Article

Sending or Not-Sending Twin-Field Quantum Key Distribution with Flawed and Leaky Sources

Yi-Fei Lu ^{1,2} , Yang Wang ^{1,2,3,*} , Mu-Sheng Jiang ^{1,2}, Xiao-Xu Zhang ^{1,2} , Fan Liu ^{1,2}, Hong-Wei Li ^{1,2}, Chun Zhou ^{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.); jms@qiclab.cn (M.-S.J.); zxx@qiclab.cn (X.-X.Z.); lf@qiclab.cn (F.L.); lhw@qiclab.cn (H.-W.L.); zc@qiclab.cn (C.Z.)

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: wy@qiclab.cn (Y.W.); bws@qiclab.cn (W.-S.B.)

Abstract: Twin-field quantum key distribution (TF-QKD) has attracted considerable attention and developed rapidly due to its ability to surpass the fundamental rate-distance limit of QKD. However, the device imperfections may compromise its practical implementations. The goal of this paper is to make it robust against the state preparation flaws (SPFs) and side channels at the light source. We adopt the sending or not-sending (SNS) TF-QKD protocol to accommodate the SPFs and multiple optical modes in the emitted states. We analyze that the flaws of the phase modulation can be overcome by regarding the deviation of the phase as phase noise and eliminating it with the post-selection of phase. To overcome the side channels, we extend the generalized loss-tolerant (GLT) method to the four-intensity decoy-state SNS protocol. Remarkably, by decomposing of the two-mode single-photon states, the phase error rate can be estimated with only four parameters. The practical security of the SNS protocol with flawed and leaky source can be guaranteed. Our results might constitute a crucial step towards guaranteeing the practical implementation of the SNS protocol.

Keywords: twin-field; practical security; loss-tolerant

Citation: Lu, Y.-F.; Wang, Y.; Jiang, M.-S.; Zhang, X.-X.; Liu, F.; Li, H.-W.; Zhou, C.; Tang, S.-B.; Wang, J.-Y.; Bao, W.-S. Sending or Not-Sending Twin-Field Quantum Key Distribution with Flawed and Leaky Sources. *Entropy* **2021**, *23*, 1103. <https://doi.org/10.3390/e23091103>

Academic Editor: Masahito Hayashi

Received: 4 August 2021

Accepted: 20 August 2021

Published: 25 August 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Quantum key distribution (QKD) promises to share a common secret key with its security guaranteed by the principles of quantum physics [1]. Notable progress has been made towards QKD over the practical security and performance [2,3]. The decoy-state method [4–6] allows the use of the practical sources while maintaining the secret key rate (SKR) at a level comparable to that of the perfect single-photon source. The measurement-device-independent QKD (MDI-QKD) [7] can remove all potential security loopholes in the photon-detection unit.

However, the fundamental limits [8,9] indicate that the SKR scales linearly with the transmittance of channel between Alice and Bob in the absence of the quantum repeater. Fortunately, remarkable progress has been made with the proposal of twin-field QKD (TF-QKD) [10] and its variants [11–16]. TF-QKD protocols improve the SKR to the square root of the channel transmittance, which means it can surpass the repeaterless secret key capacities [8,9]. In addition, TF-QKD protocols possess the property of measurement-device-independent and can be applied using the practical light source (e.g., the coherent light source) with the decoy-state method. It is equivalent to prepare the two-mode single-photon states with the coherent states through the pre-selection or post-selection of phase, which means the coherent light source is an advantage over the single-photon source.

Among all TF-QKD protocols, the sending or not-sending (SNS) TF-QKD protocol [11] can improve the tolerable threshold of misalignment error in the single-photon interference. Many effects of the SNS protocol in the practical implementation have been investigated to improve its performance [17–24]. In addition, several experiments on the SNS protocol have been performed in the laboratory [25,26] and field [27] to accelerate its application.

Despite the great progress, some deficiencies would cause the security loopholes at the light source in the practical QKD systems. There are three main causes of the security loopholes [28]: the first is the state preparation flaws (SPFs) caused by the finite precision of the modulation devices, the second is the side channels arising from the mode dependencies or due to the Trojan-horse attacks (THAs), and the third is the classical correlations between the sending pulses. Many attempts are devoted to overcome these security loopholes at the source [29–38] and many experiments have been performed with these methods in different protocols [39–41]. Among them, the loss-tolerant (LT) method [30] proposed by Tamaki et al. can tolerate the SPFs at the light source while maintaining a high SKR. The limitation of the LT method is that it requires the emitting states in the qubit space. The limitation is released by the generalized LT (GLT) method [42], which can include SPFs and the effect of side channels without qubit assumption. In addition, the GLT method does not require a detailed characterization of the side channels, which makes it more practical. The last security loophole, i.e., the classical pulses correlations, can be overcome by regarding the leaked information encoded into the correlations of the pulses as side channels [28].

In TF-QKD protocols, one major goal is the long-distance key distribution, which makes Eve could enhance the imperfections of the light sources by exploiting the large channel loss. In this paper, we adopt the SNS protocol to accommodate the SPFs and side channels at the light source. As the SNS protocol eliminates the phase drift with the method of the post-selection, the flaws can be regarded as phase noise and eliminated in this process. The flaws of intensity modulation, e.g., the intensity fluctuations, can also be overcome [24]. To overcome the side channels, we extend the GLT method [42] to the SNS protocol. It may need at least nine actual yields to calculate the transmission rate of the Pauli operators $\hat{\sigma}_t \otimes \hat{\sigma}_{t'}$ [40]. However, the yields, when Alice and Bob select different bases, cannot be obtained in the SNS protocol. In this paper, according to the characteristic of the states in SNS protocol, we modify the decomposition of the two-mode single-photon states. In this way, only two groups of parameters (two for each group) need to be calculated. To make it more practical, we consider the coherent states as the light sources and analyze how to apply the method in the four-intensity decoy-state SNS protocol.

The paper is arranged as follows. In Section 2, we make a review of the four-intensity decoy-state SNS protocol. We analyze the SNS protocol with flawed and leaky sources in Section 3 and show how to apply the GLT method with the decoy-state method in Section 4. In Section 5, we show the numerical simulations and present the simulation results. Last, the conclusion is given in Section 6.

2. Four-Intensity Decoy-State SNS Protocol

In this section, we make a review of the four-intensity decoy-state SNS protocol [11,17].

(1) State preparation. Alice and Bob independently determines the signal and decoy windows with probabilities p_z and p_x . In signal windows, Alice (Bob) prepares the phase-randomized coherent states with intensity μ_z by probability p_{z1} and denotes it as 1 (0), or prepares the vacuum states $|0\rangle$ (i.e., not sending) by probability $p_{z0} = 1 - p_{z1}$ and denotes it as 0 (1). In decoy windows, Alice (Bob) prepares the phase-randomized coherent states $|\sqrt{\mu_a}e^{i\theta_A}\rangle$, $|\sqrt{\mu_b}e^{i\theta'_A}\rangle$ 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 $p_v = 1 - p_a - p_b$, respectively.

(2) Measurement. Charlie performs the interferometric measurements on all twin fields with a beam splitter (BS) and two single-photon detectors (SPDs). The measurement results d are announced via public channels, where $d = 0$ or 1 corresponds to only the right or left detector clicks.

(3) Basis announcement and sifting. After repeating the above steps N times, Alice and Bob announce their signal and decoy windows through the public channels. Define a Z (X) window as a time window when both Alice and Bob have determined the signal (decoy) windows. Since the phase of the signal states is unknown to Eve, the signal state is equivalent to a probabilistic mixture of different photon-number states $\sum_{k=0}^{\infty} \frac{e^{-\mu_z} \mu_z^k}{k!} |k\rangle\langle k|$. Define the Z_1 windows as a subset of the Z windows when only one party determines to send and Alice (Bob) actually sends the single-photon states $|1\rangle$. In those X windows when they have chosen the same intensity μ_a (μ_b), they announce their phase information θ_A and θ_B and denote them as X_a (X_b) windows. Then they sift the effective events, which is defined as one-detector heralded events in Z windows and one-detector heralded events with θ_A and θ_B satisfying

$$|\theta_A - \theta_B - \varphi_{AB}| \leq \Delta/2 \quad (1)$$

or

$$|\theta_A - \theta_B - \pi - \varphi_{AB}| \leq \Delta/2 \quad (2)$$

in X_a (X_b) windows, where φ_{AB} is set to overcome the phase drift which can be estimated with reference pulses. In this process, they will obtain n_t raw bits in the effective Z windows, which can be used to distill the secret key bits.

(4) Parameter estimation. They can estimate the bit-flip error rate of the raw bits E_z through the error test, the lower bound counting rate $\underline{s}_1$ and the upper bound phase-flip error rate $\bar{e}_1^{ph}$ of the single-photon states in Z_1 windows with the decoy-state method.

(5) Error correction and privacy amplification. Last, they perform error correction on the raw strings and then perform the privacy amplification on the corrected strings.

(6) Key rate formula. With these quantities, the final rate of the secret keys can be expressed as [11,43]

$$R = 2p_{z0}(1 - p_{z0})\mu_z e^{-\mu_z} \underline{s}_1 [1 - H(\bar{e}_1^{ph})] - n_t f H(E_z) / N. \quad (3)$$

To improve the performance of the SNS protocol, Alice and Bob can perform the method of actively odd-parity pairing (AOPP) before error correction in the post-processing step [22,23].

3. Security Analysis of SNS with Flawed and Leaky Sources

In this section, we analyze how to guarantee the practical security of the SNS protocol with the SPFs and the side channels. In the virtual protocol (described in Appendix A) and the actual protocol, the quantum and classical information available to Eve are the same, which means Eve cannot distinguish and behave differently. Therefore, the security of the actual SNS protocol can be guaranteed once the security of the virtual protocol is proved. In the following, we analyze how to calculate the phase error rate, which quantifies the amount of information leaked to Eve and should be removed in the privacy amplification step. Moreover, the lower bound counting rate of the single-photon states $\underline{s}_1$ can be estimated with the decoy-state method [17].

The flaws of phase modulation can be overcome directly with the method of the post-selection of phase. In signal windows, Alice and Bob encode bits on their decision to sending or not-sending but not their phase, which makes the signal states immune to the flaws of the phase modulation. However, the phase-randomization assumption should be guaranteed when using the coherent light source. Attacks may be applied when the assumption is violated [44,45]. Fortunately, this assumption can be guaranteed in the SNS protocol once the flaws are known to Alice and Bob. For example, consider the actual phase as $\theta_A + \delta\theta_A/\pi$ ($\theta_B - \delta\theta_B/\pi$) for Alice (Bob), where θ_A (θ_B) is the expected phase and δ is the deviation of the phase modulation [30,42]. In this scenario, they could ensure θ_A is random to Eve and just regard $\delta\theta_A/\pi$ ($\delta\theta_B/\pi$) as phase noise, which can be eliminated with post-selection of phase. The flaws of the phase modulation in decoy windows can be overcome in the same way. In the protocol, Alice and Bob could just add $\delta(\theta_A + \theta_B)/\pi$

to φ_{AB} and use the modified parameter. Therefore, the flaws of the phase modulation do not affect the security of the SNS protocol and we only consider the side channels in the following.

The side channels may arise from mode dependencies or due to THAs. Mode dependencies mean the optical mode of signal pulses depends on their settings, which means the basis or bit information may be leaked in various degrees, e.g., the polarization, frequency spectrum, and temporal. Moreover, Eve could perform THAs actively by sending strong light into Alice and Bob's devices and steal information by analyzing the back-reflected light [46–48]. On the one hand, we could equip the systems with security patches by adding filters and isolators to resist these THAs. On the other hand, Eve could attack these components, which may compromise the SKR [49]. For these side channels, we overcome it by extending the GLT method [42] to the SNS protocol as discussed in the following.

Now, the analysis focuses on the virtual protocol. In Z windows, suppose Alice (Bob) prepares $|\Phi_z\rangle_{CE}$ ($|\Phi_z\rangle_{C'E'}$) or vacuum states $|0\rangle$ when deciding sending or not-sending, where

$$|\Phi_z\rangle_{CE} = a_z|\varphi_z\rangle_{CE} + b_z|\varphi_z^\perp\rangle_{CE}, \quad (4)$$

with $|a_z|^2 + |b_z|^2 = 1$. Here, the subscript C and E represent Charlie and Eve's systems, where the latter may include, for example, the trojan light. We assume that $|\varphi_z\rangle_{CE} = |1\rangle_C \otimes |0\rangle_E$ is a pure state in the single-mode qubit space, and $|\varphi_z^\perp\rangle_{CE}$ is orthogonal to $|\varphi_z\rangle_{CE}$. Therefore, the system E is independent on the system C when considering the states $|\varphi_z\rangle_{CE}$ and $|0\rangle_{CE}$. Ideally, the state prepared by Alice should be $|\Phi_z\rangle_{CE}^{ideal} = |\varphi_z\rangle_{CE}$ with no side channels. Please note that the system C of the state $|\varphi_z^\perp\rangle_{CE}$ only include the single-photon component which may have side channels (e.g. with different polarization). The form of the pure state in Equation (4) is the most general independently and identically distributed state. For the mixed states in a single-mode qubit space, the analysis is also applicable by introducing the ancillary systems as discussed in Appendix A. Similarly, suppose $|\Phi_z\rangle_{C'E'} = a'_z|\varphi_z\rangle_{C'E'} + b'_z|\varphi_z'^\perp\rangle_{C'E'}$ for Bob, where $|\varphi_z\rangle_{C'E'} = |\varphi_z\rangle_{CE}$.

In the following, we assume $|\Phi_z\rangle_{C'E'} = |\Phi_z\rangle_{CE}$ for simplicity. On the one hand, this assumption is not unreasonable in the following analysis. At first glance, this assumption is unreasonable, because, for example, the trojan light of both sides cannot be controlled by Alice and Bob. However, Alice and Bob do not need to characterize the states $|\varphi_z^\perp\rangle_{CE}$ and $|\varphi_z'^\perp\rangle_{C'E'}$ in the GLT method. Instead, they only need to characterize the lower bound of a_z and a'_z , i.e., the amplitude of the state $|10\rangle_{CE}$. Therefore, we could replace a_z and a'_z with $\min\{a_z, a'_z\}$, and neglect the specific formulas of states $|\varphi_z^\perp\rangle_{CE}$ and $|\varphi_z'^\perp\rangle_{C'E'}$, which will lead to conservative results. On the other hand, this assumption is not necessary and the analysis can also be applied but will be cumbersome without this assumption.

In the virtual protocol, Alice and Bob prepares the following states in Z windows by introducing the local ancillary systems A and B as

$$|\Psi_z^q\rangle_{CEC'E'AB} = \frac{1}{\sqrt{2}}[|0\Phi_z\rangle_{CEC'E'} \otimes |01\rangle_{AB} + (-1)^q |\Phi_z0\rangle_{CEC'E'} \otimes |10\rangle_{AB}], \quad (5)$$

where $q = 0$ or 1 corresponds to the phase difference 0 or π between Alice and Bob. In the actual protocol, Alice and Bob only need to prepare $(|0\Phi_z\rangle\langle 0\Phi_z| + |\Phi_z0\rangle\langle \Phi_z0|)/2$ without encoding the phase difference to 0 or π exactly, which makes it immune to the flaws of the phase modulation. To obtain the phase error rate, they could measure the ancillary system A and B virtually in the basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$ jointly or in the X basis separately [11]. Suppose they obtain the bit values k_x and m_x when measuring the ancillary systems A and B in the X basis. Depending on the phase difference q and the measurement result d , the phase error rate can be defined as

$$E_{(q,d)} = \frac{\sum_{k,m \in \{0,1\}, k \oplus m = q \oplus d} Y_{k_x, m_x}^{(q,d), vir}}{\sum_{k,m \in \{0,1\}} Y_{k_x, m_x}^{(q,d), vir}}, \quad (6)$$

where $Y_{k_x, m_x}^{(q,d),vir}$ is the conditional probability that Alice and Bob obtain bit value k_x and m_x in the X basis and Charlie announces the measurement result d conditioned on that they prepare the states $|\Psi_z^q\rangle_{CEC'E'AB}$. In fact, the states sent out by Alice and Bob are the same for different q , which can be seen by taking partial trace over the systems A and B . In particular, we have $Y_{k_x, m_x}^{(q,d),vir} = Y_{k'_x, m'_x}^{(\bar{q},d),vir}$ when $k_x + m_x = k'_x + m'_x + 1 \pmod{2}$. Hence, the phase error rate corresponding to the measurement result d can be defined as

$$E_d = \frac{\sum_{k,m,q \in \{0,1\}, k \oplus m = q \oplus d} Y_{k_x, m_x}^{(q,d),vir}}{\sum_{k,m,q \in \{0,1\}} Y_{k_x, m_x}^{(q,d),vir}}. \quad (7)$$

With these phase error rates, the cost of performing privacy amplification to remove the correlations between the sifted key bits and Eve is $[n_0 H(E_0) + n_1 H(E_1)] / (n_0 + n_1)$, where n_d is the number of the effective events corresponds to d in Z windows. We can define the overall phase error rate as

$$E_{ph} = \frac{E_0 n_0 + E_1 n_1}{n_0 + n_1}. \quad (8)$$

It will consume more bits to use the formula E_{ph} than E_d when $n_0 \neq n_1$, which may be caused by the imperfect beam splitting ratio of the beam splitter (BS) or the mismatch of the detection efficiency of the two SPDs on Charlie's side. Therefore, we consider the formulas in Equation (7) in this paper.

To obtain the denominator of E_d in Equation (7), we define $Y_{k_z, m_z}^{(q,d)}$ as the conditional probability that Alice and Bob obtains bit values k_z and m_z when measuring the ancillary systems A and B in the Z basis and only the d detector clicks on Charlie's side conditioned on that Alice and Bob prepare the states $|\Psi_z^q\rangle_{CEC'E'AB}$. Please note that Alice and Bob's measurements on the ancillary systems A and B in the Z or X basis is virtual, which can be regarded as ideal measurements with no difference in detection efficiency. Therefore, the denominator of E_d is equal to $\sum_{k,m,q \in \{0,1\}} Y_{k_z, m_z}^{(q,d)}$, which can be observed in the experiment directly. This means we only need to calculate the $Y_{k_x, m_x}^{(q,d),vir}$ in the numerator of E_d .

In the virtual protocol, after obtaining the bit values k_x and m_x in the X basis, they will send Charlie the (unnormalized) state

$$\hat{\sigma}_{CEC'E', k_x, m_x}^{q,vir} = \text{Tr}(I_{CEC'E'} \otimes |k_x\rangle\langle k_x|_A \otimes |m_x\rangle\langle m_x|_B |\Psi_z^q\rangle\langle \Psi_z^q|_{CEC'E'AB}). \quad (9)$$

Substituting Equation (5) into Equation (9), we obtain $\hat{\sigma}_{CEC'E', k_x, m_x}^{q,vir} = |\varphi_{k_x, m_x}^{q,vir}\rangle\langle \varphi_{k_x, m_x}^{q,vir}|_{CEC'E'}$ with

$$|\varphi_{k_x, m_x}^{q,vir}\rangle_{CEC'E'} = \frac{a_z}{2} |\gamma_{k_x, m_x}^{q,vir}\rangle_{CEC'E'} + \frac{b_z}{2} |\gamma_{k_x, m_x}^{\perp, q,vir}\rangle_{CEC'E'}. \quad (10)$$

Here, the normalized state $|\varphi_{k_x, m_x}^{q,vir}\rangle_{CEC'E'}$ is

$$|\gamma_{k_x, m_x}^{q,vir}\rangle_{CEC'E'} = \frac{1}{\sqrt{2}} [|0\varphi_z\rangle_{CEC'E'} + (-1)^{q+k+m} |\varphi_z 0\rangle_{CEC'E'}]. \quad (11)$$

Since the inner products $\langle \varphi_z | 0 \rangle_{CE}$ and $\langle \varphi_z^\perp | 0 \rangle_{CE}$ are equal to 0, the normalized states $|\gamma_{k_x, m_x}^{\perp, q,vir}\rangle_{CEC'E'}$ that is orthogonal to $|\varphi_{k_x, m_x}^{q,vir}\rangle_{CEC'E'}$ can be shown as

$$|\gamma_{k_x, m_x}^{\perp, q,vir}\rangle_{CEC'E'} = \frac{1}{\sqrt{2}} [|0\varphi_z^\perp\rangle_{CEC'E'} + (-1)^{q+k+m} |\varphi_z^\perp 0\rangle_{CEC'E'}]. \quad (12)$$

Therefore, the conditional probability $Y_{k_x, m_x}^{(q,d),vir}$ can be expressed as

$$Y_{k_x, m_x}^{(q,d),vir} = \text{Tr}(\hat{D}_d \hat{\sigma}_{CEC'E', k_x, m_x}^{q,vir}), \quad (13)$$

where $\hat{D}_d = \sum_k \hat{A}_k^\dagger \hat{M}_d \hat{A}_k$ corresponds to Eve's action represented by the Kraus operators $\{\hat{A}_k\}$ and Charlie's measurement with POVMs $\{\hat{M}_d\}$. Here, we assume that Eve applies the same quantum operation to every pulses, which corresponds to the collective attack. The analysis can be extended to coherent attacks which is discussed in Appendix B. Combining Equations (9), (10) and (13), we obtain the following expression

$$Y_{k_x, m_x}^{(q,d),vir} = \frac{1}{4} \left[|a_z|^2 \text{Tr}(\hat{D}_d |\gamma_{k_x, m_x}^{q,vir}\rangle \langle \gamma_{k_x, m_x}^{q,vir}|_{CEC'E'}) + \text{Tr}(\hat{D}_d (a_z^* b_z |\gamma_{k_x, m_x}^{\perp,q,vir}\rangle \langle \gamma_{k_x, m_x}^{q,vir}|_{CEC'E'} + a_z b_z^* |\gamma_{k_x, m_x}^{q,vir}\rangle \langle \gamma_{k_x, m_x}^{\perp,q,vir}|_{CEC'E'} + |b_z|^2 |\gamma_{k_x, m_x}^{\perp,q,vir}\rangle \langle \gamma_{k_x, m_x}^{\perp,q,vir}|_{CEC'E'}) \right] \quad (14)$$

The lower and upper bounds of $Y_{k_x, m_x}^{(q,d),vir}$ can be obtained by calculating the bounds of the first and second terms in Equation (14), separately.

The density matrix of the state $|\gamma_{k_x, m_x}^{q,vir}\rangle_{CEC'E'}$ can be decomposed as

$$|\gamma_{k_x, m_x}^{q,vir}\rangle \langle \gamma_{k_x, m_x}^{q,vir}|_{CEC'E'} = [\rho_x + (-1)^{q+k+m} \rho_y] \otimes |00\rangle \langle 00|_{EE'}, \quad (15)$$

with $\rho_x = (|01\rangle \langle 01|_{CC'} + |10\rangle \langle 10|_{CC'})/2$ and $\rho_y = (|01\rangle \langle 10|_{CC'} + |10\rangle \langle 01|_{CC'})/2$. Here, $\rho_x + (-1)^{q+k+m} \rho_y$ is the density operator of the two-mode single-photon state $(|01\rangle + (-1)^{q+k+m} |10\rangle)/\sqrt{2}$, but ρ_x and ρ_y are not density operator of some particular states, which is different from the original GLT method [42]. Therefore, the component in the first term of Equation (14) can be expressed as

$$\text{Tr}(\hat{D}_d |\gamma_{k_x, m_x}^{q,vir}\rangle \langle \gamma_{k_x, m_x}^{q,vir}|_{CEC'E'}) = x_d + (-1)^{q+k+m} y_d, \quad (16)$$

where $x_d = \text{Tr}[\hat{D}_d \rho_x]$ and $y_d = \text{Tr}[\hat{D}_d \rho_y]$. Here, $x_d + (-1)^{q+k+m} y_d$ can be regarded as the transmission rate of the state $(|01\rangle + (-1)^{q+k+m} |10\rangle)/\sqrt{2}$. In this way, we only need to calculate the parameters x_d and y_d . The number of parameters that need to be solved is reduced. The second term of Equation (14) can be written as $\text{Tr}(\hat{D}_d N_z)$, where the matrix

$$N_z = \begin{bmatrix} |b_z|^2 & a_z^* b_z & 0_{1 \times 2} \\ a_z b_z^* & 0_{1 \times 1} & 0_{1 \times 2} \\ 0_{2 \times 1} & 0_{2 \times 1} & 0_{2 \times 2} \end{bmatrix}. \quad (17)$$

with eigenvalues

$$\begin{aligned} \lambda_{\min}^z &= \frac{|b_z|^2 - |b_z| \sqrt{|b_z|^2 + 4|a_z|^2}}{2}, \\ \lambda_{\max}^z &= \frac{|b_z|^2 + |b_z| \sqrt{|b_z|^2 + 4|a_z|^2}}{2}, \end{aligned} \quad (18)$$

and $\lambda_0 = 0$. Using the properties of POVMs, the eigenvalues of $\hat{D}_d$ are between 0 and 1. Hence, $\text{Tr}(\hat{D}_d N_z)$ can be bounded by $\lambda_{\min}^z \leq \text{Tr}(\hat{D}_d N_z) \leq \lambda_{\max}^z$.

In the following, we analyze how to obtain the bounds of x_d, y_d with the events in X windows. Consider the X_α windows in the virtual protocol and assume they prepare the states as

$$|\Psi_\alpha^{(\theta_A, \theta_B)}\rangle_{CEC'E'AB} = \frac{1}{\sqrt{2}} [e^{i\theta_B} |0\rangle_{\Phi_\alpha} \rangle_{CEC'E'} \otimes |01\rangle_{AB} + e^{i\theta_A} |\Phi_\alpha 0\rangle_{CEC'E'} \otimes |10\rangle_{AB}], \quad (19)$$

where

$$|\Phi_\alpha\rangle_{CE} = a_\alpha |\varphi_\alpha\rangle_{CE} + b_\alpha |\varphi_\alpha^\perp\rangle_{CE}. \quad (20)$$

Similar to Z windows, we suppose that $|\varphi_\alpha\rangle_{CE} = |1\rangle_C \otimes |0\rangle_E$ is a pure state in a single-mode qubit space and $|\varphi_\alpha^\perp\rangle_{CE}$ is orthogonal to $|\varphi_\alpha\rangle_{CE}$. Therefore, the system E is

independent on the system C for the states $|\varphi_\alpha\rangle_{CE}$, $|\varphi_z\rangle_{CE}$, and $|00\rangle_{CE}$, which means the side channels are only included in the states $|\varphi_\alpha^\perp\rangle_{CE}$ and $|\varphi_z^\perp\rangle_{CE}$.

Define the conditional probability $Y_{k_x, m_x}^{(c,d), \alpha, \Delta}$ that Alice and Bob obtain k_x and m_x in the X basis and only the d detector clicks on Charlie's side conditioned on that Alice and Bob prepare the state $|\Psi_\alpha^{(\theta_A, \theta_B)}\rangle_{CEC'E'AB}$ with phase θ_A and θ_B satisfying Equation (1) or Equation (2) (denoted as $c = 0$ or 1 , respectively). After measuring the ancillary systems A and B in the X basis, they will send Charlie the (unnormalized) state

$$\hat{\sigma}_{CEC'E', k_x, m_x}^{(\theta_A, \theta_B), \alpha} = \text{Tr}(I_{CEC'E'} \otimes |k_x\rangle\langle k_x|_A \otimes |m_x\rangle\langle m_x|_B |\Psi_\alpha^{(\theta_A, \theta_B)}\rangle\langle\Psi_\alpha^{(\theta_A, \theta_B)}|_{CEC'E'AB}). \quad (21)$$

Substituting Equation (19) into Equation (21), we obtain $\hat{\sigma}_{CEC'E', k_x, m_x}^{(\theta_A, \theta_B), \alpha} = |\varphi_{k_x, m_x}^{(\theta_A, \theta_B), \alpha}\rangle\langle\varphi_{k_x, m_x}^{(\theta_A, \theta_B), \alpha}|_{CEC'E'}$ with the unnormalized state

$$|\varphi_{k_x, m_x}^{(\theta_A, \theta_B), \alpha}\rangle_{CEC'E'} = \frac{a_\alpha}{2} |\gamma_{k_x, m_x}^{(\theta_A, \theta_B), \alpha}\rangle_{CEC'E'} + \frac{b_\alpha}{2} |\gamma_{k_x, m_x}^{\perp, (\theta_A, \theta_B), \alpha}\rangle_{CEC'E'}. \quad (22)$$

The normalized state $|\gamma_{k_x, m_x}^{(\theta_A, \theta_B), \alpha}\rangle_{CEC'E'}$ can be shown as

$$|\gamma_{k_x, m_x}^{(\theta_A, \theta_B), \alpha}\rangle_{CEC'E'} = \frac{1}{\sqrt{2}} [e^{i\theta_B} |0\varphi_\alpha\rangle_{CEC'E'} + (-1)^{k+m} e^{i\theta_A} |\varphi_\alpha 0\rangle_{CEC'E'}]. \quad (23)$$

And the normalized state $|\gamma_{k_x, m_x}^{\perp, (\theta_A, \theta_B), \alpha}\rangle_{CEC'E'}$ which is orthogonal to $|\gamma_{k_x, m_x}^{(\theta_A, \theta_B), \alpha}\rangle_{CEC'E'}$ can be shown as

$$|\gamma_{k_x, m_x}^{\perp, (\theta_A, \theta_B), \alpha}\rangle_{CEC'E'} = \frac{1}{\sqrt{2}} [e^{i\theta_B} |0\varphi_\alpha^\perp\rangle_{CEC'E'} + (-1)^{k+m} e^{i\theta_A} |\varphi_\alpha^\perp 0\rangle_{CEC'E'}]. \quad (24)$$

Therefore, the conditional probability $Y_{k_x, m_x}^{(c,d), \alpha, \Delta}$ can be expressed as

$$\begin{aligned} Y_{k_x, m_x}^{(c,d), \alpha, \Delta} &= \frac{1}{\Delta} \int_{\pi\delta(c-1)-\Delta/2}^{\pi\delta(c-1)+\Delta/2} \text{Tr}(\hat{D}_d \hat{\sigma}_{CEC'E', k_x, m_x}^{(\theta_A, \theta_B)}) d(\theta_A - \theta_B) \\ &= \frac{1}{4} [|a_\alpha|^2 (x_d + 2(-1)^{(c+k+m)} (y_d/\Delta) \sin(\Delta/2)) + \text{Tr}(\hat{D}_d N_\alpha)], \end{aligned} \quad (25)$$

where $\delta(x) = 1$ when $x = 0$, and $\delta(x) = 0$ when $x \neq 0$. The matrix N_α can be shown as

$$N_\alpha = \begin{bmatrix} |b_\alpha|^2 & a_\alpha^* b_\alpha & 0_{1 \times 2} \\ a_\alpha b_\alpha^* & 0_{1 \times 1} & 0_{1 \times 2} \\ 0_{2 \times 1} & 0_{2 \times 1} & 0_{2 \times 2} \end{bmatrix}. \quad (26)$$

Therefore, $\text{Tr}(\hat{D}_d N_\alpha)$ can be bounded as $\lambda_{\min}^\alpha \leq \text{Tr}(\hat{D}_d N_\alpha) \leq \lambda_{\max}^\alpha$, where

$$\begin{aligned} \lambda_{\min}^\alpha &= \frac{|b_\alpha|^2 - |b_\alpha| \sqrt{|b_\alpha|^2 + 4|a_\alpha|^2}}{2}, \\ \lambda_{\max}^\alpha &= \frac{|b_\alpha|^2 + |b_\alpha| \sqrt{|b_\alpha|^2 + 4|a_\alpha|^2}}{2}, \end{aligned} \quad (27)$$

are the eigenvalues of the matrix N_α .

Set Δ_2 be equal to the parameter Δ selected in the protocol in Equations (1) and (2), and $\Delta_1 = 2\Delta$, we obtain two linear equalities of $Y_{k_x, m_x}^{(c,d), \alpha, \Delta_1}$ and $Y_{k_x, m_x}^{(c,d), \alpha, \Delta_2}$ according to Equation (25). By solving the linear equalities, we obtain

$$x_d = \frac{4}{|a_\alpha|^2} \frac{\Delta_1 Y_{k_x, m_x}^{(c,d), \alpha, \Delta_1} \sin(\Delta_2/2) - \Delta_2 Y_{k_x, m_x}^{(c,d), \alpha, \Delta_2} \sin(\Delta_1/2)}{\Delta_1 \sin(\Delta_2/2) - \Delta_2 \sin(\Delta_1/2)} - \frac{\text{Tr}(\hat{D}_d N_\alpha)}{|a_\alpha|^2}, \quad (28)$$

and

$$y_d = \frac{2\Delta_1\Delta_2}{(-1)^{c+k+m}|a_\alpha|^2} \frac{Y_{k_x, m_x}^{(c,d), \alpha, \Delta_2} - Y_{k_x, m_x}^{(c,d), \alpha, \Delta_1}}{\Delta_1 \sin(\Delta_2/2) - \Delta_2 \sin(\Delta_1/2)}. \quad (29)$$

Therefore, x_d and y_d can be obtained with the yields $Y_{k_x, m_x}^{(c,d), \alpha, \Delta}$. In the actual protocol, we analyze how to obtain the yields $Y_{k_x, m_x}^{(c,d), \alpha, \Delta}$ with the decoy-state method in the next section.

4. Parameter Estimation

In the actual protocol, Alice and Bob do not have the single-photon source and will prepare the coherent states. They neither prepare the ancillary systems A and B nor perform the local measurement. Therefore, we need to reduce it to the actual protocol and analyze how to calculate the yields $Y_{k_x, m_x}^{(c,d), \alpha, \Delta}$ in the actual protocol.

In the virtual protocol, consider that Alice and Bob measure the ancillary systems A and B in the basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$ jointly, we define $Y_s^{(c,d), \alpha, \Delta} = \sum_{k_x, m_x, k_x \oplus m_x = s} Y_{k_x, m_x}^{(c,d), \alpha, \Delta}$. Therefore we have $Y_{k_x, m_x}^{(c,d), \alpha, \Delta} = Y_{k_x \oplus m_x}^{(c,d), \alpha, \Delta} / 2$. Actually, the states sent are the same for two different s , which means that $Y_s^{(c,d), \alpha, \Delta} = Y_{\bar{s}}^{(c,d), \alpha, \Delta}$. When the parameter c is announced, the parameter $Y_s^{(c,d), \alpha, \Delta}$ can be obtained without knowing the parameter s . In this way, the virtual measurements on the ancillary systems A and B can be eliminated by regarding the measurement results as s . In the following, we analyze how to obtain the parameter $Y_s^{(c,d), \alpha, \Delta}$ with the four-intensity decoy-state method.

In the actual protocol, the ideal two-mode weak coherent states in X_α windows prepared by them are $|\sqrt{\mu_\alpha}e^{i\theta_A}\rangle \otimes |\sqrt{\mu_\alpha}e^{i\theta_B}\rangle$ ($\alpha \in \{a, b\}$) with the restriction of Equations (1) and (2). By introducing two independent variables $\delta_\pm = (\theta_A \pm \theta_B)/2$, we can integrate the two-mode state on variable δ_+ and obtain a classical mixture

$$\sum_{t=0}^{\infty} p_t^\alpha |\psi_t\rangle \langle \psi_t|, \quad (30)$$

with $|\psi_t\rangle$ being the state of total photon number t for the two-mode state and p_t^α being its probability. To be specific,

$$|\psi_t\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^t \sqrt{C_t^j} e^{i[j\theta_A + (t-j)\theta_B]} |j, t-j\rangle, \quad (31)$$

with probability

$$p_t^\alpha = e^{-2\mu_\alpha} \frac{2^t \mu_\alpha^t}{t!}. \quad (32)$$

Define $Q_\alpha^{(c,d), \Delta}$ as the conditional probability that the measurement result is d conditioned on that they both send the coherent states with intensity μ_α , the phase slice is Δ , and their phases satisfy Equation (1) ($c = 0$) or Equation (2) ($c = 1$). Here, $Q_\alpha^{(c,d), \Delta}$ can be obtained by statistics in the actual protocol. According to Equation (30), we have

$$Q_\alpha^{(c,d), \Delta} = \sum_{t=0}^{\infty} p_t^\alpha Y_{(t)}^{(c,d), \Delta}, \quad (33)$$

where $Y_{(t)}^{(c,d), \Delta}$ is the probability that the measurement result is d when the two-mode state is $|\psi_t\rangle$ with phases satisfying c and Δ . Thus, we have $Y_s^{(d), \alpha, \Delta} = Y_{(1)}^{(c,d), \Delta} / 2$.

In this paper, we consider the four-intensity decoy states and the value of $Y_{(1)}^{(c,d), \Delta}$ cannot be calculated precisely. However, we can obtain the bounds of $Y_{(1)}^{(c,d), \Delta}$ analytically

or by linear programming. We give an example, which is used in the simulation in Section 5, as follows.

Using two decoy states, i.e., $Q_a^{(c,d),\Delta}$ and $Q_b^{(c,d),\Delta}$, a crude upper bound of $Y_{(1)}^{(c,d),\Delta}$ can be given by abandoning the parts when $t \geq 2$ as

$$Q_a^{(c,d),\Delta} = \sum_{t=0}^{\infty} p_t^\alpha Y_{(t)}^{(c,d),\Delta} \geq p_0^\alpha Y_0 + p_1^\alpha Y_{(1)}^{(c,d),\Delta}, \quad (34)$$

where Y_0 can be estimated with the events when they both send the vacuum states in X windows. Hence, the upper bound of $Y_{(1)}^{(c,d),\Delta}$ can be expressed by

$$Y_{(1)}^{(c,d),\Delta} \leq \frac{Q_a^{(c,d),\Delta} - p_0^\alpha Y_0}{p_1^\alpha}. \quad (35)$$

For the lower bound of $Y_{(1)}^{(c,d),\Delta}$, we consider the linear combination as

$$\begin{aligned} & p_2^b Q_a^{(c,d),\Delta} - p_2^a Q_b^{(c,d),\Delta} - p_0^a p_2^b Y_0 + p_2^a p_0^b Y_0 \\ &= p_1^a p_2^b Y_{(1)}^{(c,d),\Delta} - p_2^a p_1^b Y_{(1)}^{(c,d),\Delta} + \sum_{t=3}^{\infty} (p_t^a p_2^b - p_2^a p_t^b) Y_{(t)}^{(c,d),\Delta}. \end{aligned} \quad (36)$$

The last item of Equation (36) satisfies

$$\sum_{t=3}^{\infty} (p_t^a p_2^b - p_2^a p_t^b) Y_{(t)}^{(c,d),\Delta} = e^{-2(\mu_a + \mu_b)} \mu_a^2 \mu_b^2 \sum_{t=3}^{\infty} \frac{2^{t+1}}{t!} (\mu_a^{t-2} - \mu_b^{t-2}) Y_{(t)}^{(c,d),\Delta} \leq 0. \quad (37)$$

Hence, rewrite Equation (36) with Equation (37), the lower bound of $Y_{(1)}^{(c,d),\Delta}$ is given by

$$Y_{(1)}^{(c,d),\Delta} \geq \frac{p_2^b Q_a^{(c,d),\Delta} - p_2^a Q_b^{(c,d),\Delta} + (p_2^a p_0^b - p_0^a p_2^b) Y_0}{4e^{-2(\mu_a + \mu_b)} \mu_a \mu_b (\mu_b - \mu_a)}. \quad (38)$$

Last, we note that $0 \leq Y_{(1)}^{(c,d),\Delta} \leq 1$.

In this way, the upper bound of the phase error rate can be estimated. We have released the restriction of single-photon states and the preparation of ancillary systems. The above formulas can be used directly in the actual protocol with the decoy-state method.

5. Simulation

In this section, we simulate the performance of the four-intensity decoy-state SNS protocol with AOPP with a particular leaky source. For this purpose, we only consider the polarization side channels and a particular THA.

Suppose the state of system C (C') is dependent on the polarization which can be decomposed as

$$|\Omega_\beta\rangle_C = \cos\theta_\beta |\omega_\beta\rangle_{HC} + \sin\theta_\beta |\omega_\beta^\perp\rangle_{VC}, \quad (39)$$

where $\beta \in \{z, a, b\}$, and the subscripts H and V represent the horizontal and vertical polarization modes. And for the THA, consider the trojan light as the system E (E') shown as

$$|\xi_\beta\rangle_E = C_{I\beta} |e\rangle_E + C_{D\beta} |e_\beta\rangle_E, \quad (40)$$

with $C_{I\beta}^2 + C_{D\beta}^2 = 1$. Here, the state $|e\rangle_E$ is independent on Alice and Bob's choice while $|e_\beta\rangle_E$ is not. Then Equations (4) and (20) can be expressed as

$$\begin{aligned} |\Phi_\beta\rangle_{CE} &= \cos\theta_\beta C_{I\beta} |\omega_\beta\rangle_{HC} |e\rangle_E + \cos\theta_\beta C_{D\beta} |\omega_\beta\rangle_{HC} |e_\beta\rangle_E \\ &\quad + \sin\theta_\beta |\omega_\beta^\perp\rangle_{VC} \otimes (C_{I\beta} |e\rangle_E + C_{D\beta} |e_\beta\rangle_E), \end{aligned} \quad (41)$$

where the first item corresponds to $a_\beta|\varphi_\beta\rangle_{CE}$ while others correspond to $b_\beta|\varphi_\beta^\perp\rangle_{CE}$. If we regard the states $|\zeta_\beta\rangle_E$ as a coherent state with intensity ν_β , we have $|e\rangle_E = |0\rangle$ with $C_{I\beta} = e^{-\nu_\beta/2}$. The effects of the actual systems on the parameters θ_β and ν_β may be complicated, which makes it difficult to be characterized. Fortunately, the GLT method can be applied provided the upper bounds of θ_β and ν_β denoted as $\theta = \max_\beta\{\theta_\beta\}$ and $\nu = \max_\beta\{\nu_\beta\}$. Therefore, we consider the parameters θ and ν as the upper bounds of side channels for both signal and decoy states in the simulation. In this way, we can simplify the numerical simulation with only two parameters θ and ν but not six parameters θ_β and ν_β ($\beta \in \{z, a, b\}$). In practical QKD systems, the parameters θ can be characterized using quantum state tomography [40], and the parameters ν can be characterized by monitoring the intensity of the trojan light before fixed attenuation or analyzing its possible maximum according to the isolation of reverse and forward.

We simulate the observed values with the experimental parameters about the actual devices in Table 1, and the parameters about the intensities and probabilities in different windows in Table 2 [26].

We mainly analyze its performance to surpass PLOB bound [9] under these experimental parameters with flawed and leaky sources. In Figures 1 and 2, we analyze the effects of these two kinds of side channels separately. In Figure 1, the SKR can beat the PLOB bound when θ increases to 5×10^{-6} but cannot when 10^{-5} . In Figure 2, the SKR can beat the PLOB bound when ν increases to 10^{-11} but cannot when 10^{-10} . Combining these two values, i.e., $\theta = 5 \times 10^{-6}$ and $\nu = 10^{-11}$, we can see that the SKR still can surpass the PLOB bound at 296 to 340 km in Figure 3. When $\theta = 10^{-8}$ and $\nu = 10^{-16}$, the SKR overlaps with that when $\theta = 0$ and $\nu = 0$, which means that the side channels will not affect the SKR at this time. We can see that the SKR is hardly affected by the side channels at a short distance, i.e., the lines overlap nearly before 200 km in Figures 1–3. Also, we note that the SKR estimated with the method in this paper when without side channels is lower than that of [11,17,22] by comparing the dashed line with the solid line when $\theta = 0$ and $\nu = 0$ in Figure 3. Therefore, we could choose the original method [11,17,22] when without side channels and choose the method in this paper when with side channels.

Figure 1. Secret key rate (per pulse) in logarithmic scale versus transmission distance between Alice and Bob when only one kind of side channel is considered. The dashed line corresponds to the ideal case without side channels that is estimated with the method in [11,17,22]. In addition, the dotted line is the PLOB bound. The solid lines correspond to the cases with different θ when $\nu = 0$ estimated with the method in this paper. The lines correspond to $\theta = 0$ and 10^{-8} are superimposed, which means that it will not affect SKR when θ is less than 10^{-8} . It can beat the PLOB bound when θ increases to 5×10^{-6} .

Figure 2. Secret key rate (per pulse) in logarithmic scale versus transmission distance between Alice and Bob when only one kind of side channel is considered. The dashed line corresponds to the ideal case without side channels that is estimated with the method in [11,17,22]. In addition, the dotted line is the PLOB bound. The solid lines correspond to the cases with different ν when $\theta = 0$ estimated with the method in this paper. The solid lines correspond to $\nu = 0$ and 10^{-16} are superimposed, which means that it will not affect SKR when ν is less than 10^{-16} . It can surpass the PLOB bound when increasing ν to around 10^{-11} .

Figure 3. Secret key rate (per pulse) in logarithmic scale versus transmission distance between Alice and Bob with both side channels θ and ν . The dashed line corresponds to the ideal case without side channels that is estimated with the method in [11,17,22]. In addition, the dotted line is the PLOB bound. The SKR when $\theta = 0$ and $\nu = 0$ overlaps with that when $\theta = 10^{-8}$ and $\nu = 10^{-16}$. The SKR when $\theta = 10^{-8}$, $\nu = 10^{-13}$ and $\theta = 10^{-7}$, $\nu = 10^{-13}$ are superimposed. In addition, the SKR with $\theta = 10^{-6}$ and $\nu = 10^{-11}$ surpass the PLOB bound at 296 to 340 km.

Table 1. List of experimental parameters about the active devices. 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, and p_d is the dark count rate.

γ	η_d	e_d	f_{EC}	p_d
0.2	56%	3%	1.1	10^{-8}

Table 2. List of experimental parameters about intensities and probabilities in different windows that Alice and Bob select. M is the number of phase slices [26].

μ_a	μ_b	μ_z	p_z	p_a	p_b	p_{z0}	M
0.1	0.384	0.447	0.776	0.85	0.073	0.732	16

6. Conclusions

In this paper, we take into account the imperfections at the light source and enhance the practical implementation of the SNS protocol. We analyze that the flaws of phase modulation can be overcome by regarding the deviation of the phase as phase noise and eliminating it with the method of the post-selection of phase. To overcome the side channels that may arise from THAs or device imperfections, we modify the GLT method [42] to the SNS protocol. Remarkably, we decompose the two-mode single-photon states into two special parts which are not the Pauli operators to reduce the number of parameters that need to be solved. To make it more practical, we analyze how to apply this method with the four-intensity decoy-state method. In this way, the practical implementations of the SNS protocol can be guaranteed without a detailed characterization of the side channels. Last, we note that the pulse correlations are not considered in this paper, which may be solved with the method in [28,33,34,36,50]. In conclusion, our results might constitute a crucial step towards guaranteeing the practical implementations of the SNS protocol with flawed and leaky sources.

Author Contributions: Conceptualization, Y.W. and Y.-F.L.; methodology, Y.-F.L., Y.W. and X.-X.Z.; writing—original draft preparation, Y.-F.L.; writing—review and editing, M.-S.J., F.L., H.-W.L., C.Z., 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. Virtual Protocol

In this section, we introduce the virtual protocol based on [11]. Suppose Alice and Bob preshare the classical information for different windows and the specific intensities in X windows so there are no mismatching windows, e.g., the time window when one commits to the signal window but the other commits to the decoy window, or when they choose different intensities when both decide the decoy window. Equivalently, we could assume Alice and Bob are sitting in the same lab so they can agree on the windows and intensities. This restriction can be released since these windows are a subset of the actual protocol [11].

In Z windows, they prepare the following states

$$|\Psi_z^q\rangle_{CEC'E'AB} = \frac{1}{\sqrt{2}}[|0\Phi_z\rangle_{CEC'E'} \otimes |01\rangle_{AB} + (-1)^q |\Phi_z 0\rangle_{CEC'E'} \otimes |10\rangle_{AB}], \quad (A1)$$

where $q \in \{0, 1\}$. Here, systems A and B are Alice and Bob's ancillary system, respectively. Alice (Bob) can measure the ancillary state in the basis $\{|0\rangle, |1\rangle\}$ and puts down bit 1 (0) and 0 (1) when obtaining state $|1\rangle$ and $|0\rangle$. In X_α ($\alpha \in \{a, b\}$) windows, they prepare the state

$$|\Psi_\alpha^{(\theta_A, \theta_B)}\rangle_{CEC'E'AB} = \frac{1}{\sqrt{2}}[e^{i\theta_B} |0\Phi_\alpha\rangle_{CEC'E'} \otimes |01\rangle_{AB} + e^{i\theta_A} |\Phi_\alpha 0\rangle_{CEC'E'} \otimes |10\rangle_{AB}], \quad (A2)$$

with phases θ_A and θ_B obeying uniform distribution in $[0, 2\pi)$. The states sent in systems C and C' may be mixed due to the imperfections of their devices which could include a potential entanglement between their devices and Eve's systems. Therefore, the mixed states in system C (C') in a single-mode qubit space can be purified by introducing Alice and Eve' (Bob and Eve') ancillary systems. Here, we assume that the mixed can be purified only by Eve's ancillary systems E and E' for simplicity so that the formulas in Equations (A1) and (A2) could include mixed states in single-mode qubit space. Please note that this assumption is conservative since the purification is controlled by Eve completely. We note that it would not affect the security if we abandon this assumption.

Rewrite the state in Equation (A1) in the X basis of the systems A and B as

$$\begin{aligned} |\Psi_z^q\rangle_{CEC'E'AB} = & \frac{1}{\sqrt{2}} |\varphi_{even}^{z,q,vir}\rangle_{CEC'E'} \frac{|0_x 0_x\rangle_{AB} - |1_x 1_x\rangle_{AB}}{\sqrt{2}} \\ & + \frac{1}{\sqrt{2}} |\varphi_{odd}^{z,q,vir}\rangle_{CEC'E'} \frac{|1_x 0_x\rangle_{AB} - |0_x 1_x\rangle_{AB}}{\sqrt{2}}, \end{aligned} \quad (A3)$$

where the normalized states

$$\begin{aligned} |\varphi_{even}^{z,q,vir}\rangle_{CEC'E'} &= \frac{1}{\sqrt{2}} [|0\Phi_\alpha\rangle_{CEC'E'} + (-1)^q |\Phi_\alpha 0\rangle_{CEC'E'}], \\ |\varphi_{odd}^{z,q,vir}\rangle_{CEC'E'} &= \frac{1}{\sqrt{2}} [|0\Phi_\alpha\rangle_{CEC'E'} - (-1)^q |\Phi_\alpha 0\rangle_{CEC'E'}]. \end{aligned} \quad (A4)$$

To obtain the phase error rate, Alice and Bob could measure the states in Equation (A2) of systems A and B in the X basis and then sift the results with phase satisfying Equations (1) and (2). Rewrite the state in Equation (A2) in the X basis of the systems A and B as

$$\begin{aligned} |\Psi_\alpha^{(\theta_A, \theta_B)}\rangle_{CEC'E'AB} = & \frac{1}{\sqrt{2}} |\varphi_{even}^{\alpha, (\theta_A, \theta_B), vir}\rangle_{CEC'E'} \frac{|0_x 0_x\rangle_{AB} - |1_x 1_x\rangle_{AB}}{\sqrt{2}} \\ & + \frac{1}{\sqrt{2}} |\varphi_{odd}^{\alpha, (\theta_A, \theta_B), vir}\rangle_{CEC'E'} \frac{|1_x 0_x\rangle_{AB} - |0_x 1_x\rangle_{AB}}{\sqrt{2}}, \end{aligned} \quad (A5)$$

where the normalized states

$$\begin{aligned} |\varphi_{even}^{\alpha, (\theta_A, \theta_B), vir}\rangle_{CEC'E'} &= \frac{1}{\sqrt{2}} [e^{i\theta_B} |0\Phi_\alpha\rangle_{CEC'E'} + e^{i\theta_A} |\Phi_\alpha 0\rangle_{CEC'E'}], \\ |\varphi_{odd}^{\alpha, (\theta_A, \theta_B), vir}\rangle_{CEC'E'} &= \frac{1}{\sqrt{2}} [e^{i\theta_B} |0\Phi_\alpha\rangle_{CEC'E'} - e^{i\theta_A} |\Phi_\alpha 0\rangle_{CEC'E'}]. \end{aligned} \quad (A6)$$

In the virtual protocol, Alice and Bob send the virtual states $|\varphi_{even}^{\alpha, (\theta_A, \theta_B), vir}\rangle_{CEC'E'}$, $|\varphi_{odd}^{\alpha, (\theta_A, \theta_B), vir}\rangle_{CEC'E'}$ ($\alpha \in \{a, b\}$), $|\Psi_z^q\rangle_{CEC'E'AB}$, $|\varphi_{odd}^{z,q,vir}\rangle_{CEC'E'}$, and the actual state $|00\rangle_{CEC'E'}$, where $|00\rangle_{CEC'E'}$ is the states in X window which are used to estimate Y_0 . Then by intro-

ducing the shield system S_A and S_B , the selection of these actual and virtual states can be shown as

$$|\varphi\rangle_{S_AS_BCEC'E'} = \sum_{l=1}^{13} \sqrt{P(l)} |l_A\rangle_{S_A} |l_B\rangle_{S_B} |\vartheta_l\rangle_{CEC'E'}, \quad (\text{A7})$$

where

$$\begin{aligned} |\vartheta_1\rangle_{CEC'E'} &= |\vartheta_2\rangle_{CEC'E'} = |\varphi_{\text{even}}^{a,(\theta_A,\theta_B),\text{vir}}\rangle_{CEC'E'}, \\ |\vartheta_3\rangle_{CEC'E'} &= |\vartheta_4\rangle_{CEC'E'} = |\varphi_{\text{odd}}^{a,(\theta_A,\theta_B),\text{vir}}\rangle_{CEC'E'}, \\ |\vartheta_5\rangle_{CEC'E'} &= |\vartheta_6\rangle_{CEC'E'} = |\varphi_{\text{even}}^{b,(\theta_A,\theta_B),\text{vir}}\rangle_{CEC'E'}, \\ |\vartheta_7\rangle_{CEC'E'} &= |\vartheta_8\rangle_{CEC'E'} = |\varphi_{\text{odd}}^{b,(\theta_A,\theta_B),\text{vir}}\rangle_{CEC'E'}, \\ |\vartheta_9\rangle_{CEC'E'} &= |\vartheta_{10}\rangle_{CEC'E'} = |\varphi_{\text{even}}^{z,q,\text{vir}}\rangle_{CEC'E'}, \\ |\vartheta_{11}\rangle_{CEC'E'} &= |\vartheta_{12}\rangle_{CEC'E'} = |\varphi_{\text{odd}}^{z,q,\text{vir}}\rangle_{CEC'E'}, \\ |\vartheta_{13}\rangle_{CEC'E'} &= |00\rangle_{CEC'E'}, \end{aligned} \quad (\text{A8})$$

with probabilities

$$\begin{aligned} P(l) &= \frac{1}{4} P_x P_a, \quad l = 1, 2, 3, 4, \\ P(l) &= \frac{1}{4} P_x P_b, \quad l = 5, 6, 7, 8, \\ P(l) &= \frac{P_z}{4}, \quad l = 9, 10, 11, 12, \\ P(13) &= P_x P_v. \end{aligned} \quad (\text{A9})$$

For $l = 1$ to 12 we list $l_A l_B$ in order in the following, which corresponds to the measurement results they will obtain in the X basis

$$\{0_x 0_x, 1_x 1_x, 1_x 0_x, 0_x 1_x, 0_x 0_x, 1_x 1_x, 1_x 0_x, 0_x 1_x, 0_x 0_x, 1_x 1_x, 1_x 0_x, 0_x 1_x\}. \quad (\text{A10})$$

Denote the measurement result as vv for $l = 13$ which corresponds to the events when both send $|0\rangle$ in decoy windows.

Here, as we do not consider the mismatching windows, we set

$$\begin{aligned} P_x &= \frac{p_x^2}{p_x^2 + p_z^2}, \\ P_z &= \frac{p_z^2}{p_x^2 + p_z^2}, \\ P_a &= \frac{p_a^2}{p_a^2 + p_b^2 + p_v^2}, \\ P_b &= \frac{p_b^2}{p_a^2 + p_b^2 + p_v^2}, \\ P_v &= \frac{p_v^2}{p_a^2 + p_b^2 + p_v^2}. \end{aligned} \quad (\text{A11})$$

In the following, we introduce the virtual protocol.

(1) State preparation. Alice and Bob prepare systems S (i.e., $S_A S_B$), CE and $C'E'$ in Equation (A7), and then send the systems CE and $C'E'$ to Charlie. They repeat this step N times.

(2) Interferometric measurement. Charlie does the same as Step 2 in the actual protocol in Section 2.

(3) Sifting and measurement. They announce their phases in X_α windows and sift the effective events as defined in the actual protocol but with two different phase slices, Δ denoted as Δ_1 and Δ_2 . Then they measure their shield system S_A and S_B and obtain l for those effective events, and measure the systems A and B in X (Z) when $l = 1$ to 12 ($l = 13$).

(4) Announcement. They announce their measurement results when $l = 1$ to 8 which are used to estimate the phase error rate with Charlie's measurement results.

Appendix B. Security Proof Against Coherent Attacks

In coherent attacks, Eve is allowed to interact with all states and then perform a joint measurement. For this, we could use Azuma's inequality [42,51] to derive a relation between the expected and observed values which can include the dependencies.

Consider all the states Alice and Bob prepare in the whole process as

$$|\tau\rangle_{SCEC'E'} = |\varphi_{k-1}\rangle_{SCEC'E'} |\varphi_k\rangle_{SCEC'E'} |\varphi_r\rangle_{SCEC'E'}, \quad (A12)$$

where $|\varphi_{k-1}\rangle_{SCEC'E'}$, $|\varphi_k\rangle_{SCEC'E'}$ and $|\varphi_r\rangle_{SCEC'E'}$ correspond to all the states before the k th runs, in the k th run and in the rest of the all runs, respectively. The system S represents the systems S_A and S_B . Suppose Eve's operation on all systems as

$$\hat{U}_{CEC'E'E''} |\tau\rangle_{SCEC'E'} \otimes |0\rangle_{E''} = \sum_t \hat{B}_{tCEC'E'} |\tau\rangle_{SCEC'E'} |t\rangle_{E''}, \quad (A13)$$

where $\hat{U}_{CEC'E'E''}$ is a unitary transformation on systems $CEC'E'E''$, and $\hat{B}_{tCEC'E'}$ is the Kraus operator acting on systems $CEC'E'$ depending on Eve's measurement result t , and $\{|t\rangle\}$ is an orthonormal basis. Here, system E'' is an ancillary system Eve prepares to operate and measure so as to obtain information. Let the joint operator

$$\hat{O}_{k-1, SCEC'E'} = \bigotimes_{v=1}^{k-1} \hat{M}_{S_v CEC'E'_v}, \quad (A14)$$

where $\hat{M}_{S_v CEC'E'_v}$ denotes the Kraus operator corresponds to the v th measurement results of the Alice, Bob and Charlie. Therefore, the normalized state of the k th systems $SCEC'E'$ conditioned on the measurement results $\hat{O}_{k-1}$ of the first $k-1$ systems can be shown as

$$\hat{\rho}_{k|O_{k-1}}^{SCEC'E'} = \frac{\hat{\sigma}_{k|O_{k-1}}^{SCEC'E'}}{\text{Tr}(\hat{\sigma}_{k|O_{k-1}}^{SCEC'E'})}, \quad (A15)$$

where

$$\hat{\sigma}_{k|O_{k-1}}^{SCEC'E'} = \sum_t \sum_{\vec{x}_{k-1}, \vec{x}_r} A_{t, CEC'E'|k-1}^{(\vec{x}_{k-1}, \vec{x}_r)} |\varphi_k\rangle_{SCEC'E'} \langle \varphi_k| A_{t, CEC'E'|k-1}^{\dagger(\vec{x}_{k-1}, \vec{x}_r)} \quad (A16)$$

with

$$A_{t, CEC'E'|k-1}^{(\vec{x}_{k-1}, \vec{x}_r)} = \langle \vec{x}_r | \langle \vec{x}_{k-1} | \hat{O}_{k-1, SCEC'E'} \hat{B}_{tCEC'E'} |\varphi_{k-1}, \varphi_r\rangle_{SCEC'E'}, \quad (A17)$$

and the basis $\{|\vec{x}_{k-1}\rangle, |\vec{x}_r\rangle\}$, where $|\vec{x}_{k-1}\rangle$ corresponds to all the systems in the first $k-1$ runs and $|\vec{x}_r\rangle$ corresponds to the rest of the systems after k th run. Then by substituting Equation (A17) into Equation (A16), we obtain

$$\begin{aligned} \hat{\sigma}_{k|O_{k-1}}^{SCEC'E'} &= \sum_{l, l'} \sqrt{P(l)P(l')} \\ &\times \sum_t \sum_{\vec{x}_{k-1}, \vec{x}_r} A_{t, CEC'E'|k-1}^{(\vec{x}_{k-1}, \vec{x}_r)} |l_A l_B\rangle_S \langle l'_A l'_B| \otimes |\vartheta_l\rangle_{CEC'E'} \langle \vartheta_{l'}| A_{t, CEC'E'|k-1}^{\dagger(\vec{x}_{k-1}, \vec{x}_r)} \end{aligned} \quad (A18)$$

Hence, the probability that Alice and Bob obtain $l_A l_B$ ($l = 1$ to 8) in the X basis and only d detector clicks on Charlie's side conditional on that all the previous measurement

results and Alice and Bob's phases satisfy Equation (1) or (2) (i.e., $c = 0$ or 1) can be shown as

$$P_{l|O_{k-1}}^{(c,d),\Delta} = \frac{1}{\Delta} \int_{\pi\delta(c-1)-\Delta/2}^{\pi\delta(c-1)+\Delta/2} \frac{P(l)}{\text{Tr}(\hat{\sigma}_{k|O_{k-1}}^{SCEC'E'})} \text{Tr}(\hat{D}_{d|O_{k-1}}|\vartheta_l\rangle_{CEC'E'}\langle\vartheta_l|)d(\theta_A - \theta_B), \quad (\text{A19})$$

where

$$\hat{D}_{d|O_{k-1}} = \sum_t \sum_{\vec{x}_{k-1}, \vec{x}_r} A_{t,CEC'E'|k-1}^{+(\vec{x}_{k-1}, \vec{x}_r)} \hat{M}_d A_{t,CEC'E'|k-1}^{(\vec{x}_{k-1}, \vec{x}_r)} \quad (\text{A20})$$

represents Eve's operation and Charlie's measurement. The conditional probability $P_{l|O_{k-1}}^{(c,d),\Delta}/P(l)$ corresponds to the conditional probability in Equation (25) except that the conditions of the former probability include all previous measurement results. Please note that the parameters k_x, m_x and α are indicated by the parameter l . Similarly, we can give the conditional probability for $l = 9$ to 12 corresponds to Equation (13) as $P_{l|O_{k-1}}^{(q,d),\Delta}/P(l)$ where

$$P_{l|O_{k-1}}^{(q,d),\Delta} = \frac{P(l)}{\text{Tr}(\hat{\sigma}_{k|O_{k-1}}^{SCEC'E'})} \text{Tr}(\hat{D}_{d|O_{k-1}}|\vartheta_l\rangle_{CEC'E'}\langle\vartheta_l|), \quad (\text{A21})$$

In fact, we do not need the explicit form of $\hat{D}_{d|O_{k-1}}$ just as $\hat{D}_d$ in Section 3. With the actual yields corresponding to $Y_{k_x, m_x}^{(c,d),\alpha,\Delta}$ and the relationship between $Y_{k_x, m_x}^{(q,d),\text{vir}}$ and $Y_{k_x, m_x}^{(c,d),\alpha,\Delta}$ which is similar to that in Section 3, we can obtain the bounds of the actual yields corresponding to $Y_{k_x, m_x}^{(q,d),\text{vir}}$ by using Azuma's inequality [42,51] twice. Therefore, the phase error rate can be obtained under coherent attacks.

References

- Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [\[CrossRef\]](#)
- Wang, X.B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [\[CrossRef\]](#) [\[PubMed\]](#)
- Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [\[CrossRef\]](#)
- Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [\[CrossRef\]](#)
- Takeoka, M.; Guha, S.; Wilde, M.M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **2014**, *5*, 5235. [\[CrossRef\]](#)
- Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Wang, X.B.; Yu, Z.W.; Hu, X.L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. [\[CrossRef\]](#)
- Ma, X.; Zeng, P.; Zhou, H. Phase-Matching Quantum Key Distribution. *Phys. Rev. X* **2018**, *8*, 031043. [\[CrossRef\]](#)
- Curty, M.; Azuma, K.; Lo, H.K. Simple security proof of twin-field type quantum key distribution protocol. *NPJ Quant. Inf.* **2019**, *5*, 64. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Lin, J.; Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **2018**, *98*, 042332. [\[CrossRef\]](#)
- 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.

17. 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. [\[CrossRef\]](#)
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. Wang, X.B.; Hu, X.L.; Yu, Z.W. Practical Long-Distance Side-Channel-Free Quantum Key Distribution. *Phys. Rev. Appl.* **2019**, *12*, 054034. [\[CrossRef\]](#)
20. 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. [\[CrossRef\]](#)
21. 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. [\[CrossRef\]](#)
22. 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. [\[CrossRef\]](#)
23. 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. [\[CrossRef\]](#)
24. Lu, Y.F.; Wang, Y.; Jiang, M.S.; Liu, F.; Zhang, X.X.; Bao, W.S. Finite-key analysis of sending-or-not-sending twin-field quantum key distribution with intensity fluctuations. *Quantum Inf. Process.* **2021**, *20*, 135. [\[CrossRef\]](#)
25. 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. [\[CrossRef\]](#)
26. 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. [\[CrossRef\]](#)
27. Liu, H.; Jiang, C.; Zhu, H.T.; Zou, M.; Yu, Z.W.; Hu, X.L.; Xu, H.; Ma, S.; Han, Z.; Chen, J.P.; et al. Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km. *Phys. Rev. Lett.* **2021**, *126*, 250502. [\[CrossRef\]](#)
28. Pereira, M.; Kato, G.; Mizutani, A.; Curty, M.; Tamaki, K. Quantum key distribution with correlated sources. *Sci. Adv.* **2020**, *6*, 4487. [\[CrossRef\]](#)
29. Gottesman, D.; Lo, H.K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **2004**, *4*, 325–360.
30. Tamaki, K.; Curty, M.; Kato, G.; Lo, H.K.; Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **2014**, *90*, 052314. [\[CrossRef\]](#)
31. Mizutani, A.; Curty, M.; Lim, C.C.W.; Imoto, N.; Tamaki, K. Finite-key security analysis of quantum key distribution with imperfect light sources. *New J. Phys.* **2015**, *17*, 093011. [\[CrossRef\]](#)
32. Tamaki, K.; Curty, M.; Lucamarini, M. Decoy-state quantum key distribution with a leaky source. *New J. Phys.* **2016**, *18*, 065008. [\[CrossRef\]](#)
33. Yoshino, K.I.; Fujiwara, M.; Nakata, K.; Sumiya, T.; Sasaki, T.; Takeoka, M.; Sasaki, M.; Tajima, A.; Koashi, M.; Tomita, A. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *NPJ Quant. Inf.* **2018**, *4*, 8. [\[CrossRef\]](#)
34. Mizutani, A.; Kato, G.; Azuma, K.; Curty, M.; Ikuta, R.; Yamamoto, T.; Imoto, N.; Lo, H.K.; Tamaki, K. Quantum key distribution with setting-choice-independently correlated light sources. *NPJ Quant. Inf.* **2019**, *5*, 8. [\[CrossRef\]](#)
35. Mizutani, A.; Sasaki, T.; Takeuchi, Y.; Tamaki, K.; Koashi, M. Quantum key distribution with simply characterized light sources. *NPJ Quant. Inf.* **2019**, *5*, 87. [\[CrossRef\]](#)
36. Wang, Y.; Primaatmaja, I.W.; Lavie, E.; Varvitsiotis, A.; Lim, C.C.W. Characterising the correlations of prepare-and-measure quantum networks. *NPJ Quant. Inf.* **2019**, *5*, 17. [\[CrossRef\]](#)
37. Navarrete, Á.; Pereira, M.; Curty, M.; Tamaki, K. Practical Quantum Key Distribution That is Secure Against Side Channels. *Phys. Rev. Appl.* **2021**, *15*, 034072. [\[CrossRef\]](#)
38. Sun, S.; Xu, F. Security of quantum key distribution with source and detection imperfections. *New J. Phys.* **2021**, *23*, 023011. [\[CrossRef\]](#)
39. Xu, F.; Wei, K.; Sajeed, S.; Kaiser, S.; Sun, S.; Tang, Z.; Qian, L.; Makarov, V.; Lo, H.K. Experimental quantum key distribution with source flaws. *Phys. Rev. A* **2015**, *92*, 032305. [\[CrossRef\]](#)
40. Tang, Z.; Wei, K.; Bedroia, O.; Qian, L.; Lo, H.K. Experimental measurement-device-independent quantum key distribution with imperfect sources. *Phys. Rev. A* **2016**, *93*, 042308. [\[CrossRef\]](#)
41. Boaron, A.; Boso, G.; Rusca, D.; Vulliez, C.; Autebert, C.; Caloz, M.; Perrenoud, M.; Gras, G.; Bussieres, F.; Li, M.J.; et al. Secure Quantum Key Distribution over 421 km of Optical Fiber. *Phys. Rev. Lett.* **2018**, *121*, 190502. [\[CrossRef\]](#)
42. Pereira, M.; Curty, M.; Tamaki, K. Quantum key distribution with flawed and leaky sources. *NPJ Quant. Inf.* **2019**, *5*, 62. [\[CrossRef\]](#)
43. Tomamichel, M.; Lim, C.C.W.; Gisin, N.; Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **2012**, *3*, 634. [\[CrossRef\]](#)
44. Sun, S.H.; Gao, M.; Jiang, M.S.; Li, C.Y.; Liang, L.M. Partially random phase attack to the practical two-way quantum-key-distribution system. *Phys. Rev. A* **2012**, *85*, 032304. [\[CrossRef\]](#)
45. 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. [\[CrossRef\]](#)

-
46. 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](#)]
 47. 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](#)]
 48. 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](#)]
 49. Huang, A.; Li, R.; Egorov, V.; Tchouragoulov, S.; Kumar, K.; Makarov, V. Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution. *Phys. Rev. Appl.* **2020**, *13*, 034017. [[CrossRef](#)]
 50. Nagamatsu, Y.; Mizutani, A.; Ikuta, R.; Yamamoto, T.; Imoto, N.; Tamaki, K. Security of quantum key distribution with light sources that are not independently and identically distributed. *Phys. Rev. A* **2016**, *93*, 042325. [[CrossRef](#)]
 51. Azuma, K. Weighted sums of certain dependent random variables. *Tohoku Math. J.* **1967**, *19*, 357–367. [[CrossRef](#)]