PAPER • OPEN ACCESS

Security of quantum key distribution with source and detection imperfections

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
26 November 2020

REVISED
12 January 2021

ACCEPTED FOR PUBLICATION
25 January 2021

PUBLISHED
9 February 2021

PAPER

Security of quantum key distribution with source and detection imperfections

Shihai Sun[1,*] and **Feihu Xu**[2,3,*]

[1] School of Physics and Astronomy, Sun Yat-Sen University, Zhuhai, Guangdong 519082, People's Republic of China
[2] Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, People's Republic of China
[3] Shanghai Branch, CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, People's Republic of China
[*] Authors to whom any correspondence should be addressed.

E-mail: sunshh8@mail.sysu.edu.cn and feihuxu@ustc.edu.cn

Keywords: quantum key distribution, quantum cryptography, practical security, quantum information processing, quantum communication

Abstract

In practice, the device imperfections might introduce deviations from the idealized models used in the security proofs of quantum key distribution (QKD). This requires the refined security analysis for practical QKD. However, in most of previous analysis, the imperfections are individually considered with different models. Here, we derive a security analysis which takes *both* the source and detection imperfections into account. Particularly, the efficiency mismatch in the detection and a number of flaws in the source (such as, inaccuracy of encoded quantum state, side-channel of source, distinguishable decoy states, Trojan-horse, and so on) are analyzed in a general security model. Then the performance of the QKD system with the devices imperfections is evaluated. Our results present an important step toward the practical security of QKD wit realistic devices.

1. Introduction

Quantum key distribution (QKD), such as BB84 [1], provides a way to share *key* between Alice and Bob with information-theoretical security. The unconditional security of QKD have been widely proved in theory [2–4] and demonstrated in experiments based on fiber [5–7] or free-space [8–10]. Some quantum networks based on QKD are also available now [11–13]. However, it is well known that the imperfections of practical devices will compensate the security of generated key. In fact, some quantum attacks have been discovered and demonstrated by exploiting these imperfections of practical devices [14–19]. Some detail information about the advances of QKD and quantum hacking can be found in recent review papers [20, 21].

In order to overcome the gap between theory and practice, two methods, security patch and device-independent QKD, are approached. In the former one, by adopting monitor or taking parameters of practical devices into the security model as many as possible, most of known quantum hacking can be defeated. The later one tries to propose new QKD protocol, in which the security can be proved with just a few of basic assumptions. Three typical device-independent protocols are full device-independent QKD [22, 23], measurement-device-independent QKD [24] and semi-device-independent QKD [25].

For BB84 protocol with single photon source (SPS), the key rate are given by

$$r \geqslant 1 - H(\delta_{\mathrm{b}}^{z}) - H(\delta_{\mathrm{p}}^{z}). \tag{1}$$

Here the key is distilled from $Z-$basis. If key is generated from both of two bases, equation (1) can be easily expended. δ_{b}^{z} is the bit error in Z-basis, which is directly measured in experiment. δ_{p}^{z} is the phase error in Z-basis. If the QKD system is perfect, δ_{p}^{z} equals with the bit error in X-basis (δ_{b}^{x}). But, when imperfections are taken into account, $\delta_{\mathrm{p}}^{z} \neq \delta_{\mathrm{b}}^{x}$, then new method is required to estimate the upper bound of δ_{p}^{z}. In fact,

Table 1. The considered imperfections in our model and the required parameters that used to evaluate these imperfections. Alice and Bob can measure the required parameters for practical QKD system in experiment, then evaluate the security of QKD based on our model given in the following sections. The superscript $i, j = 1, 2, 3, 4$ are the index of four quantum states sent by Alice, which represent z_0, z_1, x_0, x_1 respectively. The subscript of $D_{k,l}$ is the index of different decoy states k and l. And $[\eta_0(\lambda_k, \lambda_m)]$ is a matrix with element $\eta_0(\lambda_k, \lambda_m)$ for $k, m = 1, 2, \ldots$. The detail calculation of these security parameters are descried in the main text.

Considered imperfection	Required parameter	Symbol
Inaccuracy of encoded quantum state	Fidelity between practical states $\|\gamma_i\rangle$ and ideal states $\|i\rangle$	$f_{\text{en}}^{i} = \|\langle i\|\gamma_i\rangle\|^2 \equiv 1 - \varepsilon_1^i$
Side channel of source	Fidelity of different quantum state in other dimensions $\|\omega_i\rangle$ and $\|\omega_j\rangle$ (ω includes wavelength, time, *et al*)	$f_{\text{sc}}^{i,j} = \|\langle\omega_i\|\omega_j\rangle\|^2 \equiv 1 - \varepsilon_2^{i,j}$
Trojan-horse	The intensity of reflected Trojan-horse photon with different quantum state $\|\mu_{\text{out}}^i\rangle$ and $\|\mu_{\text{out}}^j\rangle$	$f_{\text{th}}^{i,j} = \|\langle\mu_{\text{out}}^i\|\mu_{\text{out}}^j\rangle\|^2 \equiv 1 - \varepsilon_3^{i,j}$
Distinguishable decoy state	Trace distance of different decoy states in all dimensions $\rho_i(\lambda)$ and $\rho_j(\lambda)$ (λ includes wavelength, time, *et al*)	$D_{k,l} = \frac{1}{2}\|\rho_i(\lambda) - \rho_j(\lambda)\| \equiv \varepsilon_4^{k,l}$
Detection mismatch	The detection efficiency matrices of two detectors $\lambda_{k(m)}$ is variable that control the efficiency of detectors	$F_0^+ F_0 = [\eta_0(\lambda_k, \lambda_m)]$, $F_1^+ F_1 = [\eta_1(\lambda_k, \lambda_m)]$

based on different imperfections, many works have been done, such as GLLP's analysis [3], basis-dependent source flaws [4], Trojan-horse [18], decoy state [26–28] and distinguishable decoy state [29], leaked source [30], detection mismatch [31, 32], weak randomness of basis choice [33], and so on. However, in most of these security analysis, the flaws are considered individually with different models.

In this paper, following the GLLP's analysis which is security under collective attack (if the source is independent and identically distributed, it is also security under coherent attack), the security of BB84 protocol with *both* source and detection imperfections are analyzed. In one model, the efficiency mismatch in detection and almost all of imperfections in source are taken into account together. The considered imperfections and the required parameters to evaluate these imperfections are listed in table 1. The legitimate parties can first measure the required parameters for practical QKD system in experiment, then evaluate the final key rate based on our analysis in following. When source flaws are taken into account, one major problem is that Eve could enhance the source flaws by exploiting the loss of system. Then the phase error is loss-dependent, which will rapidly worse the key rate even the source flaw is very small. In order to improve the key rate, a practical assumption is proposed, in which parts of loss in Bob's site can be carefully calibrated and monitored. In fact, this assumption has been used to secure the single photon detectors (SPDs) [34, 35]. Then we discuss the performance of QKD system based on this assumption.

2. Protocol

The model is shown in figure 1. Alice randomly prepares one of four quantum states $|\gamma_{\beta_j}\rangle$, here $\beta = Z, X$ is the basis and $j = 0, 1$ is the bit. Due to the imperfection of state preparing, $|\gamma_{\beta_j}\rangle$ may do not equal with the standard BB84 state $|\beta_j\rangle$, and they are also distinguishable in other dimensions. Thus, the practical quantum state prepared by Alice should be written as

$$\left|\varphi_{\beta_j}\right\rangle_{\text{BS}} = \left|\gamma_{\beta_j}\right\rangle_{\text{B}} \left|\omega_{\beta_j}\right\rangle_{\text{S}}. \tag{2}$$

The subscript B means the encoded state sent to Bob. $\left|\omega_{\beta_j}\right\rangle_{\text{S}}$ is the quantum state leaked to Eve due to the side-channel of source. The index ω includes all side-channels of Alice's quantum state, such as time, wavelength, waveform, Trojan-horse photon, and so on. Note that for simple of discussion, we assume $|\gamma_{\beta_j}\rangle$ is pure in equation (2), but the following analysis can be easily expended to the case of mixed state by introducing an auxiliary system belonging to Eve.

Now we consider the entanglement-based protocol according to the practical quantum state of equation (2), in which Alice prepares the following entanglement states in two bases,

$$\begin{aligned} |\psi_Z\rangle_{\text{ABS}} &= \frac{1}{\sqrt{2}}(|z_0\rangle_{\text{A}}|\varphi_{z_0}\rangle_{\text{BS}} + |z_1\rangle_{\text{A}}|\varphi_{z_1}\rangle_{\text{BS}}) \\ |\psi_X\rangle_{\text{ABS}} &= \frac{1}{\sqrt{2}}(|x_0\rangle_{\text{A}}|\varphi_{x_0}\rangle_{\text{BS}} + |x_1\rangle_{\text{A}}|\varphi_{x_1}\rangle_{\text{BS}}). \end{aligned} \tag{3}$$

After the state preparing, Alice measures the auxiliary system A to determine her bit, and sends B (S) to Bob (Eve). Generally speaking, due to the imperfection of source, $|\psi_Z\rangle \neq |\psi_X\rangle$. And since the system A is virtual, the state $\left|\beta_j\right\rangle_{\text{A}}$ and the measurement of Alice are perfect.

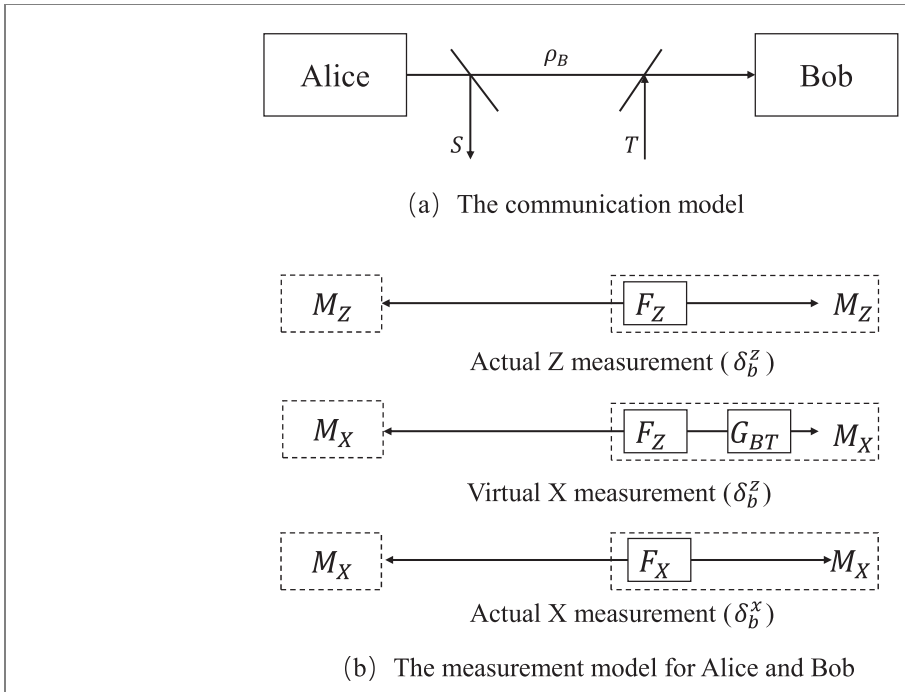

Figure 1. (a) The communication model among Alice, Bob and Eve. The system S means the side-channel of source, and T is for detection flaws. ρ_{B} is the quantum state sent to Bob by Alice. (b) The detection model for Alice and Bob based on reference [31]. The imperfect detection can be divided as two parts, a filter (F_Z, F_X or G_{BT}) followed by a perfect measurement (M_Z or M_X). The key is distilled from Z-basis, and the virtual X measurement is used to estimate the phase error.

When the quantum state $\left|\varphi_{\beta_j}\right\rangle_{\mathrm{BS}}$ flies in the quantum channel, Eve can perform collective attack on system B. Due to the existence of detection flaws, Eve also tries to control the click of SPDs by introducing another system T (see figure 1(a)). Generally speaking, Eve's interaction can be described by a set of POVM operators. But due to the existence of flaws in source and detection, Eve's operations may depend on the system S and T. Thus, the POVM elements of Eve should be written as,

$$\{E_{\mathrm{SBT}}^{i,t} = |\omega_t\rangle\langle\omega_t| \otimes E_{\mathrm{BT}}^{i,t}\}, \tag{4}$$

here i is the index of POVM elements, and $t = 1, 2, 3, 4$ means z_0, z_1, x_0, x_1 respectively. Then the quantum state shared by Alice, Bob and Eve is given by

$$\begin{aligned} |\Psi_Z\rangle_{\mathrm{ABSTE}} &= \sum_{i,t} E_{\mathrm{BT}}^{i,t} |\psi_Z\rangle_{\mathrm{ABS}} |0\rangle_{\mathrm{T}} |i\rangle_{\mathrm{E}}, \\ |\Psi_X\rangle_{\mathrm{ABSTE}} &= \sum_{i,t} E_{\mathrm{BT}}^{i,t} |\psi_X\rangle_{\mathrm{ABS}} |0\rangle_{\mathrm{T}} |i\rangle_{\mathrm{E}}. \end{aligned} \tag{5}$$

Here E is Eve's system to perform her collective attack with basis $\{|i\rangle_{\mathrm{E}}\}$. In order to determine Alice's basis, a quantum coin with basis $\{|0_{\mathrm{c}}\rangle, |1_{\mathrm{c}}\rangle\}$ is introduced [4]. Then the final entanglement state shared by Alice, Bob, and Eve is given by

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|0_{\mathrm{c}}\rangle|\Psi_Z\rangle + |1_{\mathrm{c}}\rangle|\Psi_X\rangle\right). \tag{6}$$

When Alice and Bob shared the entanglement state above, they randomly measure their quantum state with one of two bases, X or Z. Since Alice's measurements are virtual, thus her performances on system C and A are perfect. But, due to the flaws of detection, Bob's measurements may be controlled by Eve. According to reference [31] (see figure 1(b) for detail), when the detection mismatch is taking into account, Bob's measurement can be divided as two parts, a filter followed by a perfect measurement. The filter operators for actual $Z-$ and $X-$measurement, and virtual $X-$measurement are given by

$$\begin{aligned} F_Z &= |z_0\rangle_{\mathrm{B}}\langle z_0| \otimes (F_0)_{\mathrm{T}} + |z_1\rangle_{\mathrm{B}}\langle z_1| \otimes (F_1)_{\mathrm{T}}, \\ F_X &= |x_0\rangle_{\mathrm{B}}\langle x_0| \otimes (F_0)_{\mathrm{T}} + |x_1\rangle_{\mathrm{B}}\langle x_1| \otimes (F_1)_{\mathrm{T}}, \\ G_{\mathrm{BT}} &= |z_0\rangle_{\mathrm{B}}\langle z_0| \otimes (CF_0^{-1})_{\mathrm{T}} + |z_1\rangle_{\mathrm{B}}\langle z_1| \otimes (CF_1^{-1})_{\mathrm{T}}. \end{aligned} \tag{7}$$

Here F_0 and F_1 are detection efficiency matrices of SPDs, which characterize the mismatch of two detectors. C is a virtual filter used to estimate the phase error, which can be constructed by using F_0 and F_1. Here actual Z- (or X-) measurement means that Alice and Bob share $|\Psi_Z\rangle$ (or $|\Psi_X\rangle$) given by equation (5), and both Alice and Bob measure their quantum state with Z-basis (or X-basis), which indexes the bit error $\delta_{\rm b}^z$ (or $\delta_{\rm b}^x$). The virtual X-measurement means that Alice and Bob share $|\Psi_Z\rangle$, but both of them measure the quantum state with X-basis, which indexes the phase error $\delta_{\rm p}^z$. Since the phase error could not be directly measured in the BB84 protocol, it should be estimated with the measured bit error $\delta_{\rm b}^z$ and $\delta_{\rm b}^x$.

According to the model given above, the bit error and phase error can be written as,

$$\delta_{\rm b}^z = \frac{\langle\Psi_Z^1|M_{\rm b}^z|\Psi_Z^1\rangle}{\langle\Psi_Z^1|\Psi_Z^1\rangle}, \tag{8a}$$

$$\delta_{\rm b}^x = \frac{\langle\Psi_X^2|M_{\rm b}^x|\Psi_X^2\rangle}{\langle\Psi_X^2|\Psi_X^2\rangle}, \tag{8b}$$

$$\delta_{\rm p}^z = \frac{\langle\Psi_Z^3|M_{\rm p}^z|\Psi_Z^3\rangle}{\langle\Psi_Z^3|\Psi_Z^3\rangle}. \tag{8c}$$

Here $|\Psi_Z^1\rangle$, $|\Psi_X^2\rangle$ and $|\Psi_Z^3\rangle$ are the final quantum states when the quantum state from the quantum channel pass through the filter in actual Z measurement, actual X measurement and virtual X measurement, respectively (see part (b) of figure 1). And $M_{\rm b}^z$, $M_{\rm b}^x$ and $M_{\rm p}^z$ are perfect measurement in Z and X bases. Since the measurement is perfect, $M_b^{\rm x} = M_{\rm p}^z$. These parameters can be given by,

$$\begin{aligned} |\Psi_Z^1\rangle &= F_Z|\Psi_Z\rangle, \\ |\Psi_X^2\rangle &= F_X|\Psi_X\rangle, \\ |\Psi_Z^3\rangle &= G_{\rm BT}F_Z|\Psi_Z\rangle. \end{aligned} \tag{9a}$$

$$\begin{aligned} M_{\rm b}^z &= |z_0z_1\rangle_{\rm AB}\langle z_0z_1| + |z_1z_0\rangle_{\rm AB}\langle z_1z_0|, \\ M_{\rm b}^x &= |x_0x_1\rangle_{\rm AB}\langle x_0x_1| + |x_1x_0\rangle_{\rm AB}\langle x_1x_0|, \\ M_{\rm p}^z &= |x_0x_1\rangle_{\rm AB}\langle x_0x_1| + |x_1x_0\rangle_{\rm AB}\langle x_1x_0|. \end{aligned} \tag{9b}$$

Furthermore, due to the existence of filter $G_{\rm BT}$, not all the photons can pass the filter and be detected by Bob, thus the key rate of equation (1) should be rewritten as

$$r \geqslant P_{\rm succ}\left[1 - H(\delta_{\rm p}^z)\right] - H(\delta_{\rm b}^z). \tag{10}$$

Here $P_{\rm succ}$ is the probability that Bob successfully performs the virtual $X-$basis measurement, which is given by

$$P_{\rm succ} = \frac{\langle\Psi_Z^3|\Psi_Z^3\rangle}{\langle\Psi_Z^1|\Psi_Z^1\rangle}. \tag{11}$$

3. Key rate

According to the model given above, Alice and Bob should maximize the phase error $\delta_{\rm p}^z$ and minimize the probability $P_{\rm succ}$ to estimate the lower bound of key rate. In other words, the legitimate users should solve the following problem,

$$\begin{gathered} \max_{\rho_{\rm E}} : \delta_{\rm p}^z, \quad \text{and} \quad \min_{\rho_{\rm E}} : P_{\rm succ} \\ \text{subject to} : \delta_{\rm b}^z, \delta_{\rm b}^x, P_{ij}^{\beta\beta'} \end{gathered} \tag{12}$$

Here the constrictions $\delta_{\rm b}^{z(x)}$ is the bit error in Z-basis (X-basis), and $P_{ij}^{\beta\beta'}$ is the probability that Alice sends the quantum state in $\beta-$basis with bit i and Bob successfully detects bit j in $\beta'-$basis. Note that all of them ($\delta_{\rm b}^z(x)$ and $P_{ij}^{\beta\beta'}$) can be directly measured in experiment. In the appendix A, we prove that $P_{i,j}^{\beta,\beta'}$ can be written as

$$\begin{aligned} P_{ij}^{zz} &= {\rm Tr}\{\rho_{\rm E}[(f_{z_i}\otimes Z_{ij})^+ \cdot f \cdot (f_{z_i}\otimes Z_{ij})]\otimes F_j^+F_j\}, \\ P_{ij}^{xx} &= {\rm Tr}\{\rho_{\rm E}[(f_{x_i}\otimes X_{ij})^+ \cdot f \cdot (f_{x_i}\otimes X_{ij})]\otimes F_j^+F_j\}, \\ P_{ij}^{xx,{\rm vir}} &= \frac{1}{4}\,{\rm Tr}\left[\rho_{\rm E}(Z_{ij}^{\rm p}\otimes C^+C)\right]. \end{aligned} \tag{13}$$

The upscript 'vir' means the virtual measurement in $X-$basis is performed by Alice and Bob. The parameters required in the equation above are given in appendix A. Z_{ij} and X_{ij} represent the accuracy of encoded quantum state in Z-basis and X-basis, which are given by equations (A13) and (A17). Z_{ij}^{p} is the accuracy of encoded quantum state in virtual $X-$basis measurement, which is defined by equation (A28). $f_{z_{0(1)}}$ is a diagonal matrix that represents the fidelity of side-channel state between the given quantum state $|\omega_{z_{0(1)}}\rangle$ and all the four quantum state $|\omega_i\rangle$, which is defined in equations (A11) and (A14). And the definition of $f_{x_{0(1)}}$ is the same as that of $f_{z_{0(1)}}$, which is given by equation (A18). $F_j^+F_j$ is the detection matrix of two detectors ($j=0,1$), and C can be directly calculated by using $F_j^+F_j$.

Then the bit/phase error rate (equation (8)) and the probability that Bob successfully performed the virtual measurement (equation (11)) can be rewritten as

$$\delta_{\mathrm{b}}^{z}=\frac{P_{01}^{zz}+P_{10}^{zz}}{P_{00}^{zz}+P_{01}^{zz}+P_{10}^{zz}+P_{11}^{zz}}, \tag{14a}$$

$$\delta_{\mathrm{b}}^{x}=\frac{P_{01}^{xx}+P_{10}^{xx}}{P_{00}^{xx}+P_{01}^{xx}+P_{10}^{xx}+P_{11}^{xx}}, \tag{14b}$$

$$\delta_{\mathrm{p}}^{z}=\frac{P_{01}^{xx,\mathrm{vir}}+P_{10}^{xx,\mathrm{vir}}}{P_{00}^{xx,\mathrm{vir}}+P_{01}^{xx,\mathrm{vir}}+P_{10}^{xx,\mathrm{vir}}+P_{11}^{xx,\mathrm{vir}}}, \tag{14c}$$

$$P_{\mathrm{succ}}=\frac{P_{00}^{xx,\mathrm{vir}}+P_{01}^{xx,\mathrm{vir}}+P_{10}^{xx,\mathrm{vir}}+P_{11}^{xx,\mathrm{vir}}}{P_{00}^{zz}+P_{01}^{zz}+P_{10}^{zz}+P_{11}^{zz}}. \tag{14d}$$

By solving equation (12) under the given condition equation (14), the lower bound of key rate can be estimated, when SPS is adopted by Alice and Bob. However, due to the unavailability of SPS in practical applications, the weak coherent source is always used. Then, according to the GLLP's analysis [3], the key rate should be rewritten as

$$r_w \geqslant P_{\mathrm{succ}}\mu \mathrm{e}^{-\mu}Y_1^{\mu}\left[1-H(\delta_{\mathrm{p},1}^{z,\mu})\right]-Q_{\mu}f_{\mathrm{EC}}H(E_{\mu}^{\mathrm{b}}). \tag{15}$$

Here μ is the intensity of signal state. f_{EC} is the efficiency of error correction. Q_{μ} (E_{μ}^{b}) is the total gain (bit error rate) of signal state. Y_1^{μ} and $\delta_{\mathrm{p},1}^{z,\mu}$ are the yield and phase error rate of single photon pulse from signal state. The phase error rate $\delta_{\mathrm{p},1}^{z,\mu}$ should be estimated and maximized with the same method given above (equation (12)), which is given by

$$\begin{aligned}&\min_{\rho_{\mathrm{E}}}: P_{\mathrm{succ}} \quad \text{and} \quad \max_{\rho_{\mathrm{E}}}\delta_{\mathrm{p},1}^{z,\mu}\\ &\text{subject to}: \delta_{\mathrm{b},1}^{x,\mu},\delta_{\mathrm{b},1}^{z,\mu},P_{i,j}^{\beta,\beta'}\end{aligned} \tag{16}$$

Here $\delta_{\mathrm{b},1}^{x,\mu},\delta_{\mathrm{b},1}^{z,\mu}$ are the bit error rate of single photon pulse, which can be estimated by the decoy state method [26–28],

$$\begin{aligned}Y_1^{\mu}&\geqslant\frac{\mu}{\mu\nu-\nu^2}\left[\mathrm{e}^{\nu}Q_{\nu}-\frac{\nu^2}{\mu^2}\mathrm{e}^{\mu}Q_{\mu}-\frac{\mu^2-\nu^2}{\mu^2}Y_0-2D_{\mu\nu}\left(\mathrm{e}^{\nu}-\mathrm{e}^{\nu\left(1-\eta_{\mathrm{Bob}}^{\mathrm{cal}}\right)}\right)\right]\\ \delta_{b,1}^{z(x),\mu}&\leqslant\min\left\{K^{\mu},K^{\nu},K^{\mu\nu}\right\},\end{aligned} \tag{17}$$

where $D_{\mu\nu}=\frac{1}{2}\mathrm{tr}\left|\rho_{\mu}-\rho_{\nu}\right|$ is the trace distance of different decoy states [29], which shows the distinguishability of signal state and decoy state. And

$$\begin{aligned}K^{\mu}&=\frac{\mathrm{e}^{\mu}Q_{\mu}E_{\mu}-e_0Y_0}{\mu Y_1^{\mu}}\\ K^{\nu}&=\frac{\mathrm{e}^{\nu}Q_{\nu}E_{\nu}-e_0Y_0+2\nu D_{\mu\nu}\eta_{\mathrm{Bob}}^{\mathrm{cal}}}{\nu Y_1^{\mu}}\\ K^{\mu\nu}&=\frac{\mathrm{e}^{\mu}Q_{\mu}E_{\mu}-\mathrm{e}^{\nu}Q_{\nu}E_{\nu}+2D_{\mu\nu}\left(\mathrm{e}^{\nu}-\mathrm{e}^{\nu\left(1-\eta_{\mathrm{Bob}}^{\mathrm{cal}}\right)}\right)}{(\mu-\nu)Y_1^{\mu}}.\end{aligned} \tag{18}$$

Here $\eta_{\mathrm{Bob}}^{\mathrm{cal}}$ is the calibrated transmittance of Bob's system. In the worst case, the transmittance of Bob's system is unknown, $\eta_{\mathrm{Bob}}^{\mathrm{cal}}=1$. But if the transmittance of Bob's optical devices η_{Bob} and detection efficiency of SPDs (η_{d}) are carefully calibrated and monitored, $\eta_{\mathrm{Bob}}^{\mathrm{cal}}=\eta_{\mathrm{Bob}}\times\eta_{\mathrm{d}}$.

4. Simulation and discussion

In this section we evaluate the performance of practical QKD system with potential imperfections in source and detection. Before the simulation, we first discuss the imperfections considered in our model (also see table 1).

4.1. Inaccuracy of encoded state

In practical QKD system, due to the finite extinction ratio of encoder, the prepared quantum states by Alice may different from the ideal states required by the QKD protocol. For example, Alice wants to send a quantum state with polarization H, but the practical quantum state may be $\sqrt{1-\delta}|H\rangle+\sqrt{\delta}|V\rangle$, here $\delta \neq 0$ is a small deviation. Generally speaking, the practical quantum states prepared by Alice can be written as

$$\begin{aligned}|\gamma_{z_0}\rangle &= \cos(\delta_1)|z_0\rangle + \sin(\delta_1)|z_1\rangle,\\ |\gamma_{z_1}\rangle &= \sin(\delta_2)|z_0\rangle + \cos(\delta_2)|z_1\rangle,\\ |\gamma_{x_0}\rangle &= \cos(\delta_3)|x_0\rangle + \sin(\delta_3)|x_1\rangle,\\ |\gamma_{x_1}\rangle &= \sin(\delta_4)|x_0\rangle + \cos(\delta_4)|x_1\rangle.\end{aligned} \tag{19}$$

Note that although here we assume the quantum prepared by Alice is pure, our analysis is also valid for the case of mixed state. Since the mixed state can be purified by introducing another system belonging to Eve. Thus, as defined in table 1, the fidelity between practical quantum state and ideal quantum state is given by

$$f_{\mathrm{en}}^{i} = \cos^2(\delta_i) \equiv 1-\varepsilon_1^i. \tag{20}$$

Here $i = 1, 2, 3, 4$, and $\varepsilon_1^i = \sin^2(\delta_i)$ represents the inaccuracy of each practical quantum state.

4.2. Distinguishable side-channels

As one of security assumptions, Alice should only modulate her bit and basis information in the encode dimension. But, duo to the imperfection of devices or implementation, the quantum states sent by Alice may be distinguishable in other side-channels, such as time (t), wavelength (λ), waveform (w), mode (m), and so on. Generally speaking, there may be correlation in all of these side-channels, thus the quantum state of side channel should be written as

$$|\omega_{\beta_i}(t,\lambda,w,m,\ldots)\rangle. \tag{21}$$

However, in practical situations, it is difficult for the legitimate parties to evaluate the correlation of different side-channels for the practical QKD system in experiment, then it is hard to completely describe the quantum state above. Thus, for simple of simulation, here we assume that each side-channel is independent, then the quantum state can be rewritten as

$$\begin{aligned}&|\omega_{\beta_i}(t,\lambda,w,m,\ldots)\rangle\\ &\quad= |\omega_{\beta_i}(t)\rangle\otimes|\omega_{\beta_i}(\lambda)\rangle\otimes|\omega_{\beta_i}(w)\rangle\otimes|\omega_{\beta_i}(m)\rangle\otimes\cdots\end{aligned} \tag{22}$$

Thus, as defined in table 1, the fidelity between different side-channels is given by

$$\begin{aligned}f_{\mathrm{sc}}^{i,j} &= |\langle\omega_{\beta_i}(t,\lambda,w,m,\ldots)|\omega_{\beta_i}(t,\lambda,w,m,\ldots)|^2\\ &= |\langle|\omega_{\beta_i}(t)|\omega_{\beta_i}(t)\rangle|^2\cdot|\langle|\omega_{\beta_i}(\lambda)|\omega_{\beta_i}(\lambda)\rangle|^2\cdot|\langle|\omega_{\beta_i}(w)|\omega_{\beta_i}(w)\rangle|^2\cdot|\langle|\omega_{\beta_i}(m)|\omega_{\beta_i}(m)\rangle|^2\ldots\\ &\equiv 1-\varepsilon_2^{i,j}\end{aligned} \tag{23}$$

Here $\varepsilon_2^{i,j}$ represent the consistency of each quantum state in side-channels.

4.3. Trojan-horse

Due to the reflection of optical devices and the finite isolation, Eve could inject strong pulse into Alice's zone, and gets parts of information by analyzing the reflected photon. The four quantum states of reflected Trojan-horse photon can be written as [18]

$$|\sqrt{\mu_{\mathrm{out}}}\rangle,\quad |-\sqrt{\mu_{\mathrm{out}}}\rangle,\quad |+i\sqrt{\mu_{\mathrm{out}}}\rangle,\quad |-i\sqrt{\mu_{\mathrm{out}}}\rangle. \tag{24}$$

Here μ_{out} is the intensity of reflected Trojan-horse photon. In the simulation, we assume phase-coding is used and the average intensities of all Trojan-horse pulses are the same. For other coding method

(polarization, time-bin) and different intensity of Trojan-horse pulse, it is easily to rewrite the quantum state above. Then, as defined in table 1, the fidelity of Trojan-horse pulse is given by

$$f_{\mathrm{th}} = \left[f_{\mathrm{th}}^{i,j}\right] = \begin{bmatrix} 1 & e^{-4\mu_{\mathrm{out}}} & \mathrm{e}^{-2\mu_{\mathrm{out}}} & e^{-2\mu_{\mathrm{out}}} \\ \mathrm{e}^{-4\mu_{\mathrm{out}}} & 1 & \mathrm{e}^{-2\mu_{\mathrm{out}}} & \mathrm{e}^{-2\mu_{\mathrm{out}}} \\ \mathrm{e}^{-2\mu_{\mathrm{out}}} & \mathrm{e}^{-2\mu_{\mathrm{out}}} & 1 & \mathrm{e}^{-4\mu_{\mathrm{out}}} \\ \mathrm{e}^{-2\mu_{\mathrm{out}}} & \mathrm{e}^{-2\mu_{\mathrm{out}}} & \mathrm{e}^{-4\mu_{\mathrm{out}}} & 1 \end{bmatrix} \equiv \left[1 - \varepsilon_3^{i,j}\right]. \tag{25}$$

4.4. Distinguishable decoy state

Decoy state method has been considered as a standard technology to defeat photon-number dependent attacks when non-single photon source is used. One of important assumptions for decoy state method is that the decoy states are indistinguishable in any dimension excepting the intensity. But, due to the imperfection of implementation, this assumption may be broken in practical system. If the density matrix of decoy state is written as [29]

$$\rho_k' = \rho_k \otimes \rho_k(\lambda) = \sum_{n=0}^{\infty} \int_{\lambda} \mathrm{d}\lambda P_n^k f_k(\lambda) |n, \lambda\rangle\langle n, \lambda|. \tag{26}$$

Here $\rho_k(\lambda)$ is the quantum state leaked to Eve to distinguish different decoy states, λ includes all the dimensions that can be measured by Eve. $f_k(\lambda)$ is the probability distribution of decoy states in variable λ. Then the imperfection of decoy states can be characterized by the trace distance, which is given by

$$D_{k,l} = \frac{1}{2}\mathrm{tr}\,|\rho_k(\lambda) - \rho_l(\lambda)| \equiv \varepsilon_4^{k,l}. \tag{27}$$

4.5. Detection mismatch

The detection mismatch is one of major problems in SPDs, which can be described by the detection efficiency matrices F_0 and F_1. Generally speaking, duo to the following reasons, it is very difficult to completely characterize the matrices F_0 and F_1 in experiment. (1) There may be many dimensions which can induce the detection mismatch, such as time [36], wavelength [37], polarization [38], and so on. (2) In parts of dimensions, e.g. time, the detection efficiency curve of SPDs follow continuous distribution. Then the dimension of detection matrices is infinite. (3) The matrices F_0 and F_1 may be non-diagonal, since the detector may have non-trivial efficiency responses to signals entangled across the different dimension or variable.

Thus, for simple of simulation, here we ignore the correlation of different dimension and variable, and assume the matrices F_0 and F_1 are diagonal. We also only consider two detection variables λ_0 and λ_1, which means F_0 and F_1 are matrices with dimension two. Here λ_0 and λ_1 can be any variable that control the efficiency of detector, such as time, wavelength, polarization, and son on. Then, F_0 and F_1 can be written as

$$F_0 = \begin{bmatrix} \eta_0(\lambda_0) & 0 \\ 0 & \eta_0(\lambda_1) \end{bmatrix}, \qquad F_1 = \begin{bmatrix} \eta_1(\lambda_0) & 0 \\ 0 & \eta_1(\lambda_1) \end{bmatrix}, \tag{28}$$

here $\eta_m(\lambda_n)$ means the detection efficiency of detector m at variable λ_n, and $m, n = 0, 1$.

4.6. Numerical simulation

With the definition above, all the required parameters can be rewritten as the function of ε_1^i, $\varepsilon_2^{i,j}$, $\varepsilon_3^{i,j}$ and $\varepsilon_4^{k,l}$. For example, Z_{00} and Z_{10} in equation (A13) can be rewritten as

$$\begin{aligned} Z_{00} &= (\sqrt{1-\varepsilon_1^1}, \sqrt{\varepsilon_1^1}, 0, 0) \\ Z_{10} &= (\sqrt{\varepsilon_1^2}, \sqrt{1-\varepsilon_1^2}, 0, 0) \end{aligned} \tag{29}$$

and the fidelity of side channels can be rewritten as

$$f_{i,j} = \sqrt{(1-\varepsilon_2^{i,j})(1-\varepsilon_3^{i,j})} = \sqrt{1-\varepsilon_{23}^{i,j}}. \tag{30}$$

Here $\varepsilon_{23}^{i,j} = \varepsilon_2^{i,j} + \varepsilon_3^{i,j} - \varepsilon_2^{i,j}\varepsilon_3^{i,j} \approx \varepsilon_2^{i,j} + \varepsilon_3^{i,j}$ is the total deviation of side-channel and Trojan-horse pulse.

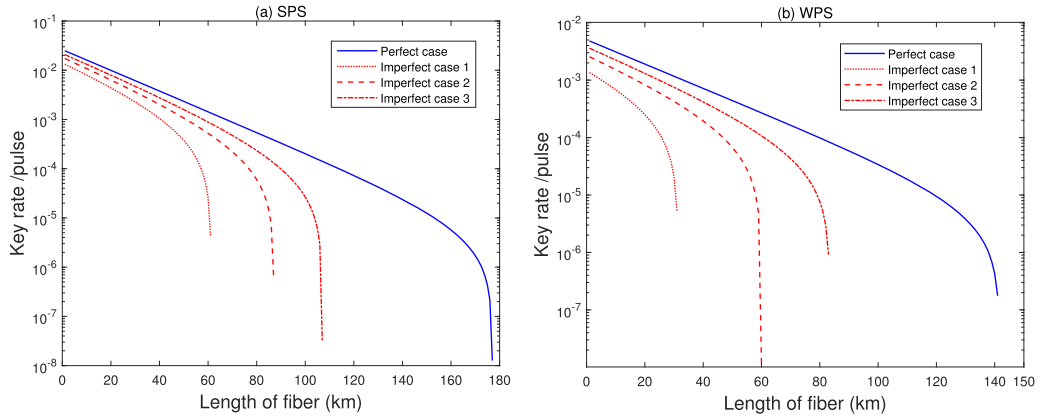

Figure 2. The estimated key rate for both SPS (a) and WPS (b), when both source and detection imperfections are considered. The blue lines are the key rate for perfect system. The red lines are the key rate with different imperfections. In the simulation, the value of security parameters is selected based on different experiments [18, 36, 38, 39] which is listed in table 2, and other parameters about the QKD system come from the experiment results of GYS [40]: dark count $Y_0 = 1.7 \times 10^{-6}$, the optical error rate $e_{\rm det} = 3.3\%$, the transmittance of Bob's optical system $\eta_{\rm Bob} = 0.045$, the loss of fiber 0.21dB km^{-1}, the efficiency of error correction $f_{\rm EC} = 1.22$. In the case of WPS, we assume that weak + vacuum decoy state method is used, and the intensity of signal state (decoy state) is set as $\mu = 0.48$ ($\nu = 0.01$) which is optimal under the GYS parameters [41]. The method for simulations is given in appendix B.

Table 2. The value of security parameters used in the simulations of figures 2 to 4. Here, for simple of simulation, we assume that $\varepsilon_1^i \equiv \varepsilon_1$ for all i, $\varepsilon_2^{i,j} \equiv \varepsilon_2$ for all i, j, $\eta_0(\lambda_0) = \eta_1(\lambda_1) = 1$ and $\eta_0(\lambda_1) = \eta_1(\lambda_0) = \eta_{\rm DM}$. At the same time, we also assume that only weak + vacuum decoy state method with intensities μ (signal state) and ν (decoy state) is used, thus $D_{k,l} = D_{\mu,\nu}$. The value of security parameters is selected based on different experiments [18, 36, 38, 39].

	Source			Detection	
Parameter	ε_1	ε_2	$\mu_{\rm out}$	$D_{\mu\nu}$	$\eta_{\rm DM}$
Value (Case 1)	10^{-4}	10^{-5}	10^{-6}	10^{-4}	0.15
Value (Case 2)	10^{-5}	10^{-4}	10^{-5}	10^{-5}	0.1
Value (Case 3)	10^{-5}	10^{-5}	10^{-6}	10^{-5}	0.05

Furthermore, since the loss of channel and finite detection efficiency of SPDs, Eve could enhance the source flaws by exploiting these kinds of loss. Thus, the inaccuracy of quantum state and consistence of side-channel should be rewritten as

$$\begin{aligned} \varepsilon_1^i &\to \varepsilon_1'^i = \varepsilon_1^i/\eta \\ \varepsilon_{2,3}^{i,j} &\to \varepsilon_{2,3}'^{i,j} = \varepsilon_{2,3}^{i,j}/\eta \approx \varepsilon_2^{i,j}/\eta + \varepsilon_3^{i,j}/\eta \end{aligned} \tag{31}$$

where η is the transmittance of system, including the transmittance of channel $\eta_{\rm c}$, the transmittance of Bob's optical devices $\eta_{\rm Bob}$, and the detection efficiency of Bob's SPDs $\eta_{\rm d}$. Generally speaking,

$$\eta = \eta_{\rm c} \times \eta_{\rm Bob} \times \eta_{\rm d}. \tag{32}$$

Submitting equations (31) and (32) into the model given above, the key rate for both SPS (equation (10)) and WPS (equation (16)) can be estimated, which is shown in figure 2. The results clearly show that the estimated key rate will be rapidly decreased, but communication with distance longer than 100 km is still possible if the maker of the QKD system can make sure the deviation of practical devices is small.

In order to analyze which part, source or detection, is the main factor for the decrease of key rate, the estimated key rate for WPS with only source or detection imperfection is also shown in figure 3. It shows that the decrease of key rate in source is much larger than that of the detection. One of major reasons is that Eve can enhance the source flaws by exploiting the total loss of system, including the channel, the optical device of Bob and detection efficiency of SPDs (see equation (32)). But, in some practical situations, parts of loss can be carefully calibrated and monitored. For example, in some QKD system, only passive optical devices are used by Bob, and the transmittance of these devices is not easy to be changed by Eve (or Bob can locally monitor the transmittance of these optical devices). At the same time, the average detection efficiency of SPDs may also be monitored by Bob. In fact, calibrating and monitoring the detection

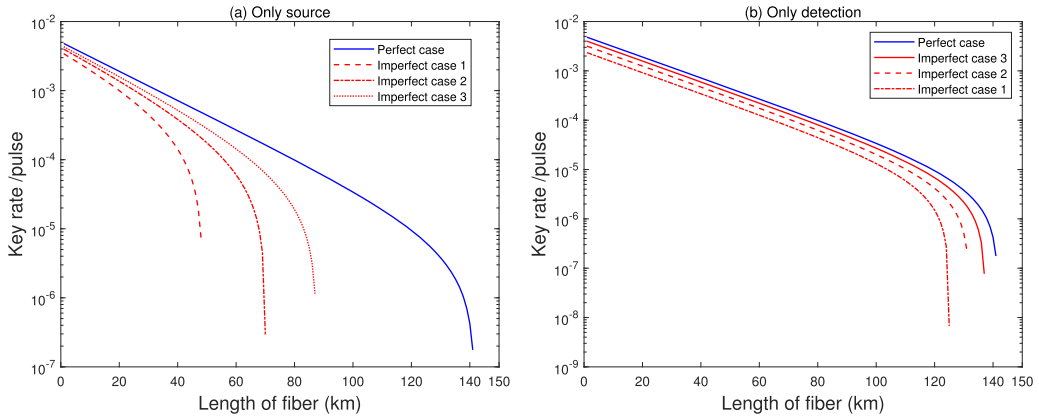

Figure 3. The estimated key rate for WPS, if only imperfections on source (a) or detection (b) are taken into account. The blue lines are the key rate for perfect system, and the red lines are the key rate with different imperfections. The parameters used in the simulation are the same as that of figure 2 and table 2. In part (a), only source imperfections are considered and the detection is assumed as perfect devices. And in part (b), only detection mismatch is analyzed and the source is assumed as perfect devices.

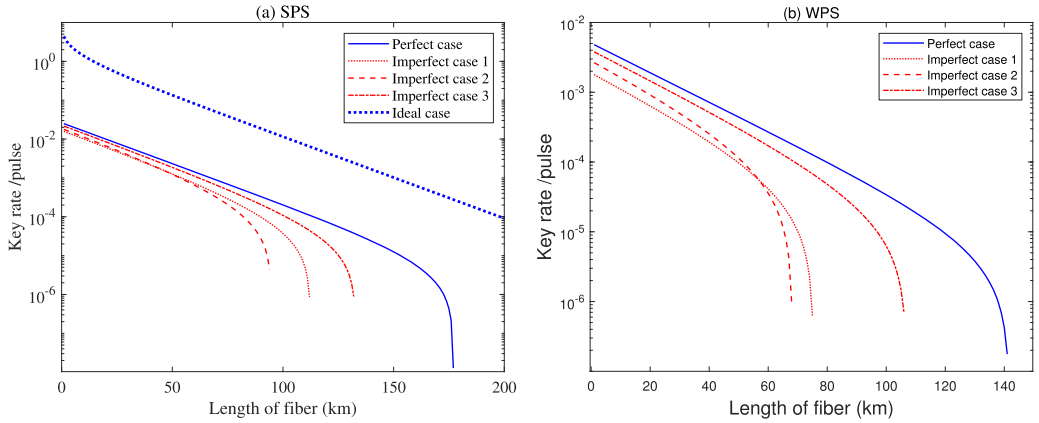

Figure 4. The improved key rate for both SPS and WPS, when parts of loss in Bob's devices can be carefully calibrated and monitored (see equation (33)), for example, the optical devices and the SPDs. The blue lines are the key rate for perfect QKD system without any practical flaws, and the read lines are the practical key rate with different imperfections of practical devices. The doted blue line shows the fundamental rate-loss bound for the ideal system, such as unit detector efficiencies, zero dark count rates, zero intrinsic error, unit error-correction efficiency, and so on. According to the analysis of reference [42], the linear bound is about $-\log_2(1-\eta_c)$. The parameters used in the simulation are the same as that of figure 2 and table 2.

efficiency of SPDs have been used to secure the SPDs [34, 35]. In other words, equation (32) is a worst case, and it can be improved in some practical situations, thus a reasonable assumption is that

$$\eta = \eta_c. \tag{33}$$

With the calibrated transmittance above, the practical key rate can be improved, see figure 4. For example, in the case of WPS with $\varepsilon_1 = \varepsilon_2 = 10^{-5}$, $\mu_{\text{out}} = 10^{-6}$, $D_{\mu\nu} = 10^{-5}$ and $\eta_{\text{DM}} = 0.05$, the maximal distance of security communication can be increased from about 80 km to 110 km.

5. Summary

The unconditional security of generated key by QKD will be compensated by the imperfection of practical devices. Many models have been proposed to analyze these imperfections in practical QKD system. But, in most of these models, the imperfection are considered individually. In this paper, we take both the source and detection imperfections into account in one model, then the performance of practical QKD system is evaluated.

In the source parts, our model includes almost all of imperfection of source, such as, inaccuracy of encoded quantum state, distinguishable side-channels of source, distinguishable decoy states, Trojan-horse, and so on. But, when source flaws are taken into account, the key rate will be rapidly reduced. One of major reasons is that Eve could enhance the source flaws by exploiting the loss of system, since the channel is

totally controlled by her. Here we discuss a possible way to overcome this problem by introducing a reasonable assumption. It is that the legitimate parties can divide the loss as two parts, untrusted loss (the loss of quantum channel) and trusted loss (the transmittance of Bob's optical devices or the detection efficiency of SPDs). Then if the trusted loss can be carefully calibrated and monitored, the key rate will be improved.

In the detection parts, although the major imperfection (detection mismatch) is considered in our model, there still are many other flaws, such as weak-randomness of basis choice, the backflash of SPDs, and so on. In fact, how to take all of these detection flaws together is still an open question. And we will discuss it in our further work.

Acknowledgments

The authors thank Fred Fung for helpful discussion about the detection model and simulation. This work was supported by the National Natural Science Foundation of China (NSFC) (11674397).

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors.

Appendix A. The proof of 13

According to equation (5), we have

$$\begin{aligned}
|\Psi_\beta\rangle &= \sum_{i,t} E^{it}_{\mathrm{BT}}|\psi_\beta\rangle|0\rangle_{\mathrm{T}}|i\rangle_{\mathrm{E}} \\
&= \frac{1}{\sqrt{2}}\sum_{i,t,k} E^{it}_{\mathrm{SBT}}|\beta_k\rangle_{\mathrm{A}}\left|\gamma_{\beta_k}\right\rangle_{\mathrm{B}}\left|\omega_{\beta_k}\right\rangle_{\mathrm{S}}|0\rangle_{\mathrm{T}}|i\rangle_{\mathrm{E}} \\
&= \frac{1}{\sqrt{2}}\sum_{i,t,k} E^{it}_{\mathrm{BT}}|\beta_k\rangle_{\mathrm{A}}\left|\gamma_{\beta_k}\right\rangle_{\mathrm{B}}|\omega_t\rangle\langle\omega_t\left|\omega_{\beta_k}\right\rangle_{\mathrm{S}}|0\rangle_{\mathrm{T}}|i\rangle_{\mathrm{E}} \\
&= \frac{1}{\sqrt{2}}\sum_{i,t,k} E^{it}_{\mathrm{BT}}|\beta_k\rangle_{\mathrm{A}}\left|\gamma_{\beta_k}\right\rangle_{\mathrm{B}}|\omega_t\rangle_{\mathrm{S}} f_t^{\beta_k}|0\rangle_{\mathrm{T}}|i\rangle_{\mathrm{E}} \\
&= \frac{1}{\sqrt{2}}\sum_{i,t,j,k} |\beta_k\rangle_{\mathrm{A}}(E^{i,t,j}_{\mathrm{B}}\left|\gamma_{\beta_k}\right\rangle_{\mathrm{B}})|\omega_t\rangle_{\mathrm{S}} f_t^{\beta_k}(E^{i,t,j}_{\mathrm{T}}|0\rangle_{\mathrm{T}})|i\rangle_{\mathrm{E}} \\
&= \frac{1}{\sqrt{2}}\sum_{i,t,j,k} |\beta_k\rangle_{\mathrm{A}}(E^{i,t,j}_{\mathrm{B}}\left|\gamma_{\beta_k}\right\rangle_{\mathrm{B}})|\omega_t\rangle_{\mathrm{S}} f_t^{\beta_k}|\xi(i,t,j)\rangle_{\mathrm{T}}|i\rangle_{\mathrm{E}}.
\end{aligned} \tag{A1}$$

Here $E^{it}_{\mathrm{BT}} = \sum_j E^{i,t,j}_{\mathrm{B}} \otimes E^{i,t,j}_{\mathrm{T}}$, $f_t^{\beta_k} = \langle\omega_t|\omega_{\beta_k}\rangle$, and $|\xi(i,t,j)\rangle = E^{i,t,j}_{\mathrm{T}}|0\rangle$. Note the fact that $E^{i,t,j}_{\mathrm{B}} = a_I^{i,t,j} I + a_X^{i,t,j} X + a_Y^{i,t,j} Y + a_Z^{i,t,j} Z$, here I is the unity matrix and X, Y, Z are Pauli matrices, and $|\gamma_{\beta_k}\rangle = \alpha^0_{\beta_k}|\beta_0\rangle + \alpha^1_{\beta_k}|\beta_1\rangle$. Thus,

$$\begin{aligned}
|\Psi_\beta\rangle &= \frac{1}{\sqrt{2}}\sum_{i,t,j,k} |\beta_k\rangle_{\mathrm{A}}\left(\sum_{l,k'} a_l^{i,t,j}\alpha^{k'}_{\beta_k} L|\beta_{k'}\rangle_{\mathrm{B}}\right) f_t^{\beta_k}|\omega_t\rangle_{\mathrm{S}}|\xi(i,t,j)\rangle_{\mathrm{T}}|i\rangle_{\mathrm{E}} \\
&= \frac{1}{\sqrt{2}}\sum_{i,t,j}\left[\sum_{l,k,k'} |\beta_k\rangle_{\mathrm{A}}(a_l^{i,t,j}\alpha^{k'}_{\beta_k} L|\beta_{k'}\rangle_{\mathrm{B}}) f_t^{\beta_k}|\omega_t\rangle_{\mathrm{S}}\right]|\xi(i,t,j)\rangle_{\mathrm{T}}|i\rangle_{\mathrm{E}}
\end{aligned} \tag{A2}$$

here $l, L = I, X, Y, Z$, and $k, k' = 0, 1$.

(a) $|\Psi^1_Z\rangle$

We first get the bit error rate in Z-basis δ_b^z. According to equation (A2), we have

$$\begin{aligned}|\Psi_Z^1\rangle &= F_Z|\Psi_Z\rangle \\ &= \frac{1}{\sqrt{2}}\sum_{i,t,j}\left[\sum_{l,k,k'}\langle z_0|L|z_{k'}\rangle|z_k\rangle_{\mathrm{A}}(a_l^{i,t,j}\alpha_{z_k}^{k'}|z_0\rangle_{\mathrm{B}})f_t^{z_k}|\omega_t\rangle_{\mathrm{S}}\right]F_0|\xi(i,t,j)\rangle_{\mathrm{T}}|i\rangle_{\mathrm{E}} \\ &\quad+\frac{1}{\sqrt{2}}\sum_{i,t,j}\left[\sum_{l,k,k'}\langle z_1|L|z_{k'}\rangle|z_k\rangle_{\mathrm{A}}(a_l^{i,t,j}\alpha_{z_k}^{k'}|z_1\rangle_{\mathrm{B}})f_t^{z_k}|\omega_t\rangle_{\mathrm{S}}\right]F_1|\xi(i,t,j)\rangle_{\mathrm{T}}|i\rangle_{\mathrm{E}} \\ &\equiv \sum_{i,t,j}\widetilde{L}_0F_0|\xi(i,t,j)\rangle|i\rangle+\sum_{i,t,j}\widetilde{L}_1F_1|\xi(i,t,j)\rangle|i\rangle.\end{aligned} \tag{A3}$$

Here

$$\begin{aligned}\widetilde{L}_0 &= \frac{1}{\sqrt{2}}\sum_{l,k,k'}\langle z_0|L|z_{k'}\rangle|z_k\rangle_{\mathrm{A}}(a_l^{i,t,j}\alpha_{z_k}^{k'}|z_0\rangle_{\mathrm{B}})f_t^{z_k}|\omega_t\rangle_{\mathrm{S}} \\ &= \frac{1}{\sqrt{2}}\sum_k\left[\sum_l a_l^{i,t,j}(\alpha_{z_k}^0\langle z_0|L|z_0\rangle+\alpha_{z_k}^1\langle z_0|L|z_1\rangle)\right]|z_k\rangle|z_0\rangle f_t^{z_k}|\omega_t\rangle \\ &= \sum_k\left[\frac{1}{\sqrt{2}}(a_I^{i,t,j}+a_Z^{i,t,j})\alpha_{z_k}^0+\frac{1}{\sqrt{2}}(a_X^{i,t,j}-a_Y^{i,t,j})\alpha_{z_k}^1\right]|z_k\rangle|z_0\rangle f_t^{z_k}|\omega_t\rangle \\ &= \sum_k(a_{00}^{i,t,j}\alpha_{z_k}^0+a_{01}^{i,t,j}\alpha_{z_k}^1)|z_k\rangle|z_0\rangle f_t^{z_k}|\omega_t\rangle \\ &\equiv f_t^{z_0}(a_{00}^{i,t,j}\alpha_{z_0}^0+a_{01}^{i,t,j}\alpha_{z_0}^1)|z_0\rangle|z_0\rangle|\omega_t\rangle+f_t^{z_1}(a_{00}^{i,t,j}\alpha_{z_1}^0+a_{01}^{i,t,j}\alpha_{z_1}^1)|z_1\rangle|z_0\rangle|\omega_t\rangle\end{aligned} \tag{A4}$$

and

$$\begin{aligned}\widetilde{L}_1 &= \frac{1}{\sqrt{2}}\sum_{l,k,k'}\langle z_1|L|z_{k'}\rangle|z_k\rangle_{\mathrm{A}}(a_l^{i,t,j}\alpha_{z_k}^{k'}|z_1\rangle_{\mathrm{B}})f_t^{z_k}|\omega_t\rangle_{\mathrm{S}} \\ &= \frac{1}{\sqrt{2}}\sum_k\left[\sum_l a_l^{i,t,j}(\alpha_{z_k}^0\langle z_1|L|z_0\rangle+\alpha_{z_k}^1\langle z_1|L|z_1\rangle)\right]|z_k\rangle|z_1\rangle f_t^{z_k}|\omega_t\rangle \\ &= \sum_k\left[\frac{1}{\sqrt{2}}(a_X^{i,t,j}+a_Y^{i,t,j})\alpha_{z_k}^0+\frac{1}{\sqrt{2}}(a_I^{i,t,j}-a_Z^{i,t,j})\alpha_{z_k}^1\right]|z_k\rangle|z_1\rangle f_t^{z_k}|\omega_t\rangle \\ &= \sum_k(a_{10}^{i,j}\alpha_{z_k}^0+a_{11}^{i,j}\alpha_{z_k}^1)|z_k\rangle|z_1\rangle f_t^{z_k}|\omega_t\rangle \\ &= f_t^{z_0}(a_{10}^{i,t,j}\alpha_{z_0}^0+a_{11}^{i,t,j}\alpha_{z_0}^1)|z_0\rangle|z_1\rangle|\omega_t\rangle+f_t^{z_1}(a_{10}^{i,t,j}\alpha_{z_1}^0+a_{11}^{i,t,j}\alpha_{z_1}^1)|z_1\rangle|z_1\rangle|\omega_t\rangle\end{aligned} \tag{A5}$$

where

$$\begin{aligned}a_{00}^{(i,t,j)} &= \frac{a_I^{(i,t,j)}+a_Z^{(i,t,j)}}{\sqrt{2}} & a_{01}^{(i,t,j)} &= \frac{a_X^{(i,t,j)}-a_Y^{(i,t,j)}}{\sqrt{2}} \\ a_{10}^{(i,t,j)} &= \frac{a_X^{(i,t,j)}+a_Y^{(i,t,j)}}{\sqrt{2}} & a_{11}^{(i,t,j)} &= \frac{a_I^{(i,t,j)}-a_Z^{(i,t,j)}}{\sqrt{2}}.\end{aligned} \tag{A6}$$

Thus the probability that Alice gets Z_0 and Bob gets Z_0 can be written as

$$\begin{aligned}P_{00}^{zz} &= \sum_i\sum_{tt',jj'}\langle\xi(i,t,j)|F_0^+f_t^{z_0}(a_{00}^{i,t,j}\alpha_{z_0}^0+a_{01}^{i,t,j}\alpha_{z_0}^1)f_t^{t'}(a_{00}^{i,t',j'}\alpha_{z_0}^0+a_{01}^{i,t',j'}\alpha_{z_0}^1)f_{t'}^{z_0}F_0|\xi(i,t,j)\rangle \\ &= \sum_i\sum_{tt'}\xi^+(i,t)A_{i,t}^+f_t^{t'}A_{i,t}\otimes F_0^+F_0\xi(i,t)\end{aligned} \tag{A7}$$

where

$$\xi(i,t)=(|\xi(i,t,1)\rangle,|\xi(i,t,2)\rangle,\dots)^+, \tag{A8}$$

and

$$A_{i,t} = f_t^{z_0}(\alpha_{z_0}^0, \alpha_{z_0}^1, 0, 0) \begin{bmatrix} a_{00}^{i,t,1} & a_{00}^{i,t,2} & \cdots \\ a_{01}^{i,t,1} & a_{01}^{i,t,2} & \cdots \\ a_{10}^{i,t,1} & a_{10}^{i,t,2} & \cdots \\ a_{11}^{i,t,1} & a_{00}^{i,t,2} & \cdots \end{bmatrix} \equiv f_t^{z_0}(\alpha_{z_0}^0, \alpha_{z_0}^1, 0, 0) B_{i,t}. \tag{A9}$$

Thus

$$\begin{aligned} P_{00}^{zz} &= \sum_i \langle \xi(i) | [(f_{z_0} \otimes Z_{00})^+ \cdot f \cdot (f_{z_0} \otimes Z_{00})] \otimes F_0^+ F_0 | \xi(i) \rangle \\ &= \mathrm{Tr}\{\rho_E [(f_{z_0} \otimes Z_{00})^+ \cdot f \cdot (f_{z_0} \otimes Z_{00})] \otimes F_0^+ F_0\}, \end{aligned} \tag{A10}$$

where $\rho_{\mathrm{E}} = |\xi(i)\rangle\langle\xi(i)|$, $Z_{00} = (\alpha_{z_0}^0, \alpha_{z_0}^1, 0, 0)$ and

$$f_{z_0} = \begin{bmatrix} f_1^{z_0} & 0 & 0 & 0 \\ 0 & f_2^{z_0} & 0 & 0 \\ 0 & 0 & f_3^{z_0} & 0 \\ 0 & 0 & 0 & f_4^{z_0} \end{bmatrix}, \qquad f = \begin{bmatrix} f_1^1 & f_2^1 & f_3^1 & f_4^1 \\ f_1^2 & f_2^2 & f_3^2 & f_4^2 \\ f_1^3 & f_2^3 & f_3^3 & f_4^3 \\ f_1^4 & f_2^4 & f_3^4 & f_4^4 \end{bmatrix}, \tag{A11}$$

with $f_i^j = \langle \omega_i | \omega_j \rangle$.

With the same method given above, we have

$$\begin{aligned} P_{01}^{zz} &= \mathrm{Tr}\{\rho_{\mathrm{E}} [(f_{z_0} \otimes Z_{01})^+ \cdot f \cdot (f_{z_0} \otimes Z_{01})] \otimes F_1^+ F_1\} \\ P_{10}^{zz} &= \mathrm{Tr}\{\rho_{\mathrm{E}} [(f_{z_1} \otimes Z_{10})^+ \cdot f \cdot (f_{z_1} \otimes Z_{10})] \otimes F_0^+ F_0\} \\ P_{11}^{zz} &= \mathrm{Tr}\{\rho_{\mathrm{E}} [(f_{z_1} \otimes Z_{11})^+ \cdot f \cdot (f_{z_1} \otimes Z_{11})] \otimes F_1^+ F_1\} \end{aligned} \tag{A12}$$

where

$$\begin{aligned} Z_{01} &= (0, 0, \alpha_{z_0}^0, \alpha_{z_0}^1), \\ Z_{10} &= (\alpha_{z_1}^0, \alpha_{z_1}^1, 0, 0), \\ Z_{11} &= (0, 0, \alpha_{z_1}^0, \alpha_{z_1}^1), \end{aligned} \tag{A13}$$

and

$$f_{z_1} = \begin{bmatrix} f_1^{z_1} & 0 & 0 & 0 \\ 0 & f_2^{z_1} & 0 & 0 \\ 0 & 0 & f_3^{z_1} & 0 \\ 0 & 0 & 0 & f_4^{z_1} \end{bmatrix}. \tag{A14}$$

The bit error rate in Z-basis (equation (8a)) is given by

$$\delta_{\mathrm{b}}^z = \frac{P_{01}^{zz} + P_{10}^{zz}}{P_{00}^{zz} + P_{01}^{zz} + P_{10}^{zz} + P_{11}^{zz}}. \tag{A15}$$

(b) $|\Psi_X^2\rangle$

According to equation (A2) and the method given above, it is easy to get the probability, $P_{i,j}^{xx}$, that Alice sends x_i and Bob measures x_j in X-basis, which is

$$\begin{aligned} P_{00}^{xx} &= \mathrm{Tr}\{\rho_{\mathrm{E}} [(f_{x_0} \otimes X_{00})^+ \cdot f \cdot (f_{x_0} \otimes X_{00})] \otimes F_0^+ F_0\} \\ P_{01}^{xx} &= \mathrm{Tr}\{\rho_{\mathrm{E}} [(f_{x_0} \otimes X_{01})^+ \cdot f \cdot (f_{x_0} \otimes X_{01})] \otimes F_1^+ F_1\} \\ P_{10}^{xx} &= \mathrm{Tr}\{\rho_{\mathrm{E}} [(f_{x_1} \otimes X_{10})^+ \cdot f \cdot (f_{x_1} \otimes X_{10})] \otimes F_0^+ F_0\} \\ P_{11}^{xx} &= \mathrm{Tr}\{\rho_{\mathrm{E}} [(f_{x_1} \otimes X_{11})^+ \cdot f \cdot (f_{x_1} \otimes X_{11})] \otimes F_1^+ F_1\}. \end{aligned} \tag{A16}$$

Here

$$\begin{aligned} X_{00} &= Z_{00} U, \qquad X_{01} = Z_{01} U, \\ X_{10} &= Z_{10} U, \qquad X_{11} = Z_{11} U, \end{aligned} \tag{A17}$$

and

$$f_{x_0}=\begin{bmatrix} f_1^{x_0} & 0 & 0 & 0\\ 0 & f_2^{x_0} & 0 & 0\\ 0 & 0 & f_3^{x_0} & 0\\ 0 & 0 & 0 & f_4^{x_0}\end{bmatrix},\qquad f_{x_1}=\begin{bmatrix} f_1^{x_1} & 0 & 0 & 0\\ 0 & f_2^{x_1} & 0 & 0\\ 0 & 0 & f_3^{x_1} & 0\\ 0 & 0 & 0 & f_4^{x_1}\end{bmatrix},$$
$$U=\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}. \tag{A18}$$

Thus, the bit error in X-basis (equation (8b)) can be written as

$$\delta_{\mathrm{b}}^{x}=\frac{P_{01}^{xx}+P_{10}^{xx}}{P_{00}^{xx}+P_{01}^{xx}+P_{10}^{xx}+P_{11}^{xx}}. \tag{A19}$$

(c) $|\Psi_Z^3\rangle$

According to equation (A3), we have

$$|\Psi_Z^3\rangle\equiv\sum_{i,t,j}(\widetilde{L}_0+\widetilde{L}_1)C|\xi(i,t,j)\rangle|i\rangle \tag{A20}$$

with

$$\begin{aligned}\widetilde{L}_0&=f_t^{z_0}(a_{00}^{i,t,j}\alpha_{z_0}^0+a_{01}^{i,t,j}\alpha_{z_0}^1)|z_0\rangle|z_0\rangle|\omega_t\rangle+f_t^{z_1}(a_{00}^{i,t,j}\alpha_{z_1}^0+a_{01}^{i,t,j}\alpha_{z_1}^1)|z_1\rangle|z_0\rangle|\omega_t\rangle\\ \widetilde{L}_1&=f_t^{z_0}(a_{10}^{i,t,j}\alpha_{z_0}^0+a_{11}^{i,t,j}\alpha_{z_0}^1)|z_0\rangle|z_1\rangle|\omega_t\rangle+f_t^{z_1}(a_{10}^{i,t,j}\alpha_{z_1}^0+a_{11}^{i,t,j}\alpha_{z_1}^1)|z_1\rangle|z_1\rangle|\omega_t\rangle.\end{aligned} \tag{A21}$$

We first consider the case that $|x_0\rangle|x_0\rangle$, both Alice and Bob measure $|\Psi_Z^3\rangle$ in X-basis and gets results 0, which is given by

$$\begin{aligned}\langle x_0|\langle x_0|\Psi_Z^3\rangle&=\frac{1}{2}\sum_{i,t,j}\Big[f_t^{z_0}(a_{00}^{i,t,j}\alpha_{z_0}^0+a_{01}^{i,t,j}\alpha_{z_0}^1)+f_t^{z_1}(a_{00}^{i,t,j}\alpha_{z_1}^0+a_{01}^{i,t,j}\alpha_{z_1}^1)\\ &\quad+f_t^{z_0}(a_{10}^{i,t,j}\alpha_{z_0}^0+a_{11}^{i,t,j}\alpha_{z_0}^1)+f_t^{z_1}(a_{10}^{i,t,j}\alpha_{z_1}^0+a_{11}^{i,t,j}\alpha_{z_1}^1)\Big]|\omega_t\rangle C|\xi(i,t,j)\rangle|i\rangle\\ &=\frac{1}{2}\sum_{i,t,j}\Big[f_t^{z_0}(a_{00}^{i,t,j}\alpha_{z_0}^0+a_{01}^{i,t,j}\alpha_{z_0}^1+a_{10}^{i,t,j}\alpha_{z_0}^0+a_{11}^{i,t,j}\alpha_{z_0}^1)\\ &\quad+f_t^{z_1}(a_{00}^{i,t,j}\alpha_{z_1}^0+a_{01}^{i,t,j}\alpha_{z_1}^1)+a_{10}^{i,t,j}\alpha_{z_1}^0+a_{11}^{i,t,j}\alpha_{z_1}^1\Big]|\omega_t\rangle C|\xi(i,t,j)\rangle|i\rangle\\ &=\frac{1}{2}\sum_{i,t,j}(f_t^{z_0}x_{i,t,j}+f_t^{z_1}y_{i,t,j})|\omega_t\rangle C|\xi(i,t,j)\rangle|i\rangle.\end{aligned} \tag{A22}$$

Thus the probability

$$\begin{aligned}P_{00}^{xx,\mathrm{vir}}&=\frac{1}{4}\sum_{i,t,t',j,j'}\langle\xi(i,t,j)C^+(f_t^{z_0}x_{i,t,j}+f_t^{z_1}y_{i,t,j})\langle\omega_t|\omega_{t'}\rangle(f_{t'}^{z_0}x_{i,t',j'}+f_{t'}^{z_1}y_{i,t',j'})C|\xi(i,t',j')\rangle\\ &=\frac{1}{4}\sum_{i,t,t',j,j'}\langle\xi(i,t,j)|C^+\Big(f_t^{z_0}f_{t'}^{z_0}x_{i,t,j}x_{i,t',j'}f_t^{t'}+f_t^{z_1}y_{i,t,j}f_{t'}^{z_1}y_{i,t',j'}f_t^{t'}\\ &\quad+f_t^{z_0}x_{i,t,j}f_{t'}^{z_1}y_{i,t',j'}f_t^{t'}+f_t^{z_1}y_{i,t,j}f_{t'}^{z_0}x_{i,t',j'}f_t^{t'}\Big)C|\xi(i,t',j')\rangle.\end{aligned} \tag{A23}$$

Thus, with the same method above, we have

$$P_{00}^{xx,\mathrm{vir}}=\frac{1}{4}\ \mathrm{Tr}\left[\rho_{\mathrm{E}}Z_{00}^{\mathrm{p}}\otimes C^+C\right], \tag{A24}$$

here

$$Z_{00}^{\mathrm{p}}=(V_{00}^0)^+\cdot f\cdot V_{00}^0+(V_{00}^1)^+\cdot f\cdot V_{00}^1+(V_{00}^0)^+\cdot f\cdot V_{00}^1+(V_{00}^1)^+\cdot f\cdot V_{00}^0 \tag{A25}$$

with

$$\begin{aligned} V_{00}^{0} &= \Omega_{00}^{0} \otimes f_{z_0}, \\ V_{00}^{1} &= \Omega_{00}^{1} \otimes f_{z_1}, \\ \Omega_{00}^{0} &= (\alpha_{z_0}^{0}, \alpha_{z_0}^{1}, \alpha_{z_0}^{0}, \alpha_{z_0}^{1}), \\ \Omega_{00}^{1} &= (\alpha_{z_1}^{0}, \alpha_{z_1}^{1}, \alpha_{z_1}^{0}, \alpha_{z_1}^{1}). \end{aligned} \tag{A26}$$

Thus the probability that Alice gets k and Bob gets k' in the virtual X-basis measurement is given by

$$P_{k,k'}^{xx,\mathrm{vir}} = \frac{1}{4}\ \mathrm{Tr}\left[\rho_{\mathrm{E}} Z_{k,k'}^{\mathrm{p}} \otimes C^{+}C\right] \tag{A27}$$

with

$$Z_{k,k'}^{\mathrm{p}} = (V_{k,k'}^{0})^{+} \cdot f \cdot V_{k,k'}^{0} + (V_{k,k'}^{1})^{+} \cdot f \cdot V_{k,k'}^{1} + (V_{k,k'}^{0})^{+} \cdot f \cdot V_{k,k'}^{1} + (V_{k,k'}^{1})^{+} \cdot f \cdot V_{k,k'}^{0} \tag{A28}$$

here $k, k' = 0, 1$, $V_{k,k'}^{0} = \Omega_{k,k'}^{0} \otimes f_{z_0}$, $V_{k,k'}^{1} = \Omega_{k,k'}^{1} \otimes f_{z_1}$, and

$$\begin{aligned} \Omega_{01}^{0} &= (\alpha_{z_0}^{0}, \alpha_{z_0}^{1}, -\alpha_{z_0}^{0}, -\alpha_{z_0}^{1}) \\ \Omega_{01}^{1} &= (\alpha_{z_1}^{0}, \alpha_{z_1}^{1}, -\alpha_{z_1}^{0}, -\alpha_{z_1}^{1}) \\ \Omega_{10}^{0} &= (\alpha_{z_0}^{0}, \alpha_{z_0}^{1}, \alpha_{z_0}^{0}, \alpha_{z_0}^{1}) \\ \Omega_{10}^{1} &= (-\alpha_{z_1}^{0}, -\alpha_{z_1}^{1}, -\alpha_{z_1}^{0}, -\alpha_{z_1}^{1}) \\ \Omega_{11}^{0} &= (\alpha_{z_0}^{0}, \alpha_{z_0}^{1}, -\alpha_{z_0}^{0}, -\alpha_{z_0}^{1}) \\ \Omega_{11}^{1} &= (-\alpha_{z_1}^{0}, -\alpha_{z_1}^{1}, \alpha_{z_1}^{0}, \alpha_{z_1}^{1}). \end{aligned} \tag{A29}$$

The phase error in Z-basis is given by

$$\delta_{p}^{z} = \frac{P_{01}^{xx,\mathrm{vir}} + P_{10}^{xx,\mathrm{vir}}}{P_{00}^{xx,\mathrm{vir}} + P_{01}^{xx,\mathrm{vir}} + P_{10}^{xx,\mathrm{vir}} + P_{11}^{xx,\mathrm{vir}}}. \tag{A30}$$

Appendix B. The gain and error rate for simulation

In the case of SPS, when Eve is absent, the estimated count rate and error rate can be written as

$$\begin{aligned} Q_z &= 1 - (1 - Y_0)(1 - \eta) \\ \delta_{\mathrm{b}}^{z} &= \left[e_0 Y_0 + e_{\mathrm{det}}\ \eta\right] / Q_z. \end{aligned} \tag{B1}$$

$\eta = \eta_{\mathrm{Bob}} \times \eta_{\mathrm{d}} \times \eta_{\mathrm{c}}$ is the total transmittance of system with $\eta_{\mathrm{c}} = 10 \times 10^{-\alpha l/10}$, and $\alpha = 0.21$ dB km^{-1} is loss of fiber and l is the length of fiber. $e_0 = 0.5$ is the error rate of background. Y_0 is the dark count of SPDs. e_{det} is the optical error of the QKD system.

In the case of WPS, the total gain and error rate can be written as

$$\begin{aligned} Q_s &= 1 - (1 - Y_0)\mathrm{e}^{-\eta s}, \\ Q_s E_s &= e_0 Y_0 + e_{\mathrm{det}}\ (1 - \mathrm{e}^{-\eta s}). \end{aligned} \tag{B2}$$

Here $s = \ \mu, \nu$ is the intensity of signal state and decoy state.

ORCID iDs

Shihai Sun https://orcid.org/0000-0003-3720-1757
Feihu Xu https://orcid.org/0000-0002-1643-225X

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* (New York: IEEE Press) pp 175–9
[2] Lo H-K and Chau H F 1999 *Science* **283** 2050
[3] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325

[4] Lo H-K and Preskill J 2007 *Quantum Inf. Comput.* **7** 431
[5] Yin H-L *et al* 2016 *Phys. Rev. Lett.* **117** 190501
[6] Boaron A *et al* 2018 *Phys. Rev. Lett.* **121** 190502
[7] Liu H, Wang J, Ma H and Sun S 2018 *Optica* **5** 902
[8] Schmitt-Manderbach T *et al* 2007 *Phys. Rev. Lett.* **98** 010504
[9] Liao S-K *et al* 2017 *Nat. Photon.* **11** 509
[10] Liao S-K *et al* 2017 *Nature* **549** 43
[11] Wang S *et al* 2014 *Opt. Express* **22** 21739
[12] Sasaki M *et al* 2011 *Opt. Express* **19** 10387
[13] Stucki D *et al* 2011 *New J. Phys.* **13** 123001
[14] Fung C-H F, Qi B, Tamaki K and Lo H-K 2007 *Phys. Rev.* A **75** 032314
[15] Xu F, Qi B and Lo H-K 2010 *New J. Phys.* **12** 113026
[16] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[17] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev.* A **73** 022320
[18] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z and Shields A J 2015 *Phys. Rev.* X **5** 031030
[19] Sun S-H, Xu F, Jiang M-S, Ma X-C, Lo H-K and Liang L-M 2015 *Phys. Rev.* A **92** 022304
[20] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 *Rev. Mod. Phys.* **92** 025002
[21] Pirandola S *et al* 2020 *Adv. Opt. Photonics* **12** 1012
[22] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[23] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 *New J. Phys.* **11** 045021
[24] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[25] Pawłowski M and Brunner N 2011 *Phys. Rev.* A **84** 010302
[26] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
[27] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[28] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[29] Huang A, Sun S-H, Liu Z and Makarov V 2018 *Phys. Rev.* A **98** 159901
[30] Tamaki K, Curty M and Lucamarini M 2016 *New J. Phys.* **18** 065008
[31] Fung C-H F, Tamaki K, Qi B, Lo H-K and Ma X 2009 *Quantum Inf. Comput.* **9** 131
[32] Zhang Y, Coles P J, Winick A, Lin J and Lütkenhaus N 2021 *Phys. Rev. Research* **3** 013076
[33] Li H W, Yin Z Q, Wang S, Qian Y J, Chen W, Guo G C and Han Z F 2015 *Sci. Rep.* **5** 16200
[34] Marøy Ø, Lydersen L and Skaar J 2010 *Phys. Rev.* A **82** 032337
[35] Marøy Ø, Makarov V and Skaar J 2017 *Quantum Science and Technology* **2** 044013
[36] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 *Phys. Rev.* A **78** 042333
[37] Li H-W *et al* 2011 *Phys. Rev.* A **84** 062308
[38] Wei K, Zhang W, Tang Y-L, You L and Xu F 2019 *Phys. Rev.* A **100** 022325
[39] Xu F, Wei K, Sajeed S, Kaiser S, Sun S, Tang Z, Qian L, Makarov V and Lo H-K 2015 *Phys. Rev.* A **92** 032305
[40] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[41] Ma X, Qi B, Zhao Y and Lo H-K 2005 *Phys. Rev.* A **72** 012326
[42] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043