alpha} = \mu_i r_{i|\alpha}$. Here $e^{-\mu_{i|\alpha}}$ is the probatility of zero photons in internal T_α with intensity μ_i.

Since the TF-QKD protocols are proposed for the implementation of long optical-fiber communications, Eve's best target is to acquire a higher percentage of the key bits as far as possible while maintaining the key rate and communication distance under Alice and

Bob's estimation. When the communication distance is long enough, Eve may steal secret key bits.

There are two key rates that matter: the lower bound of the secret key rate under Alice and Bob's estimation R_e and the upper bound of the actual secret key rate R_u. In the QKD protocols, it is challenging to obtain the actual secret key rate with one communication step by sending N pulses. Fortunately, Alice and Bob can estimate the lower bound of the secret key rate. It is risky to exceed the lower bound because the security of those bits is uncertain, although the final key bits may still be secure. Note that Alice and Bob could not estimate R_e correctly under this attack because it is impossible to pick out the decoy states that have undergone the same operation as the signal states, i.e., the decoy-state method does not work properly. The key rate R_u, which is an upper bound of the actual secret key rate, is introduced to evaluate the effect of this attack. In the following, we analyze how to obtain the formula of R_u.

When the attack is applied, the phase-randomized coherent states with μ_z sent by Alice (Bob) will be transformed with one of four transmittances $\eta_{z,k}$ with probability $p_{z,k}$. As Alice and Bob will announce their signal and decoy windows, the Z windows are known to Eve. Hence, Eve can obtain Alice's (Bob's) raw bits as 1 (0) when obtaining a detection event with three SPDs in Z windows. In other words, only the raw bits of Alice (Bob) that are caused by the pulses transmitted with $\eta_{z,v}$ are unknown to Eve. Considering the raw-bit strings of both parties at the same time, there will be four kinds of twin bits, given as $\{10, 1x, x0, xx\}$ according to Eve's information on raw bits, where the first (second) bit indicates that Alice's (Bob's) bits are known to Eve as 1 (0) or unknown as x.

In the SNS protocol, Alice and Bob will perform the AOPP method on raw bits before error correction. When the AOPP method is performed with partial bits leaked to Eve, from Eve's perspective, Bob will only choose pairs $0x$, $x0$ and, xx, and Alice's pairs can only be $11, 1x, x1, xx$ accordingly (12 scenarios in total). Note that these bit pairs are between Alice and Bob's own bit strings. Since Bob only chooses odd-parity bit pairs and will keep the second bits if Alice's bit pairs are odd too, Eve can infer that Alice's (Bob's) result bit (i.e., the second bit) is $1, 0, x$ $(1, 0, 1, x)$, correspondingly. At this time, there will be nine kinds of twin bits $\{11_P, 10_P, 01_P, 00_P, 1x_P, x1_P, 0x_P, x0_P, xx_P\}$ according to Eve's information on raw bits, where the subscript P represents that the AOPP method is applied. Only the last twin bit xx_P can be used to distill the secret-key bits because, for all other twin bits, at least one's bit is leaked and all will be revealed or discarded in the error-correction step. Finally, we note that the twin bits xx_P can only be generated with two twin bits xx which correspond to states transmitted with $\eta_{z,v}$.

In the decoy-state method [5–7], the secret key is only derived from the single-photon component, i.e., the untagged bits [55,56]. In the decoy-state SNS protocol [11,30], the untagged bits are defined during effective events, which are caused by the two-mode single-photon states $|01\rangle$ or $|10\rangle$ in Z windows (see Appendix A for details). The secret twin bits xx_P can only be generated with two untagged-twin bits when the AOPP method is applied. Therefore, the upper bound of the actual secret key rate can be shown as

$$R_u = \frac{n_{1,\mathrm{sec}}}{N} = \frac{n_p}{N}\frac{n_{1s}^0}{n_{t0}}\frac{n_{1s}^1}{n_{t1}}, \tag{8}$$

where n_{1s}^0 and n_{1s}^1 are the upper bound of the untagged bits when they make the opposite decision and obtain twin bits 0 and 1, respectively. Note that for the above simplified attack scheme,

$$n_{1s}^0 = n_{1s}^1 = N p_z^2 p_{z0}(1 - p_{z0}) p_{z,v} G(u_z \eta_{z,v}), \tag{9}$$

where $G(x) = e^{-x}x$ is obtained without considering dark counts.

In addition, note that the above attack scheme is clumsy since Eve does not consider the relevance of the response of the SPDs at Alice and Bob's side. We modify the attack in the following.

There are 16 kinds of state pairs according to the intensities of Alice and Bob, which can be denoted as $\mu_i\mu_j$ with $i, j \in \{z, a, b, v\}$, regardless of the type of windows. Similarly, there will be 16 scenarios about the response of the SPDs denoted as km at Alice and Bob's side, where $k, m \in \{1, 2, 3, v\}$. Therefore, when Alice and Bob select states with intensities μ_i and μ_j, the probability when SPDk and SPDm clicks can be shown as

$$p_{ij,km} = p_{i,k}p_{j,m}. \tag{10}$$

Given the loss due to Eve's interception, the total transmission for Alice and Bob can be shown as

$$\begin{aligned} \eta^A_{ij,km} &= \eta^A_{km}\eta_{i,k}/\eta_k, \\ \eta^B_{ij,km} &= \eta^B_{km}\eta_{j,m}/\eta_m, \end{aligned} \tag{11}$$

where η^A_{km} (η^B_{km}) is the total transmission between Alice (Bob) and Charlie that Eve sets when SPDk and SPDm clicks at Alice and Bob's side, respectively.

Similarly, only the raw bits that are caused by those signal states transmitted with $\eta_{zv,vv}$ ($\eta_{vz,vv}$) are secured. At this time, Equation (8) is the upper bound of the actual secret key rate combined with

$$\begin{aligned} n^0_{1s} &= Np_z^2p_{z0}(1-p_{z0})p_{zv,vv}G(\mu_z\eta^A_{zv,vv}), \\ n^1_{1s} &= Np_z^2p_{z0}(1-p_{z0})p_{vz,vv}G(\mu_z\eta^B_{vz,vv}). \end{aligned} \tag{12}$$

This side-channel attack is a passive attack on the imperfect implementation of the SNS protocol that applies only an IM since the violation of the security assumption is caused by Alice and Bob themselves. The security of the SNS protocol is not dependent on the channels or detectors. This side-channel attack can be applied as long as the wavelength-spectrum distributions of the signal and decoy states are different. The effect of this attack varies based on the distinguishability of the different states.

4. Numerical Simulations

We numerically simulate the behavior of the SNS protocol with AOPP, which applies an imperfect IM, under the passive frequency-shift attack in this section.

In the actual systems, the key rate under Alice and Bob's estimation may be affected by the spectral distribution of signal pulses. Ideally, there will be an expected key rate without attack denoted as R_{ideal} when eliminating the effects of the spectral distribution. Here, we ignore the effect of the spectral distribution for simplicity. We suppose that Eve's target is to acquire more key bits, i.e., lower the upper bound of the secret key rate while maintaining the key rate under Alice and Bob's estimation constant with the expected key rate. Therefore, Eve need to maximize R_u while keeping R_e equal to the expected key rate R_{ideal} by optimizing the transmittances η^A_{km} and η^B_{km}, which can be expressed as

$$\min_{\eta^A_{km},\eta^B_{km}} R_u, \text{ s.t. } R_e = R_{ideal}. \tag{13}$$

When R_u is lower than R_e, it means the final key bits are partially insecure. And the secret key rate is reduced to 0 when $R_u = 0$.

For simulation purposes, the experimental parameters listed in Tables 1 and 2 are taken according to the SNS experiment [36]. The most important of the passive frequency-shift attack is the side channels in the frequency domain. To distinguish the states and obtain raw bits probabilistically, Eve will intercept pulses in three internals T_z, T_a and T_b. According to our experimental results, the internals are marked in Figures 1b and 3a,b. And the parameters $r_{i|\alpha}$, the proportion if state with intensity μ_i in internals T_α, are listed in Table 3. Note that the side channels in Table 3 are independent with the experiment [36] which we have discussed at the beginning of Section 3.

Table 1. List of the experimental parameters. Here, γ is the fiber loss coefficient (dB/km), η_d is the detection efficiency of detectors, e_d is the misalignment-error probability, f_{EC} is the error-correction inefficiency, ξ is the failure probability of the statistical-fluctuations analysis, p_d is the dark-count rate, M is the number of phase slices, and N is the number of pulses sent at one communication step.

γ	η_d	e_d	f_{EC}	ξ	p_d	M	N
0.2	56%	0.1	1.1	2.2×10^{-9}	10^{-10}	16	1.55×10^{12}

Table 2. List of the experimental parameters about the intensity and probability Alice and Bob select.

μ_a	μ_b	μ_z	p_z	p_a	p_b	p_{z0}
0.1	0.384	0.447	0.776	0.85	0.073	0.732

Table 3. List of the parameter $r_{i|\alpha}$, which is the proportion of the state μ_i in the internal T_α. The left column indicates the numbers of the groups. The parameters are taken from Figures 1b and 3a,b. The valus in the table are multiplied by 100.

	Width	$r_{z\|z}$	$r_{z\|a}$	$r_{z\|b}$	$r_{a\|z}$	$r_{a\|a}$	$r_{a\|b}$	$r_{b\|z}$	$r_{b\|a}$	$r_{b\|b}$
1	1 ns	3.996	1.367	0.376	3.592	1.531	0.357	4.033	1.225	0.454
2	300 ps	2.071	6.910	2.071	1.325	8.563	1.325	1.958	6.994	1.958
3	100 ps	1.791	6.028	1.616	0.963	8.544	0.911	1.522	6.420	1.618

Last, we simulate the expected secret key rate without attack R_{ideal}, the key rate under Alice and Bob's estimation R_e, and the upper bound of the secret key rate under the frequency-shift attack R_u. There are nine parameters should be obtained by statistics in the practical systems, including $n_{\alpha\beta}$ ($\alpha\beta \in S = \{vv, va, av, vb, bv\}$), $n^R_{\Delta+}$, $n^L_{\Delta-}$, n_t, and E_z. Here, $n_t = n_{\mathrm{sig}} + n_{\mathrm{err}}$ is the length of the raw bits, and $E_z = n_{\mathrm{err}}/n_t$ is the bit-flip error rate of the raw bits, where n_{sig} and n_{err} are the number of right and wrong raw bits, respectively. Under the passive frequency-shift attack, these parameters could be simulated as discussed in the Appendix B.

In Figure 5, the estimated key rate R_e under the passive frequency-shift attack represented by the blue solid line is the same as the expected key rate, which means that Eve's action would not be detected by Alice and Bob. In comparison, the dashed lines represent the upper bounds of the secret key rates R_{ul} ($l \in \{1, 2, 3\}$) under the frequency-shift attack with the parameters taken from Group l in Table 3. And the details of transmission η^A_{km} and η^B_{km} are shown in Appendix C. The effects of the side-channel attack can be analyzed by comparing R_e and R_{ul}. Specifically, the upper bounds R_{u1}, R_{u2} and R_{u3} are lower than R_e at 230 km, 298 km, and 376 km, respectively. At this time, the final key bits are partially insecure which can be depicted with the upper bounds of the percentage of the secret key bits, defined as $R_{rl} = R_{ul}/R_e$ and shown in Figure 6. And the farther the distance, the smaller the proportion of secret key bits. R_{u1}, R_{u2}, and R_{u3} are reduced to zero at 412 km, 370 km, and 306 km, respectively, which means no secret-key bits can be distributed when exceeding this distance.

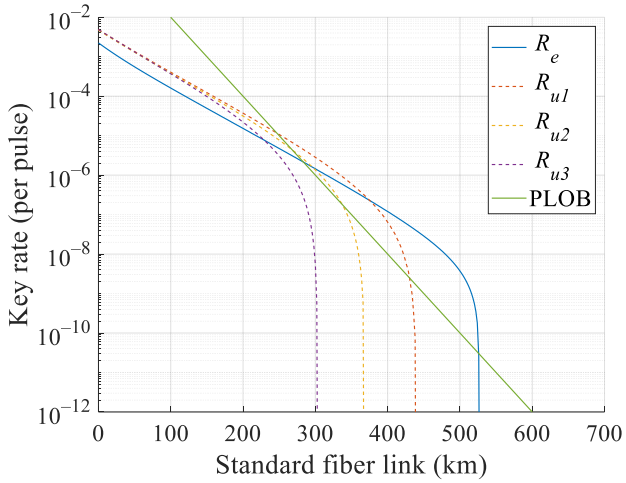

Figure 5. The estimated lower bound of the secret key rate R_e and the upper bound of the real secret key rates R_{ul} ($l \in \{1,2,3\}$) in logarithmic scale versus transmission distance (between Alice and Bob) under the passive frequency-shift attack. The experimental parameters $r_{i|\alpha}$ about the side channels are listed in the Table 3.

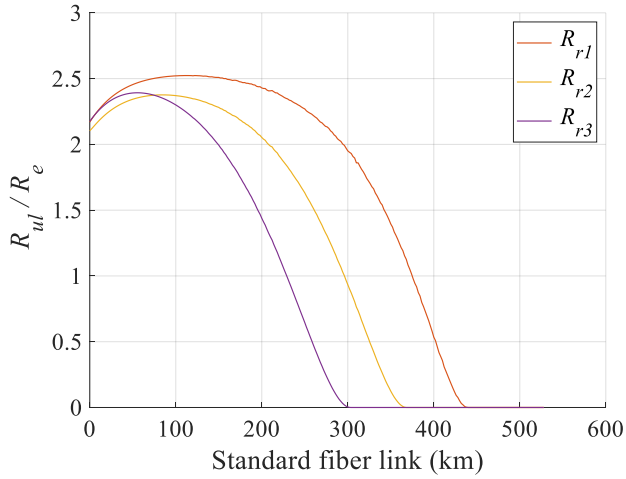

Figure 6. The upper bounds of the percentage of the secret key bits $R_{rl} = R_{ul}/R_e, l \in \{1,2,3\}$.

5. Discussion

It is widely known that the inevitable side channels are detrimental to the security of the practical QKD systems. For this reason, how can Eve exploit these side channels and how much the systems may be affected are worth researching. The side-channel attack proposed above on the imperfect implementation of the SNS protocol, which applies an imperfect IM, truly proves that even small side channels at the light source can compromise the secret key rate severely.

We note that there are two key points of the side-channel attack. The first and the most important is the imperfect IM is applied, which produces the decoy and signal states differently in the frequency domain, i.e., the frequency side channels. The second is the long-distance key distribution where the channel attenuation is large enough, which could be utilized by Eve to amplify the effects of the side channels. Since the long-distance key distribution is a primary goal of the SNS protocol, the above attack emphasizes the harmfulness of the side channels specifically and may provide a reference for the practical implementation.

To guarantee the security in the practical systems with the side channels, the first potential way is to improve the experimental techniques or modulation methods to restrain the side channels [57,58]. For example, three IMs can be used to modulate the signal

pulses and reference pulses, where the last IM is used to eliminate the side-channels [35,36]. The second alternative is to develop the mathematical models in theory to include the side channels, such as the loss-tolerant method [59–63] with the characterization of the real apparatuses [64]. Finally, it would be a good choice to improve the protocol theoretically to resist the side-channel attack [65]. An ongoing search for the side channels may be needed to guarantee the practical security of QKD systems.

6. Conclusions

The goal of QKD at present is to provide long-distance and high-speed key distribution. Increasing the repetition rate and narrowing the pulse width may make the pulses complex and the parameters, such as the frequency, polarization, and temporal shape, more distinguishable. Any small imperfections may be exploited and enhanced by Eve utilizing the channel loss. Therefore, it is necessary to pay more attenuation to the practical implementations of the TF-QKD systems.

In this paper, we investigate and test the frequency side channels with the external modulation method. The imperfect IM will produce the signal and decoy states distinguishable in the frequency domain. Based on this, we propose a side-channel attack, named the passive frequency-shift attack, on the imperfect implementation of the SNS TF-QKD protocol that applies to the most general case of frequency side channels. Normally, when without the side channels, Alice and Bob could estimate the lower bound of the secret key rate correctly no matter what Eve does. However, this estimation is not accurate once Eve's operations on the signal and decoy states are different, which may cause insecure bits when the upper bound of the secret key rate is lower than the estimated lower bound. The numerical results quantitatively show the effectiveness of the attack at a long distance if Alice and Bob neglect this distinguishability.

Finally, we note that at present the side channel in the frequency domain can be restrained with more than one IM in the actual QKD systems [35,36]. We test with only one IM in this study just to prove the harmfulness of the side channels and emphasize the practical security of the light source specifically. Our results might provide a reference for the device selection in the practical implementation. The final goal is to build the hardened implementations of the practical QKD systems.

Author Contributions: Conceptualization, M.-S.J. and Y.-F.L.; methodology, Y.-F.L., M.-S.J. and Y.W.; writing—original draft preparation, Y.-F.L.; writing—review and editing, X.-X.Z., F.L., C.Z., H.-W.L., S.-B.T. and J.-Y.W.; project administration, W.-S.B.; funding acquisition, W.-S.B., Y.W., H.-W.L. and C.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program of China (Grant No. 2020YFA0309702), the National Natural Science Foundation of China (Grant Nos. 62101597, 61605248, 61675235 and 61505261), the China Postdoctoral Science Foundation (Grant No. 2021M691536), the Natural Science Foundation of Henan (Grant Nos. 202300410534 and 202300410532) and the Anhui Initiative in Quantum Information Technologies.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. SNS TF-QKD Protocol with AOPP

We make a review of the SNS protocol with AOPP and the key rate formula [11,19,29] in the following.

(1) Preparation and measurement. At any time window i, Alice (Bob) randomly determines whether it is a signal window or a decoy window with probabilities p_z and $p_x = 1 - p_z$. If it is a signal window, Alice (Bob) sends a phase-randomized coherent state with intensity μ_z and denotes it as 1 (0), or a vacuum state $|0\rangle$ and denotes it as 0 (1) with

probabilities $p_{z1} = 1 - p_{z0}$ and p_{z0}, seperately. If it is a decoy window, Alice (Bob) sends a phase-randomized coherent state $|\sqrt{\mu_a}e^{i\theta_A}\rangle$, $|\sqrt{\mu_b}e^{i\theta'_A}\rangle$ or $|0\rangle$ ($|\sqrt{\mu_a}e^{i\theta_B}\rangle$, $|\sqrt{\mu_b}e^{i\theta'_B}\rangle$ or $|0\rangle$) with probabilities p_a, p_b and $p_v = 1 - p_a - p_b$, where $\mu_a < \mu_b$. The third party, Chrelie, renamed as Eve is supposed to perform the interferometic measurements on the incoming pulses and announce the results.

(2) Different types of time windows. Suppose Alice and Bob repeat the above process N times, then they announce their signal windows and decoy windows through the public channels. If both Alice and Bob determine a signal window, it is a Z window. The effective events in Z windows are defined as the one-detector heralded events no matter which detector clicks. Alice and Bob will get two raw n_t-bit strings Z_A and Z_B according to the effective events in Z windows. Note that the phase-randomized coherent state of intensity μ is equivalent to a probabilistic mixture of different photon-number states $\sum_{k=0}^{\infty}\frac{e^{-\mu}\mu^k}{k!}|k\rangle\langle k|$. Therefore, we can define the Z_1 windows as a subset of the Z windows when only one party determines to send and she (he) actually sends the single-photon state $|1\rangle$. The bits from the effective Z_1 windows are regarded as the untagged bits by the tagged model [56]. Then, the intensity of pulses would be announced to each other expect the intensity in Z windows. If both commit to a decoy window, it is an X window. Alice and Bob also announce their phase information θ_A, θ_B when they choose the same intensity μ_a in an X window denoted as an X_a window. And if only one detector clicks in X_a windows with phases satisfying

$$|\theta_A - \theta_B - \varphi_{AB}| \leq \Delta/2 \tag{A1}$$

or

$$|\theta_A - \theta_B - \pi - \varphi_{AB}| \leq \Delta/2, \tag{A2}$$

it is an effective event. All effective events in X_a windows can be divided into two subsets as C_{Δ^+} and C_{Δ^-} according Equations (A1) and (A2), respectively. And the number of the events in C_{Δ^+} and C_{Δ^-} can be defined as N_{Δ^+} and N_{Δ^-}. Here, φ_{AB} is set properly to obtain a satisfactory key rate which will be different over time due to the phase drift. In the following, we will omit the phase drift without loss of generality and set $\varphi_{AB} = 0$.

(3) Parameter estimation. They can estimate parameters, including the bit-flip error rate of the raw bits E_Z, the lower bound of untagged bits $\underline{n}_1$ (or the lower bound of the counting rate $\underline{s}_1$ equivalently), and the upper bound of the phase-flip error rate of the untagged bits $\bar{e}_1^{ph}$. The bit-flip error rate E_Z can be obtained by error test, $\underline{s}_1$ and $\bar{e}_1^{ph}$ can be estimated with the decoy-state method as follows.

Denote $\rho_v = |0\rangle\langle 0|$, $\rho_a = \sum_{k=0}^{\infty} e^{-\mu_a}\mu_a^k/k!|k\rangle\langle k|$ and $\rho_b = \sum_{k=0}^{\infty} e^{-\mu_b}\mu_b^k/k!|k\rangle\langle k|$, where ρ_a and ρ_b are density operators of the phase-randomized coherent states used in X windows in which the phase is not announced. Let $N_{\alpha\beta}$ be the number of intsnces when Alice sends state ρ_α and Bob sends state ρ_β, and $n_{\alpha\beta}$ be the number of corresponding one-detector heralded events, where $\alpha\beta \in S = \{vv, va, av, vb, bv\}$. Thus, the counting rate can be defined as $S_{\alpha\beta} = n_{\alpha\beta}/N_{\alpha\beta}$. And $\underline{s}_1$ can be estimated with the decoy-state method as [30,66]

$$\underline{s}_1 \geq \frac{1}{2\mu_a\mu_b(\mu_b - \mu_a)}[\mu_b^2 e^{\mu_a}(S_{va} + S_{av}) - \mu_a^2 e^{\mu_b}(S_{vb} + S_{bv}) - 2(\mu_b^2 - \mu_a^2)S_{vv}]. \tag{A3}$$

Denote the bit-flip errors in C_{Δ^+} (C_{Δ^-}) as the effective events when the right (left) detector clicks and its total number as $n_{\Delta^+}^R$ ($n_{\Delta^-}^L$). The bit-flip error rate in $C_\Delta = C_{\Delta^+} \bigcup C_{\Delta^-}$ can be shown as

$$T_\Delta = \frac{n_{\Delta^+}^R + n_{\Delta^-}^L}{N_{\Delta^+} + N_{\Delta^-}}. \tag{A4}$$

Therefore $\bar{e}_1^{ph}$ can be estimated with the decoy-state method as [11,30]

$$\bar{e}_1^{ph} \leq \frac{T_\Delta - 1/2e^{-2\mu_a}S_{vv}}{2\mu_a e^{-2\mu_a}\underline{s}_1}. \tag{A5}$$

(4) Key rate formula. With these quantities, the final key length can be expressed as [11,67]

$$R = 2p_{z0}(1-p_{z0})\mu_z e^{-\mu_z}\underline{s}_1[1-H(\bar{e}_1^{ph})] - n_t f H(E_Z)/N. \tag{A6}$$

where N_f is the number of the final bits, $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function, and f is the error correction efficiency factor.

(5) AOPP method. AOPP method [19,29] is a pre-error correction process on the raw strings Z_A and Z_B, which can improve the direct transmission key rate. In the AOPP method, Bob randomly select two unequal bits as the pairs and will obtain $n_p = \min(n_{t0}, n_{t1})$ pairs, where n_{t0} (n_{t1}) is the number of the bits 0 (1) in the raw string Z_B. There will be only two types of pairs that can survive when Alice makes exactly the same or opposite decision as Bob for two bits. Denote the correspond number as n_{vd} or n_{cc}, respectively. Therefore, the bit error after the AOPP is shown as

$$E_Z' = \frac{n_{vd}}{n_{cc}+n_{vd}}. \tag{A7}$$

The lower bound of the number of the untagged bits is

$$\underline{n}_1' = n_p \frac{\underline{n}_1^0}{n_{t0}} \frac{\underline{n}_1^1}{n_{t1}}, \tag{A8}$$

where $\underline{n}_1^0$ and $\underline{n}_1^1$ is the lower bound of the untagged bits when they make the opposite decision and obtain bits 0 and 1, correspondingly. The phase-flip error rate changes into $\bar{e}'^{ph}_1 = 2\bar{e}_1^{ph}(1-\bar{e}_1^{ph})$. Besides, the finite-key effects should be considered in the practical systems using the Chernoff bound [68,69]. The parameters can be estimated as $n_1' = \varphi^L(\underline{n}_1')$ and $e_1'^{ph} = \varphi^U(\underline{n}_1'\bar{e}_1'^{ph})/\underline{n}_1'$. Finally, the improved key length can be shown as [19,29,67]

$$N_f' = n_1'[1-H(e'^{ph}_1)] - n_t' f H(E_Z') - \log_2\frac{2}{\varepsilon_{cor}} - 2\log_2\frac{1}{\sqrt{2}\varepsilon_{PA}\hat{\varepsilon}}. \tag{A9}$$

Appendix B. Details of Numerical Simulations

Under the passive frequency-shift attack, the parameters obtained by statistics can be shown in the following. The number of the right raw bits can be simulated as

$$\begin{aligned} n_{\text{sig}} = \sum_{k,m\in M} \Big[& p_{zv,km}\left[\overline{p}_d e^{-\frac{\mu^A_{zv,km}}{2}} - \overline{p}_d^2 e^{-\mu^A_{zv,km}}\right] \\ & + p_{vz,km}\left[\overline{p}_d e^{-\frac{\mu^B_{vz,km}}{2}} - \overline{p}_d^2 e^{-\mu^B_{vz,km}}\right]\Big] \times 2N p_z^2 p_{z0} p_{z1}, \end{aligned} \tag{A10}$$

and the wrong raw bits as

$$\begin{aligned} n_{\text{err}} = & 2N p_z^2 \Big[p_{z1}^2 \sum_{k,m\in M} p_{zz,km}\left[-\overline{p}_d^2 e^{-(\mu^A_{zz,km}+\mu^B_{zz,km})}\right. \\ & \left. + \overline{p}_d e^{-\frac{\mu^A_{zz,km}+\mu^B_{zz,km}}{2}} I_0\left(\sqrt{\mu^A_{zz,km}\mu^B_{zz,km}}\right)\right] + p_{z0}^2 p_d \overline{p}_d \Big]. \end{aligned} \tag{A11}$$

The number of the effective events when Alice sends the states with intensity μ_a and Bob sends vacuum states can be shown as

$$n_{av} = 2N_{av} \sum_{k,m\in M} p_{av,km}\left(\overline{p}_d e^{-\mu^A_{av,km}/2} - \overline{p}_d^2 e^{-\mu^A_{av,km}}\right). \tag{A12}$$

Similarly, we can obtain the parameters n_{va}, n_{vb}, and n_{bv}. The number of the effective events when both Alice and Bob send the vacuum states is

$$n_{vv} = 2N_{vv}p_d\overline{p}_d. \tag{A13}$$

Above, p_d is the dark count rate and $\overline{p}_d = 1 - p_d$, $\mu^A_{av,km} = \mu_a\eta^A_{av,km}$, $\mu^B_{va,km} = \mu_a\eta^B_{va,km}$, $\mu^A_{bv,km} = \mu_b\eta^A_{bv,km}$, and $\mu^A_{vb,km} = \mu_b\eta^A_{vb,km}$. Note that the intensities of state $|e^{i\theta_A}\sqrt{\mu_a\eta^A_{aa,km}}\rangle$ and $|e^{i\theta_B}\sqrt{\mu_a\eta^B_{aa,km}}\rangle$ from Alice and Bob in X_a windows may be different, but this does not mean it could not cause right detection. After the interference, the intensity of the left and right detectors will be

$$\begin{aligned}\mu^l_{aa,km} &= \frac{\mu^A_{aa,km} + \mu^B_{aa,km}}{2} + \sqrt{\mu^A_{aa,km}\mu^B_{aa,km}}\cos\delta,\\ \mu^r_{aa,km} &= \frac{\mu^A_{aa,km} + \mu^B_{aa,km}}{2} - \sqrt{\mu^A_{aa,km}\mu^B_{aa,km}}\cos\delta,\end{aligned} \tag{A14}$$

where $\delta = \theta_B - \theta_A$. The number of the error events in $C_{\Delta^\pm}$ can be shown as

$$n^R_{\Delta^+} = N_{\Delta^+}\sum_{k,m\in W} p_{aa,km}\Big[-\overline{p}_d^2 e^{-\mu^A_{aa,km}-\mu^B_{aa,km}} + \overline{p}_d\int_{-\Delta/2}^{\Delta/2} e_d e^{-\mu^r_{aa,km}} + \overline{e}_d e^{-\mu^l_{aa,km}} d\frac{\delta}{\Delta}\Big], \tag{A15}$$

where e_d is the misalignment-error probability and $\overline{e}_d = 1 - e_d$. Similarly, we can obtain the parameter $n^L_{\Delta^-}$.

Appendix C. Details of Transmission

We show the total transmission η^A_{km} which are set to acquire R_e and R_{ul} in the following. And for Bob we set $\eta^B_{km} = \eta^A_{mk}$, symmetrically. Figure A1 corresponds to R_{u1}, Figure A2 corresponds to R_{u2}, and Figure A3 corresponds to R_{u3}. Among them the key parameter η^A_{vv} is shown by dashed lines.

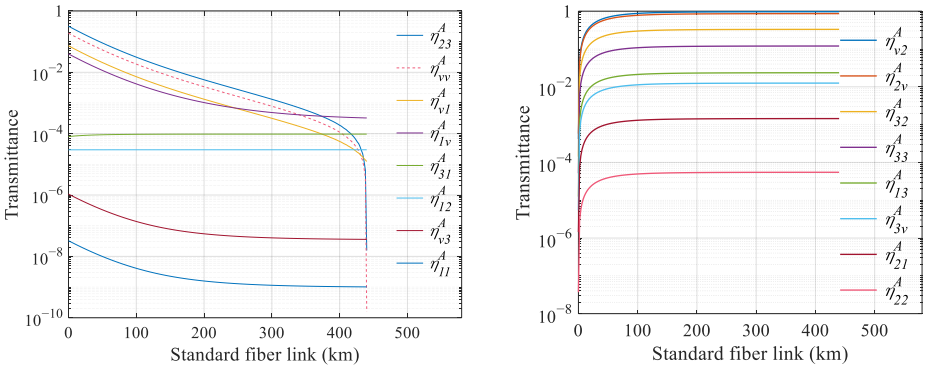

Figure A1. Alice's transmission corresponding to R_{u1}.

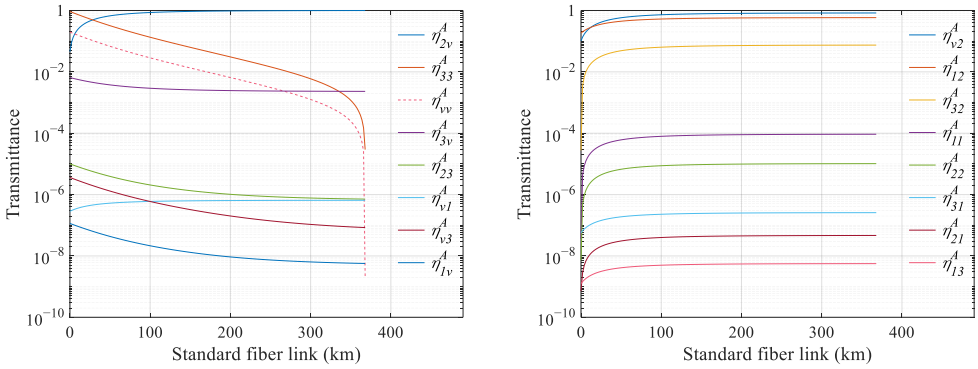

Figure A2. Alice's transmission corresponding to R_{u2}.

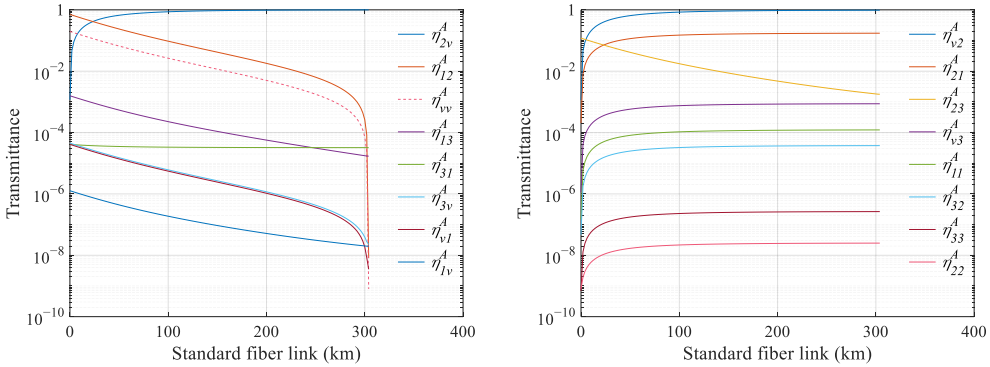

Figure A3. Alice's transmission corresponding to R_{u3}.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
2. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, *12*, 1012–1236. [CrossRef]
3. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
4. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [PubMed]
5. Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
6. Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
7. Wang, X.B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
8. Takeoka, M.; Guha, S.; Wilde, M.M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **2014**, *5*, 5235. [CrossRef]
9. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef]
10. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef]
11. Wang, X.B.; Yu, Z.W.; Hu, X.L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. [CrossRef]
12. Ma, X.; Zeng, P.; Zhou, H. Phase-Matching Quantum Key Distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
13. Curty, M.; Azuma, K.; Lo, H.K. Simple security proof of twin-field type quantum key distribution protocol. *Npj Quant. Inf.* **2019**, *5*, 64. [CrossRef]
14. Cui, C.; Yin, Z.Q.; Wang, R.; Chen, W.; Wang, S.; Guo, G.C.; Han, Z.F. Twin-Field Quantum Key Distribution without Phase Postselection. *Phys. Rev. Appl.* **2019**, *11*, 034053. [CrossRef]

15. Yin, H.L.; Fu, Y. Measurement-Device-Independent Twin-Field Quantum Key Distribution. *Sci. Rep.* **2019**, *9*, 3045. [CrossRef] [PubMed]
16. Lin, J.; Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **2018**, *98*, 042332. [CrossRef]
17. Tamaki, K.; Lo, H.; Wang, W.; Lucamarini, M. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. *arXiv* **2018**, arXiv:1805.05511v1.
18. Jiang, C.; Yu, Z.W.; Hu, X.L.; Wang, X.B. Unconditional Security of Sending or Not Sending Twin-Field Quantum Key Distribution with Finite Pulses. *Phys. Rev. Appl.* **2019**, *12*, 024061. [CrossRef]
19. Jiang, C.; Hu, X.L.; Xu, H.; Yu, Z.W.; Wang, X.B. Zigzag approach to higher key rate of sending-or-not-sending twin field quantum key distribution with finite-key effects. *New J. Phys.* **2020**, *22*, 053048. [CrossRef]
20. Currás-Lorenzo, G.; Navarrete, Á.; Azuma, K.; Kato, G.; Curty, M.; Razavi, M. Tight finite-key security for twin-field quantum key distribution. *Npj Quant. Inf.* **2021**, *7*, 22. [CrossRef]
21. Lu, F.Y.; Yin, Z.Q.; Wang, R.; Fan-Yuan, G.J.; Wang, S.; He, D.Y.; Chen, W.; Huang, W.; Xu, B.J.; Guo, G.C.; et al. Practical issues of twin-field quantum key distribution. *New J. Phys.* **2019**, *21*, 123030. [CrossRef]
22. Hu, X.L.; Jiang, C.; Yu, Z.W.; Wang, X.B. Sending-or-not-sending twin-field protocol for quantum key distribution with asymmetric source parameters. *Phys. Rev. A* **2019**, *100*, 062337. [CrossRef]
23. Zhou, X.Y.; Zhang, C.H.; Zhang, C.M.; Wang, Q. Asymmetric sending or not sending twin-field quantum key distribution in practice. *Phys. Rev. A* **2019**, *99*, 062316. [CrossRef]
24. Wang, W.; Lo, H.K. Simple method for asymmetric twin-field quantum key distribution. *New J. Phys.* **2020**, *22*, 013020. [CrossRef]
25. Currás-Lorenzo, G.; Wooltorton, L.; Razavi, M. Twin-Field Quantum Key Distribution with Fully Discrete Phase Randomization. *Phys. Rev. Appl.* **2021**, *15*, 014016. [CrossRef]
26. Zhang, C.M.; Xu, Y.W.; Wang, R.; Wang, Q. Twin-Field Quantum Key Distribution with Discrete-Phase-Randomized Sources. *Phys. Rev. Appl.* **2020**, *14*, 064070. [CrossRef]
27. Zeng, P.; Wu, W.; Ma, X. Symmetry-Protected Privacy: Beating the Rate-Distance Linear Bound Over a Noisy Channel. *Phys. Rev. Appl.* **2020**, *13*, 064013. [CrossRef]
28. Wang, R.; Yin, Z.Q.; Lu, F.Y.; Wang, S.; Chen, W.; Zhang, C.M.; Huang, W.; Xu, B.J.; Guo, G.C.; Han, Z.F. Optimized protocol for twin-field quantum key distribution. *Commun. Phys.* **2020**, *3*, 149. [CrossRef]
29. Xu, H.; Yu, Z.W.; Jiang, C.; Hu, X.L.; Wang, X.B. Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate. *Phys. Rev. A* **2020**, *101*, 042330. [CrossRef]
30. Yu, Z.W.; Hu, X.L.; Jiang, C.; Xu, H.; Wang, X.B. Sending-or-not-sending twin-field quantum key distribution in practice. *Sci. Rep.* **2019**, *9*, 3080. [CrossRef]
31. Grasselli, F.; Curty, M. Practical decoy-state method for twin-field quantum key distribution. *New J. Phys.* **2019**, *21*, 073001. [CrossRef]
32. Minder, M.; Pittaluga, M.; Roberts, G.L.; Lucamarini, M.; Dynes, J.F.; Yuan, Z.L.; Shields, A.J. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photon.* **2019**, *13*, 334–338. [CrossRef]
33. Wang, S.; He, D.Y.; Yin, Z.Q.; Lu, F.Y.; Cui, C.H.; Chen, W.; Zhou, Z.; Guo, G.C.; Han, Z.F. Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System. *Phys. Rev. X* **2019**, *9*, 021046. [CrossRef]
34. Zhong, X.; Hu, J.; Curty, M.; Qian, L.; Lo, H.K. Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution. *Phys. Rev. Lett.* **2019**, *123*, 100506. [CrossRef]
35. Liu, Y.; Yu, Z.W.; Zhang, W.; Guan, J.Y.; Chen, J.P.; Zhang, C.; Hu, X.L.; Li, H.; Jiang, C.; Lin, J.; et al. Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending. *Phys. Rev. Lett.* **2019**, *123*, 100505. [CrossRef] [PubMed]
36. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.; Hu, X.L.; Guan, J.Y.; Yu, Z.W.; Xu, H.; Lin, J.; et al. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. *Phys. Rev. Lett.* **2020**, *124*, 070501. [CrossRef] [PubMed]
37. Fang, X.T.; Zeng, P.; Liu, H.; Zou, M.; Wu, W.; Tang, Y.L.; Sheng, Y.J.; Xiang, Y.; Zhang, W.; Li, H.; et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photon.* **2020**, *14*, 422–425. [CrossRef]
38. Liu, H.; Jiang, C.; Zhu, H.T.; Zou, M.; Yu, Z.; Hu, X.L.; Xu, H.; Ma, S.; Han, Z.; Chen, J.; et al. Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km. *arXiv* **2021**, arXiv:2101.00276v1.
39. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.J.; Han, Z.Y.; Ma, S.Z.; Hu, X.L.; Li, Y.H.; Liu, H.; et al. Twin-Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans. *arXiv* **2021**, arXiv:2102.00433v1.
40. Tang, Y.L.; Yin, H.L.; Ma, X.; Fung, C.H.F.; Liu, Y.; Yong, H.L.; Chen, T.Y.; Peng, C.Z.; Chen, Z.B.; Pan, J.W. Source attack of decoy-state quantum key distribution using phase information. *Phys. Rev. A* **2013**, *88*, 022308. [CrossRef]
41. Tamaki, K.; Curty, M.; Lucamarini, M. Decoy-state quantum key distribution with a leaky source. *New J. Phys.* **2016**, *18*, 065008. [CrossRef]
42. Huang, A.; Sun, S.H.; Liu, Z.; Makarov, V. Quantum key distribution with distinguishable decoy states. *Phys. Rev. A* **2018**, *98*, 012330. [CrossRef]
43. Sajeed, S.; Radchenko, I.; Kaiser, S.; Bourgoin, J.P.; Pappa, A.; Monat, L.; Legré, M.; Makarov, V. Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing. *Phys. Rev. A* **2015**, *91*, 032326. [CrossRef]

44. Vakhitov, A.; Makarov, V.; Hjelme, D.R. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *J. Mod. Opt.* **2001**, *48*, 2023–2038. [CrossRef]
45. Gisin, N.; Fasel, S.; Kraus, B.; Zbinden, H.; Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **2006**, *73*, 022320. [CrossRef]
46. Jain, N.; Anisimova, E.; Khan, I.; Makarov, V.; Marquardt, C.; Leuchs, G. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.* **2014**, *16*, 123030. [CrossRef]
47. Lucamarini, M.; Choi, I.; Ward, M.B.; Dynes, J.F.; Yuan, Z.L.; Shields, A.J. Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution. *Phys. Rev. X* **2015**, *5*, 031030. [CrossRef]
48. Bugge, A.N.; Sauge, S.; Ghazali, A.M.M.; Skaar, J.; Lydersen, L.; Makarov, V. Laser Damage Helps the Eavesdropper in Quantum Cryptography. *Phys. Rev. Lett.* **2014**, *112*, 070503. [CrossRef]
49. Sun, S.H.; Xu, F.; Jiang, M.S.; Ma, X.C.; Lo, H.K.; Liang, L.M. Effect of source tampering in the security of quantum cryptography. *Phys. Rev. A* **2015**, *92*, 022304. [CrossRef]
50. Pang, X.L.; Yang, A.L.; Zhang, C.N.; Dou, J.P.; Li, H.; Gao, J.; Jin, X.M. Hacking Quantum Key Distribution via Injection Locking. *Phys. Rev. Appl.* **2020**, *13*, 034008. [CrossRef]
51. Yin, H.L.; Liu, P.; Dai, W.W.; Ci, Z.H.; Gu, J.; Gao, T.; Wang, Q.W.; Shen, Z.Y. Experimental composable security decoy-state quantum key distribution using time-phase encoding. *Opt. Express* **2020**, *28*, 29479–29485. [CrossRef]
52. Jiang, M.S.; Sun, S.H.; Li, C.Y.; Liang, L.M. Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states. *Phys. Rev. A* **2012**, *86*, 032310. [CrossRef]
53. Jiang, M.S.; Sun, S.H.; Li, C.Y.; Liang, L.M. Frequency shift attack on 'plug-and-play' quantum key distribution systems. *J. Mod. Opt.* **2014**, *61*, 147–153. [CrossRef]
54. Winzer, P.J.; Essiambre, R. Advanced Optical Modulation Formats. *Proc. IEEE* **2006**, *94*, 952–985. [CrossRef]
55. Gottesman, D.; Lo, H.K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **2004**, *4*, 325–360.
56. Inamori, H.; Lütkenhaus, N.; Mayers, D. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D* **2007**, *41*, 599. [CrossRef]
57. Zhang, W.; Kadosawa, Y.; Tomita, A.; Ogawa, K.; Okamoto, A. State preparation robust to modulation signal degradation by use of a dual parallel modulator for high-speed BB84 quantum key distribution systems. *Opt. Express* **2020**, *28*, 13965–13977. [CrossRef] [PubMed]
58. Nakata, K.; Tomita, A.; Fujiwara, M.; Yoshino, K.I.; Tajima, A.; Okamoto, A.; Ogawa, K. Intensity fluctuation of a gain-switched semiconductor laser for quantum key distribution systems. *Opt. Express* **2017**, *25*, 622–634. [CrossRef] [PubMed]
59. Tamaki, K.; Curty, M.; Kato, G.; Lo, H.K.; Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **2014**, *90*, 052314. [CrossRef]
60. Pereira, M.; Curty, M.; Tamaki, K. Quantum key distribution with flawed and leaky sources. *Npj Quant. Inf.* **2019**, *5*, 62. [CrossRef]
61. Mizutani, A.; Sasaki, T.; Takeuchi, Y.; Tamaki, K.; Koashi, M. Quantum key distribution with simply characterized light sources. *Npj Quant. Inf.* **2019**, *5*, 87. [CrossRef]
62. Navarrete, Á.; Pereira, M.; Curty, M.; Tamaki, K. Practical Quantum Key Distribution That is Secure Against Side Channels. *Phys. Rev. Appl.* **2021**, *15*, 034072. [CrossRef]
63. Pereira, M.; Kato, G.; Mizutani, A.; Curty, M.; Tamaki, K. Quantum key distribution with correlated sources. *Sci. Adv.* **2020**, *6*, 4487. [CrossRef]
64. Dynes, J.F.; Lucamarini, M.; Patel, K.A.; Sharpe, A.W.; Ward, M.B.; Yuan, Z.L.; Shields, A.J. Testing the photon-number statistics of a quantum key distribution light source. *Opt. Express* **2018**, *26*, 22733–22749. [CrossRef] [PubMed]
65. Wang, X.B.; Hu, X.L.; Yu, Z.W. Practical Long-Distance Side-Channel-Free Quantum Key Distribution. *Phys. Rev. Appl.* **2019**, *12*, 054034. [CrossRef]
66. Yu, Z.W.; Zhou, Y.H.; Wang, X.B. Three-intensity decoy-state method for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2013**, *88*, 062339. [CrossRef]
67. Tomamichel, M.; Lim, C.C.W.; Gisin, N.; Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **2012**, *3*, 634. [CrossRef]
68. Chernoff, H. A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations. *Ann. Math. Stat.* **1952**, *23*, 493–507. [CrossRef]
69. Curty, M.; Xu, F.; Cui, W.; Lim, C.C.; Tamaki, K.; Lo, H.K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **2014**, *5*, 3732. [CrossRef]