Security of practical quantum key distribution with weak-randomness basis selection

Hong-Wei Li,[1,*] Zheng-Mao Xu,[1] Zhen-Qiang Yin,[2] and Qing-Yu Cai[3,†]

[1] *Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou Information Science and Technology Institute, Henan, Zhengzhou 450000, China*
[2] *Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*
[3] *Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan 430071, China*

(Received 16 March 2020; accepted 13 July 2020; published 10 August 2020)

The security of the perfect quantum key distribution protocol can be guaranteed by applying the fundamental laws of quantum mechanics, but the practical quantum key distribution system may be attacked by utilizing imperfect state preparation and measurement devices. In this work, we analyze the security of the practical quantum key distribution system with weak-randomness basis selection, where the basis selection may be partly controlled by the eavesdropper due to the imperfect quantum devices. We propose the parameter ϵ to quantify the deviation value between the practical basis selection probability and the perfect basis selection probability, and the secret key rate of the practical quantum key distribution system is obtained under different ϵ values. By applying the practical experimental parameters, the analysis result demonstrates that the maximal transmission distance will be reduced from 142 to 139 km if $\epsilon \leqslant 0.1$, but no secret key can be generated in the case of $\epsilon \geqslant 0.34$.

DOI: 10.1103/PhysRevA.102.022605

I. INTRODUCTION

Quantum key distribution (QKD) [1] is the art of sharing the unconditional secret key between two different remote parties Alice and Bob. The unconditional security of the perfect QKD protocol has been proved by applying the fundamental laws of quantum mechanics and the quantum information theory [2–4]. However, the practical QKD system may be attacked [5,6] by utilizing imperfect quantum state preparation and measurement devices, such as the wavelength attack [7], detector blinding attack [8], time shift attack [9], randomness attack [10,11], probabilistic blinding attack [12], etc. [5,13–20]. In these attack models, the quantum devices can be assumed to be partly controlled by the eavesdropper Eve, and thus she can obtain more information by comparing with the perfect QKD protocol, and the secret key rate will be reduced correspondingly.

In the perfect QKD protocol, the quantum states will be detected by randomly selecting two different measurement bases in Bob's side. However, the randomness of the basis selection may be weakened in the practical QKD system. For example, the measurement bases may be selected by a beam splitter in the polarization encoded QKD system. However, the coupling ratio values can be affected by utilizing different wavelength sources, and thus the practical QKD system may have the weak-randomness basis selection by considering that Eve applies the wavelength attack [18]. On the other side, the quantum states modulated in different bases may be detected by different single-photon detectors, which have different detection efficiency values [6], and thus different measurement bases may be selected by the weak-random number. Note that the weak-randomness basis selection model was first proposed in the seminal paper [18], but the previous work did not consider the practical weak coherent source and imperfect single-photon detector, and the previous security analysis method is not optimal. Recently, a new QKD protocol based on the pseudorandom basis modulation was proposed [21], which has high key generation efficiency, but this protocol strongly requires single-photon source preparation.

To illustrate the weak-randomness basis selection model in the practical QKD system, the basis selection probability has a small deviation value compared to the perfect case. More precisely, we propose the imperfect parameter ε to illustrate the deviation value between the perfect and the weak-randomness basis selection, where different ε values can be controlled by some hidden variables in Eve's side. Based on this weak-randomness basis selection model, we prove the final secret key rate under different ε values. Based on the practical experimental parameter [22], we can calculate the secret key rate with different transmission distances and ε values, and the analysis result demonstrates that the maximal transmission distance will be reduced from 142 to 139 km if $\epsilon \leqslant 0.1$, but no secret key can be generated in the case of $\epsilon \geqslant 0.34$.

The paper is organized as follows. In Sec. II, the weak-randomness basis selection model is described. In Sec. III, the modified intercept resend attack model is proposed, and we prove that Eve can apply the weak-randomness basis selection to reduce the quantum bit error rate (QBER) value. Based on the weak-randomness basis selection model, we analyze the security of the practical QKD system with the single-photon

[*] To whom correspondence should be addressed; lihow@ustc.edu.cn

[†] qycai@wipm.ac.cn

source preparation in Sec. IV. In Sec. V, we analyze the security of the practical QKD system with the weak coherent source preparation, where the secret key rate and the maximal transmission distance will be analyzed correspondingly.

II. THE PRACTICAL QKD SYSTEM WITH WEAK-RANDOMNESS BASIS SELECTION

In the practical QKD system, the quantum state will be prepared and measured in the rectilinear basis and the diagonal basis, respectively, where the $p(y=0)$ $[p(y=1)=1-p(y=0)]$ value determines the rectilinear [diagonal] basis selection probability. The perfect QKD protocol requires a perfect random number to select the basis, which means that Eve can only get $p(y=0)=p(y=1)=\frac{1}{2}$ by considering all of the hidden variables in her side. However, in the practical QKD system, the basis selection probability value y may be partly controlled by Eve with the hidden variable values $\lambda=\{0,1\}$, where different hidden variable values λ have different basis selection probability $p(y|\lambda)$. Thus the practical observed basis selection probability $p(y)$ can be given by the following equations:

$$p(y=0)=\sum_{i=0,1}p(\lambda=i)p(y=0|\lambda=i),$$
$$p(y=1)=\sum_{i=0,1}p(\lambda=i)p(y=1|\lambda=i), \tag{1}$$

where $\sum_{i=0,1}p(\lambda=i)=1$. By considering this equations, it can be found that even if the practical experimental realization has observed $p(y=0)=p(y=1)=\frac{1}{2}$, it cannot guarantee $p(y|\lambda)=\frac{1}{2}$ for arbitrary hidden variable value λ. Correspondingly, the security analysis result based on the perfect-randomness basis selection demonstrates that $p(y|\lambda)=\frac{1}{2}$, which cannot be applied to prove the security of the practical QKD system with the weak-randomness basis selection.

To estimate the randomness deviation for the arbitrary hidden variable λ, we define the weak-randomness model as the following inequality:

$$\left|p(y=0|\lambda=i)-\tfrac{1}{2}\right|\leqslant\varepsilon. \tag{2}$$

In the security analysis model, the hidden variable λ can be controlled by Eve, and thus she can control the basis selection probability $p(y|\lambda)$ with different hidden variable λ. More precisely, the blinding attack model can be analyzed by considering that the rectilinear [diagonal] basis has the basis selection probability $p(y=0|\lambda=0)=1$ $[p(y=1|\lambda=1)=1]$ with the hidden variable value $\lambda=0$ $[\lambda=1]$, and thus Eve can apply the intercept and resend attack without introducing any error rate. More generally, this weak-randomness basis selection model can also be applied in the case of $\frac{1}{2}\leqslant p(y=0|\lambda=0)\leqslant 1$ and $0\leqslant p(y=0|\lambda=1)=1\leqslant\frac{1}{2}$. Note that the analysis model considers the weak-randomness basis selection with different hidden variable λ, but the measurement outcomes 0 and 1 may have the same guessing probability $p(y)=\frac{1}{2}$, and thus the weak-randomness basis selection model cannot be analyzed by utilizing the efficient QKD scheme [23].

III. INTERCEPT AND RESEND ATTACK WITH WEAK-RANDOMNESS BASIS SELECTION MODEL

Intercept and resend attack is an important attacking model to prove the security of the practical QKD system, and it has been proved that this attack model will introduce the QBER value of 25% with perfect state preparation and measurement. Based on the intercept and resend attack model, we can analyze the upper bound of the maximal tolerated QBER value. By applying the blind light to control the basis selection in Bob's side, the blinding attack can decrease the QBER value from 25% to 0, and thus this attack model will be difficult to observe. Similar to the blinding attack model, by considering the weak-randomness basis selection, we propose the modified intercept and resend attack model. More precisely, Eve will first measure the quantum states by randomly choosing the measurement bases. Based on the measurement outcomes, she will reprepare the corresponding quantum state, which will be transmitted to Bob with different hidden variable λ. In the case where Eve gets the measurement outcome in the rectilinear basis, the reprepared rectilinear basis quantum state will be detected in the rectilinear basis with probability $p(y=0|\lambda=0)>\frac{1}{2}$. In the case where Eve gets the measurement outcome in the diagonal basis, the reprepared diagonal basis quantum state will be detected in the diagonal basis with probability $p(y=1|\lambda=1)>\frac{1}{2}$. Based on this attack model, the corresponding QBER value can be given by

$$Q=\tfrac{1}{4}[1-p(y=0|\lambda=0)+p(y=0|\lambda=1)]. \tag{3}$$

In the case of $p(y=0|\lambda=0)=p(y=0|\lambda=1)=\frac{1}{2}$, the Q value is 25%, which has been analyzed in the perfect QKD protocol. However, if the basis selection probability can be illustrated by $p(y=0|\lambda=0)>\frac{1}{2}$ and $p(y=0|\lambda=1)<\frac{1}{2}$, the Q value satisfies $0\leqslant Q<25\%$. More precisely, in the special case $p(y=0|\lambda=0)=1$ and $p(y=0|\lambda=1)=0$, we can get the Q value is 0, and this situation can be satisfied with the blinding attack model [8].

By considering the weak-randomness model with $|p(y=0|\lambda=i)-\frac{1}{2}|\leqslant\varepsilon$, it is easy to check that the upper bound of the maximal tolerated Q value is $\frac{1-2\varepsilon}{4}$; the detailed calculation result is given in Fig. 1. Note that the upper bound of the maximal tolerated Q value is 25% in the perfect QKD protocol, but this value will be reduced to 0 in the case of $\varepsilon=\frac{1}{2}$.

IV. WEAK-RANDOMNESS BASIS SELECTION MODEL WITH THE SINGLE-PHOTON SOURCE

To prove the security of the practical QKD system with the weak-randomness basis selection, the entanglement distillation purification (EDP) technology needs to estimate the upper bound of the phase error rate in two different bases. Since Eve can control Bob's basis selection probability with the hidden variable λ, we need to estimate the phase error rate and bit error rate with different hidden variable values. The corresponding security analysis model is given in Fig. 2.

By considering that the quantum state preparation and measurement operators are perfect, it has been proved that Eve's general attack can be reduced to the Pauli attack [24,25], which can be described by the classical probability theory. Thus, we can only consider the Pauli attack model in the

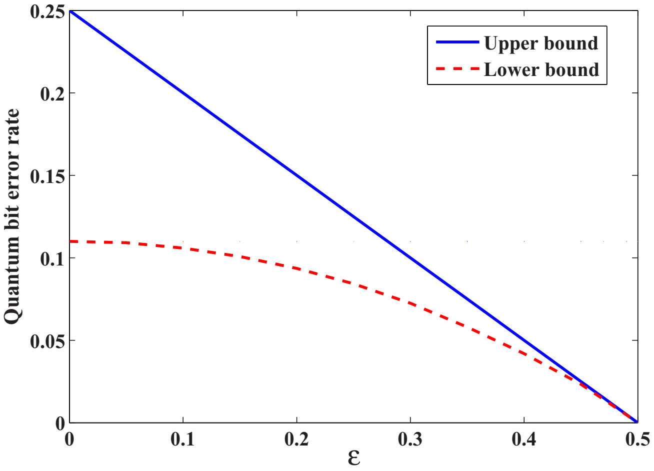

FIG. 1. The upper bound and the lower bound of the quantum bit error rate Q value with different ε values, where the upper bound value is the Q value given by the modified intercept and resend attack, while the lower bound value can be analyzed by the entanglement distillation and purification technology.

quantum channel with two different hidden variable values $\lambda = 0$ and $\lambda = 1$.

In the first case with the hidden variable $\lambda = 0$, Eve will control Bob to choose the rectilinear [diagonal] basis with the probability $p \equiv p(y=0|\lambda=0)$ $[1-p = p(y=1|\lambda=0)]$, and thus the final shared quantum state between Alice and Bob can be given by

$$\rho_1 = p\rho_{11} + (1-p)\rho_{12}, \tag{4}$$

where

$$\rho_{11} = \Sigma_{u,v} q_{u,v} I \otimes X^u Z^v |\phi_1\rangle\langle\phi_1| X^u Z^v \otimes I, \tag{5}$$

$$\rho_{12} = \Sigma_{u,v} q_{u,v} I \otimes H X^u Z^v H |\phi_1\rangle\langle\phi_1| H X^u Z^v H \otimes I, \tag{6}$$

$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is the maximal entangled quantum state, $u, v \in \{0, 1\}$, $0 \leqslant q_{u,v} \leqslant 1$, $\Sigma_{u,v\in\{0,1\}} q_{u,v} = 1$, $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadamard matrix, $q_{0,0}$ is the probability that the identity operation $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has been applied in the quantum channel, $q_{0,1}$ is the probability that the phase error operation $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ has been applied in the quantum channel, $q_{1,0}$ is the probability that the bit error operation $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has been applied in the quantum channel, and $q_{1,1}$ is the probability that the bit phase error operation XZ has been applied in the quantum channel.

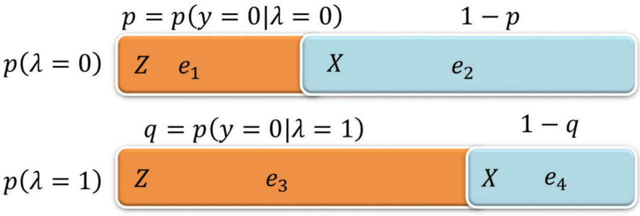

FIG. 2. The security analysis model with the weak-randomness basis selection model. Eve controls different hidden variables $\lambda = 0$ and $\lambda = 1$ with the probabilities $p(\lambda = 0)$ and $p(\lambda = 1)$, respectively. In the first case with the hidden variable $\lambda = 0$, the rectilinear basis and the diagonal basis have the QBER values e_1 and e_2, respectively. In the second case with the hidden variable $\lambda = 1$, the rectilinear basis and the diagonal basis have the QBER values e_3 and e_4, respectively.

By considering that the quantum state ρ_{11} modulated in the rectilinear basis has been shared between Alice and Bob, the QBER value e_1 can be given by

$$e_1 = \langle\phi_2|\rho_{11}|\phi_2\rangle + \langle\phi_4|\rho_{11}|\phi_4\rangle, \tag{7}$$

and the corresponding phase error rate value e_2 can be given by

$$e_2 = \langle\phi_3|\rho_{11}|\phi_3\rangle + \langle\phi_4|\rho_{11}|\phi_4\rangle, \tag{8}$$

where

$$\begin{aligned} |\phi_2\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\phi_3\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\phi_4\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{9}$$

By considering that the quantum state ρ_{12} modulated in the diagonal basis has been prepared, the QBER value can be given by

$$\langle\phi_2|\rho_{12}|\phi_2\rangle + \langle\phi_4|\rho_{12}|\phi_4\rangle = e_2, \tag{10}$$

and the corresponding phase error rate value can be given by

$$\langle\phi_3|\rho_{12}|\phi_3\rangle + \langle\phi_4|\rho_{12}|\phi_4\rangle = e_1. \tag{11}$$

By applying the EDP technology, the secret key rate in the first case can be given by

$$\begin{aligned} R_0 &\geqslant p[1 - h(e_1) - h(e_2)] + (1-p)[1 - h(e_1) - h(e_2)] \\ &= 1 - h(e_1) - h(e_2), \end{aligned} \tag{12}$$

where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the Shannon entropy function, the first part $p[1 - h(e_1) - h(e_2)]$ is the secret key rate generated by the rectilinear basis, and the second part $(1-p)[1 - h(e_1) - h(e_2)]$ is the secret key rate generated by the diagonal basis.

In the second case with the hidden variable $\lambda = 1$, Eve will control Bob to choose the rectilinear [diagonal] basis with the probability $q \equiv p(y=0|\lambda=1)$ $[1-q = p(y=1|\lambda=1)]$, and thus the final quantum state preparation under the Pauli quantum channel is given by

$$\rho_2 = q\rho_{21} + (1-q)\rho_{22}, \tag{13}$$

$$\rho_{21} = \Sigma_{u,v} q'_{u,v} I \otimes X^u Z^v |\phi_1\rangle\langle\phi_1| X^u Z^v \otimes I, \tag{14}$$

$$\rho_{22} = \Sigma_{u,v} q'_{u,v} I \otimes H X^u Z^v H |\phi_1\rangle\langle\phi_1| H X^u Z^v H \otimes I, \tag{15}$$

where $u, v \in \{0, 1\}$, $0 \leqslant q'_{u,v} \leqslant 1$, $\Sigma_{u,v\in\{0,1\}} q'_{u,v} = 1$. Since Eve can utilize a different attacking strategy if she chooses a different hidden variable λ, the Pauli channel parameters $q'_{u,v}$ may be different by comparing with the first case.

By considering that the quantum state ρ_{21} modulated in the rectilinear basis has been prepared, the QBER value e_3 can be given by

$$e_3 = \langle\phi_2|\rho_{21}|\phi_2\rangle + \langle\phi_4|\rho_{21}|\phi_4\rangle, \tag{16}$$

and the corresponding phase error rate value e_4 can be given by

$$e_4 = \langle\phi_3|\rho_{21}|\phi_3\rangle + \langle\phi_4|\rho_{21}|\phi_4\rangle. \tag{17}$$

By considering that the quantum state ρ_{22} modulated in the diagonal basis has been prepared, the QBER value can be given by

$$\langle\phi_2|\rho_{22}|\phi_2\rangle + \langle\phi_4|\rho_{22}|\phi_4\rangle = e_4, \tag{18}$$

and the corresponding phase error rate value can be given by

$$\langle\phi_3|\rho_{22}|\phi_3\rangle + \langle\phi_4|\rho_{22}|\phi_4\rangle = e_3. \tag{19}$$

By applying the EDP technology, the secret key rate in the second case can be given by

$$\begin{aligned} R_1 &\geqslant q[1 - h(e_3) - h(e_4)] + (1-q)[1 - h(e_3) - h(e_4)] \\ &= 1 - h(e_3) - h(e_4), \end{aligned} \tag{20}$$

where the first part $q[1 - h(e_3) - h(e_4)]$ is the secret key rate generated by the rectilinear basis, and the second part $(1 - q)[1 - h(e_3) - h(e_4)]$ is the secret key rate generated by the diagonal basis.

Since the two cases are prepared with the probabilities $p(\lambda = 0)$ and $p(\lambda = 1)$, respectively, the final secret key rate can be given by

$$R \geqslant p(\lambda = 0)R_0 + p(\lambda = 1)R_1. \tag{21}$$

In the practical QKD experimental realization, the QBER value and the count rate value in the rectilinear basis and the diagonal basis can be respectively calculated. Without loss of generality, we can assume that different bases have the same QBER value Q and the count rate value $[p(\lambda = 0)p + p(\lambda = 1)q = p(\lambda = 0)(1 - p) + p(\lambda = 1)(1 - q) = \frac{1}{2}]$, and thus the lower bound of the secret key rate can be estimated by utilizing the following optimization method:

$$\begin{aligned} &\text{Minimize}: R \geqslant p(\lambda = 0)R_0 + p(\lambda = 1)R_1, \\ &\text{Subject to}: p(\lambda = 0) + p(\lambda = 1) = 1, \\ &\qquad p(\lambda = 0)p + p(\lambda = 1)q = \frac{1}{2}, \\ &\qquad p(\lambda = 0)pe_1 + p(\lambda = 1)qe_3 = \frac{Q}{2}, \\ &\qquad p(\lambda = 0)(1-p)e_2 + p(\lambda = 1)(1-q)e_4 = \frac{Q}{2}, \\ &\qquad \frac{1}{2} - \varepsilon \leqslant p, q \leqslant \frac{1}{2} + \varepsilon, \\ &\qquad 0 \leqslant p(\lambda = 0), p(\lambda = 1) \leqslant 1, \\ &\qquad 0 \leqslant e_1, e_2, e_3, e_4 \leqslant \frac{1}{2}. \end{aligned} \tag{22}$$

In a more general situation, the QBER value and the count rate value may be different in two different bases, but a similar optimization method can also be applied to generate the final secret key rate. Based on the optimization calculation result, we can calculate the final secret key rate under different ε values in Fig. 3.

From the calculation result, we can find that the secret key rate and the maximal tolerated QBER value will be decreased when ε is increasing. The lower bound of the maximal tolerated QBER values with different ε values has also been calculated in Fig. 3, where the lower bound of the maximal tolerated QBER value will be reduced from 0.11 to 0 by increasing the ε value from 0 to 0.5.

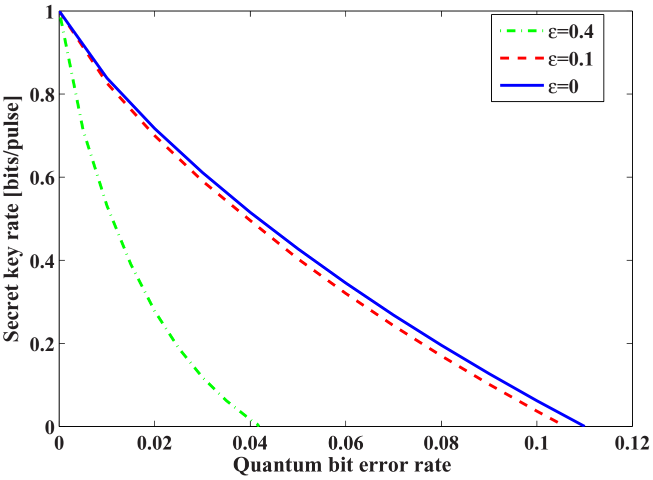

FIG. 3. The secret key rate with different quantum bit error rate values and ε values. The solid blue line is the secret key rate with $\varepsilon = 0$, which is the perfect-randomness basis selection case. The dashed red line is the secret key rate with $\varepsilon = 0.1$, and the dash-dotted red line is the secret key rate with $\varepsilon = 0.4$. By comparing with the perfect-randomness basis selection, the weak-randomness basis selection will decrease the secret key rate.

In the practical QKD system, the quantum states modulated in two different bases may be detected by two different single-photon detectors. Obviously, the two detectors cannot have the same detection efficiency, and thus the measurement basis selection probability may be imperfect. By applying the experimental result given by [26], the ε value can be estimated by $\varepsilon \leqslant 0.377$, and the lower bound of the maximal tolerated QBER value is 4.98% by applying the previous analysis result. In the other case, the measurement basis may be selected by a beam splitter, where the coupling ratio value can be affected by utilizing different wavelength sources. By applying the experimental result given by [27], the ε value can be estimated by $\varepsilon \leqslant 0.0327$, and the lower bound of the maximal tolerated QBER value is 10.9% by applying the previous analysis result.

V. WEAK-RANDOMNESS BASIS SELECTION MODEL WITH THE WEAK COHERENT SOURCE

The previous analysis result is based on the single-photon state preparation, but the practical QKD system usually uses the weak coherent state. Thus we will analyze the weak-randomness basis selection model with the weak coherent state preparation, where the difficultly is how to estimate the upper bound of Eve's information with the given count rate value, QBER value, and randomness deviation value ε.

By applying the previous security analysis result with the single-photon source, we can modify the final secret key rate formula in the following inequality:

$$\begin{aligned}R &\geqslant p(\lambda=0)R_0+p(\lambda=1)R_1\\&\geqslant 1-p(\lambda=0)[ph(e_2)+(1-p)h(e_1)]\\&\quad -p(\lambda=1)[qh(e_4)+(1-q)h(e_3)]\\&\quad -p(\lambda=0)[ph(e_1)+(1-p)h(e_2)]\\&\quad -p(\lambda=1)[qh(e_3)+(1-q)h(e_4)]\\&\geqslant 1-p(\lambda=0)[ph(e_2)+(1-p)h(e_1)]\\&\quad -p(\lambda=1)[qh(e_4)+(1-q)h(e_3)]-h(Q),\end{aligned}\tag{23}$$

where the second inequality in considering the Shannon entropy function is the convex function. $Q=p(\lambda=0)[pe_1+(1-p)e_2]+p(\lambda=1)[qe_3+(1-q)e_4]$ is the QBER value, which can be observed in the practical QKD experimental realization. In this secret key rate, the leaked key information can be divided into two parts, where the first part $p(\lambda=0)[ph(e_2)+(1-p)h(e_1)]+p(\lambda=1)[qh(e_4)+(1-q)h(e_3)]$ demonstrates the leaked key information during the quantum channel, and the second part $h(Q)$ demonstrates the leaked key information during the error correction step. Note that the first part $p(\lambda=0)[ph(e_2)+(1-p)h(e_1)]+p(\lambda=1)[qh(e_4)+(1-q)h(e_3)]$ can be applied to estimate Eve's information with the single-photon state preparation, which can also be applied in the weak coherent state case.

In the practical QKD experimental realization with the weak coherent source, the multiphoton state may be utilized by Eve to apply the photon-number splitting attack [28,29]. Fortunately, the decoy state method [30–32] can be applied to monitor the photon-number splitting attack. Based on the security analysis result given by [33], the secret key rate with the decoy state method is given by

$$R\geqslant Y_1P_1[1-h(E_1)]-fQ_\mu h(E_\mu),\tag{24}$$

where Y_1 is the single-photon count rate, P_1 is the single-photon probability in Alice's side, E_1 is the single-photon error rate in Bob's side, Q_μ is the total count rate value, E_μ is the total error rate value, and f is the error correction efficiency.

In the secrete key rate formula, $h(E_1)$ can be applied to estimate the leaked key information during the quantum channel. Note that the phase error rate and the bit error rate are equal in the perfect single-photon state preparation case, and thus only the single-photon bit error rate should be estimated. However, this simple estimation cannot be directly applied in the practical QKD system with the weak-randomness basis selection. To estimate Eve's information with the single-photon state preparation, we should use $p(\lambda=0)[ph(e_2)+(1-p)h(e_1)]+p(\lambda=1)[qh(e_4)+(1-q)h(e_3)]$ to replace $h(E_1)$, where $p(\lambda=0)pe_1+p(\lambda=1)qe_3=\frac{E_1}{2}$, $p(\lambda=0)(1-p)e_2+p(\lambda=1)(1-q)e_4=\frac{E_1}{2}$. Correspondingly, the final secret key rate can be estimated by applying the following optimization method:

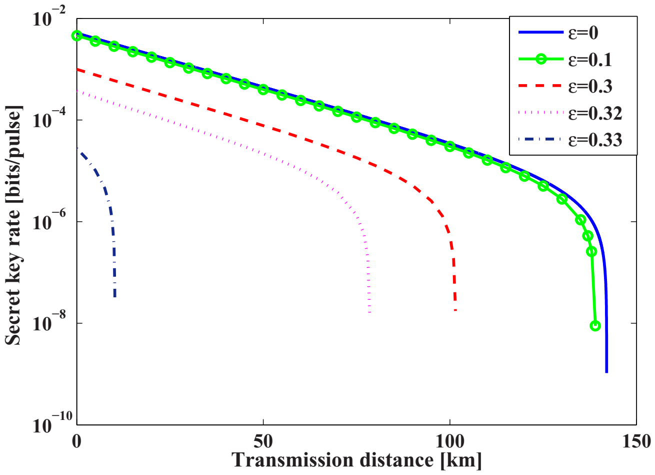

FIG. 4. The relationship between the transmission distance and the secret key rate with different ε values. The solid blue line is the secret key rate with $\varepsilon=0$, the solid green circle line is the secret key rate with $\varepsilon=0.1$, the dashed red line is the secret key rate with $\varepsilon=0.3$, the dotted pink line is the secret key rate with $\varepsilon=0.32$, and the dash-dotted black line is the secret key rate with $\varepsilon=0.33$. By comparing with the perfect-randomness basis selection, the weak-randomness basis selection will decrease the secret key rate and the maximal transmission distance. In the case of $\varepsilon\geqslant 0.34$, the maximal transmission distance will be sharply reduced to 0 km.

$$\begin{aligned}&\text{Minimize}: Y_1P_1\{1-p(\lambda=0)[ph(e_2)+(1-p)h(e_1)]\\&\qquad -p(\lambda=1)[qh(e_4)+(1-q)h(e_3)]\}-fQ_\mu h(E_\mu),\\&\text{Subject to}: p(\lambda=0)+p(\lambda=1)=1,\\&\qquad p(\lambda=0)p+p(\lambda=1)q=\frac{1}{2},\\&\qquad p(\lambda=0)pe_1+p(\lambda=1)qe_3=\frac{E_1}{2},\\&\qquad p(\lambda=0)(1-p)e_2+p(\lambda=1)(1-q)e_4=\frac{E_1}{2},\\&\qquad \frac{1}{2}-\varepsilon\leqslant p,q\leqslant\frac{1}{2}+\varepsilon,\\&\qquad 0\leqslant p(\lambda=0),p(\lambda=1)\leqslant 1,\\&\qquad 0\leqslant e_1,e_2,e_3,e_4\leqslant\frac{1}{2}.\end{aligned}\tag{25}$$

In the asymptotic case, infinite decoy states have been applied to estimate the final secret key rate; the corresponding parameters Y_1, P_1, E_1, Q_μ, and E_μ can be estimated by [34]

$$\begin{aligned}P_1&=\mu e^{-\mu},\\\eta&=10^{\frac{-\alpha l}{10}}\eta_D,\\Y_1&=Y_0+\eta,\\E_1&=\frac{0.5Y_0+e_{Det}\eta}{Y_1},\\Q_\mu&=Y_0+1-e^{-\eta\mu},\\E_\mu&=\frac{0.5Y_0+e_{Det}(1-e^{-\eta\mu})}{Q_\mu},\end{aligned}\tag{26}$$

where μ is the mean photon number of the source, α is the loss coefficient in the quantum channel, l is the length of the fiber, η_D is the detection efficiency in Bob's side, Y_0 is the background rate in Bob's side, and e_{Det} is the probability that a photon hit the erroneous detector.

By applying the Gobby-Yuan-Shields experimental parameters [22] ($\alpha = 0.21$ dB/km, $e_{Det} = 0.033$, $Y_0 = 1.7 \times 10^{-6}$, $\eta_D = 0.045$, $f = 1.22$), the relationship between the transmission distance and the secret key rate with different ε values is given in Fig. 4.

From the calculation result, we can find that the secret key rate and the maximal transmission distance may be significantly reduced under the weak-randomness basis selection model. More precisely, in the case of $\varepsilon = 0.34$, the maximal transmission distance will be sharply reduced from 142 to 0 km, and thus no secret key can be generated correspondingly. However, in the case of $\varepsilon = 0.1$, the maximal transmission distance will be reduced only from 142 to 139 km. By considering the typical transmission distance 50 km with $\varepsilon = 0.1$, the secret key rate will be reduced from 4.45×10^{-4} per pulse to 3.99×10^{-4} per pulse.

VI. CONCLUSION AND DISCUSSION

In this work, we propose a general security analysis model to analyze the security of the practical QKD system with the weak-randomness basis selection. The imperfect basis selection is characterized by the parameter ε; then the secret key rate with the single-photon source and the weak coherent source have been proved, respectively. The analysis result demonstrates that the maximal tolerated error rate and transmission distance will be decreased by comparing with the perfect case. To guarantee security of the practical QKD system, the imperfect basis selection parameter ε should be carefully tested. In future research, it will be interesting to analyze the weak-randomness basis selection in other QKD protocols.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (Grants No. 61675235 and No. 11725524) and the National Key Research and Development Program of China (Grant No. 2016YFA030260).

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[2] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] R. Renner, Ph.D. thesis, Diss. ETH No 16242, 2005, arXiv:quant-ph/0512258.
[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[6] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, Contemp. Phys. **57**, 366 (2016).
[7] H. W. Li, S. Wang, J. Z. Huang, W. Chen, Z. Q. Yin, F. Y. Li, Z. Zhou, D. Liu, Y. Zhang, G. C. Guo, W. S. Bao, and Z. F. Han, Phys. Rev. A **84**, 062308 (2011).
[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, p686 (2010).
[9] B. Qi, C. H. F. Fung, H. K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).
[10] H. W. Li, Z. M. Xu, and Q. Y. Cai, Phys. Rev. A **98**, 062325 (2018).
[11] C. M. Zhang, W. B. Wang, H. W. Li, and Q. Wang, Opt. Lett. **44**, 1226 (2019).
[12] Y. J. Qian, H. W. Li, D. Y. He *et al.*, Chin. Phys. B **24**, 090305 (2015).
[13] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011)
[14] V. Makarov and D. Hjelme, J. Mod. Opt. **52**, 691 (2005).
[15] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).
[16] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[17] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[18] H. W. Li, Z. Q. Yin, S. Wang, Y. Jun Qian, W. Chen, G. C. Guo, and Z. F. Han, Sci. Rep. **5**, 16200 (2015).
[19] M. Huber and M. Pawlowski, Phys. Rev. A **88**, 032309 (2013).
[20] J. Bouda, M. Pivoluska, M. Plesch, and C. Wilmott, Phys. Rev. A **86**, 062308 (2012).
[21] A. S. Trushechkin, P. A. Tregubov, E. O. Kiktenko, Y. V. Kurochkin, and A. K. Fedorov, Phys. Rev. A **97**, 012311 (2018).
[22] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[23] H. K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).
[24] D. Gottesman and H. K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[25] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[26] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H. K. Lo, Phys. Rev. A **78**, 042333 (2008).
[27] J. Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z. Q. Yin, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Phys. Rev. A **89**, 032304 (2014).
[28] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[29] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[30] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[31] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[32] H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[33] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[34] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).