Reference-Frame-Independent Quantum Key Distribution Using Fewer States

Hongwei Liu, Jipeng Wang, Haiqiang Ma, and Shihai Sun

1 School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
2 College of Liberal Arts and Science, National University of Defense Technology, Hunan, Changsha 410073, China

(Dated: March 14, 2022)

Reference-frame-independent quantum key distribution (RFI QKD) protocol can reduce the requirement on the alignment of reference frames in practical systems. However, comparing with the Bennett-Brassard (BB84) QKD protocol, the main drawback of RFI QKD is that Alice needs to prepare six encoding states in the three mutually unbiased bases (X, Y, and Z), and Bob also needs to measure the quantum state with such three bases. Here, we show that the RFI QKD protocol can be secured in the case where Alice sends fewer states. In particular, we find that transmitting three states (two eigenstates of the Z basis and one of the eigenstates in the X basis) is sufficient to obtain the comparable secret key rates and the covered distances, even when the security against coherent attacks with statistical fluctuations of finite-key size is considered. Finally, a proof-of-principle experiment based on time-bin encoding is demonstrated to show the feasibility of our scheme, and its merit to simplify the experimental setup.

I. INTRODUCTION

Quantum key distribution (QKD) has been attracting major attentions due to its higher-level security for information privacy. Unlike the classical cryptography, QKD is based on the principles of quantum physics and one-time pad, which has been proved unconditional secure [1–5]. Secure communication via QKD is one of important applications of the quantum information science, which can be realized with current technologies. Nowadays, QKD has been studied not only in laboratories [6–11], but also in companies [12]. Some companies have started making hardware and doing field tests focused on it [13, 14].

For the practical applications, realistic security of QKD has been investigated to close the gap between the assumptions made in the security proofs and the actual implementations [15–17]. Experimentally, it has been implemented via optical means, achieving key rate of 13.72 megabits per second over 2-dB of standard optical fiber [18] and of 1.16 bits per hour over 404 km of ultralow-loss fiber in measurement-device-independent configuration [19]. Most recently, a new scheme was proposed, which is a promising step towards overcoming the rate-distance limit of QKD without quantum repeaters and greatly extending the range of secure quantum communications [20–21]. However, reducing the systems complexity is still a vital issue in real-life applications of QKD.

In most QKD systems, a shared reference frame is required between a sender (Alice) and a receiver (Bob): alignment of polarization states for polarization encoding, interferometric stability for phase encoding. Hence, an active reference frame calibration is needed to ensure the achievable secure key rate. Although additional alignment parts appear feasible, they will increase the complexity of practical systems, and even lead to extra information leakage through these ancillary processes [22]. Fortunately, a promising scheme, named reference-frame-independent (RFI) QKD, is proposed to eliminate the requirement of alignment [23–24]. In this protocol, three orthogonal bases (X, Y, and Z) are required to encode the information, in which the X and Y are used as monitoring-bases to estimate eavesdropper’s information, and Z basis is generally used to generate the final key. The states in the Z basis, such as the time-bin eigen-states, are naturally well-aligned, whereas the states in X and Y bases are allowed changing slowly in the quantum channel. Due to this significance, RFI QKD could be very useful in several scenarios, such as earth-to-satellite QKD [25] and path-encoded chip-to-chip QKD [26]. Several theoretical studies and experimental works have been reported [27–31].

As mentioned above, the RFI QKD protocol needs six states in the processes of key distribution, whereas only four states are required in the Bennett-Brassard (BB84) QKD protocol. Is it possible that we use only four or even less states to complete the task and meanwhile keep the merit of RFI QKD protocol? A theoretical study have explored this possibility, whose advantage is that doing so may simplify the implementation, e.g., less randomness is required and possibly fewer optical elements are need. By exploiting the additional information gleaned from the mismatches basis statistics [32–34], Tamaki et al. [32] showed that three states (two eigenstates of Z basis and one of the eigenstates each in X) are enough to secure the BB84 protocol, and Wang et al. [35] showed that the RFI QKD protocol can be fully secured using only four states (two eigenstates of Z basis and one of the eigenstates each in X and Y bases), and the resulting secret key rate is exactly the same as the original RFI QKD protocol. Hence, it still needs one more state compared with the BB84 protocol.

Recently, by adopting the method of convex opti-
mization to estimate the Eve’s information, Islam et al. [36] reduced the number of the state in arbitrary $d$-dimensional QKD system. They show that the protocol can be secure even when using just one monitoring-basis state as long as the channel noise is low enough. In this paper, under the assumption of basis-independent state preparation, we find the number of states required in the RFI QKD protocol can be further reduced to three states (two eigenstates of $Z$ basis plus one of the eigenstates in $X$ basis) by using the semidefinite programming (SDP), and the secret key rate and transmission distance is still comparable to the original RFI QKD protocol. We noted that Bob also need randomly choose one of the $X, Y$ and $Z$ bases to measure the states sent from Alice, just like that in the original RFI QKD protocol.

In the following of this paper, we first analyze the security for the generic RFI QKD protocol against arbitrary collective attacks, and then show that this protocol can be secure when using fewer states. An experimental demonstration based on time-bin encoding is proceeded to show the feasibility of our scheme, and its merit to simplify the experimental setup. In the experiment, we also consider the finite-key security against coherent attacks.

II. PROTOCOL AND SECURITY

We first briefly review the RFI QKD protocol [23]. It denotes the three Pauli matrices written $\{\sigma_x, \sigma_y, \sigma_z\}$ by $\{X, Y, Z\}$, and assume the one direction is well defined, i.e., $Z_A = Z_B$. The other two direction 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 $\beta$ depends on specific systems, such as the phase drift between Alice and Bob in time-bin encoding protocol. Besides, $\beta$ is unknown and may vary in time.

In each run, Alice (Bob) selects independently one of the three bases to prepare (measure) the quantum state. At the end of key distribution, They announce their bases. The raw keys are distilled from the events when they both use the well-defined $Z$ basis. The quantum bit error rate (QBER) is given by

$$e_{ZZ} = 1 - \frac{\langle Z_A Z_B \rangle}{2}. \quad (1)$$

According the information collected on the bases complementary to $Z$, Alice and Bob can utilize an intermediate quantity $C$ to estimate Eve’s knowledge. This quantity is defined as

$$C = \langle X_A X_B \rangle^2 + \langle X_A Y_B \rangle^2 + \langle Y_A X_B \rangle^2 + \langle Y_A Y_B \rangle^2. \quad (2)$$

Here, note that $C$ is independent of relative angle $\beta$ when plugging the relations $X_B$ and $Y_B$ mentioned above into Eq. (2). The maximal value under Pauli algebra is $C = 2$, in this case, $e_{ZZ} = 0$ as well: the two parameters $C$ and $e_{ZZ}$ are not independent, as we shall see in more detail later. When $e_{ZZ} \leq 15.9\%$, Eve’s information is given by

$$I_E = (1 - e_{ZZ}) \frac{1}{2} \left(1 + \frac{1 + \mu}{2} e_{ZZ} \right), \quad (3)$$

where $h(x)$ is the binary Shannon entropy, and

$$\mu = \min \left[ \sqrt{C/2 \frac{1}{1-e_{ZZ}}} + 1, \right], \quad \nu = \sqrt{C/2 - (1 - e_{ZZ})^2 \mu^2} / e_{ZZ}. \quad (4)$$

We present this protocol in an equivalent entanglement-based version where Alice and Bob share the state of the form $|\phi\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$. They independently implement a projective measurement on the entangled state to determine the state received by the counterpart. This fact, together with the assumption that it is possible to deal with finite-dimensional systems, guarantees that the security of the RFI QKD protocol can be analyzed against arbitrary collective attacks [37]. Thus, each pair shared by Alice and Bob is supposed to be in two-qubit state $\rho_{AB}$, of which Eve holds a purification $\rho_E = \text{Tr}_{AB}(\rho_{AB})$, where $\rho_{AB}$ is the density matrix shared among Alice, Bob and Eve after the transmission, and the state is $|\Psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |\phi_i\rangle_{AB} |E_i\rangle$, where $|E_i\rangle |\phi_i\rangle = \delta_{ij}$ is the orthogonal basis of system possessed by Eve.

In RFI QKD, it is obvious that the key ingredient is to generate an entanglement-based version where Alice and Bob share a state of the form $|\phi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$. They independently implement a projective measurement on the entangled state to determine the state received by the counterpart. This fact, together with the assumption that it is possible to deal with finite-dimensional systems, guarantees that the security of the RFI QKD protocol can be analyzed against arbitrary collective attacks [37]. Thus, each pair shared by Alice and Bob is supposed to be in two-qubit state $\rho_{AB}$, of which Eve holds a purification $\rho_E = \text{Tr}_{AB}(\rho_{AB})$, where $\rho_{AB}$ is the density matrix shared among Alice, Bob and Eve after the transmission, and the state is $|\Psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |\phi_i\rangle_{AB} |E_i\rangle$, where $|E_i\rangle |\phi_i\rangle = \delta_{ij}$ is the orthogonal basis of system possessed by Eve.

In RFI QKD, it is obvious that the key ingredient is to generate an entanglement-based version where Alice and Bob share a state of the form $|\phi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$. They independently implement a projective measurement on the entangled state to determine the state received by the counterpart. This fact, together with the assumption that it is possible to deal with finite-dimensional systems, guarantees that the security of the RFI QKD protocol can be analyzed against arbitrary collective attacks [37]. Thus, each pair shared by Alice and Bob is supposed to be in two-qubit state $\rho_{AB}$, of which Eve holds a purification $\rho_E = \text{Tr}_{AB}(\rho_{AB})$, where $\rho_{AB}$ is the density matrix shared among Alice, Bob and Eve after the transmission, and the state is $|\Psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |\phi_i\rangle_{AB} |E_i\rangle$, where $|E_i\rangle |\phi_i\rangle = \delta_{ij}$ is the orthogonal basis of system possessed by Eve.

In RFI QKD, it is obvious that the key ingredient is to generate an entanglement-based version where Alice and Bob share a state of the form $|\phi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$. They independently implement a projective measurement on the entangled state to determine the state received by the counterpart. This fact, together with the assumption that it is possible to deal with finite-dimensional systems, guarantees that the security of the RFI QKD protocol can be analyzed against arbitrary collective attacks [37]. Thus, each pair shared by Alice and Bob is supposed to be in two-qubit state $\rho_{AB}$, of which Eve holds a purification $\rho_E = \text{Tr}_{AB}(\rho_{AB})$, where $\rho_{AB}$ is the density matrix shared among Alice, Bob and Eve after the transmission, and the state is $|\Psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |\phi_i\rangle_{AB} |E_i\rangle$, where $|E_i\rangle |\phi_i\rangle = \delta_{ij}$ is the orthogonal basis of system possessed by Eve.

In RFI QKD, it is obvious that the key ingredient is to generate an entanglement-based version where Alice and Bob share a state of the form $|\phi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$. They independently implement a projective measurement on the entangled state to determine the state received by the counterpart. This fact, together with the assumption that it is possible to deal with finite-dimensional systems, guarantees that the security of the RFI QKD protocol can be analyzed against arbitrary collective attacks [37]. Thus, each pair shared by Alice and Bob is supposed to be in two-qubit state $\rho_{AB}$, of which Eve holds a purification $\rho_E = \text{Tr}_{AB}(\rho_{AB})$, where $\rho_{AB}$ is the density matrix shared among Alice, Bob and Eve after the transmission, and the state is $|\Psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |\phi_i\rangle_{AB} |E_i\rangle$, where $|E_i\rangle |\phi_i\rangle = \delta_{ij}$ is the orthogonal basis of system possessed by Eve.

In RFI QKD, it is obvious that the key ingredient is to generate an entanglement-based version where Alice and Bob share a state of the form $|\phi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$. They independently implement a projective measurement on the entangled state to determine the state received by the counterpart. This fact, together with the assumption that it is possible to deal with finite-dimensional systems, guarantees that the security of the RFI QKD protocol can be analyzed against arbitrary collective attacks [37]. Thus, each pair shared by Alice and Bob is supposed to be in two-qubit state $\rho_{AB}$, of which Eve holds a purification $\rho_E = \text{Tr}_{AB}(\rho_{AB})$, where $\rho_{AB}$ is the density matrix shared among Alice, Bob and Eve after the transmission, and the state is $|\Psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |\phi_i\rangle_{AB} |E_i\rangle$, where $|E_i\rangle |\phi_i\rangle = \delta_{ij}$ is the orthogonal basis of system possessed by Eve.

In RFI QKD, it is obvious that the key ingredient is to generate an entanglement-based version where Alice and Bob share a state of the form $|\phi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$. They independently implement a projective measurement on the entangled state to determine the state received by the counterpart. This fact, together with the assumption that it is possible to deal with finite-dimensional systems, guarantees that the security of the RFI QKD protocol can be analyzed against arbitrary collective attacks [37]. Thus, each pair shared by Alice and Bob is supposed to be in two-qubit state $\rho_{AB}$, of which Eve holds a purification $\rho_E = \text{Tr}_{AB}(\rho_{AB})$, where $\rho_{AB}$ is the density matrix shared among Alice, Bob and Eve after the transmission, and the state is $|\Psi\rangle_{AB} = \sum_i \sqrt{\lambda_i} |\phi_i\rangle_{AB} |E_i\rangle$, where $|E_i\rangle |\phi_i\rangle = \delta_{ij}$ is the orthogonal basis of system possessed by Eve.
Eve can perform any operations on the states transmitted between Alice and Bob, and hence the bound is valid for any collective attacks respecting the given measurement statistics. This optimization problem can be efficiently solved by using Matlab package CVX designed for disciplined convex programming. The detail of calculations are shown in Appendix A.

![Graph](image)

**FIG. 1.** (Color online) (a) The numerically obtained lower bounds of $C_L$ plotted as a function of the quantum bit error rates $e_{ZZ}$ for the case where Alice sends six, four, and three states respectively. (b) The lower bounds of $C_L$ as a function of the quantum bit error rates $e_{ZZ}$ and misalignments of the reference frame $\beta$ when only three states are sent.

To demonstrate our scheme, we treat the bit-flip rates in the $X$, $Y$ and $Z$ bases equivalently for simplicity, i.e., $e_z = e_x = e_y = e_{ZZ}$, which are caused by channel noise in the transmission. In the original RFI QKD protocol, Alice needs to randomly prepare six states $\{|Z_0\rangle, |Z_1\rangle, |X_0\rangle, |X_1\rangle, |Y_0\rangle, and |Y_1\rangle\}$. By using the method proposed in Ref. [35], the number of states can be reduced to four, where states $|X_1\rangle$ and $|Y_1\rangle$ are redundant to estimate $C_L$. It can be seen from Fig. (a) that the method of optimization applied here correspond to this result, as $C_L$ is the same when Alice sends only four states in comparison to the case when she send all six states (red solid line). Furthermore, our SDP approach is available to estimate the lower bound of $C$ when only three states are sent by Alice, as shown by the solid blue line in Fig. (a).

Note that it is still required for Bob to randomly pick one of three bases $X$, $Y$ and $Z$ to measure Alice’s three states $|Z_0\rangle, |Z_1\rangle$ and $|X_0\rangle$. In the four-state scenario, complete knowledge of the remaining unused states can be reconstructed from the statistics of four used states and from the statistics of the events where Alice and Bob choose different basis. However, when Alice sends only three states, complete knowledge of the non-transmitted states cannot be reconstructed using the experimentally determined statistics. Thus, the lower bound of $C$ decreased faster as $e_{ZZ}$ increased. Nonetheless, $C_L$ at the three-state scenario is still independent to the change of $\beta$, as shown in Fig. (b). This validates that our scheme is reference frame independent, even if only $X$ and $Z$ bases are employed to prepare encoded states.

## III. ESTIMATION OF THE SECRET KEY RATES

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

### A. Single-photon source

In the original six states RFI QKD protocol, the calculation of $C$ need applies the equivalent formula of Eq. (2), it can be written as:

$$C' = (1 - 2e_{XX})^2 + (1 - 2e_{XY})^2 + (1 - 2e_{YY})^2,$$

where $e_{\alpha\chi}$ is the phase error rate defined as a fictitious bit error rate in the $\alpha$ basis and the $\chi$ basis. It is a virtual procedure that Alice first prepares an entanglement state in the $Z$ basis and then Alice (Bob) measure it in the $\alpha$ ($\chi$) basis. If there are no basis-dependent source flaws, the $e_{\alpha\chi}$ equals the QBER when Alice prepares her state in the $\alpha$ basis, and Bob measures it in the $\chi$ basis, which can be directly measured in experiments. For our three states scheme, only $e_{ZZ}, e_{XX}$, and $e_{XY}$ can be extracted from the experiment, these parameters as prior known statistics are sufficient to estimate the lower bound of $C$, since the fictious bit error rates $e_{XX}$ and $e_{YY}$ can be well bounded using the SDP method, as shown in Appendix A. After obtaining $C$ and $e_{ZZ}$, we can estimate Eve’s information $I_E$ in Eq. (3) for the RFI QKD protocol.

In an asymptotic case, the secret key rate defined as the number of bits per pulse is given by

$$R = 1 - h(e_{ZZ}) - I_E.$$

By consider the channel model proposed in Ref. [32], we simulate the secret key rates along with the change of the transmission distances and $e_{ZZ}$ as shown in Fig. (a) and

...
Fig. 2(b) respectively. For comparison, we also simulate the key generation rate of three states BB84 protocol using the SDP approach [50]. When the state-preparation process is assumed ideal, Eve’s information is estimated as $I_E = h(e_{XX})$ for the BB84 protocol. The parameters in our method are set according our experiment system, i.e., the dark count rate of single photon detector (SPD) is $e_d = 8 \times 10^{-6}$, the detection efficiency is $\eta_d = 13\%$, the optical intrinsic error rate is $e_o = 0.01$ and the loss coefficient of the channel is $0.21$ dB/km.

For the specific case where Alice sends all six states (Fig. 2(a), solid red line), it is evident that the maximum error tolerance is $\sim 12.6\%$, which is in agreement with existing findings [22]. The error tolerance is defined as the error rate $e_{ZZ}$ beyond which $R = 0$. Furthermore, we find that secret key rates are identical when Alice sends only four states (Fig. 2(a), solid red line) in comparison to the case when she sends all six states, illustrating that two of the states are redundant. For the case where Alice sends only three states, $e_{XX}$ and $e_{XY}$ can be substitute into our SDP method (shown in Appendix A) to estimate a low bound of $C_L$. It is evident that the three states RFI QKD protocol still generates a positive secret key rate, as illustrated by blue dashed line in Fig. 2, but with a lower error tolerance ($\sim 9.8\%$). Despite the lower error tolerance, we observe that the maximal transmission distances of the three states RFI QKD protocol is close to that of the RFI QKD with four and six states and that of the BB84 protocol when no misalignment of reference frame occurs. Moreover, at the distances of less than 80 km, it is evident that their curves are almost overlapped. In the case of reference frame misalignment, the secret key rates of the RFI QKD protocol remain the same at different $\beta$ whenever six states or three states are sent by Alice. However, the transmission distance and the secret key rate of the BB84 protocol are decreased dramatically at $\beta = \pi/4$, as shown dotted yellow line in Fig. 2(a). These results verify that our scheme based on the single-photon source can release the requirement of the calibration of reference frame, even when only three states are prepared by Alice. We noted that Bob still need pick one of the $X, Y, Z$ bases to measure the states sent from Alice, just like that in the original RFI QKD protocol.

### B. Phase-randomized WCS with decoy-state method

The secret key rate calculated above is based on an ideal single-photon source. However, in most practical QKD systems, a phase-randomized WCS combined with decoy-state method is generally employed to overcome the photon-number-splitting (PNS) attack against the multiphoton pulses [7, 8, 41]. In particular, we assume that Alice can set the intensity of each laser pulse to one of the three predetermined intensity levels, $K \in \{\mu, \nu, \omega\}$, each transmitted with a probability $p_k$. Three intensity levels satisfy the conditions: $\mu > \nu + \omega$ and $0 \leq \omega \leq \nu$. Furthermore, in the applications, the number of total pulses $N$ sent by Alice is always finite; thus, we must consider the effect of statistical fluctuation caused by a finite size fo pulses to ensure the security of the RFI QKD protocol.

In such a scenario, we consider the number of pulses sent by Alice to be $N = 10^{10}$. The probability of Alice (Bob) preparing (measuring) a state with $\alpha$ basis is $Pr_A(\alpha)$. Here, we use all intensity levels for the key generation. According to Ref. [12, 33], the secret key length against coherent attack is

$$\ell = \frac{1}{2} s_{zz,0} + s_{zz,1} (1 - I_E) - n_{zz} f h(E_{ZZ}) - \log_2 \frac{2}{\xi_{EC}} - 2 \log_2 \frac{1}{\xi_{PA}} - 7 n_{zz} \left[ \frac{\log_2 (2/\epsilon)}{n_{zz}} - 30 \log_2 (N + 1) \right],$$

where $s_{zz,0}$ and $s_{zz,1}$ are the number of vacuum events and the number of single-photon events associated with the single-photon events in $Z_A$ respectively. $E_{ZZ}$ is the average of the observed error rate in basis $Z$, $f$ denotes
the inefficiency of error correction, $n_{zz}$ is the number of detected pulses when Alice prepares her state in the $Z$ basis and Bob measures it in the $Z$ basis. $\varepsilon_{EC}$ ($\varepsilon_{PA}$) denotes the probability that error correction (privacy amplification) fails, and $\tilde{\varepsilon}$ measures the accuracy of estimating the smooth min-entropy \cite{42}. In this paper, we set $\varepsilon_{EC} = \varepsilon_{PA} = \tilde{\varepsilon} = \varepsilon = 10^{-10}$.

The number of single-photon events in $Z_A$ is

$$s_{zz,1} \geq \max \left\{ \frac{\tau_1 \mu}{\mu (\nu - \omega) - \nu^2 + \omega^2} n_{zz,0} - \frac{n_{zz,\omega}}{n_{zz,\nu} - n_{zz,\omega}} - \frac{\nu^2 - \omega^2}{\mu^2} (n_{zz,\mu} - s_{zz,0}/\tau_0) \right\},$$

(14)

The QBER $e_{ZZ}$ associated with the single-photon events in $Z_A$ is given by

$$e_{ZZ} \leq \min \left\{ \tau_1 (\nu - \omega) s_{zz,1} + \frac{1}{2}, s_{zz,0} \right\},$$

(15)

where

$$m_{zz,k}^\pm := \max \left\{ \frac{e_k}{p_k} \left( m_{zz,k} \pm \sqrt{\frac{m_{zz,k}}{2} \ln \frac{1}{\varepsilon}} \right), 0 \right\}. \quad (16)$$

We also calculate the number of vacuum events, $s_{\kappa\zeta,0}$, and the number of single-photon events, $s_{\kappa\zeta,1}$, for $\kappa = \cup_{\kappa,\zeta} \in \mathcal{K}_m$, where $\forall \{\kappa, \zeta\} \in \{X, Y\}$, i.e., by using Eqs. (12) and (14) with statistics from the basis $\kappa$. In addition, the formula for the phase error rate of single-photon events in $\kappa \in \mathcal{K}_m$ is \cite{44}

$$e_{\kappa\zeta} \leq \min \left\{ [e_{\kappa\zeta} + \gamma (\varepsilon, e_{\kappa\zeta}, s_{\kappa\zeta,1}, s_{\kappa\zeta,1})] \right\},$$

(17)

where $e_{\kappa\zeta}$ can be calculated using Eq. (15), and

$$\gamma (a, b, c, d) := \sqrt{\frac{(c + d)(1 - b)}{cd} \ln \frac{c + d}{2\pi c d (1 - b) d a^2}}.$$  

(18)

For the evaluation, we numerically optimize the secret key rate $R := \ell/N$ over the free parameters $\{\Pr_X, p_u, p_v, \mu, \nu\}$ as shown in Fig. 3(a). Due to the symmetry of the $X, Y$ basis in Eq. (2), we treat the parameters of the two bases equivalently for simplicity. Accordingly, $\Pr_X^Y = \Pr_X^X = \Pr_Y^Y = \Pr_Y^X$, expect for $\Pr_Y^X = 0$ as Alice sent three states to Bob. According to the experiment system, we set $\omega = 0$ to be a vacuum state. For purposes of comparison, the secret key rates in the asymptotic case are simulated as shown in Fig. 3(b), and the secret key rates for the BB84 protocol are also depicted in Fig. 3 by using the blue solid line and the blue dotted line. In the finite-key case for the BB84 protocol, we adopt the formula proposed in Ref. \cite{41} to estimate its secret key rates. For the RFI QKD protocol, the achieved key rates will be the lowest in the finite-key case at $\beta = \pi/4$, which can be explained by poor estimation of $C$ with the increase of $\beta$. It is evident that the secret key rates of the RFI QKD protocol are still an order of magnitude higher compared with that of the BB84 protocol at $\beta = \pi/4$. For the case where Alice only sends three states, the phase error rates $e_{XX}$ and $e_{XY}$ can be estimated according to Eq. (17), and they are then taken into SDP approach to get the value of $C_L$. We show that the secret key rate and the transmission distance are comparable with that of the original six states RFI QKD protocol, which verify the feasibility of our scheme in the real-world applications.

FIG. 3. (Color online) Secret key rate vs. transmission distances when the weak coherent source is used. (a) Considering the statistical fluctuations due to the finite-size pulses, numerically optimized secret key rates against coherent attacks are obtained for a fixed postprocessing block size $N = 10^{10}$. The dot symbols are the experimental results when Alice sends three states to Bob, and the triangle markers are the results for the four-states protocol. The green color and the red color respectively represent $\beta = 0$ and $\beta = \pi/4$. (b) The secret key rates in the asymptotic case, i.e., in the limit of infinitely large keys.

Applying the method proposed in Ref. \cite{41}, the number of vacuum events in $Z_A$ satisfies

$$s_{zz,0} \geq \max \left\{ \frac{(\nu n_{zz,\omega} - \omega n_{zz,\nu})}{\nu - \omega}, 0 \right\}, \quad (12)$$

where $\tau_n := \sum_{k \in \mathcal{K}} e^{-k} k^n p_k/n!$ is the probability that Alice sends a $n$-photon state, and

$$n_{zz,k}^\pm := \max \left\{ \frac{e_k}{p_k} \left( n_{zz,k} \pm \sqrt{\frac{n_{zz,k}}{2} \ln \frac{1}{\varepsilon}} \right), 0 \right\}. \quad (13)$$
IV. EXPERIMENTAL SETUP AND RESULTS

To demonstrate the application of our scheme to a real QKD system, we proceed a proof-of-principle experiment using time-bin encoding, as shown in Fig. 4. The light pulses generated by Alice’s coherent light source (1550 nm) are randomly modulated into two intensities of decoy states using an intensity modulator (IM1). The vacuum state is generated by stopping the trigger on the laser. Then, the quantum states of photons are modulated by an asymmetric Mach-Zehnder interferometer (AMZ1) together with IM2 according to the coding information. For an asymmetric Mach-Zehnder interferometer (AMZ1) to simulate the change of the reference frame, the relative phase, 0 or $\pi/2$ needs to modulate in the $X$ basis measurement, and $\pi/2$ needs to modulate in the $Y$ basis measurement. As expected, it is seen that the secret key rates are almost identical for the four-states and three-states scheme at the transmission distance of 15 km.

In summary, we propose an efficient scheme to realize the RFI QKD by using only three states, which is identical to the BB84 protocol. Furthermore, the secret key rates and the transmission distance are comparable to the original RFI QKD protocol. Experiments considering the finite-key analysis are demonstrated at the transmission distance of 15 km and 55 km. Our scheme is also suitable to the free-space RFI QKD systems, and can be upgraded to the RFI measurement-device-independent (MDI) QKD protocol and high-dimension RFI QKD protocol with simple modifica-
TABLE I. Implementation parameters and experimental results.

| Protocol | β | Parameters | Estimation | Performance |
|----------|---|------------|------------|-------------|
|          |   | µ  ν  pµ  pν  Pr\text{\textgreek{A}}  s_{zz,0}  s_{zz,1}  e_{XX}  e_{XY}  C_L  E_{ZZ}  R |
| 15 km 7.95 dB |
| Four 0 | 0.59 0.26 0.59 0.32 0.89 0 1.78 × 10^7 | 0.83% 4.60% 50% 1.68 0.44% 1.16 × 10^{-3} |
| Three 0 | 0.58 0.25 0.60 0.31 0.90 0 1.97 × 10^7 | 0.72% 2.62% 50% 1.77 0.42% 1.42 × 10^{-3} |
| Four π/4 | 0.47 0.14 0.43 0.39 0.79 2.18 × 10^4 | 1.07 × 10^7 0.97% 20.74% 21.15% 1.33 0.61% 4.88 × 10^{-4} |
| Three π/4 | 0.44 0.12 0.44 0.39 0.78 1.83 × 10^4 | 1.00 × 10^7 0.70% 20.39% 19.44% 1.42 0.63% 5.00 × 10^{-4} |
| 55 km 16.35 dB |
| Four 0 | 0.59 0.28 0.36 0.48 0.82 4.88 × 10^4 | 2.21 × 10^6 2.08% 6.21% 50% 1.50 1.89% 8.48 × 10^{-5} |
| Three 0 | 0.55 0.28 0.38 0.42 0.81 7.47 × 10^4 | 2.00 × 10^6 1.85% 8.20% 50% 1.34 2.30% 5.02 × 10^{-5} |
| Four π/4 | 0.43 0.15 0.22 0.47 0.62 5.50 × 10^4 | 7.25 × 10^5 1.32% 23.36% 23.41% 1.13 3.90% 8.36 × 10^{-6} |
| Three π/4 | 0.39 0.12 0.23 0.45 0.59 5.20 × 10^4 | 5.40 × 10^5 1.71% 21.76% 21.56% 1.23 4.25% 4.98 × 10^{-6} |

tions to the setup, thereby reducing the complexity of these systems.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (NSFC) (11674397), and the Fund of State Key Laboratory of Information Photonics and Optical Communications (Beijing University of Posts and Telecommunications) (No. IPOC2017ZT04), P. R. China.

Appendix A: Explicit calculation for \(C_L\)

The estimation of lower bound of \(C\) can be turned into an optimization framework [36]. In an equivalent entanglement distillation version, Alice prepares an entangled state of the form

\[
|\phi\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B),
\]

where she chooses one of photons to measure either in \(\{\sigma_X^A, \sigma_Y^A, \sigma_Z^A\}\), the other one is then sent to Bob, who chooses to measure in \(\{\sigma_X^B, \sigma_Y^B, \sigma_Z^B\}\). According to Eq. (2), the optimization problem is

\[
\text{minimize} : C_L = \sum_{\kappa, \zeta} \text{Tr} (\sigma_\kappa^A \otimes \sigma_\zeta^B \rho_{AB})^2,
\]

where \(\forall \{\kappa, \zeta\} \in \{X, Y\}\). We are allowing \(\rho_{AB}\) to be arbitrary, which implies that Eve can perform any arbitrary operations on the states transmitted between Alice and Bob, and hence the bound is valid for any collective attacks.

Based on Eq. (1), the error operator in the \(Z\) basis is given by

\[
\hat{\nu}_{ZZ} = \frac{1}{2} (I \otimes I - \sigma_Z^A \otimes \sigma_Z^B).
\]

Except for the case when Alice use the \(Y\) basis to prepare her states, the probabilities \(P_{\alpha,\chi_i}\) can be simulated by

\[
P_{\alpha,\chi_i} \equiv \frac{1}{2} \left( \langle \alpha^A_i | \chi_j^B \rangle^2 + e_\alpha \langle \chi_j^A | \chi_j^B \rangle^2 \right),
\]

where \(\alpha \in \{X, Z\}\), \(\chi \in \{X, Y, Z\}\), and the symbol \(\oplus\) denotes the modulo two addition. The factor 1/2 is the conditional probability that the state \(|\alpha_i^A\rangle\) is sent, given that it is prepared in \(\alpha\) basis. \(e_\alpha\) is the bit-flip rate of state \(|\alpha_i^A\rangle\), which is caused by the channel noise along the transmission. In Eq. (A4), the first (second) term models the probability that Bob detects a state \(|\chi_j^B\rangle\) after he received a state \(|\alpha_i^A\rangle\) sent from Alice.

Due to \(\langle \sigma_Y \otimes \sigma_Y \rangle = -1\) for the state \(|\phi\rangle_{AB}\), Alice actually sends Bob a state \(|\chi_j^B\rangle\) after she got a state \(|\chi_j^B\rangle\) in the equivalent entanglement-based protocol. Thus, the \(P_{Y,\chi_i}\), when Alice sends states in \(Y\) basis, should be given by

\[
P_{Y,\chi_i} = \frac{1}{2} \left( e_\gamma \langle \chi_j^A | \chi_j^B \rangle^2 + (1 - e_\gamma) \langle \chi_j^A | \chi_j^B \rangle^2 \right).
\]

The QBERs \(e_{ZZ}, e_{XX}, e_{XY}, e_{YY}\), and \(e_{YY}\) can be extracted from the experiment, but not all of them equal to the corresponding bit-flip error rate as \(\beta \neq 0\). Here, we assume that they are all less than 0.5 (if not, Bob can simply flip his bits). For the convenience of experiment and simulation, we list the probabilities \(P_{\alpha,\chi_i}\) in detail.
as follows:

\[
P_{Z,i,j} = \frac{1}{4} \quad P_{\alpha_i,z_j} = \frac{1}{4};
\]

\[
P_{X,i,i} = \frac{1}{4} \left[ 1 + \cos \beta \left( 1 - 2e_x \right) \right] = \frac{1}{2} \left( 1 - e_{XX} \right);
\]

\[
P_{X,i,i} = \frac{1}{4} \left[ 1 - \sin \beta \left( 1 - 2e_x \right) \right] = \frac{1}{2} e_{XY};
\]

\[
P_{Y,i,i} = \frac{1}{4} \left[ 1 - \cos \beta \left( 1 - 2e_y \right) \right] = \frac{1}{2} e_{YY};
\]

\[
P_{Y,i,i} = \frac{1}{4} \left[ 1 - \sin \beta \left( 1 - 2e_y \right) \right] = \frac{1}{2} e_{XY}; \quad (A6)
\]

\[
P_{X,i,j \neq i} = \frac{1}{4} \left[ 1 - \cos \beta \left( 1 - 2e_x \right) \right] = \frac{1}{2} e_{XY};
\]

\[
P_{X,i,j \neq i} = \frac{1}{4} \left[ 1 + \sin \beta \left( 1 - 2e_x \right) \right] = \frac{1}{2} \left( 1 - e_{XX} \right);
\]

\[
P_{Y,i,j \neq i} = \frac{1}{4} \left[ 1 + \cos \beta \left( 1 - 2e_y \right) \right] = \frac{1}{2} \left( 1 - e_{YY} \right);
\]

\[
P_{Y,i,j \neq i} = \frac{1}{4} \left[ 1 + \sin \beta \left( 1 - 2e_y \right) \right] = \frac{1}{2} \left( 1 - e_{XY} \right).
\]

When the RFI QKD protocol with three states is applied, the fictitious bit error rates \(e_{XY}\) and \(e_{YY}\) can also be well bounded using the following optimization problem:

\[
\text{maximize : } e_{XY} = \text{Tr} \left( \hat{E}_{XY} \rho_{AB} \right); \quad (A7)
\]

\[
\text{maximize : } e_{YY} = \text{Tr} \left( \hat{E}_{YY} \rho_{AB} \right),
\]

where

\[
\hat{E}_{XY} = \frac{1}{2} \left( \mathbb{1} \otimes \sigma^A_Y \otimes \sigma^B_X \right),
\]

\[
\hat{E}_{YY} = \frac{1}{2} \left( \mathbb{1} \otimes \sigma^A_Y \otimes \sigma^B_Y \right). \quad (A8)
\]

In Fig. 5 we show the dependence of \(e_{XY}\) and \(e_{YY}\) on \(e_{ZZ}\) when Alice transmits different states at \(\beta = 0\) (solid lines) and \(\beta = \pi/4\) (dashed lines). In simulations, it is noted that we treat the bit-flip rates in different bases equivalently for simplicity, i.e., \(e_z = e_x = e_y = e_{ZZ} \). It is evident that for sending six and four states at \(\beta = 0\), \(e_{ZZ} = e_{XY} \) and \(e_{XY} = 0.5\), as respectively indicated by the red solid line and black solid line. This is expected for RFI QKD protocol when no misalignment of reference frame occurs. However, the phase error rate \(e_{YY}\) and \(e_{YY}\) increase faster when Alice sends three states, resulting in lower \(C_L\) as shown in Fig. 4(a) and lower error tolerance as shown in Fig. 4(b).

**Appendix B: Channel model**

1. **For the single-photon source**

We consider the channel model proposed by Ref. 32–35, where the conditional probability that Bob obtain \(j\) when he chooses \(\chi\) basis for measurement given that Alice sent him the state \(|\alpha_i\rangle\) can be written as

\[
V_{X_j|\alpha_i} = \eta T_{X_j|\alpha_i} (1 - e_d) + (1 - \eta) e_{d} (1 - e_d) + \frac{1}{2} \left( \eta e_d + (1 - \eta) e_{d}^2 \right), \quad (B1)
\]

where \(e_d\) is the dark count rate of SPD and \(\eta\) denotes the total transmittance of the system. The term \(T_{X_j|\alpha_i}\) is the theoretical probability that Bob measures the state \(|\alpha_i\rangle\) and obtains the bit value \(j\) when he chooses \(\chi\) basis. It is calculated by

\[
T_{X_j|\alpha_i} = |\langle \alpha_i | \chi_j \rangle|^2. \quad (B2)
\]

Then the single-photon gain and the QBER are given by, respectively,

\[
Q^1_{\alpha_i} = \frac{1}{2} \left( V_{X_0|\alpha_0} + V_{X_1|\alpha_1} + V_{X_1|\alpha_0} + V_{X_0|\alpha_1} \right), \quad (B3)
\]

\[
E^1_{\alpha_i} = \min \left[ \hat{E}^1_{\alpha_i}, 1 - \hat{E}^1_{\alpha_i} \right],
\]

where

\[
\hat{E}^1_{\alpha_i} = e_o (1 - 2e^1_{\alpha_i}) + e^1_{\alpha_i},
\]

\[
e^1_{\alpha_i} = \frac{V_{X_1|\alpha_0} + V_{X_0|\alpha_1}}{2Q^1_{\alpha_i}}. \quad (B4)
\]

The factor 1/2 in Eq. (B3) denotes the probability of Alice preparing quantum states \(|\alpha_0\rangle\) or \(|\alpha_1\rangle\), and \(e_o\) in Eq. (B4) is the optical intrinsic error rate \(15, 36, \). For simplicity, we assume \(E^1_{\alpha_i} \leq 0.5\) in Eq. (B3), if not, either Alice or Bob flips her or his bit strings to make it hold.

2. **For the WCS with decoy technique**

In this case, according to the decoy state method \(35, \) the overall gain, given that Alice sends a state \(|\alpha_i\rangle\) using \(k \in K\) intensity and Bob obtains a state \(|\chi_j\rangle\), can be
written as

\[ Q_{k,\alpha,\chi} = \sum_{n=0}^{\infty} \frac{Y_n e^{-k}}{m!} \]

\[ = \frac{1}{2} \left\{ 1 + D \left[ e^{(-\eta + a)k} - e^{-ak} - De^{-\eta k} \right] \right\}, \quad (B5) \]

where we use the notations

\[ a = \eta T_{\chi_j|\alpha}, D = 1 - e_d. \quad (B6) \]

According to the above formula, we can obtain the overall gain, the overall error gain, and the average of observed error rate in the \( \alpha \) basis. They are given by, respectively

\[ Q^k_{\alpha} = \frac{1}{2} \left( Q_{k,0,\chi_0} + Q_{k,1,\chi_1} + Q_{k,0,\chi_0} \right), \]

\[ W^k_{\alpha} = e_d \left( Q^k_{\alpha} - 2W^k_{\alpha} \right) + \tilde{W}^k_{\alpha}, \]

\[ E^k_{\alpha} = \min \left\{ E^k_{\alpha} - 1 - \tilde{E}^k_{\alpha} \right\}, \quad (B7) \]

Thus, the overall number of detected pulses and the overall number of bit errors for all intensity levels are

\[ n_{\alpha, \chi} = \sum_{k \in K} n_{\alpha, \chi, k}, \]

\[ m_{\alpha, \chi} = \sum_{k \in K} m_{\alpha, \chi, k}. \quad (B10) \]

where

\[ \tilde{W}^k_{\alpha} = \frac{1}{2} \left( Q_{k,0,\chi_0} + Q_{k,0,\chi_1} \right), \]

\[ \tilde{E}^k_{\alpha} = W^k_{\alpha} / Q^k_{\alpha}. \quad (B8) \]

Considering the probabilities that Alice prepares her state in the \( \alpha \) basis, \( \Pr^A_{\chi} \), its mean photon number \( k \), \( p_k \), and Bob measures this state in the \( \chi \) basis, \( \Pr^B_{\chi} \), we can calculate the number of detected pulses, \( n_{\alpha, \chi, k} \), and the number of bit errors, \( m_{\alpha, \chi, k} \), when Alice prepares her state in the \( \alpha \) basis with intensity \( k \) and Bob measures it in the \( \chi \) basis. They are given by

\[ n_{\alpha, \chi, k} = N p_k \frac{\Pr^B_{\chi}}{\Pr^A_{\chi}} Q^k_{\alpha}, \]

\[ m_{\alpha, \chi, k} = N p_k \frac{\Pr^B_{\chi}}{\Pr^A_{\chi}} W^k_{\alpha}. \quad (B9) \]

[1] C. E. Shannon, Communication theory of secrecy systems, Bell System Tech. J 28 (1949).
[2] C. H. Bennett and G. Brassard, in Proc. 1984 IEEE International Conference on Computers, Systems, and Signal Processing (1984) pp. 175–179.
[3] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[4] H.-K. Lo and H. F. Chau, Science 283, 2050 (1999).
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
[6] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. 92, 057901 (2004).
[7] X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
[8] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
[9] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature 509, 475 (2014).
[10] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tan, Z. Yuan, R. V. Penty, and A. Shields, Nat. Photon. 10, 312 (2016).
[11] S. Wang, W. Chen, Z.-Q. Yin, D.-Y. He, C. Hui, P.-L. Hao, G.-J. Fan-Yuan, C. Wang, L.-J. Zhang, J. Kuang, S.-F. Liu, Z. Zhou, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, Opt. Lett. 43, 2030 (2018).
[12] For instance, QuantumCTek: http://www.quantum-info.com/ Qasky: http://www.qasky.com/ ID Quantique: http://www.idquantique.com/ MagiQ: http://www.magiqtech.com/
[13] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, Opt. Express 19, 10387 (2011).
[14] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Phys. Rev. X 6, 011024 (2016).
[15] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. 105, 070501 (2010).
[16] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. 108, 130502 (2012).
[17] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
[18] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, J. Lightwave Technol. 36, 3427 (2018).
[19] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. 117, 190501 (2016).
[20] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Nature 557, 400 (2018).
[21] X. Ma, P. Zeng, and H. Zhou, Phys. Rev. X 8, 031043 (2018).
[22] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. 107, 110501 (2011).
[23] A. Laing, V. Scarani, J. G. Rarity, and J. L. O’Brien,
[24] Z.-Q. Yin, S. Wang, W. Chen, H.-W. Li, G.-C. Guo, and Z.-F. Han, Quant. Info. Proc. 13, 1237 (2014).
[25] J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. O’Brien, and A. O. Niskanen, New J. Phys. 15, 073001 (2013).
[26] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. W. Nock, J. Munns, D. Bonneau, P. Jiang, H. W. Li, A. Laing, J. G. Rarity, A. O. Niskanen, M. G. Thompson, and J. L. O’Brien, Phys. Rev. Lett. 112, 130501 (2014).
[27] W.-Y. Liang, S. Wang, H.-W. Li, Z.-Q. Yin, W. Chen, Y. Yao, J.-Z. Huang, G.-C. Guo, and Z.-F. Han, Sci. Rep. 4, 3617 (2014).
[28] F. Wang, P. Zhang, X. Wang, and F. Li, Phys. Rev. A 94, 062330 (2016).
[29] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Phys. Rev. Lett. 115, 160502 (2015).
[30] H. Liu, J. Wang, H. Ma, and S. Sun, Optica 5, 902 (2018).
[31] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Optica 4, 1016 (2017).
[32] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A 90, 052314 (2014).
[33] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, Phys. Rev. A 92, 032305 (2015).
[34] Z. Tang, K. Wei, O. Bedroya, L. Qian, and H.-K. Lo, Phys. Rev. A 93, 042308 (2016).
[35] C. Wang, S.-H. Sun, X.-C. Ma, G.-Z. Tang, and L.-M. Liang, Phys. Rev. A 92, 042319 (2015).
[36] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Phys. Rev. A 97, 042347 (2018).
[37] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A 72, 012332 (2005).
[38] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Nature communications 7, 11712 (2016).
[39] M. Grant and S. Boyd, “CVX: Matlab software for disciplined convex programming, version 2.1,” http://cvxr.com/cvx (2014).
[40] M. Grant and S. Boyd, in Recent Advances in Learning and Control, Lecture Notes in Control and Information Sciences, edited by V. Blondel, S. Boyd, and H. Kimura (Springer-Verlag Limited, 2008) pp. 95–110, http://stanford.edu/~boyd/graph_dcp.html.
[41] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A 89, 022307 (2014).
[42] L. Sheridan, T. P. Le, and V. Scarani, New J. Phys. 12, 123019 (2010).
[43] C.-M. Zhang, J.-R. Zhu, and Q. Wang, J. Lightwave Technol. 35, 4574 (2017).
[44] H. F. Chau, Phys. Rev. A 97, 040301 (2018).
[45] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A 86, 052305 (2012).
[46] F. Xu, H. Xu, and H.-K. Lo, Phys. Rev. A 89, 052333 (2014).