Twin-field quantum key distribution with large misalignment error

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

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

[2]*Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

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

[4]*Data Communication Science and Technology Research Institute, Beijing 100191, People's Republic of China*

(Received 23 May 2018; published 18 December 2018)

Based on the novel idea of twin-field quantum key distribution [TF-QKD; Lucamarini *et al.*, Nature (London) **557**, 400 (2018)], we present a protocol named the "sending or not sending TF-QKD" protocol, which can tolerate large misalignment error. A revolutionary theoretical breakthrough in quantum communication, TF-QKD changes the channel-loss dependence of the key rate from linear to square root of channel transmittance. However, it demands the challenging technology of long-distance single-photon interference, and also, as stated in the original paper, the security proof was not finalized there due to the possible effects of the later announced phase information. Here we show by a concrete eavesdropping scheme that the later phase announcement does have important effects and the traditional formulas of the decoy-state method do not apply to the original protocol. We then present our "sending or not sending" protocol. Our protocol does not take postselection for the bits in Z-basis (signal pulses), and hence the traditional decoy-state method directly applies and automatically resolves the issue of security proof. Most importantly, our protocol presents a negligibly small error rate in Z-basis because it does not request any single-photon interference in this basis. Thus our protocol greatly improves the tolerable threshold of misalignment error in single-photon interference from the original a few percent to more than 45%. As shown numerically, our protocol exceeds a secure distance of 700, 600, 500, or 300 km even though the single-photon interference misalignment error rate is as large as 15%, 25%, 35%, or 45%.

DOI: 10.1103/PhysRevA.98.062323

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] can in principle present secure private communications with its security guaranteed by principles of quantum physics. With the development [3–15] in both theory and experiment, it is more and more hoped to be extensively applied in practice, though there are barriers for doing so. Among all barriers, channel loss of long-distance QKD is the major one [10,12].

Very recently, revolutionary theoretical progress was made by Lucamarini *et al.* They proposed the novel idea of twin-field quantum key distribution (TF-QKD) [14], which has historically changed the relationship between key rate and the channel loss from linearly dependent to square root dependent. Consequently, TF-QKD makes a great breakthrough for a secure distance longer than 500 km.

In the TF-QKD [14], Alice and Bob send fields to the untrusted third party Charlie. In a virtual ideal protocol, Alice and Bob initially share single-photon entangled states of $|\Phi^0\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. They each will take a phase shift of either 0 or π to each one's local field, and they will send their fields to Charlie. After a collective measurement, Charlie will see whether the bipartite is $|\Phi^0\rangle$ or $|\Phi^1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Except for Alice and Bob, no one knows which value, 0 or π was selected by Alice or Bob in doing their phase shift, although it is known to everyone whether Alice and Bob has used the same phase shift or a different phase shift. So they can use the information whether Alice has taken a phase shift 0 or π for their secret key.

However, in practice, we do not have such an initially shared state. The TF-QKD proposed to use weak coherent states at each side. As was stated in the original article [14], the security is not finally completed because the possible effects of the later announcement of the phase information are not taken into consideration. As shown by a concrete eavesdropping scheme in the supplement, we find that the phase information announced later makes the traditional formulas of the decoy-state method [5–7] not apply to the original protocol [14]. In fact, given the scheme in the Appendix, Eve can have full information for the key bits while the traditional decoy-state method can give a key rate of 50%. Our eavesdropping scheme shows that the fraction of single-photon bits among all raw bits must be not less than 50%, otherwise Eve may have full information for all bits without causing any disturbance. Although one may naturally turn to the key rate formulas for non-random-phase coherent states to resolve the issue, however, TF-QKD relied on the challenging technology of long-distance single-photon interference, which may produce large misalignment error. Here we construct a "sending or

*xbwang@mail.tsinghua.edu.cn

not sending" TF-QKD protocol where there is no phase-slice-dependent postselection for signal bits. Not only does this itself increase the amount of key bits, but also this makes the traditional calculation formulas for the decoy state method directly apply, the security proof is automatically completed, and the less efficient key rate formula for non-phase-random coherent states is not necessary. Most importantly, our protocol can tolerate large misalignment error rate due to the long-distance single-photon interference.

II. SENDING OR NOT-SENDING (SNS) PROTOCOL

Step 0. At any time window i, as requested by the TF-QKD, *they* (Alice and Bob) take random phase shifts δ_{Ai}, δ_{Bi} to their coherent states accompanied by the strong reference light which will be sent to Charlie in Step 1. (Charlie is supposed to do appropriate phase compensation in the protocol, but he is possibly dishonest.)

Step 1. At any time window i, Alice (Bob) independently determines whether it is a decoy window or a signal window. If it is a decoy window, she (he) sends out to Charlie a decoy pulse in coherent state $|\sqrt{\mu}e^{i\delta_{Ai}+i\gamma_{Ai}}\rangle$ ($|\sqrt{\mu}e^{i\delta_{Bi}+i\gamma_{Bi}}\rangle$), and μ can randomly change among a few different values at different decoy windows. If it is a signal window, she (he) decides to send out to Charlie a signal pulse $|\sqrt{\mu'}e^{i\delta_{Ai}+i\gamma_{Ai}}\rangle$ ($|\sqrt{\mu'}e^{i\delta_{Bi}+i\gamma_{Bi}}\rangle$) by probability ϵ, and she (he) decides not to send it out by probability $1-\epsilon$. Given whatever window she (he) commits, and whatever decision she (he) makes, the global phases γ_{Ai} (γ_{Bi}) are always announced by sending out a strong reference light.

Note: This sending by a small probability ϵ or not sending by probability $1-\epsilon$ is the heart of our protocol.

Note: For simplicity, we shall omit subscript i here after if there is no confusion. A coherent state of intensity x and global phase γ is a linear superposition of photon number states $\{|k\rangle\}$ of $|\sqrt{x}e^{i\gamma}\rangle = \sum_{k=0}^{\infty} \frac{e^{-x/2}(\sqrt{x}e^{i\gamma})^k}{\sqrt{k!}}|k\rangle$. In a signal window, if Alice or Bob decides to send, she (he) shall always send a coherent state of intensity μ'. For example, at a certain time when they both determined signal windows, if Alice decides to send while Bob decides not to send, the two-mode state from this time window is $|\sqrt{\mu'}e^{i\delta_A+i\gamma_A}\rangle|0\rangle$; if both of them decide to send, the two-mode state is $|\sqrt{\mu'}e^{i\delta_A+i\gamma_A}\rangle|\sqrt{\mu'}e^{i\delta_B+i\gamma_B}\rangle$; if both of them decide not to send, the state at that time window is $|00\rangle$. States from a decoy window can have different intensities. If at a certain time both of them have chosen a decoy window and both of them have happened to choose the same intensity μ, the two-mode coherent state from this time window is $|\sqrt{\mu}e^{i\delta_A+i\gamma_A}\rangle|\sqrt{\mu}e^{i\delta_B+i\gamma_B}\rangle$. Here γ_A, γ_B are global phases of the coherent states. They are known to Eve because Alice and Bob always send strong reference pulses to accompany each two-mode states above. In the protocol, Charlie is supposed to do phase compensation, trying to remove the global phases. If Charlie does this perfectly, the states from each side after the compensation have the same global phases. For example, state $|\sqrt{\mu}e^{i\delta_A+i\gamma_A}\rangle|\sqrt{\mu}e^{i\delta_B+i\gamma_B}\rangle$ will be changed into $|\sqrt{\mu}e^{i\delta_A}\rangle|\sqrt{\mu}e^{i\delta_B}\rangle$ after a perfect phase compensation by Charlie.

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

Note: We define an *effective event* by the following criterion: (1) If Charlie announces only one detector counting corresponding to a time window i when both of them have determined a signal window, it is an effective event; (2) if Charlie announces only one detector counting corresponding to a time window i when both of them have determined a decoy window and used the same intensity of coherent states, and in that time window, the prechosen values δ_A, δ_B satisfy

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

Here the value λ is determined by the size of phase slice [14] chosen by Alice and Bob. Whenever an effective event happens, a bit in the corresponding basis is recorded.

Step 3. *They* announce each one's decoy windows and signal windows. *They* also announce details for intensities and values δ_A, δ_B of pulses sent from decoy windows.

Note: We define a Z-window as a time window when both Alice and Bob have determined a signal window. We name states from such Z-windows as states in Z-basis, or simply Z-pairs, Z-states. Effective events that happen in Z-basis are named Z-bits. Given that δ_A value (δ_B value) is randomized, whenever Alice or Bob sends a coherent state of intensity μ', it can be equivalently regarded as a density matrix of $\int_0^{2\pi} |\sqrt{\mu'}e^{i\delta_A+i\gamma_A}\rangle\langle\sqrt{\mu'}e^{i\delta_A+i\gamma_A}|d\delta_A/2\pi = \sum_{k=0}^{\infty} \frac{e^{-\mu'}\mu'^k}{k!}|k\rangle\langle k|$, which is a classical mixture of different photon number states only. Hence we can define Z_1-windows as a subset of Z-windows when only one party of Alice and Bob decides to send and she (he) actually sends a single-photon state. In a Z_1-window, the two-mode single-photon state sent out is either $|z_0\rangle = |01\rangle$ or $|z_1\rangle = |10\rangle$. We shall call them Z_1-states or Z_1-pairs. Also, effective events caused in Z_1-windows are named Z_1-bits. Furthermore, we define an X-window as a time window when (1) both of them have chosen the decoy window, (2) both of them have chosen the same intensity for the coherent state to send, and (3) the random phase δ_A, δ_B chosen for the window satisfies Eq. (1). We name the two-mode states from X-windows states in X-basis, or simply X-pairs or X-states, and an X-bit is a bit caused by X-pair. Also, as shown later, states of X-pairs can be regarded as a probabilistic mixture of different photon-number states, with the two-mode single-photon ingredient $|\psi_1\rangle\langle\psi_1|$, and $|\psi_1\rangle = \frac{1}{\sqrt{2}}(e^{i(\delta_B+\gamma_B)}|01\rangle + e^{i(\delta_A+\gamma_A)}|10\rangle)$. Therefore we can define an $\mathcal{X}_1$-window as an X-window when *they* send a (two-mode) single-photon state. We also name those states from $\mathcal{X}_1$-windows $\mathcal{X}_1$-pairs or $\mathcal{X}_1$-states, and the bits caused $\mathcal{X}_1$-pairs as $\mathcal{X}_1$-bits. *They* do not know which time windows are Z_1-windows and $\mathcal{X}_1$-windows, neither do *they* know which bits are Z_1-bits and $\mathcal{X}_1$-bits, though *they* can know the number of these windows and bits by calculation. If we consider only Z_1-windows and $\mathcal{X}_1$-windows, the states set here is similar to that in a BB84 protocol [1].

Step 4. *They* randomly choose some Z-bits to do error test. By this they can know the bit-error rate in Z-basis, E^Z. *They* discard the test bits, and the remaining Z-bits will be distilled for the final key.

Note: For any effective event happens in Z-basis, Alice (Bob) judges the bit value in this way: if she (he) has decided to send out a signal pulse, she (he) denotes a bit value 1 (0); if she (he) has decided not to send, she (he) denotes a bit value 0 (1). One can see straight away, if an effective event happens while both Alice and Bob have decided not to send, or both of them have decided to send, a wrong bit in Z-basis is created, because in such a case, the bit value denoted by Alice is different from the bit value denoted by Bob.

Step 5. They use the announced data from X-pairs to calculate the counting rate (yield) s_1 for $\mathcal{X}_1$-windows (which is also the value for Z_1-windows). The number of bits created in Z_1-windows can be directly calculated from this value. Also, by observing the error rate of X-pairs of intensity μ, E_μ^X, the counting rate of intensity μ, S_μ, and the counting rate of vacuum s_0, they can calculate the upper bound value of flipping rate of $\mathcal{X}_1$-bits by

$$e_1^{\mathcal{X}_1} \leqslant \bar{e}_1^{\mathcal{X}_1} = \frac{S_\mu E_\mu^X - e^{-2\mu} s_0/2}{2\mu e^{-2\mu} s_1}. \tag{2}$$

Asymptotically, the phase-flip rate e_1^{ph} for Z_1 bits is $e_1^{ph} = e_1^{\mathcal{X}_1}$.

Note: In the protocol, Charlie does the beam-splitter measurement [14] after he takes the phase compensation. There are two output ports of the beam splitter: the right detector and left detector. *They* use the following criterion to judge a right bit or a wrong bit in X-basis: A right X-bit is the left (right) detector clicking caused by an X-pair with positive (negative) value of $\cos(\delta_A - \delta_B)$. A wrong X-bit is the right (left) detector clicking caused by an X-pair with positive (negative) value of $\cos(\delta_A - \delta_B)$. Given the observed error rate in X-basis and s_1, the phase-flip error rate e_1^{ph} for Z_1-bits can be obtained because asymptotically it is just the error rate of those single-photon-caused X-bits, as shown in the supplement. Note that, although they know the number of $\mathcal{X}_1$-bits, *they* don't know which ones are $\mathcal{X}_1$-bits, and hence quantity $e_1^{\mathcal{X}_1}$ cannot be directly observed, it can be only *calculated* by the formula above.

Note: Also, as one can easily see, if Charlie does the phase compensation perfectly, the output of the beam-splitter measurement [14] will produce a small observed error rate in X-basis, if $|\lambda|$ is small in the postselection criterion [Eq. (1)]. Charlie does not have to be honest or do the compensation perfectly. But this will only change the observed error rate in X-basis rather than the security of the protocol.

Step 6. They distill the final key with an asymptotic key rate formula

$$N_f = n_1 - n_1 H\left(e_1^{ph}\right) - n_t f H(E^Z), \tag{3}$$

where N_f is the number of final bits, n_1 is the number of remaining Z_1-bits after the error test in Step 4, n_t is the number of remaining Z-bits after the error test in Step 4, $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function, and f is error correction efficiency factor. The formula can be equivalently written in the following form of key rate per time window:

$$R = 2\epsilon(1-\epsilon)\mu' e^{-\mu'} s_1\left[1 - H\left(e_1^{ph}\right)\right] - S_Z f H(E^Z), \tag{4}$$

where S_Z is the observed counting rate of Z-windows.

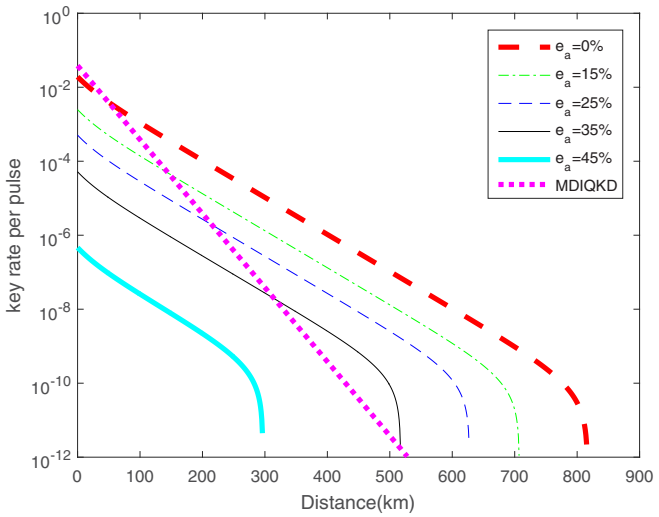

FIG. 1. Log scale of the key rate as a function of the distance between Alice and Bob with different misalignment errors. e_a: misalignment error rate of single-photon interference. MDIQKD: The optimized key rate for existing decoy-state MDI-QKD with coherent states. In calculating MDI-QKD, we take misalignment error rate 1.5% for X-basis and 0 for Z-basis. The numerical result here shows that asymptotically our protocol can have an obvious advantage to the existing decoy-state MDI-QKD even though the misalignment error is as large as 35%. Here, infinite intensities are assumed in the decoy state calculation.

III. NUMERICAL SIMULATION

In our protocol, we use the traditional formulas for the decoy-state method. Since we don't need any postselection in Z-basis and we need only sending or not-sending, there is no misalignment error in this basis. This makes the protocol able to work with large misalignment from the single-photon interference in X-basis. The results of numerical simulation are summarized in Figs. 1 and 2.

In the calculation, we have assumed a detector with a dark count rate of 10^{-11} and detection efficiency of 80%. An error correction coefficient of 1.1 is set in our calculation. Here we

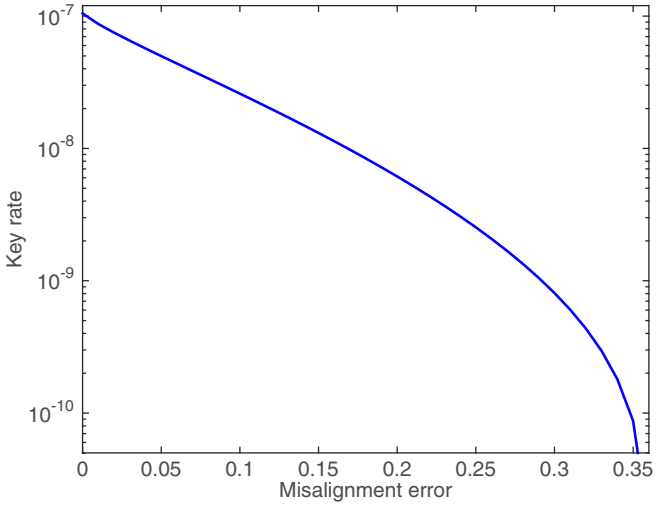

FIG. 2. Log scale of the key rate as a function of the misalignment error when the distance between Alice and Bob is 500 km.

have considered only the asymptotic result, and we have set the phase slice infinitely small. We can do so because in our case we take no postselection in Z-basis. And, at each data point, we have optimized ϵ and the signal pulse intensity so as to obtain the best key rate. We can see that our protocol is so robust to misalignment errors that it can exceed a secure distance of nearly 300 km even with a misalignment error rate of 45%. It exceeds a secure distance of 700 or 600 km even though the single-photon misalignment error rate is as large as 15% or 25%. Also, when the distance is fixed to be 500 km, the key rates are shown with different misalignment errors. The largest tolerable error rate can be 35%. These results show that our protocol by far breaks the existing few percent threshold of the single-photon misalignment error rate for a larger-than-zero secure distance. When there is no misalignment error, our protocol exceeds a secure distance of more than 800 km.

IV. VALIDITY OF THE DECOY-STATE METHOD

Specifically, in the protocol Alice takes a random phase shift δ_A to her coherent state, and Bob takes a random phase shift δ_B to his coherent state. The two-mode weak coherent state prepared by them is $|\sqrt{\mu}e^{i\delta_A+i\gamma_A}\rangle\otimes|\sqrt{\mu}e^{i\delta_B+i\gamma_B}\rangle$. Here the global phases γ_A and γ_B cannot be regarded as random phases because *they* also send the strong reference pulses. First, we introduce the new independent variables $\delta_\pm=(\delta_B\pm\delta_A)/2$. Integrating the two-mode state of X pulses on variable δ_+ over the range of $[0,2\pi)$, we obtain a classical mixture in the convex form

$$\sum_k p_k(\mu)|\psi_k\rangle\langle\psi_k| \tag{5}$$

with $|\psi_k\rangle$ being the state of total photon number k for the two-mode state $|\psi_k\rangle$ and $p_k(\mu)$ being its probability. For example,

$$|\psi_0\rangle=|00\rangle,\ \ p_0(\mu)=e^{-2\mu}, \tag{6}$$

$$|\psi_1\rangle=\frac{1}{\sqrt{2}}(e^{i\delta_B+i\gamma_B}|01\rangle+e^{i\delta_A+i\gamma_A}|10\rangle), \tag{7}$$

with

$$\begin{aligned} p_1(\mu)&=2\mu e^{-2\mu},\\ |\psi_2\rangle&=\frac{1}{\sqrt{2}}e^{i(\delta_A+\gamma_A+\delta_B+\gamma_B)}|11\rangle\\ &\quad+\frac{1}{2}e^{2i(\delta_B+\gamma_B)}|02\rangle+\frac{1}{2}e^{2i(\delta_A+\gamma_A)}|20\rangle, \end{aligned} \tag{8}$$

with

$$p_2(\mu)=2\mu^2e^{-2\mu}, \tag{9}$$

and so on. This means states from X-windows are actually classical mixture of different photon numbers. The phase randomized states from Z-windows can also be regarded as a mixture of different photon-number states, in particular, the ingredients of single photons are randomly on states $|01\rangle$ or $|10\rangle$. As shall be shown later in virtual protocols, single-photon states of Eq. (7) can be used to test the phase-flip rate of those single photons from Z-windows.

One may argue that there is a later announcement of phase information for decoy pulses, how to guarantee the validity of the traditional decoy-state method here, e.g., Eq. (3). Since the phase-shift information of signal pulses is never announced, we can regard signal pulses as a classical mixture of different photon number states. What we want to know is the number of single-photon-caused bits and their phase-flip error rate from signal bits. Once we know the facts, they do not change by any action outside the laboratory. Consider a virtual protocol where Alice and Bob secretly decided the random phase-shift values prior to the protocol. In such a case, our calculations at Step 6 are obviously solid. Note that the values of single-photon counts and phase-flip error rate are objective facts which do not change by any outside actions. After Alice and Bob know the fact, they can announce the phase information of all decoy pulses. But they can also choose to first announce the phase information and then calculate the crucial values for the signal bits, because no one knows at which time they have done the calculation. In such a case, they do not need to predetermine the random phase values, they just use the protocol we proposed above. Also, there is a similar story in the MDI-QKD: the bases information cannot be announced before the states are measured. But it can be announced later, for, the X-basis states are used only to know the phase-flip value of those qubits in Z-basis.

Explicitly, we divide the whole space into two subspaces, $\mathcal{E}$ for Eve and $\mathcal{AB}$ for Alice and Bob. After Alice and Bob postannounce phase-shift information, they will not receive any information from Charlie (Eve). Suppose Eve has a machine $\mathcal{M}$ which automatically stores all those postannounced information on phase-shift values of effective states in X-windows. Eve can in principle have two different choices:

Choice 1: Ignores the machine $\mathcal{M}$ and does not take any actions.

Choice 2: Makes use of the stored information of $\mathcal{M}$ and takes whatever actions she can to her probe.

Definitely, under Choice 1, all decoy-state methods are valid, all calculated values for signal states, such as $\underline{s}_1$ the lower bound of single-photon counts for Z-windows and the $\bar{e}_1^{ph}$ upper bound of phase-flip rate of those single-photon counts of Z-windows, are correct and the final key is secure. On the other hand, both Choice 1 and Choice 2 are *local* actions in subspace $\mathcal{E}$, and they do not cause detectable effects in subspace $\mathcal{AB}$. Therefore, even if Eve takes Choice 2, it makes no difference to subspace $\mathcal{AB}$. That is, no matter which choice Eve takes, there will be no detectable difference in subspace $\mathcal{AB}$. Therefore, Alice and Bob can always assume Choice 1 for Eve. This can be stated as the following theorem.

Theorem: Given whatever information is announced by Alice and Bob, Eve's actions to her probe only cannot cause any detectable effects in Alice and Bob's subspace $\mathcal{AB}$.

The phase-flip error is not detectable in the real protocol presented earlier. But, imagine a purification protocol where Alice and Bob use entangled photons in Z-windows and coherent states in X-windows only. Then the phase-flip error is detectable and the purification result will be all the same no matter which choice Eve has taken. Reducing this virtual protocol to the real protocol we conclude that later announcement of phase-shift values does not change the security. Details of this are shown in the notes to Virtual Protocol 3.

V. SECURITY PROOF WITH VIRTUAL PROTOCOLS AND REDUCTION

We first recall the definition of time windows in the sending or not-sending (SNS) protocol: Any time window i, if both Alice and Bob commit to a signal window, is called a Z-window; if both of them commit to a decoy window, and if each of them has sent out to Charlie a coherent state of the same intensity μ_k it is called an X-window. Besides Z-windows and X-windows, in a complete SNS protocol, there are also mismatching windows, e.g., a time window when Alice commits to a signal window while Bob commits to a decoy window, or when Alice and Bob each commit to a decoy window but choose different intensities μ_k for the coherent state. For presentation conciseness, we shall first prove the security of the *simplified form* of the SNS protocol which has Z-windows and X-windows only. After the *simplified* SNS protocol is proven secure, we then show that the proof also holds for the complete SNS protocol.

A. Z-basis encoding on ancillary photons of an extended state

If the ith time window is a Z-window, Alice and Bob each make a decision on either *sending* or *not-sending*. If Alice (Bob) decides *sending*, she (he) puts down a bit value 1 (0) and then sends out a coherent state to Charlie; if Alice (Bob) decides *not-sending*, she (he) puts down a bit value 0 (1) and does not send out anything (i.e., sends out a vacuum $|0\rangle$) to Charlie.

The Z-basis encoding of the SNS protocol is done by decisions on *sending* or *not-sending* made by Alice and Bob locally. More precisely, the *sending* or *not-sending* decision of a time window that always corresponds to the local classical bits 1, 0 to Alice or 0, 1 to Bob. We can also imagine that whenever Alice (Bob) decides *sending* or *not-sending*, she (he) always produces a local ancillary photon-number state $|1\rangle$ or $|0\rangle$ and the corresponding bit values are encoded in the local ancillary state. To Alice (Bob), state $|0\rangle$ corresponds to a bit value 0 (1), and state $|1\rangle$ corresponds to a bit value 1 (0). This is equivalent to say that *they* (Alice and Bob) have used an extended state including a real-photon state which will be sent out to Charlie and ancillary state placed locally. For example, in a certain window when Alice decides sending and Bob decides not sending, we can imagine that *they* have actually prepared an extended state

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

where ρ_A is the coherent state sent out by Alice in a Z-window when she decides *sending*. We shall also use notation ρ_B as the coherent state sent out by Bob in a Z-window when he decides *sending*. As stated already, each one's bit value is actually encoded in the local ancillary photon-number state. If the ith time window is a Z-window, Alice and Bob each make a decision on either *sending* or *not-sending*. Define subspace $\mathcal{T}$ for the subspace of sent-out states and $\mathcal{A}n$ for the subspace of local ancillary states with Alice and Bob. We can also construct an extended quantum state in the complex space $\mathcal{T}\otimes\mathcal{A}n$ for a Z-window as

$$\begin{aligned}\Omega = {} & (p_1/2)(|0\rangle\langle 0|\tilde{\otimes}\rho_B)\otimes|01\rangle\langle 01| \\ & + (p_1/2)(\rho_A\tilde{\otimes}|0\rangle\langle 0|)\otimes|10\rangle\langle 10| \\ & + p_2|00\rangle\langle 00|\otimes|00\rangle\langle 00| \\ & + p_3(\rho_A\tilde{\otimes}\rho_B)|\otimes|11\rangle\langle 11|.\end{aligned} \tag{11}$$

Here both symbols $\tilde{\otimes}$ and $\otimes$ are for a tensor product, and $\tilde{\otimes}$ is the tensor product inside subspace $\mathcal{T}$, and $\otimes$ is the tensor product between subspace $\mathcal{T}$ and $\mathcal{A}n$. On the right-hand side of Eq. (11), those states left of $\otimes$, such as $|0\rangle\langle 0|\tilde{\otimes}\rho_B$, $\rho_A\tilde{\otimes}|0\rangle\langle 0|$, $|00\rangle\langle 00|$, and $\rho_A\tilde{\otimes}\rho_B$, are in the subspace $\mathcal{T}$, and those states right of $\otimes$, such as $|10\rangle\langle 10|$, $|01\rangle\langle 01|$, $|00\rangle\langle 00|$, and $|11\rangle\langle 11|$, are in the subspace $\mathcal{A}n$. For presentation simplicity, we shall name the light field of subspace $\mathcal{T}$ in an extended state a *real-photon state*, or *real photons*, and name the local light field in subspace $\mathcal{A}n$ an *ancillary-photon state*, or *ancillary photons*.

Ancillary state $|01\rangle\langle 01|$ ($|10\rangle\langle 10|$) is for the decisions that Alice decides *not-sending* (*sending*) and Bob decides *sending* (*not-sending*). Ancillary-photon state $|00\rangle\langle 00|$ ($|11\rangle\langle 11|$) is for the decisions that both of them decide *not-sending* (*sending*). In a Z-window of SNS protocol, *their* action is equivalent to just sending out the *real photons* of Ω to Charlie and keep their *ancillary photons*.

Also, since ρ_A and ρ_B are phase-randomized coherent states, each of these states can be regarded as classical mixtures of different photon number states. Suppose that we can replace ρ_A or ρ_B by

$$\rho_{\mu'} = \sum_{n=0}^{\infty}\frac{e^{-\mu'}\mu'^n}{n!}|n\rangle\langle n| = \mu' e^{-\mu'}|1\rangle\langle 1| + (1-\mu'\,e^{-\mu'})\bar{\rho}, \tag{12}$$

where

$$\bar{\rho} = \frac{1}{1-\mu' e^{-\mu'}}\sum_{n\neq 1}\frac{e^{-\mu'}\mu'^n}{n!}|n\rangle\langle n|, \tag{13}$$

and hence we can rewrite the extended state Ω in the following equivalent format:

$$\Omega = \sum_r q_r\,\Omega_r, \tag{14}$$

where $r = 1, 2, 3, 4$ and

$$\begin{aligned}\Omega_1 = {} & (1/2)(|01\rangle\langle 01|\otimes|01\rangle\langle 01| \\ & + |10\rangle\langle 10|\otimes|10\rangle\langle 10|), \\ \Omega_2 = {} & (1/2)[(|0\rangle\langle 0|\tilde{\otimes}\bar{\rho})\otimes|01\rangle\langle 01| \\ & + (\bar{\rho}\tilde{\otimes}|0\rangle\langle 0|)\otimes|10\rangle\langle 10|], \\ \Omega_3 = {} & |00\rangle\langle 00|\otimes|00\rangle\langle 00|, \\ \Omega_4 = {} & (\rho_{\mu'}\tilde{\otimes}\rho_{\mu'})\otimes|11\rangle\langle 11|.\end{aligned} \tag{15}$$

Also, for any time window i, if it is an X-window of the SNS protocol, *they* (Alice and Bob) send out two-mode coherent state

$$\rho_X = |\tilde{\beta}_k\rangle\langle\tilde{\beta}_k|, \tag{16}$$

where, i.e., in the form of a two-mode coherent state,

$$|\tilde{\beta}_k\rangle = |\sqrt{\mu}_k e^{i\delta_A + i\gamma_A}\rangle |\sqrt{\mu}_k e^{i\delta_B + i\gamma_B}\rangle, \tag{17}$$

and k is randomly chosen from a few different values for different intensities, μ_k, δ_A, δ_B are random values taken privately by Alice and Bob, respectively, and γ_A, γ_B are global phases announced to Charlie publicly.

In the SNS protocol above, the state for a Z-window is a classical mixture of different kinds of time windows. The Z-windows are a classical mixture of Z_1-windows which uses only the extended states Ω_1 and other types of Z-windows which use the extended states of $\Omega_2, \Omega_3, \Omega_4$. (Note that all these states are orthogonal.) To show the security of this protocol, we can take the following theme: We first show the security of a protocol with only state Ω_1 for a Z-window, and then extend it to the case of state Ω for a Z-window by the tagged model [15]: we regard the bit values of Z-basis encoding from state Ω_1 as the set of *untagged bits* and the bit values from other states (Ω_2, Ω_3, Ω_4) as the set of *tagged bits*.

In a complete SNS protocol, besides X-windows and Z-windows, there are other time windows (those mismatching windows [16]), but as shown in the end of the proof, in that case another extended state including all time windows is constructible, and it is still a mixture of Ω_1 and other states, and therefore the tagged model and the security proof here still holds. At this moment, for presentation conciseness, we consider the *simplified form* of the SNS protocol where there are only Z-windows and X-windows.

We shall start from our Virtual Protocol 1 where Alice and Bob preshare extended quantum entangled states and classical information for both X-windows and Z-windows. The security of the outcome of this virtual protocol can be shown by entanglement purification to the ancillary photons. After reductions, we find that Eve cannot distinguish this protocol from a simpler protocol, Protocol 2. We then show that, based on the proven security of Protocol 2, Protocol 3 must be secure because we can equivalently regard that states of X-windows of Protocol 2 are a subset of that of Protocol 3. Eve cannot distinguish Protocol 3 and Protocol 4, which is the simplified form of SNS. Finally, we can construct that the complete SNS protocol, Protocol 5, can be obtained through assigning specific probabilities to each preshared extended states in a virtual protocol. This completes the security proof.

B. Virtual Protocol 1

Definition of effective event: We define an *effective event* of a Z-window if Charlie announces one and only one detector clicking for an individual Z-window. We define an *effective event* of an X-window if Charlie announces one and only one detector clicking for an individual X-window and values δ_A, δ_B in the corresponding state satisfy Eq. (24). *They* will then use only states or data corresponding to effective events in the protocol. A time window that presents an effective event is named an effective time window. An *effective ancillary photon* is an ancillary photon corresponding to an effective event.

1. Preparation stage

They preshare classical information for different time windows *they* will use, X-windows and Z-windows. *They* also preshare an extended state

$$\Omega_{0i} = |\Psi_{1i}\rangle\langle\Psi_{1i}|,$$
$$|\Psi_{1i}\rangle = \frac{1}{\sqrt{2}}(e^{i\gamma_{B_i}}|01\rangle \otimes |01\rangle + e^{i\gamma_{A_i}}|10\rangle \otimes |10\rangle) \tag{18}$$

for the ith time window. Here values of γ_{A_i}, γ_{B_i} are announced publicly.

For any time window i, if it is an X-window, Alice takes a local random phase shift δ_{Ai} and Bob takes a local random phase shift δ_{Bi} locally to the real photon of state Ω_{0i}. We name the state after the random phase shifts Ω_{Xi}. Explicitly

$$\Omega_{X_i} = |\Psi'_{1i}\rangle\langle\Psi'_{1i}|, \quad |\Psi'_{1i}\rangle = \frac{1}{\sqrt{2}}(e^{i\delta_{B_i}+i\gamma_{B_i}}|01\rangle \otimes |01\rangle + e^{i\delta_{A_i}+i\gamma_{A_i}}|10\rangle \otimes |10\rangle) \tag{19}$$

with the random values δ_{Ai}, δ_{Bi} being privately chosen by Alice and Bob, respectively.

For any time window i, if it is an Z-window, through discussions by a secret channel, Alice takes a local restricted random phase shift δ_{Ai} and Bob takes a local restricted random phase shift δ_{Bi} to the real photon of state Ω_{0i}, with the restriction

$$1 - |\cos(\delta_{B_i} - \delta_{A_i})| \leqslant |\lambda|. \tag{20}$$

We name the state after the restricted random phase shifts Ω_{Zi}, which has the form

$$\Omega_{Z_i} = |\Psi'_{1i}\rangle\langle\Psi'_{1i}|, \quad |\Psi'_{1i}\rangle = \frac{1}{\sqrt{2}}(e^{i\delta_{B_i}+i\gamma_{B_i}}|01\rangle \otimes |01\rangle + e^{i\delta_{A_i}+i\gamma_{A_i}}|10\rangle \otimes |10\rangle). \tag{21}$$

Compared with Ω_{Xi}, it has an additional restriction of Eq. (20).

The constraint Eq. (20) makes the state in Z-windows not identical to that in all X-windows. If we define an $\tilde{X}$-window as a time window whose parameters $\delta_{A_i}, \delta_{B_i}$ are in extended state Ω_{X_i} satisfying Eq. (20), the extended state for Z-windows is identical to the extended state of $\tilde{X}$-windows.

For presentation simplicity, we shall omit the subscripts i in all phase values $\delta_{A_i}, \delta_{B_i}, \gamma_{A_i}, \gamma_{B_i}$ and states. Also, we introduce states $|\chi^0\rangle, |\chi^1\rangle$ in the real-photon space for any time window:

$$|\chi^0\rangle = \frac{1}{\sqrt{2}}(e^{i\delta_B+i\gamma_B}|01\rangle + e^{i\delta_A+i\gamma_A}|10\rangle),$$
$$|\chi^1\rangle = \frac{1}{\sqrt{2}}(e^{i\delta_B+i\gamma_B}|01\rangle - e^{i\delta_A+i\gamma_A}|10\rangle),$$
$$\times \text{if } \cos(\delta_B - \delta_A) \geqslant 0, \tag{22}$$

and

$$|\chi^0\rangle = \frac{1}{\sqrt{2}}(e^{i\delta_B+i\gamma_B}|01\rangle - e^{i\delta_A+i\gamma_A}|10\rangle),$$
$$|\chi^1\rangle = \frac{1}{\sqrt{2}}(e^{i\delta_B+i\gamma_B}|01\rangle + e^{i\delta_A+i\gamma_A}|10\rangle),$$
$$\times \text{if } \cos(\delta_B - \delta_A) < 0. \tag{23}$$

2. *Virtual Protocol 1*

1-1: At any time window i, if it is a Z-window (X-window), *they* send out to Charlie the real-photon state from state Ω_Z (Ω_X) as defined by Eq. (21) [Eq. (19)] to Charlie and keep the ancillary photons locally.

1-2: Charlie announces his measurement outcome of all time windows. *They* tell each other δ_A, δ_B values through classical communication and then take postselection to all X-windows and the one-detector-clicking events from the X-windows by the following criterion:

$$1 - |\cos(\delta_B - \delta_A)| \leqslant |\lambda|, \tag{24}$$

which is identical to Eq. (20). Taking postselection by this criterion, *they* obtain $\tilde{X}$-windows and effective events of X-windows, which can be regarded as effective events of $\tilde{X}$-windows. According to our definition, an $\tilde{X}$-window satisfies Eq. (20) therefore identical to a Z-window.

Definition: After the postselection taken in Step 1-2, *they* divide their effective time windows and corresponding effective ancillary photons into four subsets according to the clicking detector (the left or the right) and the sign of $\cos(\delta_B - \delta_A)$ (positive or negative). Each subset of time windows is labeled by $\xi = (a, d)$ where $a = +, -$ and $d = L, R$.

Explicitly, time window $\xi = (a, d)$ is an effective time window heralded by joint events of a and d as defined in the following:

Event a: the sign of $\cos(\delta_B - \delta_A)$ is a ($+$ or $-$). Explicitly, $a = +$ for $\cos(\delta_B - \delta_A) \geqslant 0$, $a = -$ for $\cos(\delta_B - \delta_A) < 0$.

Event d: Detector d has clicked and the other detector has not clicked. d can be either L for the left detector or R for the right detector.

Definitions: We shall use notation Z_ξ (X_ξ) for a Z-window (X-window) with joint events of a, d for $\xi = (a, d)$. We shall also use set $\mathcal{A}_{Z_\xi}$ ($\mathcal{A}_{X_\xi}$) for the set of effective ancillary photons of time windows Z_ξ (X_ξ).

1-3: They check the phase-flip error rate E_ξ for set of $\mathcal{A}_{X_\xi}$, where $\xi = (+, L), (-, L), (+, R), (-, R)$, which is also the estimated phase-flip error rates of set $\mathcal{A}_{Z_\xi}$ and $\xi = (+, L), (-, L), (+, R), (-, R)$.

1-4: They purify the ancillary photons of time windows Z_ξ and $\xi = (+, L), (-, L), (+, R), (-, R)$ separately. After purification, *they* obtain a high-quality single-photon state $|\Phi^0\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ or $|\Phi^1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ 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 0 or 1 whenever she obtains a measurement outcome of vacuum or one photon, Bob puts down a bit value 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, i.e., the estimation of the phase-flip error rate. Charlie has determined effective ancillary photons, but Alice and Bob test the phase-flip error rate themselves in Step 1-3. Although the extended state of an X-window is not identical to that of a Z-window, the extended state of an $\tilde{X}$-window *is* identical to that of a Z-window. After the postselection condition in Step 1-2, it is equivalent to say that all effective events of X-windows are just effective events from $\tilde{X}$ windows. Therefore, an ancillary photon from set $\mathcal{A}_{X_\xi}$ is identical to an ancillary photon from set $\mathcal{A}_{Z_\xi}$. So, statistically, the phase-flip-error rate value of set $\mathcal{A}_{X_\xi}$ is exactly the value of set $\mathcal{A}_{Z_\xi}$.

Note 2: Definitions of phase-flip-error rate. Suppose set $\mathcal{A}_{X_\xi}$ contains n_ξ effective ancillary photons. If each photon of set $\mathcal{A}_{X_\xi}$ was measured in basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$ and there were $n_\xi^{(0)}$ outcomes of $|\Phi^0\rangle\langle\Phi^0|$, and $n_\xi^{(1)}$ outcomes of $|\Phi^1\rangle\langle\Phi^1|$, the phase-flip error rate for set $\mathcal{A}_{X_\xi}$ is

$$E_\xi = \frac{\min\left(n_\xi^{(0)}, n_\xi^{(1)}\right)}{n_\xi}. \tag{25}$$

Changing the values of $n_\xi^{(0)}, n_\xi^{(1)}, n_\xi$ into the corresponding values of set $\mathcal{A}_{Z_\xi}$ in Eq. (25), we can define the phase flip error rate for set $\mathcal{A}_{Z_\xi}$. Statistically, E_ξ for set $\mathcal{A}_{X_\xi}$ is also the asymptotic phase-flip error rate of set $\mathcal{A}_{Z_\xi}$. To know the values E_ξ, *they* can choose to measure each photon of set $\mathcal{A}_{X_\xi}$ in basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$. But instead of this, *they* can also choose to take local measurements in basis $\{|x\pm\rangle\}$ in each side and check the parity of each measurement outcome. (Outcomes of $|x+\rangle|x+\rangle$ or $|x-\rangle|x-\rangle$) are even-parity while $|x+\rangle|x-\rangle$ or $|x-\rangle|x+\rangle$ are odd parity.) Note that all effective ancillary photons are single photons. As is easy to see, for single photons, the fraction of odd parity (even parity) outcome from measurement of each sides in basis $\{|x\pm\rangle\}$ is exactly equal to the fraction of $|\Phi^1\rangle\langle\Phi^1|$ ($|\Phi^0\rangle\langle\Phi^0|$) outcome from the measurement in basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$. Moreover, this measurement step is needed here only for this virtual protocol, it is not needed for a real protocol. For ease of presentation, we suppose *they* use the measurement basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$.

Note 3: Reduction of preshared states for X-windows.

Reduction 1. It makes no difference to anyone outside if *they* measure all ancillary photons of X-windows in basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$ before the protocol starts. This measurement operation is on an ancillary photon, while the initial random phase-shift operation (δ_A, δ_B) is on the real-photon space, so these two operations commute. We assume *they* first take measurement of ancillary photons and then take local random phase shifts of the real-photon state for an X-window. *They* start from the preshared pair of Eq. (18). After measurement of the ancillary photon, *they* obtain one of the following outcome extended states for an X-window, depending on the measurement outcome of ancillary photon:
either

$$|\tilde{W}_0\rangle \otimes |\Phi^0\rangle, \quad |\tilde{W}_0\rangle = \frac{1}{\sqrt{2}}(e^{i\gamma_B}|01\rangle + e^{i\gamma_A}|10\rangle), \tag{26}$$

or

$$|\tilde{W}_1\rangle \otimes |\Phi^1\rangle, \quad |\tilde{W}_1\rangle = \frac{1}{\sqrt{2}}(e^{i\gamma_B}|01\rangle - e^{i\gamma_A}|10\rangle). \tag{27}$$

They then take local phase shifts δ_A, δ_B of a real-photon state of outcome extended state, which is one of the above two states. If *they* then take all steps in Virtual Protocol 1 from Step 1-1 to Step 1-4 as if *they* were using the original preshared extended states without measurement of the ancillary photons at this stage, the result should be equivalent to the original virtual protocol.

Reduction 2. Alternatively, *they* can just start with states of Eqs. (26) and (27) for their X-windows. In such a

case, an X-window is either an X_0-window with real-photon state $|\tilde{W}_0\rangle$ or an X_1-window with real-photon state $|\tilde{W}_1\rangle$. *They* need preshare classical information on Z-windows, X_0-windows, and X_1-windows. *They* preshare real-photon states $|\tilde{W}_0\rangle = \frac{1}{\sqrt{2}}(e^{i\gamma_B}|01\rangle + e^{i\gamma_A}|10\rangle)$ for X_0-windows and $|\tilde{W}_1\rangle = \frac{1}{\sqrt{2}}(e^{i\gamma_B}|01\rangle - e^{i\gamma_A}|10\rangle)$ for X_1-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; to show everything clearly we assume so for the moment.)

In an X_0-window, *they* take local private random phase shift δ_A, δ_B on the preshared state $|\tilde{W}_0\rangle$, changing it to

$$|W_0\rangle = \frac{1}{\sqrt{2}}(e^{i\delta_B+i\gamma_B}|01\rangle + e^{i\delta_A+i\gamma_A}|10\rangle). \tag{28}$$

They label a preshared state $|\Phi^0\rangle$ as the ancillary photon for this state $|W_0\rangle$ above. *They* then send the real-photon state $|W_0\rangle$ out to Charlie. After Step 1-2, *they* have known the values of δ_A, δ_B, and *they* now know the original extended state with the labeled ancillary photon

$$\Omega_{+,0} = |\chi^0\rangle\langle\chi^0| \otimes |\Phi^0\rangle\langle\Phi^0| \text{ if } \cos(\delta_B - \delta_A) \geqslant 0, \tag{29}$$

$$\Omega_{-,0} = |\chi^1\rangle\langle\chi^1| \otimes |\Phi^0\rangle\langle\Phi^0| \text{ if } \cos(\delta_B - \delta_A) < 0. \tag{30}$$

Here we have used the same definition for $|\chi^0\rangle, |\chi^1\rangle$ as used in Eqs. (22) and (23).

In an X_1-window, *they* take the same operations above to state $|\tilde{W}_1\rangle$, changing it to

$$|W_1\rangle = \frac{1}{\sqrt{2}}(e^{i\delta_B+i\gamma_B}|01\rangle - e^{i\delta_A+i\gamma_A}|10\rangle). \tag{31}$$

They label a preshared state $|\Phi^1\rangle$ as the ancillary photon for this state $|W_1\rangle$ above. *They* then send the real-photon state $|W_1\rangle$ out to Charlie. After Step 1-2, *they* will know the values of δ_A, δ_B, and *they* now know the original extended state with the labeled ancillary photon is

$$\Omega_{+,1} = |\chi^1\rangle\langle\chi^1| \otimes |\Phi^1\rangle\langle\Phi^1| \text{ if } \cos(\delta_B - \delta_A) \geqslant 0, \tag{32}$$

$$\Omega_{-,1} = |\chi^0\rangle\langle\chi^0| \otimes |\Phi^1\rangle\langle\Phi^1| \text{ if } \cos(\delta_B - \delta_A) < 0. \tag{33}$$

Here we have used the same definition for $|\chi^0\rangle, |\chi^1\rangle$ as used in Eqs. (22) and (23).

Given the orthogonal extended states by Eqs. (29), (30), (32), and (33), we can define four subsets of time windows by $X_{(a,b)}$, where $a = +, -$ and $b = 0, 1$. An $X_{(a,b)}$-window is an effective time window heralded by joint events a and b defined in the following:

Event a: the sign of $\cos(\delta_B - \delta_A)$ is a.

Event b: the ancillary state is $|\Phi^b\rangle$. Specifically,

$$\begin{aligned} &X_{(a,b)} - \text{window:} \\ &\quad a = + \text{ for } \cos(\delta_B - \delta_A) \geqslant 0, \\ &\quad a = - \text{ for } \cos(\delta_B - \delta_A) < 0, \\ &\quad b = 0 \text{ for ancillary state } |\Phi^0\rangle\langle\Phi^0|, \\ &\quad b = 1 \text{ for ancillary state } |\Phi^1\rangle\langle\Phi^1|. \end{aligned} \tag{34}$$

On the other hand, after Step 1-2, *they* can judge explicitly the values a and b if it is an effective window. Value b is determined by the preshared information, $b = 0$ for an X_0-window and $b = 1$ for an X_1-window. Value a is determined by the random phase-shift values of δ_A, δ_B chosen for the time window, $a = +$ if $\cos(\delta_B - \delta_A) \geqslant 0$, $a = -$ if $\cos(\delta_B - \delta_A) < 0$. Given an X_0-window or an X_1-window, the measurement outcome in basis $\{|\Phi^0\rangle, |\Phi^1\rangle\}$ in Step 1-3 is actually deterministic, and hence the measurement in Step 1-3 is not necessary. Therefore, according to our *Definition 1*, *they* can use the following operable definition to calculate each quantity in Eq. (25) after Step 1-2. We introduce $X_{(a,b,d)}$ for an effective time window with joint events a, b, and d, as defined in the following:

Event a: The sign of $\cos(\delta_A - \delta_B)$.

Event b: The time window is an X_b-window.

Event d: Detector d has clicked and the other detector has not clicked, $d = L$ for left detector and $d = R$ for the right detector.

For example, an $X_{(+,1,L)}$-window is a time window satisfying the following conditions:

1. At this window, $\cos(\delta_B - \delta_A) \geqslant 0$.
2. It is an X_1-window, i.e., the the ancillary photon state is $|\Phi^1\rangle\langle\Phi^1|$.
3. The left detector clicks and the right detector does not click.

We also introduce notation $N_{X_{(a,b,d)}}$ for the number of $X_{(a,b,d)}$-windows in the protocol. Therefore we have

$$n^{(0)}_{(a,d)} = N_{X_{(a,0,d)}}, \tag{35}$$

$$n^{(1)}_{(a,d)} = N_{X_{(a,1,d)}} \tag{36}$$

for Eq. (25). Given Eqs. (35) and (36), we can apply Eq. (25) immediately after Step 1-2, i.e., we have removed the measurement operation in Step 1-3.

Importantly, all values of a, b, d can be determined from the values of δ_A, δ_B, the preshared information for time window X_0 or X_1, and Charlie's announcement on the clicking detector, L or R. The ancillary photons for X-windows are actually *not* needed in the protocol.

C. Virtual Protocol 2

Here we assume *they* preshare a classical information for windows of Z, X_0, and X_1. *They* preshare the same extended states Ω_Z for Z-windows as in Virtual Protocol 1. *They* initially preshare real-photon states $|\tilde{W}_0\rangle = \frac{1}{\sqrt{2}}(e^{i\gamma_B}|01\rangle + e^{i\gamma_A}|10\rangle)$ for X_0-windows and $|\tilde{W}_1\rangle = \frac{1}{\sqrt{2}}(e^{i\gamma_B}|01\rangle - e^{i\gamma_A}|10\rangle)$ for X_1-windows. *They* take local random phase shifts δ_A, δ_B on a state $|\tilde{W}_0\rangle$ for an X_0-window and on state $|\tilde{W}_1\rangle$ for an X_1-window. After local phase shifts, *they* share a state $|W_0\rangle = \frac{1}{\sqrt{2}}(e^{i\delta_B+i\gamma_B}|01\rangle + e^{i\delta_A+i\gamma_A}|10\rangle)$ for an X_0-window and a state $|W_1\rangle = \frac{1}{\sqrt{2}}(e^{i\delta_B+i\gamma_B}|01\rangle - e^{i\delta_A+i\gamma_A}|10\rangle)$ for an X_1-window.

1. Virtual Protocol 2

2-1: At any time window i, if it is a Z-window, *they* send out the real-photon from state Ω_Z to Charlie and keep the ancillary photon locally. If it is an X_0-window (X_1-window), *they* send out to Charlie the real-photon state $|W_0\rangle$ ($|W_1\rangle$).

2-2: Charlie announces his measurement outcome of all time windows. *They* tell each other δ_A, δ_B values through classical communication and then take postselection for X-windows by the criterion of Eq. (24).

2-3: They estimate the phase-flip error rate E_ξ for sets of $\mathcal{A}_{Z_\xi}$, where $\xi = (+, L), (-, L), (+, R), (-, R)$ by the formula

$$E_{(a,d)} = \frac{\min\left(N_{X_{(a,0,d)}}, N_{X_{(a,1,d)}}\right)}{n_{(a,d)}}, \tag{37}$$

where $a = +, -$ and $d = L, R$.

2-4: They purify the effective ancillary photons in sets $\mathcal{A}_{Z_\xi}$ and $\xi = (+, L), (-, L), (+, R), (-, R)$ separately. After purification, *they* obtain a number of final states all in $|\Phi^0\rangle$ from sets $(+, L), (-, R)$, and all in $|\Phi^1\rangle$ from sets $(-, L), (+, R)$. *They* each measure the photon number locally for each purified single photon and obtain the final key k_f.

Note 1. The X_1-window is not needed. It is easy to show that the density operator ρ_0 for a time window X_0 is actually identical to the density operator ρ_1 for a time window X_1. Also, it is easy to see

$$\rho_{+,0} = \rho_{-,1}, \ \rho_{-,0} = \rho_{+,1}, \tag{38}$$

where $\rho_{a,b}$ is the density operator for time windows of $X_{(a,b)}$, taken average on all allowed values of δ_A, δ_B. This means we have

$$N_{X_{(a,1,d)}} = N_{X_{(\bar{a},0,d)}}; \tag{39}$$

therefore we can simply replace $N_{X_{(a,1,d)}}$ in the phase-flip error rate formula Eq. (37) by $N_{X_{(\bar{a},0,d)}}$. Also since $\rho_0 = \rho_1$, Eve can find no difference if we replace all X_1-windows by X_0-windows. Therefore, we don't need X_1-windows; consequently, *they* need only a classical information for Z-windows and X-windows (i.e., X_0-windows), and *they* need only an initial state $|\tilde{W}_0\rangle$ for X-windows. In this way, an X-window is just an X_0-window. Consider $N_{X_{a,1,d}}$ in Eq. (37). It can be replaced by $N_{X_{\bar{a},0,d}}$ because of Eq. (39). Further, since there is no X_1-window now, the X_0-window is just an X-window, $N_{X_{a,1,d}}$ can be further replaced by $N_{X_{(\bar{a},d)}}$, and Eq. (37) is replaced by

$$E_{(a,d)} = \frac{\min\left(N_{X_{(a,d)}}, N_{X_{(\bar{a},d)}}\right)}{n_{(a,d)}}. \tag{40}$$

Note 2. They don't need to preshare any state for X-windows. As was shown by Eq. (5) already, the two-mode coherent state can be regarded as a mixture of different two-mode photon number state. The single-photon state in Eq. (7) is equivalent to the preshared state of $|W_0\rangle$.

Note 3. Purifying all effective ancillary photon in one batch. Definitely, *they* can choose to purify all effective ancillary photons of Z-windows in one batch. The phase-flip error rate is

$$E^{ph} = \frac{\sum_{a,d} \min\left(N_{X_{(a,d)}}, N_{X_{(\bar{a},d)}}\right)}{n_1} \tag{41}$$

$$= \frac{2\sum_{d} \min\left(N_{X_{(+,d)}}, N_{X_{(-,d)}}\right)}{N_{X_{(+,L)}} + N_{X_{(-,L)}} + N_{X_{(+,R)}} + N_{X_{(-,R)}}}, \tag{42}$$

where $n_1 = N_{X_{(+,L)}} + N_{X_{(-,L)}} + N_{X_{(+,R)}} + N_{X_{(-,R)}}$ is the total number of effective X-windows. Surely, $N_{X_{(-,L)}} \geqslant \min(N_{X_{(+,L)}}, N_{X_{(-,L)}})$ and $N_{X_{(+,R)}} \geqslant \min(N_{X_{(+,R)}}, N_{X_{(-,R)}})$. Therefore the phase-flip error rate formula of Eq. (41) can be simplified into

$$E^{ph} \leqslant \frac{N_{X_{(-,L)}} + N_{X_{(+,R)}}}{n_1}, \tag{43}$$

which is simply to count the following two types of joint events as phase-flip errors:

1. Left-detector-clicking only and $\cos(\delta_B - \delta_A) < 0$.
2. Right-detector-clicking only and $\cos(\delta_B - \delta_A) \geqslant 0$.

If *they* use this formula, Charlie can make a high-quality raw state of effective ancillary photons for Alice and Bob by setting his measurement setup properly with very small probability for the left-detector-clicking (right-detector-clicking) due to the incident state of $|\chi^1\rangle$ ($|\chi^0\rangle$).

D. Virtual Protocol 3

Here we assume *they* preshare a classical information for windows of Z and X. *They* preshare the same extended states Ω_Z for Z-windows only as in Virtual Protocols 1 and 2.

1. Virtual Protocol 3

3-1: They send out the real photons of state Ω_Z in Eq. (18) for a Z-window and state ρ_X as defined in Eq. (16) in an X-window.

3-2: Charlie announces his measurement outcome. *They* each announce the random phase-shift values δ_A, δ_B and take postselection for X-windows by Eq. (24).

3-3: They verify the phase-flip error rate e_1^{ph} for effective ancillary photons with classical data of X-windows announced by Charlie through decoy-state analysis. In an X-window, an error is counted if the $\cos(\delta_B - \delta_A) \geqslant 0$ and the right detector clicks, or $\cos(\delta_B - \delta_A) < 0$ and the left detector clicks.

3-4: They take purification and local measurement of purified single photons to obtain the final key.

Note 1: e_1^{ph}, E^{ph}, and validity of the decoy-state method. The physical meaning of e_1^{ph} is the same as that of E^{ph} that appeared in Virtual Protocol 2, just the phase-flip error rate of effective ancillary photons of Z-windows. But there, the value E^{ph} is directly observed, whereas here the value e_1^{ph} is calculated by the decoy-state method.

We use notation $\mathcal{I}$ for the information of random phase-shift values δ_A, δ_B of state ρ_X postannounced in Step 3-2. According to our theorem, Eve's action with information $\mathcal{I}$ does not cause any detectable effects for any set of ancillary photons. Therefore, for any physically testable conclusion on the ancillary photons, if it is correct in the case that Eve ignores information $\mathcal{I}$, it must be also correct in the case that

Eve uses $\mathcal{I}$. Here the decoy-state analysis is to conclude the upper bound value of the phase-flip error rate of the effective ancillary photons. The conclusion is physically testable because the phase-flip error rate for the ancillary photons here is physically detectable. The conclusion from the decoy-state method for the upper bound definitely is correct if Eve ignores information $\mathcal{I}$. According to our theorem the upper-bound conclusion must also be correct in the case that Eve uses $\mathcal{I}$.

Note 2: Probabilistic mixture of different photon-number states and the decoy-state analysis. Consider Eqs. (5) and (7). We can regard the X-windows as a classical mixture of an $\mathcal{X}_1$-window and other types of X-windows, and an $\mathcal{X}_1$-window is defined as an X-window when a two-mode single photon is sent out to Charlie by Alice and Bob. We need the yield value of s_1, which is just the effective-event rate of all $\mathcal{X}_1$-windows. If, e.g., k_1 effective events are produced from K_1 $\mathcal{X}_1$-windows in the whole protocol, then $s_1 = k_1/K_1$. This can be worked out by decoy-state analysis, e.g., given three intensities $\mu_0 = 0, \mu_1, \mu_2$ and $\mu_0 = 0 < \mu_1 < \mu_2$, through directly applying Eq. (17) of Ref. [17] we have

$$s_1 \geqslant \underline{s}_1 = \frac{p_2(\mu_2)[S_{\mu_1} - p_0(\mu_1)s_0] - p_2(\mu_1)[S_{\mu_2} - p_0(\mu_2)s_0]}{p_2(\mu_2)p_1(\mu_1) - p_2(\mu_1)p_1(\mu_2)}, \tag{44}$$

where $p_k(\mu)$ is defined by Eqs. (6), (8), and (9) and s_0, S_{μ_1}, S_{μ_2} are an experimentally observed effective-event rate of X_{μ_0}-windows, X_{μ_1}-windows, X_{μ_2}-windows, and $\mu_0 = 0$. We also have the following formula for the upper bound value of the phase-flip error rate of effective ancillary photons of Z-windows:

$$e_1^{ph} \leqslant \bar{e}_1^{ph} = \frac{S_{\mu_1} E_{\mu_1}^X - e^{-2\mu_1} s_0/2}{2\mu_1 e^{-2\mu_1} s_1}. \tag{45}$$

If we use infinite intensities, we can even verify the exact value of s_1, as was applied in our numerical simulation and other works on TF-QKD.

Note 3: Quasipurification. Since *their* goal is to have the final key only, a true purification to ancillary photons is not necessary [18]. *They* can choose to measure all ancillary photons of Z-windows in advance [18] in photon-number basis and then take virtual purification to classical data of Z-windows corresponding to those effective events. *They* then take a virtual quasipurification to the classical data, which is just the final key distillation. Also, the preshared extended state for a Z-window is just $(|01\rangle\langle 01| \otimes |01\rangle\langle 01| + |10\rangle\langle 10| \otimes |10\rangle\langle 10|)/2$. The prearranged restriction of local phase shifts by Eq.(20) is now trivial and ignored in Z-windows.

E. Virtual Protocol 4

Virtual Protocol 4 is exactly equivalent to the simplified SNS protocol; *they* need an extended state Ω as Eq. (14) for a Z-window and preshare a classical information for Z-windows and X-windows.

4-1: They send out to Charlie the real photons of state Ω in a Z-window and two-mode coherent state ρ_X as defined in Eq. (16) in an X-window.

4-2: They take postselection for X-windows by the criterion of Eq. (24).

4-3: They verify the phase-flip error rate e_1^{ph} by the decoy-state analysis. Also, *they* verify n_1, the number of untagged bits in Z-basis, by decoy-state analysis.

4-4: They each observe the ancillary state for the bit value of an effective event in a Z-window. *They* take the error test for Z-basis encoding by classical communication.

4-5: After virtual purification to the classical data (final key distillation), *they* obtain the final key with the length given by Eq. (46).

Note 1. In this protocol, the state Ω of Eq. (14) for Z-basis is a classical mixture of state Ω_1 of Eq. (15) and other states. Given the notes under Virtual Protocol 3, if *they* have used only state Ω_1 for Z-windows in Virtual Protocol 4, it is equivalent to Virtual Protocol 3, which has been shown to be secure already. We can now apply the tagged model [15]. Consider Z-windows. Some of the Z-windows use the extended states of Ω_1; we name these Z-windows Z_1-windows. Suppose there are n_1 bits from Z_1-windows. These n_1 bits from Z_1-bits are regarded as the *untagged bits*. All the other bits corresponding are regarded as *tagged bits*. Applying the tagged model, *they* can distill a secure final key from all bits with length

$$n_F = n_1 - n_1 H\left(e_1^{ph}\right) - n_t H(E_Z), \tag{46}$$

where n_t is the number of total raw bits corresponding to effective events and E_Z is the bit error rate in Z-basis. An error bit in Z-basis is defined as the case that Alice's bit value is different from Bob's bit value in an effective Z-window. In the formula above, values of n_1, e_1^{ph} can be computed by the decoy-state method, while n_t, E_Z are directly observed by test. In practice, we have a coefficient f for the error correction efficiency. Taking this factor f, it is just the key length formula of Eq. (3).

Note 2: Equivalence to the real SNS protocol. Suppose in the Virtual Protocol 4 that the preshared classical information takes probability p_Z for a Z-window, probability p_{μ_k} for an X-window using intensity μ_k, and $p_Z + \sum_k p_{\mu_k} = 1$. In our real protocol, *they* each take probability q_z for a signal window and q_{μ_k} for a decoy window with intensity μ_k. In this way, the real protocol has a probability q_Z^2 for a Z-window, $q_{\mu_k}^2$ for an X_{μ_k}-window. Discarding events of all those mismatching windows, the real protocol is equivalent to Virtual Protocol 4 with a setting of

$$p_Z = q_Z^2/\mathcal{N}, \quad p_{\mu_k} = q_{\mu_k}^2/\mathcal{N}, \tag{47}$$

$$\mathcal{N} = q_Z^2 + \sum_k q_{\mu_k}^2. \tag{48}$$

But the security of Virtual Protocol 4 has already been proven. On the other hand, we can also construct another virtual protocol, including events of mismatching windows in the real protocol. Suppose in the real protocol that the real-photon state sent out for a mismatching window is $\rho_{\mathcal{M}}$.

F. Virtual Protocol 5 and complete SNS protocol

They preshare classical information on time windows of Z, $\{X_{\mu_k}\}$, and mismatching windows $\mathcal{M}$, assigning probabilities

of p_Z, $\{p_{\mu_k}\}$, and $p_{\mathcal{M}}$ for each of them. *They* also prearrange the different window commitment of Alice and Bob for the mismatching windows, i.e., make sure they have committed differently for all preagreed mismatching windows.

5-1. They send out the real photons of state Ω of Eq. (14) in a Z-window, the two-mode coherent state ρ_X as defined in Eq. (16) in an X-window, and state $\rho_{\mathcal{M}}$ in an mismatching window.

5-2: They each announce the specific type of window committed and discard those mismatching windows. *They* take postselection for X-windows by Eq. (24).

5-3 and 5-4 are identical to Virtual Protocol 4.

Note 1. The first half of 5-2 is not necessary in Virtual Protocol 5 itself, but we arrange it in order to show that the real protocol is strictly equivalent to Virtual Protocol 5. Explicitly, if we set

$$p_Z = q_Z^2,\ \ p_{\mu_k} = q_{\mu_k}^2,\ \ p_{\mathcal{M}} = 1 - p_Z - \sum_k q_{\mu_k}^2, \tag{49}$$

in Virtual Protocol 5, the real protocol is strictly equivalent to it provided that in any signal window, Alice (Bob) always places a local state $|0\rangle\langle 0|$ there whenever she (he) decides not-sending, and a local state $|1\rangle\langle 1|$ there whenever she (he) decides sending. Obviously, placing a local state is not needed in the real protocol. This completes the security of the SNS protocol.

VI. CONCLUDING REMARKS

In conclusion, following the novel idea of TF-QKD [14], we proposed the sending or not-sending TF-QKD protocol. Our protocol does not need to announce the phase information of signal pulses, and hence the traditional decoy-state formulas can be directly applied. The single-photon interference is not needed in Z-basis, and thus the error rate in Z-basis can be negligibly small. This makes the protocol tolerable to a fairly large error rate in X-basis, where single-photon interference must be done. Numerical simulation shows that the protocol can exceed a secure distance of 800 km without misalignment error, and more than 700 km with a misalignment error of 15%. Even though the misalignment error for the single-photon interference is as large as 25%, the protocol can still reach a secure distance of more than 600 km, because of the revolutionary progress made by TF-QKD proposed in Ref. [14].

Note added. Recently we became aware of recent work where it was suggested to use different key rate formulas directly pointing to non-random-phase coherent states [19,20].

ACKNOWLEDGMENTS

We acknowledge the financial support in part by The National Key Research and Development Program of China Grant No. 2017YFA0303901; NSFC Grants No. 11474182, No. 11774198, and No. U1738142; the key Research and Development Plan Project of Shandong Province, Grant No. 2015GGX101035; Shandong Peninsula National Innovation Park Development Project.

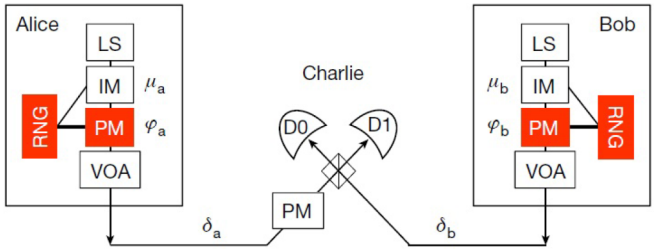

FIG. 3. Schematic picture of TF-QKD taken from Ref. [14].

APPENDIX: EAVESDROPPING SCHEME BASED ON LATER ANNOUNCED PHASE INFORMATION OF SIGNAL STATES

Earlier we showed that our protocol can apply the traditional decoy-state method directly because the phase information of signal states is never announced. But if it were announced and it took a role in the bit value, then there were eavesdropping schemes effectively attacking the secret bits. Here we show this by a specific scheme. Consider the original TF-QKD protocol [14] as shown in Fig. 3. Suppose that a coherent state of intensity μ is used by each side for signal pulses. The pulse pairs are phase modulated before being sent out for Charlie. The phase modulation includes the coding phase (0 or π) at each side and the random phase shift we assume to be ρ at both sides [14]. After modulation, the states of signal pulse pairs are two-mode coherent states $|\psi^+\rangle = |\sqrt{\mu}e^{i\rho}\rangle|-\sqrt{\mu}e^{i\rho}\rangle$ for bit value 0 and $|\psi^-\rangle = |-\sqrt{\mu}e^{i\rho}\rangle|\sqrt{\mu}e^{i\rho}\rangle$ for bit value 1, which will cause clicking of detector $D0$ only, and also $|\phi^+\rangle = |\sqrt{\mu}e^{i\rho}\rangle|\sqrt{\mu}e^{i\rho}\rangle$ for bit value 0 and $|\phi^-\rangle = |-\sqrt{\mu}e^{i\rho}\rangle|-\sqrt{\mu}e^{i\rho}\rangle$ for bit value 1, which will cause the clicking of detector $D1$ only. Note that the strong reference light is controlled by Eve; here we have assumed the reference phase to be 0 for conciseness. Eve applies the following scheme:

Step 0: Eve can set whatever channel transmittance. For simplicity, we assume Eve sets the channel transmittance to be 1 here. Consider Fig. 1. Before the twin pulses enter the beam splitter, Eve (Charlie) just honestly does whatever as requested by the the TF-QKD protocol.

Step 1: Eve takes nondestructive crude measurement to project the output light from the beam splitter to the vacuum or nonvacuum subspace. Suppose she obtains nonvacuum, she stores the detected state and continues the attacking scheme.

Step 2: Eve takes a crude measurement to project the stored state either to the subspace $\mathcal{S} = \{|1\rangle, |2\rangle\}$ or to the subspace $\tilde{\mathcal{S}} = \{|3\rangle, |4\rangle, |5\rangle, \dots\}$. Suppose the outcome is $\mathcal{S}$, she stores the state and continues.

Step 3: Eve takes the following unitary transformation to her stored state above: $|1\rangle \to \sqrt{\mu}|1\rangle + \sqrt{1-\mu}|m_0\rangle$, $|2\rangle \to |2\rangle$ where $|m_0\rangle$ is a state orthogonal to both $|1\rangle$ and $|2\rangle$. Eve takes a crude measurement which collapses the stored state in Step 3 either to state $|m_0\rangle$ or to the subspace $\mathcal{S}$ spanned by the Fock states $\{|1\rangle, |2\rangle\}$. Suppose she obtains subspace $\mathcal{S}$ in Step 3, she stores

the state and announces which detector ($D0$ or $D1$) has counted. She waits until Alice and Bob's announcement, then goes to Step 4.

Note: Until now we always assume Eve obtains the results in favor of her attacking in those non-trace-preserving maps. The point is that, at any step, if Eve doesn't obtain the measurement outcome in her favor, she just announces that she has not detected anything.

Step 4: After Alice and Bob announce the value of ρ, bases of each pulse pairs, and which pulses are decoy pulses and which pulses are signal pulses, Eve can take a phase-shift operation to her stored state, changing it into one of the following two states corresponding to bit value 0 or 1 of the incident pulse pair: $\frac{1}{\sqrt{2}}(|1\rangle \pm |2\rangle)$. This enables Eve to know the bit value for sure without causing any noise by a projective measurement.

Here are details of the state evolution for the non-trace-preserving map above. Suppose at Step 1 only detector $D0$ counts, and the incident state can be either $|\psi^+\rangle$ or $|\psi^-\rangle$. If the incident state is $|\psi^+\rangle$, the stored states $\{|\psi_i^+\rangle\}$ at the end of each step $\{i\}$ are $|\psi_1^+\rangle = \mathcal{N}_1 \sum_{k=1}^{\infty} \frac{(\sqrt{2\mu}e^{i\rho})^k}{\sqrt{k!}}|k\rangle$; $|\psi_2^+\rangle = \mathcal{N}_2(\sqrt{\mu}|1\rangle + \mu e^{i\rho}|2\rangle)$; $|\psi_4^+\rangle = \frac{1}{\sqrt{2}}(|1\rangle + e^{i\rho}|2\rangle)$; $|\psi_5^+\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$. All parameters $\mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_4$ are normalization factors.

Similarly, given the incident states $\{|\psi^-\rangle\}$, we can also calculate the time evolution of $\{|\psi^-\rangle\}$ at each step $\{i\}$, and we obtain $|\psi_5^-\rangle = \frac{1}{\sqrt{2}}(-|1\rangle + |2\rangle)$. This means $|\psi_5^+\rangle$ and $|\psi_5^-\rangle$ are orthogonal to each either and Eve can know the corresponding bit value for sure. In the same way, one can easily show that Eve can also obtain full information of bit values without causing a disturbance.

In the eavesdropping above, the fraction of bits caused by the single-photon state is 50% among all raw bits. According to the key rate formula [Eq. (2)] of Ref. [14], TF-QKD will present a key rate of 50% from raw key to final key, although the actual key rate is obviously 0. This means the key rate formula does not match the protocol itself there. The root of the problem is that Eve can make use of the postannounced phase information of signal states there. Given that protocol, one has to apply a different key rate formula.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] N. Gisin, G. Ribordy, W. Tittel *et al.*, Rev. Mod. Phys. **74**, 145 (2002); N. Gisin and R. Thew, Nat. Photonics **1**, 165 (2006); M. Dušek, N. Lütkenhaus, M. Hendrych, in *Progress in Optics VVVX*, edited by E. Wolf (Elsevier, Amsterdam, 2006), pp. 381–454; V. Scarani, H. Bechmann-Pasqunucci, N. J. Cerf *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).

[3] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[4] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[5] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[6] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[7] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

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

[9] Y. Liu, T.-Y. Chen, L.-J. Wang *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).

[10] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **93**, 042324 (2016).

[11] L. C. Comandar, M. Lucamarini, B. Fröhlich *et al.*, Nat. Photonics **10**, 312 (2016).

[12] H.-L. Yin, T.-Y. Chen, Z.-W. Yu *et al.*, Phys. Rev. Lett. **117**, 190501 (2016).

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

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

[15] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007); D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, in *Proceedings of the International Symposium on Information Theory (ISIT 2004), Chicago, IL, USA* (IEEE, New York, 2004).

[16] The data of time windows other than Z-windows and X-windows, e.g., a time window when one party decides to send a decoy pulse and the other party decides not-sending, can offer more data for the decoy-state analysis. This is useful in nonasymptotic study of the decoy-state method application.

[17] X.-B. Wang, C.-Z. Peng, J. Zhang, L. Yang, and J.-W. Pan, Phys. Rev. A **77**, 042311 (2008).

[18] P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

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

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