Reference-frame-independent quantum key distribution with source flaws

Can Wang,[1] Shi-Hai Sun,[1] Xiang-Chun Ma,[1] Guang-Zhao Tang,[1] and Lin-Mei Liang[1,2,*]

[1]*College of Science, National University of Defense Technology, Changsha 410073, People's Republic of China*

[2]*State Key Laboratory of High Performance Computing, National University of Defense Technology, Changsha 410073, People's Republic of China*

(Received 1 July 2015; published 15 October 2015)

Compared with the traditional protocols of quantum key distribution (QKD), the reference-frame-independent (RFI)–QKD protocol has been generally proved to be very useful and practical, since its experimental implementation can be simplified without the alignment of a reference frame. In most RFI-QKD systems, the encoding states are always taken to be perfect, which, however, is not practical in realizations. In this paper, we consider the security of RFI QKD with source flaws based on the loss-tolerant method proposed by Tamaki *et al.* [Phys. Rev. A **90**, 052314 (2014)]. As the six-state protocol can be realized with four states, we show that the RFI-QKD protocol can also be performed with only four encoding states instead of six encoding states in its standard version. Furthermore, the numerical simulation results show that the source flaws in the key-generation basis (Z basis) will reduce the key rate but are loss tolerant, while the ones in X and Y bases almost have no effect and the key rate remains almost the same even when they are very large. Hence, our method and results will have important significance in practical experiments, especially in earth-to-satellite or chip-to-chip quantum communications.

DOI: 10.1103/PhysRevA.92.042319 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Based on the basic principles of quantum mechanics, quantum key distribution (QKD) allows two remote parties, Alice and Bob, to share an unconditionally secure key [1–6]. Since the first QKD protocol, BB84 [7], was proposed, QKD has been developing quickly in both theories (including protocols [8–12] and security proofs for ideal and imperfect devices [1–6,13]) and experiments (with long distances and high repetition rates) [14–18].

In most QKD systems mentioned above, a shared reference frame is required between Alice and Bob. For example, Alice and Bob need to align the polarization states in the polarization encoding protocols or keep the interferometer stable in the phase encoding and time-bin encoding protocols. Although it is feasible for Alice and Bob to share the reference frame, it will increase the cost and reduce the performance of the practical systems. Especially in earth-to-satellite QKD [19–21], tracking and aligning quantum signals are very tough and costly, which, in a way, affects the realization of global-scale quantum communication. Luckily, the reference-frame-independent (RFI)–QKD protocol [22–24] is proposed to overcome this problem and has a direct application for earth-to-satellite quantum communication. In RFI QKD, three mutually unbiased bases (Z, X, and Y bases) are used to encode the information. Generally only the Z basis is used to generate the final key, while the X and Y bases are used to estimate the channel parameters. Note the fact that, in practical situations, it is possible and easy to maintain the stability of Z basis while allowing the states in X and Y bases to change slowly in the quantum channel. For example, in the time-bin encoding QKD, the temporal bit (Z basis) is stable, but the superposition states of the two temporal bits (such as the eigenstates of X and Y bases) will change slowly due to the birefringence effect of the channel. Thus in a short time interval, we can assume that the noise of channel for X and Y bases keeps constant, which thus makes it possible to estimate the channel parameters without the match of frame between Alice and Bob. That is, the time-bin encoding QKD can be implemented with reference frame independence, which is very important in experiments. Due to this significance, RFI QKD has been demonstrated experimentally by a few groups both in fiber links and the free space [25–28]. With these experiments carried out, the two relevant scenarios of RFI QKD, earth-to-satellite QKD [19–21] and path-encoded chip-to-chip QKD, are much closer to practical application.

However, one of the main drawbacks of the standard RFI QKD in the previous theoretical analyses and experimental demonstrations is that the imperfections of the source are not considered, which may compromise the security of practical QKD systems. Furthermore, the source flaws caused by the imperfect modulations are always unavoidable, and if using the traditional Gottesman-Lo-Lütkenhaus-Preskill (GLLP) method to deal with such source imperfections, the achievable rate and distance are dramatically degraded such that the RFI-QKD protocol cannot be realized in practice. More severely, if the prepared states, especially in the X and Y bases, have some source flaws, it is not clear whether the RFI-QKD protocol is still reference independent. In this paper, we propose a way to consider the source flaws of RFI QKD with the loss-tolerant technique [29]. As Ref. [29] claims that the six-state protocol [30] can be realized with four states, we show that the same is also true for the protocol of RFI QKD. That is, instead of using six encoding states (all eigenstates of X, Y, and Z bases) in the standard RFI QKD, only four encoding states (two eigenstates of Z basis plus one of the eigenstates each in X and Y bases) are required for Alice and Bob. Furthermore, we analyze the key rate with source flaws in single-photon source and phase-randomized weak coherent source (vacuum + weak decoy state and infinite number of decoy states). The results show that the source flaws in Z basis

*nmliang@nudt.edu.cn

will reduce the key rate but are loss tolerant, while the ones in X and Y bases almost have no effect on the key rate even when they are very large. Additionally, compared to the three-state protocol with infinite number of decoy states, our RFI-QKD scheme with only four encoding states can achieve a better performance.

II. METHOD

A. RFI-QKD protocol

We first briefly review the RFI-QKD protocol [22]. Alice randomly prepares the eigenstates of three mutually unbiased bases $\{X_A, Y_A, Z_A\}$ and sends them to Bob. When Bob receives Alice's sending states, he measures them in his randomly selected bases $\{X_B, Y_B, Z_B\}$. In the standard six-state protocol [30], Alice and Bob should ensure that $Z_A = Z_B$, $X_A = X_B$, and $Y_A = Y_B$, but in RFI QKD, only one pair of bases Z_A and Z_B is required to be well defined, i.e., $Z_A = Z_B$. The other two pairs of bases are allowed to change slowly in the quantum channel, that is, $X_B = \cos\beta X_A + \sin\beta Y_A$ and $Y_B = \cos\beta Y_A - \sin\beta X_A$. The meaning of β depends on specific systems, for example, the phase drift between Alice and Bob in our time-bin encoding protocol. Besides, β is unknown and may vary in time [22]. After the measurements, Alice and Bob announce their bases. The raw keys are distilled from the events in which both Alice and Bob use the Z basis. The quantum bit error rate (QBER) in these raw keys is given by

$$E_{ZZ} = \frac{1 - \langle Z_A Z_B \rangle}{2}. \tag{1}$$

When $E_{ZZ} \leqslant 15.9\%$, Eve's information I_E can be bounded by [22]

$$I_E = (1 - E_{ZZ}) h\left(\frac{1 + v_{\max}}{2}\right) + E_{ZZ} h\left(\frac{1 + f(v_{\max})}{2}\right), \tag{2}$$

where $h(x)$ is the Shannon entropy function and

$$v_{\max} = \min\left[\frac{1}{1 - E_{ZZ}}\sqrt{C/2}, 1\right], \tag{3}$$

$$f(v_{\max}) = \sqrt{C/2 - (1 - E_{ZZ})^2 v_{\max}^2}\Big/ E_{ZZ}. \tag{4}$$

C is an intermediate quantity used to estimate Eve's information and can be written as

$$C = \langle X_A X_B \rangle^2 + \langle X_A Y_B \rangle^2 + \langle Y_A X_B \rangle^2 + \langle Y_A Y_B \rangle^2. \tag{5}$$

Here, note that C is independent of β when plugging the relations X_B and Y_B mentioned above into Eq. (5). However, as Ref. [22] pointed out, in order to accurately estimate C, it is necessary for β to vary slowly in a time short enough for key distribution since C is a statistical quantity [31]. In RFI QKD, the key ingredient is trying to obtain an optimal lower bound of C.

B. Calculation of C

As shown previously, the quantity C plays an important role in the calculation of the key rate for RFI QKD. Therefore, in this subsection, we present a method different from what the previous references [22–24,26] gave to calculate the parameter C.

Similar to Eq. (1), we can rewrite the parameters in Eq. (5) as

$$\begin{aligned} E_{XX} &= \frac{1 - \langle X_A X_B \rangle}{2}, \\ E_{XY} &= \frac{1 - \langle X_A Y_B \rangle}{2}, \\ E_{YX} &= \frac{1 - \langle Y_A X_B \rangle}{2}, \\ E_{YY} &= \frac{1 - \langle Y_A Y_B \rangle}{2}. \end{aligned} \tag{6}$$

And then C can be written as [32]

$$\begin{aligned} C = {} & (1 - 2E_{XX})^2 + (1 - 2E_{XY})^2 \\ & + (1 - 2E_{YX})^2 + (1 - 2E_{YY})^2. \end{aligned} \tag{7}$$

In the following we first calculate E_{XX} and the other three parameters E_{XY}, E_{YX}, and E_{YY} can be obtained analogously by applying the same method. The phase error rate E_{XX} is defined as a fictitious bit error rate in the X basis [33]. It is a virtual procedure that Alice first prepares an entanglement state in the Z basis and then both Alice and Bob measure it in the X basis.

In our RFI-QKD scheme, actually, Alice only needs to randomly prepare the four states $\hat{\rho}_{0Z}$, $\hat{\rho}_{1Z}$, $\hat{\rho}_{0X}$, and $\hat{\rho}_{0Y}$ with probability of $1/4$ in Z, X, and Y bases, respectively. The coefficients of the Bloch vector of $\hat{\rho}_{j\alpha}$, with $j \in \{0,1\}$ and $\alpha \in \{X,Y,Z\}$, can be denoted as $(P_X^{j\alpha}, P_Y^{j\alpha}, P_Z^{j\alpha})$ [29]. That is, $\hat{\rho}_{j\alpha} = \frac{1}{2}(\hat{I} + P_X^{j\alpha}\hat{\sigma}_X + P_Y^{j\alpha}\hat{\sigma}_Y + P_Z^{j\alpha}\hat{\sigma}_Z)$, where I is the identity operator and $\hat{\sigma}_X$, $\hat{\sigma}_Y$, and $\hat{\sigma}_Z$ are Pauli operators. Note that, compared with the standard protocol of RFI QKD, $\hat{\rho}_{1X}$ and $\hat{\rho}_{1Y}$ are not needed in our scheme. This is because, based on the loss-tolerant technique, the six-state protocol [30] can be reduced to the four-state protocol shown in Ref. [29]. Below, we show that the four parameters in Eq. (7) can be exactly calculated in our RFI-QKD protocol with the above four states.

The emission of $\hat{\rho}_{jZ}$ can be equivalently expressed by the following process: Alice prepares the state $|\Psi_Z\rangle_{AA_eB} = \frac{1}{\sqrt{2}}\sum_{j=0,1}|j_Z\rangle_A|\phi_{jZ}\rangle_{A_eB}$ and measures system A in the Z basis. Then she sends the system B to Bob. Here, $|\phi_{jZ}\rangle_{A_eB}$ denotes the purification of $\hat{\rho}_{jZ}$, with A_e representing the extended system possessed by Alice. The emissions of $\hat{\rho}_{0X}$ and $\hat{\rho}_{0Y}$ can be considered analogously. So Alice also needs to prepare the states $|\Psi_X\rangle_{AA_eB} = |0_X\rangle_A|\phi_{0X}\rangle_{A_eB}$ and $|\Psi_Y\rangle_{AA_eB} = |0_Y\rangle_A|\phi_{0Y}\rangle_{A_eB}$ in this virtual protocol. As mentioned earlier, the phase error rate E_{XX} is defined as a fictitious bit error rate by measuring $|\Psi_Z\rangle_{AA_eB}$ in the X basis [33], i.e.,

$$E_{XX} = \frac{Y_{0X,1X}^{(Z)} + Y_{1X,0X}^{(Z)}}{Y_{0X,0X}^{(Z)} + Y_{1X,0X}^{(Z)} + Y_{0X,1X}^{(Z)} + Y_{1X,1X}^{(Z)}}, \tag{8}$$

where $Y_{s\gamma,j\alpha}^{(Z)}$, with $s,j \in \{0,1\}$ and $\alpha,\gamma = X$, denotes the joint probability that Alice (Bob) measures the sate $|\Psi_Z\rangle_{AA_eB}$ in the X basis and obtains a bit value j (s). Note that if there are no basis-dependent source flaws, then E_{XX} equals the bit error rate in the X basis [34], which can be directly measured in experiments. However, if taking source flaws into account,

such equivalence no longer holds. That is, the bit error rate in the X basis is unequal to the phase error rate in the Z basis. Thus a method needs to be developed to estimate the phase error rate in the Z basis, since the estimation of E_{XX} in Eq. (8) is a virtual process. Note that when considering source flaws, by taking the relationships $X_B = \cos\beta X_A + \sin\beta Y_A$ and $Y_B = \cos\beta Y_A - \sin\beta X_A$ into Eq. (5), it is easy to obtain that C is still independent of β. So once E_{XX} and the other three parameters in Eq. (7) are computed accurately and C is obtained, then we can use the security proof in Sec. II A (cf. Ref. [22]) to carry out our analysis on source flaws.

Here, for simplicity, we assume that the states prepared by Alice are pure (the following method can be directly applied to the case that Alice prepares mixed states up to a purification of them first). Then Alice actually prepares $|\Psi_Z\rangle_{AB} = (|0_Z\rangle_A|\phi_{0Z}\rangle_B + |1_Z\rangle_A|\phi_{1Z}\rangle_B)/\sqrt{2}$. In the virtual process, Alice measures system A in the X basis and sends system B (a virtual state) to Bob. Thus the term $Y^{(Z)}_{sX,jX}$ can be written as [29]

$$Y^{(Z)}_{sX,jX} = p_{jX,vir}\big(q_{sX|Id} + P_X^{jX,(vir)} q_{sX|X} + P_Y^{jX,(vir)} q_{sX|Y} + P_Z^{jX,(vir)} q_{sX|Z}\big)/4, \quad (9)$$

where $p_{jX,vir}$ is the probability that the virtual state (system B) is emitted, and $1/4$ is the probability that Bob chooses the X basis for his measurements (note that the probabilities of his selections of Y and Z bases are $1/4$ and $1/2$, respectively). $q_{sX|t} = \mathrm{Tr}(\hat{D}_{sX}\hat{\sigma}_t)/2$, with $t \in \{Id, X, Y, Z\}$, is defined as the transmission rate of $\hat{\sigma}_t$, and the operator $\hat{D}_{sX}$ contains Eve's operation as well as Bob's measurement [29]. The channel parameters are totally described by $\hat{\sigma}_t$, so once $q_{sX|t}$ is obtained, we can get the transmission rate $Y^{(Z)}_{sX,jX}$ of the virtual state.

Here, we consider the protocol of RFI QKD based on time-bin encoding. The perfect encoding states of the Z basis can be denoted as $|0_Z\rangle$ for the short path and $|1_Z\rangle$ for the long path. However, due to the extinction ratio of the practical optical attenuator or intensity modulator (IM) introducing source flaws, Alice actually produces $|0_Z\rangle$ and $|1_Z\rangle$ with probabilities of $\cos^2\frac{\delta_1}{2}$ and $\cos^2\frac{\delta_2}{2}$, respectively. In the X and Y bases, the unsymmetrical splitting rate of beam splitters as well as other imperfections also introduce source flaws into the states, which we denote by δ_3 and δ_4 in a general manner. Besides, the phase modulator may also add some wrong phases which are defined by θ_1 and θ_2. Based on the above description, in general, the four states sent to Bob can be expressed as

$$\begin{aligned}
|\phi_{0Z}\rangle &= \cos\frac{\delta_1}{2}|0_Z\rangle + \sin\frac{\delta_1}{2}|1_Z\rangle,\\
|\phi_{1Z}\rangle &= \sin\frac{\delta_2}{2}|0_Z\rangle + \cos\frac{\delta_2}{2}|1_Z\rangle,\\
|\phi_{0X}\rangle &= \sin\left(\frac{\pi}{4}+\frac{\delta_3}{2}\right)|0_Z\rangle + \cos\left(\frac{\pi}{4}+\frac{\delta_3}{2}\right)e^{i\theta_1}|1_Z\rangle,\\
|\phi_{0Y}\rangle &= \sin\left(\frac{\pi}{4}+\frac{\delta_4}{2}\right)|0_Z\rangle + \cos\left(\frac{\pi}{4}+\frac{\delta_4}{2}\right)e^{i(\frac{\pi}{2}+\theta_2)}|1_Z\rangle.
\end{aligned} \quad (10)$$

Then the probabilities $p_{jX,vir}$ can be calculated by $p_{jX,vir} = |\langle j_X|\Psi_Z\rangle_{AB}|^2$, where $|j_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + (-1)^j|1_Z\rangle)$. So we obtain that $p_{0X,vir} = (1+\sin\frac{\delta_1+\delta_2}{2})/2$ and $p_{1X,vir} = (1-\sin\frac{\delta_1+\delta_2}{2})/2$. In addition, the actual states in experiments also satisfy Eqs. (9), i.e.,

$$\begin{aligned}
&\big(Y^{(Z)}_{sX,0Z}, Y^{(Z)}_{sX,1Z}, Y^{(X)}_{sX,0X}, Y^{(Y)}_{sX,0Y}\big)\\
&\quad = (q_{sX|Id}, q_{sX|X}, q_{sX|Y}, q_{sX|Z})\hat{A}/16,
\end{aligned} \quad (11)$$

where $1/16$ is the joint probability that Alice sends one of the four states and Bob chooses the X basis for his measurement. $\hat{A} := (\vec{V}^T_{0Z}, \vec{V}^T_{1Z}, \vec{V}^T_{0X}, \vec{V}^T_{0Y})$ and $\vec{V}^T_{j\alpha} := (1, P_X^{j\alpha}, P_Y^{j\alpha}, P_Z^{j\alpha})$ with T representing the transposition. Given the prepared states in Eqs. (10), the matrix A equals

$$A = \begin{pmatrix} 1 & 1 & 1 & 1\\ \sin\delta_1 & \sin\delta_2 & \cos\delta_3\cos\theta_1 & -\cos\delta_4\sin\theta_2\\ 0 & 0 & \cos\delta_3\sin\theta_1 & \cos\delta_4\cos\theta_2\\ \cos\delta_1 & -\cos\delta_2 & \sin\delta_3 & \sin\delta_4 \end{pmatrix}. \quad (12)$$

Note that when a single-photon source is used, the yield $Y^{(\gamma)}_{s\alpha,j\gamma}$ can be directly obtained from experimental measurements. By using Eq. (11) and the matrix A, $q_{sX|t}$ can be easily obtained. Then, combined with Eq. (9) we can exactly estimate the value of E_{XX} in Eq. (8).

C. Estimation of the key generation rate

After obtaining the value of C, in this subsection, we estimate the key-generation rate of RFI QKD based on two kinds of source: single-photon source and phase-randomized weak coherent source (WCS) with vacuum+weak decoy state.

1. Single-photon source

We consider the channel model proposed by Ref. [29], where the conditional probability for single-photon state is $V_{s\alpha|j\gamma}$ (i.e., the conditional probability that Bob obtains s when he chooses α basis for measurement given that Alice sent him the state $|\phi_{j\gamma}\rangle$). It can be written as

$$\begin{aligned}
V_{s\alpha|j\gamma} &= \eta C_{s\alpha|j\gamma}(1-e_d) + (1-\eta)e_d(1-e_d)\\
&\quad + \tfrac{1}{2}\big[\eta e_d + (1-\eta)e_d^2\big],
\end{aligned} \quad (13)$$

where e_d is the dark count rate of the detector and η denotes the total transmittance of the system including the channel as well as Bob's detection apparatus (η_d). The term $C_{s\alpha|j\gamma}$ denotes the theoretical probability that Bob measures the state $|\phi_{j\gamma}\rangle$ and obtains the value s when he chooses the α basis. In Eq. (13), the first (second) term models a single click detection at Bob's side produced by a photon (dark count), while the last term represents the simultaneous clicks. Note that in the case of simultaneous clicks, Bob assigns a random bit value to the measurement result. Based on $V_{s\alpha|j\gamma}$ as well as the fact that Alice sends each of the four states with probability of $1/4$, we can readily obtain $Y^{(\gamma)}_{s\alpha,j\gamma}$. Then the single-photon gain $Q^{(1)}_Z$ and the bit error rate E_{ZZ} are given by, respectively,

$$\begin{aligned}
Q^{(1)}_Z &= Y^{(Z)}_{0Z,0Z} + Y^{(Z)}_{1Z,0Z} + Y^{(Z)}_{1Z,1Z} + Y^{(Z)}_{0Z,1Z},\\
W^{(1)}_Z &= Y^{(Z)}_{1Z,0Z} + Y^{(Z)}_{0Z,1Z},\\
E_{ZZ} &= W^{(1)}_Z \big/ Q^{(1)}_Z.
\end{aligned} \quad (14)$$

After obtaining C and E_{ZZ}, then we can estimate Eve's information I_E in Eq. (2). Finally, the key generation rate in the case of single-photon source is given by

$$R = 1 - h(E_{ZZ}) - I_E. \tag{15}$$

2. *Phase-randomized WCS with vacuum and weak decoy state*

In most practical QKD systems, a weak coherent source combined with decoy-state method [35–37] is generally used to overcome the photon-number-splitting (PNS) attack against the multiphoton pulses. In this case, we must calculate the conditional probability $V_{n,s\alpha|j\gamma}$ for n-photon state. Note that there are two detectors in our scheme and thus the valid click contains two situations: Only one of detectors clicks and both of them click. For example, if Alice sends the single-photon state $|\phi_{0Z}\rangle$ and meanwhile Bob chooses the Z basis to measure the coming photon, then in the ideal case, Bob gets the correct result (bit 0) with the probability of $C_{0Z|0Z}$ and wrong result (bit 1) with the probability of $C_{1Z|0Z}$. However, when Alice sends the weak coherent state, Bob will obtain the correct result with the probability of $[(1-\eta C_{1Z|0Z})^n(1-e_d) - (1-\eta)^n(1-e_d)^2]$ and the wrong result with the probability of $[(1-\eta C_{0Z|0Z})^n(1-e_d) - (1-\eta)^n(1-e_d)^2]$ after considering the total transmittance η, where n means the number of photons in the coming pulse. The probability that two detectors click simultaneously is given by $D_{two} = 1 - [(1-\eta C_{0Z|0Z})^n(1-e_d) - (1-\eta)^n(1-e_d)^2] - (1-\eta C_{1Z|0Z})^n(1-e_d)$. Thus, when the n-photon state $|\phi_{j\gamma}\rangle$ is sent and Bob randomly chooses the α basis to measure, the conditional probability $V_{n,s\alpha|j\gamma}$ is given by

$$\begin{aligned} V_{n,s\alpha|j\gamma} = {} & \tfrac{1}{2} + \tfrac{1}{2}(1-e_d)[(1+\eta C_{s\alpha|j\gamma} - \eta)^n \\ & - (1-\eta C_{s\alpha|j\gamma})^n - (1-e_d)(1-\eta)^n]. \end{aligned} \tag{16}$$

In the following, for simplicity, we use the notations

$$a = \eta C_{s\alpha|j\gamma}, \quad D = 1 - e_d. \tag{17}$$

According to the decoy-state method [38], the overall gains for the signal and decoy states are written as

$$\begin{aligned} Q_{\mu,s\alpha,j\gamma} &= \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{n!} e^{-\mu} \\ &= \frac{1}{2}\{1 + D[e^{(-\eta+a)\mu} - e^{-a\mu} - De^{-\eta\mu}]\}, \end{aligned} \tag{18}$$

$$\begin{aligned} Q_{\nu,s\alpha,j\gamma} &= \sum_{n=0}^{\infty} Y_n \frac{\nu^n}{n!} e^{-\nu} \\ &= \frac{1}{2}\{1 + D[e^{(-\eta+a)\nu} - e^{-a\nu} - De^{-\eta\nu}]\}, \end{aligned} \tag{19}$$

where μ and ν denote the intensities of signal and decoy states, respectively. Since the overall gain Q_μ and Q_ν can be directly available in experiments, the lower bound of the yield of the single-photon pulse is given by [38]

$$Y^l_{1,s\alpha,j\gamma} = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right), \tag{20}$$

where $Y_0 = e_d(1 - \frac{1}{2}e_d)$ mainly arises from the dark count of detectors. Then the gain of the single-photon pulse $Q^{(1)}_Z$ in the Z basis and the bit error rate E_{ZZ} can be obtained by [29]

$$\begin{aligned} Q^{(1)}_Z &= e^{-\mu}\mu\left(Y^l_{1,0Z,0Z} + Y^l_{1,0Z,1Z} + Y^l_{1,1Z,1Z} + Y^l_{1,1Z,0Z}\right), \\ W^{(1)}_Z &= Y^l_{1,1Z,0Z} + Y^l_{1,0Z,1Z}, \\ E_{ZZ} &= W^{(1)}_Z \big/ Q^{(1)}_Z. \end{aligned} \tag{21}$$

Additionally, we can easily obtain the overall gain Q_Z and the bit error rate e_Z in the Z basis directly from the statistics of experimental data. They are given by

$$\begin{aligned} Q_Z &= \tfrac{1}{4}(Q_{\mu,0Z,0Z} + Q_{\mu,1Z,0Z} + Q_{\mu,1Z,1Z} + Q_{\mu,0Z,1Z}), \\ W_Z &= \tfrac{1}{4}(Q_{\mu,1Z,0Z} + Q_{\mu,0Z,1Z}), \\ e_Z &= W_Z/Q_Z. \end{aligned} \tag{22}$$

Finally, the key generation rate in the case of phase-randomized WCS with vacuum+weak decoy state is given by [26]

$$R = -Q_Z f h(e_Z) + Q^{(1)}_Z(1 - I_E). \tag{23}$$

In addition, after replacing $Q^{(1)}_Z$ and E_{ZZ} in the above equation with those in Eqs. (14), we can also easily obtain the key rate of RFI QKD based on phase-randomized WCS with infinite number of decoy states.

III. SIMULATION RESULTS

As mentioned previously, currently, almost all the theoretical analyses and experimental realizations do not include the consideration of source flaws in RFI QKD. This is because the performance given by the standard GLLP model with source flaws is rather pessimistic and not loss tolerant [3,13,39]. However, combined with the loss-tolerant technique proposed in Ref. [29], we have obtained the key-generation rate of RFI QKD, taking into account the source flaws in a general method shown in the previous section. Numerical simulation results show that, when considering the source flaws, our protocol of RFI QKD is still able to obtain a high performance, as shown in Fig. 1.

Figure 1 shows the key-generation rates of RFI QKD with source flaws based on the single-photon source [part (a)] and phase-randomized WCS with vacuum + weak decoy state [part (b)], respectively. Here, the intensity of weak coherent state is optimized for each line to maximize the key rate (the same optimization is also carried out in the following figures). It can be seen clearly that both the rates and distances have a small decrease with the source flaws but the source flaws are loss tolerant. And, even with large errors, say $\delta_1 = \delta_2 = 0.3006$, the maximal distance can still be nearly 150 km for the vacuum + weak decoy state, which indicates that our method is able to give a high performance for RFI QKD with source flaws instead of a pessimistic result with the GLLP method [3,13,39], since in the GLLP model the flaws are assumed to be able to be enhanced by Eve exploiting the losses and thus leading to a severe degradation of performance. Here, $\delta_1 = \delta_2 = 0.3006$ corresponds to the 16 dB $[\sin^2(\frac{0.3006}{2}) = 10^{-16/10}]$ extinction ratio of the practical optical attenuator or intensity modulator

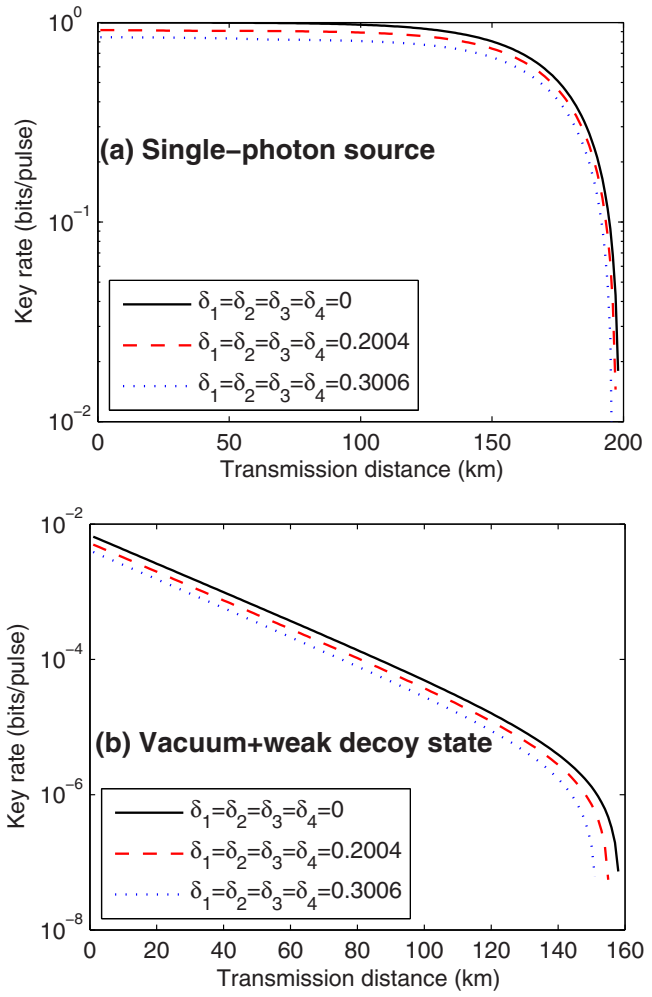

FIG. 1. (Color online) Secret key rates of RFI-QKD with source flaws based on (a) single-photon source and (b) phase-randomized WCS with vacuum + weak decoy state. The source flaws are indicated by $\delta_1,\delta_2,\delta_3,\delta_4,\theta_1$, and θ_2 (all in radian units) shown in Eqs. (10). Here, we have assumed $\theta_1 = \theta_2 = 0$, for they have the same effect as the rotation angle β of the X and Y bases in the standard RFI QKD. The parameters used in our method are coming from Ref. [29], i.e., $e_d = 0.85 \times 10^{-6}$, $\eta_d = 0.15$, $f = 1.22$, and the loss coefficient of the channel is $0.21dB/km$.

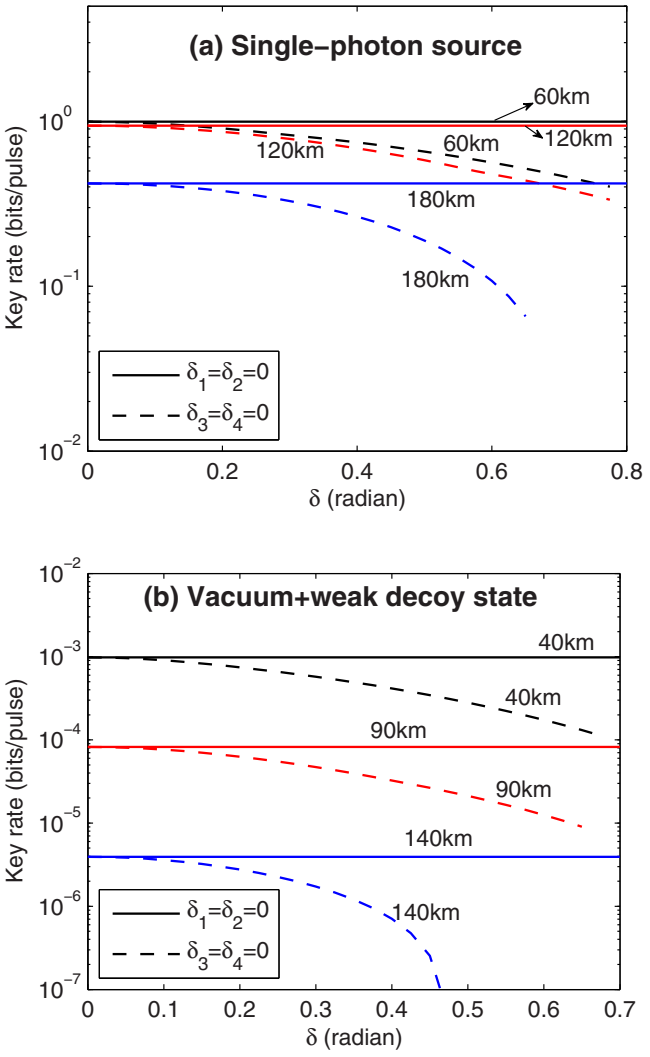

FIG. 2. (Color online) Secret key rates vs source flaws in RFI QKD based on (a) single-photon source and (b) phase-randomized WCS with vacuum + weak decoy state for a given transmission distance. In both figures, solid lines indicate that the source flaws only exist in the X and Y bases while the states in the Z basis are perfect, i.e., $\delta_1 = \delta_2 = 0$; dashed lines are vice versa. The other parameters are the same as those in Fig. 1.

in a system with time-bin encoding, and 0.2004 corresponds to 20 dB [$\sin^2(\frac{0.2004}{2}) = 10^{-20/10}$], which are typical values in practical experiments. Besides, we have assumed the same errors exist in the X, Y, and Z bases for simplicity, and also assumed $\theta_1 = \theta_2 = 0$, for they have the same effect as the rotation angle β of the X and Y bases in the standard RFI QKD.

Moreover, we also find that, shown in Fig. 2, the source flaws in the X and Y bases almost have no effect on the key rates in both cases, single-photon source and phase-randomized WCS, although flaws in the Z basis decrease key rates, as shown by dashed lines, due to the increase of the error rates with the increase of source flaws. This is because, using our method, we can give a precise estimation of the quantity C in Eq. (7) and Eve cannot amplify the source flaws by exploiting the channel loss; i.e., the key rates are independent of the source flaws in the X and Y bases shown by the solid lines in Fig. 2. Here, we point out that the source flaws (δ_3 and δ_4) in the X and Y bases are different from the rotation of X and Y bases in RFI QKD. In standard RFI-QKD protocol, the X and Y bases between Alice and Bob have an rotation angle β on the $X-Y$ plane of the Bloch sphere, which means that Bob's receiving states have errors in the X and Y bases. The errors can be seen as a unitary operation on the states sent by Alice, and thus do not affect the key rate since a lower bound of C in Eq. (2) can be found independent of β in RFI QKD as mentioned previously. However, in our method, the errors (δ_3 and δ_4) in the X and Y bases are arbitrary instead of arising from unitary operations.

In the above figures, we assume that the same errors consist in Alice's two sending states of the Z basis, i.e., $\delta_1 = \delta_2$, which is reasonable since the optical attenuators or intensity

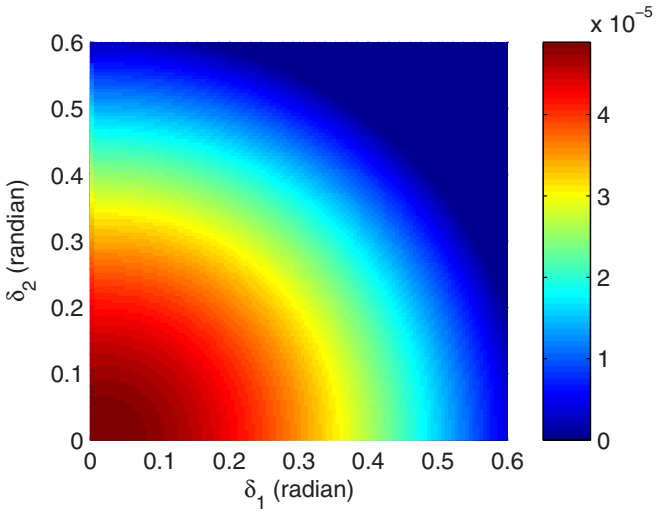

FIG. 3. (Color online) Secret key rates as a function of source flaws δ_1 and δ_2 in the Z basis while the states in X and Y bases are perfect, i.e., $\delta_3 = \delta_4 = 0$, $\theta_1 = \theta_2 = 0$, in RFI QKD for a given distance of 100 km. The other parameters are the same as those in Fig. 1.

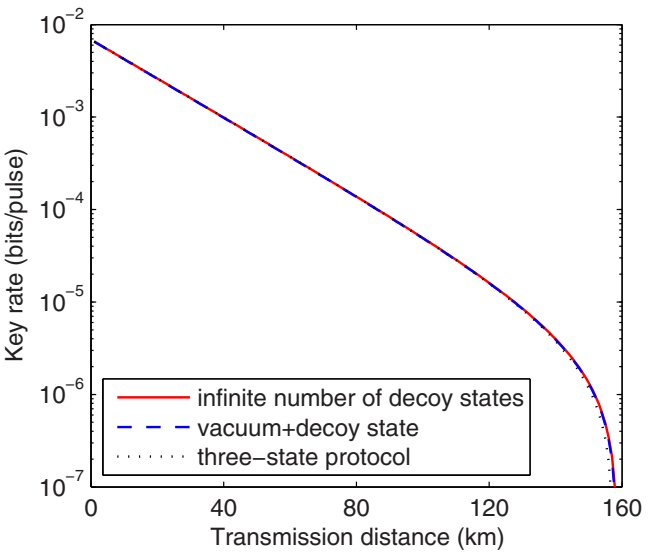

FIG. 4. (Color online) Comparison of secret key rates in the three-state protocol [29] (dotted line), the RFI-QKD protocol with infinite number of decoy states (solid line), and the RFI-QKD protocol with the vacuum + weak decoy state (dashed line). The results of the three lines are all based on the same probability of the Z-basis-matched events. That is, Alice prepares each of the two states in the Z basis with probability $1/4$ and Bob chooses the Z basis with probability $1/2$, so the probability of the Z-basis-matched events is $1/4$.

modulators used in practical systems are generally symmetric in the long path and short path for the time-bin encoding protocol. However, even they are different ($\delta_1 \neq \delta_2$), we can still get the same results as above. For example, in Fig. 3, we plot the key rates as a function of source flaws δ_1 and δ_2 in the Z basis for a given distance, 100 km, while the states in X and Y bases are set to be perfect since flaws in these two bases have no effect. We can see that, with increase of the source flaws in the Z basis, the key rates decrease due to the increase of error rates in the Z basis, and even with very large errors, there still exist key rates for 100-km transmission distance, which clearly shows that Eve cannot enhance the flaws by exploiting the channel loss. Moreover, Fig. 3 also shows that equal errors ($\delta_1 = \delta_2$) in the two encoding states of the Z basis can result in higher key rates than the biased errors ($\delta_1 \neq \delta_2$) in these two encoding states. Here, we have set the same form errors [$\sin^2\frac{\delta_1}{2}$ and $\sin^2\frac{\delta_2}{2}$ in Eqs. (10)] in the two states of the Z basis, so the key rates are symmetric with respect to δ_1 and δ_2. Consequently, when implementing RFI QKD, it is necessary to confirm the perfect encoding of the key generation basis (e.g., Z basis) as much as possible, and the encoding of other bases can be relaxed as long as the prepared four states' terminal points of the Bloch vectors form a triangular pyramid in the Bloch sphere as claimed in Ref. [29].

In addition, we also give a comparison of performance between our RFI-QKD scheme with only four states (solid and dashed lines) and the three-state protocol (dotted line) [29] based on the same probability of the Z-basis-matched events in Fig. 4. As mentioned earlier, the key rate of the three-state protocol coincides with that of the BB84 protocol (both protocols are based on infinite number of decoy states) [29]. In other words, our RFI-QKD scheme with four states can achieve a comparable performance but with a longer achievable distance compared with the three-state protocol and BB84 protocol. Besides, the two almost overlapped lines show the key rates of our RFI-QKD scheme with two kinds of decoy states: infinite number of decoy states (solid line) and vacuum + weak decoy state (dashed line). It means that our RFI-QKD scheme can be easily performed with the vacuum + weak decoy state, instead of the infinite number of decoy states, but can obtain almost the same performance as the latter.

IV. CONCLUSION

In conclusion, we have analyzed the security of RFI QKD with source flaws. Compared with the standard RFI-QKD protocol, only four states are needed in our method, even if imperfect sources are used. Our results suggest that it is important to have precise state preparations in the key-generation basis, while in other bases, there is no such strict requirement. In other words, only if the four states are appropriately prepared, we can get a very high performance in RFI QKD with source flaws. In addition, the RFI-QKD scheme can supply a performance comparable to the three-state protocol [29] and BB84 protocol. More importantly, it will be much simpler to demonstrate our scheme experimentally, in particular, to realize the quantum communications in earth-to-satellite links and chip-to-chip integrated photonic wave guides, because only four states are required for encoding and only key-generation basis needs to be aligned. Besides, the currently mature finite-size method of RFI QKD [23,25–28] can be directly applied to our scheme without any difficulty, which should be included in the further research and the practical experiments.

ACKNOWLEDGMENTS

The authors thank the referee for helpful suggestions and discussions. This work is supported by the National Natural Science Foundation of China, Grants No. 61072071 and No. 11304391. L.-M.L. is supported by the Program for New Century Excellent Talents.

[1] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[2] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[3] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[4] M. Koashi, New J. Phys. **11**, 045018 (2009).
[5] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
[6] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commum. **3**, 604 (2012).
[7] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[8] K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[9] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
[10] T. C. Ralph, Phys. Rev. A **61**, 010303 (1999).
[11] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[12] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[13] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).
[14] I. Lucio-Martinez, P. Chan, X. Mo, and W. Tittel, New J. Phys. **11**, 095001 (2009).
[15] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).
[16] Y. Liu *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).
[17] Z.-Y. Tang, Z.-F. Liao, F.-H. Xu, B. Qi, L. Qian, and H.-K Lo, Phys. Rev. Lett. **112**, 190503 (2014).
[18] Y.-L. Tang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).
[19] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).
[20] C. Bonato, A. Tomaello, V.-D. Deppo, G. Naletto, and P. Villoresi, New J. Phys. **11**, 045017 (2009).
[21] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel, and T. Jennewein, Phys. Rev. A **84**, 062326 (2011).
[22] A. Laing, V. Scarani, J. G. Rarity, and J.-L. OBrien, Phys. Rev. A **82**, 012304 (2010).
[23] L. Sheridan, T.-P. Le, and V. Scarani, New J. Phys. **12**, 123019 (2010).
[24] T.-P. Le, L. Sheridan, and V. Scarani, Int. J. Quantum. Inform. **10**, 1250035 (2012).
[25] M. S. Palsson, J. J. Wallman, A. J. Bennet, and G. J. Pryde, Phys. Rev. A **86**, 032322 (2012).
[26] W.-Y. Liang, S. Wang, H.-W. Li, Z.-Q. Yin, W. Cen, Y. Yao, J.-Z. Huang, G.-C. Guo, and Z.-F. Han, Sci. Rep. **4**, 3617 (2014).
[27] J. Wabnig, D. Bitauld, H.-W. Li, A. Laing, J. L. O'Brien, and A. O. Niskanen, New J. Phys. **15**, 073001 (2013).
[28] P. Zhang *et al.*, Phys. Rev. Lett. **112**, 130501 (2014).
[29] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).
[30] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).
[31] Note that although C is independent of β, it does not mean that the variation of β during the run of the protocol will not affect C. Actually, since C is a statistical quantity, the fast variation of β can make the estimated value of C so small such that the key rate turns to zero. See details in Refs. [22–28].
[32] Z.-Q. Yin, S. Wang, W. Chen, H.-W. Li, G.-C. Guo, and Z.-F. Han, Quant. Info. Proc. **13**, 1237 (2014).
[33] M. Koashi, arXiv:0704.3661 [quant-ph].
[34] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 431 (2007).
[35] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[36] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[37] H.-K. Lo, X.-F. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[38] X.-F. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[39] E. Woodhead and S. Pironio, Phys. Rev. A **87**, 032315 (2013).