Sending-or-not-sending twin-field protocol for quantum key distribution with asymmetric source parameters

Xiao-Long Hu,[1] Cong Jiang,[1] Zong-Wen Yu,[2] and Xiang-Bin Wang[1,3,4,5,*]

[1]*State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China*

[2]*Data Communication Science and Technology Research Institute, Beijing 100191, China*

[3]*Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China Hefei, Anhui 230026, China*

[4]*Jinan Institute of Quantum Technology, SAICT, Jinan 250101, People's Republic of China*

[5]*Shenzhen Institute for Quantum Science and Engineering, and Department of Physics, Southern University of Science and Technology, Shenzhen 518055, China*

(Received 12 August 2019; published 27 December 2019)

The sending-or-not-sending (SNS) protocol of the twin-field quantum key distribution can tolerate large misalignment error and its key rate can exceed the linear bound of repeaterless quantum key distribution. But the original SNS protocol requires the two users to use the same source parameters. Here we propose an SNS protocol with asymmetric source parameters and give the security proof of this protocol. Our asymmetric protocol has a much better performance than that of the original SNS protocol when the channel is asymmetric.

DOI: 10.1103/PhysRevA.100.062337

I. INTRODUCTION

Quantum key distribution (QKD) provides a method for unconditionally secure communication [1–9] between two parties, Alice and Bob. Combined with the decoy-state method [10–15] and the measurement-device-independent QKD (MDIQKD) protocol [16,17], QKD can overcome the security loophole from the nonideal single-photon sources [18–20] and imperfect detection devices [21,22] and has developed rapidly, both in theory [23–40] and experiment [41–63]. The maximum distance of decoy-state MDIQKD has been experimentally increased to 404 kilometers [64]. But the key rate of the BB84, MDIQKD protocol, or any modified version of these protocols cannot exceed the linear bounds of repeaterless QKD, such as the TGW (Takeoka, Guha, and Wilde) bound [65] and the PLOB (Pirandola, Laurenza, Ottaviani, and Banchi) bound [66].

Recently, a new protocol named the twin-field quantum key distribution (TFQKD) was proposed [67] whose key rate dependence on the channel transmittance η is $R \sim O(\sqrt{\eta})$. Following this protocol, many variants of TFQKD were proposed [68–79] and some experiments of TFQKD were demonstrated [80–83]. Among those protocols, one efficient protocol named the sending-or-not-sending (SNS) protocol [68] has the advantages of unconditional security under coherent attacks and it can tolerate large misalignment error, and the SNS protocol with finite data size has been studied [84,85]. However, the security proof of the SNS protocol requires the condition that the two users, Alice and Bob, use the same source parameters, such as the intensities of signal and decoy states and the probability for sending coherent pulses in Z-windows.

Here we propose a SNS protocol where Alice and Bob are not required to use the same source parameters. We give a security proof for this protocol. Then we apply our asymmetric protocol to the case with asymmetric channels, i.e., the channel between Alice and Charlie (we will call it "Alice's channel" for simplicity in this paper) and that between Bob and Charlie (we will call it "Bob's channel" for simplicity in this paper) are not the same. The numerical results show that in this case the key rate of our asymmetric protocol is much higher than that of the original SNS protocol.

This paper is arranged as follows. In Sec. II, we present the procedures of our SNS protocol with asymmetric source parameters. In Sec. III, we give a security proof of our protocol through three virtual protocols and their reductions. We show the results of numerical simulation of the asymmetric SNS protocol compared with the original SNS protocol in Sec. IV. The article ends with some concluding remarks in Sec. V. We give the formulas for key rate calculation in the Appendix.

II. SNS PROTOCOL WITH ASYMMETRIC SOURCE PARAMETERS

A schematic of the asymmetric SNS protocol is shown in Fig. 1. The two legitimate users, Alice and Bob, independently send coherent pulses and vacuum pulses to an untrusted third party (UTP), Charlie. Charlie takes compensation to the pulses, measures them, and announces the measurement results. Then Alice and Bob distill the final key from a set of the pulses according to the announced data. The details of the protocol are shown as follows.

Step 1. In each time window i, *they* (Alice and Bob) independently decide whether this is a decoy window or a signal window. In her (his) decoy window, she (he) randomly chooses one of a few states ρ_{Ak} (ρ_{Bk}), for $k = 0, 1, 2, \ldots$, to send out a decoy pulse to Charlie where $\rho_{A0} = \rho_{B0} = |0\rangle\langle 0|$

*xbwang@mail.tsinghua.edu.cn

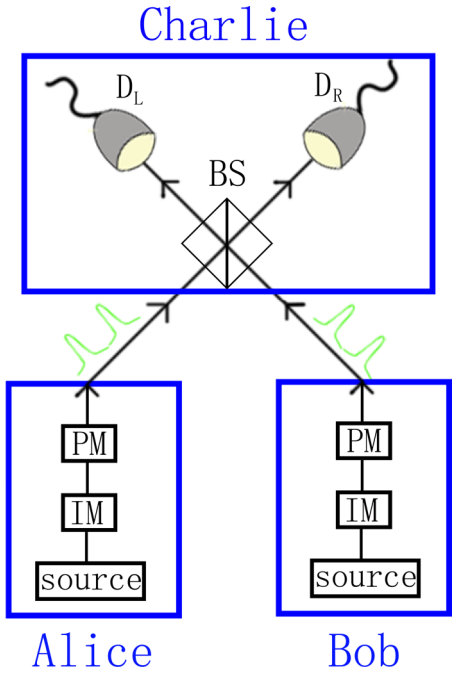

FIG. 1. A schematic of the setup for the asymmetric SNS protocol. IM: intensity modulator; PM: phase modulator; BS: beam splitter; D_L & D_R: single-photon detector in the measurement station of Charlie.

are the vacuum states and ρ_{Ak} (ρ_{Bk}), $k > 0$, are coherent states $|\sqrt{\mu_{Ak}}e^{i\delta_{Ai}+i\gamma_{Ai}}\rangle$ ($|\sqrt{\mu_{Bk}}e^{i\delta_{Bi}+i\gamma_{Bi}}\rangle$). (In this paper, we denote the imaginary unit as i.) In her (his) signal window, she (he) decides to send out to Charlie a signal pulse in the state $|\sqrt{\mu'_A}e^{i\delta_{Ai}+i\gamma_{Ai}}\rangle$ ($|\sqrt{\mu'_B}e^{i\delta_{Bi}+i\gamma_{Bi}}\rangle$) and puts down a bit value 1 (0) with a probability of ϵ_A (ϵ_B), or decides not to send it out, and puts down a bit value 0 (1) with a probability of $1-\epsilon_A$ ($1-\epsilon_B$). Here, δ_{Ai}, δ_{Bi}, γ_{Ai}, and γ_{Bi} are random phases. The global phases γ_{Ai} and γ_{Bi} can be any reference phase and known by anyone. The private phase δ_{Ai} (δ_{Bi}) is a random phase taken by Alice (Bob) secretly. Besides, we request the following mathematical constraint for source parameters:

$$\frac{\mu_{Ak}}{\mu_{Bk}} = \frac{\epsilon_A(1-\epsilon_B)\mu'_A e^{-\mu'_A}}{\epsilon_B(1-\epsilon_A)\mu'_B e^{-\mu'_B}} \tag{1}$$

for each $k > 0$.

Definition. We define a Z-window when both of *them* determine signal windows and an X-window when both of *them* determine decoy windows. Among X-windows, we define $X^{(k)}$-windows when Alice chooses the intensity μ_{Ak} and Bob chooses the intensity μ_{Bk}.

As the major result of this work, this constraint guarantees the security of the asymmetric SNS protocol. The real protocol here is actually the same as that in Ref. [68] except for this mathematical constraint, and the virtual protocols for security proof will use different types of entangled states.

Intuitively, the constraint in Eq. (1) guarantees that the density matrix of the untagged state (two-mode single-photon state) in X-windows is the same as that of the untagged state in Z-windows so that *they* can use the error rate in X-windows to estimate the phase-flip error rate in Z-windows. In MDIQKD, no matter what asymmetric source parameters are chosen, the states of single-photon pairs are always identical in X basis and Z basis, and hence the virtual protocol of entanglement swapping and purification always holds [25,32,33].

For ease of presentation, we will omit the subscript i if it does not cause any confusion. But keep in mind that all δ_A, δ_B, γ_A, and γ_B are chosen differently in different time windows.

Note: The sufficient condition for security is that all decoy pulses satisfy Eq. (1). But in a specific decoy-state method, e.g., our four-intensity decoy-state method in the Appendix, not all μ_{Am} and μ_{Bm} are required to satisfy Eq. (1). Some details can be found in the Appendix.

Step 2. Charlie is supposed to measure all twin fields with a beam splitter after taking phase compensation and announce the measurement outcome.

Note: Charlie is expected to remove phases γ_A and γ_B by phase compensation. His action affects only the key rate and has no influence on the security of the protocol.

Definition. We define an *effective event* when one and only one of Charlie's detector clicks, and the corresponding window is called an *effective window*.

Step 3. They announce each one's decoy windows and signal windows. And *they* announce the intensities that they choose in each decoy window and the private phases δ_A and δ_B in each decoy window. The data of effective events is kept for parameter estimation and key distillation.

Given that δ_A (δ_B) is randomized, whenever Alice (Bob) sends a coherent state with intensity μ'_A (μ'_B), this coherent state can be equivalently regarded as a state with the density matrix $\sum_{k=0}^{\infty}\frac{e^{-\mu'_A}\mu'^k_A}{k!}|k\rangle\langle k|$ ($\sum_{k=0}^{\infty}\frac{e^{-\mu'_B}\mu'^k_B}{k!}|k\rangle\langle k|$) in the photon-number space, which is a classical mixture of different photon-number states only. Hence among all Z-windows, we can define a set of Z_1-windows in which one and only one of *them* decides to send and she (he) actually sends a single-photon state. *They* do not know which time window is a Z_1-window, but *they* can calculate the number of Z_1-windows in an experiment.

Among all X-windows, we define a set of $\tilde{X}$-windows in which *they* choose the intensities μ_{Ak} and μ_{Bk} with the same k and the phase shifts δ_A and δ_B satisfy the restriction

$$1 - |\cos(\delta_A - \delta_B + \Delta\varphi)| \leqslant |\lambda|. \tag{2}$$

Here the values $\Delta\varphi$ and λ are some values determined by Alice and Bob according to the result of channel testing and calibration in the experiment to obtain a satisfactory key rate, and the value of $\Delta\varphi$ can be different from time to time. Similarly, among $X^{(k)}$-windows, we define a set of $\tilde{X}^{(k)}$ in which the phase shifts δ_A and δ_B satisfy the restriction in Eq. (2).

Step 4. They randomly choose some events from the effective Z-windows to do the error test. A bit-flip error occurs when Alice's bit value is different from Bob's in a Z-window. *They* discard the test bits, and the remaining events from effective Z-windows will be distilled for the final key.

Step 5. Based on the measurement outcome in effective X-windows, *they* calculate n_1, the number of effective events in Z_1-windows. Based on the measurement outcome and the announced values of δ_A and δ_B in effective $\tilde{X}$-windows, *they* calculate e_1^{ph}, the phase-flip error rate of the states in effective Z_1-windows.

Note: In effective $\tilde{X}$-windows, an error occurs when
(1) the left detector clicks and $\cos(\delta_A - \delta_B) < 0$ or
(2) the right detector clicks and $\cos(\delta_A - \delta_B) > 0$.

Given this definition, *they* can observe the error rates in $\tilde{X}$-windows for each intensity of input light. With this, *they* can estimate e_1^{ph} through the decoy-state analysis which requests them to observe the counting rates of various intensities of input light. As proved in Ref. [68], the decoy-state method can applied to our protocol as if the phases δ_A and δ_B were not announced. In the asymptotic case that there are decoy states with infinite different intensities, *they* can obtain the exact value of e_1^{ph}. In the case that there are decoy states with finite different intensities, *they* can obtain the upper bound of e_1^{ph}.

Note: The Appendix shows the four-intensity method of this protocol. In this case, the formulas for n_1 and e_1^{ph} are given in Eqs. (A2)–(A5).

Step 6. They perform the postprocessing and obtain the final key with length

$$N_f = n_1\left[1 - H\left(e_1^{ph}\right)\right] - f n_t H(E_Z), \tag{3}$$

where f is the correction efficiency, n_t is the number of effective Z-windows, and E_Z is the bit-flip error rate in effective Z-windows, which can be obtained directly in the error test in step 4. If in the error test Alice and Bob choose n_{test} effective events and there are n_{error} bit-flip error events, then $E_Z = n_{\text{error}}/n_{\text{test}}$. Details for calculating the length of the final key (or the key rate) with the four-intensity decoy-state method are presented in the Appendix.

Note: If we set $\epsilon_A = \epsilon_B$ and $\mu'_A = \mu'_B$, this protocol is actually the same as the original SNS protocol in Ref. [68].

III. SECURITY PROOF WITH VIRTUAL PROTOCOLS AND REDUCTION

A. Introduction of the ancillary photons and the extended states

Similarly to the security proof in Ref. [68], we use the idea of entanglement distillation with ancillary photons to prove the security of our protocol. Image that in a Z-window, if Alice (Bob) decides to send a coherent state ρ_A (ρ_B) to Charlie, she (he) puts down a local ancillary qubit in the state $|1\rangle$ ($|0\rangle$), and if Alice (Bob) decides not to send, she (he) puts down a local ancillary qubit in state $|0\rangle$ ($|1\rangle$). To Alice (Bob), state $|1\rangle$ corresponds to the bit value 1 (0), and state $|0\rangle$ corresponds to bit value 0 (1). We define subspace $\mathcal{T}$ for the subspace of the sent-out states and $\mathcal{A}n$ for the subspace of the local ancillary states. Therefore, the extended state in the complex space $\mathcal{T} \otimes \mathcal{A}n$ in the Z-window can be written as

$$\begin{aligned}\Omega = {} & \epsilon_A\epsilon_B(\rho_A\tilde{\otimes}\rho_B)\otimes|11\rangle\langle 11| \\ & + \epsilon_A(1-\epsilon_B)(\rho_A\tilde{\otimes}|0\rangle\langle 0|)\otimes|10\rangle\langle 10| \\ & + (1-\epsilon_A)\epsilon_B(|0\rangle\langle 0|\tilde{\otimes}\rho_B)\otimes|01\rangle\langle 01| \\ & + (1-\epsilon_A)(1-\epsilon_B)(|0\rangle\langle 0|\tilde{\otimes}|0\rangle\langle 0|)\otimes|00\rangle\langle 00|. \end{aligned} \tag{4}$$

Here both symbols $\otimes$ and $\tilde{\otimes}$ are for a tensor product, and $\tilde{\otimes}$ is the tensor product inside $\mathcal{T}$, and $\otimes$ is the tensor product between $\mathcal{T}$ and $\mathcal{A}n$. The states on the left side of $\otimes$ are in $\mathcal{T}$ and we name them *real-photon states*. The states on the right side of $\otimes$ are in $\mathcal{A}n$ and we name them *ancillary-photon states*. Since the private phases δ_A and δ_B in Z-windows are kept secret all the time, the coherent states ρ_A and ρ_B are actually phase-randomized coherent states whose density matrices are

$$\rho_k = \sum_{n=0}^{\infty} \frac{e^{-\mu'_k}\mu'^n_k}{n!}|n\rangle\langle n| = \mu'_k e^{-\mu'_k}|1\rangle\langle 1| + (1-\mu'_k e^{-\mu'_k})\bar{\rho}_k, \tag{5}$$

with $k = A, B$ and

$$\bar{\rho}_k = \frac{1}{1-\mu'_k e^{-\mu'_k}} \sum_{n\neq 1} \frac{e^{-\mu'_k}\mu'^n_k}{n!}|n\rangle\langle n|. \tag{6}$$

So the extended state in the Z-window can be written in another form:

$$\Omega = \sum_{r=1}^{4} q_r \Omega_r \tag{7}$$

and

$$\begin{aligned}\Omega_1 = {} & C_1[\epsilon_A(1-\epsilon_B)\mu'_A e^{-\mu'_A}|10\rangle\langle 10|\otimes|10\rangle\langle 10| \\ & + \epsilon_B(1-\epsilon_A)\mu'_B e^{-\mu'_B}|01\rangle\langle 01|\otimes|01\rangle\langle 01|] \\ \Omega_2 = {} & C_2[\epsilon_A(1-\epsilon_B)(1-\mu'_A e^{-\mu'_A})(\bar{\rho}_A\tilde{\otimes}|0\rangle\langle 0|)\otimes|10\rangle\langle 10| \\ & + \epsilon_B(1-\epsilon_A)(1-\mu'_B e^{-\mu'_B})(|0\rangle\langle 0|\tilde{\otimes}\bar{\rho}_B)\otimes|01\rangle\langle 01|] \\ \Omega_3 = {} & |00\rangle\langle 00|\otimes|00\rangle\langle 00| \\ \Omega_4 = {} & (\rho_A\tilde{\otimes}\rho_B)\otimes|11\rangle\langle 11|, \end{aligned} \tag{8}$$

where C_1 and C_2 are some normalization factors. With the condition in Eq. (1), Ω_1, the target state we used to prove the security can be written as

$$\Omega_1 = C^2(\mu_{A1}|10\rangle\langle 10|\otimes|10\rangle\langle 10| + \mu_{B1}|01\rangle\langle 01|\otimes|01\rangle\langle 01|), \tag{9}$$

with

$$C = 1/\sqrt{\mu_{A1}+\mu_{B1}}. \tag{10}$$

In $X^{(k)}$-windows, the two-mode states sent by *them* are

$$\rho_{X^{(k)}} = |\beta_k\rangle\langle\beta_k|, \tag{11}$$

where

$$|\beta_k\rangle = |\sqrt{\mu_{Ak}}e^{i\delta_A + i\gamma_A}\rangle|\sqrt{\mu_{Bk}}e^{i\delta_B + i\gamma_B}\rangle. \tag{12}$$

In our protocol, the states in the Z-windows are actually classical mixtures of Ω_1, Ω_2, Ω_3, and Ω_4. In the security proof, we first show the security of the protocol with only state Ω_1 and then show the security of the protocol with Ω by the tagged model [10,11].

B. Virtual Protocol 1

Definition. We have defined an *effective event* in the protocol—an event when one and only one of Charlie's detector clicks. An *effective ancillary photon* is an ancillary photon corresponding to an effective event.

1. Preparation stage

For each time window i, *they* preshare the classical information about whether this time window is an X-window or

Z-window. *They* preshare an extended state

$$\Omega_0 = |\Psi\rangle\langle\Psi|, \tag{13}$$

where

$$|\Psi\rangle = C(\sqrt{\mu_{A1}}e^{i\gamma_A}|10\rangle \otimes |10\rangle + \sqrt{\mu_{B1}}e^{i\gamma_B}|01\rangle \otimes |01\rangle) \tag{14}$$

and γ_A and γ_B are announced publicly. (Remember that γ_A and γ_B vary in different time windows).

In the time window i which is a Z-window, through discussion by a secret channel, Alice chooses a random phase δ_A and Bob chooses a random phase δ_B, which satisfy the restriction in Eq. (2). Then *they* take phase shifts δ_A and δ_B on their own real photons, respectively. In the time window i which is a X-window, *they* take random and independent phase shifts δ_A and δ_B on their own real photons, respectively. After the phase shifts, the extended state changes into

$$\Omega_Z = |\Psi'\rangle\langle\Psi'|, \ \Omega_X = |\Psi'\rangle\langle\Psi'| \tag{15}$$

and

$$\begin{aligned}|\Psi'\rangle = C(&\sqrt{\mu_{A1}}e^{i\gamma_A+i\delta_A}|10\rangle \otimes |10\rangle \\ &+ \sqrt{\mu_{B1}}e^{i\gamma_B+i\delta_B}|01\rangle \otimes |01\rangle).\end{aligned} \tag{16}$$

Among all X-windows, we define a set of $\tilde{X}$-windows in which the phase shifts δ_A and δ_B satisfy the restriction Eq. (2). The states in Z-windows are not identical to those in X-windows, but they are identical to those in $\tilde{X}$-windows.

Besides, we define real-photon states $|\chi^0\rangle$ and $|\chi^1\rangle$ for any time window:

$$\begin{aligned}|\chi^0\rangle &= C(\sqrt{\mu_{A1}}e^{i\gamma_A+i\delta_A}|10\rangle + \sqrt{\mu_{B1}}e^{i\gamma_B+i\delta_B}|01\rangle) \\ |\chi^1\rangle &= C(\sqrt{\mu_{A1}}e^{i\gamma_A+i\delta_A}|10\rangle - \sqrt{\mu_{B1}}e^{i\gamma_B+i\delta_B}|01\rangle) \\ &\text{if} \quad \cos(\delta_A - \delta_B) \geqslant 0\end{aligned} \tag{17}$$

or

$$\begin{aligned}|\chi^0\rangle &= C(\sqrt{\mu_{A1}}e^{i\gamma_A+i\delta_A}|10\rangle - \sqrt{\mu_{B1}}e^{i\gamma_B+i\delta_B}|01\rangle) \\ |\chi^1\rangle &= C(\sqrt{\mu_{A1}}e^{i\gamma_A+i\delta_A}|10\rangle + \sqrt{\mu_{B1}}e^{i\gamma_B+i\delta_B}|01\rangle) \\ &\text{if} \quad \cos(\delta_A - \delta_B) < 0.\end{aligned} \tag{18}$$

2. Protocol

V1-1: In any Z-window (X-window), *they* send the real photons of Ω_Z (Ω_X) defined in Eq. (15) to Charlie and keep the ancillary photons locally.

V1-2: Charlie measures the real photons from Alice and Bob with a beam splitter after taking phase compensation according to the strong reference lights with phases γ_A and γ_B. He announces his measurement outcome and then *they* announce the values of δ_A and δ_B of all X-windows. With the preshared information of X- and Z-windows, the measurement outcome, and the announced values of δ_A and δ_B, *they* can obtain effective Z-windows and effective $\tilde{X}$-windows. The data of other time windows will be discarded.

Definition. After step V1-2, the remaining effective events can be divided into eight subsets according to the window information (Z-window or X-window), the clicking detector (the left L or the right R), and the sign of $\cos(\delta_A - \delta_B)$ (positive $+$ or negative $-$). These subsets are labeled as $\Gamma_{(a,d)}$, where $\Gamma = \tilde{X}, Z$, $a = +, -$, and $d = L, R$. For example, the subset $Z_{(-,R)}$ is the set of effective Z-windows when the right detector clicks and $\cos(\delta_A - \delta_B) < 0$. Correspondingly, the effective ancillary photons can be divide into eight subsets labeled as $\mathcal{A}_{\Gamma_{(a,d)}}$.

V1-3: *They* check the phase-flip error rate $E_{(a,d)}$ of the set $\mathcal{A}_{\tilde{X}_{(a,d)}}$, where $a = +, -$ and $d = L, R$. Since the effective Z-windows are identical to the effective $\tilde{X}$-windows, the phase-flip error rate of $\mathcal{A}_{\tilde{X}_{(a,d)}}$ should be the same as that of $\mathcal{A}_{Z_{(a,d)}}$ (asymptotically).

Note: The state $|\Psi'\rangle$ in Eq. (16) can be written in another form:

$$|\Psi'\rangle = \frac{1}{\sqrt{2}}(|\chi^0\rangle \otimes |\Phi^0\rangle + |\chi^1\rangle \otimes |\Phi^1\rangle), \ \text{if } a = + \tag{19}$$

or

$$|\Psi'\rangle = \frac{1}{\sqrt{2}}(|\chi^1\rangle \otimes |\Phi^0\rangle + |\chi^0\rangle \otimes |\Phi^1\rangle), \ \text{if } a = -, \tag{20}$$

where $|\Phi^k\rangle, k = 0, 1,$ are two-mode states of ancillary photons:

$$|\Phi^0\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle), |\Phi^1\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle). \tag{21}$$

To obtain the phase-flip error rate $E_{(a,d)}$ of the set $\mathcal{A}_{\tilde{X}_{(a,d)}}$, each ancillary photon of this set is measured in the basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$ and there are $n^{(0)}_{(a,d)}$ outcomes of $|\Phi^0\rangle\langle\Phi^0|$ and $n^{(1)}_{(a,d)}$ outcomes of $|\Phi^1\rangle\langle\Phi^1|$. The phase-flip error rate $E_{(a,d)}$ of $\mathcal{A}_{\tilde{X}_{(a,d)}}$ is defined as

$$E_{(a,d)} = \frac{\min\left(n^{(0)}_{(a,d)}, n^{(1)}_{(a,d)}\right)}{n_{(a,d)}}, \tag{22}$$

where $n_{(a,d)} = n^{(0)}_{(a,d)} + n^{(1)}_{(a,d)}$ is the number of the ancillary photons in $\mathcal{A}_{\tilde{X}_{(a,d)}}$.

V1-4: With the estimated value of $E_{(a,d)}$, *they* can purify the ancillary photons in $\mathcal{A}_{Z_{(a,d)}}$ with $(a, d) = (+, R), (+, L), (-, R), (-, L)$ separately. After purification, *they* obtain ancillary photons in (almost 100%) pure single-photon entangled states $|\Phi^0\rangle$ (or $|\Phi^1\rangle$). Then *they* perform local measurement on their own ancillary photons and obtain the final key. Alice (Bob) puts down a bit value 0 (1) or 1 (0) when her (his) measurement outcome is $|0\rangle\langle 0|$ or $|1\rangle\langle 1|$.

Note 1—Security. The security of the final key is based on the faithfulness of the purification. If *they* estimate the error rate $E_{(a,d)}$ of a set of ancillary photons exactly, *they* can purify these ancillary photons to get pure entangled photons. Although Charlie measured the real photons and *they* selected the set of ancillary photons based on his announced measurement outcomes, *they* check the phase-flip error rate of these photons by themselves. Since the extended states of effective $\tilde{X}$-windows are identical to those of effective Z-windows, the phase-flip error rate of $\mathcal{A}_{\tilde{X}_{(a,d)}}$ is exactly the same as that of $\mathcal{A}_{Z_{(a,d)}}$ statistically. *They* can obtain the phase-flip error rate in $\mathcal{A}_{Z_{(a,d)}}$ by testing the ancillary photon in $\mathcal{A}_{\tilde{X}_{(a,d)}}$ and then perform the purification to $\mathcal{A}_{Z_{(a,d)}}$. As a result, the security of the key does not rely on Charlie's honesty.

Note 2—Estimation of the phase-flip error rate. According to the definition of $E_{(a,d)}$ in Eq. (22), *they* have to measure the ancillary photons in the basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$. It's easy to prove that *they* can perform local measurement in the basis $\{|\pm x\rangle =$

$(|0\rangle \pm |1\rangle)/\sqrt{2}\}$ and check the parity of the outcome instead of measuring in the basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$. Explicitly, their outcome with even parity ($|x+\rangle|x+\rangle$ or $|x-\rangle|x-\rangle$) corresponds to the outcome $|\Phi^0\rangle$ and that with odd parity ($|x+\rangle|x-\rangle$ or $|x-\rangle|x+\rangle$) corresponds to the outcome $|\Phi^1\rangle$.

Note 3—Reduction of the preshare states in X-windows. Since measurement in the basis $\{|\pm x\rangle\}$ is a local operation on the ancillary photons, it makes no difference whether *they* measure their ancillary photons after sending the real photons or before that. So *they* can measure the ancillary photons before the protocol starts and label this time window an X_0-window if the outcome is even parity, or label it an X_1-window if the outcome is odd parity. Then *they* prepare and send the real photon in the state

$$|\chi^+\rangle = C(\sqrt{\mu_{A1}}e^{i\gamma_A+i\delta_A}|10\rangle + \sqrt{\mu_{B1}}e^{i\gamma_B+i\delta_B}|01\rangle) \tag{23}$$

in an X_0-window or prepare and send that in the state

$$|\chi^-\rangle = C(\sqrt{\mu_{A1}}e^{i\gamma_A+i\delta_A}|10\rangle - \sqrt{\mu_{B1}}e^{i\gamma_B+i\delta_B}|01\rangle) \tag{24}$$

in an X_1-window.

Alternatively, *they* can start with the information of X_0-windows and X_1-windows and the states in Eqs. (23) and (24). *They* prepare and send real photons in the state $|\chi^+\rangle$ in X_0-windows or in the state $|\chi^-\rangle$ in X_1-windows. In this way, the ancillary photons in X-windows in the above virtual protocol are not necessary, and the formula of phase-flip error rate should be changed correspondingly. We introduce a symbol $\tilde{X}_{(a,b,d)}$ for the set of effective time windows, which satisfies the restriction in Eq. (2), with joint events a, b, d where

Event a ($a = +, -$): the sign of $\cos(\delta_A - \delta_B)$.

Event b ($b = 0, 1$): this times window is an X_b-window.

Event d ($d = L, R$): the d-detector clicks and the other does not click.

And we also introduce $n_{\tilde{X}_{(a,b,d)}}$ for the number of time windows in the set $\tilde{X}_{(a,b,d)}$. Therefore, we have

$$n^{(b)}_{(a,d)} = N_{\tilde{X}_{(a,b,d)}} \tag{25}$$

and

$$E_{(a,d)} = \frac{\min\left(N_{\tilde{X}_{(a,0,d)}}, N_{\tilde{X}_{(a,1,d)}}\right)}{n_{(a,d)}}. \tag{26}$$

This reduction of X-windows leads to the Virtual Protocol 2.

C. Virtual Protocol 2

1. Preparation stage

For each time window i, *they* preshare the classical information about whether this time window is an X_0-window, an X_1-window, or a Z-window. *They* preshare an extended state Ω_Z in Eq. (15) for Z-windows, a real-photon state $|\chi^+\rangle$ for X_0-windows, or a real state $|\chi^-\rangle$ for X_1-windows.

2. Protocol

V2-1: In any Z-window, *they* send out the real photons of Ω_Z to Charlie and keep the ancillary photons locally. In any X_0-window (X_1-window), *they* send $|\chi^+\rangle$ ($|\chi^-\rangle$) to Charlie.

V2-2: Charlie measures the real photons from Alice and Bob with a beam splitter after taking phase compensation according to the strong reference lights with phases γ_A and γ_B. He announces his measurement outcome and then *they* announce the values of δ_A and δ_B of all X-windows.

V2-3: *They* check the phase-flip error rate $E_{(a,d)}$ by the set $\tilde{X}_{(a,0,d)}$ and $\tilde{X}_{(a,1,d)}$, where $a = +, -$ and $d = L, R$.

V2-4: *They* purify the ancillary photons in $\mathcal{A}_{Z_{(a,d)}}$ with $(a, d) = (+, R), (+, L), (-, R), (-, L)$ separately with the estimated value of $E_{(a,d)}$. Then *they* perform local measurement on their own ancillary photons and obtain the final key.

Note: Reduction of preshared states in X-windows

Reduction 1. The real-photon states with $a = +$ ($a = -$) in X_0-windows are actually identical to those with $a = -$ ($a = +$) in X_1-windows, e.g.,

$$\rho_{(+,0)} = \rho_{(-,1)}, \rho_{(-,0)} = \rho_{(+,1)}. \tag{27}$$

So we can conclude that $N_{\tilde{X}_{(a,0,d)}} = N_{\tilde{X}_{(\bar{a},1,d)}}$, where $\bar{a}$ stands for the opposite sign of a. This means that all the values $N_{\tilde{X}_{(a,1,d)}}$ in the phase-flip error rate in Eq. (26) can be replaced by $N_{\tilde{X}_{(\bar{a},0,d)}}$ so that X_1-windows are not necessary. *They* can just use the data from X_0-windows to estimate the phase-flip error rate, and no one else will find any difference. Therefore, *they* use only X_0-windows and send only the state $|\chi^+\rangle$ in X-windows. The number of effective events from the state $|\chi^+\rangle$ and the joint events a, d (with $a = +, -; d = L, R$) is denoted as $n_{\tilde{X}_{(a,d)}}$. The formula of the phase-flip error rate should be changed into

$$E_{(a,d)} = \frac{\min\left(n_{\tilde{X}_{(a,d)}}, n_{\tilde{X}_{(\bar{a},d)}}\right)}{n_{(a,d)}}, \tag{28}$$

where the formula for $n_{(a,d)}$ should be changed into $n_{(a,d)} = n_{\tilde{X}_{(a,d)}} + n_{\tilde{X}_{(\bar{a},d)}}$.

Reduction 2. All the effective ancillary photons in Z-windows can be purified in one batch. The phase-flip error rate is

$$\begin{aligned} E^{ph} &= \frac{\sum_{a,d}\min\left(n_{\tilde{X}_{(a,d)}}, n_{\tilde{X}_{(\bar{a},d)}}\right)}{\sum_{a,d} n_{(a,d)}} \\ &= \frac{2\sum_{d}\min\left(n_{\tilde{X}_{(+,d)}}, n_{\tilde{X}_{(-,d)}}\right)}{2n_1}, \end{aligned} \tag{29}$$

where $n_1 = n_{\tilde{X}_{(+,L)}} + n_{\tilde{X}_{(+,R)}} + n_{\tilde{X}_{(-,L)}} + n_{\tilde{X}_{(-,R)}}$ is the total number of effective events in $\tilde{X}$-windows. Using the relations that $n_{\tilde{X}_{(-,L)}} \geqslant \min(n_{\tilde{X}_{(+,L)}}, n_{\tilde{X}_{(-,L)}})$ and $n_{\tilde{X}_{(+,R)}} \geqslant \min(n_{\tilde{X}_{(+,R)}}, n_{\tilde{X}_{(-,R)}})$, the phase-flip error rate can be bounded by

$$E^{ph} \leqslant \frac{n_{\tilde{X}_{(-,L)}} + n_{\tilde{X}_{(+,R)}}}{n_1}. \tag{30}$$

In this formula for the phase-flip error rate, we only need the total number of effective events in $\tilde{X}$-windows and the number of these two kinds of effective events:

(1) The left detector clicks and $\cos(\delta_A - \delta_B) < 0$;

(2) The right detector clicks and $\cos(\delta_A - \delta_B) \geqslant 0$.

Therefore, we can define these two kinds of effective events as *error events* and the corresponding time windows are defined as *error windows*. If *they* set the value of λ small enough and Charlie perform the compensation honestly, *they* may get few error events so that the phase-flip error rate will be quite low and the key rate will be high.

Reduction 3. The density matrix in Eq. (11) with randomized δ_A and δ_B can be written as the classical mixture of a set

of states $\{|\psi_l^{(k)}\rangle\}$:

$$\rho_{X^{(k)}} = \sum_l p_l^{(k)} |\psi_l^{(k)}\rangle\langle\psi_l^{(k)}| \tag{31}$$

with

$$|\psi_l^{(k)}\rangle = D_l^{(k)} \sum_{n=0}^{l} \frac{(\sqrt{\mu_{Ak}} e^{i\delta_A + i\gamma_A})^n}{\sqrt{n!}} \frac{(\sqrt{\mu_{Bk}} e^{i\delta_B + i\gamma_B})^{l-n}}{\sqrt{(l-n)!}} |n, l-n\rangle, \tag{32}$$

where $D_l^{(k)}$ are some normalization factors and $|\psi_1^{(k)}\rangle$ is exactly $|\chi^+\rangle$ when the condition in Eq. (1) is satisfied. So *they* do not need to preshare the state $|\chi^+\rangle$. *They* can send the phase-randomized coherent state $|\sqrt{\mu_{Ak}} e^{i\delta_A + i\gamma_A}\rangle$ and $|\sqrt{\mu_{Bk}} e^{i\delta_B + i\gamma_B}\rangle$ to Charlie in X-windows and then use the decoy-state method to estimate the bound of the phase-flip error rate of $|\chi^+\rangle$, e_1^{ph}.

D. Virtual Protocol 3

1. Preparation stage

For each time window i, *they* preshare the classical information about whether this time window is an X window or a Z-window. *They* preshare an extended state Ω_Z in Eq. (15) for Z-windows.

2. Protocol

V3-1: In any Z-window, *they* send out the real photons of Ω_Z to Charlie and keep the ancillary photons locally. In any X-window, Alice (Bob) sends a coherent state $|\sqrt{\mu_{Ak}} e^{i\delta_A + i\gamma_A}\rangle$ ($|\sqrt{\mu_{Bk}} e^{i\delta_B + i\gamma_B}\rangle$) with random δ_A and γ_A (δ_B and γ_B) to Charlie.

V3-2: Charlie measures the real photons from Alice and Bob with a beam splitter after taking phase compensation according to the strong reference lights with phases γ_A and γ_B. He announces his measurement outcome, and then *they* announce the values of δ_A and δ_B of all X-windows.

V3-3: *They* apply decoy-state method with the data of the effective $\tilde{X}$-windows to estimate the phase-flip error rate e_1^{ph}.

V3-4: *They* purify the ancillary photons in the effective Z-windows with the estimated value of e_1^{ph}. Then *they* perform local measurement on their own ancillary photons and obtain the final key.

Note 1: Reduction of preshared states in Z-windows

Reduction 1. The state Ω_Z with the restriction Eq. (2) is identical to Ω_Z without the restriction Eq. (2). If we regard all Z-windows as a whole, the condition in Eq. (2) can be loosened, which means that the phase shifts δ_A and δ_B to the real photons can be randomized in the range $[0, 2\pi)$ independently. In this way, *they* do not need any mutual information about the phase shifts δ_A and δ_B.

Reduction 2. The process that *they* purify the effective ancillary photons in Z-windows and then perform local measurement on them is equivalent to the process that *they* measure these ancillary photons in the photon-number basis and then do classical distillation to the classical data, which is called quasipurification [3]. In the latter process, the state in Z-window is

$$\Omega_Z' = C^2(\mu_{A1}|10\rangle\langle 10| \otimes |10\rangle\langle 10| + \mu_{B1}|01\rangle\langle 01| \otimes |01\rangle\langle 01|), \tag{33}$$

which is equivalent to the state Ω_1 in Eq. (9). This means that the protocol can just start with state Ω and apply the tagged model to distill the final key from the effective events using state Ω_1. The length of the final key should be

$$n_f = n_1\left[1 - H\left(e_1^{ph}\right)\right] - n_t H(E_Z), \tag{34}$$

where n_1 is the number of effective events with state Ω_1 estimated by the decoy-state method, n_t is the number of effective events in Z-windows, and E_Z is the bit-flip error rate of n_t. A bit-flip error occurs when Alice's bit value is different from Bob's in a Z-window.

Note 2: Reduction of preshared information of time windows

Alice (Bob) determines a signal window with a probability of p_A^Z (p_B^Z) and determines a decoy window with intensity μ_{Ak} (μ_{Bk}) with a probability of p_{Ak}^X (p_{Bk}^X), where $p_A^Z + \sum_k p_{Ak}^X = 1$ ($p_B^Z + \sum_k p_{Bk}^X = 1$). A Z-window is defined when both of *them* determine signal windows, and an X-window is defined when both of *them* determine decoy windows. Other time windows are regarded as mismatch windows and they will be discarded. In this way, *they* do not need to preshare any information of time windows, and the states in Z-windows and X-windows are Ω and $\rho_{X^{(k)}}$, respectively. With the reductions above, the virtual protocol is equivalent to our asymmetric SNS protocol.

IV. NUMERICAL SIMULATION WITH ASYMMETRIC CHANNELS

With the constraint in Eq. (1), we can do the optimization of the SNS protocol with asymmetric channels. Some recent research also studies the asymmetric TFQKD [78,86,87].

Here we present the results of numerical simulation of different SNS protocols in the case that the channels are asymmetric, i.e., Alice' channel and Bob's channel are different, e.g., they have different channel losses.

The original SNS with the asymmetric channels can be modified a little to fit the asymmetric channels, which we call "the modified SNS protocol" in the following. Consider the case that the original SNS protocol is applied to the asymmetric channels, when *they* use the same source, the intensities of the pulses interfering at the beam-splitter will differ a lot due to different channel transmittances, which will cause a high error rate in X-windows and therefore enhance the phase-flip error rate of a single photon, e_1^{ph}. In the modified SNS protocol, *they* still use the same source parameters, but Charlie adds an extra loss to one of the channels to make the transmittances of two channels the same. Explicitly, if the transmittance of Alice's channel, η_A, is larger than that

TABLE I. Devices' parameters used in numerical simulations. N_t is the total number of pulse pairs; e_d is the misalignment error in the X windows; d is the dark count rate of each detector at the UTP; η_d is the detection efficiency of each detector at the UTP; f_e is the error correction inefficiency. ξ is the failure probability in the parameter estimation, and α is the channel loss.

N_t	e_d	d	η_d	f_e	ξ	α
10^{13}	5%	10^{-10}	50%	1.1	10^{-10}	0.2 dB/km

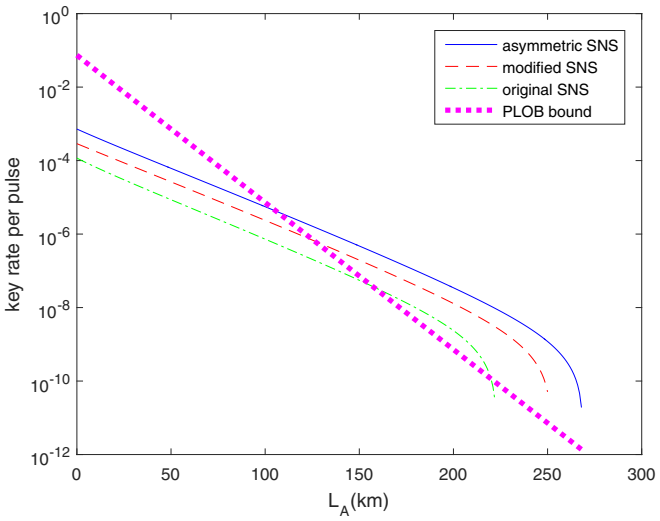

FIG. 2. The optimized key rates (per pulse pair) vs transmission distance between Alice and Charlie with three different SNS protocols. Here the difference in length between Alice's and Bob's channels is fixed at 50 km.

of Bob's channel, η_B, Charlie adds an extra loss $1-\eta_B/\eta_A$ to Alice's channel to make the transmittances of these two channels η_B. On the contrary, if $\eta_A < \eta_B$, Charlie adds an extra loss $1-\eta_A/\eta_B$ to Bob's channel. Since Charlie's action does not affect the security, the security of the modified SNS protocol is guaranteed automatically.

We show the numerical results of the optimal key rate of the original, the modified, and the asymmetric SNS protocols with the asymmetric channels. The effect of the finite data size has been considered in our calculation. The device parameters used in the simulation are listed in Table I. In Figs. 2 and 3, we show the optimal key rates of three protocols with the difference in length between the two channels ($L_B - L_A$) fixed at 50 and 100 km, respectively. In the figures, we have also compared our results with the linear bound of the repeaterless

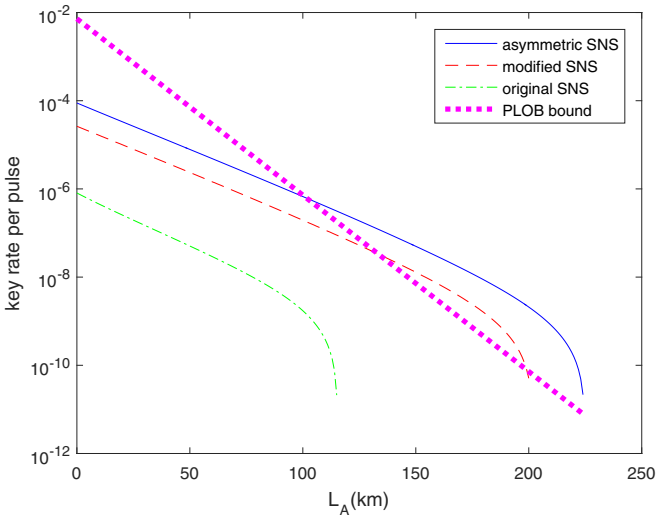

FIG. 3. The optimized key rates (per pulse pair) vs transmission distance between Alice and Charlie with three different SNS protocols. Here the difference in length between Alice's and Bob's channels is fixed at 100 km.

TABLE II. The optimal key rates with different SNS protocols. The device parameters used in the simulation are listed in Table I.

L_A (km)	L_B (km)	Asymmetric SNS	Modified SNS	Original SNS
0	50	7.21×10^{-4}	2.89×10^{-4}	1.17×10^{-4}
150	200	4.73×10^{-7}	1.95×10^{-7}	5.52×10^{-8}
250	300	1.19×10^{-9}	5.08×10^{-11}	0
0	100	8.89×10^{-5}	2.63×10^{-5}	8.09×10^{-7}
100	200	6.71×10^{-7}	1.95×10^{-7}	1.73×10^{-9}
200	300	2.09×10^{-9}	5.08×10^{-11}	0

QKD. There are excellent theoretical linear bounds for the key rate of a repeaterless QKD, such as the famous TGW bound [65] and the PLOB bound [66]. Also, we show some details of the optimal key rates with different SNS protocols in Table II. It is easy to find that in the asymmetric channels, the performance of the asymmetric SNS protocol is much better than that of the other two protocols, especially when the difference in length between Alice's and Bob's channels is large.

V. CONCLUSION

In this paper, we propose an SNS protocol with asymmetric source parameters and give a security proof of this protocol. The intensities and the probabilities for sending at Alice's and Bob's sides should satisfy the condition given in Eq. (1) to guarantee the security in the asymmetric case. We present the numerical results of different SNS protocols to show that our asymmetric SNS protocol gives much higher key rate than the other SNS protocols when Alice's and Bob's channels are different. When the difference in length between Alice's and Bob's channels is 100 km, the key rate of the asymmetric SNS protocol is tens to hundreds of times higher than that of the original SNS protocol. Our asymmetric SNS protocol can be applied directly to the SNS experiments with asymmetric channels.

If we use the method of two-way classical communication [76] on our protocol, the key rate of our asymmetric protocol can be improved further. We shall report this elsewhere.

ACKNOWLEDGMENTS

We acknowledge financial support in part by the National Key Research and Development Program of China through Grant No. 2017YFA0303901 and the National Natural Science Foundation of China through Grants No. 11474182, No. 11774198, and No. U1738142.

APPENDIX: FORMULAS FOR KEY RATE CALCULATION

1. Four-intensity decoy-state method and parameter estimation

In order to make our protocol easy to demonstrate in the experiment, we give the four-intensity decoy-state method for our protocol. "Four-intensity" means that Alice (Bob) uses four different intensities, μ_A' (μ_B') in signal windows and 0, μ_{A1} (μ_{B1}), μ_{A2} (μ_{B2}) in decoy windows. All measurement results in effective X-windows are used to estimate the bound

of n_1. Only measurement results in effective $\tilde{X}^{(1)}$-windows are used to estimate the bound of e_1^{ph}.

The sufficient condition for security is that all decoy pulses satisfy Eq. (1). If all decoy pulses satisfy Eq. (1), the phase-flip rate of single-photon states of Z-windows is equal to the bit-flip rate of single-photon states from any $X^{(i)}$-windows. In our specific method in the numerical simulation, we estimate the phase-flip rate of single-photon states of Z-windows by the bit-flip rate of single-photon states from $X^{(1)}$-windows only. Therefore, we actually need only decoy pulses of $X^{(1)}$-windows to satisfy Eq. (1).

The formula for the length of the final key in Eq. (3) can be written in the form of key rate per time window:

$$R = p_A^Z p_B^Z \{[\epsilon_A(1-\epsilon_B)\mu_A' e^{-\mu_A'} + \epsilon_B(1-\epsilon_A)\mu_B' e^{-\mu_B'}] \times s_1^Z[1 - H(e_1^{ph})] - f S_Z H(E_Z)\}, \tag{A1}$$

where s_1^Z is the counting rate in Z_1-windows, and S_Z is the counting rate of Z-windows. If there are m effective windows in a set ζ of n time windows, the counting rate of ζ is defined as $S_\zeta = m/n$.

So we need to estimate the bound of $\langle s_1^Z\rangle$ and $\langle e_1^{ph}\rangle$ by the four-intensity decoy-state method. Here $\langle\cdot\rangle$ stands for the expected value of a variable. Similarly to the methods in Ref. [84], the lower bound of $\langle s_1^Z\rangle$ is given by

$$\langle s_1^Z\rangle \geqslant \underline{\langle s_1^Z\rangle} = \frac{\mu_{A1}}{\mu_{A1}+\mu_{B1}}\underline{\langle s_{10}^Z\rangle} + \frac{\mu_{B1}}{\mu_{A1}+\mu_{B1}}\underline{\langle s_{01}^Z\rangle}, \tag{A2}$$

where $\underline{\langle s_{10}^Z\rangle}$ is lower bound of the expected value of the counting rate of the state $|10\rangle\langle 10|$ with

$$\underline{\langle s_{10}^Z\rangle} = \frac{\mu_{A2}^2 e^{\mu_{A1}}\langle S_{\mu_{A1}0}\rangle - \mu_{A1}^2 e^{\mu_{A2}}\langle S_{\mu_{A2}0}\rangle - (\mu_{A2}^2-\mu_{A1}^2)\langle S_{00}\rangle}{\mu_{A1}\mu_{A2}(\mu_{A2}-\mu_{A1})}, \tag{A3}$$

and $\underline{\langle s_{01}^Z\rangle}$ is lower bound of the expected value of the counting rate of the state $|01\rangle\langle 01|$ with

$$\underline{\langle s_{01}^Z\rangle} = \frac{\mu_{B2}^2 e^{\mu_{B1}}\langle S_{0\mu_{B1}}\rangle - \mu_{B1}^2 e^{\mu_{B2}}\langle S_{0\mu_{B2}}\rangle - (\mu_{B2}^2-\mu_{B1}^2)\langle S_{00}\rangle}{\mu_{B1}\mu_{B2}(\mu_{B2}-\mu_{B1})}. \tag{A4}$$

Here $\langle S_{\alpha\beta}\rangle$ is the expected value of the counting rate of the time windows when Alice and Bob send the decoy pulses with intensities α and β, respectively. If the data size is infinite, these expected values are exactly the values observed in the experiments. If the data size is finite, we should use the Chernoff bound introduced in the next section to estimate the bound of the expected values from the observed values and then substitute the worst cases, the bounds that make the key rate lowest, of these expected values in the key rate formula. The upper bound of $\langle e_1^{ph}\rangle$ is given by

$$\langle e_1^{ph}\rangle \leqslant \overline{\langle e_1^{ph}\rangle} = \frac{\langle T_\Delta\rangle - e^{-(\mu_{A1}+\mu_{B1})}\langle S_{00}\rangle/2}{e^{-(\mu_{A1}+\mu_{B1})}(\mu_{A1}+\mu_{B1})\underline{\langle s_1^Z\rangle}}, \tag{A5}$$

where $\langle T_\Delta\rangle$ is the expected value of the error counting rate of $\tilde{X}^{(1)}$-windows. If there are m error windows in a set ζ of n time windows, the error counting rate of ζ is defined as $T_\zeta = m/n$.

2. Chernoff bound

In the asymptotic case where the data size is infinite, the observed values are the same as the expected values. But in the nonasymptotic case where the data size is finite, the observed values are different from the expected values. So we need the Chernoff bound [88] to estimate the range of expected values from the observed values and use the worst case to ensure that the final key is secure.

Let $X_1, X_2, \ldots, X_n$ be n random variables whose observed values are either 0 or 1, X be their sum $X = \sum_i X_i$, and ϕ be the expected value of X. We have the lower and the upper bound of ϕ:

$$\phi^L(X) = \frac{X}{1+\delta_1(X)}, \tag{A6}$$

$$\phi^U(X) = \frac{X}{1-\delta_2(X)}, \tag{A7}$$

where $\delta_1(X)$ and $\delta_2(X)$ are the solutions of the following equations:

$$\left(\frac{e^{\delta_1}}{(1+\delta_1)^{1+\delta_1}}\right)^{\frac{X}{1+\delta_1}} = \frac{\xi}{2}, \tag{A8}$$

$$\left(\frac{e^{-\delta_2}}{(1-\delta_2)^{1-\delta_2}}\right)^{\frac{X}{1-\delta_2}} = \frac{\xi}{2}, \tag{A9}$$

where ξ is the failure probability. With the above equations, we have

$$N_{\alpha\beta}\underline{\langle S_{\alpha\beta}\rangle} = \phi^L(N_{\alpha\beta}S_{\alpha\beta}), N_{\alpha\beta}\overline{\langle S_{\alpha\beta}\rangle} = \phi^U(N_{\alpha\beta}S_{\alpha\beta}). \tag{A10}$$

Here $S_{\alpha\beta}$ is the observed value of the counting rate.

Then in Eq. (A1) we need the real values of s_1^Z and e_1^{ph} in a specific experiment. So Eqs. (A6)–(A10) can be written in another form to estimate the upper and the lower bound of real values from expected values:

$$X^U(\phi) = [1+\delta_1'(\phi)]\phi, \tag{A11}$$

$$X^L(\phi) = [1-\delta_2'(\phi)]\phi, \tag{A12}$$

where $\delta_1'(\phi)$ and $\delta_2'(\phi)$ are the solutions of the following equations:

$$\left(\frac{e^{\delta_1'}}{(1+\delta_1')^{1+\delta_1'}}\right)^{\phi} = \frac{\xi}{2}, \tag{A13}$$

$$\left(\frac{e^{-\delta_2'}}{(1-\delta_2')^{1-\delta_2'}}\right)^{\phi} = \frac{\xi}{2}. \tag{A14}$$

With the above equations, we have

$$\begin{aligned} N_1^Z s_1^Z &\geqslant X^L\big(N_1^Z\underline{\langle s_1^Z\rangle}\big), \\ N_1^Z\underline{\langle s_1^Z\rangle}e_1^{ph} &\leqslant X^U\big(N_1^Z\underline{\langle s_1^Z\rangle}\overline{\langle e_1^{ph}\rangle}\big), \end{aligned} \tag{A15}$$

where $N_1^Z = N_t p_A^Z p_B^Z[\epsilon_A(1-\epsilon_B)\mu_A' e^{-\mu_A'} + \epsilon_B(1-\epsilon_A)\mu_B' e^{-\mu_B'}]$ is the number of single-photon states in the Z windows when one and only one of *them* decides to send and N_t is the total number of time windows.

3. Finite key size effect

Similarly to the analysis of the effect of the finite key size in Ref. [85], we give the key rate formula with the effect of the finite key size of our asymmetric SNS protocol in the universally composable framework [89].

If the length of the final key satisfies

$$N_f = n_1\left[1 - H\left(e_1^{ph}\right)\right] - f n_t H(E_Z) - \log_2 \frac{2}{\varepsilon_{\rm cor}} - 2\log_2 \frac{1}{\sqrt{2}\varepsilon_{\rm PA}\hat{\varepsilon}}, \tag{A16}$$

the protocol is $\varepsilon_{\rm sec}$-secret with $\varepsilon_{\rm sec} = 2\hat{\varepsilon} + 4\bar{\varepsilon} + \varepsilon_{\rm PA} + \varepsilon_{n_1}$, and the total security coefficient of the protocol is $\varepsilon_{\rm tot} = \varepsilon_{\rm cor} + \varepsilon_{\rm sec}$. Here $\varepsilon_{\rm cor}$ is the probability that the error correction fails, $\bar{\varepsilon}$ is the probability that the real value of e_1^{ph} is not in the range that we estimate, $\varepsilon_{\rm PA}$ is the failure probability of the privacy amplification, and ε_{n_1} is the probability that the real value of n_1 is not in the range that we estimate. According to Eqs. (A2)–(A15), we have $\bar{\varepsilon} = 3\xi$ and $\varepsilon_{n_1} = 6\xi$. If we set $\varepsilon_{\rm cor} = \hat{\varepsilon} = \varepsilon_{\rm PA} = \xi$ in our numerical simulation, the total security coefficient of our protocol is $\varepsilon_{\rm tot} = 22\xi = 2.2 \times 10^{-9}$.

Also, Eq. (A16) can be written in the form of key rate per time window with some source parameters:

$$R = p_A^Z p_B^Z \{[\epsilon_A(1-\epsilon_B)\mu_A' e^{-\mu_A'} + \epsilon_B(1-\epsilon_A)\mu_B' e^{-\mu_B'}] \times s_1^Z\left[1 - H\left(e_1^{ph}\right)\right] - f S_Z H(E_Z)\} - \frac{1}{N_t}\left(\log_2 \frac{2}{\varepsilon_{\rm cor}} + 2\log_2 \frac{1}{\sqrt{2}\varepsilon_{\rm PA}\hat{\varepsilon}}\right). \tag{A17}$$

[1] C. Bennett, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[2] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] D. Mayers, J. ACM (JACM) **48**, 351 (2001).
[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[6] N. Gisin and R. Thew, Nat. Photon. **1**, 165 (2007).
[7] R. Renner, Int. J. Quantum Inform. **6**, 1 (2008).
[8] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[9] M. Koashi, New J. Phys. **11**, 045018 (2009).
[10] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[11] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, in *International Symposium on Information Theory, 2004, ISIT 2004* (IEEE, New York, 2004), p. 136.
[12] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[13] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[14] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[15] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007).
[16] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[17] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[18] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[19] H. P. Yuen, Quantum Semiclassical Opt. **8**, 939 (1996).
[20] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[21] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).
[22] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).
[23] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Phys. Rep. **448**, 1 (2007).
[24] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).
[25] X.-B. Wang, Phys. Rev. A **87**, 012320 (2013).
[26] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature (London) **509**, 475 (2014).
[27] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[28] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013).
[29] F. Xu, H. Xu, and H.-K. Lo, Phys. Rev. A **89**, 052333 (2014).
[30] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, and X.-Q. Tan, Phys. Rev. A **86**, 022332 (2012).
[31] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **89**, 052325 (2014).
[32] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Phys. Rev. A **91**, 032318 (2015).
[33] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **93**, 042324 (2016).
[34] C. Jiang, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **94**, 062323 (2016).
[35] C. Jiang, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **95**, 032325 (2017).
[36] X.-Y. Zhou, C.-H. Zhang, C.-M. Zhang, and Q. Wang, Phys. Rev. A **96**, 052337 (2017).
[37] A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, Phys. Rev. A **98**, 012330 (2018).
[38] H. F. Chau, Phys. Rev. A **97**, 040301(R) (2018).
[39] X.-L. Hu, Y. Cao, Z.-W. Yu, and X.-B. Wang, Sci. Rep. **8**, 17634 (2018).
[40] W. Wang, F. Xu, and H.-K. Lo, Phys. Rev. A **97**, 032337 (2018).
[41] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).
[42] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).
[43] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).

[44] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li *et al.*, Phys. Rev. Lett. **121**, 190502 (2018).

[45] Z. Yuan, A. Sharpe, and A. Shields, Appl. Phys. Lett. **90**, 011118 (2007).

[46] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, Phys. Rev. Lett. **100**, 090501 (2008).

[47] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes *et al.*, New J. Phys. **11**, 075001 (2009).

[48] A. R. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, Appl. Phys. Lett. **96**, 161102 (2010).

[49] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, Opt. Express **19**, 10387 (2011).

[50] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, Nature (London) **501**, 69 (2013).

[51] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).

[52] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).

[53] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).

[54] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok, and W. Tittel, Opt. Express **22**, 12716 (2014).

[55] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).

[56] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).

[57] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nat. Photon. **9**, 827 (2015).

[58] 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).

[59] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 397 (2015).

[60] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Nat. Photon. **10**, 312 (2016).

[61] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Optica **4**, 1016 (2017).

[62] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, Nature (London) **549**, 43 (2017).

[63] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu *et al.*, Phys. Rev. Lett. **120**, 030501 (2018).

[64] 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 *et al.*, Phys. Rev. Lett. **117**, 190501 (2016).

[65] M. Takeoka, S. Guha, and M. M. Wilde, Nat. Commun. **5**, 5235 (2014).

[66] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).

[67] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Nature (London) **557**, 400 (2018).

[68] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Phys. Rev. A **98**, 062323 (2018).

[69] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, arXiv:1805.05511.

[70] X. Ma, P. Zeng, and H. Zhou, Phys. Rev. X **8**, 031043 (2018).

[71] J. Lin and N. Lütkenhaus, Phys. Rev. A **98**, 042332 (2018).

[72] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Phys. Rev. Appl. **11**, 034053 (2019).

[73] M. Curty, K. Azuma, and H.-K. Lo, npj Quantum Inf. **5**, 64 (2019).

[74] F.-Y. Lu, Z.-Q. Yin, C.-H. Cui, G.-J. Fan-Yuan, S. Wang, D.-Y. He, W. Chen, G.-C. Guo, and Z.-F. Han, New J. Phys. **21**, 123030 (2019).

[75] F. Grasselli and M. Curty, New J. Phys. **21**, 073001 (2019).

[76] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, arXiv:1904.06331.

[77] C.-H. Zhang, C.-M. Zhang, and Q. Wang, Opt. Lett. **44**, 1468 (2019).

[78] X.-Y. Zhou, C.-H. Zhang, C.-M. Zhang, and Q. Wang, Phys. Rev. A **99**, 062316 (2019).

[79] K. Maeda, T. Sasaki, and M. Koashi, Nat. Commun. **10**, 3140 (2019).

[80] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Nat. Photon. **13**, 334 (2019).

[81] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, T.-Y. Chen, L. You *et al.*, Phys. Rev. Lett. **123**, 100505 (2019).

[82] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Phys. Rev. X **9**, 021046 (2019).

[83] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **123**, 100506 (2019).

[84] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, Sci. Rep. **9**, 3080 (2019).

[85] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Phys. Rev. Appl. **12**, 024061 (2019).

[86] F. Grasselli, A. Navarrete, and M. Curty, New J. Phys. **21**, 113032 (2019).

[87] W. Wang and H.-K. Lo, arXiv:1907.05291.

[88] H. Chernoff *et al.*, Ann. Math. Statistics **23**, 493 (1952).

[89] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).