Phase-matching quantum key distribution with imperfect sources

Xiao-Xu Zhang(张晓旭)[1,2,3], Yi-Fei Lu(陆宜飞)[1,2], Yang Wang(汪洋)[1,2,†], Mu-Sheng Jiang(江木生)[1,2], Hong-Wei Li(李宏伟)[1,2], Chun Zhou(周淳)[1,2], Yu Zhou(周雨)[1,2], and Wan-Su Bao(鲍皖苏)[1,2,‡]

[1] *Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou* 450001, *China*
[2] *Synergetic Innovation Centre of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*
[3] *Basic Department, SSF IEU, Zhengzhou* 450001, *China*

(Received 9 July 2022; revised manuscript received 22 September 2022; accepted manuscript online 18 October 2022)

The huge discrepancies between actual devices and theoretical assumptions severely threaten the security of quantum key distribution. Recently, a general new framework called the reference technique has attracted wide attention in defending against the imperfect sources of quantum key distribution. Here, the state preparation flaws, the side channels of mode dependencies, the Trojan horse attacks, and the pulse classical correlations are studied by using the reference technique on the phase-matching protocol. Our simulation results highlight the importance of the actual secure parameters choice for transmitters, which is necessary to achieve secure communication. Increasing the single actual secure parameter will reduce the secure key rate. However, as long as the parameters are set properly, the secure key rate is still high. Considering the influences of multiple actual secure parameters will significantly reduce the secure key rate. These actual secure parameters must be considered when scientists calibrate transmitters. This work is an important step towards the practical and secure implementation of phase-matching protocol. In the future, it is essential to study the main parameters, find out their maximum and general values, classify the multiple parameters as the same parameter, and give countermeasures.

Keywords: quantum key distribution, reference technique, imperfect sources, phase-matching

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a **DOI:** 10.1088/1674-1056/ac9b03

1. Introduction

Quantum key distribution (QKD) can offer two distant parties of information theoretic security based on the laws of quantum mechanics. In recent years, QKD has made tremendous progress, which includes the realization of long-distance fiber communication systems[1–11] and the deployment of QKD networks.[12–15] Although the theoretical assumptions of QKD are impeccable, the actual devices have potential security loopholes,[16–34] which seriously threaten the security of QKD.

To further strengthen security between actual devices and theoretical assumptions, scientists proposed the device-independent QKD (DI-QKD) protocol,[35,36] which measures the violation of Bell's inequality to guarantee the unconditional security of QKD. However, current experimental techniques face challenges in implementing the DI-QKD. As a compromise, the measurement-device-independent QKD (MDI-QKD) has been proposed and favored,[37–39] which can reduce the difficulty of the experiment[1–4] and close the security loopholes on the detector side. Nonetheless, the theoretical and actual security problems still exist on the source side. Recently, a new version of MDI-QKD called the twin-field QKD (TF-QKD) has been proposed,[40–44] which uses single-photon interference and closes the security loopholes on the detector side. TF-QKD can overcome the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) linear bound,[45] its key rate scales with the square root of the channel transmittance. TF-QKD has excellent application prospects in long-distance communication, and related experimental works have been extensively carried out.[5–11]

So far, there are three main practical variants of TF-QKD protocols. The phase-matching QKD (PM-QKD) protocol gives the first rigorous security analysis for the coherent-state-based QKD protocols.[42,46,47] PM-QKD employs a phase-post-compensated technology, so there is no need for pre-phase feedback, and it is easy to implement experimentally. The sending-or-not-sending TF-QKD (SNS-TF-QKD) protocol can tolerate large misalignment errors,[42] so it has strong anti-noise capability and can achieve long-distance key distribution. The signal state of the no-phase-postselection TF-QKD (NPP-TF-QKD) protocol has no phase randomization,[43,44] which provides better key rate performance. However, NPP-TF-QKD needs pre-phase feedback in experiment.

Security loopholes on the source side can be summarized as three main causes:[16] the first is the state preparation flaws (SPFs), which are derived from the precision of the modulators and discrete phase randomization of coherent states. The second is the information leakage, which includes the side channels of mode dependencies (MDs) and the Trojan horse attacks (THAs). The MDs come from various degrees of freedom, and the THAs are used to observe the back-reflected light from

†Corresponding author. E-mail: wy@qiclab.cn
‡Corresponding author. E-mail: bws@qiclab.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd

the source side. The third is the classical correlations (CCs) between pulses, which are mainly introduced by the limited bandwidth of the modulators.

Therefore, if these security loopholes on the source side are not addressed, they will pose significant threats to the security of QKD.[16,17] Recently, scientists have perfromed a lot of works on addressing security loopholes, e.g., the uncharacterized qubit sources have been studied theoretically and experimentally in Refs. [18–20], and the upper bound of information leakage can be correctly estimated even in the absence of the quantum state characteristics. For the SPFs, with the original loss-tolerant (LT) protocol,[21] the limitation of the Gottesman–Lo–Lutkenhaus–Preskill (GLLP) analysis can be solved, and the secure key rate is almost independent of the source's flaws. The SPFs caused by randomization of discrete are also studied in Refs. [22,23]. For the side channels of MDs, which exist in various degrees of freedom, the polarization MDs (PMDs) are common loopholes in phase coding, and the security may be severely affected by the PMDs. For the THAs, when Eve injects strong light into Alice and Bob, information leakage can be detected by observing back-reflected light. For both the PMDs and THAs, the state may not be a qubit, the generalized LT (GLT) protocol can solve this problem,[24,25] but the GLT protocol is more complex and requires a lot of calculations. The existing security analysis assumes that the state is independent and identically distributed. When the CCs are considered, this assumption is not satisfied. The CCs have been ignored because they are difficult to quantify and have little influence on low-speed QKD systems. Recently, with the development of the high-speed QKD system, the CCs between pulse and previous settings have become more extensive, which will lead to severe and general security loopholes. Pereira treated the CCs as side channels and used a general new framework called the reference technique (RT) to solve the severe loophole.[16] The key idea of the RT is to consider some reference states close to the actual states, using these reference states can simplify the calculation process and ensure security. Scientists have given in-depth studies about the CCs from experimental and theoretical perspectives.[48–53]

In this paper, we investigate the variant scheme of PM-QKD, the imperfect sources with the SPFs, PMDs, THAs, and CCs are all considered here. At present, none of these imperfections have simultaneously considered on PM-QKD. Meanwhile, the actual secure key rate of PM-QKD is given by using the scheme of the RT.

The paper is arranged as follows: In Section 2, we characterize the imperfect basis-dependent states of the SPFs, the side channels of the PMDs, THAs, and CCs. In Section 3, we use the RT for security analysis. In Section 4, we show the numerical simulation results and discussion. Countermeasures are shown in Section 5, and then we conclude in Section 6.

2. Imperfect sources

We characterize the imperfect basis-dependent states of the SPFs, the side channels of the PMDs, THAs, and CCs.

2.1. The ideal states

In the PM-QKD, the signal states adopt weak coherent states with discrete phase randomization. For Alice, the ideal state is

$$|\Psi_Z\rangle_{\mathrm{AE}}^{\mathrm{ideal}} = \frac{1}{\sqrt{2}}\sum_{g=0,1}(|\Psi_{gZ}\rangle_{\mathrm{AE}}^{\mathrm{ideal}}) = \frac{1}{\sqrt{2}}\sum_{g=0,1}(|(-)^g\varphi\rangle_{\mathrm{AE}}),$$

where $|\varphi\rangle_{\mathrm{AE}} = |\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|e\rangle_{\mathrm{E}}$, $|-\varphi\rangle_{\mathrm{AE}} = |-\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|e\rangle_{\mathrm{E}}$, $\phi_{\mathrm{A}} = \frac{2\pi}{D}d_{\mathrm{A}}$, $|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}$ and $|-\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}$ are the states sent to Charlie, $|e\rangle_{\mathrm{E}}$ is the state that contains nothing of information about Alice, D is the number of maximum discrete phase, d_{A} is the discrete phase randomization number of Alice, which is randomly chosen from $\{0,1,\cdots,D-1\}$, the intensity $|\alpha|^2 \in \{\frac{\mu}{2},\frac{\nu}{2},\frac{\omega}{2}\}$.

The ideal joint state of Alice is

$$\begin{aligned}|\Psi_Z\rangle_{\mathrm{aAE}}^{\mathrm{ideal}} &= \frac{1}{\sqrt{2}}\sum_{g=0,1}(|g_Z\rangle_{\mathrm{a}}|\Psi_{gZ}\rangle_{\mathrm{AE}}^{\mathrm{ideal}})\\ &= \frac{1}{\sqrt{2}}\sum_{g=0,1}(|g_Z\rangle_{\mathrm{a}}|(-)^g\varphi\rangle_{\mathrm{AE}}),\end{aligned} \tag{1}$$

where the state $|g_Z\rangle_{\mathrm{a}}$ is kept in hand by Alice, $\{|0_Z\rangle,|1_Z\rangle\}$ is the eigenstate of the Pauli operator σ_Z.

Similarly, the ideal joint state of Bob is $|\Psi_Z\rangle_{\mathrm{bBE}}^{\mathrm{ideal}} = \frac{1}{\sqrt{2}}\sum_{h=0,1}(|h_Z\rangle_{\mathrm{b}}|\Psi_{hZ}\rangle_{\mathrm{BE}}^{\mathrm{ideal}}) = \frac{1}{\sqrt{2}}\sum_{h=0,1}(|h_Z\rangle_{\mathrm{b}}|(-)^h\varphi\rangle_{\mathrm{BE}})$. In the ideal scenario, if the phase shift ϕ_δ can be perfectly post-compensated and the SPFs caused by discrete phase randomization are not considered, there are no the SPFs in the phase match pairs, $\phi_{\mathrm{AB}} = \phi_{\mathrm{A}} - \phi_{\mathrm{B}} - \phi_\delta = 0$.

2.2. The actual states with the SPFs

The SPFs are derived from the imperfection of modulators and discrete phase randomization. The actual joint states of Alice and Bob with the SPFs can be expressed as

$$\begin{aligned}|\Psi_Z\rangle_{\mathrm{aAE}} &= \frac{1}{\sqrt{2}}\sum_{g=0,1}(|g_Z\rangle_{\mathrm{a}}|(-)^g\mathrm{e}^{\mathrm{i}(\phi_{\mathrm{A}}+\phi_{\mathrm{Af}})}\varphi\rangle_{\mathrm{AE}}),\\ |\Psi_Z\rangle_{\mathrm{bBE}} &= \frac{1}{\sqrt{2}}\sum_{h=0,1}(|g_Z\rangle_{\mathrm{b}}|(-)^g\mathrm{e}^{\mathrm{i}(\phi_{\mathrm{B}}+\phi_{\mathrm{Bf}})}\varphi\rangle_{\mathrm{BE}}),\end{aligned} \tag{2}$$

where ϕ_{Af} and ϕ_{Bf} are the SPFs introduced by modulators of Alice and Bob.

Considering the phase shift ϕ_δ, the phase match pairs read $\phi_{\mathrm{AB}} = \phi_{\mathrm{A}} + \phi_{\mathrm{Af}} - \phi_{\mathrm{B}} - \phi_{\mathrm{Bf}} - \phi_\delta \neq 0$.

2.3. The actual states with the SPFs and PMDs

The side channels of MDs are important actual security issues, which are derived from encoding in various degrees of freedom, then Eve can obtain the key in a degree different from the encoding degree. Here, we mainly consider the side

channels of the PMDs. Concretely, Eve can attack the polarization dual modes scenario to obtain keys. The expression for the polarization dual modes of Alice can be written as

$$|(-)^g \mathrm{e}^{\mathrm{i}(\phi_\mathrm{A}+\phi_\mathrm{Af})}\varphi\rangle'_{\mathrm{AE}} = \cos\theta_\mathrm{p}|(-)^g \mathrm{e}^{\mathrm{i}(\phi_\mathrm{A}+\phi_\mathrm{Af})}\varphi\rangle_{H|\mathrm{AE}} + \sin\theta_\mathrm{p}|(-)^g \mathrm{e}^{\mathrm{i}(\phi_\mathrm{A}+\phi_\mathrm{Af})}\varphi\rangle_{V|\mathrm{AE}}, \quad (3)$$

where H and V are horizontal and vertical polarization modes, respectively; and θ_p is the polarization angle. The horizontal polarization mode H is used to generate the key.

For simplicity, we uniformly consider the worst polarization angle θ_p, no matter whether it is Alice's or Bob's. Then we can write the actual joint state of Alice with the SPFs and the side channels of the PMDs as

$$|\Psi_Z\rangle'_{\mathrm{aAE}} = \frac{1}{\sqrt{2}}\sum_{g=0,1}(|g_Z\rangle_\mathrm{a}|(-)^g \mathrm{e}^{\mathrm{i}(\phi_\mathrm{A}+\phi_\mathrm{Af})}\varphi\rangle'_{\mathrm{AE}}). \quad (4)$$

Similarly, the actual joint state of Bob is $|\Psi_Z\rangle'_{\mathrm{bBE}} = \frac{1}{\sqrt{2}}\sum_{h=0,1}(|h_Z\rangle_\mathrm{b}|(-)^h \mathrm{e}^{\mathrm{i}(\phi_\mathrm{B}+\phi_\mathrm{Bf})}\varphi\rangle'_{\mathrm{BE}})$.

2.4. The actual states with the SPFs, PMDs, and THAs

The plug-and-play systems can get good stability for implementation, but they are easily suffered from serious threats by the THAs. When Eve injects strong light into Alice and Bob, the back-reflected light can be observed from the source side to obtain some information, some of which is the directly encoded phase information from which we can obtain the keys directly, and some of which is of indirect intensity information so that we can use the distinguish ability of signal states and decoy states to obtain keys. Suppose that Eve injects strong light into Alice, then the actual joint state of Alice with the SPFs and the side channels of the PMDs and the THAs can be written as

$$|\Psi_Z\rangle''_{\mathrm{aAE}} = \frac{1}{\sqrt{2}}\sum_{g=0,1}(|g_Z\rangle_\mathrm{a}|(-)^g \mathrm{e}^{\mathrm{i}(\phi_\mathrm{A}+\phi_\mathrm{Af})}\varphi\rangle'_{\mathrm{AE}}|\varsigma_{gZ}\rangle_\mathrm{E}), \quad (5)$$

where $|\varsigma_{gZ}\rangle_\mathrm{E}$ is the back-reflected light Eve sends to Alice, $|\varsigma_{gZ}\rangle_\mathrm{E} = \mathrm{e}^{-\mu_\mathrm{b}/2}|v\rangle_\mathrm{E} + \sqrt{1-\mathrm{e}^{-\mu_\mathrm{b}}}|e_{gZ}\rangle_\mathrm{E}$, μ_b is the intensity of back-reflected light sent by Eve, $|v\rangle_\mathrm{E}$ is the vacuum state with no information, $|e_{gZ}\rangle_\mathrm{E}$ is the coherent state that provides Eve with some information.

For simplicity, we consider the worst situation $\langle e_{0Z}||e_{1Z}\rangle_\mathrm{E} = 0$. Similarly, the actual joint state of Bob is $|\Psi_Z\rangle''_{\mathrm{bBE}} = \frac{1}{\sqrt{2}}\sum_{h=0,1}(|h_Z\rangle_\mathrm{b}|(-)^h \mathrm{e}^{\mathrm{i}(\phi_\mathrm{B}+\phi_\mathrm{Bf})}\varphi\rangle'_{\mathrm{BE}}|\varsigma_{hZ}\rangle_\mathrm{E})$.

2.5. The actual states with the SPFs, PMDs, THAs, and CCs

The CCs are security loopholes that are often ignored by us, with multiple dimensions, such as polarization, phase, and intensity. The reasons why we ignore the CCs are such that they are difficult to quantify and have little influence on low-speed QKD systems. Until accurate quantitative simulations were carried out in Ref. [16] the problems of the CCs did not attract attention again.

The key idea is that we regard the leaked information encoded into the CCs as the side channels, so the actual joint state of Alice with the SPFs, PMDs, THAs, and CCs can be characterized as

$$|\Psi_Z\rangle'''_{\mathrm{aAE}} = \sqrt{1-\varepsilon_{\mathrm{cor}(n)}}|\Psi_Z\rangle''_{\mathrm{aAE}} + \sqrt{\varepsilon_{\mathrm{cor}(n)}}|\Psi_Z^\perp\rangle''_{\mathrm{aAE}}, \quad (6)$$

where $\varepsilon_{\mathrm{cor}(n)}$ represents a parameter related to the information leakage, which is introduced by modulations, $\mathrm{cor}(n)$ represents the correlation range, $|\Psi_Z^\perp\rangle''_{\mathrm{aAE}}$ is orthogonal to $|\Psi_Z\rangle''_{\mathrm{aAE}}$, we can ignore the specific characterization of $|\Psi_Z^\perp\rangle''_{\mathrm{aAE}}$.

Correlation range $\mathrm{cor}(n)$ is also an important parameter,[16] not only we should consider the nearest-neighbor pulse correlations $\mathrm{cor}(1)$, but also our analysis needs apply to arbitrarily long-range correlations $\mathrm{cor}(n)$, where $n \geq 2$, specific derivation of long-range correlations can be found in Ref. [16]. Similarly, the actual joint state of Bob is $|\Psi_Z\rangle'''_{\mathrm{bBE}} = \sqrt{1-\varepsilon_{\mathrm{cor}(n)}}|\Psi_Z\rangle''_{\mathrm{bBE}} + \sqrt{\varepsilon_{\mathrm{cor}(n)}}|\Psi_Z^\perp\rangle''_{\mathrm{bBE}}$.

3. Security proof

3.1. Phase error rate of the actual states

The actual joint states of Alice and Bob can be characterized as

$$|\Psi^{\mathrm{act}|(ZZ)}\rangle_{\mathrm{ABabE}} = |\Psi_Z\rangle'''_{\mathrm{aAE}}|\Psi_Z\rangle'''_{\mathrm{bBE}}. \quad (7)$$

In this actual scenario, the density operators of the actual transmitted states $|\Psi^{\mathrm{act}|(ZZ)}\rangle_{\mathrm{ABE}}$ sent by Alice and Bob can be given by

$$|\Psi^{\mathrm{act}|(ZZ)}\rangle_{\mathrm{ABE}}\langle\Psi^{\mathrm{act}|(ZZ)}| = \mathrm{Tr}_{\mathrm{ab}}[|g_z,h_z\rangle\langle g_z,h_z|_{\mathrm{ab}} \otimes I_{\mathrm{ABE}}|\Psi^{\mathrm{act}|(ZZ)}\rangle\langle\Psi^{\mathrm{act}|(ZZ)}|_{\mathrm{abABE}}], \quad (8)$$

where I_{ABE} is the identity operator acting on ABE.

In this virtual scenario, the unnormalized density operators of the actual transmitted states sent by Alice and Bob can be expressed as

$$\bar{\sigma}^{\mathrm{act}|\mathrm{vir},(ZZ)}_{g_x,h_x} = \mathrm{Tr}_{\mathrm{ab}}[|g_x,h_x\rangle\langle g_x,h_x|_{\mathrm{ab}} \otimes I_{\mathrm{ABE}}|\Psi^{\mathrm{act}|(ZZ)}\rangle\langle\Psi^{\mathrm{act}|(ZZ)}|_{\mathrm{abABE}}]. \quad (9)$$

The normalized form can be written as

$$\sigma^{\mathrm{act}|\mathrm{vir},(ZZ)}_{g_x,h_x} = \bar{\sigma}^{\mathrm{act}|\mathrm{vir},(ZZ)}_{g_x,h_x}/\mathrm{Tr}[\bar{\sigma}^{\mathrm{act}|\mathrm{vir},(ZZ)}_{g_x,h_x}],$$

where $p^{\mathrm{act}|\mathrm{vir},(ZZ)}_{g_x,h_x} = \mathrm{Tr}[\bar{\sigma}^{\mathrm{act}|\mathrm{vir},(ZZ)}_{g_x,h_x}]$.

The phase error rate is the bit error rate of the virtual scheme. In this protocol, the phase error occurs when Alice and Bob measure the states kept in hand by $|0_x,0_x\rangle_{\mathrm{ab}}$ or $|1_x,1_x\rangle_{\mathrm{ab}}$ (see Subsections 3.2 and 3.3 for a specific description) and Charlie announces the successful events.

Therefore, the phase error rate can be expressed as

$$E_{ph}^{\mathrm{act|vir},(ZZ)}=\frac{\sum_{g,h\in\{0,1\},g=h}p_{g_x,h_x}^{\mathrm{act|vir},(ZZ)}Y_{g_x,h_x}^{\mathrm{act|vir},(ZZ)}}{\sum_{g,h\in\{0,1\}}p_{g_x,h_x}^{\mathrm{act|vir},(ZZ)}Y_{g_x,h_x}^{\mathrm{act|vir},(ZZ)}}. \quad (10)$$

We have the denominator term

$$\begin{aligned}&\sum_{g,h\in\{0,1\}}p_{g_x,h_x}^{\mathrm{act|vir},(ZZ)}Y_{g_x,h_x}^{\mathrm{act|vir},(ZZ)}\\=&\sum_{g,h\in\{0,1\}}p_{g_z,h_z}^{\mathrm{act|vir},(ZZ)}Y_{g_z,h_z}^{\mathrm{act|vir},(ZZ)},\end{aligned}$$

which can be directly observed in the actual experiment. It is equal to the probability that Charles announces the successful events and both Alice and Bob send the key states. Then we only need to estimate the numerator term

$$\Gamma_{\mathrm{act}}=\sum_{g,h\in\{0,1\},g=h}p_{g_x,h_x}^{\mathrm{act|vir},(ZZ)}Y_{g_x,h_x}^{\mathrm{act|vir},(ZZ)}.$$

3.2. Phase error rate of the reference states

The RT is first introduced by Pereira *et al.*[16] As soon as it was put forward, it was widely applied because it can simplify the calculation. Meanwhile, it is generally compatible with various side channels (including the MDs, THAs, and CCs). The method of the RT is how to select the reference states, the choice of the reference states has a certain degree of freedom, so the core is to simplify the relationship of the phase error rate between actual states and the reference states. The ideal transmitted states sent by Alice and Bob are chosen as the reference states, which can be given by

$$|\Phi^{\mathrm{ref|}(ZZ)}\rangle_{\mathrm{ABE}}=|\Psi_Z\rangle_{\mathrm{AE}}^{\mathrm{ideal}}|\Psi_Z\rangle_{\mathrm{BE}}^{\mathrm{ideal}}. \quad (11)$$

The reference joint states of Alice and Bob can be characterized by

$$\begin{aligned}|\Psi_Z\rangle_{\mathrm{abABE}}^{\mathrm{ref}}&=\frac{1}{2}\sum_{g,h=0,1}(|g_Z\rangle_{\mathrm{a}}|h_Z\rangle_{\mathrm{b}}|\Psi_{g_Z}\rangle_{\mathrm{AE}}^{\mathrm{ideal}}|\Psi_{h_Z}\rangle_{\mathrm{BE}}^{\mathrm{ideal}})\\&=\frac{1}{2}\sum_{g,h=0,1}(|g_Z\rangle_{\mathrm{a}}|g_Z\rangle_{\mathrm{b}}|(-)^g\varphi\rangle_{\mathrm{AE}}|(-)^h\varphi\rangle_{\mathrm{BE}}).\end{aligned} \quad (12)$$

From the definitions of probabilities of the actual states, we can define analogous probabilities of reference states. The normalized form reads

$$p_{g_x,h_x}^{\mathrm{ref|vir},(ZZ)}Y_{g_x,h_x}^{\mathrm{ref|vir},(ZZ)}=\mathrm{Tr}[\hat{M}\sigma_{g_x,h_x}^{\mathrm{ref|vir},(ZZ)}],$$

where $\hat{M}=\sum\hat{K}_{\tilde{e}}^{\dagger}(\hat{M}_{k_{\mathrm{c}},k_{\mathrm{d}}}^{\mathrm{A,B}})^{\dagger}\hat{M}_{k_{\mathrm{c}},k_{\mathrm{d}}}^{\mathrm{A,B}}\hat{K}_{\tilde{e}}$. $\hat{K}_{\tilde{e}}$ is the Kraus operator representing Eve's action, $\tilde{e}$ corresponds to the measurement outcome, $\hat{M}_{k_{\mathrm{c}},k_{\mathrm{d}}}^{\mathrm{A,B}}$ is the Kraus operator corresponding to the announcement of left detector k_{c} and right detector k_{d}, $k_{\mathrm{c}}=0$ and $k_{\mathrm{c}}=1$ ($k_{\mathrm{d}}=0$ and $k_{\mathrm{d}}=1$) represent the no-click and click events. Then the phase error rate of the reference states can be described as (see Subsection 3.3 for a specific description of the reference states)

$$E_{ph}^{\mathrm{ref|vir},(ZZ)}=\frac{\sum_{g,h\in\{0,1\},g=h}p_{g_x,h_x}^{\mathrm{ref|vir},(ZZ)}Y_{g_x,h_x}^{\mathrm{ref|vir},(ZZ)}}{\sum_{g,h\in\{0,1\}}p_{g_x,h_x}^{\mathrm{ref|vir},(ZZ)}Y_{g_x,h_x}^{\mathrm{ref|vir},(ZZ)}}, \quad (13)$$

where the numerator term

$$\Gamma_{\mathrm{ref}}=\sum_{g,h\in\{0,1\},g=h}p_{g_x,h_x}^{\mathrm{ref|vir},(ZZ)}Y_{g_x,h_x}^{\mathrm{ref|vir},(ZZ)}.$$

3.3. Virtual protocol of the reference states

In this section, we describe the virtual protocol of the reference states. The reference joint states of Alice and Bob can be further characterized as

$$\begin{aligned}&|\Psi_Z\rangle_{\mathrm{abAB}}^{\mathrm{ideal}}\\=&\frac{1}{2}\sum_{g,h=0,1}(|g_Z\rangle_{\mathrm{a}}|h_Z\rangle_{\mathrm{b}}|(-)^g\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|(-)^h\mathrm{e}^{\mathrm{i}\phi_{\mathrm{B}}}\alpha\rangle_{\mathrm{B}}).\end{aligned} \quad (14)$$

Rewrite the states in Eq. (14) in the X basis of the systems a and b as

$$\begin{aligned}|\Psi_Z\rangle_{\mathrm{abAB}}^{\mathrm{ideal}}=&\frac{1}{2}[(|0_X0_X\rangle_{\mathrm{ab}}+|1_X1_X\rangle_{\mathrm{ab}})|\varphi_{Z,\mathrm{same}}^{\mathrm{vir,even}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}\\&+(|0_X1_X\rangle_{\mathrm{ab}}+|1_X0_X\rangle_{\mathrm{ab}})|\varphi_{Z,\mathrm{same}}^{\mathrm{vir,odd}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}\\&+(|0_X0_X\rangle_{\mathrm{ab}}-|1_X1_X\rangle_{\mathrm{ab}})|\varphi_{Z,\mathrm{diff}}^{\mathrm{vir,even}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}\\&+(|1_X0_X\rangle_{\mathrm{ab}}-|0_X1_X\rangle_{\mathrm{ab}})|\varphi_{Z,\mathrm{diff}}^{\mathrm{vir,odd}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}].\end{aligned} \quad (15)$$

The unnormal states can be written as

$$\begin{aligned}&|\varphi_{Z,\mathrm{same}}^{\mathrm{vir,even}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}\\=&\frac{1}{2}(|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{B}}}\alpha\rangle_{\mathrm{B}}+|-\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|-\mathrm{e}^{\mathrm{i}\phi_{\mathrm{B}}}\alpha\rangle_{\mathrm{B}}),\\&|\varphi_{Z,\mathrm{same}}^{\mathrm{vir,odd}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}\\=&\frac{1}{2}(|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{B}}}\alpha\rangle_{\mathrm{B}}-|-\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|-\mathrm{e}^{\mathrm{i}\phi_{\mathrm{B}}}\alpha\rangle_{\mathrm{B}}),\\&|\varphi_{Z,\mathrm{diff}}^{\mathrm{vir,even}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}\\=&\frac{1}{2}(|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{B}}}-\alpha\rangle_{\mathrm{B}}+|-\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{B}}}\alpha\rangle_{\mathrm{B}}),\\&|\varphi_{Z,\mathrm{diff}}^{\mathrm{vir,odd}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}\\=&\frac{1}{2}(|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{B}}}-\alpha\rangle_{\mathrm{B}}-|-\mathrm{e}^{\mathrm{i}\phi_{\mathrm{A}}}\alpha\rangle_{\mathrm{A}}|\mathrm{e}^{\mathrm{i}\phi_{\mathrm{B}}}\alpha\rangle_{\mathrm{B}}).\end{aligned} \quad (16)$$

Here, we usually need to consider the influence of discrete phase randomization. When D is larger, we can ignore the effect of discrete phase randomization. Meanwhile, we can set $\phi_{\mathrm{A}}=\phi_{\mathrm{B}}=0$, then the unnormal states can be simplified to

$$\begin{aligned}|\varphi_{Z,\mathrm{same}}^{\mathrm{vir,even}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}&\approx\sum_{j\in\mathrm{even}}\sqrt{P_{j||\alpha|^2}}|\lambda_j^+\rangle_{\mathrm{AB}},\\|\varphi_{Z,\mathrm{same}}^{\mathrm{vir,odd}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}&\approx\sum_{j\in\mathrm{odd}}\sqrt{P_{j||\alpha|^2}}|\lambda_j^+\rangle_{\mathrm{AB}},\\|\varphi_{Z,\mathrm{diff}}^{\mathrm{vir,even}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}&\approx\sum_{j\in\mathrm{even}}\sqrt{P_{j||\alpha|^2}}|\lambda_j^-\rangle_{\mathrm{AB}},\\|\varphi_{Z,\mathrm{diff}}^{\mathrm{vir,odd}}\rangle_{\mathrm{AB}}^{\mathrm{ideal}}&\approx\sum_{j\in\mathrm{odd}}\sqrt{P_{j||\alpha|^2}}|\lambda_j^-\rangle_{\mathrm{AB}},\end{aligned} \quad (17)$$

where

$$P_{j||\alpha|^2}=\frac{\mathrm{e}^{-2|\alpha|^2}(2|\alpha|^2)^j}{j!}$$

is the Poisson distribution of photon number. The j-photon two-mode Fock state reads

$$|\lambda_j^+\rangle_{\rm AB} = \frac{1}{\sqrt{2^j j!}}(A^\dagger + B^\dagger)|00\rangle_{\rm AB},$$

$$|\lambda_j^-\rangle_{\rm AB} = \frac{1}{\sqrt{2^j j!}}(A^\dagger - B^\dagger)|00\rangle_{\rm AB}.$$

Using the Kraus operator acting on the state $|\varphi_{Z,\rm same}^{\rm vir,even}\rangle_{\rm AB}^{\rm ideal}$ and the Cauchy–Schwarz inequality, we can reach

$$\begin{aligned}
&{\rm Tr}((\hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B})^\dagger \hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B}|\varphi_{Z,\rm same}^{\rm vir,even}\rangle_{\rm AB}^{\rm ideal}\langle\varphi_{Z,\rm same}^{\rm vir,even}|)\\
&= \sum_{j\in\rm even}\sqrt{P_{j||\alpha|^2}}_{\rm AB}\langle\lambda_j^+|(\hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B})^\dagger \hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B}\sum_{j_1\in\rm even}\sqrt{P_{j_1||\alpha|^2}}|\lambda_{j_1}^+\rangle_{\rm AB} = \sum_{j,j_1\in\rm even}\sqrt{P_{j||\alpha|^2}P_{j_1||\alpha|^2}}_{\rm AB}\langle\lambda_j^+|(\hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B})^\dagger \hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B}|\lambda_{j_1}^+\rangle_{\rm AB}\\
&\le \sum_{j,j_1\in\rm even}\sqrt{P_{j||\alpha|^2}P_{j_1||\alpha|^2}}\sqrt{{}_{\rm AB}\langle\lambda_j^+|(\hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B})^\dagger \hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B}|\lambda_j^+\rangle_{\rm AB}{}_{\rm AB}\langle\lambda_{j_1}^+|(\hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B})^\dagger \hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B}|\lambda_{j_1}^+\rangle_{\rm AB}} = \sum_{j\in\rm even}P_{j||\alpha|^2}Y_{\rm even}^{\rm ideal^+},
\end{aligned} \tag{18}$$

where $Y_{\rm even}^{\rm ideal^+}$ is the yield probability of the even photon state $|\lambda_j^+\rangle_{\rm AB}$.

Similar to the state $|\varphi_{Z,\rm diff}^{\rm vir,even}\rangle_{\rm AB}^{\rm ideal}$,

$$\begin{aligned}
&{\rm Tr}((\hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B})^\dagger \hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B}|\varphi_{Z,\rm diff}^{\rm vir,even}\rangle_{\rm AB}^{\rm ideal}\langle\varphi_{Z,\rm diff}^{\rm vir,even}|)\\
&= \sum_{j\in\rm even}\sqrt{P_{j||\alpha|^2}}_{\rm AB}\langle\lambda_j^-|(\hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B})^\dagger \hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B}\\
&\quad\times\sum_{j_1\in\rm even}\sqrt{P_{j_1||\alpha|^2}}|\lambda_{j_1}^-\rangle_{\rm AB}\\
&\le \sum_{j\in\rm even}P_{j||\alpha|^2}Y_{\rm even}^{\rm ideal^-},
\end{aligned} \tag{19}$$

where $Y_{\rm even}^{\rm ideal^-}$ is the yield probability of the even photon state $|\lambda_j^-\rangle_{\rm AB}$.

Then, we can arrive at

$$\begin{aligned}
&{\rm Tr}((\hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B})^\dagger \hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B}|\varphi_{Z,\rm same}^{\rm vir,even}\rangle_{\rm AB}^{\rm ideal}\langle\varphi_{Z,\rm same}^{\rm vir,even}|\\
&\quad+(\hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B})^\dagger \hat{M}_{k_{\rm c},k_{\rm d}}^{\rm A,B}|\varphi_{Z,\rm diff}^{\rm vir,even}\rangle_{\rm AB}^{\rm ideal}\langle\varphi_{Z,\rm diff}^{\rm vir,even}|)\\
&\le \sum_{j\in\rm even}P_{j||\alpha|^2}Y_{\rm even}^{\rm ideal},
\end{aligned} \tag{20}$$

where $Y_{\rm even}^{\rm ideal}$ is the yield probability of the even photon state.

3.4. Deviation evaluation

In this subsection, we transform the relationship between the reference states and the actual states. That is to say, we use the RT for the deviation evaluation. For the sake of convenience, we give a concise relation. For the normalized actual pure state $|{\rm act}\rangle$ and reference pure state $|{\rm ref}\rangle$, we can obtain the following inequality with the measurement operator $\hat{N}$:

$$\delta \le \sqrt{Y_{\rm act}Y_{\rm ref}} + \sqrt{(1-Y_{\rm act})(1-Y_{\rm ref})}, \tag{21}$$

where $\delta = |\langle{\rm act}|{\rm ref}\rangle|$, $Y_{\rm act} = \langle{\rm act}|\hat{N}|{\rm act}\rangle$, $Y_{\rm ref} = \langle{\rm ref}|\hat{N}|{\rm ref}\rangle$.

Then we can define function $g(x,y)$ as

$$g^{\rm L}(x,y) = \begin{cases} 0, & x < 1-y^2,\\ x+(1-y^2)(1-2x)-2y\sqrt{(1-y^2)x(1-x)}, & x \ge 1-y^2, \end{cases} \tag{22}$$

$$g^{\rm U}(x,y) = \begin{cases} x+(1-y^2)(1-2x)-2y\sqrt{(1-y^2)x(1-x)}, & x \le y^2,\\ 1, & x > y^2. \end{cases} \tag{23}$$

Using the above mathematical description, $\Gamma_{\rm act}$ can be obtained from $\Gamma_{\rm ref}^{\rm U}$ and $\delta_{\rm cor,ref}^{\rm L}$ by

$$\Gamma_{\rm act} \le g^{\rm U}(\Gamma_{\rm ref},\delta_{\rm cor,ref}) \le g^{\rm U}(\Gamma_{\rm ref}^{\rm U},\delta_{\rm cor,ref}^{\rm L}), \tag{24}$$

where $\Gamma_{\rm ref}^{\rm U}$ is the upper bound of $\Gamma_{\rm ref}$, which can be calculated from the observed statistics of the actual states $Y_{\rm even}^{\rm act}$; $\delta_{\rm cor,ref}^{\rm L}$ is the lower bound of the fidelity between the reference states and the actual states, which can be roughly calculated by $|\langle\Phi^{{\rm ref}|(ZZ)}|\Psi^{{\rm act}|(ZZ)}\rangle_{\rm ABE}|$.[52] The specific form is

$$\begin{aligned}
&\langle\Phi^{{\rm ref}|(ZZ)}|\Psi^{{\rm act}|(ZZ)}\rangle_{\rm ABE}\\
&= \frac{1}{4}\sqrt{1-\varepsilon_{{\rm cor}(n)}}\,{\rm e}^{-\mu_{\rm b}/2}\cos\theta_{\rm p}\\
&\quad\times[(1-{\rm i})\langle\alpha|{\rm i}\,{\rm e}^{{\rm i}\phi_{\rm AB}}\alpha\rangle + (1-{\rm i})\langle{\rm e}^{{\rm i}\phi_{\rm AB}}\alpha|{\rm i}\,{\rm e}^{{\rm i}\phi_{\rm AB}}\alpha\rangle\\
&\quad+(1+{\rm i})\langle\alpha|-{\rm i}\,{\rm e}^{{\rm i}\phi_{\rm AB}}\alpha\rangle + (1+{\rm i})\langle-{\rm i}\,{\rm e}^{{\rm i}\phi_{\rm AB}}\alpha|{\rm i}\,{\rm e}^{{\rm i}\phi_{\rm AB}}\alpha\rangle].
\end{aligned} \tag{25}$$

4. Simulation and discussion

In our security analysis, the equation of the final secure key rate can be written as

$$R_{\rm f} = \frac{2}{D}Q_\mu[1-H_2(E_\mu^X)-fH_2(E_\mu^Z)], \tag{26}$$

where Q_μ and E_μ^Z are the gain and bit error rate of the actual signal state, E_μ^X is the upper bound of phase error rate come from the actual signal state, f is the error correction efficiency, $H_2(x) = -x\log_2(x)-(1-x)\log_2(1-x)$ is the binary entropy function.

From the channel model, the total gain can be derived as

$$Q_{|\alpha|^2}=(1-p_{\rm d})\,{\rm e}^{-\eta|\alpha|^2\sin^2\frac{\phi_{\rm AB}}{2}}-(1-p_{\rm d})^2\,{\rm e}^{-\eta|\alpha|^2}+Q^{\rm E}_{|\alpha|^2}. \quad (27)$$

The error gain can be given by

$$Q^{\rm E}_{|\alpha|^2}=(1-p_{\rm d})\,{\rm e}^{-\eta|\alpha|^2\cos^2\frac{\phi_{\rm AB}}{2}}-(1-p_{\rm d})^2\,{\rm e}^{-\eta|\alpha|^2}. \quad (28)$$

The bit error rate of signal states is given by

$$E^Z_\mu=\frac{Q^{\rm E}_\mu(1-2e_{\rm opt})+e_{\rm opt}Q_\mu}{Q_\mu}. \quad (29)$$

We set the dark counts rate $p_{\rm d}=1\times10^{-8}$; the misalignment error probability of the system $e_{\rm opt}=1.5\%$; the error correction efficiency $f=1.1$. The transmittance $\eta=\eta_{\rm f}\eta_{\rm d}$, where $\eta_{\rm d}=0.2$ is the detection efficiency of detectors, $\eta_{\rm f}$ is the transmittance of fiber loss coefficient (dB/km).

Based on $Q^{\rm act}_\mu=\sum_{j=0}P_{j|\mu}Y^{\rm act}_{j|\mu}$, $Q^{\rm act}_\nu=\sum_{j=0}P_{j|\nu}Y^{\rm act}_{j|\nu}$, we can obtain the expression for estimating the actual single-photon yield using the standard decoy states method. However, when we consider the actual security of the PMDs, THAs, and CCs, it is realized that the fundamental implicit assumption of decoy states analysis that the yield is independent of intensity setting is invalid.[23,27] Therefore, considering the properties of trace distance, we have $|Y^{\rm act}_{j|\mu}-Y^{\rm act}_{j|\nu}|\le\sqrt{1-F^2_{j|\mu\nu}}$, where $F_{j|\mu\nu}$ is the worst-case fidelity.

Then, the observed statistics is

$$Y^{\rm act}_{1|\mu}\ge\frac{P_{2|\mu}Q^{\rm act}_\nu-P_{2|\nu}Q^{\rm act}_\mu-(P_{2|\mu}P_{0|\nu}-P_{0|\mu}P_{2|\nu})Y^{\rm act}_{0|\mu}-P_{2|\mu}\sum_{j=0}^{\infty}P_{j|\nu}\sqrt{1-F^2_{j|\mu\nu}}}{P_{2|\mu}P_{1|\nu}-P_{1|\mu}P_{2|\nu}}. \quad (30)$$

The expression for estimating the actual even photon yield is

$$Y^{\rm act}_{\rm even}\le1-Y^{\rm act}_{1|\mu}. \quad (31)$$

To evaluate the performance of the protocol theoretically, we simulate the secure key rate of the imperfect sources in the asymptotic case.

4.1. Simulation

Figure 1 mainly considers the influence of the imperfect single parameter on key rate versus communication distance of PM-QKD.

Figure 1(a) is the case with the SPFs. When we use the modulators to modulate discrete phases $\phi_{\rm A}$ and $\phi_{\rm B}$, the SPFs $\phi_{\rm Af}$ and $\phi_{\rm Bf}$ are introduced. Without considering the finite discrete phase randomization, the simulation results show that the effect of key rate is small when $\phi_{\rm AB}$ is small; with the increase of $\phi_{\rm AB}$, the key rate decreases further; when $\phi_{\rm AB}=0.65$, the key rate can just exceed the PLOB bound; with further increase of $\phi_{\rm AB}$, the key rate dramatic decreases, or even cannot be obtained.

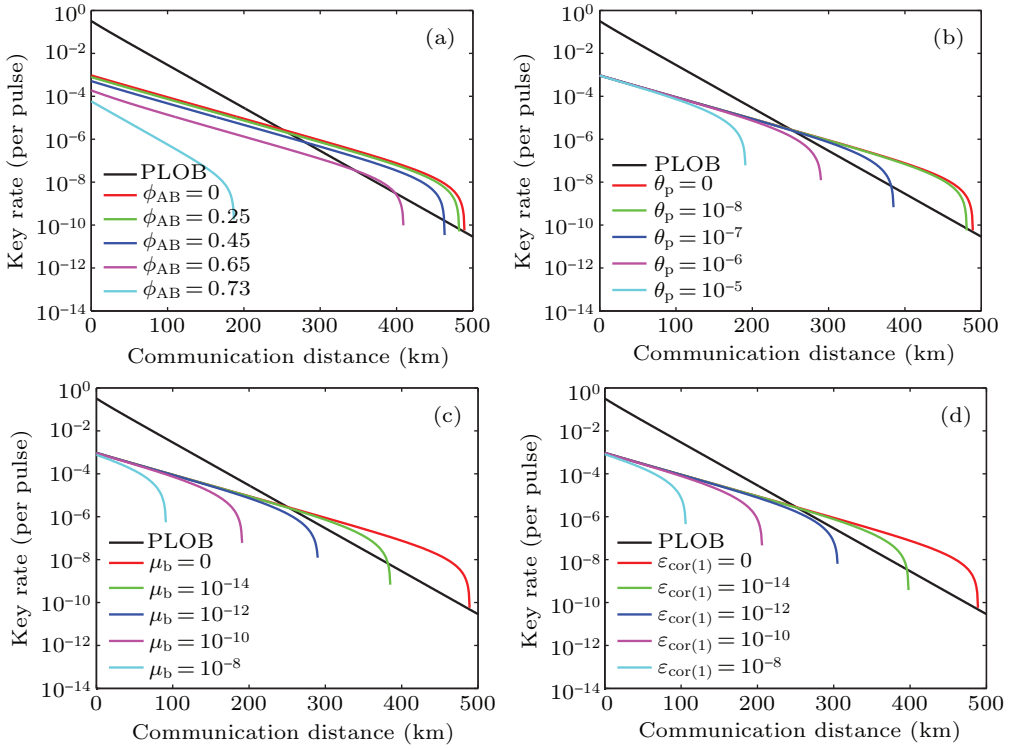


Fig. 1. Key rate versus the transmission distance of PM-QKD with the imperfect single parameter sources. (a) The imperfect source with the SPFs. (b) The imperfect source with the PMDs. (c) The imperfect source with the THAs. (d) The imperfect source with the nearest-neighbor pulse CCs.

Figure 1(b) is the side channel with the PMDs. A smaller value of $\theta_{\rm p} \approx 10^{-8}$ has little influence on the key rate, the key rate decreases significantly when $\theta_{\rm p}$ reaches the order of 10^{-7}; with the increase of $\theta_{\rm p}$, when $\theta_{\rm p} = 10^{-6}$, the key rate can not reach the PLOB bound; with further increase of $\theta_{\rm p}$, the key rate dramatically decreases.

Figure 1(c) considers the influences of the THAs. The key rate is greatly affected by the information leakage of back-reflected light intensity. As the intensity of the back-reflected light increases, more and more information is leaked. When $\mu_{\rm b} = 10^{-12}$, the key rate is lower than the PLOB bound, then the key rate decreases further as $\mu_{\rm b}$ continues to increase.

Figure 1(d) considers the influence of the nearest-neighbor CCs. Since we treat the CCs as the side channel, we introduce a parameter $\varepsilon_{\rm cor}$ to characterize information leakage. Information leakage increases with the increase of $\varepsilon_{\rm cor}$. When $\varepsilon_{\rm cor} = 10^{-12}$, the key rate is less than the PLOB bound, and the key rate further decreases with the increase of $\varepsilon_{\rm cor}$.

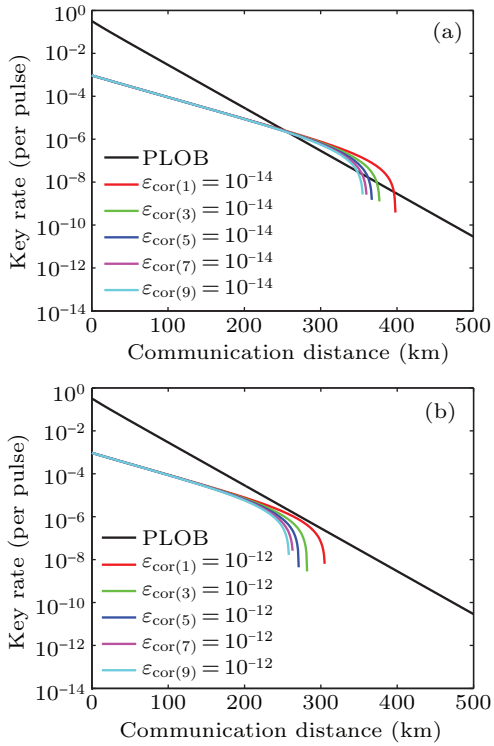


Fig. 2. Key rate versus the transmission distance of PM-QKD with imperfect long-range CCs sources: (a) $\varepsilon_{{\rm cor}(n)} = 10^{-14}$, (b) $\varepsilon_{{\rm cor}(n)} = 10^{-12}$.

Based on the nearest-neighbor CCs, we also study long-range correlations, because correlation range ${\rm cor}(n)$ is an important factor in the study of correlations. As shown in Fig. 2(a), when the correlation parameter $\varepsilon_{{\rm cor}(n)} = 10^{-14}$ is small, the PLOB bound can still be exceeded or reached even if the long-range correlations are considered. As shown in Fig. 2(b), when the correlation parameter increases to $\varepsilon_{{\rm cor}(n)} = 10^{-12}$, the key rate is less than the PLOB bound, even considering the long-range correlations. After careful analysis, we can also find that the near-range correlations have a great influence on the key rate. With further increase of the correlation range, the influence will decrease. That is, the influence of the long-range correlations on the key rate is gradually decreasing.

The influences of multiple parameters on the key rate versus communication distance are studied by considering only the nearest-neighbor CCs. As can be seen in Fig. 3, the four parameters of the SPFs, PMDs, THAs, and CCs are all set here. Even these parameters are small, there is a significant decrease in the final key rate. As the value of each parameter increases, although the key rate exceeds the PLOB bound when each parameter is taken individually, the final key rate is obviously lower than the PLOB bound. When we further increase the parameter value, although the key rate can reach the PLOB bound when each parameter is taken individually, the final key rate is very low, or even impossible to obtain.

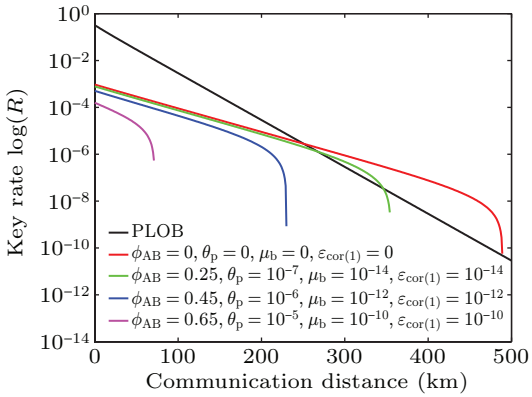


Fig. 3. Key rate versus the transmission distance of PM-QKD with imperfect multiple parameters sources.

4.2. Discussion

So far, we mainly study the actual security of the SPFs, the side channels of the PMDs, THAs, and CCs.

Firstly, when we only consider the single parameter, the influence of the key rate is small. However, when we consider the multiple parameters, they will have a large influence on the final key rate, or even unable to generate the key. In addition, we can further consider the influences of intensity fluctuation, asymmetric sources and reference frame independence,[53–59] and then we can extend the asymptotic case to the finite length.[54] Of course, these additional factors will increase the types and numbers of imperfections, thus further reducing the key rate.

Secondly, in the study of multiple parameters imperfections, the PMDs, THAs, and CCs can be uniformly regarded as a side channel with only the same parameter, which will reduce the complexity of analysis and calculation. The SPFs come from phase modulators and the flaw introduced by discrete phase randomization can also be uniformly represented as the SPFs with only the same parameter. Therefore, how to classify several imperfect factors into the same parameter is a worthy research direction.

Finally, in the experiment of the multiple parameters of imperfections, finding out the main parameter of influencing

the security, giving the characterization of its maximum value and general value, while ignoring some secondary parameters of influencing the security (such as the THAs is generally not considered if plug and play system is not adopted, the polarization beam splitters can greatly reduce the PMDs), which may be a more critical work in the future.

5. Countermeasures

The SPFs mainly include phase modulation errors and finite discrete phase randomization. We can adopt direct phase injection locking to reduce the security threat of phase modulation errors, and increase the number of discrete phase randomization to address the influence of key rate.

The side channels include not only the PMDs but also the frequency MDs (FMDs). Therefore, we can use a beam splitter with a high degree of polarization to eliminate the side channels of PMDs and a narrow band filter to eliminate the side channels of FMDs.

For the THAs, we should avoid using the plug-and-play systems and add isolators to the other QKD systems to reduce the external injection light, which are effective methods. Although the existing literature shows that ultra-strong light attack will cause damage to the isolators and effectively reduce the isolation degree of the isolator.[60] However, we can equip reverse intensity monitoring devices to detect whether the isolators have been damaged by strong light injection.

The CCs are commonly seen in intensity, polarization and phase. Low-speed system naturally has the advantage of the anti-CCs. In order not to reduce the speed, we can use external modulation instead of internal modulation, increase the bandwidth of the modulators, use the true random numbers and other schemes to avoid the influence of the pattern effect.

6. Conclusion

In this paper, using the RT of the new framework, we have studied the actual security of PM-QKD with the STFs, PMDs, THAs, and CCs. The analysis method can also accommodate other TF-QKD. Simulation results show that the key rate is higher when the single small parameter is considered, while the key rate is greatly reduced when the influences of multiple parameters are all considered. Meanwhile, these parameters are important for scientists to calibrate transmitters. Therefore, in the future, it is essential to analyze the main parameter, find out their maximum and general values, and classify the multiple parameters as the same parameter.

Acknowledgements

Project supported by the National Key Research and Development Program of China (Grant Nos. 2020YFA0309702 and 2020YFA0309701), the National Natural Science Foundation of China (Grant No. 62101597), the China Postdoctoral Science Foundation (Grant No. 2021M691536), the Natural Science Foundation of Henan (Grant Nos. 202300410534 and 202300410532), and the Anhui Initiative in Quantum Information Technologies.

References

[1] Liu Y, Chen T Y, Wang L J, Liang H, Shentu G L, Wang J, Cui K, Yin H L, Liu N L, Li L, Ma X, Pelc J S, Fejer M M, Peng C Z, Zhang Q and Pan J W 2013 *Phys. Rev. Lett.* **111** 130502
[2] 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, Chen H, Li M J, Nolan D, Zhou F, Jiang X, Wang Z, Zhang Q, Wang X B and Pan J W 2016 *Phys. Rev. Lett.* **117** 190501
[3] Tang Y L, Yin H L, Chen S J, Liu Y, Zhang W J, Jiang X, Zhang L, Wang J, You L X and Guan J Y 2014 *Phys. Rev. Lett.* **113** 190501
[4] Valivarthi R, Lucio Martinez I, Chan P, Rubenok A, John C, Korchinski D, Duffin C, Marsili F, Verma V, Shaw M D, Stern J A, Nam S W, Oblak D, Zhou Q, Slater J A and Tittel W 2015 *J. Mod. Opt.* **62** 1141
[5] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, Ye P, Zhou Y, Fan Yuan G J, Wang F X, Chen W, Zhu Y G, Morozov P V, Divochiy A V, Zhou Z, Guo G C and Han Z F 2022 *Nat. Photon.* **16** 154
[6] Wang S, He D Y, Yin Z Q, Lu F Y, Cui C H, Chen W, Zhou Z, Guo G C and Han Z F 2019 *Phys. Rev. X* **9** 021046
[7] Fang X T, Zeng P, Liu H, Zou M, Wu W, Tang Y L, Sheng Y J, Xiang Y, Zhang W, Li H, Wang Z, You L X, Li M J, Chen H, Chen Y A, Zhang Q, Peng C Z, Ma X, Chen T Y and Pan J W 2020 *Nat. Photon.* **14** 422
[8] Liu Y, Yu Z W, Zhang W, Guan J Y, Chen J P, Zhang C, Hu X L, Li H, Jiang C, Lin J, Chen T Y, You L, Wang Z, Wang X B, Zhang Q and Pan J W 2019 *Phys. Rev. Lett.* **123** 100505
[9] Chen J P, Zhang C, Liu Y, Jiang C, Zhang W, Hu X L, Guan J Y, Yu Z W, Xu H, Lin J, Li M J, Chen H, Li H, You L, Wang Z, Wang X B, Zhang Q and Pan J W 2020 *Phys. Rev. Lett.* **124** 070501
[10] Liu H, Jiang C, Zhu H T, Zou M, Yu Z W, Hu X L, Xu H, Ma S, Han Z, Chen J P, Dai Y, Tang S B, Zhang W, Li H, You L, Wang Z, Hua Y, Hu H, Zhang H, Zhou F, Zhang Q, Wang X B, Chen T Y and Pan J W 2021 *Phys. Rev. Lett.* **126** 250502
[11] 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, Zhou F, Jiang H F, Chen T Y, Li H, You L X, Wang Z, Wang X B, Zhang Q and Pan J W 2021 *Nat. Photon.* **15** 570
[12] Liao S K, Cai W Q, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren J G, Liu W Y, Li Y, Shen Q, Cao Y, Li F Z, Wang J F, Huang Y M, Deng L, Xi T, Ma L, Hu T, Li L, Liu N L, Koidl F, Wang P, Chen Y A, Wang X B, Steindorfer M, Kirchner G, Lu C Y, Shu R, Ursin R, Scheidl T, Peng C Z, Wang J Y, Zeilinger A and Pan J W 2018 *Phys. Rev. Lett.* **120** 030501
[13] Zhong X, Wang W, Mandil R, Lo H K and Qian L 2022 *Phys. Rev. Appl.* **17** 014025
[14] Dynes J F, Wonfor A, Tam W W S, Sharpe A W, Takahashi R, Lucamarini M, Plews A, Yuan Z L, Dixon A R, Cho J, Tanizawa Y, Elbers J P, Greißer H, White I H, Penty R V and Shields A J 2019 *npj Quantum Inf.* **5** 10
[15] Valivarthi R, Zhou Q, John C, Marsili F, Verma V B, Shaw M D, Nam S W, Oblak D and Tittel W 2017 *Quantum Sci. Technol.* **2** 04LT01
[16] Pereira M, Kato G, Mizutani A, Curty M and Tamaki K 2020 *Sci. Adv.* **6** aaz4487
[17] Gu J, Cao X Y, Fu Y, He Z W, Yin Z J, Yin H L and Chen Z B 2022 arXiv:2204.08323v1 [quant-ph]
[18] Yin Z Q, Fung C H F, Ma X, Zhang C M, Li H W, Chen W, Wang S, Guo G C and Han Z F 2013 *Phys. Rev. A* **88** 062322
[19] Wang C, Wang S, Yin Z Q, Chen W, Li H W, Zhang C M, Ding Y Y, Guo G C and Han Z F 2016 *Opt. Lett.* **41** 5596
[20] Zhou X Y, Ding H J, Zhang C H, Li J, Zhang C M and Wang Q 2020 *Opt. Lett.* **45** 4176
[21] Tamaki K, Curty M, Kato G, Lo H K and Azuma K 2014 *Phys. Rev. A* **90** 052314
[22] Cao Z, Zhang Z, Lo H K and Ma X 2015 *New J. Phys.* **17** 053014
[23] Zhang X, Wang Y, Jiang M, Lu Y, Li H, Zhou C and Bao W 2021 *Entropy* **23** 508
[24] Pereira M, Curty M and Tamaki K 2019 *npj Quantum Inf.* **5** 62

[25] Lu Y F, Wang Y, Jiang M S, Zhang X X, Liu F, Li H W, Zhou C, Tang S B, Wang J Y and Bao W S 2021 *Entropy* **23** 1103

[26] Gottesman D, Hoi Kwong L, Lutkenhaus N and Preskill J 2004 *Quantum Inf. Comput* **4** 325

[27] Lo H K and Preskill J 2007 *Quantum Inf. Comput* **7** 431

[28] Pinheiro P V P, Chaiwongkhot P, Sajeed S, Horn R T, Bourgoin J P, Jennewein T, Lutkenhaus N and Makarov V 2018 *Opt. Express* **26** 21020

[29] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev. A* **74** 022313

[30] Gerhardt I, Liu Q, Lamas Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 *Nat. Commun.* **2** 349

[31] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt C, Makarov V and Leuchs G 2011 *New J. Phys.* **13** 013043

[32] Pang X L, Yang A L, Zhang C N, Dou J P, Li H, Gao J and Jin X M 2020 *Phys. Rev. Appl.* **13** 034008

[33] Elezov M, Ozhegov R, Goltsman G and Makarov V 2019 *Opt. Express* **27** 30979

[34] Lamas Linares A and Kurtsiefer C 2007 *Opt. Express* **15** 9388

[35] Antonio A, Nicolas B, Nicolas G, Serge M, Stefano P and Valerio S 2007 *Phys. Rev. Lett.* **98** 230501

[36] Pironio S, Acin A, Brunner N, Gisin N, Massar S and Scarani V 2009 *New J. Phys.* **11** 045021

[37] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503

[38] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Phys. Rev. A* **85** 042307

[39] Ma X and Razavi M 2012 *Phys. Rev. A* **86** 062319

[40] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400

[41] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev. A* **98** 062323

[42] Ma X, Zeng P and Zhou H 2018 *Phys. Rev. X* **8** 031043

[43] Curty M, Azuma K and Lo H K 2019 *npj Quantum Inf.* **5** 64

[44] Cui C, Yin Z Q, Wang R, Chen W, Wang S, Guo G C and Han Z F 2019 *Phys. Rev. Appl.* **11** 034053

[45] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043

[46] Zeng P, Wu W and Ma X 2020 *Phys. Rev. Appl.* **13** 064013

[47] Zhang C M, Xu Y W, Wang R and Wang Q 2020 *Phys. Rev. Appl.* **14** 064070

[48] Kobayashi T, Tomita A and Okamoto A 2014 *Phys. Rev. A* **90** 032320

[49] Grunenfelder F, Boaron A, Rusca D, Martin A and Zbinden H 2020 *Appl. Phys. Lett.* **117** 144003

[50] Mizutani A, Kato G, Azuma K, Curty M, Ikuta R, Yamamoto T, Imoto N, Lo H K and Tamaki K 2019 *npj Quantum Inf.* **5** 8

[51] Roberts G L, Pittaluga M, Minder M, Lucamarini M, Dynes J F, Yuan Z L and Shields A J 2018 *Opt. Lett.* **43** 5110

[52] Ding H J, Zhou X Y, Zhang C H, Li J and Wang Q 2022 *Opt. Lett.* **47** 665

[53] Sekga C and Mafu M 2021 *J. Phys. Commun.* **5** 045008

[54] Zhang X X, Wang Y, Jiang M S, Zhou C, Lu Y F and Bao W S 2021 *J. Opt. Soc. Am. B* **38** 724

[55] Yu Y, Wang L, Zhao S and Mao Q 2021 *Opt. Express* **29** 2227

[56] Grasselli F, Navarrete A and Curty M 2019 *New J. Phys.* **21** 113032

[57] Lim K, Choi B S, Baek J H, Kim M, Choe J S, Kim K J, Ko Y H and Youn C J 2021 *Opt. Express* **29** 18966

[58] Zhou X Y, Ding H J, Sun M S, Zhang S H, Liu J Y, Zhang C H, Li J and Wang Q 2021 *Phys. Rev. Appl.* **15** 064016

[59] Liu J Y, Zhou X Y, Zhang C H, Ding H J, Chen Y P, Li J and Wang Q 2021 *J. Lightwav. Technol.* **39** 5486

[60] Makarov V, Bourgoin J P, Chaiwongkhot P, Gagne M, Jennewein T, Kaiser S, Kashyap R, Legre M, Minshull C and Sajeed S 2016 *Phys. Rev. A* **94** 030302