Improved security analysis for phase-encoding twin-field quantum key distribution

Yang-Guang Shan,[1,2] Yao Zhou,[1,2] Zhen-Qiang Yin,[1,2,3,*] Shuang Wang,[1,2,3,†]
Wei Chen,[1,2,3] De-Yong He,[1,2,3] Guang-Can Guo,[1,2,3] and Zheng-Fu Han[1,2,3]

[1] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, China*
[2] *CAS Center for Excellence in Quantum Information and Quantum Physics,*
University of Science and Technology of China, Hefei, Anhui 230026, China
[3] *Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

(Received 15 April 2024; accepted 8 July 2024; published 22 July 2024)

Twin-field (TF) quantum key distribution (QKD) has been extensively researched because of its long transmission distance. The phase-encoding TF-QKD can realize both a high key rate and a long transmission distance, so it has attracted a lot of attention. In this article, we are inspired by the sending-or-not-sending TF-QKD, in which the information leakages of correct rounds and erroneous rounds are calculated separately. And, we notice that this kind of method has been used in many QKD protocols—for example, the six-state QKD. We apply a similar method to the phase-matching TF-QKD and find some improvement in it. With the new analysis, the transmission distance can be improved without any changes in experiments. We also apply the new analysis in the four-phase partial-phase-postselection protocol, and a similar improvement can be achieved.

DOI: 10.1103/PhysRevA.110.012450

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] could help to establish secret communication between two distant peers (Alice and Bob) by sharing private keys remotely. QKD is of high practicability with the present technology and has been the subject of wide concern in the last few decades.

In the pursuit of a long distance and a high key rate, twin-field (TF) QKD [3] is a landmark invention. Before the appearance of TF-QKD, the PLOB bound [4,5] gives a linear key rate limitation for point-to-point QKD protocols, in which the key rate decreases linearly with the transmittance of the channel [$R \leqslant O(\eta)$] (see another bound called TGW bound in Ref. [6]). TF-QKD is the first protocol that can break the PLOB bound without a quantum repeater to realize a key rate of $O(\sqrt{\eta})$ level. With this advantage, TF-QKD is suitable for long-distance key distribution, so it has been extensively researched both in theory [7–11] and experiments [12–24].

The variants of TF-QKD can be divided into two kinds, sending-or-not-sending (SNS) TF-QKD [8] and phase-encoding TF-QKD [7,9–11]. In SNS-TF-QKD, the information is encoded in the selection of sending a vacuum state or a weak coherent state. In phase-encoding TF-QKD, the information is encoded in the phase of a weak coherent state. We noticed that in the analysis of the SNS-TF-QKD, the information leakages of the correct rounds and erroneous rounds are estimated separately. The phase error rate of erroneous rounds can be directly set to 50% and one only needs to estimate the phase error rate of correct rounds.

In phase-encoding QKD protocols, the security analysis is usually conducted by treating all rounds as a whole. In this article, we try to analyze the information leakage of correct rounds and erroneous rounds separately. We give our improved security analysis for the phase-matching (PM) TF-QKD [7] and the four-phase partial-phase-postselection (FP-PPP) TF-QKD [25]. We conducted numerical simulations to see the improvement of our analysis. For both PM-TF-QKD and FP-PPP-TF-QKD, our analysis could improve the channel loss tolerance of about 1.5 dB. Though the improvement seems not so large, our analysis could bring this improvement without any changes in experiments.

This article is organized as follows. In Sec. II, we give our improved analysis for the PM-TF-QKD. In Sec. III, we give our improved analysis for the FP-PPP-TF-QKD. In Sec. IV, we introduce the result of our simulation. Finally, we come to a conclusion in Sec. V.

II. IMPROVED ANALYSIS FOR THE PHASE-MATCHING TF-QKD

A. Protocol description

Firstly, we review the process of the PM-TF-QKD for the completeness of the article. We describe a case of infinite decoy states [26–28] below. For a realistic case, two intensities of decoy states are enough to realize a good performance [29].

(1) *State preparation.* For each round, Alice (Bob) randomly selects an intensity $\mu_I \in \{\mu, \nu_1, \nu_2, \dots\}$ with probabilities $\{p_\mu, p_{\nu_1}, p_{\nu_2}, \dots\}$ separately. The intensity μ corresponds to the signal state and the intensities $\nu_1, \nu_2, \dots$ correspond to decoy states. Alice (Bob) randomly prepares a state $|\sqrt{\mu_I} e^{i(\theta_A + s_A \pi)}\rangle$ ($|\sqrt{\mu_I} e^{i(\theta_B + s_B \pi)}\rangle$), where θ_A (θ_B) is randomly selected in $[0, 2\pi)$ and s_A (s_B) is randomly selected in $\{0, 1\}$. She (he) records θ_A and s_A (θ_B and s_B) locally. Then, Alice and Bob send the states to Charlie, who is located in the middle of the channel.

[*] Contact author: yinzq@ustc.edu.cn

[†] Contact author: wshuang@ustc.edu.cn

(2) *State measurement.* If Charlie is honest, he will measure the states from Alice and Bob in an interferometer and use two single-photon detectors to detect the outputs. We assume that the left detector corresponds to constructive interference and the right detector corresponds to destructive interference. Then, Charlie will declare a left click (only the left detector clicks), a right click (only the right detector clicks), or a failed measurement (both detectors click or no clicks) according to the clicks of the detectors. Left clicks and right clicks are collectively called successful clicks and the corresponding rounds are called successful rounds. For the rounds with right clicks, Bob flips his corresponding local key bits s_B.

(3) *Intensity sifting.* After enough rounds of the first two steps, Alice and Bob announce their choices of intensities of all rounds. For the rounds where both Alice and Bob choose the signal intensity μ, the key bits s_A and s_B are kept as the raw key bits. The rounds where Alice and Bob choose the same decoy intensity ν_i $(i = 1, 2, \dots)$ are also kept as decoy rounds, which will be used in the parameter estimation.

(4) *Phase postselection.* Alice and Bob announce the phases θ_A and θ_B of each round that has passed the intensity sifting. If $|\theta_A - \theta_B| \leqslant \Delta$ or $||\theta_A - \theta_B| - 2\pi| \leqslant \Delta$, they keep the round. If $||\theta_A - \theta_B| - \pi| \leqslant \Delta$, they also keep the round, and Bob flips his local key bit s_B.

(5) *Parameter estimation and postprocessing.* Alice and Bob announce s_A and s_B of decoy rounds. They count the click rates and error rates of decoy rounds to estimate the phase error rates of signal states. Then, Alice and Bob conduct error correction and privacy amplification to the raw key bits s_A and s_B of successful signal rounds that have passed the phase postselection to generate the final key.

B. The improved security analysis

In the phase postselection step, when the phases of Alice and Bob are opposite ($||\theta_A - \theta_B| - \pi| \leqslant \Delta$), the phase of Bob's state becomes $\theta_B + (s_B + 1)\pi$ after the flip of s_B. We can define $\theta_B' = \theta_B + \pi$ and the phase of Bob becomes $\theta_B' + s_B\pi$. Then, we have $|\theta_A - \theta_B'| \leqslant \Delta$ or $||\theta_A - \theta_B'| - 2\pi| \leqslant \Delta$. This case is equivalent to the case where θ_A and θ_B are close at the state preparation step. We only need to analyze the case where θ_A and θ_B are close in the following.

Because the left-click events and right-click events can be separated by Alice and Bob, we can also analyze the security of left clicks and right clicks separately. In the following, we give the analysis of the left clicks. The analysis of right clicks is analogous.

Before the security analysis, we need to give the equivalent protocol based on entanglement. We define that $\delta = \theta_B - \theta_A$ and $\theta_A = \theta$. Then, the state of the equivalent protocol can be given as

$$|\psi(\theta,\delta)\rangle = \frac{1}{2}(|0\rangle_A |\sqrt{\mu}e^{i\theta}\rangle_a + |1\rangle_A |\sqrt{\mu}e^{i(\theta+\pi)}\rangle_a) \otimes (|0\rangle_B |\sqrt{\mu}e^{i(\theta+\delta)}\rangle_b + |1\rangle_B |\sqrt{\mu}e^{i(\theta+\delta+\pi)}\rangle_b), \tag{1}$$

where the subscripts A, B correspond to the local ancillas of Alice and Bob, and the subscripts a, b correspond to the states prepared and sent out by Alice and Bob. The phase θ is randomly chosen from $[0, 2\pi)$ and the phase δ is randomly chosen from $[-\Delta, \Delta]$. After the preparation of this state, if Alice and Bob measure their ancillas on the $\mathbb{Z}$ basis ($|0\rangle$ and $|1\rangle$), the measurement results correspond to s_A and s_B of the state preparation step. If they measure on the $\mathbb{X}$ basis ($|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$), the error rates of successful rounds are related to the potential information leakage to an eavesdropper. Thus, the core of the security analysis is estimating the error rate when they measure on the $\mathbb{X}$ basis.

We define that in $\mathbb{C}$ rounds, the encoding bits s_A and s_B of Alice and Bob are the same, and in $\mathbb{E}$ rounds s_A and s_B are opposite. The key length of the protocol can be given from the Devetak-Winter bound [30], which is shown as

$$\begin{aligned} l &= I(\mathbb{Z}_\mathbb{C}\mathbb{Z}_\mathbb{E} : B) - I(\mathbb{Z}_\mathbb{C}\mathbb{Z}_\mathbb{E} : E) \\ &= H(\mathbb{Z}_\mathbb{C}\mathbb{Z}_\mathbb{E}|E) - H(\mathbb{Z}_\mathbb{C}\mathbb{Z}_\mathbb{E}|B) \\ &= H(\mathbb{Z}_\mathbb{C}|\mathbb{Z}_\mathbb{E}E) + H(\mathbb{Z}_\mathbb{E}|E) - H(\mathbb{Z}_\mathbb{C}\mathbb{Z}_\mathbb{E}|B), \end{aligned} \tag{2}$$

where $I(\cdot:\cdot)$ is the quantum mutual information and $H(\cdot|\cdot)$ is the quantum conditional entropy [31]. The second equality is from the definition of mutual information and the third equality is from the definition of conditional entropy. $\mathbb{Z}_\mathbb{C}$ corresponds to Alice's information of successful-click $\mathbb{C}$ rounds measured by the $\mathbb{Z}$ basis, and $\mathbb{Z}_\mathbb{E}$ is similarly defined. Note that $\mathbb{Z}_\mathbb{C}$ and $\mathbb{Z}_\mathbb{E}$ only include the information of signal rounds in which both Alice and Bob select the intensity μ. E is the system of eavesdroppers and B is the system of Bob. The term $H(\mathbb{Z}_\mathbb{C}\mathbb{Z}_\mathbb{E}|B)$ corresponds to the consumption from error correction and we will discuss it later.

From the uncertainty relations of the quantum entropy [32,33], the first two terms of Eq. (2) can be converted to Alice's information measured by the $\mathbb{X}$ basis conditioned on Bob's system, which is shown as

$$\begin{aligned} &H(\mathbb{Z}_\mathbb{C}|\mathbb{Z}_\mathbb{E}E) + H(\mathbb{Z}_\mathbb{E}|E) \\ &\quad \geqslant n_\mathbb{C} - H(\mathbb{X}_\mathbb{C}|B) + n_\mathbb{E} - H(\mathbb{X}_E|B) \\ &\quad \geqslant n_\mathbb{C}\left[1 - H_2\left(e_{\text{ph}}^\mathbb{C}\right)\right] + n_\mathbb{E}\left[1 - H_2\left(e_{\text{ph}}^\mathbb{E}\right)\right], \end{aligned} \tag{3}$$

where $\mathbb{X}_\mathbb{C}$ corresponds to Alice's information of successful-click $\mathbb{C}$ rounds measured by the $\mathbb{X}$ basis. We use the uncertainty relation twice for the first inequality, and for the first term, we can treat the subsystems $\mathbb{Z}_\mathbb{E}$ and E as a whole. Thus, the uncertainty relation can be directly used. $n_\mathbb{C}$ is the number of successful-click $\mathbb{C}$ signal rounds and $n_\mathbb{E}$ is the number of successful-click $\mathbb{E}$ signal rounds. $e_{\text{ph}}^\mathbb{C}$ and $e_{\text{ph}}^\mathbb{E}$ are the corresponding phase error rates. $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function. The following analysis aims to estimate these two phase error rates.

The $\mathbb{C}$ rounds correspond to the case where $s_A = s_B$ in the analysis of left clicks. To estimate their phase error rate, we should give the state of $\mathbb{C}$ rounds by operating $|00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB}$ on Eq. (1), which is shown as

$$\begin{aligned} &(|00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB})|\psi(\theta,\delta)\rangle \\ &\quad = \frac{1}{2}(|00\rangle_{AB}|\sqrt{\mu}e^{i\theta}\rangle_a|\sqrt{\mu}e^{i(\theta+\delta)}\rangle_b \\ &\qquad + |11\rangle_{AB}|\sqrt{\mu}e^{i(\theta+\pi)}\rangle_a|\sqrt{\mu}e^{i(\theta+\delta+\pi)}\rangle_b). \end{aligned} \tag{4}$$

If Alice and Bob measure their ancillas on the $\mathbb{X}$ basis, we define that $|+-\rangle_{AB}$, $|-+\rangle_{AB}$ correspond to correct results and $|++\rangle_{AB}$, $|--\rangle_{AB}$ correspond to phase errors. Operating $|++\rangle\langle++|_{AB} + |--\rangle\langle--|_{AB}$ on Eq. (4), the state becomes $\frac{|00\rangle_{AB}+|11\rangle_{AB}}{\sqrt{2}} \otimes \frac{|\sqrt{\mu}e^{i\theta}\rangle_a|\sqrt{\mu}e^{i(\theta+\delta)}\rangle_b+|\sqrt{\mu}e^{i(\theta+\pi)}\rangle_a|\sqrt{\mu}e^{i(\theta+\delta+\pi)}\rangle_b}{2\sqrt{2}}$. Thus, the probability of a phase error can be estimated as

$$P_{\mathrm{ph}}^{L\mathbb{C}}(\theta,\delta) = P^L\left(\frac{|\sqrt{\mu}\mathrm{e}^{i\theta}\rangle_a|\sqrt{\mu}\mathrm{e}^{i(\theta+\delta)}\rangle_b + |\sqrt{\mu}\mathrm{e}^{i(\theta+\pi)}\rangle_a|\sqrt{\mu}\mathrm{e}^{i(\theta+\delta+\pi)}\rangle_b}{2\sqrt{2}}\right), \tag{5}$$

where $P^L(|\cdot\rangle)$ [or $P^L(\rho)$] is the left-click rate when a state $|\cdot\rangle$ (with the density matrix ρ) is sent by Alice and Bob. For the unnormalized state, we define $P^L(c\,|\cdot\rangle) = |c|^2 P^L(|\cdot\rangle)$ [$P^L(r\rho) = rP^L(\rho)$, r is a real number]. Note that $P^L(\rho_1) + P^L(\rho_2) = P^L(\rho_1 + \rho_2)$.

Note that the probability of a $\mathbb{C}$ round (equal to $1/2$) has been included in Eq. (5), because of the unnormalized probability from Eq. (4).

Since θ and δ are randomized in all rounds, we can get the average phase error probability in Eq. (6), where $\mathcal{P}[|\cdot\rangle] = |\cdot\rangle\langle\cdot|$. Thus, the phase error probability can be estimated by a linear combination of click rates of even-photon states. Every term of the $P_{\mathrm{ph}}^{L\mathbb{C}}$ can be estimated with decoy states shown in the Appendix.

$$\begin{aligned}
P_{\mathrm{ph}}^{L\mathbb{C}} &= \frac{1}{4\Delta\pi}\int_{-\Delta}^{\Delta} d\delta \int_0^{2\pi} d\theta P_{\mathrm{ph}}^{L\mathbb{C}}(\theta,\delta)\\
&= P^L\left(\frac{1}{4\Delta\pi}\int_{-\Delta}^{\Delta} d\delta \int_0^{2\pi} d\theta \mathcal{P}\left[\frac{|\sqrt{\mu}\mathrm{e}^{i\theta}\rangle_a|\sqrt{\mu}\mathrm{e}^{i(\theta+\delta)}\rangle_b + |\sqrt{\mu}\mathrm{e}^{i(\theta+\pi)}\rangle_a|\sqrt{\mu}\mathrm{e}^{i(\theta+\delta+\pi)}\rangle_b}{2\sqrt{2}}\right]\right)\\
&= P^L\left(\frac{1}{4\Delta\pi}\int_{-\Delta}^{\Delta} d\delta \int_0^{2\pi} d\theta \frac{1}{2}\mathcal{P}\left[\sum_{\substack{n=0\\ n\text{ is even}}}^{\infty}\sqrt{\frac{\mathrm{e}^{-2\mu}(2\mu)^n}{n!}}\mathrm{e}^{in\theta}\sum_{j=0}^{n}\frac{\sqrt{\binom{n}{j}}\mathrm{e}^{i(n-j)\delta}|j\rangle_a|n-j\rangle_b}{\sqrt{2^n}}\right]\right)\\
&= \frac{1}{2}\sum_{\substack{n=0\\ n\text{ is even}}}^{\infty}\frac{\mathrm{e}^{-2\mu}(2\mu)^n}{n!}P^L\left(\frac{1}{2\Delta}\int_{-\Delta}^{\Delta} d\delta\mathcal{P}\left[\sum_{j=0}^{n}\frac{\sqrt{\binom{n}{j}}\mathrm{e}^{i(n-j)\delta}|j\rangle_a|n-j\rangle_b}{\sqrt{2^n}}\right]\right)
\end{aligned} \tag{6}$$

The phase error estimation of $\mathbb{E}$ rounds is a little more complex. Firstly, the state of the $\mathbb{E}$ rounds can be given as

$$\begin{aligned}
&(|01\rangle\langle01|_{AB} + |10\rangle\langle10|_{AB})|\psi(\theta,\delta)\rangle\\
&= \frac{1}{2}(|01\rangle_{AB}|\sqrt{\mu}\mathrm{e}^{i\theta}\rangle_a|\sqrt{\mu}\mathrm{e}^{i(\theta+\delta+\pi)}\rangle_b\\
&\quad + |10\rangle_{AB}|\sqrt{\mu}\mathrm{e}^{i(\theta+\pi)}\rangle_a|\sqrt{\mu}\mathrm{e}^{i(\theta+\delta)}\rangle_b).
\end{aligned} \tag{7}$$

In this case, it is not easy to judge which group has a larger click rate, the $|++\rangle_{AB}$, $|--\rangle_{AB}$ group or the $|+-\rangle_{AB}$, $|-+\rangle_{AB}$ group. The $|++\rangle_{AB}$, $|--\rangle_{AB}$ group corresponds to the destructive interference of even photons. The $|+-\rangle_{AB}$, $|-+\rangle_{AB}$ group corresponds to the destructive interference of odd photons. When the protocol runs on a normal transmission distance, the click rate of the single-photon term is larger than others, so defining $|++\rangle_{AB}$ and $|--\rangle_{AB}$ as errors is a good choice. However, when the protocol runs on an extremely long distance, the click rate of the zero-photon term becomes larger because of the dark counts, so we need to define $|+-\rangle_{AB}$ and $|-+\rangle_{AB}$ as errors. In the following, we give the phase error probabilities of these two cases separately.

With a similar calculation of the $\mathbb{C}$ rounds, when $|++\rangle_{AB}$ and $|--\rangle_{AB}$ are defined as errors the phase error probability is shown in Eq. (8), and when $|+-\rangle_{AB}$ and $|-+\rangle_{AB}$ are defined as errors the phase error probability is shown in Eq. (9). These two equations can be obtained by calculating the measuring probability of the projectors $|++\rangle\langle++|_{AB}$ and $|--\rangle\langle--|_{AB}$ and the measuring probability of the projectors $|+-\rangle\langle+-|_{AB}$ and $|-+\rangle\langle-+|_{AB}$ on Eq. (7),

$$P_{\mathrm{ph1}}^{L\mathbb{E}} = \frac{1}{2}\sum_{\substack{n=0\\ n\text{ is even}}}^{\infty}\frac{\mathrm{e}^{-2\mu}(2\mu)^n}{n!}P^L\left(\frac{1}{2\Delta}\int_{-\Delta}^{\Delta} d\delta\mathcal{P}\left[\sum_{j=0}^{n}\frac{(-1)^{n-j}\sqrt{\binom{n}{j}}\mathrm{e}^{i(n-j)\delta}|j\rangle_a|n-j\rangle_b}{\sqrt{2^n}}\right]\right). \tag{8}$$

$$P_{\mathrm{ph2}}^{L\mathbb{E}} = \frac{1}{2}\sum_{\substack{n=0\\ n\text{ is odd}}}^{\infty}\frac{\mathrm{e}^{-2\mu}(2\mu)^n}{n!}P^L\left(\frac{1}{2\Delta}\int_{-\Delta}^{\Delta} d\delta\mathcal{P}\left[\sum_{j=0}^{n}\frac{(-1)^{n-j}\sqrt{\binom{n}{j}}\mathrm{e}^{i(n-j)\delta}|j\rangle_a|n-j\rangle_b}{\sqrt{2^n}}\right]\right). \tag{9}$$

Every term of the average click rates can be estimated with decoy states, which is shown in the Appendix.

With the phase error probabilities above, we can give the expression of the final key rate $R^L = l^L/N$, where N is the total number of pulses sent by Alice and l^L is the key length from Eqs. (2) and (3) of the left clicks. The error correction consumption can be estimated by the bit error rate e_{bit}, which is shown as $H(\mathbb{Z}_{\mathbb{C}}\mathbb{Z}_{\mathbb{E}}|B) \leqslant f(n_{\mathbb{C}} + n_{\mathbb{E}})H_2(e_{\text{bit}})$, where f is the efficiency of error correction. The key rate is shown as

$$R^L \geqslant \frac{2\Delta p_\mu^2}{\pi}\left\{P_{\mathbb{C}}^L\left[1 - H_2\left(\frac{P_{\text{ph}}^{L\mathbb{C}}}{P_{\mathbb{C}}^L}\right)\right]\right. \\ \left. + P_{\mathbb{E}}^L\left[1 - H_2\left(\frac{\min\left(P_{\text{ph1}}^{L\mathbb{E}}, P_{\text{ph2}}^{L\mathbb{E}}\right)}{P_{\mathbb{E}}^L}\right)\right] - fP_{\text{tot}}^L H_2\left(e_{\text{bit}}^L\right)\right\}, \tag{10}$$

where $\frac{2\Delta}{\pi}$ is the efficiency of phase postselection, $P_{\mathbb{C}}^L$ ($P_{\mathbb{E}}^L$) is the correct (erroneous) left-click rate when a round has passed the phase postselection, $P_{\text{tot}}^L = P_{\mathbb{C}}^L + P_{\mathbb{E}}^L$ is the total left-click rate when a round has passed the phase postselection, and e_{bit}^L is the bit error rate of left clicks.

P_{tot}^L can be easily obtained by counting the number of successful rounds that passed the phase postselection. After the error correction step, Alice and Bob naturally know the bit error rate e_{bit}^L. Then, $P_{\mathbb{C}}^L = (1 - e_{\text{bit}}^L)P_{\text{tot}}^L$ and $P_{\mathbb{E}}^L = e_{\text{bit}}^L P_{\text{tot}}^L$ can be easily obtained.

III. IMPROVED ANALYSIS FOR THE FOUR-PHASE PARTIAL PHASE POSTSELECTION PROTOCOL

Since there are some quantities representing similar meanings in the PM-TF-QKD and the FP-PPP-TF-QKD, we may use some of the same quantity names from Sec. (II) in the following without causing any confusion.

A. Protocol description

The four-phase TF-QKD is proposed in Ref. [34], and has been experimentally verified in Ref. [23]. Then, the partial phase postselection is introduced in Ref. [25] to realize both a long distance and a high key rate. Here, we review the process of this protocol. Since this protocol is similar to the PM-TF-QKD in some steps, we only give the difference between them in the following.

(1) *State preparation.* For each round, Alice (Bob) randomly selects an intensity $\mu_I \in \{\mu, \nu_1, \nu_2, \dots\}$ with probabilities $\{p_\mu, p_{\nu_1}, p_{\nu_2}, \dots\}$ separately. The intensity μ corresponds to the signal state and the intensities $\nu_1, \nu_2, \dots$ correspond to decoy states. When Alice (Bob) selects the signal intensity μ, she (he) randomly prepares a state $|\sqrt{\mu}e^{i(s_A\pi + t_A\frac{\pi}{2})}\rangle$ [$|\sqrt{\mu}e^{i(s_B\pi + t_B\frac{\pi}{2})}\rangle$], where s_A (s_B) is randomly chosen from $\{0, 1\}$ and t_A (t_B) is also randomly chosen from $\{0, 1\}$. She (he) records s_A and t_A (s_B and t_B) locally. When she (he) selects the decoy intensity ν_i, she (he) prepares a state $|\sqrt{\nu_i}e^{i\theta_A}\rangle$ ($|\sqrt{\nu_i}e^{i\theta_B}\rangle$), where θ_A (θ_B) is randomly selected in $[0, 2\pi)$. She (he) records θ_A (θ_B) locally. Then, they send the states to Charlie, who is located in the middle of the channel.

(2) *State measurement.* The same as the PM-TF-QKD.

(3) *Intensity sifting.* The same as the PM-TF-QKD.

(4) *Phase postselection.* For the signal rounds that have passed the intensity sifting, Alice and Bob announce t_A and t_B of every round. If $t_A = t_B$, they keep the round. If $t_A \neq t_B$, they discard the round. For the decoy rounds that have passed the intensity sifting, Alice and Bob announce θ_A and θ_B of every round. They keep the rounds where $|\theta_A - \theta_B| \leqslant \Delta$ or $||\theta_A - \theta_B| - 2\pi| \leqslant \Delta$ and the rounds where $||\theta_A - \theta_B| - \pi| \leqslant \Delta$ separately [25].

(5) *Parameter estimation and postprocessing.* Alice and Bob count the click rates of decoy rounds to estimate the phase error rates of signal states. Then, they conduct error correction and privacy amplification to the raw key bits s_A and s_B of successful signal rounds that have passed the phase postselection to generate the final key.

B. The improved security analysis

In the following, we give the analysis of left clicks. The analysis of right clicks is analogous. Firstly, we give the equivalent protocol based on entanglement in the following. Because $t_A = t_B$ for the rounds that passed the phase postselection, we define $t_A = t_B = t$ in the following:

$$|\psi(t)\rangle = \frac{1}{2}(|0\rangle_A|\sqrt{\mu}e^{it\frac{\pi}{2}}\rangle_a + |1\rangle_A|\sqrt{\mu}e^{i(\pi+t\frac{\pi}{2})}\rangle_a) \\ \otimes (|0\rangle_B|\sqrt{\mu}e^{it\frac{\pi}{2}}\rangle_b + |1\rangle_B|\sqrt{\mu}e^{i(\pi+t\frac{\pi}{2})}\rangle_b), \tag{11}$$

where t is randomly chosen from $\{0, 1\}$ for each round.

With the same method shown in our analysis of the PM-TF-QKD, we can also separate all rounds into two parts. For left clicks, the $\mathbb{C}$ rounds correspond to the case where $s_A = s_B$, and the $\mathbb{E}$ rounds correspond to the case where $s_A \neq s_B$. We can analyze the information leakages of these two parts separately.

For $\mathbb{C}$ rounds, we define $|{+}{+}\rangle_{AB}$ and $|{-}{-}\rangle_{AB}$ as phase errors. The state of the $\mathbb{C}$ rounds can be obtained by operating $|00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB}$ on Eq. (11), which is shown as

$$\frac{1}{2}(|00\rangle_{AB}|\sqrt{\mu}e^{it\frac{\pi}{2}}\rangle_a|\sqrt{\mu}e^{it\frac{\pi}{2}}\rangle_b \\ + |11\rangle_{AB}|\sqrt{\mu}e^{i(\pi+t\frac{\pi}{2})}\rangle_a|\sqrt{\mu}e^{i(\pi+t\frac{\pi}{2})}\rangle_b). \tag{12}$$

The phase errors correspond to the measuring results of $|{+}{+}\rangle_{AB}$ and $|{-}{-}\rangle_{AB}$. Operating $|{+}{+}\rangle\langle{+}{+}|_{AB} + |{-}{-}\rangle\langle{-}{-}|_{AB}$ on Eq. (12), the state becomes $\frac{|00\rangle_{AB}+|11\rangle_{AB}}{\sqrt{2}} \otimes \frac{|\sqrt{\mu}e^{it\frac{\pi}{2}}\rangle_a|\sqrt{\mu}e^{it\frac{\pi}{2}}\rangle_b + |\sqrt{\mu}e^{i(\pi+t\frac{\pi}{2})}\rangle_a|\sqrt{\mu}e^{i(\pi+t\frac{\pi}{2})}\rangle_b}{2\sqrt{2}}$. Thus, the probability of a phase error can be estimated as

$$P_{\text{ph}}^{L\mathbb{C}}(t) = P^L\left(\frac{|\sqrt{\mu}e^{it\frac{\pi}{2}}\rangle_a|\sqrt{\mu}e^{it\frac{\pi}{2}}\rangle_b + |\sqrt{\mu}e^{i(\pi+t\frac{\pi}{2})}\rangle_a|\sqrt{\mu}e^{i(\pi+t\frac{\pi}{2})}\rangle_b}{2\sqrt{2}}\right). \tag{13}$$

Then, the average phase error probability for $t = 0, 1$ can be estimated in Eq. (14):

$$\begin{aligned}
P_{\rm ph}^{L\mathbb{C}} &= \frac{1}{2}\big[P_{\rm ph}^{L\mathbb{C}}(0) + P_{\rm ph}^{L\mathbb{C}}(1)\big]\\
&= \frac{1}{2}P^L\bigg[\mathcal{P}\bigg(\frac{|\sqrt{\mu}\rangle_a|\sqrt{\mu}\rangle_b + |{-\sqrt{\mu}}\rangle_a|{-\sqrt{\mu}}\rangle_b}{2\sqrt{2}}\bigg) + \mathcal{P}\bigg(\frac{|i\sqrt{\mu}\rangle_a|i\sqrt{\mu}\rangle_b + |{-i\sqrt{\mu}}\rangle_a|{-i\sqrt{\mu}}\rangle_b}{2\sqrt{2}}\bigg)\bigg]\\
&= \frac{1}{4}P^L\left[\mathcal{P}\left(\sum_{\substack{n=0\\ n \text{ is even}}}^{\infty}\sqrt{\frac{\mathrm{e}^{-2\mu}(2\mu)^n}{n!}}\sum_{j=0}^{n}\frac{\sqrt{\binom{n}{j}}\,|j\rangle_a|n-j\rangle_b}{\sqrt{2^n}}\right) + \mathcal{P}\left(\sum_{\substack{n=0\\ n \text{ is even}}}^{\infty}\sqrt{\frac{\mathrm{e}^{-2\mu}(2\mu)^n}{n!}}\,i^n\sum_{j=0}^{n}\frac{\sqrt{\binom{n}{j}}\,|j\rangle_a|n-j\rangle_b}{\sqrt{2^n}}\right)\right]\\
&= \frac{1}{2}P^L\left(\sum_{\substack{n=0\\ n\equiv 0 \mod 4}}^{\infty}\sqrt{\frac{\mathrm{e}^{-2\mu}(2\mu)^n}{n!}}\sum_{j=0}^{n}\frac{\sqrt{\binom{n}{j}}\,|j\rangle_a|n-j\rangle_b}{\sqrt{2^n}}\right) + \frac{1}{2}P^L\left(\sum_{\substack{n=0\\ n\equiv 2 \mod 4}}^{\infty}\sqrt{\frac{\mathrm{e}^{-2\mu}(2\mu)^n}{n!}}\sum_{j=0}^{n}\frac{\sqrt{\binom{n}{j}}\,|j\rangle_a|n-j\rangle_b}{\sqrt{2^n}}\right).
\end{aligned} \tag{14}$$

The phase error probability shown above is still hard to estimate, so we use the Cauchy-Schwarz inequality to give the upper bound of $P_{\rm ph}^{L\mathbb{C}}$. Note that the left-click rate of a state can be calculated with a measurement matrix M^L, which is shown as $P^L(|\cdot\rangle) = \mathrm{Tr}(M^L|\cdot\rangle\langle\cdot|)$ $[P^L(\rho) = \mathrm{Tr}(M^L\rho)]$. Thus, we have the inequality shown in Eq. (15) using the Cauchy-Schwarz inequality.

$$\begin{aligned}
P^L\left(\sum_n c_n|n\rangle\right) &= \mathrm{Tr}\left[M^L\left(\sum_n c_n|n\rangle\right)\left(\sum_m c_m^*\langle m|\right)\right]\\
&= \sum_n |c_n|^2\mathrm{Tr}(M^L|n\rangle\langle n|) + \sum_{m\neq n} c_nc_m^*\mathrm{Tr}(M^L|n\rangle\langle m|)\\
&\leqslant \sum_n |c_n|^2\mathrm{Tr}(M^L|n\rangle\langle n|) + \sum_{m\neq n}|c_nc_m|\sqrt{\mathrm{Tr}(M^L|n\rangle\langle n|)}\sqrt{\mathrm{Tr}(M^L|m\rangle\langle m|)}\\
&= \sum_n |c_n|^2P^L(|n\rangle) + \sum_{m\neq n}|c_nc_m|\sqrt{P^L(|n\rangle)}\sqrt{P^L(|m\rangle)}.
\end{aligned} \tag{15}$$

Applying Eq. (15) into Eq. (14), we can give the upper bound of the phase error probability, which is shown in Eq. (16). Note that in Eq. (16) every term is the same as the corresponding term in Eq. (6) when $\Delta = 0$. Thus, the phase errors can also be estimated by decoy states with a similar method. The decoy estimation with finite intensities can be seen in Ref. [25].

$$\begin{aligned}
P_{\rm ph}^{L\mathbb{C}} \leqslant{}& \frac{1}{2}\sum_{n=0}^{\infty}\frac{\mathrm{e}^{-2\mu}(2\mu)^{2n}}{(2n)!}P^L\left(\sum_{j=0}^{2n}\frac{\sqrt{\binom{2n}{j}}\,|j\rangle_a|2n-j\rangle_b}{\sqrt{2^{2n}}}\right)\\
&+ \frac{1}{2}\sum_{m\neq n}\mathrm{e}^{-2\mu}\sqrt{\frac{(2\mu)^{4m+4n}}{(4m)!(4n)!}}\sqrt{P^L\left(\sum_{j=0}^{4m}\frac{\sqrt{\binom{4m}{j}}\,|j\rangle_a|4m-j\rangle_b}{\sqrt{2^{4m}}}\right)}\sqrt{P^L\left(\sum_{j=0}^{4n}\frac{\sqrt{\binom{4n}{j}}\,|j\rangle_a|4n-j\rangle_b}{\sqrt{2^{4n}}}\right)}\\
&+ \frac{1}{2}\sum_{m\neq n}\mathrm{e}^{-2\mu}\sqrt{\frac{(2\mu)^{4m+4n+4}}{(4m+2)!(4n+2)!}}\sqrt{P^L\left(\sum_{j=0}^{4m+2}\frac{\sqrt{\binom{4m+2}{j}}\,|j\rangle_a|4m+2-j\rangle_b}{\sqrt{2^{4m+2}}}\right)}\sqrt{P^L\left(\sum_{j=0}^{4n+2}\frac{\sqrt{\binom{4n+2}{j}}\,|j\rangle_a|4n+2-j\rangle_b}{\sqrt{2^{4n+2}}}\right)}
\end{aligned} \tag{16}$$

For the $\mathbb{E}$ rounds, we also give the phase error probabilities for the two cases where when $|{+}{+}\rangle_{AB}$, $|{-}{-}\rangle_{AB}$ are defined as errors and when $|{+}{-}\rangle_{AB}$, $|{-}{+}\rangle_{AB}$ are defined as errors. Firstly, the state of the $\mathbb{E}$ rounds can be given as

$$(|01\rangle\,\langle 01|_{AB} + |10\rangle\,\langle 10|_{AB})\,|\psi(t)\rangle = \frac{1}{2}\big(|01\rangle_{AB}\,|\sqrt{\mu}\mathrm{e}^{it\frac{\pi}{2}}\rangle_a\,|\sqrt{\mu}\mathrm{e}^{i(\pi+t\frac{\pi}{2})}\rangle_b + |10\rangle_{AB}\,|\sqrt{\mu}\mathrm{e}^{i(\pi+t\frac{\pi}{2})}\rangle_a\,|\sqrt{\mu}\mathrm{e}^{it\frac{\pi}{2}}\rangle_b\big). \tag{17}$$

The calculation of these two phase error upper bounds is similar to the analysis above by calculating the measuring probability of the projectors $|{+}{+}\rangle\,\langle{+}{+}|_{AB}$ and $|{-}{-}\rangle\,\langle{-}{-}|_{AB}$ and the measuring probability of the projectors $|{+}{-}\rangle\,\langle{+}{-}|_{AB}$ and $|{-}{+}\rangle\,\langle{-}{+}|_{AB}$. The results are shown in Eqs. (18) and (19).

$$\begin{aligned}
P^{L\mathbb{E}}_{\mathrm{ph1}} \leqslant{}& \frac{1}{2}\sum_{n=0}^{\infty}\frac{\mathrm{e}^{-2\mu}(2\mu)^{2n}}{(2n)!}P^L\left(\sum_{j=0}^{2n}\frac{(-1)^{2n-j}\sqrt{\binom{2n}{j}}\,|j\rangle_a\,|2n-j\rangle_b}{\sqrt{2^{2n}}}\right)\\
&+\frac{1}{2}\sum_{m\neq n}\mathrm{e}^{-2\mu}\sqrt{\frac{(2\mu)^{4m+4n}}{(4m)!(4n)!}}\sqrt{P^L\left(\sum_{j=0}^{4m}\frac{(-1)^{4m-j}\sqrt{\binom{4m}{j}}\,|j\rangle_a\,|4m-j\rangle_b}{\sqrt{2^{4m}}}\right)}\sqrt{P^L\left(\sum_{j=0}^{4n}\frac{(-1)^{4n-j}\sqrt{\binom{4n}{j}}\,|j\rangle_a\,|4n-j\rangle_b}{\sqrt{2^{4n}}}\right)}\\
&+\frac{1}{2}\sum_{m\neq n}\mathrm{e}^{-2\mu}\sqrt{\frac{(2\mu)^{4m+4n+4}}{(4m+2)!(4n+2)!}}\sqrt{P^L\left(\sum_{j=0}^{4m+2}\frac{(-1)^{4m+2-j}\sqrt{\binom{4m+2}{j}}\,|j\rangle_a\,|4m+2-j\rangle_b}{\sqrt{2^{4m+2}}}\right)}\\
&\times\sqrt{P^L\left(\sum_{j=0}^{4n+2}\frac{(-1)^{4n+2-j}\sqrt{\binom{4n+2}{j}}\,|j\rangle_a\,|4n+2-j\rangle_b}{\sqrt{2^{4n+2}}}\right)}
\end{aligned}\tag{18}$$

$$\begin{aligned}
P^{L\mathbb{E}}_{\mathrm{ph2}} \leqslant{}& \frac{1}{2}\sum_{n=0}^{\infty}\frac{\mathrm{e}^{-2\mu}(2\mu)^{2n+1}}{(2n+1)!}P^L\left(\sum_{j=0}^{2n+1}\frac{(-1)^{2n+1-j}\sqrt{\binom{2n+1}{j}}\,|j\rangle_a\,|2n+1-j\rangle_b}{\sqrt{2^{2n+1}}}\right)\\
&+\frac{1}{2}\sum_{m\neq n}\mathrm{e}^{-2\mu}\sqrt{\frac{(2\mu)^{4m+4n+2}}{(4m+1)!(4n+1)!}}\sqrt{P^L\left(\sum_{j=0}^{4m+1}\frac{(-1)^{4m+1-j}\sqrt{\binom{4m+1}{j}}\,|j\rangle_a\,|4m+1-j\rangle_b}{\sqrt{2^{4m+1}}}\right)}\\
&\times\sqrt{P^L\left(\sum_{j=0}^{4n+1}\frac{(-1)^{4n+1-j}\sqrt{\binom{4n+1}{j}}\,|j\rangle_a\,|4n+1-j\rangle_b}{\sqrt{2^{4n+1}}}\right)}\\
&+\frac{1}{2}\sum_{m\neq n}\mathrm{e}^{-2\mu}\sqrt{\frac{(2\mu)^{4m+4n+6}}{(4m+3)!(4n+3)!}}\sqrt{P^L\left(\sum_{j=0}^{4m+3}\frac{(-1)^{4m+3-j}\sqrt{\binom{4m+3}{j}}\,|j\rangle_a\,|4m+3-j\rangle_b}{\sqrt{2^{4m+3}}}\right)}\\
&\times\sqrt{P^L\left(\sum_{j=0}^{4n+3}\frac{(-1)^{4n+3-j}\sqrt{\binom{4n+3}{j}}\,|j\rangle_a\,|4n+3-j\rangle_b}{\sqrt{2^{4n+3}}}\right)}
\end{aligned}\tag{19}$$

With the given phase error probabilities, the key rate is shown as

$$R^L = \frac{p_\mu^2}{2}\left\{P^L_{\mathbb{C}}\left[1-H_2\left(\frac{\bar{P}^{L\mathbb{C}}_{\mathrm{ph}}}{P^L_{\mathbb{C}}}\right)\right]+P^L_{\mathbb{E}}\left[1-H_2\left(\frac{\min\left(\bar{P}^{L\mathbb{E}}_{\mathrm{ph1}},\bar{P}^{L\mathbb{E}}_{\mathrm{ph2}}\right)}{P^L_{\mathbb{E}}}\right)\right]-fP^L_{\mathrm{tot}}H_2\left(e^L_{\mathrm{bit}}\right)\right\}, \tag{20}$$

where $\bar{P}^{L\mathbb{C}}_{\mathrm{ph}}$ ($\bar{P}^{L\mathbb{E}}_{\mathrm{ph1}}$, $\bar{P}^{L\mathbb{E}}_{\mathrm{ph2}}$) is the upper bound of $P^{L\mathbb{C}}_{\mathrm{ph}}$ ($P^{L\mathbb{E}}_{\mathrm{ph1}}$, $P^{L\mathbb{E}}_{\mathrm{ph2}}$).

TABLE I. The device parameters we used in our simulation.

p_d	d	f	e_{mis}
1	10^{-6}	1.1	0.01

IV. NUMERICAL SIMULATION

We conduct numerical simulations to see the improvement of our analysis. In our simulation, infinite decoy states are assumed. The parameters we used are shown in Table I. p_d is the detecting efficiency of detectors. d is the dark counting rate per pulse of each detector. f is the error correction efficiency. e_{mis} is the misalignment error rate of the interferometer.

The simulation result of the PM-TF-QKD is shown in Fig. 1. We simulated the key rate under the original analysis for comparison. Note that in most of the situations, the requirement for performance is not very strict. Thus, we can only use the clicks of $\mathbb{C}$ rounds to generate the key, which means that the phase error rate of $\mathbb{E}$ rounds is set to 50%. Thus, the parameter estimation of the $\mathbb{E}$ rounds can be removed. We also simulated this case in Fig. 1.

The simulation of the FP-PPP-TF-QKD is given in Fig. 2. We also give the simulation when the phase error rate of $\mathbb{E}$ rounds is set to 50%.

The simulation shows that at low transmission distance, the improved performance is nearly the same as the original one. However, our analysis can improve the channel loss tolerance of about 1.5 dB, which means our analysis can improve the transmission distance of about 7.5 km in a standard fiber channel. With only $\mathbb{C}$ rounds, the key rate is reduced by about 10% in the PM-TF-QKD, but the distance improvement is still retained. In the last 10 dB of the channel loss, the key rate improvement is distinct. A similar improvement can be seen in the simulation result of the FP-PPP-TF-QKD.

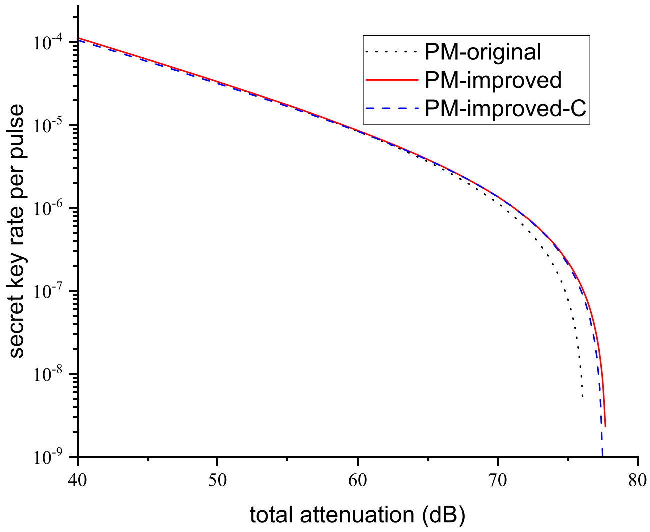

FIG. 1. The key rate simulation of the PM-TF-QKD. The PM-original line corresponds to the key rate under the original security analysis. The PM-improved line corresponds to the key rate under our improved security analysis. The PM-improved-C line corresponds to the key rate under our improved analysis when the phase error rate of $\mathbb{E}$ rounds is set to 50%.

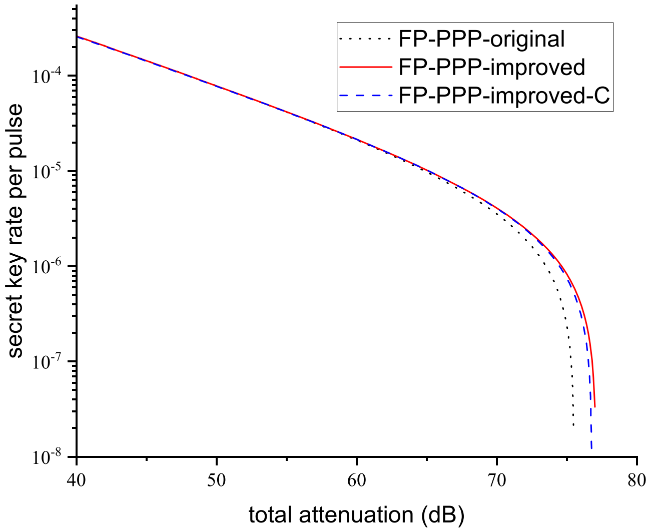

FIG. 2. The key rate simulation of the FP-PPP-TF-QKD. The FP-PPP-original line corresponds to the key rate under the original security analysis. The FP-PPP-improved line corresponds to the key rate under our improved security analysis. The FP-PPP-improved-C line corresponds to the key rate under our improved analysis when the phase error rate of $\mathbb{E}$ rounds is set to 50%.

The improvement can be explained as follows. In our improved analysis, the information leakage is estimated as $P_{\mathbb{C}}H_2(\frac{P_{\text{ph}}^{\mathbb{C}}}{P_{\mathbb{C}}}) + P_{\mathbb{E}}H_2(\frac{P_{\text{ph}}^{\mathbb{E}}}{P_{\mathbb{E}}})$. In the original analysis, it is estimated as $(P_{\mathbb{C}} + P_{\mathbb{E}})H_2(\frac{P_{\text{ph}}^{\mathbb{C}}+P_{\text{ph}}^{\mathbb{E}}}{P_{\mathbb{C}}+P_{\mathbb{E}}})$. Our analysis cannot reduce the total number of phase errors but divides them into two parts. Due to the concavity of the H_2 function, the information leakage of our analysis is smaller. Thus, we can give a better performance. At the condition of short distance, the error rate is relatively low. With a small $P_{\mathbb{E}}$, the difference is not notable. For the case of extreme distance, the dark counts increase the error rate a lot, so a longer distance can be achieved with our analysis.

V. CONCLUSION

To conclude, we give the improved security analysis for two phase-encoding TF-QKD protocols by analyzing the information leakages of correct rounds and erroneous rounds separately. With our analysis, no modifications to experiments are needed and the transmission distance can be improved. In our numerical simulation, our analysis could improve the channel loss tolerance of the PM-TF-QKD and the FP-PPP-TF-QKD by about 1.5 dB. Since our analysis does not change any experimental settings of the protocols, our analysis can be a better choice for all situations when using these protocols.

Our method might be able to be applied in some other protocols. We also tried it on the measurement-device-independent protocol and the no-phase-postselection protocol, but the efforts were not good. Thus, we do not show them in the article. Since our improvement lies on the ratio of bit errors, our method might not be able to work for time-bin encoding protocols, but other phase encoding protocols—for example, the phase-encoding measurement-device-independent protocol—may be able to benefit from our method.

ACKNOWLEDGMENTS

This work has been supported by the National Key Research and Development Program of China (Grant No. 2020YFA0309802), the National Natural Science Foundation of China (Grants No. 62171424, No. 62271463, and No. 62301524), the Prospect and Key Core Technology Projects of Jiangsu provincial key R & D Program (Grant No. BE2022071), the Fundamental Research Funds for the Central Universities, the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300701), the Natural Science Foundation of Anhui (Grant No. 2308085QF216), and the China Postdoctoral Science Foundation (Grant No. 2022M723064).

APPENDIX: FEASIBILITY OF DECOY-STATE ESTIMATION OF OUR IMPROVED ANALYSIS

In our calculation of the phase error rate, we need to estimate the click rates of the following states:

$$\frac{1}{2\Delta}\int_{-\Delta}^{\Delta} d\delta\mathcal{P}\left[\sum_{j=0}^{n}\frac{\sqrt{\binom{n}{j}}\mathrm{e}^{i(n-j)\delta}\,|j\rangle_a\,|n-j\rangle_b}{\sqrt{2^n}}\right], \tag{A1}$$

$$\frac{1}{2\Delta}\int_{-\Delta}^{\Delta} d\delta\mathcal{P}\left[\sum_{j=0}^{n}\frac{(-1)^{n-j}\sqrt{\binom{n}{j}}\mathrm{e}^{i(n-j)\delta}\,|j\rangle_a\,|n-j\rangle_b}{\sqrt{2^n}}\right]. \tag{A2}$$

For ease of description, we define the states in Eqs. (A1) and (A2) as $\bar{\rho}_n^+$ and $\bar{\rho}_n^-$. One may find that when $\Delta \to 0$ these two states correspond to the n-photon states causing constructive and destructive interference separately.

When Alice and Bob both send the phase-randomized decoy state with an intensity ν, we also use the phase postselection to select the rounds with a phase difference less than Δ. The state of these rounds is shown as

$$\begin{aligned}\frac{1}{4\pi\Delta}\int_{-\Delta}^{\Delta} d\delta\int_{0}^{2\pi} d\theta\mathcal{P}(|\sqrt{\nu}\mathrm{e}^{i\theta}\rangle_a\,|\sqrt{\nu}\mathrm{e}^{i(\theta+\delta)}\rangle_b)\\ =\sum_{n=0}^{\infty}\frac{\mathrm{e}^{-2\nu}(2\nu)^n}{n!}\bar{\rho}_n^+.\end{aligned} \tag{A3}$$

Thus, the click rate of these decoy rounds can be expressed by a linear combination of the click rates of $\bar{\rho}_n^+$. Note that Alice and Bob can send decoy states with different intensities and get different combinations of $\bar{\rho}_n^+$. Then, with linear programming, one can get the upper bound of every click rate of $\bar{\rho}_n^+$. In practical use, one may not need to estimate $\bar{\rho}_n^+$ for all n since the items are too small for a large n. For a large n, one can just use 1 as the click rate upper bound.

The estimation of the click rates of $\bar{\rho}_n^-$ is similar by selecting the decoy states with a phase difference in $[\pi-\Delta, \pi+\Delta]$ because of the following equation:

$$\begin{aligned}\frac{1}{4\pi\Delta}\int_{-\Delta}^{\Delta} d\delta\int_{0}^{2\pi} d\theta\mathcal{P}(|\sqrt{\nu}\mathrm{e}^{i\theta}\rangle_a\,|-\sqrt{\nu}\mathrm{e}^{i(\theta+\delta)}\rangle_b)\\ =\sum_{n=0}^{\infty}\frac{\mathrm{e}^{-2\nu}(2\nu)^n}{n!}\bar{\rho}_n^-.\end{aligned} \tag{A4}$$

Note that the same parameter estimation is also used in the original analysis of the PM-TF-QKD. Thus, our estimation above does not change any steps or devices of the experimental realization.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *International Conference on Computers, Systems and Signal Processing* (Bangalore, India, 1984), pp. 175–179.

[2] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).

[4] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Direct and reverse secret-key capacities of a quantum channel, Phys. Rev. Lett. **102**, 050503 (2009).

[5] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[6] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[7] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, Phys. Rev. X **8**, 031043 (2018).

[8] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).

[9] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, Phys. Rev. A **98**, 042332 (2018).

[10] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution without phase postselection, Phys. Rev. Appl. **11**, 034053 (2019).

[11] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).

[12] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photonics **13**, 334 (2019).

[13] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system, Phys. Rev. X **9**, 021046 (2019).

[14] Y. Liu *et al.*, Experimental twin-field quantum key distribution through sending or not sending, Phys. Rev. Lett. **123**, 100505 (2019).

[15] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Proof-of-principle experimental demonstration of twin-field type quantum key distribution, Phys. Rev. Lett. **123**, 100506 (2019).

[16] X.-T. Fang *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nat. Photonics **14**, 422 (2020).

[17] J.-P. Chen *et al.*, Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km, Phys. Rev. Lett. **124**, 070501 (2020).

[18] X. Zhong, W. Wang, L. Qian, and H.-K. Lo, Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses, npj Quantum Inf. **7**, 8 (2021).

[19] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, Nat. Photonics **15**, 530 (2021).

[20] C. Clivati *et al.*, Coherent phase transfer for real-world twin-field quantum key distribution, Nat. Commun. **13**, 157 (2022).

[21] H. Liu *et al.*, Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km, Phys. Rev. Lett. **126**, 250502 (2021).

[22] J.-P. Chen *et al.*, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, Nat. Photonics **15**, 570 (2021).

[23] S. Wang *et al.*, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).

[24] Y. Liu *et al.*, Experimental twin-field quantum key distribution over 1000 km fiber distance, Phys. Rev. Lett. **130**, 210801 (2023).

[25] Y. Zhou, Z.-Q. Yin, R.-Q. Wang, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution with partial phase postselection, Phys. Rev. Appl. **18**, 054026 (2022).

[26] W.-Y. Hwang, Quantum key distribution with high loss: toward global secure communication, Phys. Rev. Lett. **91**, 057901 (2003).

[27] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[28] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[29] P. Zeng, W. Wu, and X. Ma, Symmetry-protected privacy: Beating the rate-distance linear bound over a noisy channel, Phys. Rev. Appl. **13**, 064013 (2020).

[30] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. London A **461**, 207 (2005).

[31] M. M. Wilde, From classical to quantum Shannon theory, *Quantum Information Theory*, 2nd ed. (Cambridge University Press, Cambridge, 2017).

[32] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, The uncertainty principle in the presence of quantum memory, Nat. Phys. **6**, 659 (2010).

[33] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, Uncertainty relations from simple entropic properties, Phys. Rev. Lett. **108**, 210405 (2012).

[34] R. Wang, Z.-Q. Yin, F.-Y. Lu, S. Wang, W. Chen, C.-M. Zhang, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, Optimized protocol for twin-field quantum key distribution, Commun. Phys. **3**, 149 (2020).