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

Xiao-Long Hu\textsuperscript{1}, Cong Jiang\textsuperscript{1}, Zong-Wen Yu\textsuperscript{2}, and Xiang-Bin Wang\textsuperscript{1,3,4,5}\textsuperscript{*}

\textsuperscript{1}State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, Peoples Republic of China
\textsuperscript{2}Data Communication Science and Technology Research Institute, Beijing 100092, China
\textsuperscript{3}Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China Hefei, Anhui 230026, China
\textsuperscript{4}Jinan Institute of Quantum technology, SAICT, Jinan 250101, Peoples Republic of China
\textsuperscript{5}Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, China

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

PACS numbers: 03.67.Dd, 42.81.Gs, 03.67.Hk

I. INTRODUCTION

Quantum key distribution provides a method for unconditionally secure communication\textsuperscript{[1,2]} between two parties, Alice and Bob. Combined with the decoy-state method\textsuperscript{[10–15]} and measurement-device-independent QKD (MDIQKD) protocol\textsuperscript{[16,17]}, QKD can overcome the security loophole from the nonideal single-photon sources\textsuperscript{[18–20]} and imperfect detection devices\textsuperscript{[21,22]} and has developed rapidly both in theory\textsuperscript{[23–40]} and experiment\textsuperscript{[41–63]}. The maximum distance of decoy-state MDIQKD has been experimentally increased to 404 kilometers\textsuperscript{[64]}. But the key rate of BB84, MDIQKD protocol, or any modified version of these protocols cannot exceed the linear bounds of repeaterless QKD, such as the TGW bound\textsuperscript{[65]} and the PLOB bound\textsuperscript{[66]}.

Recently, a new protocol named twin-field quantum key distribution (TFQKD) was proposed\textsuperscript{[67]} whose key rate dependence on the channel transmittance $\eta$ is $R \sim O(\sqrt{\eta})$. Following this protocol, many variants of TFQKD were proposed\textsuperscript{[68–79]} and some experiments of TFQKD were demonstrated\textsuperscript{[80–83]}. Among those protocols, one efficient protocol named the sending-or-not-sending (SNS) protocol\textsuperscript{[68]} has the advantages of unconditionally secure under coherent attacks and it can tolerate large misalignment error. And the SNS protocol with finite data size has been studied\textsuperscript{[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 sources and the probability for sending coherent pulses in the $Z$ windows.

II. GENERAL SNS PROTOCOL WITH ASYMMETRIC SOURCE PARAMETERS

A schematic of our general SNS protocol is shown in Figure\textsuperscript{[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
and known by anyone. The private phase $\delta_A$ parameters:

\[ \mu_A, \mu_B, \epsilon_A, \epsilon_B, \gamma_A, \text{ and } \gamma_B \] are random variables chosen differently in different time windows.

**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 the phase $\gamma_A$ and $\gamma_B$ by phase compensation. His action only affects the key rate, but has not influence on the security of the protocol.

**Step 3.** They announce each one’s decoy windows and signal windows. And they announce the intensities of the decoy pulses and the private phases $\delta_A$ and $\delta_B$ in each decoy window.

**Definition:** We define a $Z$-window when both of them determine signal windows and an $X$-window when both of them determine decoy windows. We define an effective event when one and only one Charlie’s detector clicks, and the corresponding window is called an effective window.

Given that $\delta_A$ ($\delta_B$) is randomized, whenever Alice (Bob) sends a coherent state with intensity $\mu_A$ ($\mu_B$), it can be equivalently regarded as a density matrix $\sum_{k=0}^{\infty} e^{-\nu_A} \mu_A^k |k\rangle \langle k|$ ($\sum_{k=0}^{\infty} e^{-\nu_B} \mu_B^k |k\rangle \langle k|$), 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 don’t 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 $X_1$-windows, in which they choose the intensities $\mu_A$ and $\mu_B$ with the same $k$ and the phase shifts $\delta_A$ and $\delta_B$ satisfy the restriction

\[ 1 - | \cos(\delta_A - \delta_B + \Delta \varphi) | \leq |\lambda|. \tag{2} \]

Here the values $\Delta \varphi$ and $\lambda$ are some values determined by Alice and Bob according to the result of channel test and calibration in the experiment to obtain a satisfactory key rate and the value of $\Delta \varphi$ can be different from time to time. In this paper, we will set $\Delta \varphi = 0$ for presentation simplicity, i.e.

\[ 1 - | \cos(\delta_A - \delta_B) | \leq |\lambda|, \tag{3} \]

but this doesn’t affect the validity of the security proof if we use Eq. (2) for the post selection. They keep the data of the effective events and discard all the others.

**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 $\delta_A$ and $\delta_B$ in effective $X$-windows, they calculate $c_1^{ph}$, the phase-flip error rate of effective events in $Z$-windows.

**Note:** In effective $X$-windows, an error occurs when (1) the left detector clicks and $\cos(\delta_A - \delta_B) < 0$ (2) the right detector clicks and $\cos(\delta_A - \delta_B) > 0$. Given this definition, they can observe the error rates in $X$-windows for each intensities of input light. With this, they can estimate $c_1^{ph}$ through the decay state analysis which requests them to observe the counting rates of various intensities of input light. As proved in ref. [68], decay state method can applied to our protocol as if the phases $\delta_A$ and $\delta_B$ were not announced. In the asymptotic case that there are decoy states with finite different intensities, they can obtain the exact value of $c_1^{ph}$. In the case that there are decoy states with finite different intensities, they can obtain the upper bound of $c_1^{ph}$.

**Note:** The Appendix shows the four-intensity method of this protocol. In this case, the formulas for $n_1$ and $c_1^{ph}$ are given in Eqs. (37)-(40).

**Step 6.** They perform the post-processing and obtain the final key with length

$$N_f = n_1[1 - H(e_1^{ph})] - fn_t H(E_Z)$$

(4)

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. Details for calculating the length of the final key (or the key rate) with 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 proof the security of our protocol.

Imagine that in a $Z$-window, if Alice (Bob) decides to send a coherent state $\rho_A$ ($\rho_B$) 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 the state $|0\rangle$ ($|1\rangle$). To Alice (Bob), the state $|1\rangle$ corresponds to the bit value 1 (0), and the state $|0\rangle$ corresponds to the bit value 0 (1). We define subspace $T$ 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 $T \otimes \mathcal{A}_n$ in the $Z$-window can be written as

$$\Omega = \epsilon_A \epsilon_B (\rho_A \hat{\otimes} \rho_B) \otimes |11\rangle \langle 11|$$

$$+ \epsilon_A (1 - \epsilon_B)(\rho_A \hat{\otimes} |0\rangle \langle 0| \otimes |10\rangle \langle 10|)$$

$$+ (1 - \epsilon_A)\epsilon_B(|0\rangle \langle 0| \hat{\otimes} \rho_B \otimes |01\rangle \langle 01|)$$

$$+ (1 - \epsilon_A) (1 - \epsilon_B)(|0\rangle \langle 0| \hat{\otimes} |00\rangle \langle 00| \otimes |00\rangle \langle 00|).$$

(5)

Here both symbols $\otimes$ and $\hat{\otimes}$ are for a tensor product, and $\hat{\otimes}$ is the tensor product inside $T$, and $\otimes$ is the tensor product between $T$ and $\mathcal{A}_n$. The states on the left side of $\otimes$ are in $T$ 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 $\delta_A$ and $\delta_B$ in $Z$-windows are kept secret all the time, the coherent states $\rho_A$ and $\rho_B$ are actually phase-randomized coherent states, whose density matrices are

$$\rho_k = \sum_{n=0}^{\infty} \frac{\epsilon^{n_k} \mu_k^n}{n!} |n\rangle \langle n| = \mu_k e^{-\mu_k} [1] + (1 - \mu_k e^{-\mu_k}) \tilde{\rho}_k,$$

(6)

with $k = A, B$ and

$$\tilde{\rho}_k = \frac{1}{1 - \mu_k e^{-\mu_k}} \sum_{n \neq 1} \frac{\epsilon^{-\mu_k} \mu_k^n}{n!} |n\rangle \langle n|.$$

(7)

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

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

(8)

and

$$\Omega_1 = C_1 [\epsilon_A (1 - \epsilon_B) \mu_A e^{-\mu_A} |10\rangle \langle 10| \otimes |10\rangle \langle 10|]$$

$$+ \epsilon_B (1 - \epsilon_A) \mu_B e^{-\mu_B} |01\rangle \langle 01| \otimes |01\rangle \langle 01|]$$

$$\Omega_2 = C_2 [\epsilon_A (1 - \epsilon_B) (1 - \mu_A e^{-\mu_A}) (\rho_A \hat{\otimes} |0\rangle \langle 0| \otimes |10\rangle \langle 10|]$$

$$+ \epsilon_B (1 - \epsilon_A) (1 - \mu_B e^{-\mu_B}) ((|0\rangle \langle 0| \hat{\otimes} \rho_B) \otimes |01\rangle \langle 01|)$$

$$\Omega_3 = |00\rangle \langle 00| \otimes |00\rangle \langle 00|$$

$$\Omega_4 = (\rho_A \hat{\otimes} \rho_B) \otimes |11\rangle \langle 11|$$

(9)

where $C_1$ and $C_2$ are some normalization factors. With the condition in Eq. (11), $\Omega_1$, the target state we used to prove the security, can be written as

$$\Omega_2 = C^2 (\mu_A |10\rangle \langle 10| \otimes |10\rangle \langle 10| + \mu_B |01\rangle \langle 01| \otimes |01\rangle \langle 01|)$$

(10)

with

$$C = \frac{1}{\sqrt{\mu_A} + \mu_B}.$$

(11)

In $X$-windows, the two-mode states sent by them are

$$\rho_{Xk} = |\beta_k\rangle \langle \beta_k|$$

(12)
where
\[
|\beta_k\rangle = \left| \sqrt{\mu_A} e^{i\gamma_A + i\delta_k} \right|_{A} |0\rangle + \sqrt{\mu_B} e^{i\gamma_B + i\delta_k} |1\rangle_{B} \right) \right). \tag{13}
\]

In our protocol, the states in the Z-windows are actually classical mixtures of \(\Omega_1\), \(\Omega_2\), \(\Omega_3\), and \(\Omega_4\). In the security proof, we first show the security of the protocol with only the state \(\Omega_1\) and then show the security of the protocol with \(\Omega\) by the tagged model \[10, 11\].

**B. Virtual Protocol 1**

Definition: We have define an effective event in the protocol. 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
\[
\Omega_0 = |\Psi\rangle \langle \Psi| \tag{14}
\]
where
\[
|\Psi\rangle = C\left(\sqrt{\mu_A} e^{i\gamma_A} |10\rangle \otimes |10\rangle + \sqrt{\mu_B} e^{i\gamma_B} |01\rangle \otimes |01\rangle \right) \tag{15}
\]
and \(\gamma_A\) and \(\gamma_B\) are announced publicly. (Remind that \(\Omega_0\) and \(\Psi\) 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 \(\delta_A\) and Bob chooses a random phase \(\delta_B\), which satisfy the restriction Eq. (3). Then they take phase shifts \(\delta_A\) and \(\delta_B\) to their own real photons, respectively. In the time window \(i\) which is a X-window, they take random and independent phase shifts \(\delta_A\) and \(\delta_B\) to their own real photons, respectively. After the phase shifts, the extended state changes into
\[
\Omega_Z = |\Psi\rangle \langle \Psi|, \quad \Omega_X = |\Psi\rangle \langle \Psi| \tag{16}
\]
and
\[
|\Psi\rangle = C\left(\sqrt{\mu_A} e^{i\gamma_A + i\delta_A} |10\rangle \otimes |10\rangle + \sqrt{\mu_B} e^{i\gamma_B + i\delta_B} |01\rangle \otimes |01\rangle \right) \tag{17}
\]

Among all X-windows, we define a set of X-windows, in which the phase shifts \(\delta_A\) and \(\delta_B\) satisfy the restriction Eq. (3). The states in Z-windows are not identical to those in X-windows, but they are identical to those in X-windows.

Besides, we define real-photon states \(|\chi^0\rangle\) and \(|\chi^1\rangle\) for any time window:
\[
|\chi^0\rangle = C\left(\sqrt{\mu_A} e^{i\gamma_A + i\delta_A} |10\rangle + \sqrt{\mu_B} e^{i\gamma_B + i\delta_B} |01\rangle \right) \tag{18}
\]
\[
|\chi^1\rangle = C\left(\sqrt{\mu_A} e^{i\gamma_A + i\delta_A} |10\rangle - \sqrt{\mu_B} e^{i\gamma_B + i\delta_B} |01\rangle \right) \tag{19}
\]
if \(\cos(\delta_A - \delta_B) < 0\)

or
\[
|\chi^0\rangle = C\left(\sqrt{\mu_A} e^{i\gamma_A + i\delta_A} |10\rangle - \sqrt{\mu_B} e^{i\gamma_B + i\delta_B} |01\rangle \right) \tag{20}
\]
\[
|\chi^1\rangle = C\left(\sqrt{\mu_A} e^{i\gamma_A + i\delta_A} |10\rangle + \sqrt{\mu_B} e^{i\gamma_B + i\delta_B} |01\rangle \right) \tag{21}
\]
if \(\cos(\delta_A - \delta_B) > 0\)

2. Protocol

**V1-1:** At any Z-window (X-window), they send the real photons of \(\Omega_Z (\Omega_X)\) defined in Eq. (10) 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 \(\gamma_A\) and \(\gamma_B\). He announces his measurement outcome and then they announce the values of \(\delta_A\) and \(\delta_B\) of all X-windows. With the preshared information of X- and Z-windows, the measurement outcome, and the announced values of \(\delta_A\) and \(\delta_B\), they can obtain effective Z-windows and effective 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 or the right R) and the sign of \(\cos(\delta_A - \delta_B)\) (positive or negative −). These subsets is labeled as \(\Gamma_{(a,d)}\) where \(\Gamma = X, Z, a = +, -,\) 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 \(A_{\Gamma_{(a,d)}}\).

**V1-3:** They check the phase-flip error rate \(E_{(a,d)}\) of the set \(A_{\tilde{X}_{(a,d)}}\), 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 \(A_{\tilde{X}_{(a,d)}}\) should be the same as that of \(A_{\tilde{E}_{(a,d)}}\) (asymptotically).

Note: The state \(|\Psi\rangle\) in Eq. (10) can be written in another form:
\[
|\Psi\rangle = \frac{1}{\sqrt{2}}(|\chi^0\rangle \otimes |\Phi^0\rangle + |\chi^1\rangle \otimes |\Phi^1\rangle), \text{ if } a = + \tag{20}
\]
or
\[
|\Psi\rangle = \frac{1}{\sqrt{2}}(|\chi^1\rangle \otimes |\Phi^0\rangle + |\chi^0\rangle \otimes |\Phi^1\rangle), \text{ if } a = - \tag{21}
\]
where \(|\Phi^k\rangle, k = 0, 1\) are two-mode states of ancillary photons:
\[
|\Phi^0\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle), |\Phi^1\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \tag{22}
\]
To obtain the phase-flip error rate \(E_{(a,d)}\) of the set \(A_{\tilde{X}_{(a,d)}}\), each ancillary photon of this set is measured in the basis \(|\Phi^0\rangle, |\Phi^1\rangle\) and there are \(n_{(a,d)}^{(0)}\) outcomes of
|Φ⟩|Φ⟩ and n(0) and n(1) outcomes of |Φ⟩|Φ⟩. The phase-flip error rate \( E_{(a,d)} \) of \( \mathcal{A}_{X(a,d)} \) is defined as:

\[
E_{(a,d)} = \frac{\min(n(0)(a,d), n(1)(a,d))}{n(a,d)}
\]

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.

Virtual Protocol 2

1. Preparation stage

For each time window \( i \), 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. If the phase-flip error rate should be changed correspondingly. We introduce a symbol *p* for the set of effective time windows, which satisfy the restriction in Eq. (3), with joint events a, b, d where

\[
E_{(a,d)} = \frac{\min(N^{(a,d)}, N_{X(a,b,d)})}{n(a,d)}
\]

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

C. Virtual Protocol 2

1. Preparation stage

For each time window \( i \), they prepare and send real photons in the state \(|\chi^+\rangle\) in \( X_0 \)-window or in \( X_1 \)-window. They prepare and send real photons in the state \(|\chi^-\rangle\) in \( X_0 \)-window or in the state \(|\chi^-\rangle\) in \( X_1 \)-window.

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 phase \( \gamma_A \) and \( \gamma_B \). He announces his measurement outcome and then they announce the values of \( \delta_A \) and \( \delta_B \) of all X-windows.

V2-3: They check the phase-flip error rate \( E_{(a,d)} \) by the set \( \hat{X}(a,b,d) \) and \( \hat{X}(a,1,d) \), 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.

$$\rho(\pm,0) = \rho(\pm,1), \rho(-,0) = \rho(+,1).$$

(28)

So we can conclude that $N_{\bar{X}(a,0,d)} = N_{\bar{X}(a,1,d)}$, where $\bar{a}$ stands for the opposite sign of $a$. This means that all the values $N_{\bar{X}(a,1,d)}$ in the phase-flip error rate in Eq. (27) can be replaced by $N_{\bar{X}(a,0,d)}$ 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 $n_{\bar{X}(a,d)}$. The formula of the phase-flip error rate should be changed into:

$$E_{(a,d)} = \frac{\min(n_{\bar{X}(a,d)}, n_{\bar{X}(a,d)})}{n_{(a,d)}}$$

(29)

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

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

$$E_{ph}^{Z} = \frac{\sum_{a,d} \min(n_{\bar{X}(a,d)}, n_{\tilde{X}(a,d)})}{\sum_{a,d} n_{(a,d)}}$$

(30)

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

$$E_{ph}^{Z} \leq \frac{n_{\bar{X}(+,+)} + n_{\bar{X}(++,--)}}{n_1}.$$  

(31)

In this formula for the phase-flip error rate, we only need the total number of effective events in $X$-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 $\cos(\delta_A - \delta_B) > 0$.

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 $\lambda$ 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. (12) with randomized $\delta_A$ and $\delta_B$ can be written as the classical mixture of a set of states $\{|\psi^{(k)}_1\rangle\}$:

$$\rho_{X,k} = \sum_l p_l^{(k)} |\psi^{(k)}_l\rangle\langle\psi^{(k)}_l|$$

with

$$|\psi^{(k)}_l\rangle = D^{(k)}_{n} \sum_{n=0}^{\min(l,n)} \frac{(\sqrt{\mu_{Ak} e^{i\delta_A + i\gamma_A}})^n}{\sqrt{n!}} \frac{(\sqrt{\mu_{Bk} e^{i\delta_B + i\gamma_B}})^{l-n}}{\sqrt{(l-n)!}} |n,l-n\rangle$$

(33)

where $D^{(k)}_{n}$ are some normalization factors and $|\psi^{(k)}_1\rangle$ is exactly $|\chi^+\rangle$ when the condition in Eq. (11) is satisfied. So they don’t 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 $|\chi^+\rangle$, $e_{1}^{ph}$.

**Note:** If some decoy states with intensities $\mu_{Am}$ and $\mu_{Bm}$ are not used to estimate $e_{1}^{ph}$, these intensities don’t have to satisfy the constrain in Eq. (1).

### 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 $\Omega_Z$ in Eq. (16) for $Z$-windows.

#### 2. Protocol

**V3-1:** At any $Z$-window, they send out the real photons of $\Omega_Z$ to Charlie and keep the ancillary photons locally. At any $X$-window, Alice (Bob) sends a coherent state $|\sqrt{\mu_{Ak} e^{i\delta_A + i\gamma_A}}\rangle$ to $|\sqrt{\mu_{Bk} e^{i\delta_B + i\gamma_B}}\rangle$ with random $\delta_A$ and $\delta_B$ 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 $\gamma_A$ and $\gamma_B$. He announces his measurement outcome and then they announce the values of $\delta_A$ and $\delta_B$ of all $X$-windows.

**V3-3:** They apply decoy-state method with the data of the effective $\bar{X}$-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 $\Omega_2$ with the restriction Eq. 9 is identical to $\Omega_2$ without the restriction Eq. 9. If we regard all Z-windows as a whole, the condition in Eq. 9 can be loosen, which means that the phase shifts $\delta_A$ and $\delta_B$ to the real photons can be randomized in the range $[0, 2\pi]$ independently. In this way, they don’t need any mutual information about the phase shifts $\delta_A$ and $\delta_B$.

**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 9. In the latter process, the state in Z-window is

$$\Omega'_2 = C^2(\mu_{A1}|10⟩⟨10|\otimes|10⟩⟨10| + \mu_{B1}|01⟩⟨01|\otimes|01⟩⟨01|),$$

which is equivalent to the state $\Omega_1$ in Eq. 10. This means that the protocol can just start with the state $\Omega$ and apply the tagged model to distill the final key from the effective events using the state $\Omega_1$. The length of the final key should be

$$n_f = n_1[1 - H(e_1^{ph})] - n_t H(E_Z)$$

where $n_1$ is the number of effective events with state $\Omega_1$ estimated by 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 by probability $p^Z_A$ ($p^Z_B$) and determines a decoy window with intensity $\mu_{Ak}$ ($\mu_{Bk}$) by probability $p^X_A$, $p^X_B$, where $p^Z_A + \sum_k p^X_{Ak} = 1$ ($p^Z_B + \sum_k p^X_{Bk} = 1$). 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 don’t need to preshare any information of time windows, and the states in Z-windows and X-windows are $\Omega$ and $\rho_{Xk}$, respectively.

With the reductions above, the virtual protocol is equivalent to our asymmetric SNS protocol.

### IV. NUMERICAL SIMULATION WITH ASYMMETRIC CHANNELS

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.

| $N_t$ | $e_d$ | $d$ | $\eta_d$ | $f_e$ | $\xi$ | $\alpha$ |
|-------|-------|-----|----------|-------|------|--------|
| 10^{13} | 5% | 10^{-10} | 50% | 1.1 | 10^{-10} | 0.2dB/km |

**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; $\eta_d$ is the detection efficiency of each detector at the UTP; $f_e$ is the error correction inefficiency. $\xi$ is the failure probability in the parameter estimation; $\alpha$ is the channel loss.

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 single-photon, $e_1^{ph}$. In the modified SNS protocol, they still use the same source parameters, but Charlie add 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, $\eta_A$, is larger than that of Bob’s channel, $\eta_B$, Charlie adds an extra loss $1 - \eta_B/\eta_A$ to Alice’s channel. 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 doesn’t 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 general 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 Figure 2 and Figure 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 km and 100 km, respectively. In the figures, we have also compared our results with the linear bound of the repeaterless QKD. There are excellent theoretical linear bounds for key rate of a repeaterless QKD, such as the famous TGW bound 12 and the PLOB bound 13. Also, we show some details of the optimal key rates with different SNS protocols in Table I. It’s easy to find that in the asymmetric channels, the performance of our general 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 a general SNS protocol with asymmetric source parameters and give a security proof of this protocol. The intensities and the probabilities for
sensing at Alice’s and Bob’s sides should satisfy the condition given in Eq. (11) to guarantee the security in the asymmetric case. We present the numerical results of different SNS protocols to show that our general 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 general SNS protocol is tens to hundreds of times higher than that of the original SNS protocol. Our general SNS protocol can be applied directly to the SNS experiments with asymmetric channels.

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

Appendix: Formulas For Key Rate Calculation

A. 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, $\mu'_A (\mu'_B)$ in signal windows and $0, \mu_{A1} (\mu_{B1}), \mu_{A2} (\mu_{B2})$ in decoy windows. All measurement results in effective $X$-windows are used to estimate the bound of $n_1$. Only measurement results in effective $X$-windows when Alice uses the intensity $\mu_{A1}$ and Bob uses the intensity $\mu_{B1}$ are used to estimate the bound of $e_{1h}^p$.

The formula for the length of the final key in Eq. (11) can be written in the form of key rate per time window:

$$R = p_{APB}^Z \left[ \frac{e_A (1 - e_B) \mu'_A e^{-\mu'_A} + e_B (1 - e_A) \mu'_B e^{-\mu'_B}}{s_z^2 [1 - H(e_{1h}^p)] - f S_Z H(E_Z)} \right]$$

(36)

where $s_z^2$ 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 $\zeta$ of $n$ time windows, the counting rate of $\zeta$ is defined as $S_\zeta = m/n$.

So we need to estimate the bound of $\langle s_z^2 \rangle$ and $\langle e_{1h}^p \rangle$ 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. [34], the lower bound of $\langle s_z^2 \rangle$ is given by:

$$\langle s_z^2 \rangle \geq \langle s_{10}^Z \rangle = \frac{\mu_{A1}}{\mu_{A1} + \mu_{B1}} \langle s_{01}^Z \rangle + \frac{\mu_{B1}}{\mu_{A1} + \mu_{B1}} \langle s_{01}^Z \rangle$$

(37)

where $\langle s_{01}^Z \rangle$ is lower bound of the expected value of the
Here rate of $\tilde{m}$ µ pulses with intensities $|\text{counting rate of the state }|0\rangle\langle 0|$ with

$$\langle \tilde{S}_{10} \rangle = \frac{\mu_{A2}^{2}e^{\mu_{A1}}(S_{\mu_{A1}}) - \mu_{A1}^{2}e^{\mu_{A2}}(S_{\mu_{A2}}) - (\mu_{A2}^{2} - \mu_{A1}^{2})(S_{00})}{\mu_{A1}\mu_{A2}(\mu_{A2} - \mu_{A1})}$$

(38)

and $\langle \tilde{S}_{00} \rangle$ is lower bound of the expected value of the counting rate of the state $|01\rangle\langle 01|$ with

$$\langle \tilde{S}_{00} \rangle = \frac{\mu_{B2}^{2}e^{\mu_{B1}}(S_{0\mu_{B1}}) - \mu_{B1}^{2}e^{\mu_{B2}}(S_{0\mu_{B2}}) - (\mu_{B2}^{2} - \mu_{B1}^{2})(S_{00})}{\mu_{B1}\mu_{B2}(\mu_{B2} - \mu_{B1})}$$

(39)

Here $\langle S_{\alpha\beta} \rangle$ is the expected value of the counting rate of the time windows when Alice and Bob send the decay pulses with intensities $\alpha$ and $\beta$, 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. The upper bound of $\langle e_{1}^{\text{ph}} \rangle$ is given by:

$$\langle e_{1}^{\text{ph}} \rangle \leq \langle e_{1}^{\text{ph}} \rangle = \frac{(T_{\Delta}) - e^{-(\mu_{A1} + \mu_{B1})}(S_{00})/2}{e^{-(\mu_{A1} + \mu_{B1})}(\alpha_{1}^{2})}$$

(40)

where $\langle T_{\Delta} \rangle$ is the expected value of the error counting rate of $X$-windows, when Alice and Bob send the decay pulses with intensities $\mu_{A1}$ and $\mu_{B1}$, respectively. If there are many error windows in a set $\zeta$ of $n$ time windows, the error counting rate of $\zeta$ is defined as $T_{\zeta} = m/n$.

B. 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 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 $X = \sum_{i=1}^{n} X_{i}$, and $\phi$ be the expected value of $X$. We have the lower and the upper bound of $\phi$:

$$\phi^{L}(X) = \frac{X}{1 + \delta_{1}(X)}$$

(41)

$$\phi^{U}(X) = \frac{X}{1 - \delta_{2}(X)}$$

(42)

where $\delta_{1}(X)$ and $\delta_{2}(X)$ are the solutions of the following equations:

$$\left( \frac{e^{\delta_{1} \mu_{A1}}}{(1 + \delta_{1})^{1+\delta_{1}}} \right) = \frac{\xi}{2}$$

(43)

where $\xi$ is the failure probability. With the above equations, we have

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

(45)

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

Then in Eq. (30) we need the real values of $s_{\alpha}^{Z}$ and $e_{1}^{\text{ph}}$ in a specific experiment. So Eqs. (41)-(45) can be written in another form to estimate the upper and the lower bound of expected values from observed values:

$$X^{U}(\phi) = [1 + \delta_{1}(\phi)]\phi$$

(46)

$$X^{L}(\phi) = [1 - \delta_{2}(\phi)]\phi$$

(47)

where $\delta_{1}(\phi)$ and $\delta_{2}(\phi)$ are the solutions of the following equations:

$$\left( \frac{e^{\delta_{1} \mu_{A1}}}{(1 + \delta_{1})^{1+\delta_{1}}} \right) = \frac{\xi}{2}$$

(48)

$$\left( \frac{e^{-\delta_{2} \mu_{A1}}}{(1 - \delta_{2})^{1-\delta_{2}}} \right) = \frac{\xi}{2}$$

(49)

With the above equations, we have

$$N_{1}^{Z}s_{1}^{Z} \geq X^{L}(N_{1}^{Z}(s_{1}^{Z})), N_{1}^{Z}(s_{1}^{Z})e_{1}^{\text{ph}} \leq X^{U}(N_{1}^{Z}(s_{1}^{Z}))(e_{1}^{\text{ph}})).$$

(50)

where $N_{1}^{Z} = N_{1}^{Z}P_{A}P_{B}[1 - (1 - \epsilon_{B})\mu_{A}e^{-\mu_{A}} + \epsilon_{B}(1 - \epsilon_{A})\mu_{B}e^{-\mu_{B}}]$ is the number of single-photon state in the $Z$ windows when one and only one of $\epsilon_{A}$, $\epsilon_{B}$ decides to send and $N_{1}$ is the total number of time windows.

C. Finite Key Size Effect

Similarly to the analysis of the effect of the finite key size in ref. 58, we give the key rate formula with the effect of the finite key size of our general SNS protocol in the universally composable framework 59.

If the length of the final key satisfies

$$N_{f} = n_{1}[1 - H(e_{1}^{\text{ph}})] - f n_{H}(E_{Z}) - \log_{2} \frac{2}{\varepsilon_{\text{cor}}} - 2 \log_{2} \frac{1}{\sqrt{2\varepsilon_{\text{PA}}}}$$

(51)

the protocol is $\varepsilon_{\text{sec}}$-secret with $\varepsilon_{\text{sec}} = 2\bar{\varepsilon} + 4\hat{\varepsilon} + \varepsilon_{\text{PA}} + \varepsilon_{n_{1}}$, and the total security coefficient of the protocol is $\varepsilon_{\text{tot}} = \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}$. Here $\varepsilon_{\text{cor}}$ is the probability that the error correction fails, $\bar{\varepsilon}$ is the probability that the real value of $e_{1}^{\text{ph}}$ isn’t in the range that we estimate, $\varepsilon_{\text{PA}}$ is the failure
probability of the privacy amplification, and \( \epsilon_{n_t} \) is the probability that the real value of \( n_t \) isn’t in the range that we estimate. According to Eqs. (37)-(50), we have \( \bar{\epsilon} = 3\xi \) and \( \epsilon_{n_t} = 6\xi \). If we set \( \epsilon_{\text{cor}} = \bar{\epsilon} = \epsilon_{\text{PA}} = \xi \) in our numerical simulation, the total security coefficient of our protocol is \( \epsilon_{\text{tot}} = 22\xi = 2.2 \times 10^{-9} \).

Also, Eq. (51) can be written in the form of key rate per time window with some source parameters:

\[
R = \frac{\epsilon_A}{\epsilon_{\text{PA}}} - \mu_A e^{-\mu_A} + \epsilon_B(1 - \epsilon_A)\mu_B e^{-\mu_B} \cdot \frac{\epsilon_F^2}{\epsilon_{\text{F}}} [1 - H(\epsilon_{\text{F}})] - fS_Z H(E_Z)]
- \frac{1}{N_t}(\log_2 \frac{2}{\epsilon_{\text{cor}}} + 2\log_2 \frac{1}{\sqrt{2\epsilon_{\text{PA}}\epsilon_{\text{tot}}}}).
\]

(52)

[1] C. BENNETT, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (1984), pp. 175–179.
[2] H.-K. Lo and H. F. Chau, science 283, 2050 (1999).
[3] P. W. Shor and J. Preskill, Physical Review Letters 85, 441 (2000).
[4] D. Mayers, Journal of the ACM (JACM) 44, 131 (2001).
[5] N. Gisin, R. Thew, Nature photonics 1, 165 (2007).
[6] R. Renner, International Journal of Quantum Information 6, 1 (2008).
[7] W.-Y. Hwang, Physical Review Letters 91, 057901 (2003).
[8] X.-B. Wang, Physical Review Letters 94, 230503 (2005).
[9] H.-K. Lo, X. Ma, and K. Chen, Physical Review Letters 94, 230504 (2005).
[10] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Physical review letters 99, 180503 (2007).
[11] H.-K. Lo, M. Curty, and B. Qi, Physical Review Letters 108, 130503 (2012).
[12] S. L. Braunstein and S. Pirandola, Physical Review Letters 108, 130502 (2012).
[13] B. Huinann, N. Imoto, N. Gisin, and T. Mor, Physical Review A 51, 1863 (1995).
[14] H. P. Yuen, Quantum and Semiclassical Optics: Journal of the European Optical Society Part B 8, 939 (1996).
[15] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Physical Review Letters 85, 1330 (2000).
[16] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature photonics 4, 686 (2010).
[17] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature communications 2, 349 (2011).
[18] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Physics reports 448, 1 (2007).
[19] M. Hayashi, Physical Review A 76, 012329 (2007).
[20] X.-B. Wang, Physical Review A 87, 012320 (2013).
[21] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature 509, 475 (2014).
[22] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nature communications 5 (2014).
[23] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New Journal of Physics 15, 113007 (2013).
[24] F. Xu, H. Xu, and H.-K. Lo, Physical Review A 89, 052333 (2014).
[25] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, and X.-Q. Tan, Physical Review A 86, 023323 (2012).
[26] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Physical Review A 89, 052325 (2014).
[27] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Physical Review A 91, 032318 (2015).
[28] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Physical Review A 93, 042324 (2016).
[29] C. Jiang, Z.-W. Yu, and X.-B. Wang, Physical Review A 94, 062323 (2016).
[30] C. Jiang, Z.-W. Yu, and X.-B. Wang, Physical Review A 95, 032325 (2017).
[31] X.-Y. Zhou, C.-H. Zhang, C.-M. Zhang, and Q. Wang, Physical Review A 96, 052337 (2017).
[32] A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, Physical Review A 98, 012330 (2018).
[33] H.-F. Chau, Physical Review A 97, 040301 (2018).
[34] X.-L. Hu, Y. Cao, Z.-W. Yu, and X.-B. Wang, Scientific Reports 8, 17634 (2018).
[35] W. Wang, F. Xu, and H.-K. Lo, Physical Review A 97, 032337 (2018).
[36] 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, Physical Review Letters 98, 010503 (2007).
[37] C. Zhou-European Quantum Optics: Journal of the European Optical Society Part B 8, 939 (1996).
[38] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Physical Review Letters 85, 1330 (2000).
[39] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature communications 2, 349 (2011).
[40] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Physics reports 448, 1 (2007).
[45] Z. Yuan, A. Sharpe, and A. Shields, Applied physics letters 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, Physical Review Letters 100, 090501 (2008).

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

[48] A. R. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, Applied Physics Letters 96, 161102 (2010).

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

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

[51] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martínez, and W. Tittel, Physical Review Letters 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., Physical Review Letters 111, 130502 (2013).

[53] T. F. da Silva, D. Vitoreti, G. Xavier, G. do Amaral, G. Temporao, and J. von der Weid, Physical Review A 88, 052303 (2013).

[54] P. Chan, J. A. Slater, I. Lucio-Martínez, A. Rubenok, and W. Tittel, Optics express 22, 12716 (2014).

[55] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Physical Review Letters 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., Physical Review Letters 113, 190501 (2014).

[57] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nature Photonics 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, Physical Review Letters 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, Nature Photonics 9, 397 (2015).

[60] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Nature Photonics 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 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., Physical Review Letters 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. Yao, M.-Q. Huang, W.-J. Zhang, et al., Physical Review Letters 117, 190501 (2016).

[65] M. Takeoka, S. Guha, and M. M. Wilde, Natural communications 5, 5235 (2014).

[66] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nature communications 8, 15043 (2017).

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

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

[69] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, arXiv preprint arXiv:1805.05511 (2018).

[70] X. Ma, P. Zeng, and H. Zhou, Physical Review X 8, 031043 (2018).

[71] J. Lin and N. Lütkenhaus, Physical Review A 98, 042332 (2018).

[72] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Physical Review Applied 11, 034053 (2019).

[73] M. Curty, K. Azuma, and H.-K. Lo, arXiv preprint arXiv:1807.07667 (2018).

[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, arXiv preprint arXiv:1901.04264 (2019).

[75] F. Grasselli and M. Curty, New Journal of Physics (2019).

[76] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, arXiv preprint arXiv:1904.06331 (2019).

[77] C.-H. Zhang, C.-M. Zhang, and Q. Wang, Optics letters 44, 1468 (2019).

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

[79] K. Maeda, T. Sasaki, and M. Koashi, Nature communications 10, 3140 (2019).

[80] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Nature Photonics 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., arXiv preprint arXiv:1902.06268 (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, Physical Review X 9, 021046 (2019).

[83] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, arXiv preprint arXiv:1902.10209 (2019).

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

[85] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, arXiv preprint arXiv:1904.00192 (2019).

[86] H. Chernoff et al., The Annals of Mathematical Statistics 23, 493 (1952).

[87] J. Müller-Quade and R. Renner, New Journal of Physics 11, 085006 (2009).