entropy

IMPACT FACTOR 2.738

Indexed in: PubMed

Article

Finite-Key Analysis for Quantum Key Distribution with Discrete-Phase Randomization

Rui-Qiang Wang, Zhen-Qiang Yin, Xiao-Hang Jin, Rong Wang, Shuang Wang, Wei Chen, Guang-Can Guo and Zheng-Fu Han

Special Issue

Advanced Technology in Quantum Cryptography

Edited by

Prof. Dr. Qin Wang, Dr. Hong-Wei Li, Dr. Jin Dong Wang and Dr. Xing-Yu Zhou

MDPI

https://doi.org/10.3390/e25020258

entropy

MDPI

Article

Finite-Key Analysis for Quantum Key Distribution with Discrete-Phase Randomization

Rui-Qiang Wang [1,2,3,4], Zhen-Qiang Yin [1,2,3,4,*], Xiao-Hang Jin [1,2,3,4], Rong Wang [5], Shuang Wang [1,2,3,4], Wei Chen [1,2,3,4], Guang-Can Guo [1,2,3,4] and Zheng-Fu Han [1,2,3,4]

1 CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China
2 CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
3 Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China
4 State Key Laboratory of Cryptology, Beijing 100878, China
5 Department of Physics, University of Hong Kong, Pokfulam, Hong Kong
* Correspondence: yinzq@ustc.edu.cn

Abstract: Quantum key distribution (QKD) allows two remote parties to share information-theoretic secret keys. Many QKD protocols assume the phase of encoding state can be continuous randomized from 0 to 2π, which, however, may be questionable in the experiment. This is particularly the case in the recently proposed twin-field (TF) QKD, which has received a lot of attention since it can increase the key rate significantly and even beat some theoretical rate-loss limits. As an intuitive solution, one may introduce discrete-phase randomization instead of continuous randomization. However, a security proof for a QKD protocol with discrete-phase randomization in the finite-key region is still missing. Here, we develop a technique based on conjugate measurement and quantum state distinguishment to analyze the security in this case. Our results show that TF-QKD with a reasonable number of discrete random phases, e.g., 8 phases from $\{0, \pi/4, \pi/2, ..., 7\pi/4\}$, can achieve satisfactory performance. On the other hand, we find the finite-size effects become more notable than before, which implies that more pulses should be emit in this case. More importantly, as a the first proof for TF-QKD with discrete-phase randomization in the finite-key region, our method is also applicable in other QKD protocols.

Keywords: quantum key distribution; finite-key analysis; discrete-phase randomization

Citation: Wang, R.-Q.; Yin, Z.-Q.; Jin, X.-H.; Wang, R.; Wang, S.; Chen, W.; Guo, G.-C.; Han, Z.-F. Finite-Key Analysis for Quantum Key Distribution with Discrete-Phase Randomization. *Entropy* **2023**, *25*, 258. https://doi.org/10.3390/e25020258

Academic Editor: Gregg Jaeger

Received: 20 December 2022
Revised: 20 January 2023
Accepted: 24 January 2023
Published: 31 January 2023

1. Introduction

Quantum key distribution (QKD) [1,2], one of the most successful and mature applications in quantum information science, allows for two legitimate parties (Alice and Bob) to share information-theoretic secret keys. In theory, its security has been proved [3–5], while experiments towards a higher key rate [6] and longer achievable distance [7–10] have been demonstrated. Still, some large scale QKD networks are emerging [11–14]. However, owing to the inherent photon-loss in the channel, it meets a vital bottleneck that limits the communication distance and key generation rate. Specifically, some fundamental rate-loss limits [15,16] impose a restriction on any point-to-point QKD without repeaters. More precisely, the key rate R is bounded by the channel transmission probability η with the linear PLOB bound $R = -\log_2(1-\eta)$ [16]. Delightfully, M.Lucamarini et al. made a breakthrough by proposing twin-field (TF) QKD in 2018. The essential idea of TF-QKD is in code mode extracting the key bit from a single-photon click event of the measurement station located in the middle of channel, which happens with a probability proportional to $\sqrt{\eta}$; thus, surpassing the linear PLOB bound becomes possible, and a so-called phase-error rate may be estimated in decoy mode [17–19] to monitor security. Driven by this, several

TF-type QKD protocols [20–26] were proposed later to complete security proofs and improve performance. Based on these protocols, experimentalists also made great efforts to realize TF-QKD [27–35].

Since TF-QKD inherits measurement-device-independent (MDI)-QKD's [36] merit that is immune to all side-channel attacks to measurement devices and all measurement-device imperfections [37,38], one does not need to take the detection loopholes into account within the TF-type QKD system. In spite of this, the security issues of the state preparation in TF-QKD must be carefully considered. In practice, the laser source of TF-QKD is usually a continuous source emitting coherent states with a fixed phase. Meanwhile, continuous phase-randomization from 0 to π is required in the TF-QKD. More specifically, this continuous phase-randomization is assumed in both the code and test modes in Refs. [21,23,26], or at least in the test mode in Refs. [22,24,39]. To fulfill this requirement, Alice and Bob must randomize the global phase continuously and uniformly. Unluckily, two ways to achieve phase randomization introduce different problems in the experiment. Passive randomization will lead to phase correlations between adjacent pulses [40,41], while active randomization can only randomize the phase over discrete set of values.

To bridge this gap between theory and experiment, two works that analyzed the security of fully discrete-phase randomization TF-QKD protocol have been proposed [42–44] in these days. However, a security proof in the finite-key region is still missing. Hence, one natural question is that whether TF-QKD with fully discrete-phase randomization can work well non-asymptotically. This work affirms that it can.

In this paper, we analyze the security of TF-QKD protocol with fully discrete randomization in a finite-key region. Interestingly, our analysis leads to comparable performance with the continuous one. Since taking the discrete phase into account, our results make the TF-QKD more practical and can be applied to the future TF-QKD experiment. More importantly, some techniques proposed here, e.g., Lemma A1 (introduced later), can be utilized to analyze the security of other QKD protocols with discrete-phase randomization.

This work is organized as follows. In Section 2, we give a description of the TF-QKD protocol with fully discrete-phase randomization, and the sketch of the security proof is given in Section 3. Note that the proof is detailed in Appendix A. In Section 4, by the numerical simulation, we show this protocol can still beat the linear PLOB bound [16] and has satisfactory performance. Finally, a conclusion is given in Section 5.

2. Protocol Description

Indeed, the protocol analyzed here has been depicted in Ref. [43]. For ease of understanding, we illustrate the protocol as follows.

Step 1: Alice (Bob) chooses a label from $\{"\mu","0","\nu"\}$ with probabilities P_μ, P_O, P_ν, according to the label she (he) chooses, she (he) takes one of the following actions:

"μ": she (he) randomly picks an integer l_{A_c} (l_{B_c}) from $\{0,1,\cdots,M-1\}$ with equal probability $\frac{1}{M}$ where M is an even integer. This means that the phase 2π is divided into M parts. Then, she (he) randomly chooses a key bit $k_a(k_b)$ where $k_a(k_b) \in \{0,1\}$. Finally, she (he) sends a pulse with a coherent state $|e^{i(\frac{l_{A_c}}{M}2\pi+\pi k_a)}\sqrt{\mu}\rangle(|e^{i(\frac{l_{B_c}}{M}2\pi+\pi k_b)}\sqrt{\mu}\rangle)$.

"0": she (he) sends the vacumm state.

"ν": she (he) randomly picks an integer l_{A_c} and l_{B_c} from $\{0,1,\cdots,M-1\}$ with equal probability $\frac{1}{M}$ where M is an even integer. This means that the phase 2π is divided into M parts. Then, she (he) sends a pulse with a coherent state $|e^{i\frac{l_{A_c}}{M}2\pi}\sqrt{\mu}\rangle(|e^{i\frac{l_{B_c}}{M}2\pi}\sqrt{\mu}\rangle)$.

The first case is called code mode, while the other cases are decoy mode.

Step 2: Alice and Bob repeat Step 1 in total of N_{tot} times.

Step 3: After receiving N_{tot} pairs of pulses from Alice and Bob, interfering each pair at a beamsplitter and measuring the two outputs with his single photon detectors (SPDs), an honest Eve announces whether or not each measurement is successful. Here, 'successful' means only one SPD (left SPD or right SPD) clicks in the corresponding measurement, and if so, Eve reports the specific SPD clicked.

Step 4: For those rounds Eve announcing successful click, Alice and Bob announce the intensities they chose as well as the values of l_{A_c} and l_{B_c}. Then, Alice and Bob only retain those successful rounds in which the intensities of the coherent state they sent are same while the in-phase ($l_{A_c} = l_{B_c}$) or anti-phase ($|l_{A_c} - l_{B_c}| = M/2$) condition is also met. Let $n^+_{2\beta}(n^-_{2\beta})$ be the number of the retained rounds when both Alice and Bob chose the same intensity β of the coherent state and the in-phase (anti-phase) is also met. Note that we assume $l_{A_c} = l_{B_c} = 0$ always holds in the case of $\beta = 0$. Alice and Bob generate their sifted keys from $n_{2\mu} = n^+_{2\mu} + n^-_{2\mu}$ retained rounds in code mode, thus the length of sifted key bits $n_{bit} = n_{2\mu}$. Note that if it is an in-phase (anti-phase) round with right (left) SPD clicking, Bob may flip his corresponding sifted key bit.

Step 5: With all of the quantities $n_{2\beta} = n^+_{2\beta} + n^-_{2\beta}$, Alice and Bob use linear programming to obtain an upper bound on the number of phase errors(defined later) n^U_{ph} with a failure probability no more than ε; then, they can calculate the upper bound $e^U_{ph} = n^U_{ph}/n_{bit}$.

Step 6: Step 6 consists of error correction and privacy amplification.

Step 6a: Alice sends H_{EC} bits of syndrome information of her sifted key bits to Bob through an authenticated public channel. Then, Bob uses it to correct errors in his sifted keys. Alice and Bob calculate a hash of their error-corrected keys with a random universal hash function and check whether they are equal. If equal, they continue to the next step; otherwise, they abort the protocol.

Step 6b: Alice and Bob apply the privacy amplification to obtain their final secret keys. If the length of their secret key satisfies $l = n_{bit}(1 - h(e^U_{ph})) - H_{EC} - \log_2 \frac{2}{\epsilon_{cor}} - \log_2 \frac{1}{4\epsilon^2_{PA}}$ where $h(\cdot)$ denotes the binary Shannon entropy, this protocol must be ϵ_{cor}-correct and ϵ_{sec}-secret with $\epsilon_{sec} = \sqrt{\varepsilon} + \epsilon_{PA}$. Here, $\epsilon_{cor}(\epsilon_{sec})$ represents the protocol is correct (secret) with a failure probability no more than $\epsilon_{cor}(\epsilon_{sec})$. Hence, the total security parameter is ϵ_{tol}-secure where $\epsilon_{tol} = \epsilon_{cor} + \epsilon_{sec}$. It is elaborated thoroughly in the widely-used universally composable security framework [45,46].

3. Security Proof

In this section, we present the security proof of this protocol. The main task of the security proof is to bound the information Eve holds. To accomplish this task, one can calculate a so-called phase-error rate. Firstly, we construct an equivalent virtual protocol, in which Alice and Bob prepare some entangled states between local states and traveling states, but traveling states must have the same density matrices as actual protocol in the channel. The sifted key bits can be seen as the outputs of measurement with Z-basis on local states made by Alice and Bob; then, the so-called phase-error rate is defined as the error rate for the outputs of measurement with the X-basis made by them. According to the complementarity argument [47], the phase-error rate can be used to bound Eve's information on the sifted keys. In the following, we give the virtual protocol and show how to bound the phase-error rate.

3.1. Equivalent Virtual Protocol

In our virtual protocol, Alice generates secret keys from the code mode in which she prepares the state

$$|\psi\rangle_{\mu,A_cAa} = \sum_{l=0}^{M-1} \frac{1}{\sqrt{M}} |l\rangle_{A_c} \left(\frac{1}{\sqrt{2}}(|0\rangle_A |e^{i\frac{2\pi}{M}l}\sqrt{\mu}\rangle_a + |1\rangle_A |-e^{i\frac{2\pi}{M}l}\sqrt{\mu}\rangle_a)\right), \quad (1)$$

where A_c and A are the local quantum systems in Alice's side, and a is the traveling quantum state Alice sent to Eve. Similarly, Bob prepares $|\psi\rangle_{\mu,B_cBb}$ defined analogously to $|\psi\rangle_{\mu,A_cAa}$. Obviously, Alice (Bob) measures $A(B)$ with Z-basis to obtain sifted key, i.e., $|0\rangle_A$ for bit 0 and $|1\rangle_A$ for bit 1. In order to obtain the phase-error rate, they measure A, B in

X-basis $\{|+\rangle, |-\rangle\}$ after Eve's attack. As for the test mode, we assume Alice prepares the following states

$$|\psi\rangle_{0,A_cAa} = |0\rangle_{A_c}|0\rangle_A|0\rangle_a, \tag{2}$$
$$|\psi\rangle_{\nu,A_cAa} = \sum_{l=0}^{M-1} \frac{1}{\sqrt{M}}|l\rangle_{A_c}|0\rangle_A|e^{i\frac{2\pi}{M}l}\sqrt{\nu}\rangle_a.$$

Here, the local states of A_c are encoded in photon-number states, and Alice can measure A_c's photon-number to learn the phase of sent states.

Finally, we can describe the process of state preparation above with a single state, namely,

$$|\psi\rangle_{A_sA_cAa} = \sqrt{p_\mu}|0\rangle_{A_s}|\psi\rangle_{\mu,A_cAa} + \sqrt{p_O}|1\rangle_{A_s}|\psi\rangle_{0,A_cAa} + \sqrt{p_\nu}|2\rangle_{A_s}|\psi\rangle_{\nu,A_cAa} \tag{3}$$

where Alice's additional local ancilla A_s is in the photon number states. Similarly, Bob can prepare $|\psi\rangle_{B_sB_cBb}$ defined analogously to $|\psi\rangle_{A_sA_cAa}$. Though Alice (Bob) may measure $A_s(B_s)$,$A_c(B_c)$, and $A(B)$ after or before Eve announcing her measurement results, Alice (Bob) must announce the measurement results after Eve's announcement then post-select the successful rounds. The following is a detailed illustration of our equivalent virtual protocol.

Step 1:

Alice and Bob prepare a gigantic quantum state $|\Phi\rangle = |\phi\rangle^{\otimes N_{tot}} = (|\psi\rangle_{A_sA_cAa} \otimes |\psi\rangle_{B_sB_cBb})^{\otimes N_{tot}}$ and send all subsystems a and b to Eve through an insecure quantum channel.

Step 2:

After performing an arbitrary quantum operation on all subsystems a and b from Alice and Bob, Eve announces whether it has a successful click (only one of her SPDs clicks) or not for each round. For a successful round, Eve continues to announce whether the left SPD clicks or the right SPD clicks. We use $\mathcal{M}(\overline{\mathcal{M}})$ to denote the set of successful (unsuccessful) rounds.

Step 3:

For those rounds in which Eve announces success, Alice and Bob jointly measure the subsystem $A_c(B_c)$ and $A_s(B_s)$ in the photon-number basis to learn whether the intensities of the coherent state they send are same or not and whether it is in-phase or anti-phase. Then, they only retain those rounds where in-phase or anti-phase is met, and they choose the same intensities. Let $\mathcal{M}_s$ denote the set of those retained rounds, while $\mathcal{M}_f$ denotes those rounds that are in $\mathcal{M}$ but not in $\mathcal{M}_s$.

Step 4:

For these rounds in $\mathcal{M}_s$, Alice (Bob) measures the subsystem $A_cA_s(B_cB_s)$ in Fock basis to learn the phase and intensity of the coherent states she (he) sent . If the result of $A_s(B_s)$ is in state $|0\rangle_{A_s}(|0\rangle_{B_s})$, she (he) measures subsystems $A(B)$ in the Z basis to decide her (his) sifted key, respectively; otherwise, she (he) measures subsystem A(B) in the Z basis but does not incorporate these measurement outcomes in her (his) sifted key.

Step 5 to Step 6:

Let $n_{2\beta}$ be the number of rounds in $\mathcal{M}_s$ satisfying that both Alice and Bob chose the intensity β. With parameters $n_{2\beta}$, perform the same operations as Step 5 to Step 6, respectively, in the actual protocol given in Section 2.

3.2. Estimation of Phase-Error Rate

The essential of security proof is to estimate the upper-bound of the phase-error rate e_{ph} of the sifted keys, i.e., how many same or different outcomes Alice and Bob have if they measure A and B with X-basis hypothetically in the rounds where sifted keys are generated. Specifically, in our protocol, we define the number of the same outcomes they have as n_{ph}, i.e., the number of phase-error events. Provided that $e_{ph} = n_{ph}/n_{2\mu}$ is bounded, one

can generate the final secret key with an appropriate ϵ_{tol} value as given in Step6.b of the actual protocol.

A detailed proof for how to estimate n_{ph} is present in Appendix A. Here, a sketch of this proof is given.

Though analyzing the equivalent protocol, it is proven that if Alice and Bob both chose intensity β, and in-phase or anti-phase is also met, they actually prepare a mixture $\tau_{2\beta}$, which consists of component $\tau_{j|2\beta}, j = 0, 1, ..., M-1$. Moreover, each phase-error event is a click by some particular components of that mixture $\tau_{2\beta}$, i.e., $\tau_{j|2\beta}, j = 0, 2, ..., M-2$. These results imply that

$$\begin{aligned} n_{2\mu} &= \sum_{j=0}^{M} n_{j|2\mu}, \\ n_{2\nu} &= \sum_{j=0}^{M} n_{j|2\nu}, \\ n_{ph} &= \sum_{j=0, j\in\mathcal{N}_0}^{M-2} n_{j|2\mu}, \end{aligned} \tag{4}$$

where $n_{j|2\beta}$ denotes the number of rounds in $\mathcal{M}_s$, in which Alice and Bob both chose intensity β, but $\tau_{2\beta}$ is actually $\tau_{j|2\beta}$. Meanwhile, $\mathcal{N}_0$ is the set of even numbers. Now, the hypothetical value n_{ph} is related to some experimentally observed values. However, just with these equations it is difficult to bound n_{ph} tightly since $n_{j|2\beta}$ cannot be known directly.

On the other hand, both $\tau_{j|2\mu}$ and $\tau_{j|2\nu}$ are very close to Fock-state $|j\rangle\langle j|$. Accordingly, it is intuitive to consider if there are constraints on the gap between $n_{j|2\mu}$ and $n_{j|2\nu}$. Then, we developed Lemma A1 (see Appendix A for details) to bound the gap between the yields of two distinct quantum states in a non-asymptotic situation. Applying this lemma, we obtained a series of constraints on $n_{j|2\mu}$ and $n_{j|2\nu}$. Finally, combined with Equation (5), an analytical upper bound of n_{ph} (given in the end of the Appendix A) was calculated to find the upper bound of phase-error rate $e_{ph}^{U} = n_{ph}^{U}/n_{2\mu}$.

4. Numerical Simulation

In this section, we simulate the final secret key rate with the parameters listed in Table 1.

Table 1. List of parameters uesd in the numerical simulations. Here, e_m is loss-independent misalignment error rate due to optical imperfect interference, p_d is dark counting probability for each SPD, ξ is fiber loss constant, η_d denotes detection efficiency of each SPD, f is error-correction inefficiency, and ϵ_{tol} denotes the total security coefficient.

e_m	p_d	ξ (dB/km)	η_d	f	ϵ_{tol}
0.03	1×10^{-8}	0.2	0.3	1.1	4.6566×10^{-10}

It is reasonable to simulate the experimentally observed values $n_{2\mu}$, $n_{2\nu}$ and n_0 with their mean values. Let $Q_{corr|2\beta}$ be the probability of only one click from left (right) SPD when both Alice and Bob prepare coherent states with intensity β and a phase difference of 0 (π), and $Q_{err|2\beta}$ be the probability of only one click from left (right) SPD when both Alice and Bob prepare coherent states with intensity β and phase difference of π (0). Then, we have

$$\begin{aligned} Q_{corr|2\beta} &= (1-(1-p_d)e^{-2\eta(1-e_m)\beta})e^{-2\eta e_m\beta}(1-p_d), \\ Q_{err|2\beta} &= (1-(1-p_d)e^{-2\eta e_m\beta})e^{-2\eta(1-e_m)\beta}(1-p_d), \end{aligned} \tag{5}$$

where $\eta = 10^{\frac{-0.2L}{20}}$ and L is the channel distance between Alice and Bob. Accordingly, in the simulation, we assume $n_{2\beta} = N_{tot}P_{\beta}^{2}2(Q_{corr|2\beta} + Q_{err|2\beta})/M$ for $\beta = \mu, \nu$. Note that $n_0 = N_{tot}P_{O}^{2}(Q_{corr|0} + Q_{err|0})$, $n_{bit} = n_{2\mu}$ and $e_{bit} = Q_{err|2\mu}/(Q_{corr|2\mu} + Q_{err|2\mu})$. With these values, setting $M = 8$ and the failure probability of estimating phase error $\varepsilon = (6M+12)\varepsilon_a = 4 \times 10^{-20}$, one can obtain the upper-bound of phase-error rate e_{ph}^{U} by the linear programming given by (A41) in Appendix A. Moreover, the amount of H_{EC} is

$H_{EC} = N_{bit} f h(e_{bit})$, $\epsilon_{cor} = 1 \times 10^{-10}$, and $\epsilon_{PA} = 1.6566 \times 10^{-10}$, which leads to a secret key of length $l = n_{bit}(1 - h(e_{ph}^{U})) - H_{EC} - \log_2 \frac{2}{\epsilon_{cor}} - \log_2 \frac{1}{4\epsilon_{PA}^2}$ with $\epsilon_{sec} = \epsilon_{PA} + \sqrt{\varepsilon}$ and the total security parameter $\epsilon_{tol} = \epsilon_{cor} + \epsilon_{sec} = 4.6566 \times 10^{-10}$.

Finally, we numerically optimize the intensities and corresponding probabilities to maximize l in the cases of the total number of pulses is $N_{tot} = 1 \times 10^{17}, 1 \times 10^{14}, 1 \times 10^{13}, 1 \times 10^{12}$. Note that because this numerical problem is very time-comsuming, these intensities and probabilities are not optimized at each distance. Additionally, we use some typical parameters instead. The simulate results (l/N_{tot} v.s. L) are illustrated below.

As Figure 1 shows, we obtain considerable secret key rates when the total number of pulses is 10^{12}, 10^{13} ,10^{14} or 10^{17}. Through numerical simulations, it is confirmed that TF-QKD with discrete-phase randomization has satisfactory performance. On the other hand, it is verified that finite-size effects become more notable here compared with the original protocol with continuous phase randomization; it seems that one has to prepare 10^{17} pulses to surpass the PLOB linear bound. This is because the statistical fluctuations in Lemma A1 are proportional to the square root of the total number of emitting pulse N_{tot}, which leads to alarge phase-error rate e_{ph} when n_{bit} is not sufficiently large.

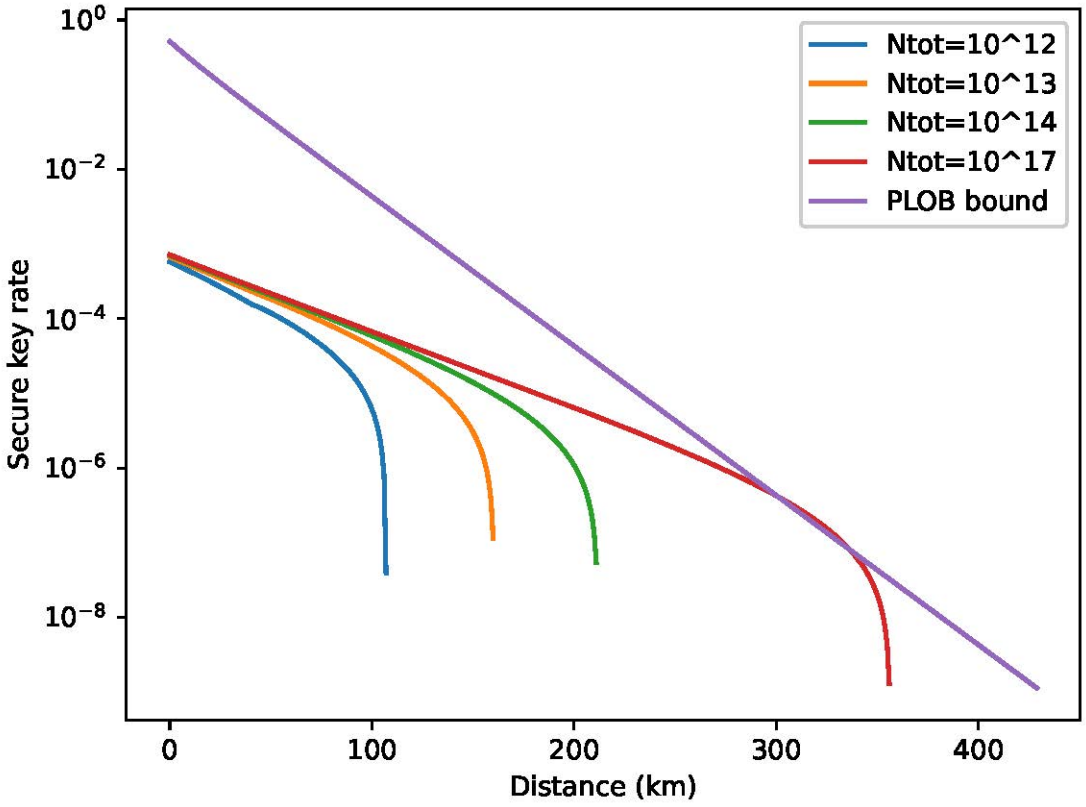

Figure 1. Secret key rate (l/N_{tot}) of fully discrete TF-QKD [43]. In this figure, the key rate corresponding to the total number of pulses N_{tot} is $1 \times 10^{12}, 1 \times 10^{13}, 1 \times 10^{14}, 1 \times 10^{17}$, plotted above. Note that we set $M = 8$ in the simulation.

5. Conclusions

In real setups of TF-QKD, continuous randomization is usually realized by actively adding a random signal to a phase modulator. On the other hand, random numbers are generated discretely in most schemes. Therefore, TF-QKD with discrete-phase randomization is more practical. It is necessary to analyze the security of TF-QKD with discrete-phase randomization. Based on conjugate measurement, the security proof of a QKD protocol is to estimate the phase-error rate. Then in case of discrete-phase randomization, a critical step is knowing how to bound the gap between yields of two distinct but very close quantum

states in a non-asymptotic situation. To achieve this goal, Lemma A1 is developed to find the upper bound of this gap. With the help of Lemma 1, linear programming is proposed to calculate the phase-error rate, and the key length is then straightforward. Through numerical simulations, it is confirmed that TF-QKD with discrete-phase randomization has satisfactory performance. On the other hand, we also find that more pulses should be prepared to alleviate the finite-size effects than previous protocol.

Moreover, it is worth noting that Lemma A1 is quite useful in a variety of scenarios, not just in the security proof of TF-QKD. For instance, if one considers the BB84 with discrete-phase randomization [48], the Lemma A1 can be utilized to bound the yield of single photon state, so then it is not difficult to give a relevant security proof. To summarize, we give the first security proof for TF-QKD with finite discrete-phase randomization in non-asymptotic scenarios. Although the proof is tailored for TF-QKD, the framework of this proof, i.e. Lemma A1, can be adapted in other protocols.

Author Contributions: Methodology, R.-Q.W.; Software, R.-Q.W. and X.-H.J.; Validation, R.-Q.W., Z.-Q.Y. and X.-H.J.; Formal analysis, R.-Q.W. and R.W.; Resources, S.W., W.C., Z.-F.H. and G.-C.G.; Data curation, X.-H.J.; Writing—original draft, R.-Q.W.; Writing—review and editing, Z.-Q.Y.; Visualization, R.-Q.W.; Project administration, Z.-Q.Y.; Funding acquisition, Z.-Q.Y. 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. 2020YFA0309802), the National Natural Science Foundation of China (Grant Nos. 62171424, 61961136004).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We thank Rong-Wang for constructive discussion.

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

Appendix A

Appendix A.1. Formula for the Number of Phase-Error Events

In this section, we show how to obtain the relation between the hypothetical phase-error events and some experimental observations.

The main result obtained here is that each key bit is a successful click from a mixed state of $\tau_{j|2\mu}, j = 0, 1, ..., M-1$ prepared by Alice and Bob. More importantly, the number of phase-error events among these key bits corresponds to $\tau_{j|2\mu}, j = 0, 2, ..., M-2$. Therefore, if we denote the length of the raw key by $n_{bit} = n_{2\mu}$ and the number of successful clicks of $\tau_{j|2\mu}$ by $n_{j|2\mu}$, $n_{bit} = n_{2\mu} = \sum_{j=0}^{M-1} n_{j|2\mu}$, the number of phase-error events $n_{ph} = \sum_{j=0, j\in\mathcal{N}_0}^{M-2} n_{j|2\mu}$ must hold, where $\mathcal{N}_0$ is the set of even integers. Next, a proof is present to show how to obtain this result.

Following the symbols in [49], let us consider the evolution of the gigantic quantum state $|\Phi\rangle = |\phi\rangle^{\otimes N_{tot}} = (|\psi\rangle_{A_sA_cAa} \otimes |\psi\rangle_{B_sB_cBb})^{\otimes N_{tot}}$ sent to Eve. After Step 2, where Eve performs her measurement on the subsystem ab, the initial quantum state is transformed to $\hat{M}_{eve}|\Phi\rangle$, where $\hat{M}_{eve}$ denotes the measurement operator of Eve. After measurement, Eve announces whether the measurement outcome is successful or not for each round. Hence, we reorder the quantum state as $|\Phi\rangle = |\phi\rangle^{\otimes M}|\phi\rangle^{\otimes \overline{M}}$, where $M(\overline{M})$ denotes the successful (unsuccessful) rounds. Then, in Step 3 of the virtual protocol, using measurement operators $\{\hat{O}_s = (|00\rangle_{A_sB_s}\langle 00| + |11\rangle_{A_sB_s}\langle 11| + |22\rangle_{A_sB_s}\langle 22|) \otimes \sum_{l=0}^{M-1}(|l,l\rangle_{A_cB_c}\langle l,l| + |l,(l + M/2)modM\rangle_{A_cB_c}\langle l,(l + M/2)modM|), \hat{O}_d = \hat{I} - \hat{O}_s\}$, Alice and Bob measure the subsystem A_sA_c and B_sB_c for those rounds that are announced successful in Step 2 and retain the trials in which A_sA_c and B_sB_c are collapsed into $\hat{O}_s$ as the final successful rounds. Hence, we reorder $|\Phi\rangle = |\phi\rangle^{\otimes M_s}|\phi\rangle^{\otimes M_f}|\phi\rangle^{\otimes \overline{M}}$ where $M_s(M_f)$ denotes the successful(unsuccessful)

rounds finally. Before they measure the subsystem AB to generate their sifted key in Step 3, the unnormalized quantum state is given by

$$\hat{O}_s^{M_s}\hat{O}_d^{M_f}\hat{I}^{\otimes\overline{M}}\hat{M}_{eve}|\Phi\rangle = \hat{M}_{eve}\hat{O}_s^{\otimes M_s}\hat{O}_d^{\otimes M_f}\hat{I}^{\otimes\overline{M}}|\Phi\rangle = \hat{M}_{eve}(\hat{O}_s|\phi\rangle)^{\otimes M_s}(\hat{O}_f|\phi\rangle)^{\otimes M_f}(|\phi\rangle)^{\otimes\overline{M}} \tag{A1}$$

Next, in Step 4, Alice and Bob measure the subsystem A_s, B_s A_c, B_c and A, B for all rounds in $\mathcal{M}_s$, one by one. We use $\alpha \in \{1, \cdots, M_s\}$ to denote the different rounds in $\mathcal{M}_s$ and ξ_α to denote the measurement outcome of the α-th subsystem. What is more, $\hat{M}_\alpha$ is used to denote the associated operator. Hence, the unnormalized state before the measurement of the α-th rounds in $\mathcal{M}_s$ is

$$|\Phi_\alpha\rangle = \hat{M}_{eve}(\otimes_{l=1}^{\alpha-1}\hat{M}_l|\phi\rangle)(\hat{O}_s|\phi\rangle)(\hat{O}_s|\phi\rangle)^{\otimes M_s-\alpha}(\hat{O}_f|\phi\rangle)^{\otimes M_f}(|\phi\rangle)^{\otimes\overline{M}}. \tag{A2}$$

Because we are only interested in the reduced state of the α-th round in $\mathcal{M}_s$, we trace out the other rounds which we denote by $\overline{\alpha}$ and obtain

$$\hat{\sigma}_\alpha = Tr_{\overline{\alpha}}[|\Phi_\alpha\rangle\langle|\Phi_\alpha|] = \sum_{\overrightarrow{\overline{\alpha}}}\langle\overrightarrow{\overline{\alpha}}|\Phi_\alpha\rangle\langle\Phi_\alpha|\overrightarrow{\overline{\alpha}}\rangle = \sum_{\overrightarrow{\overline{\alpha}}}\hat{M}_{\overrightarrow{\overline{\alpha}}}\hat{O}_s|\phi\rangle\langle\phi|\hat{O}_s^\dagger\hat{M}_{\overrightarrow{\overline{\alpha}}}^\dagger \tag{A3}$$

where

$$\hat{M}_{\overrightarrow{\overline{\alpha}}} = \langle\overrightarrow{\overline{\alpha}}|\hat{M}_{eve}|(\otimes_{l=1}^{\alpha-1}\hat{M}_l(\hat{O}_s|\phi\rangle)(\hat{O}_s|\phi\rangle)^{\otimes M_s-\alpha}(\hat{O}_f|\phi\rangle)^{\otimes M_f}(|\phi\rangle)^{\otimes\overline{M}}. \tag{A4}$$

and the quantum states $\{|\overrightarrow{\overline{\alpha}}\rangle\}$ represent the basis for the subsystems $A_s, B_s, A_c, B_c, A, B, a, b$ of all rounds in the protocol except the α-th round in $\mathcal{M}_s$.

Next, to derive the number of phase error, we expand the quantum state $\hat{O}_s|\phi\rangle$ as

$$\hat{O}_s|\phi\rangle = p_\mu|00\rangle_{A_sB_s}|\phi\rangle_\mu + p_O|11\rangle_{A_sB_s}|\phi\rangle_0 + p_\nu|22\rangle_{A_sB_s}|\phi\rangle_\nu \tag{A5}$$

where

$$\begin{aligned}&|\phi\rangle_\mu\\ =\ &\textstyle\sum_{l=0}^{M-1}\frac{1}{M}[(|ll\rangle_{A_cB_c}\frac{1}{2}(|0\rangle_A|e^{i\frac{2\pi}{M}l}\sqrt{\mu}\rangle_a + |1\rangle_A|-e^{i\frac{2\pi}{M}l}\sqrt{\mu}\rangle_a)(|0\rangle_B|e^{i\frac{2\pi}{M}l}\sqrt{\mu}\rangle_b + |1\rangle_B|-e^{i\frac{2\pi}{M}l}\sqrt{\mu}\rangle_b))\\ &+(|l,(l+\tfrac{M}{2})modM\rangle_{A_cB_c}\frac{1}{2}(|0\rangle_A|e^{i\frac{2\pi}{M}l}\sqrt{\mu}\rangle_a + |1\rangle_A|-e^{i\frac{2\pi}{M}l}\sqrt{\mu}\rangle_a)(|0\rangle_B|-e^{i\frac{2\pi}{M}l}\sqrt{\mu}\rangle_b + |1\rangle_B|e^{i\frac{2\pi}{M}l}\sqrt{\mu}\rangle_b)))],\end{aligned}$$

$$|\phi\rangle_0 = |00\rangle_{A_cB_c}|00\rangle_{AB}|00\rangle_{ab} \tag{A6}$$

and

$$\begin{aligned}&|\phi\rangle_\nu\\ =\ &\textstyle\sum_{l=0}^{M-1}\frac{1}{M}[(|ll\rangle_{A_cB_c}(|00\rangle_{AB}|e^{i\frac{2\pi}{M}l}\sqrt{\nu}\rangle_a|e^{i\frac{2\pi}{M}l}\sqrt{\nu}\rangle_b) + (|l,(l+\tfrac{M}{2})modM\rangle_{A_cB_c}|00\rangle_{AB}(|e^{i\frac{2\pi}{M}l}\sqrt{\nu}\rangle_a| - e^{i\frac{2\pi}{M}l}\sqrt{\nu}\rangle_b))].\end{aligned} \tag{A7}$$

To summarize, each key bit can be viewed as an event in which Eve announces a successful click conditioned by Alice and prepares $|\phi\rangle_\mu$ and measures AB with Z-basis . Since the measurement on AB made by Alice and Bob can be delayed after Eve's announcement of a successful click, the phase error can be estimated by Alice and Bob measuring AB with X-basis rather than Z-basis. To obtain the phase error of this part, we rewrite $|\phi\rangle_\mu$ under X-bases of AB as

$$|\phi\rangle_\mu = \sum_{l=0}^{M-1}\frac{1}{M}(|ll\rangle_{A_cB_c}|\psi\rangle_{\mu,AaBb}^l + |l,(l+\frac{M}{2})modM\rangle_{A_cB_c}|\psi'\rangle_{\mu,AaBb}^l) \tag{A8}$$

where

$$
\begin{aligned}
&|\psi\rangle^{l}_{\mu,AaBb}\\
=&\frac{1}{2}(|00\rangle_{AB}|e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b+|01\rangle_{AB}|e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b)\\
+&\frac{1}{2}(|10\rangle_{AB}|-e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b+|11\rangle_{AB}|-e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b)\\
=&\frac{1}{4}|++\rangle_{AB}(|e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b+|e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b+|-e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b+|-e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b)\\
+&\frac{1}{4}|--\rangle_{AB}(|e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b-|e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b-|-e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b+|-e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b)\\
+&\frac{1}{4}|+-\rangle_{AB}(\cdots)+\frac{1}{4}|-+\rangle_{AB}(\cdots)),
\end{aligned}
\tag{A9}
$$

$$
\begin{aligned}
&|\psi'\rangle^{l}_{\mu,AaBb}\\
=&\frac{1}{2}(|00\rangle_{AB}|e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b+|01\rangle_{AB}|e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b\\
+&\frac{1}{2}|10\rangle_{AB}|-e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b+|11\rangle_{AB}|-e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b)\\
=&\frac{1}{4}|++\rangle_{AB}(|e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b+|e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b+|-e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b+|-e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b)\\
+&\frac{1}{4}|--\rangle_{AB}(|e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b-|e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b-|-e^{i\theta_l}\sqrt{\mu}\rangle_a|-e^{i\theta_l}\sqrt{\mu}\rangle_b+|-e^{i\theta_l}\sqrt{\mu}\rangle_a|e^{i\theta_l}\sqrt{\mu}\rangle_b)\\
+&\frac{1}{4}|+-\rangle_{AB}(\cdots)+\frac{1}{4}|-+\rangle_{AB}(\cdots)),
\end{aligned}
\tag{A10}
$$

and $\theta_l=\frac{l}{M}2\pi$. For the purpose of clarification, we define some quantum states below:

$$
|e^{i\theta}\sqrt{2\mu}\rangle_{ab}=\sum_{j=0}^{\infty}e^{ij\theta}\sqrt{P_{j|2\mu}}|j\rangle_{ab} \tag{A11}
$$

and

$$
|e^{i\theta}\sqrt{2\mu}\rangle_{ab,even}=\frac{|e^{i\theta}\sqrt{\mu}\rangle_a|e^{i\theta}\sqrt{\mu}\rangle_b+|-e^{i\theta}\sqrt{\mu}\rangle_a|-e^{i\theta}\sqrt{\mu}\rangle_b}{2}=\sum_{j\in\mathcal{N}_0}e^{ij\theta}\sqrt{P_{j|2\mu}}|j\rangle_{ab}, \tag{A12}
$$

where $|j\rangle_{ab}=\sum_{i=0}^{j}\sqrt{\frac{j!}{2^j i!(j-i)!}}|i\rangle_a|j-i\rangle_b$ and $\mathcal{N}_0$ is the set of even numbers. Indeed, $|j\rangle$ is a quantum state satisfying that the total photon-number of a and b is j. Moreover, another similar quantum state is defined below:

$$
|e^{i\theta}\sqrt{2\mu}\rangle'_{ab}=\sum_{j=0}^{\infty}e^{ij\theta}\sqrt{P_{j|2\mu}}|j\rangle'_{ab} \tag{A13}
$$

and

$$
|e^{i\theta}\sqrt{2\mu}\rangle'_{ab}=\frac{|e^{i\theta}\sqrt{\mu}\rangle_a|-e^{i\theta}\sqrt{\mu}\rangle_b+|-e^{i\theta}\sqrt{\mu}\rangle_a|e^{i\theta}\sqrt{\mu}\rangle_b}{2}=\sum_{j\in\mathcal{N}_0}e^{ij\theta}\sqrt{P_{j|2\mu}}|j\rangle'_{ab} \tag{A14}
$$

where $|j\rangle'_{ab,even}=\sum_{i=0}^{j}(-1)^i\sqrt{\frac{j!}{2^j i!(j-i)!}}|i\rangle_a|j-i\rangle_b$. With these definitions, we can write the quantum states $|\psi\rangle^{l}_{\mu,AaBb}$ and $|\psi'\rangle^{l}_{\mu,AaBb}$ in a more simplified way, namely

$$|\psi\rangle^{l}_{\mu,AaBb} = \frac{1}{2}(|++\rangle_{AB}(|e^{i\theta_l}\sqrt{2\mu}\rangle_{ab,even} + |e^{i\theta_l}\sqrt{2\mu}\rangle'_{ab,even}) + |--\rangle_{AB}(|e^{i\theta_l}\sqrt{2\mu}\rangle_{ab,even} - |e^{i\theta_l}\sqrt{2\mu}\rangle'_{ab,even}) + |+-\rangle_{AB}(\cdots) + |-+\rangle_{AB}(\cdots)) \tag{A15}$$

and

$$|\psi'\rangle^{l}_{\mu,AaBb} = \frac{1}{2}(|++\rangle_{AB}(|e^{i\theta_l}\sqrt{2\mu}\rangle_{ab,even} + |e^{i\theta_l}\sqrt{2\mu}\rangle'_{ab,even}) - |--\rangle_{AB}(|e^{i\theta_l}\sqrt{2\mu}\rangle_{ab,even} - |e^{i\theta_l}\sqrt{2\mu}\rangle'_{ab,even}) + |+-\rangle_{AB}(\cdots) + |-+\rangle_{AB}(\cdots)) \tag{A16}$$

Obviously, the measurement outcome of $|++\rangle_{AB}$ and $|--\rangle_{AB}$ can be defined as phase-error event. Recall the whole density matrix $|\phi\rangle_\mu\langle\phi|$ given in Equation (A8); we can obtain the *ab* part corresponding to the phase-error event,

$$\begin{aligned}\hat{\rho}_{\mu,ph} =& \langle++|_{AB} tr_{A_cB_c}(|\phi\rangle_\mu\langle\phi|)|++\rangle_{AB} + \langle--|_{AB} tr_{A_cB_c}(|\phi\rangle_\mu\langle\phi|)|--\rangle_{AB} \\ =& \sum_{l=0}^{M-1}\langle ll|_{A_cB_c}(\langle++|_{AB} + \langle--|_{AB})|\phi\rangle_\mu\langle\phi|(|++\rangle_{AB} + |--\rangle_{AB})|ll\rangle_{A_cB_c} \\ &+\langle l,(l+M/2)modM|_{A_cB_c}(\langle++|_{AB} + \langle--|_{AB})|\phi\rangle_\mu\langle\phi|(|++\rangle_{AB} + |--\rangle_{AB})|l,(l+M/2)modM\rangle_{A_cB_c} \\ =& \sum_{l=0}^{M-1}\frac{1}{M^2}(|e^{i\theta_l}\sqrt{2\mu}\rangle_{ab}\langle e^{i\theta_l}\sqrt{2\mu}| + |e^{i\theta_l}\sqrt{2\mu}\rangle'_{ab}\langle e^{i\theta_l}\sqrt{2\mu}|)\end{aligned} \tag{A17}$$

According to Equations (2.5)–(2.7) of Ref [48], $\hat{\rho}_{\mu,ph}$ can be rewritten as

$$\begin{aligned}\hat{\rho}_{\mu,ph} =& \ \tfrac{2}{M}\textstyle\sum_{j=0,j\in\mathcal{N}_0}^{M-2}\tilde{P}_{j|2\mu}(\tfrac{1}{2}|\tilde{j}_{2\mu}\rangle_{ab}\langle\tilde{j}_{2\mu}| + \tfrac{1}{2}|\tilde{j}_{2\mu}\rangle'_{ab}\langle\tilde{j}_{2\mu}|) \\ =& \ \tfrac{2}{M}\textstyle\sum_{j=0,j\in\mathcal{N}_0}^{M-2}\tilde{P}_{j|2\mu}\tau_{j|2\mu},\end{aligned} \tag{A18}$$

where $\tilde{P}_{j|2\mu} = \sum_{n=0}^{\infty} P_{j+Mn|2\mu}$, $P_{j|2\mu}$ is the the probability of finding j photons in a Poisson source with mean photon-number 2μ, $|\tilde{j}_{2\mu}\rangle = \sum_{n=0}^{\infty}\frac{\sqrt{P_{j+Mn|2\mu}}}{\sqrt{\tilde{P}_{j|2\mu}}}|j+Mn\rangle_{ab}$ and $|\tilde{j}_{2\mu}\rangle' = \sum_{n=0}^{\infty}\frac{\sqrt{P_{j+Mn|2\mu}}}{\sqrt{\tilde{P}_{j|2\mu}}}|j+Mn\rangle'_{ab}$, and $\tau_{j|2\mu} = \frac{1}{2}|\tilde{j}_{2\mu}\rangle_{ab}\langle\tilde{j}_{2\mu}| + \frac{1}{2}|\tilde{j}_{2\mu}\rangle'_{ab}\langle\tilde{j}_{2\mu}|$.

For ease of understanding, we can easily interpret the formula of $\hat{\rho}_{\mu,ph}$. It is easy to see that $\hat{\rho}_{\mu,ph}$ is a mixture of $\tau_{j|2\mu}$, which consists of photon-number state $|j+Mn\rangle_{ab}, n = 0,1,2,...$, and the probability of finding $j+Mn$ photons is proportional to $P_{j+Mn|2\mu}$. Let $\tau_{even|2\mu}$ be the normalized $\hat{\rho}_{\mu,ph}$; then, a phase-error event for a key bit is equivalent to a successful click announced by Eve on the condition that a mixture $\tau_{even|2\mu} = \sum_{j=0,j\in\mathcal{N}_0}^{M-2}\tilde{P}_{j|2\mu}\tau_{j|2\mu}/P_{even|2\mu}$ prepared by Alice and Bob, and the probability of preparing such a mixture is obviously $P_\mu^2 P_{even|2\mu}2/M$.

To find a way to estimate the number of phase errors, we can give the density matrices Alice and Bob prepared in code mode and decoy mode. If we trace out ABA_cB_c of the quantum state $|\phi\rangle_\mu\langle\phi|$, i.e., regardless of whether the measurement outcome on AB is phase error or not, we have

$$\begin{aligned}\hat{\rho}_\mu =& \ Tr_{ABA_cB_c}(|\phi\rangle_\mu\langle\phi|) \\ =& \ \tfrac{2}{M}\textstyle\sum_{j=0}^{M-1}\tilde{P}_{j|2\mu}(\tfrac{1}{2}|\tilde{j}_{2\mu}\rangle\langle\tilde{j}_{2\mu}| + \tfrac{1}{2}|\tilde{j}_{2\mu}\rangle'\langle\tilde{j}_{2\mu}|) \\ =& \ \tfrac{2}{M}\textstyle\sum_{j=0}^{M-1}\tilde{P}_{j|2\mu}\tau_{j|2\mu}.\end{aligned} \tag{A19}$$

We define $\tau_{2\mu} = \sum_{j=0}^{M-1}\tilde{P}_{j|2\mu}\tau_{j|2\mu}$ as the normalized $\hat{\rho}_\mu$. The generation of a key bit is equivalent to a successful click announced by Eve conditioned on the premise that a mixture

$\tau_{2\mu} = \sum_{j=0}^{M-1} \tilde{P}_{j|2\mu}\tau_{j|2\mu}$ is prepared by Alice and Bob, and the probability of preparing such a mixture is obviously $P_\mu^2 2/M$.

Now we are approaching a main result of above derivations. In the N_{tot} rounds, Alice and Bob prepare $\tau_{2\mu}$ with the probability $P_\mu^2 2/M$; the number of its successful rounds is denoted by $n_{2\mu}$. Of course, the key bits are generated in these rounds, thus $n_{2\mu} = n_{bit}$. Since $\tau_{2\mu}$ is a mixture of $\tau_{j|2\mu}, j = 0, 1..., , M-1$, the $n_{2\mu}$ successful clicks are the sum of clicks by $\tau_{j|2\mu}, j = 0, 1, ..., M-1$. Then, $n_{2\mu} = \sum_{j=0}^{M-1} n_{j|2\mu}$ holds evidently, in which $n_{j|2\mu}$ is the number of successful clicks by $\tau_{j|2\mu}$. Recall that the phase errors for these events are from clicks by $\tau_{even|2\mu}$; one can assert that the number of phase-error events $n_{ph} = \sum_{j=0, j\in\mathcal{N}_0}^{M-2} n_{j|2\mu}$ must hold. This is a main result we have so far.

Appendix A.2. The Upper Bound of the Number of Phase-Error Events

We have proved that $n_{ph} = \sum_{j=0, j\in\mathcal{N}_0}^{M-2} n_{j|2\mu}$ with the constraint $n_{2\mu} = \sum_{j=0}^{M-1} n_{j|2\mu}$. Obviously, this is not sufficient for estimating n_{ph} tightly. Here, we resort to decoy states to obtain more constraints to bound n_{ph}.

Similarly with the analysis of clicks by $\hat{\rho}_\mu = Tr_{ABA_cB_c}(|\phi\rangle_\mu\langle\phi|)$, a successful click from decoy mode with intensity ν means that Alice and Bob prepare

$$\begin{aligned}\hat{\rho}_\nu &= Tr_{ABA_cB_c}(|\phi\rangle_\nu\langle\phi|)\\ &= \tfrac{2}{M}\sum_{j=0}^{M-1}\tilde{P}_{j|2\nu}(\tfrac{1}{2}|\tilde{j}_{2\nu}\rangle\langle\tilde{j}_{2\nu}| + \tfrac{1}{2}|\tilde{j}_{2\nu}\rangle'\langle\tilde{j}_{2\nu}|)\\ &= \tfrac{2}{M}\sum_{j=0}^{M-1}\tilde{P}_{j|2\nu}\tau_{j|2\nu}.\end{aligned} \tag{A20}$$

Accordingly, we also have $n_{2\nu} = \sum_{j=0}^{M-1} n_{j|2\nu}$. Here, $n_{2\nu}$ and $n_{j|2\nu}$ are defined analogously to $n_{2\mu}$ and $n_{j|2\mu}$, respectively. Intuitively, $n_{j|2\mu}$ and $n_{j|2\mu}$ are the numbers of successful clicks for $\tau_{j|2\mu}$ and $\tau_{j|2\nu}$ respectively. Typically, $\mu < \nu << 1$ is satisfied; then both $\tau_{j|2\mu}$ and $\tau_{j|2\nu}$ are very close to the photon-number state $|j\rangle_{ab}$. This implies that the gap between $n_{j|2\mu}$ and $n_{j|2\nu}$ can be bounded, and then we may estimate $n_{ph} = \sum_{j=0, j\in\mathcal{N}_0}^{M-2} n_{j|2\mu}$. Indeed, with the result in appendix B of ref [48], the gap between $n_{j|2\mu}$ and $n_{j|2\nu}$ in the asymptotic case can be obtained. Here, we develop Lemma A1 to bound this gap in finite-key situations.

Lemma A1. *If Alice prepares N_{tot} pairs of particles A and B with the quantum state $(\sum_i \sqrt{P_i}|i\rangle_A|\phi_i\rangle_B)^{\otimes N_{tot}}$ where $\langle i|j\rangle = \delta_{ij}, |\langle\phi_i|\phi_j\rangle| = F_{ij}$ and she sends the B part in each pair to Eve. For every round, Eve announces if the measurement is successful or unsuccessful, which is denoted by $M = 1$ or $M = 0$, respectively. Then, Alice measures the subsystem A with projectors $\{|i\rangle\langle i|, i = 0, 1, 2, ...\}$ to which quantum state she sent for the pairs that Eve announced $M = 1$. Let n_i denote the number of yields for the quantum state $|i\rangle$. If $P_i > P_j$, we have that the constraints between n_i and n_j, say,*

$$|\frac{P_j}{P_i}n_i - n_j| \le N_1\sqrt{1-F_{ij}^2} + 2\delta(N_1, \frac{1+\sqrt{1-F_{ij}^2}}{2}, \varepsilon_0^2) - 2\delta(N_2 - n_i - n_j, \frac{1}{2}, \varepsilon_0) + \delta(n_i, \frac{P_j}{P_i}, \varepsilon_2) \tag{A21}$$

holds with a failure probability $2\varepsilon_0 + 2\varepsilon_1 + 2\varepsilon_2$, where

$$\begin{aligned}\delta(x, y, z) &= \sqrt{3xy\ln(\tfrac{1}{z})}\\ N_1 &= 2P_jN_{tot} + \delta(N_{tot}, 2P_j, \varepsilon_1)\\ N_2 &= 2P_jN_{tot} - \delta(N_{tot}, 2P_j, \varepsilon_1)\end{aligned} \tag{A22}$$

Proof. Since we are only interested in the statistics of n_i and n_j, it is not restrictive to rewrite the quantum state $(\sum_i \sqrt{P_i}|i\rangle_A|\phi_i\rangle_B)^{\otimes N_{tot}}$ as

$$(\sum_i \sqrt{P_i}|i\rangle_A|\phi_i\rangle_B)^{\otimes N_{tot}} = \{\sqrt{P_i - P_j}|i'\rangle_A|\phi_i\rangle_B + \sqrt{2P_j}\frac{1}{\sqrt{2}}(|i''\rangle_A|\phi_i\rangle_B + |j\rangle_A|\phi_j\rangle_B) + ...\}^{\otimes N_{tot}}. \tag{A23}$$

Here, we virtually define $\sqrt{P_i}|i\rangle_A = \sqrt{P_i - P_j}|i'\rangle_A + \sqrt{P_j}|i''\rangle_A$ and $\langle i'|i''\rangle_A = 0$, which do not change the density matrix of B; thus, have no impact on Eve's operation and statistics of n_i and n_j. Let $n_{i'}(n_{i''})$ denote the number of detection for the quantum state $|i'\rangle_A(|i''\rangle_A)$ when Eve announces a successful measurement. Apparently, we know that $n_i = n_{i'} + n_{i''}$.

Let us focus on the state $\{\sqrt{2P_j}\frac{1}{\sqrt{2}}(|i''\rangle_A|\phi_i\rangle_B + |j\rangle_A|\phi_j\rangle_B)\}^{\otimes N_{tot}}$, by which the relation between $n_{i''}$ and n_j can be analyzed. The essential idea is reinterpreting the detection of B to a game of Eve guessing which states $|\phi_i\rangle_B$ or $|\phi_j\rangle_B$ Alice prepared for all of the N_{tot} trials. Specifically, we consider a virtual experiment illustrated below.

Alice prepares the quantum state $\{\sqrt{2P_j}\frac{1}{\sqrt{2}}(|i''\rangle_A|\phi_i\rangle_B + |j\rangle_A|\phi_j\rangle_B)\}^{\otimes N_{tot}}$; then, she sends the B part to Eve. Eve measures each B she received. If she obtains a successful measurement, she will announce $M = 1$. Otherwise, she will announce $M = 0$. Up to now, there is no difference from the previous protocol. A critical step is that for any trial that Eve announces $M = 0$, Alice flips corresponding M with probability $\frac{1}{2}$. Finally, Alice measures all partials A locally. It is obvious that if Alice prepares two quantum states $|\phi_i\rangle$ and $|\phi_j\rangle$ at random, the maximal probability of Eve guessing correctly which state is prepared is $\frac{1+\sqrt{1-F_{ij}^2}}{2}$ where $F_{ij} = |\langle\phi_i|\phi_j\rangle|$. With the flip operation, we can apply this maximal probability to our analysis below. In this case, we reinterpret that $M = 1$ ($M = 0$) means that Eve guessed the quantum state Alice prepared is $|\phi_i\rangle$ ($|\phi_j\rangle$), which justifies the lossless assumption. Note that this does not compromise security because as an adversary, Eve can guess in this way. In other words, we can now treat this virtual experiment as a game where Eve tries to guess whether Alice is preparing $|\phi_i\rangle$ or $|\phi_j\rangle$. For each of all the trials in such a game, it is well known that Eve's maximal probability of guessing correctly is $\frac{1+\sqrt{1-F_{ij}^2}}{2}$. Now, we are ready to find the relation between $n_{i''}$ and n_j by calculating how many trials in which Eve's guessing is correct. First, $n_{i''}$ means that announcing $M = 1$ at first and Alice also preparing $|\phi_i\rangle_B$, which of course leads to guessing correctly. Then, let $N_{i''}(N_j)$ denote Alice preparing the state $|\phi_i\rangle(|\phi_j\rangle)$, which implies that $N_{i''} + N_j \approx N_{tot}2P_j$. As a result, there are $(N_{i''} + N_j - n_{i''} - n_j)$ trials in which Eve announces $M = 0$ at first and then a random flipping operation on M follows; for every such trial, the probability of guessing correctly is obviously $1/2$. Further considering the potential statistical fluctuations made by the random flipping, with a failure probability of ε_1', the number of Eve guessing correctly in the $N_{i''} + N_j$ trials is no larger than

$$n_{i''} + \frac{1}{2}(N_{i''} - n_{i''}) + \frac{1}{2}(N_j - n_j) + \overline{\delta_1}, \tag{A24}$$

where $\overline{\delta_1} = \delta(N_{i''} + N_j - n_{i''} - n_j, \frac{1}{2}, \varepsilon_1')$ is the upper bound of the statistical fluctuation made by the random flipping of the $(N_{i''} + N_j - n_{i''} - n_j)$ trials. We let ε_1' be the probability of the amount of successful detection of quantum state $|i''\rangle$ reach $n_{i''}$. Hence the probability that we get the quantity denoted by Eq (A24) is $\varepsilon_1'^2$. On the other hand, in the $N_{i''} + N_j$ trials of guessing $|\phi_i\rangle$ and $|\phi_j\rangle$ prepared by Alice at random, the probability of Eve guessing correctly is no larger than $\frac{1+\sqrt{1-F_{ij}^2}}{2}$ [50], because the fidelity of $|\phi_i\rangle$ and $|\phi_j\rangle$ is F_{ij}, Hence, one can assert that when $\varepsilon_1'^2 \leq \varepsilon_0^2$, In this case, we let $\varepsilon_1' = \varepsilon_0$. Hence, one can assert that with a failure probability ε_0,

$$\frac{n_{i''} - n_j}{2} + \frac{N_{i''} + N_j}{2} + \overline{\delta_1} \leq (N_{i''} + N_j)\frac{1 + \sqrt{1 - F_{ij}^2}}{2} + \overline{\delta_2} \tag{A25}$$

holds, where $\overline{\delta_2} = \delta(N_{i''} + N_j, \frac{1+\sqrt{1-F_{ij}^2}}{2}, \varepsilon_0^2)$ is the upper bound of the statistical fluctuation when Eve's guessing probability for each trial achieves the upper-bound $\frac{1+\sqrt{1-F_{ij}^2}}{2}$. Note that because in such a guessing game, conditioned on other trials , the probability of

guessing correctly for any fixed trial cannot be larger than $\frac{1+\sqrt{1-F_{ij}^2}}{2}$, this lemma is applied to any attack . Furthermore, the probability of guessing correctly reaches its maximum, which equals a constant; then, the assumption of iid holds and the Bernoulli distribution is applied to this case. However, since it is hard to calculate the statistical fluctuation, we use the Chernoff bound δ_2 to approximate it [51].

According to Equation (A25), we can obtain an upper bound of $n_{i''} - n_j$ with a failure probability ε_0, say

$$n_{i''} - n_j \leq (N_{i''} + N_j)\sqrt{1-F_{ij}^2} + 2\delta(N_{i''} + N_j, \frac{1+\sqrt{1-F_{ij}^2}}{2}, \varepsilon_0^2) - 2\delta(N_{i''} + N_j - n_{i''} - n_j, \frac{1}{2}, \varepsilon_0). \tag{A26}$$

Similarly, if we redefine the guessing correctly as $M = 1$ corresponding to $|\phi_j\rangle$ and $M = 0$ corresponding to $|\phi_i\rangle$, we have that

$$n_j - n_i'' \leq (N_{i''} + N_j)\sqrt{1-F_{ij}^2} + 2\delta(N_{i''} + N_j, \frac{1+\sqrt{1-F_{ij}^2}}{2}, \varepsilon_0^2) - 2\delta(N_{i''} + N_j - n_{i''} - n_j, \frac{1}{2}, \varepsilon_0). \tag{A27}$$

Combining Equation (A26) and Equation (A27), we are clear that

$$|n_i'' - n_j| \leq (N_{i''} + N_j)\sqrt{1-F_{ij}^2} + 2\delta(N_{i''} + N_j, \frac{1+\sqrt{1-F_{ij}^2}}{2}, \varepsilon_0^2) - 2\delta(N_{i''} + N_j - n_{i''} - n_j, \frac{1}{2}, \varepsilon_0) \tag{A28}$$

holds with a failure probability $2\varepsilon_0$.

For simplicity's sake, we enlarge the R.H.S of Equation (A28). Concretely, we replace $2\delta(N_{i''} + N_j - n_{i''} - n_j, \frac{1}{2}, \varepsilon_0^2)$ by $2\delta(N_{i''} + N_j - n_i - n_j, \frac{1}{2}, \varepsilon_0^2)$ in Equation (A28), say

$$|n_{i''} - n_j| \leq (N_{i''} + N_j)\sqrt{1-F_{ij}^2} + 2\delta(N_{i''} + N_j, \frac{1+\sqrt{1-F_{ij}^2}}{2}, \varepsilon_0^2) - 2\delta(N_{i''} + N_j - n_i - n_j, \frac{1}{2}, \varepsilon_0). \tag{A29}$$

Note that these bounds of statistical fluctuations can be derived by the Chernoff bound [52].

Similarly, because of the probability that Alice sends the quantum state $\frac{1}{\sqrt{2}}(|i''\rangle_A|\phi_i\rangle_B + |j\rangle_A|\phi_j\rangle_B)$ is $2P_j$, using the well-known Chernoff bound [52], we know that

$$2N_{tot}P_j - \delta(N_{tot}, 2P_j, \varepsilon_1) \leq N_{i''} + N_j \leq 2N_{tot}P_j + \delta(N_{tot}, 2P_j, \varepsilon_1) \tag{A30}$$

Combing Equation (A29) and Equation (A30), we know that

$$|n_{i''} - n_j| \leq N_1\sqrt{1-F_{ij}^2} + 2\delta(N_1, \frac{1+\sqrt{1-F_{ij}^2}}{2}, \varepsilon_0^2) - 2\delta(N_2 - n_i - n_j, \frac{1}{2}, \varepsilon_0) \tag{A31}$$

holds with a failure probability $2\varepsilon_0 + 2\varepsilon_1$, where $N_1 = 2N_{tot}P_j + \delta(N_{tot}, 2P_j, \varepsilon_1)$ and $N_2 = 2N_{tot}P_j - \delta(N_{tot}, 2P_j, \varepsilon_1)$

Finally, to derive the relation between n_i and n_j, we have to consider the relations between $n_i$and $n_{i''}$. It is easy to know that $n_{i''} = \frac{P_j}{P_i}n_i$ on average since there is no way for Eve to distinguish $|i'\rangle$ and $|i''\rangle$. Hence, using the Chernoff bound [52] again, we know that

$$\frac{P_j}{P_i}n_i - \delta(n_i, \frac{P_j}{P_i}, \varepsilon_2) \leq n_{i''} \leq \frac{P_j}{P_i}n_i + \delta(n_i, \frac{P_j}{P_i}, \varepsilon_2) \tag{A32}$$

Combining Equation (A31) and Equation (A32), we can obtain the inequality Equation (A21).

In conclusion, we complete the proof. □

With Lemma A1, we can derive the constrains between $n_{i|2\mu}$ and $n_{j|2\nu}$. Since Alice and Bob send the quantum state $\tau_{j|2\mu}$ ($\tau_{j|2\nu}$) with the probability $\frac{2P_\mu^2}{M}\tilde{P}_{j|2\mu}$($\frac{2P_\nu^2}{M}\tilde{P}_{j|2\nu}$) and the fidelity between them is $F_{\mu\nu}^j = \sum_{n=0}^{\infty}\frac{\sqrt{P_{j+Mn|2\mu}}\sqrt{P_{j+Mn|2\nu}}}{\sqrt{\tilde{P}_{j|2\mu}\tilde{P}_{j|2\nu}}}$. By Lemma A1, we can obtain the relation between $n_{j|2\mu}$ and $n_{j|2\nu}$ which reads

$$|C_{j|2\mu}n_{j|2\mu} - C_{j|2\nu}n_{j|2\nu}| \leq \triangle_{\mu\nu}^j. \tag{A33}$$

We let $P_1 = \frac{2P_\mu^2}{M}\tilde{P}_{j|2\mu}$ and $P_2 = \frac{2P_\nu^2}{M}\tilde{P}_{j|2\nu}$. If $P_1 > P_2$, we have $C_{j|2\mu} = \frac{P_2}{P_1}$,$C_{j|2\nu} = 1$ and

$$\triangle_{\mu\nu}^j = N_1\sqrt{1-(F_{\mu\nu}^j)^2} + 2\delta(N_1, \frac{1+\sqrt{1-(F_{\mu\nu}^j)^2}}{2}, \varepsilon_0^2) - 2\delta(N_2 - n_{j|2\mu} - n_{j|2\nu}, \frac{1}{2}, \varepsilon_0) + \delta(n_{j|2\mu}, \frac{P_2}{P_1}, \varepsilon_2) \tag{A34}$$

where $N_1 = 2N_{tot}P_2 + \delta(N_{tot}, 2P_2, \varepsilon_1)$ and $N_2 = 2N_{tot}P_2 - \delta(N_{tot}, 2P_2, \varepsilon_1)$

If $P_1 < P_2$, we have that $C_{j|2\nu} = \frac{P_1}{P_2}$,$C_{j|2\mu} = 1$ and

$$\triangle_{\mu\nu}^j = N_1\sqrt{1-(F_{\mu\nu}^j)^2} + 2\delta(N_1, \frac{1+\sqrt{1-(F_{\mu\nu}^j)^2}}{2}, \varepsilon_0^2) - 2\delta(N_2 - n_{j|2\mu} - n_{j|2\nu}, \frac{1}{2}, \varepsilon_0) + \delta(n_{j|2\nu}, \frac{P_1}{P_2}, \varepsilon_2) \tag{A35}$$

where $N_1 = 2N_{tot}P_1 + \delta(N_{tot}, 2P_1, \varepsilon_1)$ and $N_2 = 2N_{tot}P_1 - \delta(N_{tot}, 2P_1, \varepsilon_1)$

One can know that the constraints Equations (A34) and (A35) are nonlinear because of the $n_{j|2\mu}$ in $\delta(n_{j|2\mu}, \frac{P_2}{P_1}, \varepsilon_2)$ or $n_{j|2\nu}$ in $\delta(n_{j|2\nu}, \frac{P_1}{P_2}, \varepsilon_2)$. To keep the linearity of these constraints for ease of numerical calculations, we replace $n_{j|2\mu}$ with $n_{2\mu}$ and replace $n_{j|2\nu}$ with $n_{2\nu}$ in $\triangle_{\mu\nu}^j$. That is to say, without compromising the security, we replace Equation (A34) by

$$\triangle_{\mu\nu}^j = N_1\sqrt{1-(F_{\mu\nu}^j)^2} + 2\delta(N_1, \frac{1+\sqrt{1-(F_{\mu\nu}^j)^2}}{2}, \varepsilon_0^2) - 2\delta(N_2 - n_{2\mu} - n_{2\nu}, \frac{1}{2}, \varepsilon_0) + \delta(n_{2\mu}, \frac{P_2}{P_1}, \varepsilon_2) \tag{A36}$$

and replace Equation (A35) by

$$\triangle_{\mu\nu}^j = N_1\sqrt{1-(F_{\mu\nu}^j)^2} + 2\delta(N_1, \frac{1+\sqrt{1-(F_{\mu\nu}^j)^2}}{2}, \varepsilon_0^2) - 2\delta(N_2 - n_{2\mu} - n_{2\nu}, \frac{1}{2}, \varepsilon_0) + \delta(n_{2\nu}, \frac{P_1}{P_2}, \varepsilon_2) \tag{A37}$$

Moreover, recalling Alice and Bob may both choose intensity 0 and obtain the corresponding number of successful clicks n_0, we have two additional constraints between n_0 and $n_{0|2\mu}, n_{0|2\nu}$ which reads

$$\begin{aligned} |C_{0,\mu}n_0 - C_{2\mu}^0 n_{0|2\mu}| &\leq \triangle_{0\mu}^0 \\ |C_{0,\nu}n_0 - C_{2\nu}^0 n_{0|2\nu}| &\leq \triangle_{0\nu}^0 \end{aligned} \tag{A38}$$

Since the probability of both Alice and Bob sending the quantum state $|0\rangle\langle 0|$ is P_O^2 and the fidelity between $|0\rangle\langle 0|$ and $\frac{1}{2}|\tilde{0}_{2\mu}\rangle\langle\tilde{0}_{2\mu}| + \frac{1}{2}|\tilde{0}_{2\mu}\rangle'\langle\tilde{0}_{2\mu}|$ ($\frac{1}{2}|\tilde{0}_{2\nu}\rangle\langle\tilde{0}_{2\nu}| + \frac{1}{2}|\tilde{0}_{2\nu}\rangle'\langle\tilde{0}_{2\nu}|$) is $F_{\mu 0}^0 = \frac{P_{0|2\mu}}{\tilde{P}_{0|2\mu}}$($F_{\nu 0}^0 = \frac{P_{0|2\nu}}{\tilde{P}_{0|2\nu}}$), we can obtain the coefficients of these two constraints according to Lemma A1. For simplicity's sake, we let $P_1 = P_O^2$ and $P_2 = \frac{2P_\mu^2\tilde{P}_{0|2\mu}}{M}$; then, if $P_1 > P_2$, we have $C_{0,\mu} = \frac{P_2}{P_1}$, $C_{2\mu}^0 = 1$ and

$$\triangle_{0\mu}^0 = N_1\sqrt{1-(F_{\mu 0}^0)^2} + 2\delta(N_1, \frac{1+\sqrt{1-(F_{\mu 0}^0)^2}}{2}, \varepsilon_0^2) - 2\delta(N_2 - n_{2\mu} - n_0, \frac{1}{2}, \varepsilon_0) + \delta(n_0, \frac{P_2}{P_1}, \varepsilon_2)$$

where $N_1 = 2N_{tot}P_2 + \delta(N_{tot}, 2P_2, \varepsilon_1)$ and $N_2 = 2N_{tot}P_2 - \delta(N_{tot}, 2P_2, \varepsilon_1)$; otherwise, we have $C_{0,\mu} = 1, C^0_{2\mu} = \frac{P_1}{P_2}$ and $C_{0,\mu} = \frac{P_2}{P_1}, C^0_{2\mu} = 1$ and

$$\triangle^0_{0\mu} = N_1\sqrt{1-(F^0_{\mu 0})^2} + 2\delta(N_1, \frac{1+\sqrt{1-(F^0_{\mu 0})^2}}{2}, \varepsilon^2_0) - 2\delta(N_2 - n_{2\mu} - n_0, \frac{1}{2}, \varepsilon_0) + \delta(n_{2\mu}, \frac{P_1}{P_2}, \varepsilon_2) \tag{A39}$$

where $N_1 = 2N_{tot}P_1 + \delta(N_{tot}, 2P_1, \varepsilon_1)$ and $N_2 = 2N_{tot}P_1 - \delta(N_{tot}, 2P_1, \varepsilon_1)$.

Similarly, we let $P_1 = P^2_O$ and $P_2 = \frac{2P^2_\nu \tilde{P}_{0|2\nu}}{M}$; then, if $P_1 > P_2$, we have $C_{0,\nu} = \frac{P_2}{P_1}, C^0_{2\nu} = 1$ and

$$\triangle^0_{0\nu} = N_1\sqrt{1-(F^0_{\nu 0})^2} + 2\delta(N_1, \frac{1+\sqrt{1-(F^0_{\nu 0})^2}}{2}, \varepsilon^2_0) - 2\delta(N_2 - n_{2\nu} - n_0, \frac{1}{2}, \varepsilon_0) + \delta(n_0, \frac{P_2}{P_1}, \varepsilon_2)$$

where $N_1 = 2N_{tot}P_2 + \delta(N_{tot}, 2P_2, \varepsilon_1)$ and $N_2 = 2N_{tot}P_2 - \delta(N_{tot}, 2P_2, \varepsilon_1)$; otherwise, we have $C_{0,\nu} = 1, C^0_{2\nu} = \frac{P_1}{P_2}$ and $C_{0,\nu} = \frac{P_2}{P_1}, C^0_{2\nu} = 1$ and

$$\triangle^0_{0\nu} = N_1\sqrt{1-(F^0_{\nu 0})^2} + 2\delta(N_1, \frac{1+\sqrt{1-(F^0_{\nu 0})^2}}{2}, \varepsilon^2_0) - 2\delta(N_2 - n_{2\nu} - n_0, \frac{1}{2}, \varepsilon_0) + \delta(n_{2\nu}, \frac{P_1}{P_2}, \varepsilon_2) \tag{A40}$$

where $N_1 = 2N_{tot}P_1 + \delta(N_{tot}, 2P_1, \varepsilon_1)$ and $N_2 = 2N_{tot}P_1 - \delta(N_{tot}, 2P_1, \varepsilon_1)$.

Now the gaps between $n_{j|2\mu}$ v.s. $n_{j|2\nu}$, $n_{0|2\mu}$ v.s. n_0, and $n_{0|2\nu}$ v.s. n_0 have been given. To bound n_{ph}, we can now resort to linear programming below:

$$\begin{aligned}
\max \quad & n_{ph} = \sum_{j=0, j\in\mathcal{N}_0}^{M-2} n_{j|2\mu} \\
\text{s.t.} \quad & \sum_{j=0}^{M-1} n_{j|2\mu} = n_{2\mu} \\
& \sum_{j=0}^{M-1} n_{j|2\nu} = n_{2\nu} \\
& |C_{0,\mu}n_0 - C^0_{2\mu}n_{0|2\mu}| \le \triangle^0_{0\mu} \\
& |C_{0,\nu}n_0 - C^0_{2\nu}n_{0|2\nu}| \le \triangle^0_{0\nu} \\
& |C_{j|2\mu}n_{j|2\mu} - C_{j|2\nu}n_{j|2\nu}| \le \triangle^j_{\mu\nu}.
\end{aligned} \tag{A41}$$

For ease of calculation, in all these constraints we let $\varepsilon_0 = \varepsilon_1 = \varepsilon_2 = \varepsilon_a$; then, the total failure probability that we obtain the bound $\triangle^j_{\mu\nu}$ is $6\varepsilon_a$. Meanwhile, the failure probability that we obtain the last two bounds on is $2\varepsilon_a$. Hence, the total failure probability of all these constraints is $6(M+2)\varepsilon_a$. To conclude, with the help of the linear programming in Equation (A41), one can calculate the upper-bound of n_{ph}.

For simplicity's sake, we give the analytical solution of this linear programming below. We divide n_{ph} into two parts, say

$$n_{ph} = n_{0|2\mu} + \sum_{j=2,4,6} n_{j|2\mu}. \tag{A42}$$

According to the inequality $|C_{0,\mu}n_0 - C^0_{2\mu}n_{0|2\mu}| \leq \triangle^0_{0\mu}$, we can obtain that the bounds of $n_{0|2\mu}$ are

$$\overline{n_{0|2\mu}} = \frac{C_{0,\mu}n_0 + \triangle^0_{0\mu}}{C^0_{2\mu}}, \tag{A43}$$

$$\underline{n_{0|2\mu}} = \frac{C_{0,\mu}n_0 - \triangle^0_{0\mu}}{C^0_{2\mu}}. \tag{A44}$$

Similarly, with the inequality $|C_{0,\nu}n_0 - C^0_{2\nu}n_{0|2\nu}| \leq \triangle^0_{0\nu}$, we have the bounds of $n_{0|2\nu}$, i.e.,

$$\overline{n_{0|2\nu}} = \frac{C_{0,\nu}n_0 + \triangle^0_{0\nu}}{C^0_{2\nu}}, \tag{A45}$$

$$\underline{n_{0|2\nu}} = \frac{C_{0,\nu}n_0 - \triangle^0_{0\nu}}{C^0_{2\nu}}. \tag{A46}$$

Besides the bound $\overline{n_{0|2\mu}}$, we need to calculate the upper bound of $\sum_{j=2,4,6} n_{j|2\mu}$ which we derive below. If we set $\mu > \nu$ and $P_\mu > P_\nu$, according to Eq A33, we have

$$\begin{aligned} C_{j|2\mu} &= \frac{P^2_\nu \tilde{P}_{j|2\nu}}{P^2_\mu \tilde{P}_{j|2\mu}}, \\ C_{j|2\nu} &= 1, \end{aligned} \tag{A47}$$

for $j \geq 1$. Hence, $n_{j|2\nu} \leq \frac{P^2_\nu \tilde{P}_{j|2\nu}}{P^2_\mu \tilde{P}_{j|2\mu}} n_{j|2\mu} + \triangle^j_{\mu\nu}$ where $j \geq 1$ hold. Then, combing with the equality $n_{2\nu} = \sum_{j=0}^{M} n_{j|2\nu}$, we have

$$\sum_{j=1,3,5,7} \frac{P^2_\nu \tilde{P}_{j|2\nu}}{P^2_\mu \tilde{P}_{j|2\mu}} n_{j|2\mu} + \sum_{j=2,4,6} \frac{P^2_\nu \tilde{P}_{j|2\nu}}{P^2_\mu \tilde{P}_{j|2\mu}} n_{j|2\mu} \geq n_{2\nu} - \sum_{j=1}^{7} \triangle^j_{\mu\nu} - \overline{n_{0|2\nu}}. \tag{A48}$$

It is easy to prove that

$$\frac{P^2_\nu \tilde{P}_{j|2\nu}}{P^2_\mu \tilde{P}_{j|2\mu}} \geq \frac{P^2_\nu \tilde{P}_{j+1|2\nu}}{P^2_\mu \tilde{P}_{j+1|2\mu}} \tag{A49}$$

for $j \geq 1$ holds in the case of $\mu > \nu$ and $P_\mu > P_\nu$. Consequently, we can know that

$$\frac{P^2_\nu \tilde{P}_{1|2\nu}}{P^2_\mu \tilde{P}_{1|2\mu}} \Big(\sum_{j=1,3,5,7} n_{j|2\mu} \Big) + \frac{P^2_\nu \tilde{P}_{2|2\nu}}{P^2_\mu \tilde{P}_{2|2\mu}} \Big(\sum_{j=2,4,6} n_{j|2\mu} \Big) \geq n_{2\nu} - \sum_{j=1}^{7} \triangle^j_{\mu\nu} - \overline{n_{0|2\nu}}. \tag{A50}$$

Finally, combing with the equality $\sum_{j=0}^{M-1} n_{j|2\mu} = n_{2\mu}$, Equations (A44) and (A46), we obtain the upper bound given by

$$\sum_{j=2,4,6} n_{j|2\mu} \leq \frac{\frac{P^2_\nu \tilde{P}_{1|2\nu}}{P^2_\mu \tilde{P}_{1|2\mu}} n_{2\mu} - n_{2\nu} + \sum_{j=1}^{7} \triangle^j_{\mu\nu} + \frac{C_{0,\nu}n_0 + \triangle^0_{0\nu}}{C^0_{2\nu}} - \frac{C_{0,\mu}n_0 - \triangle^0_{0\mu}}{C^0_{2\mu}} \frac{P^2_\nu \tilde{P}_{1|2\nu}}{P^2_\mu \tilde{P}_{1|2\mu}}}{\frac{P^2_\nu \tilde{P}_{1|2\nu}}{P^2_\mu \tilde{P}_{1|2\mu}} - \frac{P^2_\nu \tilde{P}_{2|2\nu}}{P^2_\mu \tilde{P}_{2|2\mu}}}. \tag{A51}$$

Finally, we have the upper bound of n_{ph}, say

$$n^U_{ph} = \frac{\frac{P^2_\nu \tilde{P}_{1|2\nu}}{P^2_\mu \tilde{P}_{1|2\mu}} n_{2\mu} - n_{2\nu} + \sum_{j=1}^{7} \triangle^j_{\mu\nu} + \frac{C_{0,\nu}n_0 + \triangle^0_{0\nu}}{C^0_{2\nu}} - \frac{C_{0,\mu}n_0 - \triangle^0_{0\mu}}{C^0_{2\mu}} \frac{P^2_\nu \tilde{P}_{1|2\nu}}{P^2_\mu \tilde{P}_{1|2\mu}}}{\frac{P^2_\nu \tilde{P}_{1|2\nu}}{P^2_\mu \tilde{P}_{1|2\mu}} - \frac{P^2_\nu \tilde{P}_{2|2\nu}}{P^2_\mu \tilde{P}_{2|2\mu}}} + \frac{C_{0,\mu}n_0 + \triangle^0_{0\mu}}{C^0_{2\mu}}. \tag{A52}$$

References

1. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661. [CrossRef] [PubMed]
2. 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, 9–12 December 1984 .
3. Mayers, D. Unconditional Security in Quantum Cryptography. *J. ACM* **2001**, *48*, 351–406. [CrossRef]
4. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [CrossRef]
5. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]
6. Dixon, A.; Dynes, J.; Lucamarini, M.; Fröhlich, B.; Sharpe, A.; Plews, A.; Tam, S.; Yuan, Z.; Tanizawa, Y.; Sato, H.; et al. High speed prototype quantum key distribution system and long term field trial. *Opt. Express* **2015**, *23*, 7583–7592. [CrossRef]
7. Yin, H.L.; Chen, T.Y.; Yu, Z.W.; Liu, H.; You, L.X.; Zhou, Y.H.; Chen, S.J.; Mao, Y.; Huang, M.Q.; Zhang, W.J.; et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **2016**, *117*, 190501. [CrossRef]
8. Zhou, Y.H.; Yu, Z.W.; Wang, X.B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **2016**, *93*, 042324. [CrossRef]
9. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.P.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [CrossRef]
10. Boaron, A.; Boso, G.; Rusca, D.; Vulliez, C.; Autebert, C.; Caloz, M.; Perrenoud, M.; Gras, G.; Bussières, F.; Li, M.J.; et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **2018**, *121*, 190502. [CrossRef] [PubMed]
11. Poppe, A.; Peev, M.; Maurhart, O. Outline of the SECOQC quantum-key-distribution network in Vienna. *Int. J. Quantum Inf.* **2008**, *6*, 209–218. [CrossRef]
12. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Miki, S.; Yamashita, T.; Wang, Z.; Tanaka, A.; et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409. [CrossRef] [PubMed]
13. Wang, S.; Chen, W.; Yin, Z.Q.; Li, H.W.; He, D.Y.; Li, Y.H.; Zhou, Z.; Song, X.T.; Li, F.Y.; Wang, D.; et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **2014**, *22*, 21739–21756. [CrossRef]
14. Chen, Y.A.; Zhang, Q.; Chen, T.Y.; Cai, W.Q.; Liao, S.K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.G.; Chen, Z.; et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **2021**, *589*, 214–219. [CrossRef] [PubMed]
15. Takeoka, M.; Guha, S.; Wilde, M.M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **2014**, *5*, 1–7. [CrossRef] [PubMed]
16. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 1–15. [CrossRef]
17. Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
18. Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
19. Wang, X.B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
20. 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:1805.05511.
21. Ma, X.; Zeng, P.; Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
22. Curty, M.; Azuma, K.; Lo, H.K. Simple security proof of twin-field type quantum key distribution protocol. *NPJ Quantum Inf.* **2019**, *5*, 1–6. [CrossRef]
23. 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]
24. Lin, J.; Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **2018**, *98*, 042332. [CrossRef]
25. Yin, H.L.; Fu, Y. Measurement-device-independent twin-field quantum key distribution. *Sci. Rep.* **2019**, *9*, 1–13. [CrossRef] [PubMed]
26. 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*, 1–7. [CrossRef]
27. Minder, M.; Pittaluga, M.; Roberts, G.; Lucamarini, M.; Dynes, J.; Yuan, Z.; Shields, A. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photonics* **2019**, *13*, 334–338. [CrossRef]
28. Pittaluga, M.; Minder, M.; Lucamarini, M.; Sanzaro, M.; Woodward, R.I.; Li, M.J.; Yuan, Z.; Shields, A.J. 600-km repeater-like quantum communications with dual-band stabilization. *Nat. Photonics* **2021**, *15*, 530–535. [CrossRef]
29. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.J.; Han, Z.Y.; Ma, S.Z.; Hu, X.L.; Li, Y.H.; Liu, H.; et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nat. Photonics* **2021**, *5*, 570–575. [CrossRef]
30. 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]
31. 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]

32. 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]
33. 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]
34. 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]
35. Yin, Z.Q.; Lu, F.Y.; Teng, J.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Twin-field protocols: Towards intercity quantum key distribution without quantum repeaters. *Fundam. Res.* **2021**, *1*, 93–95. [CrossRef]
36. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
37. Kwek, L.C.; Cao, L.; Luo, W.; Wang, Y.; Sun, S.; Wang, X.; Liu, A.Q. Chip-based quantum key distribution. *AAPPS Bull.* **2021**, *31*, 1–8. [CrossRef]
38. Fan-Yuan, G.J.; Wang, S.; Yin, Z.Q.; Chen, W.; He, D.Y.; Guo, G.C.; Han, Z.F. Afterpulse analysis for passive decoy quantum key distribution. *Quantum Eng.* **2020**, *2*, e56. [CrossRef]
39. 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]
40. 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] [PubMed]
41. Abellán, C.; Amaya, W.; Jofre, M.; Curty, M.; Acín, A.; Capmany, J.; Pruneri, V.; Mitchell, M. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Opt. Express* **2014**, *22*, 1645–1654. [CrossRef]
42. 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]
43. Curras Lorenzo, G.; Wooltorton, L.; Razavi, M. Twin-field quantum key distribution with fully discrete phase randomization. *Phys. Rev. Appl.* **2020**, *15*, 014016. [CrossRef]
44. 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]
45. Ben-Or, M.; Horodecki, M.; Leung, D.W.; Mayers, D.; Oppenheim, J. The universal composable security of quantum key distribution. In Proceedings of the Theory of Cryptography Conference, Cambridge, MA, USA, 10–12 February 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 386–406.
46. Müller-Quade, J.; Renner, R. Composability in quantum cryptography. *New J. Phys.* **2009**, *11*, 085006. [CrossRef]
47. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *New J. Phys.* **2009**, *11*, 045018. [CrossRef]
48. 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]
49. Currás-Lorenzo, G.; Navarrete, Á.; Azuma, K.; Kato, G.; Curty, M.; Razavi, M. Tight finite-key security for twin-field quantum key distribution. *NPJ Quantum Inf.* **2021**, *7*, 1–9. [CrossRef]
50. Ivanovic, I.D. How to differentiate between non-orthogonal states. *Phys. Lett. A* **1987**, *123*, 257–259. [CrossRef]
51. Maeda, K.; Sasaki, T.; Koashi, M. Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. *Nat. Commun.* **2019**, *10*, 1–8. [CrossRef] [PubMed]
52. Zhang, Z.; Zhao, Q.; Razavi, M.; Ma, X. Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Phys. Rev. A* **2017**, *95*, 012333. [CrossRef]