entropy

MDPI

Article

Phase-Matching Quantum Key Distribution with Discrete Phase Randomization

Xiaoxu Zhang [1,2,3], Yang Wang [1,2,*], Musheng Jiang [1,2], Yifei Lu [1,2], Hongwei Li [1,2], Chun Zhou [1,2] and Wansu Bao [1,2]

1 Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450001, China; zxx@qiclab.cn (X.Z.); jms@qiclab.cn (M.J.); lyf@qiclab.cn (Y.L.); lhw@qiclab.cn (H.L.); zc@qiclab.cn (C.Z.); bws@qiclab.cn (W.B.)
2 Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
3 Basic Department, SSF IEU, Zhengzhou 450001, China
* Correspondence: wy@qiclab.cn

Abstract: The twin-field quantum key distribution (TF-QKD) protocol and its variations have been proposed to overcome the linear Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound. One variation called phase-matching QKD (PM-QKD) protocol employs discrete phase randomization and the phase post-compensation technique to improve the key rate quadratically. However, the discrete phase randomization opens a loophole to threaten the actual security. In this paper, we first introduce the unambiguous state discrimination (USD) measurement and the photon-number-splitting (PNS) attack against PM-QKD with imperfect phase randomization. Then, we prove the rigorous security of decoy state PM-QKD with discrete phase randomization. Simulation results show that, considering the intrinsic bit error rate and sifting factor, there is an optimal discrete phase randomization value to guarantee security and performance. Furthermore, as the number of discrete phase randomization increases, the key rate of adopting vacuum and one decoy state approaches infinite decoy states, the key rate between discrete phase randomization and continuous phase randomization is almost the same.

Keywords: twin-field quantum key distribution; phase-matching; discrete phase randomization; intrinsic bit error rate

Citation: Zhang, X.; Wang, Y.; Jiang, M.; Lu, Y.; Li, H.; Zhou, C.; Bao, W. Phase-Matching Quantum Key Distribution with Discrete Phase Randomization. *Entropy* **2021**, *23*, 508. https://doi.org/10.3390/e23050508

Academic Editor: Ivan B. Djordjevic

Received: 12 March 2021
Accepted: 21 April 2021
Published: 23 April 2021

1. Introduction

Quantum key distribution (QKD) can offer information theoretically secure means to distribute secret keys between two remote parties [1], but the performance is restricted by the fundamental rate-loss limit [2,3]. Recently, a novel twin-field QKD (TF-QKD) protocol [4] is proposed to surpass the linear Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound [2], which shows the superiority relation between key rate and channel transmittance, $R \sim O(\sqrt{\eta})$. However, the security proof is not completed in the original TF-QKD protocol [4]. In order to present a more rigorous security proof, various variations [5–10] of the original TF-QKD protocol have been proposed. The related experimental works have also been extensively studied [11–20].

All of these variant TF-QKD protocols have their own advantages. The no-phase-post-selection TF-QKD (NPP-TF-QKD) protocol [5,6] provides better key rate performance in closer-to-mid distance, but it needs phase locking and pre-phase feedback in the experiment, so it is hard to implement [5,6,21]. The sending-or-not-sending TF-QKD (SNS-TF-QKD) protocol [10] can tolerate large misalignment errors and provide better performance in long distance [10,21]. The phase-matching QKD (PM-QKD) protocol [8] has no phase locking with phase slices and employs a phase post-compensation technique, so it can be easily experimentally implemented without pre-phase feedback [13,21].

In reality, the decoy state method is adopted to ensure the security of imperfect single photon source [22–25] in the actual QKD system. An important theoretical premise and assumption of the method is that the global phase of coherent sources should be continuously randomized [26–28]. However, perfect phase randomization is very difficult to achieve. In an actual experiment, there are two means to randomize the global phase. One means is to turn the laser on and off by controlling the current, but it is not suitable for PM-QKD with the phase post-compensation technique—the reason for this is that we do not know the precise phase slices. Moreover, experiments show that residual phase correlations may exist between adjacent pulses [29]. The other one is to actively modulate the phase of coherent sources controlled by a phase modulator with a true random number generator; this method is suitable for PM-QKD, but the phase randomization is not continuous. Thus, neither of these two means satisfy the assumption of the decoy state method, which may introduce a potential loophole that threatens the security of the actual protocol [30]. Then, the unambiguous state discrimination (USD) measurement [31] and the photon-number-splitting (PNS) attack [32] can be used against the imperfect phase randomization.

An earlier security analysis of discrete phase randomization appears in the decoy state Bennet-Brassard-1984 (BB84) in Reference [33], which points out, when the number of discrete phase values is larger, that the performance of discrete phase randomization is close to that of continuous phase randomization, and the number is said to be ten [33]. Similar security analysis methods are used for several other protocols, the measurement-device-independent (MDI) QKD in Reference [34], the NPP-TF-QKD in References [35,36], the SNS-TF-QKD in Reference [37], the PM-QKD in Reference [38]. Therein, Reference [38] uses a different security poof method with Reference [8], and there is no in-depth formula derivation in the decoy state PM-QKD with discrete phase randomization. In this paper, we focus on these discrete global phase randomization issues in the PM-QKD protocol [39], study a concrete attack against PM-QKD with imperfect phase randomization, apply the decoy-state method to derive the single photon yield formula to exhibit performance of the key rate and compare the yield difference of continuous phase randomization with discrete phase randomization.

The paper is arranged as follows: in Section 2, we review the PM-QKD protocol in detail, based on the security analysis of symmetric-encoding PM-QKD, we estimate the overall phase error rate. In Section 3, we show a concrete attack against PM-QKD with imperfect phase randomization. In Section 4, we show how to apply the decoy-state method to obtain the upper bound of the phase-flip error rate with discrete phase randomization; moreover, the yield difference between continuous and discrete phase randomization is also studied in this section. The numerical simulation results are shown in Section 5, and then we conclude in Section 6.

2. The Protocol of PM-QKD

We employ the attenuated laser as a single photon source, which is regarded as the coherent state. When the coherent state is randomized by continuous phase, it is equivalent to the Fock state, with the photon number distribution as

$$P_{j|\alpha} = e^{-\alpha}\frac{\alpha^j}{j!} \tag{1}$$

In this section, we review the PM-QKD protocol, and without considering the security effects of discrete phase randomization, Equation (1) is used for formula derivation.

2.1. Protocol Description

The implementation process of the PM-QKD is similar to Reference [39].

- State preparation. In each round, the coherent state $\left|\sqrt{\alpha_A}e^{i(\pi\kappa_A+\frac{2\pi}{D}d_A)}\right\rangle$ is prepared by Alice, the intensity $\alpha_A \in \{\mu_A, \nu_A, \omega_A\}$, where μ_A is she signal state, ν_A is the decoy state, ω_A is the vacuum state, the random key bit $\kappa_A \in \{0,1\}$, the discrete

phase randomization number d_A is randomly chosen from $\{0, 1, \cdots, D-1\}$, D is the number of maximum discrete phase that is modulated by Alice, for simplicity, assume D is an even number. Similarly, Bob prepares the coherent state $\left|\sqrt{\alpha_B}e^{i(\pi\kappa_B+\frac{2\pi}{D}d_B)}\right\rangle$, therein, $\alpha_A = \alpha_B = \frac{\alpha}{2} \in \left\{\frac{\mu}{2}, \frac{\nu}{2}, \frac{\omega}{2}\right\}$.

- Measurement. Alice and Bob send their quantum states to Charlie with transmittances η_A and η_B, Charlie performs an interference measurement with a beam splitter and records which detector (L or R) clicks.
- Announcement. The detection result is announced by Charlie for each round; the intensity settings α_A, α_B and phase numbers d_A, d_B are also announced by Alice and Bob.
- Sifting. After that, the phase post-compensation method is used by Charlie to calculate and then Charlie announces the phase match pairs. Assume the phase compensation $d_\delta \in \{0, 1, \cdots D/2-1\}$, only one of the two detectors clicks is the successful detection. If the left detector clicks and $|d_A - d_B - d_\delta| \bmod D = 0$, Alice and Bob keep κ_A and κ_B as the raw key. If the right detector clicks and $|d_A - d_B - d_\delta| \bmod D = D/2$, Bob flips his key bit κ_B. If $|d_A - d_B - d_\delta| \bmod D \neq 0, D/2$, for simplicity, we discard the phase mismatch pairs.
- Parameter estimation. Alice and Bob estimate the information leakage from the raw data that they have kept.
- Key generation. After reconciling the corresponding key string to perform error correction, Alice and Bob use privacy amplification to produce the final keys.

2.2. Phase Error Estimation

The security analysis of asymptotic case is considered, so there are no statistical fluctuations. The analysis method of the phase error rate that we use comes from [39], which is an important new viewpoint of QKD security, establishing the relationship between the symmetric encoding and privacy with the standard phase-error-correction approach [40], and we summarize briefly as follows.

If the joint state ρ_{AB} is a pure of even or odd state, the symmetric encoding PM-QKD protocol is perfectly private, the phase error rate $E_{ph} = 0$, if the joint state ρ_{AB} is a mixture of even and odd state, $\rho_{AB} = P_{odd}\rho_{odd} + P_{even}\rho_{even}$, the phase error rate $E_{ph} \neq 0$, the effective detection ratios of odd and even components of signal state are estimated by [39]

$$\begin{aligned} q_{odd|\mu} &= P_{odd|\mu}\frac{Y_{odd|\mu}}{Q_\mu} \\ q_{even|\mu} &= P_{even|\mu}\frac{Y_{even|\mu}}{Q_\mu} \end{aligned} \tag{2}$$

where $Q_\mu = P_{odd|\mu}Y_{odd|\mu} + P_{even|\mu}Y_{even|\mu}$ is the total gain of mixture signal state ρ_{AB}. $Y_{odd|\mu}$ and $Y_{even|\mu}$ are the yield of odd signal state ρ_{odd} and even signal state ρ_{even}, respectively. $P_{odd|\mu}$ and $P_{odd|\mu}$ are the signal state probability of odd and even photon numbers.

The overall phase error rate comes from the even components, which is estimated by [39]

$$E_{ph} = P_{even|\mu}\frac{Y_{even|\mu}}{Q_\mu} \tag{3}$$

where $P_{even|\mu}$ is given by the above section, Q_μ is given by the experiment results, the important task is to estimate the parameter $Y_{even|\mu}$.

For simplicity, we use phase match pairs and discard phase mismatch pairs, so the upper bound of phase error rate comes from the signal state bounded by

$$E_{ph} \leq 1 - q_{1|\mu} \tag{4}$$

where $q_{1|\mu} = P_{1|\mu}\frac{Y_{1|\mu}}{Q_\mu}$.

According to the above discussion, we get the final secure key rate by

$$R_f = \frac{2}{D} Q_\mu [1 - H_2(E_{ph}) - f H_2(E_\mu)] \tag{5}$$

where Q_μ is the total gain of the signal state, E_{ph} is the phase error rate of the signal state, E_μ is the bit error rate of the signal state, f is the error correction efficiency, $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function.

3. Attack PM-QKD with Imperfect Phase Randomization

Considering the extreme case that Eve knows, the exact phases of the signal and decoy states without phase randomization, the PM-QKD protocol will have a serious security loophole. Due to the signal state and the decoy state not being orthogonal, Eve can use USD measurement to distinguish the signal state and the decoy state with the probability $q < 1$. The optimal success probability [41] of USD measurement on each side is $q_{opt} = 1 - e^{-\left|\sqrt{\mu} - \sqrt{v}\right|^2/4}$, which is obtained by performing positive operator valued measurement. After performing USD measurement, Eve measures the number of photons in the pulse and performs a PNS attack.

For the sake of simplicity, we neglect the dark count and the misalignment error, and only consider the channel loss. Without attacking, the gains of the signal state and decoy state are

$$\begin{aligned} Q_\mu &= 1 - e^{-\eta\mu} \\ Q_v &= 1 - e^{-\eta v} \end{aligned} \tag{6}$$

where η is the channel loss.

Under the PNS attack, the gains of the signal state and decoy state are

$$\begin{aligned} Q_\mu^{\text{attack}} &= \sum_{j=1}^{\infty} q_{opt}^2 Z_j^\mu e^{-\mu} \frac{\mu^j}{j!} \\ Q_v^{\text{attack}} &= \sum_{j=1}^{\infty} q_{opt}^2 Z_j^v e^{-v} \frac{v^j}{j!} \end{aligned} \tag{7}$$

where Z_j^μ and Z_j^v represent the probability that Eve forwards j photons to the signal state and the decoy state, with j as the sum of the photons on both sides.

The simplified upper key rate under the PNS attack is bounded by

$$R^u = R_{\text{PNS}} = \sum_{j=1}^{\infty} q_{opt}^2 Z_j^\mu e^{-\mu} \frac{\mu^j}{j!} [1 - H_2(E_{ph})] \tag{8}$$

The lower key rate of the simplified Equation (5) is bounded by

$$R_{\text{PM}}^l = R_{\text{PM}} = Q_\mu [1 - H_2(E_{ph})] \tag{9}$$

Combining the USD measurement with PNS attack, the security of final key rate without the phase randomized system is vulnerable. We can optimize Z_j^μ to let $R_{\text{PM}}^l > R^u$, especially for long distance communication, due to channel loss is large enough, we can block single photon and release multiple photons. Then, the key rate will be higher than the secure key rate, and information will leak out. Hence, Eve's goal is to minimize R^u.

It is worth noting that the attack scheme of USD measurement and PNS attack, which requires the quantum non-demolition measurement [42] about the photon numbers, the lossless channel and the ability of controlling detector efficiency, all of these are beyond the current technology. Ma adopts the beam splitting (BS) attack [43] in Reference [8]. We briefly present his results as follows.

Ma [8] points out, under the BS attack, that the probability of successfully distinguishing the states is $P_{\text{suc}} = 1 - e^{-(1-\eta)\mu}$. The simplified key rate of PM-QKD is lower bounded by

$$R_{\text{BS}}^{l} = Q_{\mu} e^{-2(1-\eta)\mu} \tag{10}$$

Ma [8] supposes that the photon number channel model exists in PM-QKD, then Gottesman–Lo–Lutkenhaus–Preskill (GLLP) [26] analysis can be used to obtain the formula

$$R_{\text{GLLP}} = Q_{1|\mu}[1 - H_2(E_{1|\mu}^{ph})] - Q_{\mu} f H_2(E_{\mu}) \tag{11}$$

where $Q_{1|\mu}$ is the gain of the single photon signal state, $E_{1|\mu}^{ph}$ is the phase error rate.

Due to the yield being $Y_j = 1 - (1-\eta)^j$, the simplified GLLP key rate is lower bounded by

$$R_{\text{GLLP}}^{l} = R_{\text{GLLP}} = Q_{1|\mu} = \eta\mu e^{-\mu} \tag{12}$$

Final results show that, when η is smaller than a certain value, the GLLP formula cannot hold under the BS attack, so the photon number channel model is invalid. Fortunately, the PM formula can defend against BS attack; the precondition is that the intensity must be weaker.

4. The PM-QKD with Discrete Phase Modulation of Coherent State Sources

In this section, we introduce the security analysis of discrete phase randomized PM-QKD. Then, we apply the decoy-state method to derive the single photon yield formula. Finally, we compare the yield difference between continuous phase randomization and discrete phase randomization.

4.1. Coherent State with Discrete Phase Randomization

For the coherent state with discrete phase randomization, the joint state of Alice and Bob of PM-QKD is as follows

$$|\psi\rangle_{\text{AB}} = \sum_{d_{\text{A}}=0}^{D-1} \left|\sqrt{\alpha_{\text{A}}} e^{i(\pi\kappa_{\text{A}} + \frac{2\pi}{D} d_{\text{A}})}\right\rangle_{\text{A}} \left|\sqrt{\alpha_{\text{B}}} e^{i(\pi\kappa_{\text{B}} + \frac{2\pi}{D} d_{\text{B}})}\right\rangle_{\text{B}} \tag{13}$$

where $\kappa_{\text{A}}, \kappa_{\text{B}} \in \{0, 1\}$, $|d_{\text{A}} - d_{\text{B}} - d_{\delta}| \bmod D = 0$ or $|d_{\text{A}} - d_{\text{B}} - d_{\delta}| \bmod D = D/2$.

Considering the simple case, $d_{\delta} = 0$, then $|d_{\text{A}} - d_{\text{B}}| = 0$ or $|d_{\text{A}} - d_{\text{B}}| = D/2$. Now, the density matrix can be written as

$$\begin{aligned} \rho_{\text{AB}}^{D} = & \frac{1}{D} \sum_{d_{\text{A}}=0}^{D-1} \left|\sqrt{\alpha_{\text{A}}} e^{i(\pi\kappa_{\text{A}} + \frac{2\pi}{D} d_{\text{A}})}\right\rangle_{\text{A}} \left\langle\sqrt{\alpha_{\text{A}}} e^{-i(\pi\kappa_{\text{A}} + \frac{2\pi}{D} d_{\text{A}})}\right| \\ & \otimes \left|\sqrt{\alpha_{\text{B}}} e^{i(\pi\kappa_{\text{B}} + \frac{2\pi}{D} d_{\text{B}})}\right\rangle_{\text{B}} \left\langle\sqrt{\alpha_{\text{B}}} e^{-i(\pi\kappa_{\text{B}} + \frac{2\pi}{D} d_{\text{B}})}\right| \\ = & \sum_{j=0}^{D-1} P_{j|\alpha}^{D} \left|\lambda_{j|\alpha}^{D}\right\rangle_{\text{AB}} \left\langle\lambda_{j|\alpha}^{D}\right| \end{aligned} \tag{14}$$

where $P_{j|\alpha}^{D} = \sum_{l=0}^{\infty} \frac{e^{-\alpha}\alpha^{lD+j}}{(lD+j)!}$, $\left|\lambda_{j|\alpha}^{D}\right\rangle_{\text{AB}} = \frac{e^{-\alpha/2}}{\sqrt{P_{j|\alpha}^{D}}} \sum_{l=0}^{\infty} \frac{(\sqrt{\alpha})^{lD+j}}{\sqrt{(lD+j)!}} |lD+j\rangle_{\text{AB}}$, with $|lD+j\rangle_{\text{AB}} = \frac{1}{\sqrt{2^{lD+j}(lD+j)}} (a^{\dagger} \pm b^{\dagger})^{lD+j} |00\rangle_{\text{AB}}$.

In our security analysis with discrete phase randomization, we modify the final secure key rate Equation (5) to

$$R_f = \frac{2}{D} Q_\mu [1 - H_2(E_{ph}^D) - f H_2(E_\mu)] \tag{15}$$

where the upper bound of phase error rate E_{ph}^D comes from the signal state bounded by $E_{ph}^D \leq 1 - q_{1|\mu}^D$, with $q_{1|\mu}^D = P_{1|\mu}^D \frac{Y_{1|\mu}^D}{Q_\mu}$. The bit error rate E_μ and the gain Q_μ remain the same.

4.2. The Decoy-State Method

In discrete phase randomized PM-QKD, we estimate the yield $Y_{1|\mu}^D$ of the single-photon signal state. We use the vacuum and one decoy state, which is similar to the BB84 decoy state analysis [24].

We know that, in the security proof of the decoy state method with continuous phase randomization, there is an important assumption

$$Y_{j|signal} = Y_{j|decoy} \tag{16}$$

However, it is not strict in the condition of discrete phase randomization, $Y_{j|signal}^D \neq Y_{j|decoy}^D$; the reason lies in

$$\left|\lambda_{j|\mu}^D\right\rangle \neq \left|\lambda_{j|v}^D\right\rangle \tag{17}$$

Consider the properties of trace distance; we need to estimate the difference of yields for different intensities as [33]

$$\left|Y_{j|\mu}^D - Y_{j|v}^D\right| = \sqrt{1 - (F_{j|\mu v}^D)^2} \tag{18}$$

where $F_{j|\mu v}^D = \sum_{l=0}^{\infty} \frac{(\mu v)^{(lD+j)/2}}{(lD+j)!} \Big/ \sqrt{\sum_{l=0}^{\infty} \frac{\mu^{lD+j}}{(lD+j)!} \sum_{l=0}^{\infty} \frac{v^{lD+j}}{(lD+j)!}}$, that is the fidelity of $\left|\lambda_{j|\mu}^D\right\rangle$ and $\left|\lambda_{j|v}^D\right\rangle$.

The estimation of the yield $Y_{1|\mu}^D$ is similar to continuous phase randomization. The equation can be written as

$$\begin{aligned} Q_\mu &= \sum_{j=0}^{D-1} P_{j|\mu}^D Y_{j|\mu}^D \\ Q_v &= \sum_{j=0}^{D-1} P_{j|v}^D Y_{j|v}^D = \sum_{j=0}^{N-1} P_{j|v}^D Y_{j|\mu}^D + \sum_{j=0}^{D-1} P_{j|v}^D (Y_{j|v}^D - Y_{j|\mu}^D) \end{aligned} \tag{19}$$

We have

$$\begin{aligned} Y_{1|\mu}^D =& [P_{2|\mu}^D Q_v - P_{2|v}^D Q_\mu - (P_{2|\mu}^D P_{0|v}^D - P_{0|\mu}^D P_{2|v}^D) Y_{0|\mu}^D \\ & - P_{2|\mu}^D \sum_{j=0}^{D-1} P_{j|v}^D (Y_{j|v}^D - Y_{j|\mu}^D) - \sum_{j\geq 3}^{\infty} (P_{2|\mu}^D P_{j|v}^D - P_{j|\mu}^D P_{2|v}^D) Y_{j|\mu}^D] \\ & / (P_{2|\mu}^D P_{1|v}^D - P_{1|\mu}^D P_{2|v}^D) \end{aligned} \tag{20}$$

with $\sum_{j\geq 3}^{\infty} (P_{2|\mu}^D P_{j|v}^D - P_{j|\mu}^D P_{2|v}^D) Y_{j|\mu}^D \leq 0$, $Y_{0|\mu}^D \leq Q_\omega / P_{0|\omega}^D + \sqrt{1 - (F_{0|\mu\omega}^D)^2}$ and $\sum_{j=0}^{D-1} P_{j|v}^D (Y_{j|v}^D - Y_{j|\mu}^D) = \sum_{j=0}^{D-1} P_{j|\mu}^D \sqrt{1 - F_{j|\mu v}^{D\ 2}}$.

Then

$$Y_{1|\mu}^{D} \geq \frac{P_{2|\mu}^{D} Q_v - P_{2|v}^{D} Q_\mu - (P_{2|\mu}^{D} P_{0|v}^{D} - P_{0|\mu}^{D} P_{2|v}^{D}) Y_{0|\mu}^{D} - P_{2|\mu}^{D} \sum_{j=0}^{D-1} P_{j|\mu}^{D} \sqrt{1 - {F_{j|\mu\nu}^{D}}^2}}{P_{2|\mu}^{D} P_{1|v}^{D} - P_{1|\mu}^{D} P_{2|v}^{D}} \tag{21}$$

4.3. The Yield Difference between Continuous and Discrete Phase Randomization

To compare the yield difference of continuous phase randomization and discrete phase randomization, the density matrix of the continuous phase randomization can be written as

$$\begin{aligned} \rho_{\mathrm{AB}} = & \frac{1}{2\pi} \int_0^{2\pi} \left| \sqrt{\alpha_{\mathrm{A}}} e^{i(\pi\kappa_{\mathrm{A}} + \varphi_{\mathrm{A}})} \right\rangle_{\mathrm{A}} \left\langle \sqrt{\alpha_{\mathrm{A}}} e^{-i(\pi\kappa_{\mathrm{A}} + \varphi_{\mathrm{A}})} \right| \\ & \otimes \left| \sqrt{\alpha_{\mathrm{B}}} e^{i(\pi\kappa_{\mathrm{B}} + \varphi_{\mathrm{B}})} \right\rangle_{\mathrm{B}} \left\langle \sqrt{\alpha_{\mathrm{B}}} e^{-i(\pi\kappa_{\mathrm{B}} + \varphi_{\mathrm{B}})} \right| \\ = & \sum_{j=0}^{\infty} P_{j|\alpha} |j\rangle_{\mathrm{AB}} \langle j| \end{aligned} \tag{22}$$

where the general Poisson distribution $P_{j|\alpha}$ is given by Equation (1), with $|j\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2^j j!}} (a^\dagger \pm b^\dagger)^j |00\rangle_{\mathrm{AB}}$.

In the ideal case, $D \to \infty$, the fidelity $F_{j|\alpha}^{C,D}$ between $|j\rangle_{\mathrm{AB}}$ and $\left|\lambda_{j|\alpha}^{D}\right\rangle_{\mathrm{AB}}$ should be the same. In the security analysis, the fidelity $F_{j|\alpha}^{C,D}$ between $|j\rangle_{\mathrm{AB}}$ and $\left|\lambda_{j|\alpha}^{D}\right\rangle_{\mathrm{AB}}$ is bounded by

$$\begin{aligned} F_{j|\alpha}^{C,D} &= F\left(|j\rangle_{\mathrm{AB}}, \left|\lambda_{j|\alpha}^{D}\right\rangle_{\mathrm{AB}}\right) = \frac{\left|\left\langle j \mid \lambda_{j|\alpha}^{D} \right\rangle_{\mathrm{AB}}\right|}{\sqrt{\langle j \mid j\rangle_{\mathrm{AB}} \left\langle \lambda_{j|\alpha}^{D} \mid \lambda_{j|\alpha}^{D} \right\rangle_{\mathrm{AB}}}} \\ &= 1 \Big/ \frac{e^{-\alpha/2}}{\sqrt{P_{j|\alpha}^{D}}} \sum_{l=0}^{\infty} \frac{\left(\sqrt{\alpha}\right)^{lD+j}}{\sqrt{(lD+j)!}} \end{aligned} \tag{23}$$

which is related to the intensity α, photon number j and discrete phase numbers D.

Therefore, the yield difference is bounded by

$$\left|Y_{j|\alpha} - Y_{j|\alpha}^{D}\right| \leq \sqrt{1 - F_{j|\alpha}^{C,D}} = \sqrt{1 - 1 \Big/ \frac{e^{-\alpha/2}}{\sqrt{P_{j|\alpha}^{D}}} \sum_{l=0}^{\infty} \frac{\left(\sqrt{\alpha}\right)^{lD+j}}{\sqrt{(lD+j)!}}} \tag{24}$$

5. Numerical Results

Let's suppose the transmittances between Alice/Bob and Charlie are $\eta_{\mathrm{A}} = \eta_{\mathrm{B}} = \eta_f$, the detection efficiency of detectors is η_d, after the channel and detection losses, $\eta = \eta_f \eta_d$, the detection click probabilities are given by

$$\begin{aligned} P_\alpha(\bar{L}) &= (1 - p_d) e^{-\eta\alpha \cos^2 \frac{\phi_{\mathrm{AB}}}{2}} \\ P_\alpha(L) &= 1 - P_\alpha(\bar{L}) \\ P_\alpha(\bar{R}) &= (1 - p_d) e^{-\eta\alpha \sin^2 \frac{\phi_{\mathrm{AB}}}{2}} \\ P_\alpha(R) &= 1 - P_\alpha(\bar{R}) \end{aligned} \tag{25}$$

where $P_\alpha(L)/P_\alpha(R)$ and $P_\alpha(\bar{L})/P_\alpha(\bar{R})$ are the detection click probabilities of the L/R click and no L/R click, ϕ_{AB} is the phase mismatch between Alice and Bob.

Due to the discrete phase randomization, we can obtain D phase slices. Although we keep the phase match pairs and discard all of the others, there is still an intrinsic bit error rate [4], $E_D = \frac{D}{2\pi} \int_0^{2\pi/D} \sin^2 \frac{\phi_{\mathrm{AB}}}{2} d\phi_{\mathrm{AB}}$. Significantly, this is very different from BB84

protocol with the global phase mismatch value $\phi_{\mathrm{AB}} = 0$. When we use discrete phase randomization, we must consider the intrinsic bit error rate, which will deeply affect the bit error rate and phase error rate.

The error gain can be given by

$$\begin{aligned} Q_{\alpha}^{E} &= \frac{D}{2\pi} \int_{0}^{\frac{2\pi}{D}} P_{\alpha}(R) P_{\alpha}(\bar{L}) d\phi_{\mathrm{AB}} \\ &= \frac{D}{2\pi} \int_{0}^{\frac{2\pi}{D}} (1-p_d) e^{-\eta\alpha \cos^2 \frac{\phi_{\mathrm{AB}}}{2}} d\phi_{\mathrm{AB}} - (1-p_d)^2 e^{-\eta\alpha} \end{aligned} \tag{26}$$

We can derive the total gain Q_{α} as

$$\begin{aligned} Q_{\alpha} &= \frac{D}{2\pi} \int_{0}^{\frac{2\pi}{D}} [P_{\alpha}(L) P_{\alpha}(\bar{R}) + P_{\alpha}(R) P_{\alpha}(\bar{L})] d\phi_{\mathrm{AB}} \\ &= \frac{D}{2\pi} \int_{0}^{\frac{2\pi}{D}} (1-p_d) e^{-\eta\alpha \sin^2 \frac{\phi_{\mathrm{AB}}}{2}} d\phi_{\mathrm{AB}} - (1-p_d)^2 e^{-\eta\alpha} + Q_{\alpha}^{E} \end{aligned} \tag{27}$$

The bit error rate of signal states is given by

$$E_{\mu} = \frac{Q_{\mu}^{E}(1-2e_{opt}) + e_{opt} Q_{\mu}}{Q_{\mu}} \tag{28}$$

The simulate parameters are listed in Table 1.

Table 1. List of parameters used in numerical simulations. Here p_d is the dark counts rate; e_{opt} is the misalignment error probability of the system; η_d is the detection efficiency; f is the error correction efficiency; η_f is the transmission fiber loss coefficient (dB/km).

p_d	e_{opt}	η_d	f	η_f
1×10^{-8}	1.5%	0.2	1.1	0.2

In the key rate versus the transmission distance of the finite decoy states PM protocol with a different number of phase values, as shown in Figure 1, the PLOB bound is plotted for comparison. The smaller D, the lower the key rate; the reason is that the smaller the D, the larger the intrinsic bit error rate. $D = 8$ can break the PLOB bound, and meanwhile, we can find that there is an optimal $D = 10$, which can guarantee better performance. With the increase of D, the key rate will become lower due to the sifting factor $2/D$. Hence, in an actual experiment of PM-QKD, we must find the suitable discrete phases value to guarantee security and performance. When $D \to \infty$, the key rate will tend to 0; we do not present it here.

Moreover, we compare the performance of PM-QKD with discrete phase randomization between infinite decoy states and vacuum and one decoy state. As depicted in Figure 2, when we adopt vacuum and one decoy state and small D, the key rate exhibits poor performance. As D increases, the key rate of adopting vacuum and one decoy state approaches infinite decoy states. Combining the conclusion of Figure 1, we find that the discrete phase $D = 10$ still maintains good security and performance when the finite decoy states are implemented.

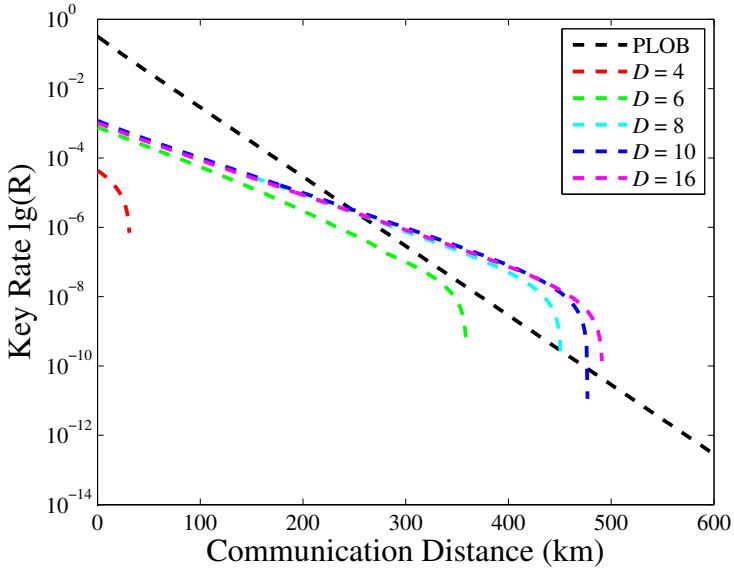


Figure 1. The key rate versus the transmission distance of the PM-QKD with different number of discrete phase values; the PLOB linear bound is plotted for comparison.

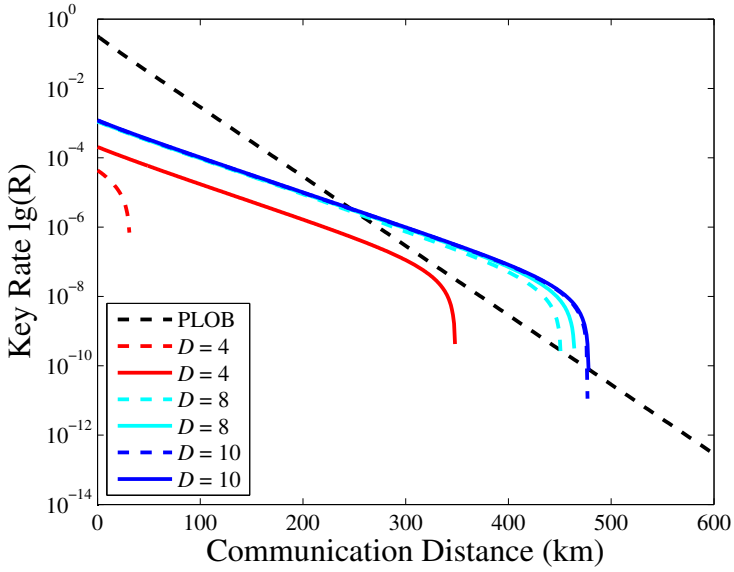
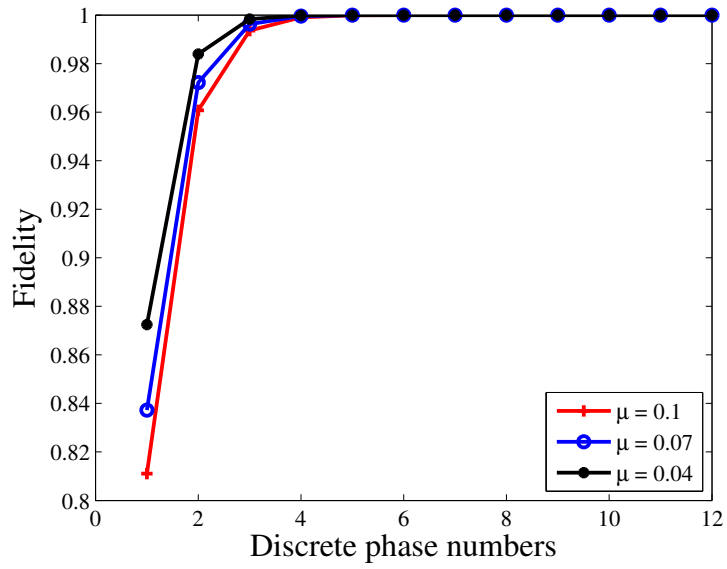


Figure 2. The key rate versus the transmission distance of the PM-QKD with different number of discrete phase values, infinite decoy states and vacuum and one decoy state are plotted for comparison. The dash line represents the case of vacuum and one decoy state; the solid line represents the case of infinite decoy states.

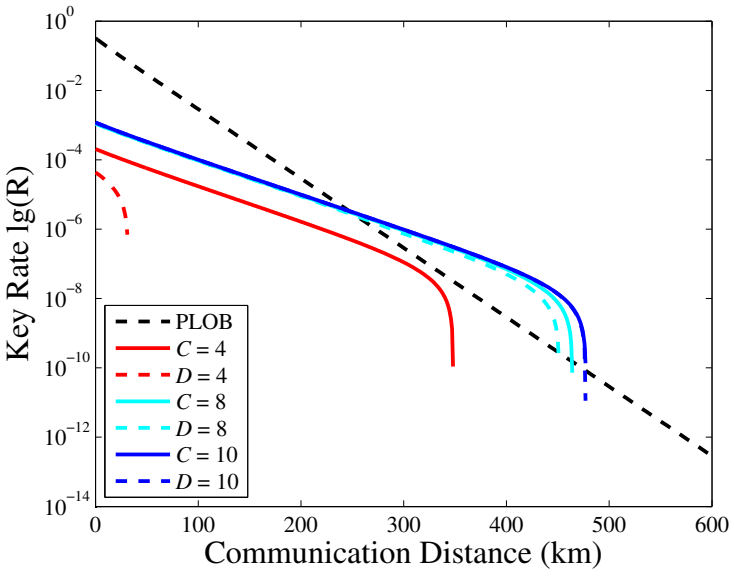
Due to there being a sifting factor $2/D$, we know that when $D \to \infty$, the key rate will tend to 0. In order to compare the key rate between continuous phase randomization and discrete phase randomization, we first compare the fidelity between $|j\rangle_{\mathrm{AB}}$ and $\left|\lambda^{D}_{j|\alpha}\right\rangle_{\mathrm{AB}}$, as shown in Figure 3a. The fidelity varies slightly with the intensity. With the increase of D, the fidelity gradually approaches 1. Therefore, when D is too small, the method of continuous phase randomization is not suitable; we cannot ignore the safety effect of discrete phase randomization.

Then, considering finite decoy states, the key rate between continuous phase randomization and discrete phase randomization has been studied in Figure 3b. As D increases,

the performance of a key rate between discrete phase randomization and continuous phase randomization is almost the same. This is consistent with the conclusion in Figure 3a.



(**a**)



(**b**)

Figure 3. (**a**) The fidelity of different mean photon numbers. The fidelity refers to Equation (23), which we take $j = 1$. (**b**) The key rate versus the transmission distance of the PM-QKD with a different number of discrete phase values. The solid line represents the coherent state with continuous phase randomization; the dash line represents the coherent state with discrete phase randomization.

6. Conclusions

In this paper, we introduce the USD measurement and PNS attack against PM-QKD with imperfect phase randomization, and simultaneously, we deeply study the security of discrete phase randomization PM-QKD protocol with a decoy state in the asymptotic case. Our simulation results show that, as D increases, the key rate of adopting vacuum and one decoy state approaches infinite decoy states, and furthermore, the performance of key rate between discrete phase randomization and continuous phase randomization is almost the same. We also find that due to the intrinsic bit error rate and sifting factor, there

is an optimal discrete phase randomization value to guarantee security and performance. Therefore, for the actual PM-QKD system, we should better adopt the suitable discrete phase randomization value to apply.

Author Contributions: X.Z. carried out numerical simulation and wrote the paper; Y.W. and W.B. assisted in discussing the research topic; M.J. contributed to attack; X.Z. and Y.L. derived the formulas; H.L. and C.Z. discussed the PM-QKD protocol. All authors participated in revising and all authors have read and agreed to the published version of the manuscript.

Funding: This work is sponsored by National Key Research and Development Program of China (Grant No. 2020YFA0309702), National Natural Science Foundation of China (Grants No. 61605248, No. 61675235 and No. 61505261) and Natural Science Foundation of Henan (Grant No. 202300410534 and No. 202300410532).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available within the article.

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

References

1. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
2. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef]
3. Takeoka, M.; Guha, S.; Wilde, M.M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **2014**, *5*, 5235. [CrossRef] [PubMed]
4. 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] [PubMed]
5. 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]
6. Curty, M.; Azuma, K.; Lo, H.K. Simple security proof of twin-field type quantum key distribution protocol. *NPJ Quantum Inf.* **2019**, *5*, 64. [CrossRef]
7. Lin, J.; Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **2018**, *98*, 042332. [CrossRef]
8. Ma, X.; Zeng, P.; Zhou, H. Phase-Matching Quantum Key Distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
9. Tamaki, K.; Lo, H.K.; Wang, W.; Lucamarini, M. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. *arXiv* **2018**, arXiv:1805.05511v3.
10. 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]
11. Clivati, C.; Meda, A.; Donadello, S.; Virzì, S.; Genovese, M.; Levi, F.; Mura, A.; Pittaluga, M.; Yuan, Z.L.; Shields, A.J.; et al. Coherent phase transfer for real-world twin-field quantum key distribution. *arXiv* **2020**, arXiv:2012.15199v1.
12. 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]
13. 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. Photonics* **2020**, *14*, 422–425. [CrossRef]
14. 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. *arXiv* **2021**, arXiv:2101.00276v1.
15. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.; 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. *Res. Sq.* **2021**. [CrossRef]
16. 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]
17. 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. Photonics* **2019**, *13*, 334–338. [CrossRef]
18. 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]
19. 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]

20. Zhong, X.; Wang, W.; Qian, L.; Lo, H.K. Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses. *NPJ Quantum Inf.* **2021**, *7*, 8. [CrossRef]
21. Mao, Y.; Zeng, P.; Chen, T. Recent Advances on Quantum Key Distribution Overcoming the Linear Secret Key Capacity Bound. *Adv. Quantum Technol.* **2021**, *4*, 2000084. [CrossRef]
22. Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef] [PubMed]
23. Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef] [PubMed]
24. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 1–127. [CrossRef]
25. Wang, X.B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef] [PubMed]
26. Gottesman, D.; Hoi-Kwong, L.; Lutkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **2004**, *4*, 325–360. [CrossRef]
27. van Enk, S.J.; Fuchs, C.A. Quantum State of an Ideal Propagating Laser Field. *Phys. Rev. Lett.* **2001**, *88*, 027902. [CrossRef] [PubMed]
28. Lo, H.K.; Preskill, J. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quantum Inf. Comput.* **2006**, *7*, 431–458.
29. Xu, F.; Qi, B.; Ma, X.; Xu, H.; Zheng, H.; Lo, H.K. Ultrafast quantum random number generation based on quantum phase fluctuations. *Opt. Express* **2012**, *20*, 12366–12377. [CrossRef]
30. Inamori, H.; Lütkenhaus, N.; Mayers, D. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D* **2007**, *41*, 599–627. [CrossRef]
31. Dušek, M.; Jahma, M.; Lütkenhaus, N. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Phys. Rev. A* **2000**, *62*, 022306. [CrossRef]
32. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330–1333. [CrossRef]
33. Cao, Z.; Zhang, Z.; Lo, H.K.; Ma, X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New J. Phys.* **2015**, *17*, 053014. [CrossRef]
34. Cao, Z. Discrete-phase-randomized measurement-device-independent quantum key distribution. *Phys. Rev. A* **2020**, *101*, 062325. [CrossRef]
35. Currás-Lorenzo, G.; Wooltorton, L.; Razavi, M. Twin-Field Quantum Key Distribution with Fully Discrete Phase Randomization. *Phys. Rev. Appl.* **2021**, *15*, 014016. [CrossRef]
36. 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]
37. Jiang, C.; Yu, Z.W.; Hu, X.L.; Wang, X.B. Sending-or-not-sending twin-field quantum key distribution with discrete-phase-randomized weak coherent states. *Phys. Rev. Res.* **2020**, *2*, 043304. [CrossRef]
38. 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]
39. 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]
40. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *New J. Phys.* **2009**, *11*, 045018. [CrossRef]
41. 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]
42. Grangier, P.; Levenson, J.A.; Poizat, J.P. Quantum non-demolition measurements in optics. *Nature* **1998**, *396*, 537–542. [CrossRef]
43. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]