

## Practical Long-Distance Side-Channel-Free Quantum Key Distribution

Xiang-Bin Wang<sup>1,2,4,5,\*</sup>, Xiao-Long Hu,<sup>1</sup> and Zong-Wen Yu<sup>3</sup>


<sup>1</sup>*State Key Laboratory of Low-Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China*

<sup>2</sup>*Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

<sup>3</sup>*Data Communication Science and Technology Research Institute, Beijing 100191, China*

<sup>4</sup>*Jinan Institute of Quantum technology, SAICT, Jinan 250101, People's Republic of China*

<sup>5</sup>*Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, China*

 (Received 5 June 2018; revised manuscript received 16 August 2019; published 14 November 2019)

We present a simple protocol for which Alice and Bob must only decide to either send out a coherent state or not send out a coherent state to Charlie. No switching of bases occurs. We demonstrate that this protocol is both source-state side-channel free and measurement-device independent. We do not have to exactly control the whole space of the state of the light pulse, which is an impossible task in practice. The protocol is immune to all adverse effects caused by quantum-state imperfections in the side-channel space, such as the photon frequency spectrum, emission time, propagation direction, spatial angular momentum, and so on. Numerical simulation shows that our scheme can reach a side-channel-free result for quantum key distribution over distances exceeding 200 km, given the single-photon interference-misalignment error rate of 20%.

DOI: [10.1103/PhysRevApplied.12.054034](https://doi.org/10.1103/PhysRevApplied.12.054034)

### I. INTRODUCTION

Guaranteed by the principles of quantum mechanics, quantum key distribution (QKD) can provide secure keys for private communication [1–5], even though Eve can completely control the channel. However, in practice, side-channel effects exist due to device imperfections [6–26]. In general, we can divide the whole space of an encoding state from a real source into two subspaces: the operational space and side-channel space. Even though the encoding state of the source appears perfect when it is examined in the operational space, there could be security loopholes because of imperfections in the side-channel space. This issue is what we call a side-channel effect. For example, in the BB84 protocol [1], even though a perfect single-photon source is applied, there are still some side-channel effects, which can undermine the security assumed in the operational space. There could be basis-dependent synchronization errors in the pulse emitting time or the frequency-spectrum difference for different encoding states or bases and Eve can make use of this to judge the basis or encoding state chosen by the legitimate users in a certain time window. In general, all encoding states from the source live in an infinite-dimensional space

formed by the operational space and side-channel space. Though we only use the encoding space (e.g., polarization) for QKD, Eve can attack in the side-channel space (such as the frequency space) to obtain information. As we demonstrate later, given the inevitable imperfections in the side-channel space for encoding states, Eve can exploit these imperfections and obtain information without disturbing the encoding states in the operational space. Here, we propose a QKD scheme that is both source-state side-channel free and measurement-device independent (MDI) [27–39]. The recently proposed twin-field QKD (TF QKD) [40] can generate secure keys at a long distance and is MDI, but it is not side-channel free. Although some existing protocols can also achieve side-channel-free security [27,41–44], our protocol is the only one based on existing mature technologies without any demand for local detection efficiency.

Our protocol is immune to all attacks in the side-channel space of emitted photons, such as the frequency spectrum, emission time, nonideal propagation direction, and so on. However, our protocol is *not* source-device independent. First, we assume that Eve has no access inside Alice's (Bob's) laboratory. This means that we do not discuss any Trojan-horse attack on the source here. Second, we assume that Alice and Bob can control their light pulses *exactly in their operationally space*, though we allow any

\*xbwang@mail.tsinghua.edu.cn

imperfection in any side-channel space for the quantum states emitted from the source device. Later, we show that, actually, we even do not need exact control of the intensities of the coherent states. What we need is the exact vacuum only. This being said, calibrating only one quantity in the simple operational space is much easier than conducting calibrations in the whole space with infinite quantities. Ideally, the condition on the operational space can be loosened in the future, as there are already many studies on security with inexact encoding states [18–20,45] in the operational space. Since our protocol is measurement-device independent, there is no condition on measurement devices for security. The security of our protocol is obviously stronger than that of normal MDI QKD because in our protocol there is no security loophole in the side-channel space of the quantum states emitted from the source. Note that device-independent QKD is not measurement-device independent, as it requests no information leakage of the measurement outcome. Most importantly, our protocol only relies on existing mature technologies and can achieve a secure distance beyond 200 km, even though the misalignment error rate is as large as 20%.

## II. SOME SIDE-CHANNEL ATTACKS AND THEOREM 1

Consider a two-basis QKD protocol, such as the BB84 protocol, where there exists an  $X$  basis and a  $Z$  basis in the protocol. Suppose that we take state encoding in the photon polarization space and regard the polarization space as the operational space. The polarization modulation can cause differences in the side-channel space. For example, the frequency spectra can be slightly varied for different encoding states or bases. In principle, by detecting the frequency difference, Eve has a chance of knowing which encoding state is being used in the operational space and will hence cause no change to the states in the operational space. As another example, if different encoding states are actually emitted at different times, Eve may just measure the photon with a very precise clock and can sometimes derive the coding state almost exactly if the photon wave packet collapses at certain time intervals. Also, Eve may make use of the channel loss and choose to block all the attacked photons on the side channel if the attack is not successful. Thus, the small bias of a state in the side-channel space may generate a flaw in the whole protocol.

Fortunately, the ideal source is not the only secure source. A real-life source is secure if it can be mapped from an ideal source. Suppose that a certain protocol  $\mathcal{K}$  requests  $k$  different encoding states. For example, in the BB84 protocol, we need four encoding states. The perfect source,  $\mathcal{P}$ , always produces a perfect encoding state in every time window and all states are identical in the side-channel space. An imperfect source produces nonideal

encoding states in the whole space, with imperfections in the side-channel space, and the states in the side-channel space can change intermittently. Say, in a certain time window  $i$ , that the imperfect source produces  $k$  encoding states in the whole space and that we call them set  $\mathcal{S}_i$ . We then randomly choose one from  $\mathcal{S}_i$  and send it out for QKD. If there always exists a (time-dependent) quantum process,  $\mathcal{M}_i$ , that maps the  $k$  perfect states to the corresponding  $k$  nonideal states in set  $\mathcal{S}_i$ , then we declare that source  $\mathcal{S}_i$  can be mapped from a perfect source  $\mathcal{P}$ .

**Theorem 1:** In any QKD protocol, a real-life source,  $\mathcal{S}$ , emitting imperfect states in the whole space is equivalent to a perfect (virtual) source,  $\mathcal{P}$ , emitting perfect states, all of which are identical in the side-channel space if there exists a quantum process,  $\mathcal{M}$ , that can map source  $\mathcal{P}$  to source  $\mathcal{S}$ . The final key of a QKD protocol using source  $\mathcal{S}$  can be calculated by assuming that the virtual source,  $\mathcal{P}$ , is used.

**Proof:** Suppose that  $\mathcal{S}$  is insecure; then in a QKD protocol where the ideal source,  $\mathcal{P}$ , is applied, Eve can first use the quantum process  $\mathcal{M}$  to transform it into source  $\mathcal{S}$  and then attack the QKD protocol as if the protocol used source  $\mathcal{S}$ . This means that if  $\mathcal{S}$  is not secure, then  $\mathcal{P}$  is also not secure. In our Theorem 1, the quantum process,  $\mathcal{M}$ , is not limited to a unitary process, although in showing the side-channel-free property of our protocol, we primarily employ a unitary map. ■

## III. OUR PROTOCOL

We adopt the sending-or-not-sending (SNS) protocol [46] of twin-field QKD (TF QKD), which has recently been studied extensively [47–50]. A schematic illustration of side-channel-free QKD is shown in Fig. 1. Our protocol differs from that used in Ref. [46] in that we directly use the whole nonrandom-phase coherent states. There are three parties: Alice, Bob, and the third party, Charlie [40]. They (Alice and Bob) will use coherent states and vacuum only. We first present our protocol in the operational space

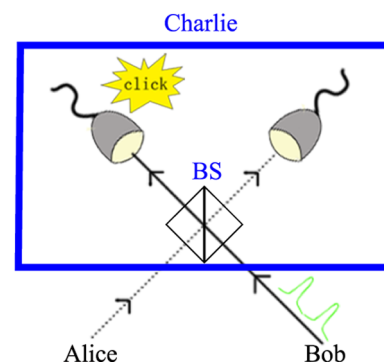


FIG. 1. A schematic illustration of side-channel-free QKD. BS: beam-splitter.

only and then demonstrate why it is side-channel free using our Theorem 1.

Protocol R, real protocol.

R-1 In any time window  $i$ , Alice (Bob) always prepares a coherent state  $|\alpha_A\rangle = \sum_{n=0}^{\infty} e^{-\mu/2} \mu^{n/2} e^{i n \gamma_A} / \sqrt{n!}$  ( $|\alpha_B\rangle = \sum_{n=0}^{\infty} e^{-\mu/2} \mu^{n/2} e^{i n \gamma_B} / \sqrt{n!}$ ) and announces the state, including the global phase  $\gamma_A$  ( $\gamma_B$ ). (In this paper, we denote the imaginary unit as  $i$ .) With probability  $q$ , Alice (Bob) decides on *sending*, and with probability  $1 - q$ , she (he) decides on *not-sending*. If she (he) decides on *sending*, she (he) sends out the coherent state  $|\alpha_A\rangle$  ( $|\alpha_B\rangle$ ) to Charlie and puts down a classical bit value 1 (0) locally; if she (he) decides on *not sending*, she (he) does not send out anything, i.e., she (he) sends out a vacuum to Charlie and puts down a classical bit value 0 (1) locally.

R-2 Charlie announces his measurement outcome and hence determines the *effective events*, i.e., the events with one and only one detector clicking as announced by Charlie. A time window or a classical bit value corresponding to an effective event is called an effective time window or an effective bit.

*Definition.*— $\tilde{Z}$  window: A time window when Alice decides on *sending* and Bob decides on *not sending*, or Alice decides on *not sending* and Bob decides on *sending*.

R-3 Through classical communication, *they* take a random subset of time windows,  $v$ , to test the bit-flip error rate. *They* take another random subset of time windows,  $u$ . Using the observed data of set  $v$ , *they* can estimate the bound values of quantities in set  $u$  to obtain the upper bound of phase-flip error rate  $\bar{e}^{\text{ph}}$  for bits of effective  $\tilde{Z}$  windows. *They* discard effective bits from the sets  $v$  and  $u$  after the error test.

R-4 *They* distill (by conducting error correction and privacy amplification) the remaining effective bits after the error test, with the following asymptotic result for the number of final bits:

$$n_F = n_{\tilde{Z}} - n_{\tilde{Z}} H(\bar{e}^{\text{ph}}) - f n_t H(E_Z), \quad (1)$$

where  $H(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$  is the entropy function;  $n_{\tilde{Z}}$  ( $n_t$ ) is the number of remaining effective bits from the  $\tilde{Z}$  windows (all time windows) after the error test;  $f$  is the correction efficiency factor;  $E_Z$  is the bit-flip error rate of the remaining effective bits from the  $Z$  windows as noted in Note 2 and Eq. (13); and  $\bar{e}^{\text{ph}}$  is the phase-flip error rate as noted in Note 2 and Eq. (14).

*Note 1:* The encoding is performed by decisions of *sending* or *not sending* made by Alice and Bob. More precisely, the *sending* or *not-sending* decision of a time window always corresponds to the local classical bits 1 to Alice and 0 to Bob, or 0 to Alice and 1 to Bob. We can also imagine that whenever Alice (Bob) decides on *sending* or *not sending*, she (he) always produces a local ancillary-photon-number state of  $|1\rangle$  or  $|0\rangle$  in which the corresponding bit value is encoded. To Alice (Bob), state

$|0\rangle$  corresponds to a bit value 0 (1) and state  $|1\rangle$  corresponds to a bit value 1 (0). In other words, *they* (Alice and Bob) have used an extended state including the real-photon state and the ancillary state. The real-photon state will be sent out to Charlie and the ancillary state will be placed locally with Alice and Bob. For example, in a certain window when Alice decides on *sending* and Bob decides on *not sending*, we can imagine that *they* have actually prepared an extended state

$$(\rho_A \tilde{\otimes} |0\rangle\langle 0|) \otimes |10\rangle\langle 10|, \quad (2)$$

where  $\rho_A = |\alpha_A\rangle\langle\alpha_A|$ . Here, both symbols  $\tilde{\otimes}$  and  $\otimes$  are for tensor products and  $\tilde{\otimes}$  is the tensor product in the two-mode state sent by Alice and Bob. In this paper, we call the state to the left of the tensor-product symbol  $\otimes$  the real-photon state and the state to the right of the tensor-product symbol  $\otimes$  the ancillary-photon state. According to the above definitions,  $\rho_A \tilde{\otimes} |0\rangle\langle 0|$  is the two-mode real-photon state sent out to Charlie. As previously mentioned, each bit value is actually encoded in the local ancillary-photon-number state.

*Note 2:* The bit-flip error and the phase-flip error. Bob has a bit-flip error whenever his bit value is different from Alice's bit value in a certain time window. For every event in the subset  $v$  randomly taken by *them*, *they* announce each corresponding bit value (decision on *sending* or *not sending*) to judge the bit-flip error rate. Also, as elaborated in Sec. V, using the details of events in set  $v$ , *they* can estimate faithfully some bound values of set  $u$  and therefore calculate the upper bound of the phase-flip error rate,  $\bar{e}^{\text{ph}}$ , using Eq. (14).

*Note 3:* Charlie's compensation. To obtain a satisfied key rate, *they* need a low phase-flip error rate. In the protocol, an event of right-detector clicking due to the real-photon state  $|\alpha_A\rangle \tilde{\otimes} |\alpha_B\rangle = |\sqrt{\mu} e^{i \gamma_A}\rangle \tilde{\otimes} |\sqrt{\mu} e^{i \gamma_B}\rangle$  will contribute to the phase-flip errors. Since the states  $|\alpha_A\rangle$  and  $|\alpha_B\rangle$  are publicly announced, Charlie can perform compensation to remove the global phases  $\gamma_A$  and  $\gamma_B$  in the states, so that the clicking detector is very unlikely to be the right detector given the real-photon state  $|\alpha_A\rangle \otimes |\alpha_B\rangle$ . Very importantly, as elucidated in our security proof, although Charlie's collaboration can lead to a high key rate, the security of the protocol does not rely on Charlie's honesty. Charlie's role in the protocol is simply a quantum relay, i.e., a memoryless quantum repeater.

*Note 4:* Why is the protocol side-channel free? Intuitively speaking, our protocol does not require switching of physical bases. Other protocols, such as the BB84 protocol, the MDI QKD protocol, the TF QKD protocol, and so on, all need to modulate the states differently by switching between different bases. We can give a strict proof for the side-channel-free property of our protocol. Using Theorem 1, we can show that the protocol R is side-channel free; in other words, if it is secure in the operational

space, it must be also secure in the whole space, including the side-channel space. Later, in Sec. V, we present the measurement-device-independent security proof of the protocol in the operational space only, i.e., in the case in which we do not consider any side-channel effects. Here, we must only demonstrate that the protocol is encoding-state side-channel free. In step R-1, *they* try to prepare coherent states  $|\alpha_A\rangle$  and  $|\alpha_B\rangle$  in the operational space. In the ideal case, we do not need to consider the side-channel space; for example, in the case in which any Fock state  $|n\rangle$ , no matter if it is from Alice's state  $|\alpha_A\rangle$  or from Bob's state  $|\alpha_B\rangle$ , is identical to another in the side-channel space. Hence, we just use the original notations of  $|\alpha_A\rangle$  and  $|\alpha_B\rangle$  to represent the *ideal whole-space state*. However, what is actually prepared in a real experiment must have imperfections in the side-channel space. Yet *the vacuum state has no side-channel space* and therefore we only need to consider the side-channel space for the nonvacuum parts in each coherent state; say,  $|\alpha_x\rangle = e^{-\mu/2}|0\rangle + \sqrt{1 - e^{-\mu}}|\tilde{\alpha}_x\rangle$  and  $\sqrt{1 - e^{-\mu}}|\tilde{\alpha}_x\rangle = |\alpha_x\rangle - e^{-\mu/2}|0\rangle$ , where  $x$  can be  $A, B$ . We must only consider the whole-space state of  $|\tilde{\alpha}_x\rangle$ . Therefore, instead of the ideal states, we need to consider the corresponding whole-space states in the following form:

$$\begin{aligned} |0\rangle &\longrightarrow |0\rangle, \\ |\alpha_A\rangle &\longrightarrow e^{-\mu/2}|0\rangle + \sqrt{1 - e^{-\mu}}|\psi_A(\tilde{\alpha}_A)\rangle, \\ |\alpha_B\rangle &\longrightarrow e^{-\mu/2}|0\rangle + \sqrt{1 - e^{-\mu}}|\psi_B(\tilde{\alpha}_B)\rangle. \end{aligned} \quad (3)$$

Here, the states to the left of the arrow are the ideal states and the states to the right of the arrow are the corresponding real-life states. States  $|\psi_A(\tilde{\alpha}_A)\rangle$  and  $|\psi_B(\tilde{\alpha}_B)\rangle$  contain the side-channel information, such as the frequency spectrum, polarization, wave shape, emission time, and so on. *We assume that Eve knows all of this information exactly.* Therefore, Eve knows all the details of the states in the whole space and can write down the whole-space states exactly, to make use of in whatever way she likes. However, consider the form of Eq. (3); it is obvious that there exists a unitary operation that can relate the ideal states and the whole-space states used in the protocol. Note that here we do not assume errors in the operational space. This means that when we assume a nonideal whole-space state, it must be able to present the same result in the operational space as in the ideal state. Say that for state  $|\psi_A(\tilde{\alpha}_A)\rangle$ , if it is measured in the photon-number space, the state can only present the same probability distribution,  $P_n$ , for different photon-number states as the result of the ideal state  $|\tilde{\alpha}_A\rangle$ . In other words,  $|\langle n|\psi_A(\tilde{\alpha}_A)\rangle|^2 = |\langle n|\tilde{\alpha}_A\rangle|^2$ . Given this, we immediately know that  $\langle 0|\psi_A(\tilde{\alpha}_A)\rangle = \langle 0|\psi_B(\tilde{\alpha}_B)\rangle = 0$ . Therefore,

there exist the following unitary transformations:

$$\begin{aligned} \mathcal{U}_A|0\rangle &= \mathcal{U}_B|0\rangle = |0\rangle, \quad \mathcal{U}_A|\tilde{\alpha}_A\rangle = |\psi_A(\tilde{\alpha}_A)\rangle, \\ \mathcal{U}_B|\tilde{\alpha}_B\rangle &= |\psi_B(\tilde{\alpha}_B)\rangle. \end{aligned} \quad (4)$$

These equations demonstrate that the real-life source that emits nonideal whole-space states can be mapped from an ideal source by a two-mode unitary transformation  $\mathcal{U}_A \otimes \mathcal{U}_B$ . Given an ideal two-mode source in the protocol, one can simply take a unitary transformation  $\mathcal{U}_A$  to every encoding state from Alice's ideal physical source and take a unitary transformation  $\mathcal{U}_B$  to every encoding state from Bob's ideal physical source. In this way, *they* can obtain all their imperfect states of the real-life source. Applying our Theorem 1, we immediately conclude that our real protocol, protocol R, is secure with a real-life source if it is secure with an ideal source.

Obviously, the protocol allows us to use a source with unstable side-channel information. Say, in any time window  $i$ , that *they* have prepared the whole-space candidature states  $|\psi_{Ai}(\tilde{\alpha}_A)\rangle$  and  $|\psi_{Bi}(\tilde{\alpha}_B)\rangle$ . In this case, we only need to replace the unitary transformation  $\mathcal{U}_A$  and  $\mathcal{U}_B$  in Eq. (4) by  $\mathcal{U}_{Ai}$  and  $\mathcal{U}_{Bi}$ , respectively.

*Note 5:* Intensity difference does not affect security. Though we demonstrate the protocol with the condition  $|\alpha_A| = |\alpha_B| = \mu$ , this condition is not necessary for security. We only require that the *intensities of all time windows are upper bounded by  $\mu$* . Say, in any individual time window  $i$ , that we have  $|\alpha_{Ai}| = \sqrt{\mu_{Ai}} \leq \sqrt{\mu}$  and  $|\alpha_{Bi}| = \sqrt{\mu_{Bi}} \leq \sqrt{\mu}$ . All these states can be obtained from an imagined coherent state of intensity,  $\mu$ , by attenuation. Again, applying our Theorem 1, we can assume that *they* are using coherent states with a stable and exact intensity  $\mu$  [51].

*Discussions:* Revised protocol by postselection. In the protocol, to produce a high key rate, we need Charlie to perform phase compensation effectively. Technically, we can further simplify the protocol without such active operation. Instead, Alice and Bob can perform postselection by only using effective events the corresponding initially prepared states  $|\alpha_A\rangle = |\sqrt{\mu}e^{i\gamma_A}\rangle$  and  $|\alpha_B\rangle = |\sqrt{\mu}e^{i\gamma_B}\rangle$  of which in the time window satisfy

$$1 - |\cos(\gamma_B - \gamma_A)| \leq |\lambda|. \quad (5)$$

If we take a very small  $|\lambda|$  value, the phase-flip error rate will be small, though the data size will also be small [46, 48, 52]. As pointed out in Ref. [48], we can choose a more general formula:

$$1 - |\cos(\delta_A - \delta_B + \Delta\varphi)| \leq |\lambda|. \quad (6)$$

Here, the value of  $\Delta\varphi$  is determined by Alice and Bob according to the result of channel testing and calibration in the experiment to obtain a satisfactory key rate and it can be different from time to time.

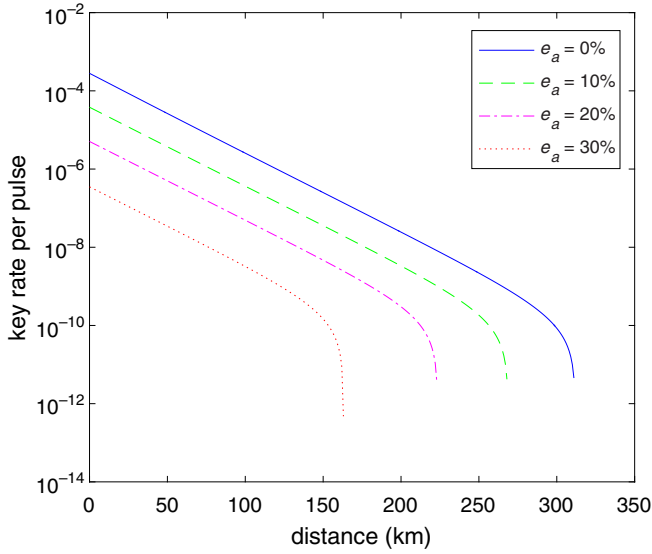


FIG. 2. The log scale of the key rate as a function of the distance between Alice and Bob with different misalignment error rates:  $e_a$ , single-photon misalignment error.

#### IV. NUMERICAL SIMULATION

Assume that the detector dark-count rate is  $10^{-11}$ , with a detection efficiency of 80%, a linear lossy channel with transmittance  $\eta = 0.1^{-L/100}$  (km), and a correction efficiency of  $f = 1.1$ . The results of the numerical simulation are displayed in Fig. 2.

Interestingly, the TGW (Takeoka, Guha, and Wilde) bound [53] or the PLOB (Pirandola, Laurenza, Ottaviani, and Banchi) bound [54] gives the secret-key capacity (SKC) of a quantum channel with losses, which quantifies the upper bound of secret information that can be transmitted in a point-to-point QKD protocol. As a comparison, we calculate the key rate of our side-channel-free (SCF) protocol in an ideal (virtual) case in which Alice and Bob could pre-share the twin-field state  $|\chi^+\rangle$  in Eq. (7). We present the numerical results of the PLOB bound, the sending-or-not-sending protocol (SNS) in Ref. [46], and the ideal SCF in Fig. 3.

#### V. SECURITY PROOF IN OPERATIONAL SPACE

##### A. Outline

The two parts for the security proof are provided here. Part 1 includes the virtual protocols and reductions, through which we first demonstrate the security if *they* only use results from  $\tilde{Z}$  windows in distilling the final key. In a real protocol, *they* sometimes use  $\tilde{Z}$  windows and sometimes use other time windows. We regard effective bits from  $\tilde{Z}$  windows as untagged bits, while the effective bits from other time windows are regarded as tagged bits. Applying the tagged model [13,14], we can obtain the key-rate formula of Eq. (1). In this formula, we need two

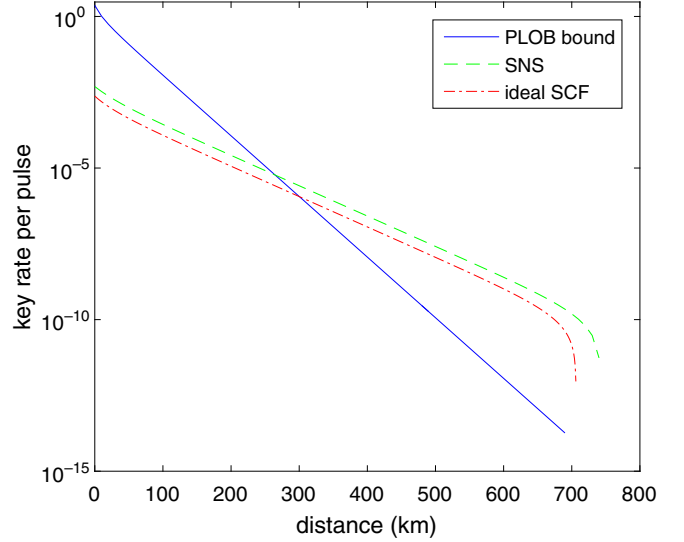


FIG. 3. The log scale of the key rate as a function of the distance between Alice and Bob with different methods. The single-photon misalignment error is set to be  $e_a = 10\%$  and the other parameters are the same as those in Fig. 2.

parameters, the bit-flip error rate and the phase-flip error rate. A bit-flip error occurs in cases in which Alice and Bob have different values for an effective bit. Therefore, the bit-flip error rate can be directly tested by the subset  $v$ . The phase-flip error is originally defined on the phase-flip error of virtual ancillary photons, which can be verified by observing the effective events of  $X$  windows in a virtual protocol, heralded by different detectors (left detector,  $L$ , or right detector,  $R$ ). The  $X$  windows in a virtual protocol contain two subsets: one with  $X_+$  windows that send out a real-photon state  $\rho_+ = |\chi^+\rangle\langle\chi^+|$  and the other with  $X_-$  windows that send out a real-photon state  $\rho_- = |\chi^-\rangle\langle\chi^-|$  and

$$|\chi^\pm\rangle = (|0, \alpha_B\rangle \pm |\alpha_A, 0\rangle) / \mathcal{N}_\pm, \quad (7)$$

where the  $1/\mathcal{N}_\pm$  are normalization factors for states  $|\chi^\pm\rangle$ . In our virtual protocol, *they* set a probability  $|\mathcal{N}_+|^2/4$  for an  $X_+$  window and a probability  $|\mathcal{N}_-|^2/4$  for an  $X_-$  window whenever they use an  $X$  window. The sent-out state of an  $X$  window is

$$\rho_X = |\mathcal{N}_+|^2 \rho_+ / 4 + |\mathcal{N}_-|^2 \rho_- / 4. \quad (8)$$

As will be demonstrated, the phase-flip error rate is

$$\begin{aligned} e^{\text{ph}} &= \frac{n_{X_+}^R + n_{X_-}^L}{n_X} = \frac{n_{X_+}^R + n_{X_-}^L - n_{X_+}^L}{n_X} \\ &\leq \bar{e}^{\text{ph}} = \frac{\bar{n}_{X_+}^R + n_{X_-}^L - \underline{n}_{X_+}^L}{n_X}, \end{aligned} \quad (9)$$

where  $n_a^d$  is the number of effective  $a$  windows heralded by detector  $d$ , with  $d = L, R$  and  $a = X_+, X_-, X$ . For example,  $n_{X_+}^R$  is the number of effective  $X_+$  windows heralded by detector  $R$ . However, in a real protocol, we do not have such a state and hence we have no way of obtaining the value by direct observation. Fortunately, we can still verify the upper bound of the phase-flip error rate by observing the data of other states in the real protocol with the calculation formulas presented in Part 2. For example, say that in the real protocol, *they* randomly take two subsets of all time windows,  $v$  and  $u$ . In this paper, a quantity with an overline denotes its upper bound and one with an underline denotes its lower bound.

Details on *sending* or *not sending* of  $u$  are never announced, but we know that set  $u$  contains a number of  $\tilde{Z}$  windows where the density operator is

$$\rho_{\tilde{Z}} = \frac{1}{2}(|0, \alpha_B\rangle\langle 0, \alpha_B| + |\alpha_A, 0\rangle\langle \alpha_A, 0|). \quad (10)$$

Obviously, the density operator has another equivalent convex form

$$\rho_{\tilde{Z}} = \rho_X. \quad (11)$$

This means that, in a virtual protocol, if we do not announce any information on *sending* or *not sending* of time windows in set  $u$ , from Eve's perspective, those  $\tilde{Z}$  windows in set  $u$  are identical to  $X$  windows. Say, in a real protocol, that set  $u$  contains fake  $X$  windows, which are identical to true  $X$  windows to Eve. This means that the values of  $n_a^d$  in Eq. (9) refer to the quantities in set  $u$ . We can then verify the value of  $\bar{e}^{\text{ph}}$  of the fake  $X$  windows by observing and calculating the data of another subset of time windows, set  $v$ , in the real protocol. Explicitly, as we show in Part 2, we need to incorporate the following data in the calculation.

The  $d$ -event rate of time windows  $A$  is denoted by  $S_A^d$ . Explicitly, denote the number of  $A$  windows in set  $v$  by  $N_A$  and denote the number of effective  $A$  windows heralded by detector  $d$  in set  $v$  by  $n_d$ . Then

$$S_A^d = n_d/N_A, \quad (12)$$

with  $d = L, R$  as announced by Charlie. We need the values of  $S_A^d$  for  $d = L, R$  and  $A = \mathcal{B}, \mathcal{O}, \tilde{Z}$ , where  $\mathcal{B}$  is for a time window in which both Alice and Bob decide on *sending*,  $\mathcal{O}$  is for a time window in which both Alice and Bob decide on *not sending*, and, as defined earlier,  $\tilde{Z}$  is for a time window in which Alice decides on *sending* and Bob decides on *not sending*, or Alice decides on *not sending* and Bob decides on *sending*.

Straightforwardly, we have

$$E_Z = \frac{n_{\mathcal{O}} + n_{\mathcal{B}}}{n_v} \quad (13)$$

for the bit-flip error rate in Eq. (1), where  $n_{\mathcal{O}}$  is the number of effective events in  $\mathcal{O}$  windows,  $n_{\mathcal{B}}$  is the number of effective events in  $\mathcal{B}$  windows, and  $n_v$  is the number of effective events in set  $v$ .

As we show in Part 2, based on these observed data, we can then calculate the upper bound of the phase-flip error rate,  $\bar{e}^{\text{ph}}$ . Explicitly,

$$e^{\text{ph}} \leq \bar{e}^{\text{ph}} = \frac{(1 + e^{-\mu}) \left[ \bar{S}_{X_+}^R - \underline{S}_{X_+}^L \right] + 2S_{\tilde{Z}}^L}{2(S_{\tilde{Z}}^L + S_{\tilde{Z}}^R)}, \quad (14)$$

where  $\bar{S}_{X_+}^d$  ( $\underline{S}_{X_+}^d$ ) is the upper bound (lower bound) of  $S_{X_+}^d$ , with  $d = L, R$  and

$$\begin{aligned} S_{X_+}^d \leq \bar{S}_{X_+}^d &= \frac{1}{2(1 + e^{-\mu})} \left\{ e^{-\mu} S_{\mathcal{O}}^d + \frac{1}{e^{-\mu}} S_{\mathcal{B}}^d + \frac{(1 - e^{-\mu})^2}{e^{-\mu}} \right. \\ &\quad + 2\sqrt{S_{\mathcal{O}}^d S_{\mathcal{B}}^d} + 2(1 - e^{-\mu})\sqrt{S_{\mathcal{O}}^d} \\ &\quad \left. + \frac{2(1 - e^{-\mu})}{e^{-\mu}} \sqrt{S_{\mathcal{B}}^d} \right\}, \quad (15) \end{aligned}$$

$$\begin{aligned} S_{X_+}^d \geq \underline{S}_{X_+}^d &= \frac{1}{2(1 + e^{-\mu})} \left\{ e^{-\mu} S_{\mathcal{O}}^d + \frac{1}{e^{-\mu}} S_{\mathcal{B}}^d \right. \\ &\quad - \left[ 2\sqrt{S_{\mathcal{O}}^d S_{\mathcal{B}}^d} + 2(1 - e^{-\mu})\sqrt{S_{\mathcal{O}}^d} \right. \\ &\quad \left. \left. + \frac{2(1 - e^{-\mu})}{e^{-\mu}} \sqrt{S_{\mathcal{B}}^d} \right] \right\}. \quad (16) \end{aligned}$$

Note that all values of  $S_{\tilde{Z}}^d, S_{\mathcal{O}}^d, S_{\mathcal{B}}^d$  in Eqs. (14)–(16) can be obtained through observing the subset  $v$  by Eq. (12).

## B. Part 1: virtual protocols, reduction, and key rate from tagged model

*Definitions.* We define an *effective event* if Charlie announces one and only one detector clicking for an individual time window. *They* will then only use states or data corresponding to effective events in the protocol. A time window that presents an effective event is called an effective time window. An *effective ancillary photon* is an ancillary photon corresponding to an effective event. A classical bit from an effective time window is called an effective bit.

An “event  $L$ ” or “ $L$  event” is an effective event of the left detector clicking and the right detector not clicking. An “event  $R$ ” or “ $R$  event” is an effective event of the right detector clicking and the left detector not clicking.

### 1. Virtual protocol VI

*a. Preparation stage.* They preshare classical information for the different time windows that they will use,  $X$  windows and  $Z$  windows. They also preshare an extended state

$$\Omega_i = |\Psi_i\rangle\langle\Psi_i|,$$

$$|\Psi_i\rangle = \frac{1}{\sqrt{2}}(|0, \alpha_B\rangle \otimes |01\rangle + |\alpha_A, 0\rangle \otimes |10\rangle), \quad (17)$$

for the  $i$ th time window. Here,  $|\alpha_A\rangle = |\alpha_B\rangle = \sqrt{\mu}$ ,  $|\alpha_{Ai}\rangle = |\sqrt{\mu}e^{i\gamma_{Ai}}\rangle$  and  $|\alpha_{Bi}\rangle = |\sqrt{\mu}e^{i\gamma_{Bi}}\rangle$ . They announce the states including the global phases  $\gamma_{Ai}, \gamma_{Bi}$ .

For simplicity of presentation, we omit the subscripts  $i$  in all phase values  $\gamma_{Ai}, \gamma_{Bi}$  and states. We also introduce states  $|\chi^+\rangle, |\chi^-\rangle$  as defined by Eq. (7) for the extended state. Explicitly, these states can be written as follows:

$$|\Psi\rangle = (\mathcal{N}_+|\chi^+\rangle \otimes |\Phi^0\rangle + \mathcal{N}_-|\chi^-\rangle \otimes |\Phi^1\rangle)/2 \quad (18)$$

where  $|\Phi^0\rangle = (1/\sqrt{2})(|01\rangle + |10\rangle)$ ,  $|\Phi^1\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$ .

*b. Virtual protocol VI.* V1-1 In any time window  $i$ , no matter if it is a  $Z$  window or an  $X$  window, they send out to Charlie the real-photon state from state  $\Omega$  as defined by Eq. (17) and keep the ancillary photons locally.

V1-2 Charlie announces his measurement outcome of all the time windows. This announcement determines the effective time windows.

*Definition.*—They can now divide their time windows into four subsets,  $X^L, X^R, Z^L, Z^R$ , where a time window of  $\mathcal{W}^d$  is an effective  $\mathcal{W}$  window heralded by detector  $d$  clicking and the other detector not clicking.  $\mathcal{W} = X, Z$  and  $d = L, R$ . We also use  $\mathcal{A}_{\mathcal{W}^d}$  for the set of effective ancillary photons of time window  $\mathcal{W}^d$ .

V1-3 They check the phase-flip error rate,  $e^{\text{ph}}$ , for a set of  $\mathcal{A}_{X^d}$ , where  $d = L, R$ , which is also the estimated phase-flip error rate for set  $\mathcal{A}_{Z^d}$ .

V1-4 They purify the ancillary photons of sets  $\mathcal{A}_{Z^L}$  and  $\mathcal{A}_{Z^R}$ , separately. After purification, they obtain high-quality single-photon states,  $|\Phi^0\rangle$  or  $|\Phi^1\rangle$ , with (almost) 100% purity. They each measure the photon number locally to the purified photons and obtain the final key,  $k_f$ . Alice puts down a bit value of 0 or 1 whenever she obtains a measurement outcome of vacuum or one photon, while Bob puts down a bit value of 1 or 0 whenever he obtains a measurement outcome of vacuum or one photon.

*Note 1: Security.* The security of the final key is based on the faithfulness of the purification [55], i.e., the faithfulness in estimating the phase-flip error rate. Charlie has determined effective ancillary photons, but Alice and Bob test the phase-flip error rate themselves in step V1-3. The extended state of an  $X$  window is identical to that of a  $Z$  window; therefore, the phase-flip error rate value of set

$\mathcal{A}_{X^d}$  is exactly the value of set  $\mathcal{A}_{Z^d}$ . Charlie's role here is actually a quantum relay, i.e., a memoryless quantum repeater. Therefore, the protocol is secure regardless of whether or not Charlie is honest. Of course, if Charlie wants to let Alice and Bob have a satisfied key rate, he needs to make an effort to produce high-quality effective pair states of the low phase-flip error rate for those local ancillary photons with Alice and Bob. To obtain this goal, he must take phase compensation to the incoming light before his measurement in step V1-2. In short, Charlie's action cannot change the security of the protocol, though he can change the key rate.

*Note 2: Definitions of the phase-flip error rate.* Suppose that set  $\mathcal{A}_{X^d}$  contains  $n^d$  effective ancillary photons. If each photon of set  $\mathcal{A}_{X^d}$  is measured in basis  $\{|\Phi^0\rangle, |\Phi^1\rangle\}$  and there are  $n_0^d$  outcomes of  $|\Phi^0\rangle\langle\Phi^0|$  and  $n_1^d$  outcomes of  $|\Phi^1\rangle\langle\Phi^1|$ , the phase-flip error rate for set  $\mathcal{A}_{X^d}$  is as follows:

$$e^{\text{ph}} = \frac{\min(n_0^d, n_1^d)}{n^d}. \quad (19)$$

Changing the values of  $n_0^d, n_1^d, n^d$  into the corresponding values for set  $\mathcal{A}_{Z^d}$  in Eq. (19), we can define the phase-flip error rate for set  $\mathcal{A}_{Z^d}$ . Statistically,  $e^{\text{ph}}$  for set  $\mathcal{A}_{X^d}$  is also the asymptotic phase-flip error rate of set  $\mathcal{A}_{Z^d}$ . To know the value  $e^{\text{ph}}$ , they can choose to measure each photon of set  $\mathcal{A}_{X^d}$  in basis  $\{|\Phi^0\rangle, |\Phi^1\rangle\}$ . But, instead, they can also choose to take local measurements in basis  $\{|x\pm\rangle\}$ , with  $|x\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ , on each side and check the parity of each measurement outcome. (The outcomes of  $|x+\rangle|x+\rangle$  or  $|x-\rangle|x-\rangle$  are even parity, while those of  $|x+\rangle|x-\rangle$  or  $|x-\rangle|x+\rangle$  are odd parity.) Note that all effective ancillary photons are single photons. As one can observe, for single photons, the fraction of odd-parity (even-parity) outcomes from measurement of each side in basis  $\{|x\pm\rangle\}$  is exactly equal to the fraction of  $|\Phi^1\rangle\langle\Phi^1|$  ( $|\Phi^0\rangle\langle\Phi^0|$ ) outcomes from the measurement in basis  $\{|\Phi^0\rangle, |\Phi^1\rangle\}$ . Moreover, this measurement step is only needed for this virtual protocol; it is not needed for a real protocol. For ease of presentation, we suppose that they use the measurement basis  $\{|\Phi^0\rangle, |\Phi^1\rangle\}$ .

*Note 3: Reduction of preshared states of  $X$  windows.* *Reduction 1:* It makes no difference to anyone outside if they measure all of the ancillary photons of the  $X$  windows in basis  $\{|\Phi^0\rangle, |\Phi^1\rangle\}$  before the protocol starts. After measuring an ancillary photon, they obtain one of the following outcome-extended states for an  $X$  window, depending on the measurement outcome of the ancillary photon: either

$$|\chi^+\rangle\langle\chi^+| \otimes |\Phi^0\rangle\langle\Phi^0|, \quad (20)$$

with probability  $|\mathcal{N}_+|^2/4$ , or

$$|\chi^-\rangle\langle\chi^-| \otimes |\Phi^1\rangle\langle\Phi^1|, \quad (21)$$

with probability  $|\mathcal{N}_-|^2/4$ .

*Reduction 2.* Alternatively, *they* can just start with the states of Eqs. (20) and (21) for their  $X$  windows. *They* need to preshare classical information on the  $Z$  windows,  $X_+$  windows, and  $X_-$  windows. The preshared classical information for the  $X$  windows assigns a probability of  $|\mathcal{N}_+|^2/4$  for the  $X_+$  windows and a probability of  $|\mathcal{N}_-|^2/4$  for the  $X_-$  windows. *They* preshare real-photon states  $|\chi^+\rangle\langle\chi^+|$  for the  $X_+$  windows and  $|\chi^-\rangle\langle\chi^-|$  for the  $X_-$  windows. Imagine that *they* also preshare some single-photon states  $|\Phi^0\rangle$  and  $|\Phi^1\rangle$ . (These states  $|\Phi^0\rangle$  and  $|\Phi^1\rangle$  are not really necessary; however, to display everything clearly, we assume so at this moment.)

In an  $X_+$  window, *they* label a preshared state,  $|\Phi^0\rangle$ , as the ancillary photon for the state  $|\chi^+\rangle$  above and also have an extended state denoted as follows:

$$\Omega_+ = |\chi^+\rangle\langle\chi^+| \otimes |\Phi^0\rangle\langle\Phi^0|. \quad (22)$$

*They* then send the real-photon state,  $|\chi^+\rangle$ , out to Charlie. In an  $X_-$  window, *they* label a preshared state,  $|\Phi^1\rangle$ , as the ancillary photon for the state  $|\chi^-\rangle$  above and also have an extended state denoted as follows:

$$\Omega_- = |\chi^-\rangle\langle\chi^-| \otimes |\Phi^1\rangle\langle\Phi^1|. \quad (23)$$

*They* then send the real-photon state,  $|\chi^-\rangle$ , out to Charlie. Here, we use the same definition for  $|\chi^+\rangle, |\chi^-\rangle$  as in Eq. (7).

From Eqs. (22) and (23), we can observe that, in an  $X_+$  window, the ancillary-photon state must be  $|\Phi^0\rangle$ ; whereas in an  $X_-$  window, the ancillary-photon state must be  $|\Phi^1\rangle$ .

Therefore, *they* can use the following more operable definition to calculate each quantity in Eq. (19):

$$n_0^d = n_{X_+}^d, \quad (24)$$

$$n_1^d = n_{X_-}^d, \quad (25)$$

for Eq. (19). Here,  $n_{X_\pm}^d$  is the number of  $X_+$  windows or  $X_-$  windows heralded by detector  $d$  clicking and the other detector not clicking, while  $d = L, R$ , where  $L$  represents the left detector and  $R$  represents the right detector:

$$e^{\text{ph}} = \frac{\min(n_{X_+}^d, n_{X_-}^d)}{n^d}. \quad (26)$$

Given this phase-flip error rate formula, the ancillary photons for the  $X$  windows are actually *not* needed in the protocol.

*Note 4: Quasipurification.* Since *their* goal is to have the final key only, a true purification of the ancillary photons is not necessary [56]. *They* can choose to measure all ancillary photons of  $Z$  windows in advance [56] on the photon-number basis and then apply virtual purification to the classical data of the  $Z$  windows that correspond to those

effective events. *They* then take a virtual quasipurification to the classical data, which is the final key distillation. Additionally, the preshared extended state for a  $Z$  window is just  $(|0, \alpha_B\rangle\langle 0, \alpha_B| \otimes |01\rangle\langle 01| + |\alpha_A, 0\rangle\langle \alpha_A, 0| \otimes |10\rangle\langle 10|)/2$ .

*Note 5: Purifying all effective ancillary photons in one batch.* Definitely, *they* can choose to purify all of the effective ancillary photons of the  $Z$  windows in one batch. The phase-flip error rate is as follows:

$$e^{\text{ph}} = \frac{\min(n_{X_+}^L, n_{X_-}^L) + \min(n_{X_+}^R, n_{X_-}^R)}{n_X}, \quad (27)$$

where  $n_X = n_{X_+}^L + n_{X_-}^L + n_{X_+}^R + n_{X_-}^R$  is the number of all effective  $X$  windows. Surely,  $n_{X_-}^L \geq \min(n_{X_+}^L, n_{X_-}^L)$  and  $n_{X_+}^R \geq \min(n_{X_+}^R, n_{X_-}^R)$ . Therefore, the phase-flip error rate formula of Eq. (27) can be simplified to

$$e^{\text{ph}} \leq \frac{n_{X_-}^L + n_{X_+}^R}{n_X}, \quad (28)$$

which allows us to first count the number of effective  $X_-$  windows heralded by the left detector and the effective  $X_+$  windows heralded by the right detector and then take the rate of errors per effective  $X$  window.

If *they* use this formula, Charlie can achieve a high-quality raw state of effective ancillary photons for Alice and Bob by preparing his measurement setup properly, with a very small probability of the left detector clicking (right detector clicking) due to the incident state of  $|\chi^-\rangle$  ( $|\chi^+\rangle$ ).

## 2. Virtual protocol V2

*a. Preparation stage.* Here, we assume that *they* preshare a mixed state of

$$\Omega = \sum_y p_y \Omega_y \quad (29)$$

$y = 0, 1, \mathcal{B}, \mathcal{O}, +, -, p_0 = p_1$ , and

$$\Omega_0 = |0, \alpha_B\rangle\langle 0, \alpha_B| \otimes |01\rangle\langle 01|, \quad (30)$$

$$\Omega_1 = |\alpha_A, 0\rangle\langle \alpha_A, 0| \otimes |10\rangle\langle 10|, \quad (31)$$

$$\Omega_{\mathcal{B}} = |\alpha_A, \alpha_B\rangle\langle \alpha_A, \alpha_B| \otimes |11\rangle\langle 11|, \quad (32)$$

$$\Omega_{\mathcal{O}} = |0, 0\rangle\langle 0, 0| \otimes |00\rangle\langle 00|, \quad (33)$$

$$\Omega_+ = |\chi^+\rangle\langle\chi^+| \otimes |2, 2\rangle\langle 2, 2|, \quad (34)$$

$$\Omega_- = |\chi^-\rangle\langle\chi^-| \otimes |3, 3\rangle\langle 3, 3|. \quad (35)$$

*They* do not preshare any classical information for the time windows. For clarity of presentation, we define different kinds of time windows by the local ancillary states:



$|01\rangle\langle 01|$  for  $Z_0$ ,  $|10\rangle\langle 10|$  for  $Z_1$ ,  $|11\rangle\langle 11|$  for  $Z_B$ ,  $|00\rangle\langle 00|$  for  $Z_O$ ,  $|2, 2\rangle\langle 2, 2|$  for  $X_+$ , and  $|3, 3\rangle\langle 3, 3|$  for  $X_-$ .

Time window  $Z_0$  ( $Z_1$ ) corresponds to the case in which Alice (Bob) chooses *not sending* and Bob (Alice) decides on *sending*. Time window  $Z_B$  ( $Z_O$ ) corresponds to the case in which both Alice and Bob choose *sending* (*not sending*).

Given the values of  $p_0, p_1$ , they know how many  $\tilde{Z}$  windows ( $Z_0$  windows or  $Z_1$  windows) exist. Also, by announcing details of a random subset of  $Z$  windows, they can judge the fraction of effective time windows among all  $\tilde{Z}$  windows. Thus, they know the total number of effective  $\tilde{Z}$  windows among all the effective  $Z$  windows. Then they can apply the tagged model to calculate the final key.

*b. Virtual protocol V2.* V2-1 In any time window,  $i$ , they send the real-photon state out to Charlie from a pre-shared extended state,  $\Omega$ . By measuring the local ancillary photon, they each know whether the time window is an  $X$  window or an  $Z$  window explicitly, a local state  $|2\rangle\langle 2|$  for an  $X_+$  window, a local state  $|3\rangle\langle 3|$  for an  $X_-$  window, and a local state  $|0\rangle\langle 0|$  or  $|1\rangle\langle 1|$  for a  $Z$  window. Though they know which time windows are  $Z$  windows, they do not know which kinds of  $Z$  windows ( $Z_0, Z_1, Z_B, Z_O$ ).

V2-2 Charlie announces his measurement outcome for all time windows.

V2-3 According to Charlie's announcement, they are aware of those effective  $Z$  windows and  $X$  windows. For a  $Z$  window, Alice (Bob) puts down a classical bit, 0 (1), if her (his) local ancillary state is vacuum and puts down a classical bit, 1 (0), if her (his) local ancillary state is one photon. They randomly take a subset,  $v$ , of  $Z$  windows, announcing the local measurement outcome of each time window in set  $v$  so that they can judge the asymptotic value of the bit-flip error rate,  $E_Z$ , by counting the number of effective  $\tilde{Z}$  windows from all of the effective  $Z$  windows of set  $v$ . They estimate the phase-flip error rate,  $e^{\text{ph}}$ , of effective bits of  $\tilde{Z}$  windows (time windows of  $Z_0$  and  $Z_1$ ) by Eq. (28) by observing the events of all  $X$  windows.

V2-4 They regard the effective bits from the  $\tilde{Z}$  windows as untagged bits and the effective bits from the time windows of  $Z_B$  and  $Z_O$  as tagged bits. Applying the tagged model [13,14], they distill the effective bits of the  $Z$  windows and obtain the final key,  $k_f$ , with the length given by Eq. (1).

*Note 1:* A bit-flip error is an effective  $Z$  window when Bob's bit value is different from Alice's. They can verify the error by testing a random subset of  $Z$  windows.

*Note 2:* An estimation of  $\bar{e}^{\text{ph}}$ , the upper bound of the phase-flip error rate, can only be achieved by observing the subset  $v$  of the  $Z$  windows. Consider Eq. (28), which is equivalent to the following:

$$e^{\text{ph}} \leq \frac{n_{X_-}^L + n_{X_+}^R}{n_X} \leq \bar{e}^{\text{ph}} = \frac{\bar{n}_{X_+}^R - n_{X_+}^L + n_{X_-}^L}{n_X}, \quad (36)$$

where the bar represents the upper bound and the underline represents the lower bound.  $n_X$  is the total number of effective  $X$  windows,  $n_X^L$  is the number of those effective  $X$  windows heralded by detector  $L$ , and  $n_a^d$  is the number of effective  $a$  windows heralded by detector  $d$ , while  $a = X_+, X_-$  and  $d = L, R$ .

*Note 3:* The  $X$  windows are not really necessary because they can obtain the bound values,  $\bar{n}_{X_+}^R$  and  $\underline{n}_{X_+}^L$ , by observing a subset of  $Z$  windows, instead of observing  $X$  windows. Therefore, we can use fake  $X$  windows to replace the original  $X$  windows, provided that the real-photon state of the fake  $X$  windows is identical to that of the original  $X$  windows. Obviously, in virtual protocol V2, a  $\tilde{Z}$  window is a fake  $X$  window.

### 3. Virtual protocol V3

*a. Preparation stage.* They preshare an extended mixed state of

$$\Omega = \sum_y p_y \Omega_y \quad (37)$$

and  $p_0 = p_1$ :

$$\begin{aligned} \Omega_0 &= |0, \alpha_B\rangle\langle 0, \alpha_B| \otimes |01\rangle\langle 01|, \\ \Omega_1 &= |\alpha_A, 0\rangle\langle \alpha_A, 0| \otimes |10\rangle\langle 10|, \\ \Omega_B &= |\alpha_A, \alpha_B\rangle\langle \alpha_A, \alpha_B| \otimes |11\rangle\langle 11|, \\ \Omega_O &= |0, 0\rangle\langle 0, 0| \otimes |00\rangle\langle 00|. \end{aligned} \quad (38)$$

In this virtual protocol, they do not preshare any classical information. We define time windows  $Z_0, Z_1, Z_B, Z_O$  by the four different ancillary states. If they each announce the local measurement outcome of the ancillary-photon state in a certain time window  $i$ , they can know the specific kind of time window for  $i$ . In the protocol, they will take a random subset of time windows,  $v$ , for the error test. They each announce the local measurement outcome of the ancillary state of every time window in set  $v$ . Afterward, for each  $i \in v$ , they know explicitly which kind of time window it is, i.e.,  $Z_0, Z_1, Z_B$ , or  $Z_O$ .

*b. Virtual protocol V3.* V3-1 In any time window  $i$ , they send out their real-photon state.

V3-2 Charlie announces his measurement outcome for all time windows.

V3-3 Alice (Bob) measures her (his) ancillary photon for all effective time windows, with the outcome vacuum for a classical bit 0 (1) and one photon for a bit value 1 (0). Through classical communications, they take two random subsets,  $v$  and  $u$ , for the error test. They do not announce the photon-state information of the random subset  $u$ . All the  $\tilde{Z}$  windows in set  $u$  are defined as set  $u_{\tilde{Z}}$ . The real-photon states of set  $u_{\tilde{Z}}$  make a fake state for the imaginary  $X$  windows defined in Note 4 of virtual protocol V2. For

every time window of set  $v$ , they each announce the local measurement outcome of the ancillary-photon state. From these announced outcomes, they can know the bit-flip error rate,  $E_Z$ , and the fraction of untagged bits, i.e., bits from time windows  $Z_0$  or  $Z_1$ . They also know the yield values of  $S_A^d$ , where  $d = L, R$  and  $A = B, O$ , respectively. Using these values, they calculate the upper bound value of  $\bar{e}^{\text{ph}}$  of Eq. (28) for the fake  $X$  windows ( $\tilde{Z}$  windows of set  $u$ ).

V3-4 They distill effective bits of  $Z$  windows and obtain the final key,  $k_f$ . Applying the tagged model [13,14], they can calculate the length of the final key using Eq. (1).

*Note 1:* They can produce the state of Eq. (37) locally. Setting  $p_0 = p_1 = q(1 - q)$ ,  $p_O = (1 - q)^2$ , and  $p_B = q^2$ , they can produce the  $\Omega$  state of Eq. (37) locally in the following manner. At every time  $i$ , Alice (Bob) randomly chooses *sending* with probability  $q$  or *not sending* with probability  $1 - q$ . For a *sending* decision, she (he) sends out a coherent state  $|\alpha_A\rangle\langle\alpha_A|$  ( $|\alpha_B\rangle\langle\alpha_B|$ ) to Charlie, puts down a bit value 1 (0), and produces a local state  $|1\rangle\langle 1|$ . For a *not-sending* decision, she (he) sends out a vacuum to Charlie, puts down a bit value 0 (1), and produces a local state  $|0\rangle\langle 0|$ . If they produce the state  $\Omega$  of Eq. (37) in this way, they do not need to preshare anything. Also, without the local ancillary-photon state, they can still complete the final key distillation. Therefore, the local ancillary state is not actually needed, which brings us back to the real protocol.

## C. Part 2: phase-flip error rate

### 1. Input-output model

Consider an input state to Charlie sent from Alice (and Bob). Alice will observe Charlie's instrument,  $\mathcal{L}$ , for the corresponding outcome (classical outcome). Charlie has no access to Alice's source.

Suppose that, at the beginning of a certain time window, Charlie receives a state,  $|\psi\rangle$ . We denote this as an input state to Charlie. Consider the extended state made up of the input state and Charlie's state,  $|\kappa\rangle$ . Charlie's instrument state,  $\mathcal{L}$ , is included in the ancillary state,  $|\kappa\rangle$ . The initial state is as follows:

$$|\Psi_{\text{ini}}\rangle = |\psi\rangle \otimes |\kappa\rangle. \quad (39)$$

At time  $t$ , Charlie's instrument,  $\mathcal{L}$ , is observed by Alice and she can then derive a result based on  $\{|i\rangle\}$  accompanied by its eigenstate,  $|i\rangle$ . Generally, after state  $|\psi\rangle$  is sent to Charlie, Charlie's initial state,  $|\Psi_{\text{ini}}\rangle = |\psi\rangle \otimes |\kappa\rangle$ , will evolve with time under a quantum process. Here, we assume a unitary quantum process,  $\mathcal{U}$ . Even though Charlie presents a nonunitary quantum process, it can still be represented by a unitary process by adding more ancillary states. Hence, given the general ancillary state  $|\kappa\rangle$ , we can simply assume a unitary quantum process for Charlie. At time  $t$ , the state

is now as follows:

$$|\Psi(t)\rangle = \mathcal{U}(t)|\Psi_{\text{ini}}\rangle = \mathcal{U}(t)(|\psi\rangle \otimes |\kappa\rangle). \quad (40)$$

In general, the state at time  $t$  can be written in a bipartite form of another two subspaces—one being the instrument space  $\mathcal{L}$  and the other being the remaining part of the space, or subspace  $\bar{\mathcal{L}}$ . Given the initial input state  $|\psi\rangle$  to Charlie, the probability that he observes the result  $I_1$  at time  $t$  is as follows:

$$p^{I_1} = \langle I_1 | \text{tr}_{\bar{\mathcal{L}}} (|\Psi(t)\rangle\langle\Psi(t)|) | I_1 \rangle. \quad (41)$$

We will omit  $(t)$  in the following formulas. If we suppose that the space  $\bar{\mathcal{L}}$  is spanned by basis states  $\{|g_k\rangle\}$ , we can rewrite Eq. (41) as follows:

$$p^{I_1} = \sum_k |\langle \gamma_k^{(I_1)} | \Psi \rangle|^2, \quad (42)$$

where  $|\gamma_k^{(I_1)}\rangle = |g_k\rangle|I_1\rangle$ .

Since in each time window  $i$ , Charlie may use different quantum processes with different ancillary states and different measurements, the quantum process should be written as  $\mathcal{U}_i$  and Eq. (42) should be written as follows:

$$n^{I_1} = \sum_{i=1}^K \sum_k |\langle \gamma_{i,k}^{(I_1)} | \Psi_i \rangle|^2, \quad (43)$$

where  $n^{I_1}$  is the number of time windows for which Alice observes the outcome  $I_1$  from instrument  $\mathcal{L}$  and  $K$  is the total number of time windows.

Equations (42) and (43) are our elementary formulas for the input-output model.

### 2. Calculate the outcome of one input state by observing the outcome of other states

Imagine different sources: source 1 emits the state  $|\phi\rangle$ , source 2 emits the state  $|\phi_0\rangle$ , and source 3 emits the state  $|\phi_1\rangle$ . State  $|\phi\rangle$  has the following form:

$$|\phi\rangle = c_0|\phi_0\rangle + c_1|\phi_1\rangle + c_2|\phi_2\rangle. \quad (44)$$

In any time window  $i$ , Alice only uses one source. She chooses one source randomly from 1, 2, 3 with probabilities  $d_1, d_2, d_3$ , respectively. To distinguish states from different sources, she produces a local ancillary state  $|1\rangle\langle 1|$ ,  $|2\rangle\langle 2|$ , or  $|3\rangle\langle 3|$ , respectively, when she uses sources 1, 2, 3. Consider a virtual case in which Alice and Bob prepare a state with the density matrix

$$\rho = d_1|\phi\rangle\langle\phi| \otimes |1\rangle\langle 1| + d_2|\phi_0\rangle\langle\phi_0| \otimes |2\rangle\langle 2| + d_3|\phi_1\rangle\langle\phi_1| \otimes |3\rangle\langle 3|, \quad d_1 + d_2 + d_3 = 1, \quad (45)$$

where  $|k\rangle, k = 1, 2, 3$  is the local ancillary state. They then keep the ancillary state and send out the real-photon state

to Charlie. (We call the state emitted by source 1, 2, or 3 the real-photon state.)

With the elementary formula Eq. (43) in Sec. VC 1 and Eq. (45), we have the following extended state after Charlie completes the operations for the real-photon state and his ancillary state:

$$\tilde{\rho} = d_1 |\Phi_i\rangle \langle \Phi_i| \otimes |1\rangle \langle 1| + d_2 |\Phi_{0i}\rangle \langle \Phi_{0i}| \otimes |2\rangle \langle 2| + d_3 |\Phi_{1i}\rangle \langle \Phi_{1i}| \otimes |3\rangle \langle 3|, \quad d_1 + d_2 + d_3 = 1, \quad (46)$$

where  $|\Phi_i\rangle = \mathcal{U}_i(t)(|\phi\rangle \otimes |\kappa_i\rangle)$ ,  $|\Phi_{ki}\rangle = \mathcal{U}_i(t)(|\phi_k\rangle \otimes |\kappa_i\rangle)$ ,  $k = 0, 1$ . On the other hand, given Eq. (44), we have

$$|\Phi_i\rangle = c_0 |\Phi_{0i}\rangle + c_1 |\Phi_{1i}\rangle + c_2 |\Phi_{2i}\rangle. \quad (47)$$

We can now write the formula for the number of  $l_1$  events of source  $k$ ,  $n_k^{l_1}$ , which is the number of time windows heralded by joint events of outcome  $l_1$  of instrument  $\mathcal{L}$  from source  $k$ , with  $k = 1, 2, 3$ . Since we have already labeled each source by an ancillary-photon state, the number of  $l_1$  events of source  $k$  is just the number of joint events of outcome  $l_1$  from the instrument and outcome  $|k\rangle \langle k|$  from the measurement to the local ancillary-photon state:

$$n_1^{l_1} = d_1 \sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \Phi_i \rangle|^2, \quad (48)$$

$$n_2^{l_1} = d_2 \sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \Phi_{0i} \rangle|^2, \quad (49)$$

$$n_3^{l_1} = d_3 \sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \Phi_{1i} \rangle|^2. \quad (50)$$

Therefore, we have the following formula for the number of  $l_1$  events of source 1:

$$\begin{aligned} n_1^{l_1}/d_1 &= \sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \Phi_i \rangle|^2 = |c_0|^2 \sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \Phi_{0i} \rangle|^2 \\ &+ |c_1|^2 \sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \Phi_{1i} \rangle|^2 \\ &+ |c_2|^2 \sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \Phi_{2i} \rangle|^2 \\ &+ 2 \sum_{i=1}^N \sum_k \operatorname{Re}(c_0 c_1 \langle \Phi_{0i} | \gamma_{i,k}^{(l_1)} \rangle \langle \gamma_{i,k}^{(l_1)} | \Phi_{1i} \rangle) \\ &+ 2 \sum_{i=1}^N \sum_k \operatorname{Re}(c_0 c_2 \langle \Phi_{0i} | \gamma_{i,k}^{(l_1)} \rangle \langle \gamma_{i,k}^{(l_1)} | \Phi_{2i} \rangle) \\ &+ 2 \sum_{i=1}^N \sum_k \operatorname{Re}(c_1 c_2 \langle \Phi_{1i} | \gamma_{i,k}^{(l_1)} \rangle \langle \gamma_{i,k}^{(l_1)} | \Phi_{2i} \rangle). \quad (51) \end{aligned}$$

For the term  $\sum_{i=1}^N \sum_k \operatorname{Re}(cc' \langle \psi | \gamma_{i,k}^{(l_1)} \rangle \langle \gamma_{i,k}^{(l_1)} | \psi' \rangle)$ , with state  $|\psi\rangle$  and  $|\psi'\rangle$ , we can use the Cauchy inequality

$$\left( \sum_{k=1}^m a_k b_k \right)^2 \leq \sum_{k=1}^m a_k^2 \sum_{k=1}^m b_k^2, \quad a_k, b_k \in \mathbb{R} \quad (52)$$

to obtain its bound

$$\begin{aligned} &\left| \sum_{i=1}^N \sum_k \operatorname{Re}(cc' \langle \psi | \gamma_{i,k}^{(l_1)} \rangle \langle \gamma_{i,k}^{(l_1)} | \psi' \rangle) \right| \\ &\leq |cc'| \sum_{i=1}^N \sum_k |\langle \psi | \gamma_{i,k}^{(l_1)} \rangle| |\langle \gamma_{i,k}^{(l_1)} | \psi' \rangle| \\ &\leq |cc'| \sqrt{\sum_{i=1}^N \sum_k |\langle \psi | \gamma_{i,k}^{(l_1)} \rangle|^2} \sqrt{\sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \psi' \rangle|^2}. \quad (53) \end{aligned}$$

Recalling Eqs. (48)–(50), we have

$$\begin{aligned} n_1^{l_1}/d_1 &= \sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \Phi_i \rangle|^2, \\ n_2^{l_1}/d_2 &= \sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \Phi_{0i} \rangle|^2, \\ n_3^{l_1}/d_3 &= \sum_{i=1}^N \sum_k |\langle \gamma_{i,k}^{(l_1)} | \Phi_{1i} \rangle|^2. \quad (54) \end{aligned}$$

Note that  $0 \leq \sum_k \langle \Phi_{2i} | \gamma_{i,k}^{(l_1)} \rangle \langle \gamma_{i,k}^{(l_1)} | \Phi_{2i} \rangle \leq 1$ . The upper bound of  $n_1^{l_1}/d_1$  can be obtained by

$$\begin{aligned} n_1^{l_1}/d_1 &\leq |c_0|^2 n_2^{l_1}/d_2 + |c_1|^2 n_3^{l_1}/d_3 + |c_2|^2 N \\ &+ 2|c_0 c_1| \sqrt{\frac{n_2^{l_1} n_3^{l_1}}{d_2 d_3}} + 2|c_0 c_2| \sqrt{\frac{n_2^{l_1} N}{d_2}} \\ &+ 2|c_1 c_2| \sqrt{\frac{n_3^{l_1} N}{d_3}} \quad (55) \end{aligned}$$

and we also have the lower bound

$$\begin{aligned} n_1^{l_1}/d_1 &\geq |c_0|^2 n_2^{l_1}/d_2 + |c_1|^2 n_3^{l_1}/d_3 - \left[ 2|c_0 c_1| \sqrt{\frac{n_2^{l_1} n_3^{l_1}}{d_2 d_3}} \right. \\ &\left. + 2|c_0 c_2| \sqrt{\frac{n_2^{l_1} N}{d_2}} + 2|c_1 c_2| \sqrt{\frac{n_3^{l_1} N}{d_3}} \right]. \quad (56) \end{aligned}$$

We then define the yield of state  $|\phi\rangle$  for outcome  $l_1$  by

$$S_\phi^{l_1} = \frac{n_1^{l_1}}{d_1 N}, \quad (57)$$

where  $d_1 N$  is the total number of time windows using source 1, which emits the real-photon state  $|\phi\rangle$ . Similarly,

$$S_{\phi_0}^{l_1} = \frac{n_2^{l_1}}{d_2 N}, \quad S_{\phi_1}^{l_1} = \frac{n_3^{l_1}}{d_3 N}. \quad (58)$$

Therefore, Eqs. (55) and (56) can be written in the form of yields

$$\begin{aligned} S_\phi^{l_1} \leq & |c_0|^2 S_{\phi_0}^{l_1} + |c_1|^2 S_{\phi_1}^{l_1} + |c_2|^2 \\ & + 2|c_0 c_1| \sqrt{S_{\phi_0}^{l_1} S_{\phi_1}^{l_1}} + 2|c_0 c_2| \sqrt{S_{\phi_0}^{l_1}} + 2|c_1 c_2| \sqrt{S_{\phi_1}^{l_1}} \end{aligned} \quad (59)$$

and

$$\begin{aligned} S_\phi^{l_1} \geq & |c_0|^2 S_{\phi_0}^{l_1} + |c_1|^2 S_{\phi_1}^{l_1} \\ & - \left[ 2|c_0 c_1| \sqrt{S_{\phi_0}^{l_1} S_{\phi_1}^{l_1}} + 2|c_0 c_2| \sqrt{S_{\phi_0}^{l_1}} + 2|c_1 c_2| \sqrt{S_{\phi_1}^{l_1}} \right]. \end{aligned} \quad (60)$$

With Eqs. (59) and (60), they can estimate the bounds of the yield of state  $|\phi\rangle$  for  $l_1$  events, even when using the observed data of other states.

### 3. Bound-value estimation in the protocol

In the protocol, we use the real-photon state  $|0, 0\rangle$  in a time window  $Z_O$  and the real-photon state  $|\alpha_A, \alpha_B\rangle$  in a time window  $Z_B$ . The yield for a  $L$  event or a  $R$  event of these two kinds of time windows can be observed directly from the time windows of the random subset  $v$ . We must use the observed data to calculate the bound values for  $S_{X_+}^{l_1}$ , the fraction of time windows heralded by the outcome  $l_1$  among all  $X_+$  windows, explicitly the lower bound for  $L$  events  $\underline{S}_{X_+}^L$  and the upper bound for  $R$  events  $\bar{S}_{X_+}^R$ . We can directly apply Eqs. (59) and (60), by replacing the real-photon states  $|\phi\rangle$ ,  $|\phi_0\rangle$ , and  $|\phi_1\rangle$  with  $|\chi^+\rangle$ ,  $|0, 0\rangle$ , and  $|\alpha_A, \alpha_B\rangle$ , respectively. We can easily obtain

$$|\chi^+\rangle = \frac{e^{-\mu}|0, 0\rangle + |\alpha_A, \alpha_B\rangle - (1 - e^{-\mu})|\tilde{\alpha}_A, \tilde{\alpha}_B\rangle}{e^{-\mu/2}\sqrt{2(1 + e^{-\mu})}}, \quad (61)$$

remembering that  $\sqrt{1 - e^{-\mu}}|\tilde{\alpha}_x\rangle = |\alpha_x\rangle - e^{-\mu/2}|0\rangle$ ,  $x = A, B$ . Therefore,

$$\begin{aligned} c_0 &= \frac{e^{-\mu/2}}{\sqrt{2(1 + e^{-\mu})}}, \\ c_1 &= \frac{1}{e^{-\mu/2}\sqrt{2(1 + e^{-\mu})}}, \\ c_2 &= \frac{1 - e^{-\mu}}{e^{-\mu/2}\sqrt{2(1 + e^{-\mu})}}. \end{aligned} \quad (62)$$

We use the notation  $S_y^{l_1}$  for the fraction of effective windows heralded by outcome  $l_1$  among all  $y$  windows of the test set  $v$  and  $l_1 = L, R$ ,  $y = X_+, Z_B, Z_O$ . Say that there are  $n_y^{l_1}$  effective windows:

$$\begin{aligned} S_{X_+}^{l_1} \leq \bar{S}_{X_+}^{l_1} &= \frac{1}{2(1 + e^{-\mu})} \left\{ e^{-\mu} S_O^{l_1} + e^\mu S_B^{l_1} + \frac{(1 - e^{-\mu})^2}{e^{-\mu}} \right. \\ &\quad \left. + 2\sqrt{S_O^{l_1} S_B^{l_1}} + 2(1 - e^{-\mu})\sqrt{S_O^{l_1}} + \frac{2(1 - e^{-\mu})}{e^{-\mu}}\sqrt{S_B^{l_1}} \right\}, \end{aligned} \quad (63)$$

$$\begin{aligned} S_{X_+}^{l_1} \geq \underline{S}_{X_+}^{l_1} &= \frac{1}{2(1 + e^{-\mu})} \left\{ e^{-\mu} S_O^{l_1} + e^\mu S_B^{l_1} - 2 \left[ \sqrt{S_O^{l_1} S_B^{l_1}} \right. \right. \\ &\quad \left. \left. + (1 - e^{-\mu})\sqrt{S_O^{l_1}} + \frac{1 - e^{-\mu}}{e^{-\mu}} \left( \sqrt{S_B^{l_1}} \right) \right] \right\}. \end{aligned} \quad (64)$$

Replacing  $l_1$  in Eq. (63) by  $R$  and  $l_1$  in Eq. (64) by  $L$ , we obtain  $\bar{S}_{X_+}^R$  and  $\underline{S}_{X_+}^L$ .

### 4. Estimation of the bound of the phase-flip error rate

Suppose that the number of  $X$  windows in set  $u$  is  $M$ . Among these windows, the number of  $X_+$  windows is  $(1 + e^{-\mu})M/2$  and the number of  $X_-$  windows is  $(1 - e^{-\mu})M/2$ . The phase-flip error rate is defined as follows:

$$e^{\text{ph}} = \frac{n_{X_+}^R + n_{X_-}^L}{n_{X_+}^L + n_{X_+}^R + n_{X_-}^L + n_{X_-}^R}, \quad (65)$$

where  $n_a^d$  represents the number of effective  $a$  windows heralded by detector  $d$  clicking,  $d = L, R$ , and  $a = X_+, X_-$ . We then have the following:

$$\begin{aligned} e^{\text{ph}} &= \frac{n_{X_+}^R - n_{X_+}^L + n_{X_-}^L}{n_X} \\ &= \frac{(1 + e^{-\mu}) \left[ S_{X_+}^R - S_{X_+}^L \right] + 2S_{X_-}^L}{2S_X}, \end{aligned} \quad (66)$$

where  $n_X$  and  $S_X$  are the number of effective events in  $X$  windows and the fraction of effective windows among all

$X$  windows, respectively. We have the following formula for the upper bound of the phase-flip error rate:

$$e^{\text{ph}} \leq \bar{e}^{\text{ph}} = \frac{(1 + e^{-\mu}) \left[ \bar{S}_{X_+}^R - \underline{S}_{X_+}^L \right] + 2S_{\bar{Z}}^L}{2S_{\bar{Z}}}. \quad (67)$$

Here,  $S_{\bar{Z}}$  is the fraction of effective windows among the  $\tilde{Z}$  windows in set  $u$ , which are fake  $X$  windows in the real protocol.  $S_{\bar{Z}}^L$  is the fraction of effective windows heralded by the left detector among all  $\tilde{Z}$  windows in set  $u$ . Since a  $\tilde{Z}$  window in set  $u$  is identical to a  $\tilde{Z}$  window in set  $v$ , they can obtain the values of  $S_{\bar{Z}}$ ,  $S_{\bar{Z}}^L$  by directly observing set  $v$ . The quantities of  $\bar{S}_{X_+}^R$  and  $\underline{S}_{X_+}^L$  can be calculated by Eqs. (63) and (64).

## VI. CONCLUDING REMARK

In this paper, we present a practical SCF protocol that can make a secure QKD over distances longer than 200 km. Though our protocol is source-side-channel free, it is not entirely source-independent, such as the device-independent protocols in Refs. [41–44] and the protocol shown in Ref. [27]. Our protocol makes no assumptions about the side-channel space of the quantum state but imposes conditions in the operational space. The security proof in its present form assumes an exact vacuum state. These conditions can possibly be loosened in future work. One solution may be to change the imperfect vacuum into a probabilistic perfect vacuum via random phase shifts and then use the tagged model. However, we believe that, even in its present form, our protocol has obvious advantages in security.

## ACKNOWLEDGMENTS

We acknowledge the financial support in part by the Ministration of Science and Technology of China through the National Key Research and Development Program of China Grant No. 2017YFA0303901 and National Natural Science Foundation of China Grants No. 11774198, No. 11974204, and No. U1738142.

- 
- [1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, India, 1984), p. 175.  
 [2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).  
 [3] N. Gisin and R. Thew, Quantum communication, *Nat. Photonics* **1**, 165 (2007).  
 [4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).

- [5] R. Renner, Security of quantum key distribution, *Int. J. Quantum Inf.* **6**, 1 (2008).  
 [6] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, *Phys. Rev. A* **51**, 1863 (1995).  
 [7] H. P. Yuen, Quantum amplifiers, quantum duplicators and quantum cryptography, *Quantum Semiclassical Opt.: J. Eur. Opt. Soc. Part B* **8**, 939 (1996).  
 [8] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, *Phys. Rev. Lett.* **85**, 1330 (2000).  
 [9] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, *Phys. Rev. A* **61**, 052304 (2000).  
 [10] N. Lütkenhaus and M. Jähma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack, *New J. Phys.* **4**, 44 (2002).  
 [11] R. König and R. Renner, A de Finetti representation for finite symmetric quantum states, *J. Math. Phys.* **46**, 122108 (2005).  
 [12] M. Christandl, R. König, G. Mitchison, and R. Renner, One-and-a-half quantum de Finetti theorems, *Commun. Math. Phys.* **273**, 473 (2007).  
 [13] H. Inamori, N. Lütkenhaus, and D. Mayers, Unconditional security of practical quantum key distribution, *Eur. Phys. J. D-At., Mol., Opt. Plasma Phys.* **41**, 599 (2007).  
 [14] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, in *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings* (IEEE, Chicago, 2004), p. 136.  
 [15] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.* **91**, 057901 (2003).  
 [16] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).  
 [17] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum key Distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).  
 [18] X.-B. Wang, C.-Z. Peng, J. Zhang, L. Yang, and J.-W. Pan, General theory of decoy-state quantum cryptography with source errors, *Phys. Rev. A* **77**, 042311 (2008).  
 [19] J.-Z. Hu and X.-B. Wang, Reexamination of the decoy-state quantum key distribution with an unstable source, *Phys. Rev. A* **82**, 012331 (2010).  
 [20] X.-B. Wang, L. Yang, C.-Z. Peng, and J.-W. Pan, Decoy-state quantum key distribution with both source errors and statistical fluctuations, *New J. Phys.* **11**, 075006 (2009).  
 [21] M. Koashi, Simple security proof of quantum key distribution based on complementarity, *New J. Phys.* **11**, 045018 (2009).  
 [22] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, *Nature* **509**, 475 (2014).  
 [23] M. Hayashi and R. Nakayama, Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths, *New J. Phys.* **16**, 063009 (2014).  
 [24] H. Chau, Quantum key distribution using qudits that each encode one bit of raw key, *Phys. Rev. A* **92**, 062324 (2015).  
 [25] M. Hayashi, Optimal decoy intensity for decoy quantum key distribution, *J. Phys. A: Math. Theor.* **49**, 165301 (2016).

- [26] H. Chau, Q. Wang, and C. Wong, Experimentally feasible quantum-key-distribution scheme using qubit-like qudits and its comparison with existing qubit- and qudit-based protocols, *Phys. Rev. A* **95**, 022311 (2017).
- [27] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130502 (2012).
- [28] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [29] X.-B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, *Phys. Rev. A* **87**, 012320 (2013).
- [30] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, *Nat. Commun.* **5**, 3732 (2014).
- [31] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Three-intensity decoy-state method for measurement-device-independent quantum key distribution, *Phys. Rev. A* **88**, 062339 (2013).
- [32] F. Xu, H. Xu, and H.-K. Lo, Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution, *Phys. Rev. A* **89**, 052333 (2014).
- [33] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method, *Phys. Rev. A* **91**, 032318 (2015).
- [34] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, *Phys. Rev. A* **93**, 042324 (2016).
- [35] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, *Phys. Rev. Lett.* **111**, 130501 (2013).
- [36] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Phase-Reference-Free Experiment of Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **115**, 160502 (2015).
- [37] 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, Measurement-Device-Independent Quantum Key Distribution over a 404 km Optical Fiber, *Phys. Rev. Lett.* **117**, 190501 (2016).
- [38] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution robust against environmental disturbances, *Optica* **4**, 1016 (2017).
- [39] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, *Nat. Photonics* **9**, 397 (2015).
- [40] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, *Nature* **557**, 400 (2018).
- [41] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)* (1998).
- [42] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, *Phys. Rev. Lett.* **98**, 230501 (2007).
- [43] V. Scarani and R. Renner, Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing, *Phys. Rev. Lett.* **100**, 200501 (2008).
- [44] V. Scarani and R. Renner, in *Workshop on Quantum Computation, Communication, and Cryptography* (Springer, Tokyo, 2008), p. 83.
- [45] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw, *Phys. Rev. A* **85**, 042307 (2012).
- [46] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, *Phys. Rev. A* **98**, 062323 (2018).
- [47] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, Sending-or-not-sending twin-field quantum key distribution in practice, *Sci. Rep.* **9**, 3080 (2019).
- [48] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses, arXiv:1904.00192 (2019).
- [49] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, General theory of sending-or-not-sending twin-field quantum key distribution, arXiv:1904.06331 (2019).
- [50] C.-H. Zhang, C.-M. Zhang, and Q. Wang, Twin-field quantum key distribution with modified coherent states, *Opt. Lett.* **44**, 1468 (2019).
- [51] X.-B. Wang, C.-Z. Peng, and J.-W. Pan, Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source, *Appl. Phys. Lett.* **90**, 031110 (2007).
- [52] More generally, we can use the postselection criterion  $1 - |\cos(\gamma_B - \gamma_A) - \psi_{AB}| \leq |\lambda|$ , since the two-mode real-photon state in general acquires an additional phase difference  $\psi_{AB}$  before arriving in Charlie's station. We can use different values of  $\lambda$  to optimize the key rate if the channel is unstable.
- [53] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, *Nat. Commun.* **5**, 5235 (2014).
- [54] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).
- [55] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283**, 2050 (1999).
- [56] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Phys. Rev. Lett.* **85**, 441 (2000).