Security proof of differential phase shift quantum key distribution in the noiseless case

Yi-Bo Zhao,[1] Chi-Hang Fred Fung,[2] Zheng-Fu Han,[1,*] and Guang-Can Guo[1]

[1]*Key Lab of Quantum Information, University of Science and Technology of China, (CAS), Hefei, Anhui 230026, China*
[2]*Department of Physics and Center of Computational and Theoretical Physics, University of Hong Kong, Pokfulam Road,*
Hong Kong, China

Differential phase shift quantum key distribution systems have a high potential for achieving high speed key generation. However, its unconditional security proof is still missing, even though it has been proposed for many years. Here, we prove its security against collective attacks with a weak coherent light source in the noiseless case (i.e., no bit error). The only assumptions are that quantum theory is correct, the devices are perfect and trusted and the key size is infinite. Our proof works on threshold detectors. We compute the lower bound of the secret key generation rate using the information-theoretical security proof method. Our final result shows that the lower bound of the secret key generation rate per pulse is linearly proportional to the channel transmission probability if Bob's detection counts obey the binomial distribution.

I. INTRODUCTION

Quantum key distribution (QKD) allows two distant parties to share secret keys that are unconditionally secure. Until now, there have been several kinds of QKD protocols. The traditional Bennett-Brassard 1984 (BB84) protocol is one based on qubits, in which Alice sends Bob a sequence of qubits to establish a secret key [1]. On the other hand, there are other non-qubit-based protocols, such as the continuous variable QKD scheme [2–4]. In these two protocols, regardless of whether qubit states or continuous states are used, each state (or state pair) received by Bob directly gives rise to one bit value. In contrast, in differential phase shift (DPS) QKD, information is encoded in the difference between each two adjacent quantum states [5–7]. Of the above protocols, the last one is designed to achieve high speed communication. In Ref. [8], Diamanti *et al.* have realized DPSQKD with a modulation frequency of 1 GHz.

DPSQKD is well suited for coherent-state sources as information is encoded in the relative phases of coherent states. Coherent-state sources can also be used with other protocols, for example, the BB84 protocol with phase-randomized coherent states [9] whose performance is substantially improved by the decoy-state method [10–17], the BB84 protocol with phase-nonrandomized coherent states [18], and the Bennett 1992 (B92) protocol with strong reference pulses [19–21] (see also Ref. [22]).

The unconditional security of the BB84 protocol is well discussed (e.g., Ref. [9,23–27]). For the CVQKD protocols, its security against collective attack is also well discussed [3,4,28]. However, for DPSQKD, we only know that it is secure against several specific attacks, e.g., the beam splitting attack and the intercept and resending attack [8,29]. Presently, we do not know whether it is secure against any quantum Eve even in the noiseless case. On the other hand, specific attacks on DPSQKD have been proposed to evaluate upper bounds on the secret key generation rates of DPSQKD [30–34].

In this paper, we prove the security of DPSQKD against collective attacks [35] with a weak coherent light source in the noiseless case. The security in this case follows from a key result that we will prove in this paper, namely, that Eve's state is independent of the positions of Bob's detected signals. This result makes sense since the fact that there is no bit error restricts what Eve can do to Bob's signals. In particular, she has to ensure that Bob receives all signals with equal intensities, since signals with different intensities will result in bit errors with nonzero probability. Our final result on the lower bound on the key generation rate is a function of the estimated parameters of the channel [see Eq. (56)]. In order to understand this result further, we compute this bound by considering a channel that produces a binomial distribution in Bob's detection statistics. Specifically, we show that the lower bound of the secret key generation rate per pulse is linearly proportional to the channel transmission probability [see Eq. (65)].

The only assumptions used in the proof are that quantum theory is correct, the key size is infinite and the devices are perfect and trusted. Our proof works on threshold detectors, which are the detectors commonly used in practice. Furthermore, we do not require quantum nondemolition (QND) measurements. Even though we consider collective attacks in this paper, we speculate that it is possible for us to extend our security proof to the most general attack, namely, the coherent attack. An intuitive justification tells us that Eve cannot get more information from coherent attacks than that from collective attacks as the key size goes to infinity [36,37]. For the finite dimension case, there is a exponential de Finetti theorem that can strictly give this result [38,39]. However, for DPSQKD, the states sent by Alice are weak coherent states and thus in theory the dimension of Bob's received states may be infinite. Thus, the current de Finetti theorem cannot be directly applied. On the other hand, there are three potential ways to solve this problem. Since in practice the states sent by Alice are weak coherent states and the probability that Bob gets a large photon number is extremely small, it is possible to prove that Alice and Bob's states can be well approximated by states that have a finite support. Then the current de Finetti theorem can be applied. The sec-
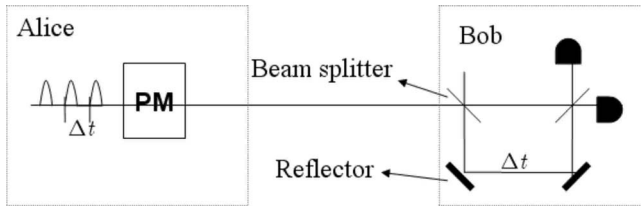
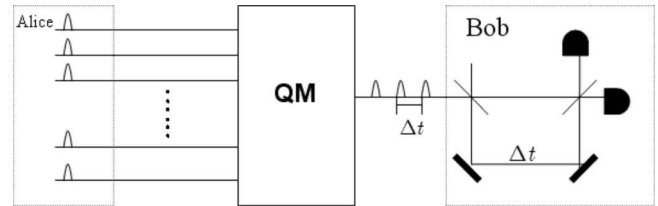FIG. 1. Illustration of the protocol 1, where the PM denotes the phase modulator.

FIG. 2. Illustration of protocol 2, where the QM system is a quantum memory that stores the N received states and sends them out one by one.

ond way is to extend the current exponential de Finetti theorem to the infinite dimensional case. We can see a hope of this in Ref. [40]. The third way is to extend the current de Finetti theorem to the case with finite number of measurement results, since we know that in DPSQKD, Bob's measurement results are finite. The work in Ref. [40] also shows that this way may be viable.

We note that there is also a recent proof [41] on the DPS protocol. Their proof assumes a single-photon source and requires QND measurements, whereas our proof allows a more general weak coherent light source and does not require QND measurements. On the other hand, their proof can handle the noisy case and applies to the most general attack, whereas ours can only handle noiseless collective attacks.

In the following analysis, we map the traditional DPS protocol into a big-state protocol and give the security proof for this big-state protocol. In doing so, we prove a key result of our paper, which is that Eve's state is independent of the positions of Bob's detected signals. With this result and some properties of the mutual information, we can upper bound Eve's information about Alice's bit string. Finally, we evaluate the key rate assuming a typical setting in which the detection statistics follows the binomial distribution. The security proof method we employ is the information-theoretical one by Renner *et al.* [37,38].

II. EQUIVALENT PROTOCOLS

A. Protocol 1: original protocol

Quantum Phase.

(1) Alice sends a sequence of coherent states, each with amplitude α, but with a randomly selected phase $|\alpha\rangle$ or $|-\alpha\rangle$ to Bob. Then she records each state with a binary variable x_i, by setting $x_i=0$ if the ith state is $|-\alpha\rangle$ and $x_i=1$ if the ith state is $|\alpha\rangle$.

(2) Using the Mach-Zehnder (MZ) interferometers shown in Fig. 1, Bob measures the phase difference between every two adjacent states. Bob stores his measurement result into binary variables y_i and z_i. While measuring the phase difference of the ith and $(i-1)$-th state, if Bob gets a photon count, he sets $z_i=1$ and if not, he sets $z_i=0$. Also, if $i=kN+1$ $(k=0,1,2,3,\ldots)$, Bob sets $z_i=0$. If $z_i=1$ and the measurement results indicates that the phase difference is zero, he sets $y_i=0$; otherwise, if it indicates a nonzero phase difference, he sets $y_i=1$. If $z_i=0$, Bob sets $y_i=0$.

Classical phase.

(3) After Bob receives each set of N states, he announces all z_i's for these N states.

(4) Alice generates another variable $l_i=x_i \oplus x_{i-1}$ for $i>1$.

(5) After many rounds of such communications, Alice and Bob randomly publish some of l_i and y_i corresponding to $z_i=1$ to test the bit error rate (BER) between them.

(6) Alice and Bob generate new binary variables u_i^A and u_i^B, respectively. Alice sets $u_i^A=l_i \cdot z_i$. Bob sets $u_i^B=y_i z_i$.

(7) Alice and Bob estimate the mutual information between the binary strings $\vec{u}^A$ and $\vec{u}^B$ conditioned on Bob's announcement.

(8) Alice announces the error correction information of binary string $\vec{u}^A$ and Bob uses it to reconcile his string $\vec{u}^B$ to the corresponding string $\vec{u}^A$.

(9) Alice and Bob perform privacy amplification on their common binary string $\vec{u}^A$ to generate the final secret key.

Instead of steps 6–9, Alice and Bob can simply discard the l_i and y_i that correspond to $z_i=0$, and perform error correction and privacy amplification on the remaining sifted bits. This protocol is then equivalent to the original DPSQKD protocol [5,7]. In this protocol, Bob measures the phase difference between every two adjacent pulses. Thus, it may not be a good idea to try to map them into single bits and then discuss the security. Here, our basic idea is to regard N states as one big state and to discuss the security of this big state. In the following, we will introduce three protocols that map the above protocol into a big state protocol, in which Alice sends Bob a big state and Bob measures it with N equipments. The security of these three protocols are weaker than the above one. Thus, if the security of these inferior protocols are proved, then the security of the above protocol is proved.

B. Protocol 2

In step 1, according to the binary string $\vec{x}=(x_{kN+1},x_{kN+2},\ldots,x_{(k+1)N})$, Alice generates a state $|\Psi_{\vec{x}}^N\rangle=\otimes_{i=kN+1}^{(k+1)N}|(-1)^{x_i+1}\alpha\rangle$ and sends it to Bob through N fibers. In the quantum channel, there is a quantum memory (QM) system that separates $|\Psi_{\vec{x}}^N\rangle$ into an N-state sequence and sends each state to Bob one by one through one fiber (see Fig. 2). Steps 2–9 remain the same.

There is no difference between protocol 1 and protocol 2 at Bob's side. The only difference between them is that in protocol 1 Alice sends Bob each coherent state one by one and in protocol 2 Alice sends them all together. The QM system that separates the big state into an N-state sequence can be realized by storing the big state and sending each state one by one. In protocol 2, the QM system can be controlled
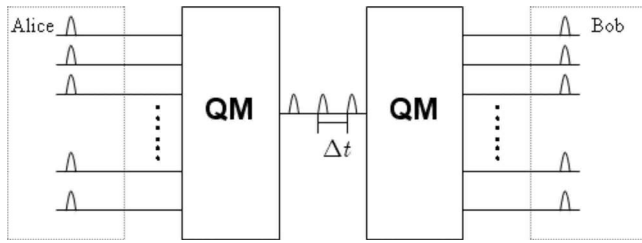
FIG. 3. Illustration of protocol 3, where Bob's measurement equipment is not shown in detail.

by Eve. However, it can be seen that if the QM system is put at Alice's side and cannot be controlled by Eve, protocol 2 is equivalent to protocol 1. Therefore, the security of protocol 2 is weaker than that of protocol 1. Therefore the secret key rate of protocol 1 is no less than that of protocol 2.

C. Protocol 3

As shown in Fig. 3 in step 2 of protocol 2, Bob stores the received pulses in another QM system. After receiving N pluses, Bob reads out the stored N signals one by one through N fibers and measures their phase differences via MZ systems which should be equivalent to the measurements in protocol 1 (these MZ systems can be realized by the detection equipments shown in Fig. 4).

It can be seen that if the QM system is at Bob's side and cannot be controlled by Eve, then protocol 3 is the same as protocol 2. Since in protocol 3 this QM system can be controlled by Eve, the security of protocol 3 is no stronger than that of protocol 2.

D. Protocol 4

In step 1, Alice generates a state $|\Psi_{\vec{x}}^N\rangle = \otimes_{i=kN+1}^{(k+1)N}$ $|(-1)^{x_i+1}\alpha\rangle$ and sends it to Bob through N fibers. In step 2, while receiving this big state, Bob measures the phase difference between each two adjacent states at the same time with the equipment shown in Fig. 4. Steps 3–9 remains the same as in protocol 1.

It can be seen that the only difference between protocol 3 and protocol 4 is that in protocol 3 Bob measures each phase difference one by one, but in protocol 4 Bob measures them all together. Since different detectors just measure different field quadratures, the measurement operators that describe these detectors commute with each other. Therefore, there is no difference between measuring the phase difference one by one and measuring them all together. Thus, protocol 4 is equivalent to protocol 3.

Since protocol 4 is inferior to protocol 1, in the following we will prove the security of protocol 4 first. Then the security of protocol 1 follows.

III. SECURITY DISCUSSION

Here we only discuss the security against the collective attack under the infinite-key-length case. It means that Alice sends Bob infinite number of the quantum state $|\Psi_{\vec{x}}^N\rangle$. We remark that we do not place any restriction on the block
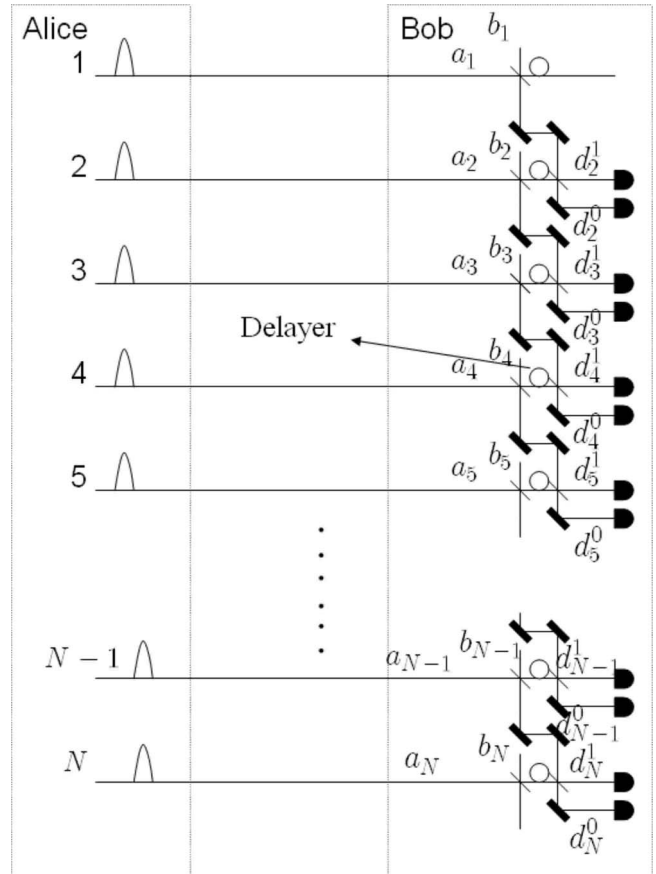

FIG. 4. Illustration of protocol 4, where the delayer generates the time delay that makes the two pulses meet at the beam splitter before the detector.

length N, which can be finite. Under the collective attack scenario Eve attacks each state individually with the same superoperator and the state Alice and Bob share is a state that can be written as a product state. This means that after Alice sends Bob M big states, the state Alice, Bob, and Eve share can be written as $(\rho_{ABE}^N)^{\otimes M}$, where ρ_{ABE}^N is evolved from $|\Psi_{\vec{x}}^N\rangle$. Then it is enough for us to only discuss the possible attacks to a single state $|\Psi_{\vec{x}}^N\rangle$ [38]. We also assume that quantum theory is correct, the device can be trusted and Bob's detectors are ideal [42]. In the following we assume that $\vec{x}$, $\vec{y}$, $\vec{z}$, $\vec{l}$, $\vec{u}^A$, and $\vec{u}^B$ are the binary strings Alice and Bob obtain from one state $|\Psi_{\vec{x}}^N\rangle$, with $\vec{x} = (x_1, x_2, \ldots, x_N)$, $\vec{y} = (y_1, y_2, \ldots, y_N)$, and similar for the others. Let $\vec{X}$, $\vec{Y}$, $\vec{Z}$, $\vec{L}$, $\vec{U}_A$ and $\vec{U}_B$ denote the variables that can take the values $\vec{x}$, $\vec{y}$, $\vec{z}$, $\vec{l}$, $\vec{u}^A$, and $\vec{u}^B$, respectively. Let X_i, Y_i, Z_i, L_i, U_i^A, and U_i^B denote the variables that can take the values x_i, y_i, z_i, l_i, u_i^A, and u_i^B, respectively. In Refs. [37,43], it has been shown that under the infinite-key-length case the secret key rate is given by the difference between mutual informations. In the above protocols, $\vec{U}_A$ and $\vec{U}_B$ are the final variables that are used to distill the secret keys. Then for protocol 4, the secret key rate per big state is given by

$$G \geqslant I(\vec{U}_A : \vec{U}_B | \vec{Z}) - S(\vec{U}_A : E | \vec{Z}), \tag{1}$$

where I and S denote the Shannon mutual information [44] and the Von Neuemann mutual information [45], respectively. Here the $I(\vec{U}_A : \vec{U}_B | \vec{Z})$ and $S(\vec{U}_A : E | \vec{Z})$ are, respectively, given by

$$I(\vec{U}_A : \vec{U}_B | \vec{Z}) = \sum_{\vec{z}} P(\vec{z}) I(\vec{U}_A : \vec{U}_B | \vec{Z} = \vec{z}),$$

$$S(\vec{U}_A : E | \vec{Z}) = \sum_{\vec{z}} P(\vec{z}) S(\vec{U}_A : E | \vec{Z} = \vec{z}). \tag{2}$$

Before discussing the properties of these two mutual informations, we introduce the following notations. We introduce vectors $w(\vec{z})$ and $\vec{c}(\vec{z})$ in relation to Bob's counting results. Let $w(\vec{z})$ denote the weight of $\vec{z}$, which gives the total number of 1 in $\vec{z}$. Let $c_i(\vec{z})$ denotes the position of the ith 1 in the string $\vec{z}$.

From step 6, we see that $u_i^A = l_i z_i$. Since if $z_i = 0$ we have $u_i^A = 0$, $\vec{u}^A$ can be given by $\vec{u}^A = (0, \ldots, l_{c_1(\vec{z})}, \ldots, 0, \ldots, l_{c_{w(\vec{z})}(\vec{z})}, \ldots, 0)$. For a given $\vec{z}$, we can change the order of elements and write $\vec{u}^A$ as $\vec{u}^A = (l_{c_1(\vec{z})}, l_{c_2(\vec{z})}, \ldots, l_{c_{w(\vec{z})}(\vec{z})}, 0, \ldots, 0)$. For convenience, we introduce $\vec{l}_{\vec{z}}$ and $\vec{y}_{\vec{z}}$, which are given by

$$\vec{l}_{\vec{z}} = (l_{c_1(\vec{z})}, l_{c_2(\vec{z})}, \ldots, l_{c_{w(\vec{z})}(\vec{z})}),$$

$$\vec{y}_{\vec{z}} = (y_{c_1(\vec{z})}, y_{c_2(\vec{z})}, \ldots, y_{c_{w(\vec{z})}(\vec{z})}). \tag{3}$$

Then for a given $\vec{z}$, $\vec{u}^A$ can simply be given by

$$\vec{u}^A = (\vec{l}_{\vec{z}}, \vec{0}),$$

where $\vec{0}$ is the zero vector of length $N - w(\vec{z})$. Now we introduce random variables $\vec{L}_{\vec{z}}$ and $\vec{Y}_{\vec{z}}$ of length $w(\vec{z})$ that take on values $\vec{l}_{\vec{z}}$ and $\vec{y}_{\vec{z}}$:

$$\vec{L}_{\vec{z}} = (L_{c_1(\vec{z})}, L_{c_2(\vec{z})}, \ldots, L_{c_{w(\vec{z})}(\vec{z})}),$$

$$\vec{Y}_{\vec{z}} = (Y_{c_1(\vec{z})}, Y_{c_2(\vec{z})}, \ldots, Y_{c_{w(\vec{z})}(\vec{z})}). \tag{4}$$

Then for a given $\vec{z}$, $\vec{U}_A$ can be given by

$$\vec{U}_A = (\vec{L}_{\vec{z}}, \vec{0}) \tag{5}$$

and similarly we have

$$\vec{u}^B = (\vec{y}_{\vec{z}}, \vec{0}),$$

$$\vec{U}_B = (\vec{Y}_{\vec{z}}, \vec{0}). \tag{6}$$

Now we can rewrite the mutual information given by Eq. (2) as follows:

$$I(\vec{U}_A : \vec{U}_B | \vec{Z}) = \sum_{\vec{z}} P(\vec{z}) I(\vec{L}_{\vec{z}} \oplus \vec{0} : \vec{Y}_{\vec{z}} \oplus \vec{0} | \vec{Z} = \vec{z})$$

$$= \sum_{\vec{z}} P(\vec{z}) [H(\vec{L}_{\vec{z}} \oplus \vec{0} | \vec{Z} = \vec{z})$$

$$+ H(\vec{Y}_{\vec{z}} \oplus \vec{0} | \vec{Z} = \vec{z}) - H(\vec{L}_{\vec{z}} \oplus \vec{0}, \vec{Y}_{\vec{z}} \oplus \vec{0} | \vec{Z} = \vec{z})]$$

$$= \sum_{\vec{z}} P(\vec{z}) I(\vec{L}_{\vec{z}} : \vec{Y}_{\vec{z}} | \vec{Z} = \vec{z}), \tag{7}$$

where $H(\cdots)$ is Shannon entropy [44], in the second line we have applied the results given by Eqs. (5) and (6), in the third and fourth lines we have used the definition of the Shannon mutual information [44] and in the fifth line we have used the formula $H(AB | C) = H(A | BC) + H(B | C)$, and the fact that the entropy of a given vector is zero and $H(\cdot | \vec{Z} = \vec{z}, \vec{0}) = H(\cdot | \vec{Z} = \vec{z})$ ($\vec{0}$ is generated from $\vec{z}$). In the same way, we have

$$S(\vec{U}_A : E | \vec{Z}) = \sum_{\vec{z}} P(\vec{z}) S(\vec{L}_{\vec{z}} : E | \vec{Z} = \vec{z}). \tag{8}$$

Then from Eqs. (7) and (8), the final secret key rate per N pulses is given by

$$G \geqslant \sum_{\vec{z}} P(\vec{z}) [I(\vec{L}_{\vec{z}} : \vec{Y}_{\vec{z}} | \vec{Z} = \vec{z}) - S(\vec{L}_{\vec{z}} : E | \vec{Z} = \vec{z})]. \tag{9}$$

If Alice and Bob just discard all l_i and y_i corresponding to $z_i = 0$, and perform error correction and privacy amplification to the sifted key, according to Ref. [37] the secret key in this case is also given by Eq. (9). Therefore, instead of steps 6–9, Alice and Bob can simply introduce such post-selection step.

IV. SECURITY PROOF

Before giving the security proof of the DPS protocol, we will show the main idea of our security proof. In the DPS protocol, what Alice sends to Bob are two weak coherent states. Since these two states are nonorthogonal Eve in principle cannot always distinguish them and cannot always know the phase difference between two adjacent pulses. The mutual information per pulse between Alice and Eve is thus less than 1. Bob uses the MZ system to measure the phase difference between two adjacent pulses. This system can let Bob definitely know the deterministic phase difference between the two pulses with certain probability (Bob can definitely know the phase difference if he gets a count.). Finally Alice and Bob only keep the measurement results of the phase differences that Bob has good knowledge of. The point is that either Bob knows that Eve has obtained good information on a pulse pair (in which case he has not gotten a photon count and this result is discarded) or Bob knows more about this result than Eve does (in which case Alice and Bob proceed to distill a secret key by applying error correction and privacy amplification to many of such result). In the following, we will rigorously prove this when there is no bit error. First, we prove that under the no-bit-error case Eve's state is uncorrelated with the permutation of $\vec{z}$, which means that Eve's state is independent with the position of

Bob's detections. Then we show that Eve's average information about the sifted keys is only determined by the total number of Bob's detections. Since the maximum total information Eve gets from Alice is restricted by Alice's modulation, through several properties of the mutual information, we can give an upper bound to Eve's information on the sifted data. Then the security of the DPS protocol under the no-bit-error case is proved.

Here, we only limit our analysis to the no-bit-error case. For a collective attack, it is enough to only discuss the attack for a single communication [37]. Therefore, in the following we only discuss the possible attacks for a single state $|\Psi_{\vec{x}}^N\rangle$. Before giving the security proof, we introduce the following notations. As shown in Fig. 4, the annihilation operator of the input fields on the ith path at Bob's side is denoted by a_i. The vacuum inject mode on the beam splitter corresponding to the ith fiber at Bob's side is denoted by b_i. The output modes to the detectors that detect the phase difference between the ith signal and $(i-1)$-th signal are described by d_i^0 and d_i^1, with 0 and 1 describing the lower and upper detectors, respectively (see Fig. 4). In the following, we denote the detectors that correspond to the modes d_i^0 and d_i^1 by DET_i^0 and DET_i^1.

We assume that Bob and Eve's conditional states conditioned on Alice's modulation is $\rho_{EB}^{N,\vec{x}}$. Now we will prove that if there is no bit error, the reduced state $\rho_E^{N,\vec{x},\vec{z}}$, which denotes Eve's conditional state after Bob's announcement of detected signals, is independent of the permutation of $\vec{z}$. With this result and several properties of the entropy, we can give a lower bound to Eq. (1).

A. Permutation invariance of Eve's state to $\vec{z}$

In this subsection we give the description of Bob's measurement first. Then we prove a requirement implied by the no-bit-error condition. Finally we prove that Eve's state is invariant under the permutation of $\vec{z}$.

From Fig. 4, we can see that the output modes d_i^0 and d_i^1 can, respectively, be given by

$$d_i^1 = \frac{1}{2}(a_i - a_{i-1}) + \frac{i}{2}(b_i + b_{i-1}),$$

$$d_i^0 = \frac{i}{2}(a_i + a_{i-1}) + \frac{1}{2}(b_{i-1} - b_i). \tag{10}$$

To simplify Eq. (10) we introduce $\tilde{d}_i^j$ and v_i^j:

$$\tilde{d}_i^1 = \frac{1}{2}(a_i - a_{i-1}),$$

$$\tilde{d}_i^0 = \frac{1}{2}(a_i + a_{i-1}), \tag{11}$$

and

$$\mathrm{vac}_i^1 = \frac{i}{2}(b_i + b_{i-1}),$$

$$\mathrm{vac}_i^0 = \frac{-i}{2}(b_{i-1} - b_i). \tag{12}$$

Since the phase factor i can be absorbed into the annihilation operators, the output modes d_i^0 and d_i^1 can simply be given by

$$d_i^1 = \tilde{d}_i^1 + \mathrm{vac}_j^1,$$

$$d_i^0 = \tilde{d}_i^0 + \mathrm{vac}_j^0. \tag{13}$$

In our security analysis we can safely assume that Eve holds the purification of $\rho_{EB}^{N,\vec{x}}$. This means that we can safely assume that $\rho_{EB}^{N,\vec{x}}$ is a pure state [37]. Let $|\Psi_{EB}^{N,\vec{x}}\rangle$ denote the pure conditional state Bob and Eve share. According to the Schmidt decomposition (see, e.g., Ref. [45]), $|\Psi_{EB}^{N,\vec{x}}\rangle$ can be decomposed into several orthogonal states

$$|\Psi_{EB}^{N,\vec{x}}\rangle = \sum_k c_k^{\vec{x}} |\Phi_{E,k}^{N,\vec{x}}\rangle |\Phi_{B,k}^{N,\vec{x}}\rangle. \tag{14}$$

For convenience, in the following we denote the $\vec{l}$ generated from $\vec{x}$ by $\vec{l}^{\vec{x}}$.

The no-bit-error condition can be described as follows. If there is no phase difference between the ith and $(i-1)$-th states, in principle, the DET_i^1 detector should not generate a count; and if there is phase difference, the DET_i^0 detector should not click. It can be seen that this condition actually requires that the output mode $\tilde{d}_i^{\vec{l}_i^{\vec{x}}}$ of $\rho_{EB}^{N,\vec{x}}$ corresponds to the vacuum state, i.e., $d_i^{\vec{l}_i^{\vec{x}}}|\Psi_{EB}^{N,\vec{x}}\rangle|\mathrm{vac}\rangle=0$, where $\vec{l}_i^{\vec{x}}=l_i^{\vec{x}}\oplus 1$ and $|\mathrm{vac}\rangle$ describes the vacuum state injected through the b_i mode. Since in Eq. (13), the annihilation operator vac_i^j ($j=0,1$) acts on the vacuum state, we can simply discard the vacuum mode. Then the no-bit-error condition can be rewritten as

$$\tilde{d}_i^{\vec{l}_i^{\vec{x}}}|\Psi_{EB}^{N,\vec{x}}\rangle = 0. \tag{15}$$

From Eqs. (14) and (11), we know that Eq. (15) is equal to

$$[a_i + (-1)^{l_i^{\vec{x}}+1} a_{i-1}]|\Phi_{B,k}^{N,\vec{x}}\rangle = 0, \tag{16}$$

for arbitrary $i > 1$ and k. Equation (16) gives the no-bit-error condition. This analysis can be summarized by the following lemma.

Lemma 1. If there is no bit error between Alice and Bob, Bob's state satisfies

$$a_i|\Phi_{B,k}^{N,\vec{x}}\rangle = (-1)^{l_i^{\vec{x}}} a_{i-1}|\Phi_{B,k}^{N,\vec{x}}\rangle. \tag{17}$$

Since $\tilde{d}_i^{l_i} = \frac{1}{2}[a_i + (-1)^{l_i} a_{i-1}]$, from Eq. (17), we get

$$\tilde{d}_i^{\vec{l}_i^{\vec{x}}}|\Phi_{B,k}^{N,\vec{x}}\rangle = a_i|\Phi_{B,k}^{N,\vec{x}}\rangle. \tag{18}$$

Eqs. (15) and (18) give us the relationship between the input modes and the output modes of the MZ system under the no-bit-error case. With this lemma we can prove the permutation invariance of Eve's state to $\vec{z}$ finally.

Combining Eqs. (17) and (18) and the result that $l_i^{\vec{x}}=x_i \oplus x_{i-1}$, we have

$$(-1)^{x_i}\tilde{d}_i^{\vec{l_i^x}}|\Phi_{B,k}^{N,\vec{x}}\rangle = (-1)^{x_{i'}}\tilde{d}_{i'}^{\vec{l_i^x}}|\Phi_{B,k}^{N,\vec{x}}\rangle \qquad (19)$$

for arbitrary i, i' and k. It can be seen that Eq. (19) can be generalized to

$$(-1)^{x_{i_1}+x_{i_2}+\ldots+x_{i_q}}\tilde{d}_{i_1}^{\vec{l_{i_1}^x}}\tilde{d}_{i_2}^{\vec{l_{i_2}^x}}\ldots\tilde{d}_{i_q}^{\vec{l_{i_q}^x}}|\Phi_{B,k}^{N,\vec{x}}\rangle$$

$$= (-1)^{x_{i_1'}+x_{i_2'}+\ldots+x_{i_q'}}\tilde{d}_{i_1'}^{\vec{l_{i_1}^x}}\tilde{d}_{i_2'}^{\vec{l_{i_2}^x}}\ldots\tilde{d}_{i_q'}^{\vec{l_{i_q}^x}}|\Phi_{B,k}^{N,\vec{x}}\rangle \qquad (20)$$

for arbitrary integer $i_p > 1$, $i_p' > 1$, k and q, where the subscription $p = 1, \ldots, q$ (p comes from i_p).

Bob's measurement is a projection. The detector DET_i^j maps the received state into the photon number space $\{|\mathrm{vac}\rangle\langle\mathrm{vac}|, |1\rangle\langle1|,\ldots\}$. This projection subspace of DET_i^j can be given by

$$\mathrm{Map}_i^j = \left\{ M_{iv}^j = \frac{1}{v!}(d_i^{j+})^v|\mathrm{vac}\rangle\langle\mathrm{vac}|(d_i^j)^v, |v = 0, 1, \ldots \right\}, \qquad (21)$$

where v denotes the number of photons received by the detector DET_i^j.

Since d_i^j is composed by an operator acting on the received state and an operator acting on the vacuum state, from Eqs. (13), (20), and (21), it can be seen that for arbitrary integer i, i', v, and k we always have

$$\langle\mathrm{vac}|\langle\Phi_{B,k}^{N,\vec{x}}|M_{iv}^{\vec{l_i^x}}|\Phi_{B,k}^{N,\vec{x}}\rangle|\mathrm{vac}\rangle = \langle\mathrm{vac}|\langle\Phi_{B,k}^{N,\vec{x}}|M_{i'v}^{\vec{l_i^x}}|\Phi_{B,k}^{N,\vec{x}}\rangle|\mathrm{vac}\rangle \qquad (22)$$

where $|\mathrm{vac}\rangle$ denotes the vacuum state injected through the b_i^j mode and this equality holds for $v=0$ because the modulus of the projection to the vacuum state plus that to other states equals to 1. Since $|\mathrm{vac}\rangle$ is always a vacuum state, in the following we just leave it out in our expression for convenience. Equation (22) can be expended to the multidetection case as follows:

$$\langle\Phi_{B,k}^{N,\vec{x}}|M_{i_1v_1}^{\vec{l_{i_1}^x}}\cdots M_{i_qv_q}^{\vec{l_{i_q}^x}}|\Phi_{B,k}^{N,\vec{x}}\rangle = \langle\Phi_{B,k}^{N,\vec{x}}|M_{i_1'v_1}^{\vec{l_{i_1}^x}}\cdots M_{i_q'v_q}^{\vec{l_{i_q}^x}}|\Phi_{B,k}^{N,\vec{x}}\rangle, \qquad (23)$$

where we have introduced subscripts 1, 2, ..., and q to enumerate different operators and have omitted the vacuum state part.

From Eqs. (14) and (23) it can be obtained that

$$\langle\Psi_{EB}^{N,\vec{x}}|M_{i_1v_1}^{\vec{l_{i_1}^x}}\cdots M_{i_qv_q}^{\vec{l_{i_q}^x}}|\Psi_{EB}^{N,\vec{x}}\rangle = \langle\Psi_{EB}^{N,\vec{x}}|M_{i_1'v_1}^{\vec{l_{i_1}^x}}\cdots M_{i_q'v_q}^{\vec{l_{i_q}^x}}|\Psi_{EB}^{N,\vec{x}}\rangle. \qquad (24)$$

Also from Eqs. (15) and (21) it can be seen that if $j \neq l_i^{\vec{x}}$ and $v > 0$ we always have

$$\langle\Phi_{B,k}^{N,\vec{x}}|M_{iv}^j|\Phi_{B,k}^{N,\vec{x}}\rangle = 0. \qquad (25)$$

With the above results, we can evaluate Eve's conditional state conditioned on Bob's announcement. We know that if Bob maps his state into the subspace $M = |\beta\rangle\langle\beta|$ (for conve-

nience we denote it by β) then Eve's state will collapse to the state

$$\rho_E^{N,\vec{x},\beta} = \frac{\mathrm{tr}_B M \rho_{EB}^{N,\vec{x}} M^+}{\mathrm{tr}_{EB} M \rho_{EB}^{N,\vec{x}} M^+}, \qquad (26)$$

where $\rho_{EB}^{N,\vec{x}}$ is the state Eve and Bob share before Bob's measurement [45]. In our security analysis we can consider the worst case (favoring Eve), in which the state $\rho_{EB}^{N,\vec{x}}$ is pure and described by $|\Psi_{EB}^{N,\vec{x}}\rangle$. For the pure state case, Eq. (26) becomes

$$|\Psi_E^{N,\vec{x},\beta}\rangle = \sum_k \frac{c_k^{\vec{x}}\sqrt{\langle\Phi_{B,k}^{N,\vec{x}}|M|\Phi_{B,k}^{N,\vec{x}}\rangle}|\Phi_{E,k}^{N,\vec{x}}\rangle}{\sqrt{\langle\Psi_{EB}^{N,\vec{x}}|M|\Psi_{EB}^{N,\vec{x}}\rangle}}, \qquad (27)$$

where we have used Eq. (14) and the results that $M = M^+ = MM^+$.

Bob's announcement $\vec{z}$ corresponds to several possible orthogonal subspaces given by

$$\{S_{\vec{z},\vec{v}>0}^{\vec{j}} = M_{c_1(\vec{z}),v_1}^{j_1}M_{c_2(\vec{z}),v_2}^{j_2}\cdots M_{c_{w(\vec{z})}(\vec{z}),v_{w(\vec{z})}}^{j_{w(\vec{z})}}$$

$$\otimes |\mathrm{vac}\rangle\langle\mathrm{vac}||j_q = 0, 1; v_q > 0\}, \qquad (28)$$

where $\vec{j} = \{j_1, j_2, \ldots, j_{w(\vec{z})}\}$, $\vec{v} = \{v_1, v_2, \ldots, v_{w(\vec{z})}\}$, $\vec{v} > 0$ means all of its element v_q is larger than zero, the element $M_{c_q(\vec{z}),v_q}^{j_q}$ corresponds to the measurement result that detector $\mathrm{DET}_{c_q(\vec{z})}^{j_q}$ receives v_q photons and $|\mathrm{vac}\rangle\langle\mathrm{vac}|$ denotes other detectors have not received any photon. The set of all operators $S_{\vec{z},\vec{v}>0}^{\vec{j}}$'s only spans a subspace. From Fig. 4 we can see that one mode coming from the first pulse and one mode coming from the Nth pulse are not detected by Bob (or the measurement results of them are discarded by Bob). Therefore we need to also consider Bob's undetected subspace. We assume Bob's undetected subspace (or the measurement results of which are discarded) is spanned by the orthogonal basis $\{|R_1\rangle, |R_2\rangle, \ldots\}$. Then all $S_{\vec{z},\vec{v}>0}^{\vec{j}}$'s and $|R_i\rangle$'s make up a complete set of projections for Bob. An announcement $\vec{z}$ corresponds to several measurement results. Each result corresponds to a collapsed state of Eve. Then an announcement $\vec{z}$ collapses Eve's state into a mixed state made up by several pure state. For convenience, we let R_i denote the projector $|R_i\rangle\langle R_i|$. Then $S_{\vec{z},\vec{v}>0}^{\vec{j}}$ is orthogonal to R_i. From Eqs. (3) and (25) we know that for a given $\vec{x}$, $\vec{z}$, if $\vec{j} \neq \vec{l_{\vec{z}}^x}$, it is always satisfied that $\langle\Phi_{B,k}^{N,\vec{x}}|S_{\vec{z},\vec{v}>0}^{\vec{j}}|\Phi_{B,k}^{N,\vec{x}}\rangle = 0$ and $\langle\Phi_{B,k}^{N,\vec{x}}|S_{\vec{z},\vec{v}>0}^{\vec{j}}R_i|\Phi_{B,k}^{N,\vec{x}}\rangle = 0$, where the second equality comes from the fact that $S_{\vec{z},\vec{v}>0}^{\vec{j}}$ is orthogonal to R_i. Then after we generalized Eq. (27) to the multioperator and multimeasurement-result case, we know that if Bob's announcement is $\vec{z}$, then Eve's conditional state becomes

$$\rho_E^{N,\vec{x},\vec{z}} = \sum_{\vec{v}>0,i} \frac{\langle \Psi_{EB}^{N,\vec{x}} | S_{\vec{z},\vec{v}>0}^{\vec{l}_{\vec{z}}^{\vec{x}}} R_i | \Psi_{EB}^{N,\vec{x}} \rangle}{P(\vec{z}|\vec{x})}$$
$$\times \mathrm{Proj}\left(\sum_k \frac{c_k^{\vec{x}} \sqrt{\langle \Phi_{B,k}^{N,\vec{x}} | S_{\vec{z},\vec{v}>0}^{\vec{l}_{\vec{z}}^{\vec{x}}} R_i | \Phi_{B,k}^{N,\vec{x}} \rangle} | \Phi_{E,k}^{N,\vec{x}} \rangle}{\sqrt{\langle \Psi_{EB}^{N,\vec{x}} | S_{\vec{z},\vec{v}>0}^{\vec{l}_{\vec{z}}^{\vec{x}}} R_i | \Psi_{EB}^{N,\vec{x}} \rangle}} \right),$$

$$(29)$$

where $\mathrm{Proj}(|\Psi\rangle)$ denotes the state $|\Psi\rangle\langle\Psi|$,

$$P(\vec{z}|\vec{x}) = \sum_{\vec{v}>0} \langle \Psi_{EB}^{N,\vec{x}} | S_{\vec{z},\vec{v}>0}^{\vec{l}_{\vec{z}}^{\vec{x}}} | \Psi_{EB}^{N,\vec{x}} \rangle \qquad (30)$$

describes the conditional probability of announcement $\vec{z}$ for a given $\vec{x}$, $\langle \Psi_{EB}^{N,\vec{x}} | S_{\vec{z},\vec{v}>0}^{\vec{l}_{\vec{z}}^{\vec{x}}} | \Psi_{EB}^{N,\vec{x}} \rangle$ gives the probability of the measurement result corresponding to the operator $S_{\vec{z},\vec{v}>0}^{\vec{l}_{\vec{z}}^{\vec{x}}}$ and we have used the result that if $\vec{j} \neq \vec{l}_{\vec{z}}^{\vec{x}}$, then $\langle \Psi_{EB}^{N,\vec{x}} | S_{\vec{z},\vec{v}>0}^{\vec{j}} R_i | \Psi_{EB}^{N,\vec{x}} \rangle = 0$.

It can be seen that for the detector DET_i^j the projector to the vacuum state $|vac\rangle\langle vac|$ can also be written as M_{i0}^j. Then from Eqs. (23) and (28), it can be seen that if $w(\vec{z})=w(\vec{z}')$, then

$$\langle \Phi_{B,k}^{N,\vec{x}} | S_{\vec{z},\vec{v}>0}^{\vec{l}_{\vec{z}}^{\vec{x}}} | \Phi_{B,k}^{N,\vec{x}} \rangle = \langle \Phi_{B,k}^{N,\vec{x}} | S_{\vec{z}',\vec{v}>0}^{\vec{l}_{\vec{z}'}^{\vec{x}}} | \Phi_{B,k}^{N,\vec{x}} \rangle,$$

$$\langle \Phi_{B,k}^{N,\vec{x}} | S_{\vec{z},\vec{v}>0}^{\vec{l}_{\vec{z}}^{\vec{x}}} R_i | \Phi_{B,k}^{N,\vec{x}} \rangle = \langle \Phi_{B,k}^{N,\vec{x}} | S_{\vec{z}',\vec{v}>0}^{\vec{l}_{\vec{z}'}^{\vec{x}}} R_i | \Phi_{B,k}^{N,\vec{x}} \rangle, \qquad (31)$$

where we have used results that the output mode $d_j^{\vec{l}_i^{\vec{x}}}$ is a vacuum state and $S_{\vec{z},\vec{v}>0}^{\vec{j}}$ is orthogonal to R_i.

We know that $P(\vec{z},\vec{x})=P(\vec{z}|\vec{x})P(\vec{x})$, $P(\vec{x}|\vec{z})=P(\vec{z},\vec{x})/P(\vec{z})$, and $P(\vec{z})=\Sigma_{\vec{x}}P(\vec{z},\vec{x})$, so from Eqs. (14), (30), and (31) it can be obtained that

$$P(\vec{z}|\vec{x}) = P(\vec{z}'|\vec{x}),$$

$$P(\vec{z},\vec{x}) = P(\vec{z}',\vec{x}),$$

$$P(\vec{z}) = P(\vec{z}'),$$

$$P(\vec{x}|\vec{z}) = P(\vec{x}|\vec{z}') \qquad (32)$$

for $w(\vec{z})=w(\vec{z}')$. By combining Eqs. (24) and (29)–(32) we obtain our final result.

Lemma 2. If there is no bit error and $w(\vec{z})=w(\vec{z}')$, we always have

$$\rho_E^{N,\vec{x},\vec{z}} = \rho_E^{N,\vec{x},\vec{z}'},$$

$$\rho_E^{N,\vec{z}} = \rho_E^{N,\vec{z}'}. \qquad (33)$$

The second equation in the Eq. (33) is derived from Eq. (32) and the fact that $\rho_E^{N,\vec{z}}=\Sigma_{\vec{x}}P(\vec{x}|\vec{z})\rho_E^{N,\vec{x},\vec{z}}$. Equation (33) shows that Eve's conditional state is only determined by the total number of Bob's detections and is independent of the positions of the detections. This means that only the weight of $\vec{z}$

matters, and we can use this instead of $\vec{z}$. In the following we introduce $\rho_E^{N,\vec{x},t}$ to denote the same conditional state that Eve holds for any $\vec{z}$ with weight t, i.e.,

$$t = w(\vec{z}),$$

$$\rho_E^{N,\vec{x},t} = \rho_E^{N,\vec{x},\vec{z}}. \qquad (34)$$

Here $\rho_E^{N,\vec{x},t}$ can be regarded as Eve's conditional state while Bob only announces the total number of his detections. With this new notation, we can simplify the expression of the mutual information discussed in the following.

B. Discussion of Eve's information

Since Eve's state is invariant under the permutation of $\vec{z}$, it is possible that Eve's information about Alice's bit string can also be bounded by a term that only depends on Bob's total detection count (the weight of $\vec{z}$). In this subsection we upper bound Eve's information about Alice's bit string by a term that is only conditioned on Bob's total detection count by applying the super subadditivity result proved in Appendix A. Then we give restrictions on Eve's information by using the fact that the maximum information Eve can get on Alice's bit string should be no larger than the Holevo quantity [45] of the states sent by Alice and the fact that the conditional mutual information should be no larger than the entropy of Alice's modulation. With these restrictions it is possible for us to give an upper bound to Eve's information about Alice's bit string.

First we define

$$F(w) := \sum_{\vec{z}} P(\vec{z}|W=w) S(\vec{L}_{\vec{z}} : E | \vec{Z}=\vec{z}), \qquad (35)$$

where we have introduced a variable W that can take the value of $w(\vec{z})$ and $P(\vec{z}|W=w)$ denotes the probability of $\vec{z}$ when $w(\vec{z})=w$.

From Eq. (8) we know that Eve's information about Alice's bit string can be rewritten as

$$S(\vec{U}_A : E | \vec{Z}) = \sum_{w=1}^{N-1} P(w) F(w). \qquad (36)$$

Now we will see that the $F(w)$ is no larger than a term that only depends on the total count w.

According to the definition of Von Neumann mutual information [45], the mutual information between Alice and Eve conditioned on Bob's announcement $\vec{z}$ can be given by

$$S(\vec{L}_{\vec{z}} : E | \vec{Z}=\vec{z}) = S(\rho_E^{N,\vec{z}}) - \sum_{\vec{l}_{\vec{z}}} P(\vec{l}_{\vec{z}}|\vec{z}) S(\rho_E^{N,\vec{l}_{\vec{z}},\vec{z}}), \qquad (37)$$

where $P(\vec{l}_{\vec{z}}|\vec{z})$ is the probability that $\vec{L}_{\vec{z}}$ takes the value of $\vec{l}_{\vec{z}}$ while $\vec{Z}=\vec{z}$,

$$\rho_E^{N,\vec{l}_{\vec{z}}\vec{z}} = \sum_{\vec{x} \in \Gamma(\vec{l}_{\vec{z}})} P(\vec{x}|\vec{l}_{\vec{z}},\vec{z})\rho_E^{N,\vec{x},\vec{z}},$$

$\Gamma(\vec{l}_{\vec{z}})$ is the collection of all $\vec{x}$'s that satisfy $x_{c_i(\vec{z})} \oplus x_{c_i(\vec{z})-1} = (l_{\vec{z}})_i$ and $P(\vec{x}|\vec{l}_{\vec{z}},\vec{z})$ is the probability that $\vec{X}$ takes the value of $\vec{x}$ while $\vec{L}_{\vec{z}} = \vec{l}_{\vec{z}}$ and $\vec{Z} = \vec{z}$.

Also From Eq. (32) we know that the conditional probability $P(\vec{x}|\vec{z})$ is actually only conditioned on the weight of $\vec{z}$, so we can introduce $P(\vec{x}|w(\vec{z}))$ to denote $P(\vec{x}|\vec{z})$. Since $\vec{l}_{\vec{z}}$ is part of $\vec{l}$ and $\vec{l}$ is generated from $\vec{x}$, the conditional probability $P(\vec{l}_{\vec{z}}|\vec{z})$ is also only conditioned on the weight of $\vec{z}$. Therefore we can also write $P(\vec{l}_{\vec{z}}|\vec{z})$ as $P(\vec{l}_{\vec{z}}|w(\vec{z}))$ and $P(\vec{x}|\vec{l}_{\vec{z}},\vec{z})$ as $P(\vec{x}|\vec{l}_{\vec{z}},w(\vec{z}))$, where $P(\vec{x}|\vec{l}_{\vec{z}},\vec{z}) = P(\vec{x},\vec{l}_{\vec{z}}|\vec{z})/P(\vec{l}_{\vec{z}}|\vec{z})$, and $P(\vec{l}_{\vec{z}}|w(\vec{z}))$ denotes the probability that $\vec{L}_{\vec{z}}$ takes the value of $\vec{l}_{\vec{z}}$ while $W = w(\vec{z})$. Then from lemma 2 we know that $\rho_E^{N,\vec{l}_{\vec{z}}\vec{z}}$ can be written as $\rho_E^{N,\vec{l}_{\vec{z}},w(\vec{z})}$. Here, that the conditional probabilities, $P(\vec{l}_{\vec{z}}|w(\vec{z}))$ and $P(\vec{x}|\vec{l}_{\vec{z}},w(\vec{z}))$, and the conditional state $\rho_E^{N,\vec{l}_{\vec{z}},w(\vec{z})}$ are conditioned on the weight of $\vec{z}$ means that they are conditioned on Bob's announcement of the total number of his detection count rather than the actual detection positions.

Now we can use lemma 2 to simplify $S(\vec{L}_{\vec{z}}:E|\vec{Z}=\vec{z})$ and thus $F(w)$. From lemma 2 and Eq. (34) we know that $\rho_E^{N,\vec{l}_{\vec{z}},\vec{z}}$ and $\rho_E^{N,\vec{z}}$ in Eq. (37) can be replaced by $\rho_E^{N,\vec{l}_{\vec{z}},w(\vec{z})}$ and $\rho_E^{N,w(\vec{z})}$. Then $S(\vec{L}_{\vec{z}}:E|\vec{Z}=\vec{z})$ becomes

$$S(\vec{L}_{\vec{z}}:E|\vec{Z}=\vec{z}) = S(\rho_E^{N,w(\vec{z})}) - \sum_{\vec{l}_{\vec{z}}} P(\vec{l}_{\vec{z}}|\vec{z})S(\rho_E^{N,\vec{l}_{\vec{z}},w(\vec{z})})$$
$$= S(\vec{L}_{\vec{z}}:E|W=w(\vec{z})), \qquad (38)$$

where we have used the definition of the conditional Von Neumann mutual information which says

$$S(\vec{L}_{\vec{z}}:E|W=w) = S(\rho_E^{N,w}) - \sum_{\vec{l}_{\vec{z}}} P(\vec{l}_{\vec{z}}|w)S(\rho_E^{N,\vec{l}_{\vec{z}},w}) \qquad (39)$$

and the result $P(\vec{l}_{\vec{z}}|w) = P(\vec{l}_{rowz}|\vec{z})$ for $w = w(\vec{z})$. Here $S(\vec{L}_{\vec{z}}:E|W=w)$ is actually Eve's information about $\vec{L}_{\vec{z}}$ while Bob only announces the total number of his counts. It can be seen that Eve's information about certain $\vec{L}_{\vec{z}}$ does not change if Bob publishes detailed position of his detection or only the total number of his detection.

We know that the mutual information $S(\vec{L}_{\vec{z}}:E|W=w(\vec{z}))$ can also be given by

$$S(\vec{L}_{\vec{z}}:E|W=w(\vec{z})) = H(\vec{L}_{\vec{z}}|W=w(\vec{z})) - S(\vec{L}_{\vec{z}}|E,W=w(\vec{z}))$$
$$\leqslant w(\vec{z}) - S(\vec{L}_{\vec{z}}|E,W=w(\vec{z})), \qquad (40)$$

where we have used the fact that $H(\vec{L}_{\vec{z}}|W=w(\vec{z})) \leqslant w(\vec{z})$.

Then by inserting Eqs. (38) and (40) to the expression of $F(w)$ given by Eq. (35) we can immediately get

$$F(w) \leqslant w - \sum_{\vec{z}} P(\vec{z}|W=w)S(\vec{L}_{\vec{z}}|E,W=w), \qquad (41)$$

where we have used the fact that $\sum_{\vec{z}} P(\vec{z}|W=w) = 1$. In the following it can be seen that the last term in Eq. (41) can be lower bounded by a term depending on Bob's total count

The probability $P(\vec{z}|W=w)$ for $w(\vec{z}) = w$ in Eq. (41) can be given by

$$P(\vec{z}|W=w) = \frac{P(\vec{z})}{\sum_{\vec{z}'|w(\vec{z}')=w} P(\vec{z}')} = \frac{1}{\sum_{\vec{z}'|w(\vec{z}')=w} 1} = \frac{1}{C_{N-1}^w}, \qquad (42)$$

where in the second line we have used the Eq. (32), and $C_{N-1}^w = \sum_{\vec{z}'|w(\vec{z}')=w} 1$ denotes the number of permutations of w in $N-1$.

Since $\vec{L}_{\vec{z}}$ can be regarded as $w(\vec{z})$ selection from $\vec{L}$, which is composed of $N-1$ elements, by using super-subadditivity of entropy (which is proved in the Appendix), we have

$$\sum_{\vec{z}|w(\vec{z})=w} S(\vec{L}_{\vec{z}}|E,W=w) \geqslant \frac{wC_{N-1}^w}{N-1}S(\vec{L}|E,W=w). \qquad (43)$$

Then by combining Eqs. (41)–(43), we can obtain

$$F(w) \leqslant w - \frac{w}{N-1}S(\vec{L}|E,W=w). \qquad (44)$$

Finally, from Eqs. (36) and (44) we know that Eve's information about Alice's bit string satisfies

$$S(\vec{U}_A:E|\vec{Z}) = \sum_{w=1}^{N-1} P(w)F_w \leqslant \sum_{w=1}^{N-1} P(w)w$$
$$- \frac{1}{N-1}\sum_{w=1}^{N-1} P(w)wS(\vec{L}|E,W=w), \qquad (45)$$

where we sum over w in the range of 1 to $N-1$, because the maximum value of w is $N-1$ and Alice and Bob discard the result while there is no detection.

Equation (45) gives us an upper bound on Eve's information about Alice's state, when there is no bit error. This upper bound no longer depends on Bob's counting positions denoted by $\vec{z}$. Now the remaining problem is to find some practical restrictions, so that the upper bound of Eve's information can be calculated.

Since all possible w is within 0 and $N-1$, it can be seen that

$$\sum_{w=0}^{N-1} P(w)S(\vec{L}|E,W=w) = S(\vec{L}|E,W). \qquad (46)$$

In the following we will see that if $S(\vec{L}|E,W)$ can be lower bounded, then $S(\vec{U}_A:E|\vec{Z})$ can be upper bounded.

According to the definition of mutual information, $S(\vec{L}|E,W)$ can be expressed as

$$S(\vec{L}|E,W) = H(\vec{L}) - S(\vec{L}:E,W) = N - 1 - S(\vec{L}:E,W), \tag{47}$$

where $H(\vec{L}) = N-1$, and $S(\vec{L}:E,W)$ is the mutual information between $\vec{L}$ and the combination of Eve and system W.

Since $\vec{L}$ is generated from X and $l_i = x_{c_i} \oplus x_{c_i-1}$, given x_1 and $\vec{l}$, we can completely reconstruct $\vec{x}$. Therefore, we have

$$S(\vec{L}, X_1 : E, W) = S(\vec{X} : E, W). \tag{48}$$

Because discarding a subsystem never increases the mutual information [45], Eq. (48) leads to

$$S(\vec{L}:E,W) \leq S(\vec{X}:E,W). \tag{49}$$

The term $S(\vec{X}:E,W)$ is the mutual information between Alice and the combination of Eve and system W. The system E, W can be regarded as a system locally generated from the original state, $\rho_A^{\otimes N} = \Sigma_{\vec{x}} P(\vec{x}) |\Psi_{\vec{x}}^N\rangle\langle\Psi_{\vec{x}}^N|$, sent out by Alice. Since local operations cannot increase the mutual information, the maximum mutual information $S(\vec{X}:E,W)$ should not be bigger than the maximum information one can obtain from the original state $\rho_A^{\otimes N}$, which is upper bounded by the Holevo quantity of $\rho_A^{\otimes N}$ [45]. The Holevo quantity of $\rho_A^{\otimes N}$ is given by $NS(A)$, where

$$S(A) = h\left[\frac{1}{2}(1 - |\langle -\alpha|\alpha\rangle|)\right] \tag{50}$$

is the entropy of a single state $\rho_A = \frac{1}{2}|-\alpha\rangle\langle-\alpha| + \frac{1}{2}|\alpha\rangle\langle\alpha|$ and $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function [44,45]. Now we know that

$$S(\vec{L}:E,W) \leq NS(A). \tag{51}$$

Then from Eqs. (46), (47), and (51), we can derive the final constraint on Eve's conditional entropy, which is given by

$$\sum_{w=1}^{N-1} P(w) S(\vec{L}|E, W=w) \geq (N-1)[1 - P(w=0)]$$

$$- NS(A) =: K. \tag{52}$$

where we have used the fact that $S(\vec{L}|E, W=0) \leq S(\vec{L}) = N-1$, and K denotes the first term in the second line.

Equation (52) gives one constraint on $S(\vec{L}|E, W=w)$. There is also another trivial constraint on $S(\vec{L}|E, W=w)$, which is

$$S(\vec{L}|E, W=w) \leq S(\vec{L}) = N - 1. \tag{53}$$

Then the remaining problem is to upper bound Eve's information (or to lower bound the secret key rate) under the constraints given by Eqs. (52) and (53).

C. Lower bound of the secret key rate

In this part we will give the lower bound of the secret key rate based on the above analysis. From Eq. (7) it can be seen that if there is no bit error, the mutual information between Alice and Bob is

$$I(\vec{U}_A : \vec{U}_B | \vec{Z}) = \sum_{\vec{z}} P(\vec{z})[H(\vec{L}_{\vec{z}} | \vec{Z} = \vec{z}) - H(\vec{L}_{\vec{z}} | \vec{Y}_{\vec{z}}, \vec{Z} = \vec{z})]$$

$$= \sum_{\vec{z}} P(\vec{z}) H(\vec{L}_{\vec{z}} | \vec{Z} = \vec{z}),$$

where we have used the fact that if there is no bit error $H(\vec{L}_{\vec{z}} | \vec{Y}_{\vec{z}}, \vec{Z} = \vec{z})] = 0$. After the channel estimation Alice and Bob can compute this mutual information. It can be seen that if for all $\vec{z}$ s, $\vec{L}_{\vec{z}}$ is evenly distributed, this mutual information becomes maximized, and $I(\vec{U}_A : \vec{U}_B | \vec{Z}) = \Sigma_{\vec{z}} P(\vec{z}) w(\vec{z})$. For simplification, in the following we introduce a term Δ to denote the difference between Bob's actual information and the maximal information he can get, in principle,

$$\Delta = \sum_w P(w) w - I(\vec{U}_A : \vec{U}_B | \vec{Z}). \tag{54}$$

Then from Eqs. (7), (45), and (54), we know that if there is no bit error the secret key rate per N pulses satisfies

$$G \geq \frac{1}{N-1} \sum_{w=1}^{N-1} P(w) w S(\vec{L}|E, W=w) - \Delta, \tag{55}$$

where $P(w)$ and Δ are known after the channel estimation.

It can be seen that under the constraints of Eqs. (52) and (53), the lower bound of the secret key rate given by Eq. (55) reaches its minimum when $S(\vec{L}|E, W=w) = 0$ for large values of w and $S(\vec{L}|E, W=w) = N-1$ for small values of w while satisfying Eq. (52) at the same time. Then the final lower bound on the secret key rate per N pulses is given by

$$G \geq \sum_{w=1}^{w_0} P(w) w - \Delta, \tag{56}$$

where the w_0 is the solution to the equations

$$\sum_{w=1}^{w_0} P(w)(N-1) \leq K,$$

$$\sum_{w=1}^{w_0+1} P(w)(N-1) \geq K, \tag{57}$$

where K is defined in the Eq. (52). This formula for the key generation rate in Eq. (56) is applicable to any N any distribution in Bob's detection statistics. In the next section, we will consider a particular distribution as an example.

V. SECRET KEY RATE UNDER THE BINOMIAL DISTRIBUTION CASE

We illustrate how to compute the key generation rate in Eq. (56) derived in the previous section for a channel that produces a binomial distribution in Bob's detection statistics. We show that in this case the secret key generation rate per pulse is linearly proportional to the channel transmission probability [see Eq. (65)].

Consider the specific case where Bob's total count obeys the binomial distribution, $\Delta = 0$ and $N \to \infty$. Under this case

$$P(w) = C_{N-1}^w r^w (1-r)^{N-w-1}, \tag{58}$$

where r denotes the detection rate per pulse.

For the $N \to \infty$ case, the binomial distribution tends to the Gaussian distribution with the same mean and variance as $P(w)$. For convenience of discussion of the $N \to \infty$ case, here we introduce λ denote the ratio of w over $N-1$:

$$\lambda = \frac{w}{N-1}.$$

Under the case that $N \to \infty$, the λ can be regarded as a real number. Then instead of dealing with the Gaussian approximation of $P(w)$ we can deal with an approximation for $P(\lambda)$, which denotes the distribution of λ. The Gaussian approximation of $P(\lambda)$ can be directly given by

$$P(\lambda) \approx \frac{N-1}{\sqrt{2\pi(N-1)r(1-r)}} \exp\left[-\frac{(N-1)(r-\lambda)^2}{2r(1-r)}\right] \tag{59}$$

which has the same mean and variance as $P(\lambda)$.

The lower bound of the secret key rate given by Eq. (56) can be approximated by

$$G \geq (N-1) \int_0^{\lambda_0} d\lambda P(\lambda)\lambda, \tag{60}$$

where the $\lambda_0 = w_0/(N-1)$, which can be given by the solution to the equation

$$\int_0^{\lambda_0} d\lambda P(\lambda) = \frac{K}{N-1}. \tag{61}$$

Here Eq. (61) is obtained by putting λ into Eq. (57).

It can be seen that when $N \to \infty$, we have $P(w=0)=0$ and $\frac{N}{N-1}=1$. Then Eq. (61) becomes

$$\int_0^{\lambda_0} d\lambda P(\lambda) = 1 - S(A). \tag{62}$$

To find a solution to Eqs. (60) and (62), we introduce another function $F(\lambda)$:

$$F(\lambda) = \begin{cases} P(\lambda), & \text{while } \lambda \leq \lambda_0 \\ 0 & \text{while } \lambda > \lambda_0. \end{cases} \tag{63}$$

Then it can be seen that when $N \to \infty$,

$$\int_{-\infty}^{\infty} d\lambda F(\lambda) = 1 - S(A),$$

$$F(\lambda) = 0 \quad \text{for } \lambda \neq r,$$

where the expression in the second line can be seen from the fact that $\lim_{N \to \infty} \frac{N}{\sqrt{2\pi Nr(1-r)}} \exp[-\frac{N(r-\lambda)^2}{2r(1-r)}] = 0$ for $\lambda \neq r$.

We see that $F(\lambda)$ is actually a delta function satisfying $F(\lambda) = [1 - S(A)]\delta(\lambda - r)$. From Eqs. (60) and (63), we can finally get the secret key rate for the binomial distribution and $N \to \infty$ case. It is given by

$$G \geq (N-1) \int_{-\infty}^{\infty} d\lambda F(\lambda)\lambda = (N-1)r[1 - S(A)]. \tag{64}$$

When given that the amplitude of coherent state is α and the total transmission probability is η, then the secret key rate per pulse can be given by

$$g \geq \eta |\alpha|^2 \left\{ 1 - h\left[\frac{1}{2}(1 - e^{-4|\alpha|^2})\right] \right\}, \tag{65}$$

where we have used Eq. (50), the result that $|\langle -\alpha | \alpha \rangle| = e^{-4|\alpha|^2}$ and the factor $N-1$ is canceled since this is a key rate per pulse. From this result it can be seen that the lower bound of the secret key rate per pulse is linearly proportional to the channel transmission probability. It can be calculated that when $\alpha = 0.338$, the right part in the Eq. (65) is maximized and is given by 0.0357η. Note that our result is consistent with the upper bounds on the key rate given in Refs. [30,33]. From Ref. [11], one can easily find that the key generation rate per tranmistted pulse of BB84 in the noiseless case scales at a higher rate than that of DPSQKD. However, the overall secret key generation rate is also determined by the modulation rate, and we remark that it is possible that DPSQKD can outperform BB84 in the modulation rate, since DPSQKD only requires one binary phase modulation at Alice's side, while BB84 requires a quaternary modulator at Alice's side and a binary or quaternary modulator at Bob's sides [46] (the binary modulation is easier to realize than the quaternary one.).

VI. CONCLUSION

We prove the security for DPSQKD with a weak-coherent light source against collective attacks in the noiseless case. The only assumption we employ are that the quantum theory is true, the device is trusted and the key size is infinite. The key point that guarantees this scheme to be secure is that Eve's state is independent of the positions of Bob's detections, so that after the post-selection, in which Alice and Bob discard the data that Bob did not receive a signal for, Bob knows Alice's sifted data better than Eve does. In addition, we consider a specific case where the total number of Bob's count obeys the binomial distribution. In this case, we derive the lower bound of the secret key rate per pulse and it is linearly proportional to the channel transmission probability. This result definitely suggests that DPSQKD has a high potential for high speed communication, since it is easy to engineer DPSQKD to operate at a high modulation rate. Although we have only proved the security of DPSQKD for the noiseless case, we hope that our work can offer some insights into the security of DPSQKD and may serve as a stepping stone for proving the security for the noisy case.

ACKNOWLEDGMENTS

APPENDIX: SUPER SUBADDITIVITY FOR THE MULTISYSTEM CASE

Theorem 1. Suppose $\Theta_n = \{A_1, \ldots, A_n\}$ is a collection of n systems and Ξ_m^n is a collection of all possible m selections from n cases. Then it is always true for arbitrary n and $m \leq n$ that

$$\sum_{\vec{i} \in \Xi_m^n} S(A_{i_1}, A_{i_2}, \ldots, A_{i_m}|E) \geq C_{n-1}^{m-1} S(A_1, A_2, \ldots, A_n|E),$$

(A1)

where $\vec{i} = (i_1, i_2, \ldots, i_m)$, E is another system, and $C_n^m = \frac{n!}{m!(n-m)!}$. This theorem is a generalization of the following lemma for subadditivity of Von Neuemann entropy (see, e.g., Ref. [45]).

Lemma 1. For three quantum systems A_1, A_2, and E, $S(A_1|E) + S(A_2|E) \geq S(A_1, A_2|E)$.

Proof of theorem 1. We will use induction to prove the theorem. First, notice that for $m = n$, this theorem is always true. In the following we will prove that for n and $m = 1$ this theorem holds, which will be called first proof (FP) in the following. Then we prove if for n and m and $m-1$ ($m > 1$) the above theorem is correct, then for $n+1$ and m it is also correct, which will be called second proof (SP). Thirdly, we will prove that if for $n-1$ and $m = n-2$ ($n > 2$) the above theorem is true then for n and $m+1$ it is also valid, which will be called third proof (TP). Since for $n = 2$ and $m = 1$, the above theorem is true, then it is also true for $n = 3$ and $m = 2$ by applying the TP.

This theorem is true for $n = 3$ and $m = 2$ and $n = 3$ and $m = 1$. Then by applying the SP, we know that it is also valid for $n = 4$ and $m = 2$ and consequently for all of n and $m = 2$. After we continuously do such induction we can see that if FP, SP and TP is correct then for all $n \geq m$ the above theorem holds.

Now we prove the FP first. Observe that for arbitrary n and $m = 1$, Eq. (A1) holds by repeated applications of lemma 1, i.e.,

$$\sum_{i=1}^{n} S(A_i|E) \geq S(A_1, A_2, \ldots, A_n|E)$$

(A2)

holds. Now we will prove the SP, which is claims that if for n and m and $m-1$ the above theorem holds, then for $n+1$ and m it also holds.

We assume that $\Theta_{n+1} = \{A_1, \ldots, A_n, A_{n+1}\} = \{A_1, \ldots, A_n, B\}$. Here we use B to denote A_{n+1}.

In the following we use $\bar{\Xi}_m^n$ to denote the collection of all possible m selections in n samples. First we have

$$T = \sum_{\vec{i} \in \Xi_m^{n+1}} S(A_{i_1}, A_{i_2}, \ldots, A_{i_m}|E)$$

$$= \sum_{\vec{i} \in \Xi_m^n} S(A_{i_1}, A_{i_2}, \ldots, A_{i_m}|E)$$

$$+ \sum_{\vec{i} \in \Xi_{m-1}^n} S(A_{i_1}, A_{i_2}, \ldots, A_{i_{m-1}}, B|E) = C + D, \quad \text{(A3)}$$

where $\vec{i} = (i_1, i_2, \ldots, i_m)$ denotes a possible m selection in n cases and we introduced T, C, and D to denote the terms given in the first, second and third line, respectively. If the theorem is valid for n and m, then we have

$$C \geq \frac{m C_n^m}{n} S(A_1, A_2, \ldots, A_n|E).$$

(A4)

Now, D can also be given by

$$D = \sum_{\vec{i} \in \Xi_{m-1}^n} S(A_{i_1}, A_{i_2}, \ldots, A_{i_{m-1}}|BE) + C_n^{m-1} S(B|E)$$

$$= D_1 + C_n^{m-1} S(B|E),$$

(A5)

where we have applied the fact that $S(A|EB) + S(B|E) = S(AB|E)$ and $\sum_{\vec{i} \in \Xi_{m-1}^n} = C_n^{m-1}$. Also, if the above theorem is correct for n and $m-1$, we have

$$D_1 \geq \frac{(m-1) C_n^{m-1}}{n} S(A_1, A_2, \ldots, A_n|BE).$$

(A6)

Here,

$$C_n^m = \frac{n!}{m!(n-m)!}.$$

(A7)

Then if we put Eqs. (A4)–(A7) into Eq. (A3) we can immediately get

$$T \geq \frac{n!(n-m+1)m}{nm!(n-m+1)!}[S(A_1, A_2, \ldots, A_n|E) + S(B|E)]$$

$$+ \frac{n! m(m-1)}{nm!(n-m+1)!}[S(A_1, A_2, \ldots, A_n|BE) + S(B|E)].$$

(A8)

Since the above theorem is correct for $n = 2$ and $m = 1$, we have

$$S(A_1, A_2, \ldots, A_n|E) + S(B|E) \geq S(A_1, A_2, \ldots, A_n, B|E).$$

(A9)

Then if we put Eq. (A9) into Eq. (A8) and apply the results that $S(A|EB) + S(B|E) = S(AB|E)$ and

$$\frac{n! m(m-1)}{nm!(n-m+1)!} = \frac{m C_{n+1}^m}{n+1},$$

we can obtain

$$T \geqslant \frac{mC_{n+1}^m}{n+1} S(A_1, A_2, \ldots, A_n, B|E)$$

which says that if for n and m and $m-1$, the above theorem is correct then for $n+1$ and m it is also correct. Now the SP is proved.

Now, we will prove the TP, that is if for $n-1$ and $m=n-2$ ($n>2$) the above theorem is true then for n and $m+1$ it is also true. We assume that $\Theta_n = \{A_1, \ldots, A_{n-1}, B\}$. Here we use B to denote A_n. Then we have that

$$S = \sum_{\vec{i} \in \Xi_{m+1}^n} S(A_{i_1}, A_{i_2}, \ldots, A_{i_m}, A_{i_{m+1}}|E) = S(A_1, A_2, \ldots, A_{n-1}|E)$$
$$+ \sum_{\vec{i} \in \Xi_m^{n-1}} S(A_{i_1}, A_{i_2}, \ldots, A_{i_m}, B|E) = S_1 + S_2, \quad (A10)$$

where the S, S_1, and S_2 are introduced to denote the expression in the first, second, and third line, respectively, and in the second line we have used the requirement that $m=n-2$.

Since $S(A|EB) + S(B|E) = S(AB|E)$, and $\sum_{\vec{i} \in \Xi_m^{n-1}} = C_{n-1}^m$,

$$S_2 = \sum_{\vec{i} \in \Xi_m^{n-1}} S(A_{i_1}, A_{i_2}, \ldots, A_{i_m}|BE) + C_{n-1}^m S(B|E)$$
$$\geqslant \frac{mC_{n-1}^m}{n-1} S(A_1, A_1, \ldots, A_{n-1}|BE) + C_{n-1}^m S(B|E)$$
$$= m[S(A_1, A_1, \ldots, A_{n-1}|BE) + S(B|E)] + S(B|E)$$
$$= mS(A_1, A_1, \ldots, A_{n-1}, B|E) + S(B|E), \quad (A11)$$

where we have applied the assumption that for $n-1$ and m the above theorem is correct and the fact that $C_{n-1}^m = n-1$ for $m = n-2$.

Now we put Eq. (A11) in to Eq. (A10) we can obtain that

$$S \geqslant mS(A_1, A_1, \ldots, A_{n-1}, B|E) + S(A_1, A_2, \ldots, A_{n-1}|E) + S(B|E)$$
$$\geqslant (m+1)S(A_1, A_1, \ldots, A_{n-1}, B|E)$$
$$= \frac{(m+1)C_n^{m+1}}{n} S(A_1, A_2, \ldots, A_{n-1}, A_n|E),$$

where in the third line we have used the subadditivity for $n=2$ and $m=1$ case. Now the TP is proved. Since the assumptions FP, SP and TP hold and the initial conditions are satisfied, it is proved that for all $n \geqslant m$ the above theorem holds.   ∎

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

[2] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[3] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).

[4] Yi-Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus, e-print arXiv:0807.3751.

[5] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).

[6] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).

[7] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, New J. Phys. **7**, 232 (2005).

[8] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, Opt. Express **14**, 13073 (2006).

[9] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).

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

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

[12] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

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

[14] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).

[15] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, e-print arXiv:quant-ph/0503002.

[16] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).

[17] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, in *Proceedings of IEEE International Symposium on Information Theory (ISIT) 2006* (IEEE Press, New York, 2006), pp. 2094–2098.

[18] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **8**, 431 (2007).

[19] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[20] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).

[21] K. Tamaki, N. Lütkenhaus, M. Koashi, and Jamie Batuwantudawe, e-print arXiv:quant-ph/0607082.

[22] K. Tamaki, Phys. Rev. A **77**, 032341 (2008).

[23] D. Mayers, J. ACM **48**, 351 (2001), ,preliminary version in D. Mayers, *Advances in Crytology–Proceedings of Crypto '96*, Vol. 1109 of Lecture Notes in Computer Science, edited by N. Koblitz (Springer-Verlag, New York, 1996), pp. 343–357.

[24] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing (ACM Press, New York, 2000), pp. 715–724.

[25] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

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

[27] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[28] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[29] E. Waks, H. Takesue, and Y. Yamamoto, e-print arXiv:quant-ph/0508112.

[30] M. Curty, L.-L. Zhang, H.-K. Lo, and N. Lütkenhaus, Quantum Inf. Comput. **7**, 665 (2007).

[31] T. Tsurumaru, Phys. Rev. A **75**, 062319 (2007).

[32] M. Curty, K. Tamaki, and T. Moroder, Phys. Rev. A **77**, 052321 (2008).

[33] C. Branciard, N. Gisin, and V. Scarani, New J. Phys. **10**, 013031 (2008).

[34] H. Gomez-Sousa and M. Curty, e-print arXiv:0806.0858.

[35] Generally, Eve's attack can be separated into three classes: individual attacks, collective attacks and coherent attacks [36,37]. In individual attacks, Eve attacks each signal system separately with the same method and later measures her quantum state right after the sifting step. In collective attacks, Eve attacks each signal system separately with the same method but can perform arbitrary measurement after all of the steps, including the reconciliation, privacy amplification and the encryption. Coherent attacks are the most general attacks, where Eve can attack all of the signals together and perform the measurement at the end of the protocol.

[36] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, e-print arXiv:0802.4155.

[37] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[38] R. Renner, e-print arXiv:quant-ph/0512258.

[39] R. Renner, Nat. Phys. **3**, 645 (2007).

[40] M. Christandl and B. Toner, e-print arXiv:0712.0916.

[41] K. Wen, K. Tamaki, and Y. Yamamoto, e-print arXiv:0806.2684.

[42] Here we mean that all of Bob's detectors are the same with perfect efficiency and there is no dead time associated with them.

[43] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).

[44] C. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).

[45] M. A. Neilson and I. L. Chuang, *Quantum Computing and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000), Chaps. 11 and 12.

[46] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, e-print arXiv:0802.3788.