Information-theoretic security proof of differential-phase-shift quantum key distribution protocol based on complementarity

Akihiro Mizutani,[1] Toshihiko Sasaki,[2] Go Kato,[3] Yuki Takeuchi,[1] and Kiyoshi Tamaki[4]

[1] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2] *Photon Science Center, Graduate School of Engineering,*
The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan
[3] *NTT Communication Science Laboratories, NTT Corporation, 3-1,*
Morinosato Wakamiya Atsugi-Shi, Kanagawa, 243-0198, Japan
[4] *Department of Intellectual Information Engineering, Faculty of Engineering,*
University of Toyama, Gofuku 3190, Toyama 930-8555, Japan

We show the information-theoretic security proof of the differential-phase-shift (DPS) quantum key distribution (QKD) protocol based on the complementarity approach [arXiv:0704.3661 (2007)]. Our security proof provides a slightly better key generation rate compared to the one derived in the previous security proof in [arXiv:1208.1995 (2012)] that is based on the Shor-Preskill approach [Phys. Rev. Lett. 85, 441 (2000)]. This improvement is obtained because the complementarity approach can employ more detailed information on Alice's sending state in estimating the leaked information to an eavesdropper. Moreover, we remove the necessity of the numerical calculation that was needed in the previous analysis to estimate the leaked information. This leads to an advantage that our security proof enables us to evaluate the security of the DPS protocol with any block size. This paper highlights one of the fundamental differences between the Shor-Preskill and the complementarity approaches.

Quantum key distribution (QKD) holds promise to achieve information-theoretically secure communication between two distant parties (Alice and Bob) against any eavesdropper (Eve). Since the first invention of the BB84 protocol, many QKD protocols have been proposed so far [1–4]. Among them, the differential-phase-shift (DPS) QKD protocol [3] has been considered as one of the promising protocols for future implementation since this protocol can be rather simply implemented with a passive detection unit. Recently, a field demonstration of the DPS protocol [5] has already been conducted, and the information-theoretical security proofs of the DPS protocol have been established when Alice employs a single-photon source [6] and a block-wise phase-randomized coherent light source [7].

The previous security proof [7] with coherent light source is based on the *Shor-Preskill approach* [8] in which Alice and Bob virtually extract a maximally-entangled state (MES) to show that they share a monogamy correlation. In order to extract an MES, Alice and Bob use some estimated information about the correlation between them. Specifically, this information consists of the bit and phase error rates, where the phase error is defined by fictitious erroneous outcomes when Alice and Bob would have measured their virtual qubits in a basis conjugate to the basis for generating the key. Since the phase error rate cannot be directly obtained in the experiment, the estimation of this quantity is a central issue in the security proof, and some security proofs have been conducted along this approach.

Another approach for the security proof is the complementarity approach [9]. In this approach, a complementary control of the actual protocol and a virtual protocol are considered, which Alice and Bob choose to execute, but cannot execute simultaneously. The goal of the actual protocol is to agree on the bit values along the key generation basis, say the X basis, while in the virtual protocol, Alice and Bob collaborate to create an eigenstate of the Z basis (a complementary basis to the X basis) in Alice's side. With these protocols, Koashi proved in [9] that the necessary and sufficient condition for the secure key distillation is to be able to execute whichever task was chosen. On one hand, once an MES is shared between Alice and Bob, they also accomplish the complementary task, which implies that the Shor-Preskill approach is included in the complementarity one. On the other hand, the purpose of the complementarity approach is to create an eigenstate of the Z basis at Alice's side, and therefore, we can employ some additional information, such as the one on Alice's sending state, which may provide an advantage over the Shor-Preskill approach.

In this paper, we show that these two approaches indeed give a different resulting secret key rate of the DPS QKD protocol by exploiting a property of pulses emitted by Alice. More specifically, we adopt the complementarity approach for the security proof where we accommodate the intuition that it is difficult to extract information from a train of weak coherent pulses employed in the DPS protocol. As a result, we show that the secure key rate based on the complementarity approach is 1.22 times as high as the one based on the Shor-Preskill approach when the bit error rate is 2%. Moreover, we remove the necessity of the numerical calculation that was needed to evaluate the leaked information to Eve in the previous analysis [7], and we provide the closed formulas for the upper bounds on the leaked information. This leads to an advantage that our security proof enables us to evaluate the security of the DPS protocol with any block size.

Assumptions on users' devices.— Alice uses a laser source emitting coherent pulses and a phase modulator, and a train of L ($L \geq 3$) pulses forms a block. Bob uses a one-bit delay interferometer with two 50:50 beam splitters and with its delay being equal to the interval of the neighboring sending pulses. After the interferometer, the pulses are detected by two photon detectors corresponding to bit values of 0 and 1. The $j^{\rm th}$ ($1 \leq j \leq L-1$) time slot is defined as an expected detection time at Bob's detectors from the superposition of the $j^{\rm th}$ and $(j+1)^{\rm th}$ incoming pulses. Also, the $0^{\rm th}$ ($L^{\rm th}$) time slot is defined as an expected detection time at Bob's detectors from the superposition of the $1^{\rm st}$ ($L^{\rm th}$) incoming pulse and the $L^{\rm th}$ incoming pulse in the previous block ($1^{\rm st}$ incoming pulse in the next block).

As for the assumptions on Alice's device, we assume that (A 1) the phase modulator randomly modulates each relative phase between adjacent sending pulses by 0 or π. Moreover, (A 2) the randomization of overall optical phase δ is done for each block of L pulses. This means that the quantum state of the L pulses is written as a classical mixture of the total photon number contained in the L pulses. Besides, (A 3) we do not consider any side-channel in Alice's site.

Regarding with the assumptions on Bob's device, we suppose that (B 1) Bob uses two photon-number-resolving (PNR) detectors, which can discriminate among the vacuum, a single-photon and multiphoton. Also, we assume that (B 2) the detection efficiency is the same for both detectors. Finally, (B 3) we do not consider any side-channel in Bob's site.

Protocol.— The actual protocol proceeds as follows. In its description, $|\boldsymbol{\kappa}|$ denotes the length of a bit string $\boldsymbol{\kappa}$.

(a 1) Alice generates a random L-bit sequence $s_1 s_2 ... s_L$ and a random common phase shift $\delta \in [0, 2\pi)$. For a random L-bit sequence $s_1 s_2 ... s_L$, she sends the following coherent state (system $\mathcal{H}_S$) to Bob through a quantum channel $\bigotimes_{i=1}^{L} |e^{{\rm i}\delta}(-1)^{s_i}\alpha\rangle_{S,i}$, where $|\alpha\rangle_{S,i}$ represents the coherent state $\sum_n e^{-|\alpha|^2/2}\alpha^n |n\rangle_{S,i}/\sqrt{n!}$ of the $i^{\rm th}$ pulse mode.

(a 2) Bob performs the interference measurement with two PNR detectors, and we call the *successful detection* event if Bob detects one-photon in the $j^{\rm th}$ time slot (with $1 \leq j \leq L-1$), and detects the vacuum in all the other time slots including the $0^{\rm th}$ and $L^{\rm th}$ time slots. If the successful detection occurs, the variable j is set to the time slot, otherwise Bob sets $j = 0$. If $j \neq 0$, he obtains his raw bit $s \in \{0, 1\}$ depending on which detector has reported a detection at the $j^{\rm th}$ time slot. Bob announces j over an authenticated public channel.

(a 3) If $j \neq 0$, Alice calculates her raw key bit as $s_j \oplus s_{j+1} \in \{0, 1\}$.

(a 4) Alice and Bob repeat steps (a 1)-(a 3) N times.

(a 5) Alice defines a sifted key $\boldsymbol{\kappa}_A$ by concatenating the successful detection events (*i.e.,* $j \neq 0$).

(a 6) Bob defines a sifted key $\boldsymbol{\kappa}_B$ by concatenating the successful detection events (*i.e.,* $j \neq 0$).

(a 7) Bob corrects the errors in his sifted key $\boldsymbol{\kappa}_B$ to make it coincide with $\boldsymbol{\kappa}_A$ by sacrificing $|\boldsymbol{\kappa}_A| f_{\rm EC}$ bits of encrypted public communication from Alice by consuming the same length of the pre-shared secret key.

(a 8) Alice and Bob conduct privacy amplification by shortening their keys by $|\boldsymbol{\kappa}_A| f_{\rm PA}$ to obtain the final keys.

In this paper, we consider the asymptotic limit of the sifted key length ($N \to \infty$). In the experiments, the following parameters are observed: $Q := \frac{|\boldsymbol{\kappa}_A|}{N}$, $e^{(\rm b)} := \frac{{\rm wt}(\boldsymbol{\kappa}_A - \boldsymbol{\kappa}_B)}{|\boldsymbol{\kappa}_A|}$, where the minus sign is a bit-by-bit modulo-2 subtraction and ${\rm wt}(\boldsymbol{\kappa})$ denotes the weight (the number of 1's) in a bit string $\boldsymbol{\kappa}$. In the asymptotic limit, $f_{\rm EC}$ is given by a function of the bit error rate $e^{(\rm b)}$. The asymptotic key generation rate per sending pulse is given by [10, 11]

$$G = [Q(1 - f_{\rm EC}(e^{(\rm b)}) - f_{\rm PA})]/L. \tag{1}$$

In this key generation formula, we omit for simplicity the random sampling procedure to estimate the bit error rate $e^{(\rm b)}$ because its cost is negligible in the asymptotic limit.

In step (a 2), when the successful detection event ($j \neq 0$) occurs, the state of the incoming L pulses is expressed by the Hilbert space $\mathcal{H}_B$ spanned by L states, and we denote its orthonormal basis by $\{|i\rangle_B\}_{i=1}^{L}$, with i representing the position of the single-photon before the first beam splitter.

Security proof.— In the following, we show the results of the security proof based on the complementarity [9]. For this, note that thanks to the assumption (A 2), we can derive the amount of privacy amplification $Qf_{\rm PA}$ for each photon number emission events separately. That is, $Qf_{\rm PA}$ in Eq. (1) is written as

$$Qf_{\rm PA} = \sum_{\nu=0}^{\infty} Q^{(\nu)} h(e^{({\rm ph},\nu)}), \tag{2}$$

where $e^{({\rm ph},\nu)}$ denotes the phase error rate for the ν-photon emission events. Below, we derive the explicit relations between the phase error rate $e^{({\rm ph},\nu)}$ and bit error rate $e^{({\rm b},\nu)}$ for the ν-photon emission events. For simplicity, we consider extracting the secret key up to the two-photon emission events ($\nu = 0, 1$ and 2), and for more than two-photon emission events, we pessimistically assume that Eve has perfect knowledge on the sifted keys.

Zero-photon emission events

We first consider the case for $\nu = 0$ where Alice emits zero-photon, and our estimation result is given by $(e^{({\rm b},0)}, e^{({\rm ph},0)}) = (1/2, 0)$. This means that Eve cannot extract any information from the zero-photon emission events though she causes 50% bit error rate.

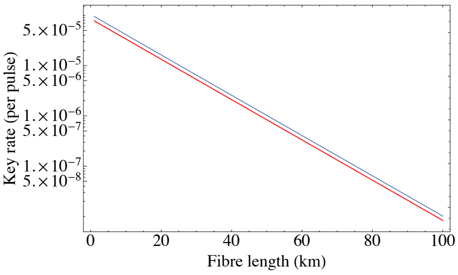

FIG. 1: The key generation rate per sending pulse of the DPS protocol based on our security analysis (upper curve) and the previous analysis (lower curve). In these plots, we set $L = 10$ and $e^{(\mathrm{b})} = 2\%$.

Single-photon emission events

Next, we show our estimation result on the upper bound on $e^{(\mathrm{ph},1)}$, which is is given by

$$e^{(\mathrm{ph},1)} \le (3+\sqrt{5})e^{(\mathrm{b},1)} =: \lambda_0 e^{(\mathrm{b},1)} \qquad (3)$$

if $0 \le e^{(\mathrm{b},1)} \le (10-3\sqrt{5})/22$ and

$$e^{(\mathrm{ph},1)} \le \inf_{0<\lambda<\lambda_0} \left\{ \lambda e^{(\mathrm{b},1)} + \frac{3-2\lambda+\sqrt{1+2\lambda^2}}{4} \right\} \qquad (4)$$

if $(10-3\sqrt{5})/22 < e^{(\mathrm{b},1)}$.

Two-photon emission events

Finally, we show our estimation result on the upper bound on $e^{(\mathrm{ph},2)}$. This is given by

$$e^{(\mathrm{ph},2)} \le \inf_{0<\lambda<\infty} \left[\lambda e^{(\mathrm{b},2)} + \max\{\Omega_{+}^{(2)}(\lambda), \Omega_{-}^{(2)}(\lambda)\} \right]. \qquad (5)$$

Here, $\Omega_{+}^{(2)}(\lambda)$ is given by $x/4$, where x is the maximum solution of the following equality for x,

$$x^3+(6\lambda-10)x^2+(32-40\lambda+9\lambda^2)x-32+64\lambda-32\lambda^2+2\lambda^3 = 0.$$

Also, $\Omega_{-}^{(2)}(\lambda)$ is the largest eigenvalue of the operator

$$\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}:\boldsymbol{a}=010\ldots0} - \lambda\hat{\Pi}, \qquad (6)$$

where $\hat{\Pi}$ and $\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}}$ are respectilvely given by $\hat{\Pi} = \sum_{j=1}^{L-1} \hat{P}\Big(\frac{\sqrt{\kappa_j}|j\rangle_B - \sqrt{\kappa_{j+1}}|j+1\rangle_B}{\sqrt{2}}\Big)$ with $\kappa_1 = \kappa_L = 1$ and $\kappa_i = 1/2$ (for $2 \le i \le L-1$) and $\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} = \delta_{a_2,1}\hat{P}(|1\rangle_B)$ $+ \sum_{i=2}^{L-1} \frac{\delta_{a_{i-1},1}+\delta_{a_{i+1},1}}{2}\hat{P}(|i\rangle_B) + \delta_{a_{L-1},1}\hat{P}(|L\rangle_B)$.

We note that in the previous analysis [7], tedious numerical calculations are needed to derive $\Omega_{\pm}^{(2)}(\lambda)$, however, we provide closed formulas of $\Omega_{\pm}^{(2)}(\lambda)$, which is an advantage of our analysis.

Simulation results.— Here, we show the simulation results of the key generation rates of the DPS protocol based on our analysis and the previous analysis in [7]. For both cases, we suppose that the total detection probability is assumed to be $Q = (L-1)\eta\alpha^2 e^{-(L+1)\eta\alpha^2}$, where we assume that the transmittance of the channel including the detection probability is given by $\eta = 0.1 \times 10^{-0.2l/10}$, and for simplicity we adopt $f_{\mathrm{EC}}(e^{(\mathrm{b})}) = h(e^{(\mathrm{b})})$. In Fig. 1, we show the key rates for the case of $e^{(\mathrm{b})} = 2\%$ and $L = 10$ by optimizing the mean photon number α^2. As a result, we find that the secure key rate of the DPS protocol based on our analysis is 1.22 times as high as the previous one.

Conclusions.— We have proven the information-theoretic security proof for the DPS QKD protocol based on the complementarity approach. As a result, we found that our security proof provides a slightly better key generation rate compared to the previous security proof based on the Shor-Preskill approach [7]. This improvement is obtained since the complementarity approach can incorporate more detailed information on Alice's sending state to estimate the leaked information to Eve. Thanks to this additional information we have obtained tighter upper bounds on the leaked information to Eve compared to those in the previous proof [7]. Moreover, we have removed the necessity of the numerical calculation, which was needed in [7] to derive the leaked information on the two-photon emission events. This leads to an advantage that our security proof enables us to evaluate the security of the DPS protocol with any block size L of $L \ge 3$.

G. K. and K. T. acknowledge support from CREST, JST. Y. T. acknowledges the support from the Program for Leading Graduate Schools: Interactive Materials Science Cadet Program. T. S. acknowledges the support from the ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Gov- ernment of Japan)

[1] A. K. Ekert. *Phys. Rev. Lett.*, 67:661-663, 1991.
[2] C. H. Bennett. *Phys. Rev. Lett.*, 68:3121-3124,1992.
[3] K. Inoue, *et al. Phys. Rev. A*, 68:022317, 2003.
[4] F. Grosshans, *et al. Phys. Rev. Lett.*, 88:057902, 2002.
[5] M. Sasaki *et al. Opt. Express*, 19(11):10387-10409, 2011.
[6] K. Wen, *et al Phys. Rev. Lett.*, 103:170503, 2009.
[7] K. Tamaki, *et al* arXiv:1208.1995v1, 2012.
[8] P. W. Shor, *et al. Phys. Rev. Lett.*, 85:441-444, 2000.
[9] M. Koashi. arXiv:0704.3661, 2007.
[10] D. Gottesman *et al. Quant. Inf. Comput.*, 4:325-360, 2004.
[11] M Koashi. *New Journal of Physics*, 11(4):045018, 2009.

[Full version of the extended abstract] Information-theoretic security proof of differential-phase-shift quantum key distribution protocol based on complementarity

Akihiro Mizutani*,[1] Toshihiko Sasaki,[2] Go Kato,[3] Yuki Takeuchi,[1] and Kiyoshi Tamaki[4]

[1] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2] *Photon Science Center, Graduate School of Engineering,*
The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan
[3] *NTT Communication Science Laboratories, NTT Corporation, 3-1,*
Morinosato Wakamiya Atsugi-Shi, Kanagawa, 243-0198, Japan
[4] *Department of Intellectual Information Engineering, Faculty of Engineering,*
University of Toyama, Gofuku 3190, Toyama 930-8555, Japan

We show the information-theoretic security proof of the differential-phase-shift (DPS) quantum key distribution (QKD) protocol based on the complementarity approach [arXiv:0704.3661 (2007)]. Our security proof provides a slightly better key generation rate compared to the one derived in the previous security proof in [arXiv:1208.1995 (2012)] that is based on the Shor-Preskill approach [Phys. Rev. Lett. **85**, 441 (2000)]. This improvement is obtained because the complementarity approach can employ more detailed information on Alice's sending state in estimating the leaked information to an eavesdropper. Moreover, we remove the necessity of the numerical calculation that was needed in the previous analysis to estimate the leaked information. This leads to an advantage that our security proof enables us to evaluate the security of the DPS protocol with any block size. This paper highlights one of the fundamental differences between the Shor-Preskill and the complementarity approaches.

I. INTRODUCTION

Quantum key distribution (QKD) holds promise to achieve information-theoretically secure communication between two distant parties (Alice and Bob) against any eavesdropper (Eve). Since the first invention of the BB84 protocol [1], many QKD protocols have been proposed so far [2–9]. Among them, the differential-phase-shift (DPS) QKD protocol [8] has been considered as one of the promising protocols for future implementation since this protocol can be rather simply implemented with a passive detection unit. Recently, a field demonstration of the DPS protocol [10] has already been conducted, and the information-theoretical security proofs of the DPS protocol have been established when Alice employs a single-photon source [11] and a block-wise phase-randomized coherent light source [12].

The previous security proof [12] with coherent light source is based on the *Shor-Preskill approach* [13] in which Alice and Bob virtually extract a maximally-entangled state (MES) to show that they share a monogamy correlation. In order to extract an MES, Alice and Bob use some estimated information about the correlation between them. Specifically, this information consists of the bit and phase error rates, where the phase error is defined by fictitious erroneous outcomes when Alice and Bob would have measured their virtual qubits in a basis conjugate to the basis for generating the key. Since the phase error rate cannot be directly obtained in the experiment, the estimation of this quantity is a central issue in the security proof, and some security proofs have been conducted along this approach [11, 14–18].

Another approach for the security proof is the complementarity approach [19]. In this approach, a complementary control of the actual protocol and a virtual protocol are considered, which Alice and Bob choose to execute, but cannot execute simultaneously. The goal of the actual protocol is to agree on the bit values along the key generation basis, say the X basis, while in the virtual protocol, Alice and Bob collaborate to create an eigenstate of the Z basis (a complementary basis to the X basis) in Alice's side. With these protocols, Koashi proved in [19] that the necessary and sufficient condition for the secure key distillation is to be able to execute whichever task was chosen. On one hand, once an MES is shared between Alice and Bob, they also accomplish the complementary task, which implies that the Shor-Preskill approach is included in the complementarity one. On the other hand, the purpose of the complementarity approach is to create an eigenstate of the Z basis at Alice's side, and therefore, we can employ some additional information, such as the one on Alice's sending state, which may provide an advantage over the Shor-Preskill approach.

In this paper, we show that these two approaches indeed give a different resulting secret key rate of the DPS QKD protocol by exploiting a property of pulses emitted by Alice. More specifically, we adopt the complementarity approach for the security proof where we accommodate the intuition that it is difficult to extract information from a train of weak coherent pulses employed in the DPS protocol. As a result, we show that the secure key rate based on the complementarity approach is 1.22 times

*mizutani@qi.mp.es.osaka-u.ac.jp

as high as the one based on the Shor-Preskill approach when the bit error rate is 2%. Moreover, we remove the necessity of the numerical calculation that was needed to evaluate the leaked information to Eve in the previous analysis [12], and we provide the closed formulas for the upper bounds on the leaked information. This leads to an advantage that our security proof enables us to evaluate the security of the DPS protocol with any block size.

This paper is organized as follows. In Sec. II, we introduce the DPS protocol including the assumptions on Alice and Bob's devices. In Sec. III, we explain our security proof based on the complementarity approach. In our security proof, we estimate the leaked information for each photon number emission separately, and in Sec. IV, we show the resulting upper bounds on the estimated leaked information up to the two-photon emission events. In Sec. V, we compare the resulting secret key rates based on the Shor-Preskill and the complementarity approaches, and finally, we conclude our paper in Sec. VI.

II. DPS QKD

We first describe the setup of the DPS protocol (see Fig. 1), and list up the assumptions we make on Alice and Bob's devices. Note that the setup and the assumptions are exactly the same as those in [12].

A. Setup and assumptions

Alice uses a laser source emitting coherent pulses and a phase modulator, and a train of L ($L \geq 3$) pulses forms a block. Bob uses a one-bit delay interferometer with two 50:50 beam splitters and with its delay being equal to the interval of the neighboring sending pulses. After the interferometer, the pulses are detected by two photon detectors corresponding to bit values of 0 and 1. The j^{th} ($1 \leq j \leq L-1$) time slot is defined as an expected detection time at Bob's detectors from the superposition of the j^{th} and $(j+1)^{\text{th}}$ incoming pulses. Also, the 0^{th} (L^{th}) time slot is defined as an expected detection time at Bob's detectors from the superposition of the 1^{st} (L^{th}) incoming pulse and the L^{th} incoming pulse in the previous block (1^{st} incoming pulse in the next block).

As for the assumptions on Alice's device, we assume that (A 1) the phase modulator randomly modulates each relative phase between adjacent sending pulses by 0 or π. Moreover, (A 2) the randomization of overall optical phase δ is done for each block of L pulses. This means that the quantum state of the L pulses is written as a classical mixture of the total photon number contained in the L pulses. Besides, (A 3) we do not consider any side-channel in Alice's site.

Regarding with the assumptions on Bob's device, we suppose that (B 1) Bob uses two photon-number-resolving (PNR) detectors, which can discriminate among the vacuum, a single-photon and multiphoton. Also, we assume that (B 2) the detection efficiency is the same for both detectors. Finally, (B 3) we do not consider any side-channel in Bob's site.

B. Actual protocol

The actual protocol proceeds as follows. In its description, $|\boldsymbol{\kappa}|$ denotes the length of a bit string $\boldsymbol{\kappa}$.

(a 1) Alice generates a random L-bit sequence $s_1 s_2 ... s_L$ and a random common phase shift $\delta \in [0, 2\pi)$. For a random L-bit sequence $s_1 s_2 ... s_L$, she sends the following coherent state (system $\mathcal{H}_S$) to Bob through a quantum channel

$$\bigotimes_{i=1}^{L} |e^{\mathrm{i}\delta}(-1)^{s_i}\alpha\rangle_{S,i}, \tag{1}$$

where $|\alpha\rangle_{S,i}$ represents the coherent state $\sum_n e^{-|\alpha|^2/2}\alpha^n |n\rangle_{S,i}/\sqrt{n!}$ of the i^{th} pulse mode.

(a 2) Bob performs the interference measurement with two PNR detectors, and we call the *successful detection* event if Bob detects one-photon in the j^{th} time slot (with $1 \leq j \leq L-1$), and detects the vacuum in all the other time slots including the 0^{th} and L^{th} time slots. If the successful detection occurs, the variable j is set to the time slot, otherwise Bob sets $j = 0$. If $j \neq 0$, he obtains his raw bit $s \in \{0, 1\}$ depending on which detector has reported a detection at the j^{th} time slot. Bob announces j over an authenticated public channel.

(a 3) If $j \neq 0$, Alice calculates her raw key bit as $s_j \oplus s_{j+1} \in \{0, 1\}$.

(a 4) Alice and Bob repeat steps (a 1)-(a 3) N times.

(a 5) Alice defines a sifted key $\boldsymbol{\kappa}_A$ by concatenating the successful detection events (*i.e.,* $j \neq 0$).

(a 6) Bob defines a sifted key $\boldsymbol{\kappa}_B$ by concatenating the successful detection events (*i.e.,* $j \neq 0$).

(a 7) Bob corrects the errors in his sifted key $\boldsymbol{\kappa}_B$ to make it coincide with $\boldsymbol{\kappa}_A$ by sacrificing $|\boldsymbol{\kappa}_A| f_{\text{EC}}$ bits of encrypted public communication from Alice by consuming the same length of the pre-shared secret key.

(a 8) Alice and Bob conduct privacy amplification by shortening their keys by $|\boldsymbol{\kappa}_A| f_{\text{PA}}$ to obtain the final keys.

In this paper, we consider the asymptotic limit of the sifted key length ($N \to \infty$). In the experiments, the following parameters are observed:

$$Q := \frac{|\boldsymbol{\kappa}_A|}{N}, \quad e^{(\text{b})} := \frac{\text{wt}(\boldsymbol{\kappa}_A - \boldsymbol{\kappa}_B)}{|\boldsymbol{\kappa}_A|}, \tag{2}$$

where the minus sign is a bit-by-bit modulo-2 subtraction and $\text{wt}(\boldsymbol{\kappa})$ denotes the weight (the number of 1's) in a bit string $\boldsymbol{\kappa}$. In the asymptotic limit, f_{EC} is given by a

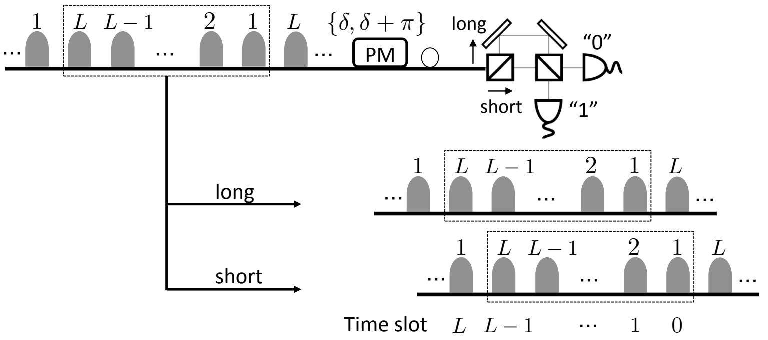

FIG. 1: Setup of the actual protocol. At Alice's site, pulse trains are generated by a laser source followed by the phase modulator (PM) that randomly modulates a phase δ or $\delta+\pi$ with δ being randomly chosen from $[0, 2\pi)$ for each block of L pulses. At Bob's site, each pulse train is fed to a one-bit delay Mach-Zehnder interferometer with two 50:50 beam splitters. The pulse trains leaving the interferometer are measured by two photon-number-resolving (PNR) detectors corresponding to bit values "0" and "1". A successful detection event occurs if Bob detects a single-photon in the only one time slot j (with $1 \le j \le L-1$), and detects the vacuum in all the other time slots including the $0^{\rm th}$ and $L^{\rm th}$ time slots.

function of the bit error rate $e^{(\rm b)}$. The asymptotic key generation rate per sending pulse is given by [20, 21]

$$G = [Q(1 - f_{\rm EC}(e^{(\rm b)}) - f_{\rm PA})]/L. \tag{3}$$

In this key generation formula, we omit for simplicity the random sampling procedure to estimate the bit error rate $e^{(\rm b)}$ because its cost is negligible in the asymptotic limit.

In step (a 2), when the successful detection event ($j \neq 0$) occurs, the state of the incoming L pulses is expressed by the Hilbert space $\mathcal{H}_B$ spanned by L states, and we denote its orthonormal basis by $\{|i\rangle_B\}_{i=1}^{L}$, with i representing the position of the single-photon before the first beam splitter. Determination of the detected time slot j and the bit value $s \in \{0, 1\}$ is represented by a generalized measurement on the system $\mathcal{H}_B$. Let $\hat{\Pi}_{j,s}$ be the POVM elements for the bit value s detected at the $j^{\rm th}$ time slot (with $1 \le j \le L-1$). Considering the action of the beam splitters, they are written as

$$\hat{\Pi}_{j,s} = \hat{P}\Big(\frac{\sqrt{\kappa_j}|j\rangle_B + (-1)^s\sqrt{\kappa_{j+1}}|j+1\rangle_B}{\sqrt{2}}\Big) \tag{4}$$

with $\kappa_1 = \kappa_L = 1$ and $\kappa_i = 1/2$ (for $2 \le i \le L-1$). Here we define $\hat{P}(|\cdot\rangle) = |\cdot\rangle\langle\cdot|$. For later discussions, we decompose $\hat{\Pi}_{j,s}$ into two consecutive measurements. The first one is a filter operation $\hat{F}_j : \mathcal{H}_B \to \mathcal{H}_{B_{\rm q}}$ with $1 \le j \le L-1$, which gives the outcome j and leaves a qubit system $\mathcal{H}_{B_{\rm q}}$. The second one measures the qubit in the Z basis $\{|0\rangle_{B_{\rm q}}, |1\rangle_{B_{\rm q}}\}$. By using the filter operation and the qubit measurement, $\hat{\Pi}_{j,s}$ can be decomposed as

$$\hat{\Pi}_{j,s} = \hat{F}_j^\dagger \hat{P}(|s\rangle_{B_{\rm q}})\hat{F}_j \tag{5}$$

if we choose $\hat{F}_j$ as

$$\hat{F}_j = \sqrt{\kappa_j}|-\rangle_{B_{\rm q}}{}_B\langle j| + \sqrt{\kappa_{j+1}}|+\rangle_{B_{\rm q}}{}_B\langle j+1|. \tag{6}$$

Here, we define the X basis state as $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

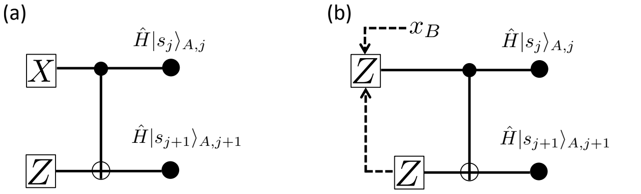
(a)
X
Z
$\hat{H}|s_j\rangle_{A,j}$
$\hat{H}|s_{j+1}\rangle_{A,j+1}$
(b)
x_B
Z
Z
$\hat{H}|s_j\rangle_{A,j}$
$\hat{H}|s_{j+1}\rangle_{A,j+1}$

FIG. 2: (a) Alice's operation in the alternative protocol. She inputs the $j^{\rm th}$ and $(j+1)^{\rm th}$ qubits to the C-NOT gate with the $j^{\rm th}$ one being the control and the $(j+1)^{\rm th}$ one being the target. After that, the $(j+1)^{\rm th}$ qubit is measured in the Z basis, and the $j^{\rm th}$ qubit is measured in the X basis. (b) Alice's procedure to estimate the outcome $z_j \in \{0, 1\}$ of the complementarity observable, that is, the Z basis measurement on the $j^{\rm th}$ qubit. After she performs the C-NOT gate, she measures her $(j+1)^{\rm th}$ qubit in the Z basis. If $z_{j+1} = 0$ (1), she uses this information (this information and $x_B \in \{+, -\}$ in step (al 3*)), and she predicts the outcome z_j.

III. SECURITY PROOF

In this section, we prove the security of the protocol described in Sec. II B, and determine the amount of privacy amplification $f_{\rm PA}$ in the asymptotic limit.

A. Alternative protocol

To explain our security proof, we introduce an alternative protocol equivalent to the actual one, which is designated to fulfill the following conditions.

(i) The state of the optical pulses emitted by Alice and the data processing for generating the final key are identical to the ones of the actual protocol.

(ii) Bob's measurement on receiving the L pulses and his announcement of j over an authenticated public channel are identical to the actual protocol.

These two conditions ensure that Eve cannot change her attack depending on which of the actual and the alternative protocols is conducted, resulting in the identical correlation between the final key and Eve's quantum system. Hence, the final key in the actual protocol is secure in terms of the composable security [22] if the alternative protocol is secure against Eve's general attack.

As an alternative protocol, we consider an *entanglement-based* protocol in which Alice prepares L auxiliary qubits of system $\mathcal{H}_A$ located in Alice's site and L coherent pulses of system $\mathcal{H}_S$ in state

$$|\Phi\rangle_{C,A,S} = \sum_{\nu=0}^{\infty} |\nu\rangle_C \hat{\pi}_\nu \bigotimes_{i=1}^{L} |\phi\rangle_{A,S,i} \tag{7}$$

with

$$|\phi\rangle_{A,S,i} = \frac{1}{\sqrt{2}} \sum_{s_i=0}^{1} \hat{H} |s_i\rangle_{A,i} |(-1)^{s_i}\alpha\rangle_{S,i}. \tag{8}$$

Here, $\hat{\pi}_\nu$ denotes the projection of the L pulses onto the subspace where ν photons are contained in the L pulses, $\mathcal{H}_C$ is a system storing the information of the outcome of the projection, and also we define the Hadamard operation as $\hat{H} = 1/\sqrt{2}\sum_{x,y=0,1}(-1)^{xy}|x\rangle\langle y|$. To generate a raw key bit, Alice measures her auxiliary qubit in the X basis.

Now, we introduce an alternative entanglement-based protocol that satisfies the above conditions (i) and (ii). A controlled-NOT (C-NOT) gate $\hat{U}^{(j)}_{\mathrm{CNOT}}$ appearing in the protocol is defined on the Z basis $\{|0\rangle, |1\rangle\}$ by $\hat{U}^{(j)}_{\mathrm{CNOT}}|x\rangle_{A,j}|y\rangle_{A,j+1} = |x\rangle_{A,j}|x \oplus y\rangle_{A,j+1}$ (with $x, y \in \{0,1\}$).

The protocol proceeds as follows.

(al 1) Alice prepares the state $|\Phi\rangle_{C,A,S}$, measures the system $\mathcal{H}_C$ to learn the total photon number ν in the L pulses, and sends the L pulses to Bob through a quantum channel.

(al 2) Bob receives the L pulses and carries out the quantum nondemolition (QND) measurement to test if there is exactly one photon in total from the $j = 1^{\mathrm{th}}$ to $j = (L-1)^{\mathrm{th}}$ time slots and the vacuum in the $j = 0^{\mathrm{th}}$ and L^{th} time slots. If this test is passed, Bob performs the filter operation $\{\hat{F}_j\}_{j=1}^{L-1}$ in Eq. (6) to know in which time slot he detects a single-photon, and the variable j is set to the time slot. Otherwise Bob sets $j = 0$. Bob announces j over an authenticated public channel. If $j = 0$, Alice and Bob skip steps (al 3) and (al 4) below.

(al 3) Bob measures his qubit B_{q} in the Z basis $\{|0\rangle_{B_{\mathrm{q}}}, |1\rangle_{B_{\mathrm{q}}}\}$ and obtains his raw key bit s.

(al 4-1) Alice applies the C-NOT gate on the j^{th} qubit (control) and $(j+1)^{\mathrm{th}}$ qubit (target) [see Fig. 2 (a)].

(al 4-2) Alice measures the $(j+1)^{\mathrm{th}}$ qubit in the Z basis $\{|0\rangle_{A,j+1}, |1\rangle_{A,j+1}\}$ to obtain the outcome $z_{j+1} \in \{0,1\}$.

(al 4-3) Alice measures the j^{th} qubit in the X basis $\{|+\rangle_{A,j}, |-\rangle_{A,j}\}$ and determines a raw key bit.

(al 5) Alice and Bob repeat steps (al 1)-(al 4) N times.

(al 6)[=(a 5)] Alice defines a sifted key $\boldsymbol{\kappa}_A$ by concatenating the successful detection events (*i.e.*, $j \neq 0$).

(al 7)[=(a 6)] Bob defines a sifted key $\boldsymbol{\kappa}_B$ by concatenating the successful detection events (*i.e.*, $j \neq 0$).

(al 8)[=(a 7)] Bob corrects the errors in his sifted key $\boldsymbol{\kappa}_B$ to make it coincide with $\boldsymbol{\kappa}_A$ by sacrificing $|\boldsymbol{\kappa}_A| f_{\mathrm{EC}}$ bits of encrypted public communication from Alice by consuming the same length of the pre-shared secret key.

This alternative protocol satisfies the above conditions (i) and (ii) because of the following reasons. First, as for (i), we show that Alice's procedure dictated in (i) is the same between both actual and alternative protocols by modifying Alice's procedure in the alternative protocol. For this, since the outcome z_{j+1} obtained in step (al 4-2) is neither announced nor used in determining the final key, we can omit this step. Next, steps (al 4-1) and (al 4-3) are equivalently done by measuring all the L qubits in the X basis to obtain an L-bit sequence $s_1 s_2 ... s_L$ as the outcome, and then setting $s_j \oplus s_{j+1}$. Since the X-basis measurement on all the qubits does not require the knowledge of j announced in step (al 2), we can consider that it is done in step (al 1). Then, using the relation

$$_{A,j}\langle \pm | \phi \rangle_{A,S,j} = \frac{1}{\sqrt{2}} |\pm\alpha\rangle_{S,j}, \tag{9}$$

we see that the random L-bit sequence $s_1 s_2 ... s_L$ is obtained, and we thus conclude that Alice's sending state is equivalent to Eq. (1). Note that the total photon number measurement to obtain ν in step (al 1) makes the pulse train diagonalized in the Fock basis, and with this measurement, the assumption (A 2) introduced in Sec. II A is satisfied. Hence, the state of the optical pulses emitted by Alice and the data processing for generating the final key are identical to the ones of the actual protocol.

Next, we see that the alternative protocol satisfies the condition (ii). In step (al 2), the QND measurement over the $j = 0^{\mathrm{th}}$ to $j = L^{\mathrm{th}}$ time slots informs Bob if the successful detection occurs or not (namely, $j = 0$ or $j \neq 0$). The probability of resulting $j \neq 0$ is the same as the one in the actual protocol. Moreover, if $j \neq 0$, the probability of announcing j (with $1 \leq j \leq L-1$) is the same between both protocols since the following equation is satisfied from Eq. (5),

$$\sum_{s=0}^{1} \hat{\Pi}_{j,s} = \hat{F}_j^{\dagger} \hat{F}_j. \tag{10}$$

Hence, the information of j announced by Bob in the alternative protocol is equivalent to the actual protocol.

Therefore, the alternative protocol satisfies the conditions (i) and (ii), which means that the security of the alternative protocol guarantees the security of the actual protocol.

B. Complementarity task

The next step is to determine the amount of privacy amplification $f_{\rm PA}$, where we employ the argument of complementarity [19]. In this approach, we consider a *virtual measurement* that is complementary to the one to determine the sifted key $\boldsymbol{\kappa}_A$. Recall that the measurement to obtain the sifted key is performed in step (al 4-3), and the complementarity measurement means that the measurement basis (X basis) in step (al 4-3) is replaced with the complementarity basis (here we consider the Z basis). In other words, the virtual measurement is described as the following step (al 4-3*).

(al 4-3*) Alice measures the $j^{\rm th}$ qubit in the Z basis $\{|0\rangle_{A,j}, |1\rangle_{A,j}\}$ and determines the outcome $z_j \in \{0,1\}$.

While Bob, instead of aiming at learning $\boldsymbol{\kappa}_A$, tries to guess the value of the complementary observable z_j. This suggests that step (al 3) is replaced with the following step (al 3*).

(al 3*) Bob measures his qubit $B_{\rm q}$ in the X basis $\{|+\rangle_{B_{\rm q}}, |-\rangle_{B_{\rm q}}\}$ and obtains its outcome $x_B \in \{+,-\}$.

In the complementarity argument [19], we need to quantify how well Alice successfully predicts the outcome z_j of the measurement defined in step (al 4-3*) with a help of Bob through quantum communication (see Fig. 2 (b) for Alice's procedure to estimate z_j). For the quantification, we employ the phase error rate. Here, the phase error rate $e^{(\rm ph)}$ is defined as the probability that Alice fails her prediction on z_j, where the phase error rate is related to the amount of privacy amplification $Qf_{\rm PA}$ [21].

To accomplish the prediction on z_j, Alice employs three information that could help her prediction, which are listed below.

- (I-1) x_B obtained in step (al 3*).
- (I-2) $z_{j+1} \in \{0,1\}$ obtained in step (al 4-2).
- (I-3) The intensity of Alice's sending state is weak.

The information (I-1) informs Alice of which of the $j^{\rm th}$ or $(j+1)^{\rm th}$ original pulse contains a single-photon, which corresponds to $x_B = -$ or $x_B = +$, respectively. The failure probability for this prediction, which we call the phase error rate, is related to the amount of privacy amplification (see Eq. (20) for the explicit formula).

As an introduction, we first consider the simplest case where Eve is absent in the quantum channel (we call this case the normal operation). In this case, if Bob successfully detects a single-photon at the $j^{\rm th}$ time slot, and depending on his X basis measurement outcome $x_B = +$ or $x_B = -$ from the information (I-1), the state of the $j^{\rm th}$ and $(j+1)^{\rm th}$ Alice's systems is written as

$$|\psi_+\rangle_{A,j,j+1} := |0\rangle_{A,j}|1\rangle_{A,j+1} \tag{11}$$

and

$$|\psi_-\rangle_{A,j,j+1} := |1\rangle_{A,j}|0\rangle_{A,j+1}, \tag{12}$$

respectively. After Alice performs the C-NOT gate in step (al 4-1), $|\psi_+\rangle_{A,j,j+1}$ and $|\psi_-\rangle_{A,j,j+1}$ are transformed to

$$\hat{U}^{(j)}_{\rm CNOT}|\psi_+\rangle_{A,j,j+1} = |0\rangle_{A,j}|1\rangle_{A,j+1} \tag{13}$$

and

$$\hat{U}^{(j)}_{\rm CNOT}|\psi_-\rangle_{A,j,j+1} = |1\rangle_{A,j}|1\rangle_{A,j+1}, \tag{14}$$

respectively. In this case, z_{j+1} obtained in step (al 4-2) is always 1, and Alice can predict z_j as 0 or 1 without causing any error depending on Bob's outcome $x_B = +$ or $-$, respectively.

Moreover, by following the same arguments above, if the quantum channel is a linear lossy channel $\mathcal{N}_\eta$: $\mathcal{N}_\eta|\alpha\rangle = |\eta\alpha\rangle$, $z_{j+1} = 0$ never occurs, and for $z_{j+1} = 1$, Alice can also perfectly predict the outcome z_j. Summarizing two examples of the normal operation and the linear lossy channel case, if $z_{j+1} = 1$ as (I-2), the following Alice's prediction succeeds with unit probability,

$$\text{if } z_{j+1} = 1 \to z_j = \begin{cases} 0 \text{ if } x_B = + \\ 1 \text{ if } x_B = -. \end{cases} \tag{15}$$

Therefore, in general case (without assuming any channel model), if $z_{j+1} = 1$, we suppose that Alice takes the above strategy on her prediction.

As we discussed above, the successful detection events never occur with $z_{j+1} = 0$ in the normal operation and the linear lossy channel case. Hence, if the successful detection occurs with $z_{j+1} = 0$, we consider that Alice always predicts z_j as 0 because before Alice sends the system $\mathcal{H}_S$ to Bob, $z_j = 0$ is more likely to occur. This tendency is rather remarkable as the intensity of the sending state becomes weaker. Mathematically, this is confirmed as

$$\begin{aligned} &||{}_{A,j}\langle z_j|_{A,j+1}\langle 0|\hat{U}^{(j)}_{\rm CNOT} \bigotimes_{k=j,j+1} |\phi\rangle_{A,S,k}||^2 \\ &\propto \frac{1+\langle-\alpha|\alpha\rangle\left[\langle-\alpha|\alpha\rangle + (-1)^{z_j}2\right]}{2(1+\langle-\alpha|\alpha\rangle^2)} =: p(\alpha, z_j) \end{aligned} \tag{16}$$

and $p(\alpha,0)/p(\alpha,1) = (\coth\alpha^2)^2 \geq 1$. Here, $||\cdot||$ denotes the trace norm.

From this consideration and (I-3), in any channel model, we suppose that Alice takes the following strategy as

$$\text{if } z_{j+1} = 0 \to z_j = 0. \tag{17}$$

It is notable that if $z_{j+1} = 0$, Alice does not use Bob's information x_B [namely, (I-1)] to estimate the outcome z_j, and her prediction is wrong when $z_j = 1$.

This prediction strategy highlights the difference between the complementarity approach and Shor-Preskill approach. Recall that in the Shor-Preskill approach [12], the goal of Alice and Bob in an alternative protocol is to generate the maximally entangled state (MES) of the two qubit systems $\mathcal{H}_{A,j}$ and $\mathcal{H}_{B_{\mathrm{q}}}$. To generate the MES, the bit and phase error rates are needed, where the phase errors are defined as the instances where Alice's Z basis measurement outcome in step (al 4-3*) and Bob's X basis measurement outcome in step (al 3) are different. Hence, the phase error is defined as the relation between z_j and x_B, which means that it cannot be defined as an instance only by focusing on Alice's specific measurement outcome, such as $z_j = 1$. In fact, if we translate the construction of the phase error POVM in [12] to the complementarity argument, Alice's prediction for $z_{j+1} = 0$ in [12] can be interpreted as follows:

$$\text{if } z_{j+1} = 0 \to z_j = \begin{cases} 0 \text{ with probability } 1/2 \\ 1 \text{ with probability } 1/2. \end{cases} \tag{18}$$

This means that if $z_{j+1} = 0$, Alice randomly selects z_j, which implies that the knowledge on Alice's sending states [namely, (I-3)] is not used.

Therefore, the prediction in Eq. (17) that uses a property of Alice's sending state highlights one of the unique features in the complementarity approach, and this difference of the prediction leads to a tighter upper bound on the phase error rate, which we show in Sec. IV. Specifically, this difference will be reflected by all the differences in two curves in Figs. 3, 4 and 5.

Our goal is to obtain the amount of Qf_{PA} in Eq. (3). For this, recall that the photon number measurement is conducted on the L pulses in step (al 1), and therefore, Qf_{PA} in Eq. (3) can be expressed as a classical mixture of Fock state, that is,

$$Qf_{\mathrm{PA}} = \sum_{\nu=0}^{\infty} Q^{(\nu)} f_{\mathrm{PA}}^{(\nu)}. \tag{19}$$

Here, $Q^{(\nu)}$ is defined as $Q^{(\nu)} = \frac{|\boldsymbol{\kappa}_A^{(\nu)}|}{N}$ with $\boldsymbol{\kappa}_A^{(\nu)}$ denoting the sifted key originating from the ν-photon emission events, and $f_{\mathrm{PA}}^{(\nu)}$ is the amount of privacy amplification for $\boldsymbol{\kappa}_A^{(\nu)}$. From [20, 21], in the asymptotic limit, the amount of privacy amplification for $\boldsymbol{\kappa}_A^{(\nu)}$ is given by

$$f_{\mathrm{PA}}^{(\nu)} = h(e^{(\mathrm{ph},\nu)}), \tag{20}$$

where $h(x) := -x\log_2 x - (1-x)\log_2(1-x)$ represents the binary entropy function, and $e^{(\mathrm{ph},\nu)}$ is a phase error rate for the ν-photon emission events.

Having finished the explanation of the prediction on z_j, next we give an overview of the proof conducted in the following sections (from Sec. III C to Sec. IV C). The goal of our discussion is to obtain the upper bound on the amount of privacy amplification $f_{\mathrm{PA}}^{(\nu)} = h(e^{(\mathrm{ph},\nu)})$ in Eq. (20) with the bit error rate $e^{(\mathrm{b},\nu)}$. To achieve this goal, in Sec. III C, we first formulate the POVM elements for the bit and phase error events. In Sec. III D, to discuss the security for each photon number emission event separately, we introduce the projection operator $\hat{P}^{(\nu)}$ representing that the state of L pulses is contained in the ν-photon subspace. In Sec. III E, we relate $e^{(\mathrm{ph},\nu)}$ and $e^{(\mathrm{b},\nu)}$, and we show that it suffices to calculate the quantity $\Omega^{(\nu)}(\lambda)$ in Eq. (37) to upper-bound the phase error rate $e^{(\mathrm{ph},\nu)}$. Then, in Sec. IV, we explicitly derive the quantity $\Omega^{(\nu)}(\lambda)$ for $\nu = 0, 1, 2$, and obtain the upper bound on $e^{(\mathrm{ph},\nu)}$ with the bit error rate $e^{(\mathrm{b},\nu)}$ and $\Omega^{(\nu)}(\lambda)$.

C. Bit and phase error POVMs

In this subsection, we construct the POVMs for the phase and bit errors. The POVM elements for the phase error when the successful detection occurs at the j^{th} (with $1 \le j \le L-1$) time slot, which act on the systems $\mathcal{H}_{A,j}$, $\mathcal{H}_{A,j+1}$ (just before the C-NOT gate in Fig. 2) and $\mathcal{H}_B$, are given by

$$\begin{aligned}\hat{e}_j^{(\mathrm{ph})} =& \hat{P}(|1\rangle_{A,j}|1\rangle_{A,j+1}) \otimes \sum_{s=0}^{1} \kappa_{j+s}\hat{P}(|j+s\rangle_B) \\ &+ \sum_{s=0}^{1} \hat{P}(|s\rangle_{A,j}|\bar{s}\rangle_{A,j+1}) \otimes \kappa_{j+s}\hat{P}(|j+s\rangle_B), \end{aligned} \tag{21}$$

where we define $\bar{s} = s \oplus 1$. Here, the first and second terms correspond to the failure prediction on z_j for $z_{j+1} = 1$ [whose prediction strategy is given in Eq. (15)] and $z_{j+1} = 0$ [whose prediction strategy is given in Eq. (17)], respectively. Next, we construct the POVM element for the bit error. A bit error is the instance where Alice's X basis measurement on her j^{th} auxiliary qubit in step (al 4-3) and the outcome of Bob's interference measurement defined in Eq. (4) are different. From this definition, the POVM elements for the bit error for the j^{th} time slot, which act on the systems $\mathcal{H}_{A,j}$, $\mathcal{H}_{A,j+1}$ and $\mathcal{H}_B$, are given by

$$\hat{e}_j^{(\mathrm{b})} = \sum_{s,s'} \hat{P}(\hat{H}|s\rangle_{A,j})\hat{P}(\hat{H}|s'\rangle_{A,j+1})\hat{\Pi}_{j,s\oplus s'\oplus 1}. \tag{22}$$

For simplicity of analysis, we introduce the unitary operator $\hat{U}$ defined by

$$\hat{U}\bigotimes_{i'=1}^{L}(\hat{H}|s_{i'}\rangle_{A,i'})|i\rangle_B = (-1)^{s_i}\bigotimes_{i'=1}^{L}(\hat{H}|s_{i'}\rangle_{A,i'})|i\rangle_B \tag{23}$$

for $1 \le i \le L$. By applying $\hat{U}$ to $\hat{e}_j^{(\mathrm{ph})}$ in Eq. (21), we obtain the following equation (see Appendix A for the derivation)

$$\hat{U}\hat{e}_j^{(\mathrm{ph})}\hat{U}^\dagger = \sum_{\boldsymbol{a}} \hat{P}(|\boldsymbol{a}\rangle_A)\otimes$$
$$\Big[\kappa_j\delta_{a_{j+1},1}\hat{P}(|j\rangle_B) + \kappa_{j+1}\delta_{a_j,1}\hat{P}(|j+1\rangle_B)\Big], \qquad (24)$$

where we denote Alice's Z basis states as $|\boldsymbol{a}\rangle_A := |a_1\rangle_{A,1}|a_2\rangle_{A,2}...|a_L\rangle_{A,L}$ with $\boldsymbol{a} := a_1a_2...a_L$ ($a_i \in \{0,1\}$). Also, by applying unitary $\hat{U}$ to Eq. (22), we have [12]

$$\hat{U}\hat{e}_j^{(\mathrm{b})}\hat{U}^\dagger = \hat{\Pi}_{j,1}. \qquad (25)$$

Then, by taking a sum over all the time slots, we obtain the operators for the phase and bit errors as

$$\hat{e}^{(\mathrm{ph})} = \sum_{j=1}^{L-1}\hat{e}_j^{(\mathrm{ph})}, \quad \hat{e}^{(\mathrm{b})} = \sum_{j=1}^{L-1}\hat{e}_j^{(\mathrm{b})}. \qquad (26)$$

When the state of Alice and Bob's quantum systems $\mathcal{H}_A$ and $\mathcal{H}_B$ just after the successful QND measurement ($j \neq 0$) at step (al 2) is $\hat{\rho}_{AB}$, the probability of having a bit error in the extracted qubit pair of systems $\mathcal{H}_{A_j}$ and $\mathcal{H}_{B_\mathrm{q}}$ is given by $\mathrm{tr}(\hat{\rho}_{AB}\hat{e}^{(\mathrm{b})})$, and the probability of having a phase error is given by $\mathrm{tr}(\hat{\rho}_{AB}\hat{e}^{(\mathrm{ph})})$.

By appling $\hat{U}$ to $\hat{e}^{(\mathrm{ph})}$ and $\hat{e}^{(\mathrm{b})}$, these error operators are concisely written as follows.

$$\hat{U}\hat{e}^{(\mathrm{ph})}\hat{U}^\dagger = \sum_{\boldsymbol{a}}\hat{P}(|\boldsymbol{a}\rangle_A)\otimes\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})}, \qquad (27)$$

where we define $\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})}$ as

$$\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} = \delta_{a_2,1}\hat{P}(|1\rangle_B) + \sum_{i=2}^{L-1}\frac{\delta_{a_{i-1},1}+\delta_{a_{i+1},1}}{2}\hat{P}(|i\rangle_B)$$
$$+ \delta_{a_{L-1},1}\hat{P}(|L\rangle_B), \qquad (28)$$

and

$$\hat{U}\hat{e}^{(\mathrm{b})}\hat{U}^\dagger = \hat{I}_A\otimes\hat{\Pi} \qquad (29)$$

with

$$\hat{\Pi} = \sum_{j=1}^{L-1}\hat{\Pi}_{j,1}. \qquad (30)$$

Here, $\hat{\Pi}$ is a tridiagonal symmetric matrix, and the matrix elements are given by

$$\begin{aligned}
{}_B\langle i|\hat{\Pi}|i\rangle_B &= 1/2 && (\text{for } 1 \le i \le L),\\
{}_B\langle i|\hat{\Pi}|i+1\rangle_B &= -1/(2\sqrt{2}) && (\text{for } i = 1, L-1),\\
{}_B\langle i|\hat{\Pi}|i+1\rangle_B &= -1/4 && (\text{for } 2 \le i \le L-2). \qquad (31)
\end{aligned}$$

D. Constraints on Alice's auxiliary qubit system $\mathcal{H}_A$

Here, we constrain Alice's auxiliary qubit system $\mathcal{H}_A$ by using the knowledge of the total photon number ν contained in the L pulses. For this, we first rewrite Eq. (7) as

$$|\Phi\rangle = 2^{-L}\sum_{\boldsymbol{a}}|\boldsymbol{a}\rangle_A\sum_{\nu}|\nu\rangle_C\hat{\pi}_\nu\bigotimes_{i=1}^{L}(|\alpha\rangle_i + (-1)^{a_i}|-\alpha\rangle_i), \qquad (32)$$

and from this equation, we see that if the total photon number is ν, $\mathrm{wt}(\boldsymbol{a}) \le \nu$ is satisfied since $|\alpha\rangle - |-\alpha\rangle$ contains at least one photon. Also, since $|\alpha\rangle + (-)|-\alpha\rangle$ contains even (odd) number of photons, we also have that the parity of ν and $\mathrm{wt}(\boldsymbol{a})$ are the same, that is, $(-1)^\nu = (-1)^{\mathrm{wt}(\boldsymbol{a})}$. Therefore,

after the successful detection event ($j \neq 0$) occurs and the system $\mathcal{H}_C$ reveals a photon number ν, the state of Alice and Bob's systems are contained in the range projection operator $\hat{P}^{(\nu)}$ with

$$\hat{P}^{(\nu)} := \sum_{\boldsymbol{a}:\mathrm{wt}(\boldsymbol{a})=\nu,\nu-2,\nu-4...}\sum_{i=1}^{L}\hat{P}(|\boldsymbol{a}\rangle_A|i\rangle_B). \qquad (33)$$

Through the unitary $\hat{U}$ in Eq. (23), we have [12]

$$\hat{U}\hat{P}^{(\nu)}\hat{U}^\dagger = \sum_{\boldsymbol{a}:\mathrm{wt}(\boldsymbol{a})=\nu-1,\nu-3...}\hat{P}(|\boldsymbol{a}\rangle_A)\otimes\hat{I}_B$$
$$+ \sum_{\boldsymbol{a}:\mathrm{wt}(\boldsymbol{a})=\nu+1}\hat{P}(|\boldsymbol{a}\rangle_A)\otimes\hat{P}_{\boldsymbol{a}} \qquad (34)$$

with

$$\hat{P}_{\boldsymbol{a}} := \sum_{i=1}^{L}\hat{P}(|i\rangle_B)\delta_{a_i,1}. \qquad (35)$$

Note that Eq. (34) can be derived by using Eq. (A1) in Appendix A.

E. Relation between the bit and phase errors

In this subsection, we derive the upper bound on the phase error rate for $e^{(\mathrm{ph},\nu)}$ for the ν-photon emission events by using the bit error rate $e^{(\mathrm{b},\nu)}$ originating from the ν-photon emission events. To obtain this, we consider deriving the largest eigenvalue $\Omega^{(\nu)}(\lambda)$ of the operator

$$\hat{P}^{(\nu)}(\hat{e}^{(\mathrm{ph})} - \lambda\hat{e}^{(\mathrm{b})})\hat{P}^{(\nu)} = \hat{e}^{(\mathrm{ph},\nu)} - \lambda\hat{e}^{(\mathrm{b},\nu)} \qquad (36)$$

with $0 < \lambda < \infty$. Here, we define the POVM elements regarding the phase and bit errors for the ν-photon emission events as $\hat{e}^{(\mathrm{ph},\nu)} := \hat{P}^{(\nu)}\hat{e}^{(\mathrm{ph})}\hat{P}^{(\nu)}$ and $\hat{e}^{(\mathrm{b},\nu)} := \hat{P}^{(\nu)}\hat{e}^{(\mathrm{b})}\hat{P}^{(\nu)}$, respectively. Once we obtain

$\Omega^{(\nu)}(\lambda)$, we can bound the phase error rate for the ν-photon emission events as

$$e^{(\mathrm{ph},\nu)} \leq \lambda e^{(\mathrm{b},\nu)} + \Omega^{(\nu)}(\lambda), \tag{37}$$

and hence to derive $\Omega^{(\nu)}(\lambda)$ is vital for determining the key rate. Since the unitary operator does not change the eigenvalues, $\Omega^{(\nu)}(\lambda)$ is also the largest eigenvalue of the operator [12].

$$\begin{aligned}
&\hat{U}\hat{P}^{(\nu)}\hat{U}^{\dagger}(\hat{U}\hat{e}^{(\mathrm{ph})}\hat{U}^{\dagger} - \lambda\hat{U}\hat{e}^{(\mathrm{b})}\hat{U}^{\dagger})\hat{U}\hat{P}^{(\nu)}\hat{U}^{\dagger} \\
&= \sum_{\boldsymbol{a}:\mathrm{wt}(\boldsymbol{a})=\nu-1,\nu-3\ldots} \hat{P}(|\boldsymbol{a}\rangle_A) \otimes (\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi}) \\
&+ \sum_{\boldsymbol{a}:\mathrm{wt}(\boldsymbol{a})=\nu+1} \hat{P}(|\boldsymbol{a}\rangle_A) \otimes \hat{P}_{\boldsymbol{a}}(\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi})\hat{P}_{\boldsymbol{a}},
\end{aligned} \tag{38}$$

where Eqs. (27), (29) and (34) are used. To obtain an upper bound on Eq. (38), we use a fact that Eq. (38) is a direct sum of $\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi}$ with different $\boldsymbol{a}$ of $\mathrm{wt}(\boldsymbol{a}) = \nu-1, \nu-3\ldots$ and $\hat{P}_{\boldsymbol{a}}(\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi})\hat{P}_{\boldsymbol{a}}$ with $\boldsymbol{a}$ of $\mathrm{wt}(\boldsymbol{a}) = \nu+1$. Since $\max_{\boldsymbol{a}}(\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi}) \geq \max_{\boldsymbol{a}'}(\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}'} - \lambda\hat{\Pi})$ holds for any $\boldsymbol{a}$ and $\boldsymbol{a}'$ with $\mathrm{wt}(\boldsymbol{a}) \geq \mathrm{wt}(\boldsymbol{a}')$, we only need to consider $\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi}$ with $\mathrm{wt}(\boldsymbol{a}) = \nu - 1$. We thus conclude that $\Omega^{(\nu)}(\lambda)$ is the larger of the two numbers $\Omega^{(\nu)}_{-}(\lambda)$ and $\Omega^{(\nu)}_{+}(\lambda)$ defined as follows; $\Omega^{(\nu)}_{-}(\lambda)$ is the largest eigenvalue of the operator

$$\{\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi} \mid \mathrm{wt}(\boldsymbol{a}) = \nu - 1\}, \tag{39}$$

and $\Omega^{(\nu)}_{+}(\lambda)$, which is the largest eigenvalue of the operator

$$\{\hat{P}_{\boldsymbol{a}}(\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi})\hat{P}_{\boldsymbol{a}} \mid \mathrm{wt}(\boldsymbol{a}) = \nu + 1\}. \tag{40}$$

Recall that $\hat{P}_{\boldsymbol{a}}$ is defined in Eq. (35), and $\hat{P}_{\boldsymbol{a}}(\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi})\hat{P}_{\boldsymbol{a}}$ is contained in the subspace $\{|i\rangle_B\}$ with $a_i = 1$.

IV. EXPLICIT RELATIONS BETWEEN THE BIT AND PHASE ERROR RATES

Here, we derive the explicit relations between $e^{(\mathrm{b},\nu)}$ and $e^{(\mathrm{ph},\nu)}$ by evaluating $\Omega^{(\nu)}(\lambda)$. For simplicity, we consider extracting the secret key up to the two-photon emission events ($\nu = 0, 1$ and 2) , and for more than two-photon emission events, we pessimistically assume that Eve has perfect knowledge on the sifted keys. Therefore, it is sufficient to provide the relationship for $\nu = 0, 1,$ and 2.

A. Zero-photon part

First, we discuss the case for $\nu = 0$ when Alice emits zero-photon. Since $\Omega^{(0)}_{-}(\lambda)$ has no candidates for $\nu = 0$, $\Omega^{(0)}(\lambda) = \Omega^{(0)}_{+}(\lambda)$. For $\Omega^{(0)}_{+}(\lambda)$, regardless of i such that $a_i = 1$, we have

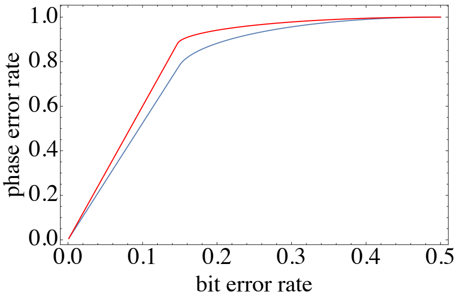

FIG. 3: Color online: The upper bound on the phase error rates $e^{(\mathrm{ph},1)}$ as a function of $e^{(\mathrm{b},1)}$. The red curve is based on the previous Shor-Preskill analysis [12] and the blue one is our analysis based on the complementarity. Note that these bounds are independent of the block length L.

$$\Omega^{(0)}(\lambda) = {}_B\langle i|(\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi})|i\rangle_B = -\lambda/2, \tag{41}$$

which corresponds to the single fixed point $(e^{(\mathrm{b},0)}, e^{(\mathrm{ph},0)}) = (1/2, 0)$.

B. Single-photon part

Next, we derive a relation between $e^{(\mathrm{b},1)}$ and $e^{(\mathrm{ph},1)}$. First, as for $\Omega^{(1)}_{-}(\lambda)$, since $\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} = 0$ from Eq. (39), $\Omega^{(1)}_{-}(\lambda)$ is a largest eigenvalue of $-\lambda\hat{\Pi}$, which is zero [1]. Next, for the derivation of $\Omega^{(1)}_{+}(\lambda)$, since $\mathrm{wt}(\boldsymbol{a}) = 2$ from its definition in Eq. (40), there are $\binom{L}{2}$ patterns to choose i and j such that $a_i = a_j = 1$ holds. In order to find the pair (i, j) to achieve the largest eigenvalue of Eq. (40), we use the following fact (see [23] for its proof).

Fact 1 *Given two $n \times n$ real matrices $A = (A_{i,j})_{i,j}$ and $\tilde{A} = (\tilde{A}_{i,j})_{i,j}$, whose off-diagonal elements are non-negative, their largest eigenvalues (respectively denoted by Λ_A and $\Lambda_{\tilde{A}}$) have a relation*

$$\Lambda_A \geq \Lambda_{\tilde{A}} \tag{42}$$

if $A_{i,j} \geq \tilde{A}_{i,j}$ holds for any i and j $(1 \leq i, j \leq n)$.

Thanks to this fact and Eqs. (28) and (30), we find that the largest eigenvalue $\Omega^{(1)}_{+}(\lambda)$ is achieved on the subspace $\{|1\rangle_B, |2\rangle_B\}$ [namely, $(i, j) = (1, 2)$], and by calculating the largest eigenvalue of $\hat{P}_{\boldsymbol{a}}(\hat{\Pi}^{(\mathrm{ph})}_{\boldsymbol{a}} - \lambda\hat{\Pi})\hat{P}_{\boldsymbol{a}}$ with $a_1 = a_2 = 1$, we have $\Omega^{(1)}_{+}(\lambda)$ in Lemma 1.

[1] Note that ${}_B\langle\psi|\hat{\Pi}|\psi\rangle_B = 0$ is achieved only for the state $|\psi\rangle_B = [\sum_{i=2}^{L-1}|i\rangle_B + (|1\rangle_B + |L\rangle_B)/\sqrt{2}]/\sqrt{L-1}$.

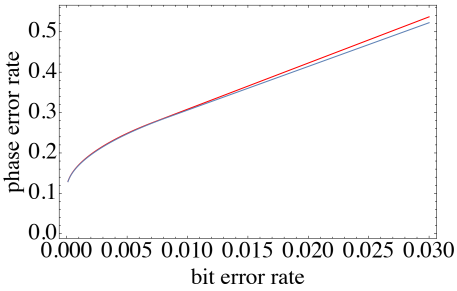

FIG. 4: Color online: The upper bound on the phase error rates $e^{(\mathrm{ph},2)}$ as a function of $e^{(\mathrm{b},2)}$ with $L = 10$. The red curve is based on the previous Shor-Preskill analysis and the blue one is our analysis based on the complementarity.

Lemma 1 *$\Omega_{+}^{(1)}(\lambda)$ is given by*

$$\Omega_{+}^{(1)}(\lambda) = (3 - 2\lambda + \sqrt{1 + 2\lambda^2})/4, \tag{43}$$

which is non-negative if $\lambda \leq (3 + \sqrt{5})$.

Then, by combining the results of $\Omega_{\pm}^{(1)}(\lambda)$, $\Omega^{(1)}(\lambda) = \max\{\Omega_{+}^{(1)}(\lambda), \Omega_{-}^{(1)}(\lambda)\}$ is given by

$$\Omega^{(1)}(\lambda) = \begin{cases} 0 & (\lambda > 3 + \sqrt{5}) \\ (3 - 2\lambda + \sqrt{1 + 2\lambda^2})/4 & (\lambda \leq 3 + \sqrt{5}). \end{cases} \tag{44}$$

Then, from Eq. (44), an upper bound on the phase error rate for the single-photon emission events is given in the Theorem 1 (see Appendix B for its proof).

Theorem 1 *The upper bound on $e^{(\mathrm{ph},1)}$ is given by*

$$e^{(\mathrm{ph},1)} \leq (3 + \sqrt{5})e^{(\mathrm{b},1)} \tag{45}$$

if $0 \leq e^{(\mathrm{b},1)} \leq (10 - 3\sqrt{5})/22$ and

$$e^{(\mathrm{ph},1)} \leq \inf_{0<\lambda<3+\sqrt{5}} \{\lambda e^{(\mathrm{b},1)} + (3 - 2\lambda + \sqrt{1 + 2\lambda^2})/4\} \tag{46}$$

if $(10 - 3\sqrt{5})/22 < e^{(\mathrm{b},1)}$.

In Fig. 3, we plot the resulting relation on $(e^{(\mathrm{b},1)}, e^{(\mathrm{ph},1)})$ (see the blue curve). For comparison, we compare our result and the previous work [12] (see the red curve), and we find that our security proof gives a tighter bound on $e^{(\mathrm{ph},1)}$.

C. Two-photon part

Here, we derive an upper bound on $e^{(\mathrm{ph},2)}$. The evaluation of $\Omega^{(2)}(\lambda) = \max\{\Omega_{+}^{(2)}(\lambda), \Omega_{-}^{(2)}(\lambda)\}$ involves the calculation of the largest eigenvalues $\Omega_{+}^{(2)}(\lambda)$ and $\Omega_{-}^{(2)}(\lambda)$. As for $\Omega_{+}^{(2)}(\lambda)$, since $\mathrm{wt}(\boldsymbol{a}) = \nu + 1 = 3$ from Eq. (40), we need to choose three indexes $1 \leq i < j < k \leq L$ such that $a_i = a_j = a_k = 1$ holds. There are $\binom{L}{3}$ patterns for the choices, and we need to find out the pair (i, j, k) that achieves the largest eigenvalue of Eq. (40). In so doing, the previous analysis [12] relies on a numerical method that compares each of all the largest eigenvalues of Eq. (40) with different (i, j, k), which becomes complicated as L becomes larger. On the other hand, we do not rely on a numerical method and derive $\Omega_{+}^{(2)}(\lambda)$ in a closed form as will be shown in Theorem 2, which holds for any L of $L \geq 3$. This can be accomplished by using the fact 1, and as a result, we find that the largest eigenvalue $\Omega_{+}^{(2)}(\lambda)$ is obtained on the subspace $\{|1\rangle_B, |2\rangle_B, |3\rangle_B\}$ [namely, $(i, j, k) = (1, 2, 3)$]. By calculating the largest eigenvalue of $\hat{P}_{\boldsymbol{a}}(\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} - \lambda\hat{\Pi})\hat{P}_{\boldsymbol{a}}$ with $a_1 = a_2 = a_3 = 1$, the largest eigenvalue $\Omega_{+}^{(2)}(\lambda)$ of Eq. (40) is given in Theorem 2.

Theorem 2 *$\Omega_{+}^{(2)}(\lambda)$ is given by $x/4$, where x is the maximum solution of the following equality for x,*

$$\begin{aligned} &-32 + 64\lambda - 32\lambda^2 + 2\lambda^3 + (32 - 40\lambda + 9\lambda^2)x \\ &+ (6\lambda - 10)x^2 + x^3 = 0. \end{aligned} \tag{47}$$

Next, we derive $\Omega_{-}^{(2)}(\lambda)$ that is the largest eigenvalue of the operator defined in Eq. (39). In this case, since $\mathrm{wt}(\boldsymbol{a}) = \nu - 1 = 1$, we need to find $\boldsymbol{a}$ with $\mathrm{wt}(\boldsymbol{a}) = 1$ that achieves the largest eigenvalue of the operator $\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} - \lambda\hat{\Pi}$. For this, we again note that the previous analysis [12] relies on a numerical method that compares each of all the largest eigenvalues of Eq. (39) with different $\boldsymbol{a}$ of $\mathrm{wt}(\boldsymbol{a}) = 1$. On the other hand, we do not rely on such a numerical method and derive $\Omega_{-}^{(2)}(\lambda)$ in a closed form as shown in Theorem 3 that can be applied for any L of $L \geq 3$ (see Appendix C for the proof).

Theorem 3 *Among various $\boldsymbol{a}$ with $\mathrm{wt}(\boldsymbol{a}) = 1$, the largest eigenvalue of $\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} - \lambda\hat{\Pi}$ realizes when $\boldsymbol{a} =$* 0100...0.

Thanks to this Theorem, we have that $\Omega_{-}^{(2)}(\lambda)$ is the largest eigenvalue of the operator $\hat{\Pi}_{\boldsymbol{a}:\boldsymbol{a}=0100...0}^{(\mathrm{ph})} - \lambda\hat{\Pi}$.

Whether $\Omega_{+}^{(2)}(\lambda)$ is larger than $\Omega_{-}^{(2)}(\lambda)$ or not depends on λ. With a constant $\tilde{\lambda}$, which is solely dependent on L, $\Omega_{+}^{(2)}(\lambda) \leq \Omega_{-}^{(2)}(\lambda)$ for $\lambda \geq \tilde{\lambda}$ and $\Omega_{+}^{(2)}(\lambda) > \Omega_{-}^{(2)}(\lambda)$ for $\lambda < \tilde{\lambda}$. As a result, the boundary of $(e^{(\mathrm{b},2)}, e^{(\mathrm{ph},2)})$ consists of two convex curves determined from $\Omega_{\pm}^{(2)}(\lambda)$ and a straight line with the slope $\tilde{\lambda}$ connecting them, which is shown in Fig. 4 (see the blue curve). We also show the previous result of the relation $(e^{(\mathrm{b},2)}, e^{(\mathrm{ph},2)})$ in [12] (see the red curve), and we find that the resulting relation is almost the same.

Recall that the secret keys are generated from the $\nu \in \{0, 1, 2\}$-photon emission events, and we take a worst case scenario that if Alice emits more than two photons, Eve has perfect knowledge on the sifted keys. From this consideration, the amount of privacy amplification in Eq. (19) is upper bounded by

$$\begin{aligned} Qf_{\mathrm{PA}} &= \sum_{\nu=0}^{\infty} Q^{(\nu)} h(e^{(\mathrm{ph},\nu)}) \leq \sum_{\nu=0}^{\infty} Q^{(\nu)} [\gamma e^{(\mathrm{b},\nu)} + \Omega_h^{(\nu)}(\gamma)] \\ &\leq \gamma e^{(\mathrm{b})} + \sum_{\nu=0}^{2} Q^{(\nu)} \Omega_h^{(\nu)}(\gamma) + \sum_{\nu\geq 3} Q^{(\nu)} \\ &= \gamma e^{(\mathrm{b})} + Q + \sum_{\nu=0}^{2} Q^{(\nu)} (\Omega_h^{(\nu)}(\gamma) - 1), \end{aligned} \tag{48}$$

where in the first inequality, we bound the convex regions of $(e^{(\mathrm{b},\nu)}, h(e^{(\mathrm{ph},\nu)}))$ specified by a set of linear inequalities with $0 < \gamma < \infty$,

$$h(e^{(\mathrm{ph},\nu)}) \leq \gamma e^{(\mathrm{b},\nu)} + \Omega_h^{(\nu)}(\gamma). \tag{49}$$

Here, $\Omega_h^{(\nu)}(\gamma)$ is the quantity depending on γ and $\Omega^{(\nu)}(\gamma)$. Also, in the second inequality of Eq. (48), we use the definition of the bit error rate $e^{(\mathrm{b})} = \sum_\nu Q^{(\nu)} e^{(\mathrm{b},\nu)}$. Since we can choose arbitrary γ to lower-bound the amount of privacy amplification, the lower bound on the asymptotic key generation rate in Eq. (3) is written as

$$\begin{aligned} &G \geq \\ &\frac{1}{L}\left\{ \sum_{\nu=0}^{2} Q^{(\nu)} - Qf_{\mathrm{EC}}(e^{(\mathrm{b})}) - \inf_{\gamma} [\gamma e^{(\mathrm{b})} + \sum_{\nu=0}^{2} Q^{(\nu)} \Omega_h^{(\nu)}(\gamma)] \right\}. \end{aligned} \tag{50}$$

Here, $Q^{(\nu)}$ is chosen to maximize Eq. (48) as [12]

$$Q^{(\nu)} = \begin{cases} p_\nu & (\nu \geq \nu_{\min} + 1) \\ Q - (1 - \sum_{\nu'=0}^{\nu_{\min}} p_{\nu'}) & (\nu = \nu_{\min}) \\ 0 & (\nu \leq \nu_{\min} - 1), \end{cases} \tag{51}$$

where $\{p_\nu\}$ is the Poisson distribution with mean $L\alpha^2$

$$p_\nu = e^{-L\alpha^2} (L\alpha^2)^\nu / \nu! \tag{52}$$

and $\nu_{\min}$ is the integer satisfying

$$1 - \sum_{\nu'=0}^{\nu_{\min}} p_{\nu'} < Q \leq 1 - \sum_{\nu'=0}^{\nu_{\min}-1} p_{\nu'}. \tag{53}$$

V. KEY GENERATION RATES

Here, we show the key generation rates of the DPS protocol based on our analysis and the previous analysis in [12]. For both cases, we suppose that the total detection probability is assumed to be given by $Q = (L-1)\eta\alpha^2 e^{-(L+1)\eta\alpha^2}$, where we assume that the transmittance of the channel including the detection probability is given by $\eta = 0.1 \times 10^{-0.2l/10}$, and for simplicity we adopt $f_{\mathrm{EC}}(e^{(\mathrm{b})}) = h(e^{(\mathrm{b})})$. In Fig. 5, we show the key rates for the case of $e^{(\mathrm{b})} = 2\%$ and $L = 10$ by optimizing the mean photon number α^2. As a result, we find that the secure key rate of the DPS protocol based on our analysis is 1.22 times as high as the previous one.

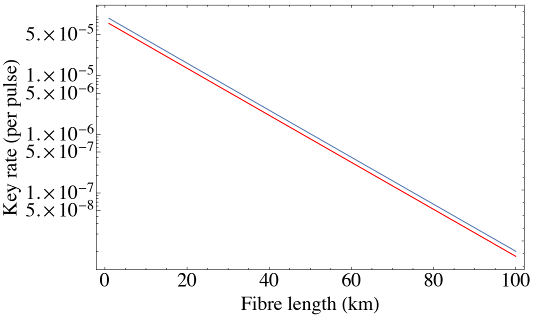

FIG. 5: Color online: The key generation rate per sending pulse of the DPS protocol based on our security analysis (blue curve) and the previous analysis (red curve). In these plots, we set $L = 10$ and $e^{(\mathrm{b})} = 2\%$.

We note that the two key generation rates in Fig. 5 do not decrease drastically after a certain distance. This is so because we consider the constant bit error rate, which is independent of the distance.

VI. CONCLUSION

In conclusion, we have proven the information-theoretic security proof for the DPS QKD protocol based on the complementarity approach. As a result, we found that our security proof provides a slightly better key generation rate compared to the previous security proof based on the Shor-Preskill approach [12]. This improvement is obtained since the complementarity approach can incorporate more detailed information on Alice's sending state to estimate the leaked information to Eve. In particular, we have employed the information that the intensity of Alice's sending states is weak, and thanks to this additional information we have obtained tighter upper bounds on the leaked information to Eve compared to those in the previous proof [12]. Moreover, we have removed the necessity of the numerical calculation, which was needed in [12] to derive the leaked information on the two-photon emission events. This leads to an advantage that our security proof enables us to evaluate the security of the DPS protocol with any block size L of $L \geq 3$.

Acknowledgments

G. K. and K. T. acknowledge support from CREST, JST. Y. T. acknowledges the support from the Program for Leading Graduate Schools: Interactive Materials Science Cadet Program. T. S. acknowledges the support from the ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan).

Appendix A: Proof of Eq. (24)

Here, we prove Eq. (24). First, from the definition of $\hat{U}$ in Eq. (23), we have

$$\hat{U}\hat{P}(|s\rangle_{A,i})\hat{P}(|i'\rangle_B)\hat{U}^\dagger = \hat{P}(|s\oplus\delta_{i,i'}\rangle_{A,i})\hat{P}(|i'\rangle_B). \tag{A1}$$

By using Eqs. (21) and (A1), a direct calculation leads to the following equation

$$\begin{aligned}
&\hat{U}\hat{e}_j^{(\mathrm{ph})}\hat{U}^\dagger = \hat{e}_j^{(\mathrm{ph})} \\
&= \sum_{\boldsymbol{a}} \hat{P}(|\boldsymbol{a}\rangle_A) \otimes \Big[\delta_{a_j,0}\delta_{a_{j+1},1}\kappa_j\hat{P}(|j\rangle_B) + \delta_{a_j,1}\delta_{a_{j+1},0}\kappa_{j+1}\hat{P}(|j+1\rangle_B) + \delta_{a_j,1}\delta_{a_{j+1},1}\Big(\kappa_{j+1}\hat{P}(|j+1\rangle_B) + \kappa_j\hat{P}(|j\rangle_B)\Big)\Big] \\
&= \sum_{\boldsymbol{a}} \hat{P}(|\boldsymbol{a}\rangle_A) \otimes \Big[\kappa_j\delta_{a_{j+1},1}\hat{P}(|j\rangle_B) + \kappa_{j+1}\delta_{a_j,1}\hat{P}(|j+1\rangle_B)\Big],
\end{aligned} \tag{A2}$$

which concludes Eq. (24). Note that in the final equation, we use the property of the Kronecker delta $\delta_{a_j,0}+\delta_{a_j,1}=1$.

Appendix B: Proof of Theorem 1

In this appendix, we prove Theorem 1. For this, we consider bounding the convex achievable reagion $(e^{(\mathrm{b},1)}, e^{(\mathrm{ph},1)})$ by a straight line with the slope either $\lambda = 3+\sqrt{5} =: \lambda_0$ or $\lambda = \lambda'(<\lambda_0)$. Here, from Eq. (44), $\lambda > \lambda_0$ never appears in the discussion since it is trivially understood from Eqs. (37) and (44) that $\lambda = \lambda_0$ gives a tighter bound on $e^{(\mathrm{ph},1)}$ than $\lambda > \lambda_0$. In a lower bit error rate regime, the convex achievable region is tightly bounded with $\lambda = \lambda_0$. On the other hand, in a higher bit error rate regime, λ' gives a tighter bound. Hence, we derive the threshold bit error rate $e^{*(\mathrm{b},1)}$ that for $e^{(\mathrm{b},1)} \le (>) e^{*(\mathrm{b},1)}$, the convex achievable region is tightly bounded with the slope $\lambda = \lambda_0$ (λ'). This threshold can be derived by solving the following equation:

$$\lambda_0 e^{(\mathrm{b},1)} + \Omega_+^{(1)}(\lambda_0) = \lambda' e^{(\mathrm{b},1)} + \Omega_+^{(1)}(\lambda'). \tag{B1}$$

By using Lemma 1, Eq. (B1) leads to

$$e^{(\mathrm{b},1)} = \frac{(3-\sqrt{5}-\lambda')}{2(3-2\lambda'-\sqrt{1+2\lambda'^2})} =: f(\lambda'). \tag{B2}$$

By taking a limit of $\lambda' \to \lambda_0$, we can derive the threshold bit error rate as $e^{*(\mathrm{b},1)} = \lim_{\lambda'\to\lambda_0} f(\lambda') = (10-3\sqrt{5})/22$. This means that for $0 \le e^{(\mathrm{b},1)} \le e^{*(\mathrm{b},1)}$, $\lambda = \lambda_0$ is the optimal slope to bound $e^{(\mathrm{ph},1)}$, and for $e^{(\mathrm{b},1)} > e^{*(\mathrm{b},1)}$, the optimal slope λ (with $0 < \lambda < \lambda_0$) changes according to the bit error rate as shown in Eq. (46).

Appendix C: Proof of Theorem 3

In this appendix, we prove Theorem 3 in the main text. We first prove the Theorem for the case of $L = 3$ and 4, and after that we prove it for the case of $L \ge 5$.

For the cases of $L = 3$ and 4, through a direct comparison of the largest eigenvalues of the operator $\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} - \lambda\hat{\Pi}$ among various $\boldsymbol{a}$ with $\mathrm{wt}(\boldsymbol{a}) = 1$, it is easy to confirm that the operator gives the largest eigenvalues when $a_2 = 1$.

Next, from now on, we move on to the general case of $L \ge 5$. We first introduce two functions $F(L,x,w,y)$ and $g_s(L,x,w,m)$ and investigate their properties, which we use in the main part of the proof in Appendix C 3. Throughout the discussion below, we assume $L \ge 5$, $0 \le x$, $-1 \le y \le 1$ and $0 < w < \infty$.

1. Function $F(L, x, w, y)$

First, we introduce $F(L, x, w, y)$, which is defined as

$$\begin{aligned} F(L,x,w,y) =& \frac{1}{2}\cosh Lx - 2w\cosh(L-1)x + (2w^2 - \frac{1}{2})\cosh(L-2)x + 2w^2\cosh(L-4)x \\ &+ 2w(2w\cosh x - \cosh 2x)\cosh{(L-3)xy}. \end{aligned} \tag{C1}$$

From this definition, it is easy to confirm that

$$F\left(L, x, \frac{\cosh 2x}{2\cosh x}, y\right) = -\sinh x \sinh(L-5)x \leq 0 \tag{C2}$$

and for $0 \leq w \leq 1/2$,

$$F(L, 0, w, y) = 4w(2w-1) \leq 0. \tag{C3}$$

Here, $w = \frac{\cosh 2x}{2\cosh x}$ is a monotonically increasing and one-to-one function from the domain $\mathbb{R}_{\geq 0}$ to $\mathbb{R}_{\geq 1/2}$. Hence, an inverse function $f(w)$ can be defined from $\mathbb{R}_{\geq 1/2}$ to $\mathbb{R}_{\geq 0}$ as

$$x_w = \begin{cases} 0 & \text{if } w \leq 1/2 \\ f(w) & \text{if } w > 1/2. \end{cases} \tag{C4}$$

With this notation and Eqs. (C2) and (C3), we have that

$$L > 5 \text{ and } w \neq \frac{1}{2} \Rightarrow F(L, x_w, w, y) < 0, \tag{C5}$$

$$L = 5 \text{ or } w = \frac{1}{2} \Rightarrow F(L, x_w, w, y) = 0. \tag{C6}$$

Also, we have a property

$$\lim_{x \to +\infty} F(L, x, w, y) = +\infty. \tag{C7}$$

From Eqs. (C5)-(C7) and the continuity of $F(L, x, w, y)$, we obtain

$$\forall L, w, y, \exists x \geq x_w,\ \ F(L, x, w, y) = 0. \tag{C8}$$

From this equation, we can define the following function

$$x_{\max}(L, w, y) = \max\{x | F(L, x, w, y) = 0\}. \tag{C9}$$

In the case of $L > 5$ and $w \neq \frac{1}{2}$, we can confirm from (C5) that $x_{\max}(L, w, y)$ is strictly larger than x_w:

$$x_w < x_{\max}(L, w, y). \tag{C10}$$

Also, Eq. (C10) holds in the case of $w = \frac{1}{2}$ or $L = 5$. For $w = \frac{1}{2}$ and $L \geq 5$, Eq. (C10) is satisfied since

$$\frac{d}{dx}F\left(L, x, \frac{1}{2}, y\right)|_{x=0} = 0 \text{ and } \frac{d^2}{dx^2}F\left(L, x, \frac{1}{2}, y\right)|_{x=0} = -2(L-2) < 0. \tag{C11}$$

Also, for $L = 5$ and $w \neq 1/2$, Eq. (C10) is satisfied since

$$\frac{d}{dx}F(5, x, w, y)|_{w=\frac{\cosh 2x}{2\cosh x}} = -\frac{1}{2}\cosh^{-2}x(1 + \cosh 2x \cosh 2xy)(3\sinh x + \sinh 3x) < 0 \tag{C12}$$

holds.

Next, since

$$\forall x \geq x_w,\ \ 2w\cosh x - \cosh 2x \leq 0 \tag{C13}$$

holds, we have the following relation if $0 \le y \le 1$

$$\forall x \ge x_w,\ \frac{d}{dy}F(L,x,w,y) = 2w(2w\cosh x - \cosh 2x)(L-3)x\sinh{(L-3)xy} \le 0. \tag{C14}$$

From this equation and Eq. (C10), we obtain

$$F(L, x_{\max}(L,w,y), w, y) \ge F(L, x_{\max}(L,w,y), w, 1), \tag{C15}$$

which leads to the inequality

$$x_{\max}(L,w,y) \le x_{\max}(L,w,1) \tag{C16}$$

if $0 \le y \le 1$. As for $-1 \le y \le 0$, from the definitions of the function $F(L,x,w,y)$ and $x_{\max}$, we find that these are even functions of y. Therefore, for $-1 \le y \le 1$,

$$x_{\max}(L,w,y) = x_{\max}(L,w,|y|) \le x_{\max}(L,w,1) \tag{C17}$$

is satisfied.

2. Property of the function $g_s(L,x,w,m)$

Next, we introduce the function $g_s(L,x,w,m)$ for $s \in \{-1,1\}$, which is given by

$$g_s(L,x,w,m) = \cosh\left(\frac{L-1}{2} + sm\right)x - 2w\cosh\left(\frac{L-3}{2} + sm\right)x. \tag{C18}$$

This function has a following property that we use in Appendix C 3.

Property 1 *For* $|m| \le \frac{L-5}{2}$,

$$g_s\left(L, x_{\max}\left(L, w, \frac{2m}{L-3}\right), w, m\right) > 0 \tag{C19}$$

and for $|m| = \frac{L-3}{2}$,

$$g_1(L, x_{\max}(L,w,y), w, m) \ne 0 \text{ or } g_{-1}(L, x_{\max}(L,w,y), w, m) \ne 0. \tag{C20}$$

Proof of Property 1

First, we prove Eq. (C19). Since $g_s(L,x,w,m)$ is a monotonically-decreasing function for w, we have

$$x > x_w, |m| \le \frac{L-5}{2} \Rightarrow g_s(L,x,w,m) > g_s\left(L, x, \frac{\cosh 2x}{2\cosh x}, m\right) = \sinh\left(\frac{L-5}{2} + sm\right)x\tanh x \ge 0, \tag{C21}$$

where we use the fact $x > x_w \Rightarrow \frac{\cosh 2x}{2\cosh x} > w$. By combining Eqs. (C21) and (C10), we obtain

$$g_s\left(L, x_{\max}\left(L, w, \frac{2m}{L-3}\right), w, m\right) > 0 \tag{C22}$$

for $|m| \le \frac{L-5}{2}$, which concludes Eq. (C19).

As for the proof of Eq. (C20), we use

$$\begin{aligned}
&g_1\left(L,x,w,\frac{L-3}{2}\right) - g_{-1}\left(L,x,w,\frac{L-3}{2}\right)\cosh(L-3)x \\
=&g_{-1}\left(L,x,w,-\frac{L-3}{2}\right) - g_1\left(L,x,w,-\frac{L-3}{2}\right)\cosh(L-3)x \\
=&\sinh x\sinh{(L-3)x} > 0,
\end{aligned} \tag{C23}$$

for $x > 0$ and since $\cosh(L-3)x > 0$, we can conclude Eq. (C20).

3. Calculation of $\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} - \lambda\hat{\Pi}$

Next, we calculate the matrix elements of $\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} - \lambda\hat{\Pi} = (\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} - \lambda\hat{\Pi}|_{j,k})_{j,k}$, which is a tridiagonal symmetric matrix. For convenience of notation, we denote the index of low and column of the matrix by $j, k \in \{-\frac{L-1}{2}, -\frac{L-3}{2}, ..., \frac{L-3}{2}, \frac{L-1}{2}\}$ (not by $\{1, 2, ..., L-1, L\}$). The diagonal elements are given by

$$\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} - \lambda\hat{\Pi}|_{j,j} = \begin{cases} \delta_{a_{\pm\frac{L-3}{2}},1} - \lambda/2 & (j = \pm\frac{L-1}{2}) \\ (\delta_{a_{j-1},1} + \delta_{a_{j+1},1})/2 - \lambda/2 & (j \neq \pm\frac{L-1}{2}), \end{cases} \tag{C24}$$

and the off-diagonal elements are given by

$$\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} - \lambda\hat{\Pi}|_{j,j-1} = \begin{cases} \sqrt{2}\lambda/4 & (j = \frac{L-1}{2}) \\ \lambda/4 & (-\frac{L-5}{2} \leq j \leq \frac{L-3}{2}) \\ \sqrt{2}\lambda/4 & (j = -\frac{L-3}{2}). \end{cases} \tag{C25}$$

Since we now consider $\mathrm{wt}(\boldsymbol{a}) = \nu - 1 = 1$, we need to choose only one j such that $a_j = 1$. If we define m that satisfies $a_m = 1$, $\hat{\Pi}_{\boldsymbol{a}}^{(\mathrm{ph})} - \lambda\hat{\Pi}$ is characterized by m, and we define $\hat{A}^{(m)} := \hat{\Pi}_{\boldsymbol{a}:a_m=1}^{(\mathrm{ph})} - \lambda\hat{\Pi}$. Below, we classify m into three cases, and for each of all the cases we calculate the matrix elements of $\hat{A}^{(m)} = (\hat{A}^{(m)}|_{j,k})_{j,k}$.

(I) For $|m| = \frac{L-1}{2}$,

$$\hat{A}^{(s\frac{L-1}{2})}|_{j,k} = \frac{\delta_{j,s\frac{L-3}{2}} - \lambda}{2}\delta_{j,k} + \lambda\frac{1 + (\sqrt{2}-1)\delta_{|j+k|,L-2}}{4}\delta_{|j-k|,1}, \tag{C26}$$

where $s \in \{-1, 1\}$.

(II) For $|m| = \frac{L-3}{2}$,

$$\hat{A}^{(s\frac{L-3}{2})}|_{j,k} = \frac{2\delta_{j,s\frac{L-1}{2}} + \delta_{j,s\frac{L-5}{2}} - \lambda}{2}\delta_{j,k} + \lambda\frac{1 + (\sqrt{2}-1)\delta_{|j+k|,L-2}}{4}\delta_{|j-k|,1}. \tag{C27}$$

(III) For $|m| \leq \frac{L-5}{2}$,

$$\hat{A}^{(m)}|_{j,k} = \frac{\delta_{j,m-1} + \delta_{j,m+1} - \lambda}{2}\delta_{j,k} + \lambda\frac{1 + (\sqrt{2}-1)\delta_{|j+k|,L-2}}{4}\delta_{|j-k|,1}. \tag{C28}$$

Now, we prove Theorem 3 that the largest eigenvalue of $\hat{A}^{(m)}$ realizes when $|m| = \frac{L-3}{2}$ for $L \geq 5$ and $0 < \lambda < \infty$. First, from the above expressions in Eqs. (C26) and (C28), $\hat{A}^{(\pm\frac{L-1}{2})} \leq \hat{A}^{(\pm\frac{L-5}{2})}$ are obtained, and hence we need not to consider the case (I) for deriving the largest eigenvalue of $\hat{A}^{(m)}$.

Next, we compare the eigenvalues of the cases (II) and (III). For this, we prepare the vector $v^{(m)} = (v^{(m)}|_j)_j$ that has L elements. As well as the matrix representation, we denote the index of column of the vector by $j \in \{-\frac{L-1}{2}, -\frac{L-3}{2}, ..., \frac{L-3}{2}, \frac{L-1}{2}\}$. For $s \in \{-1, 1\}$, $j_- \in \{-\frac{L-3}{2}, -\frac{L-5}{2}, ..., m-2, m-1\}$ and $j_+ \in \{m+1, m+2, ..., \frac{L-5}{2}\frac{L-3}{2}\}$, we define $v^{(m)}$ as

$$v^{(m)}|_{s\frac{L-1}{2}} = \frac{1}{\sqrt{2}}g_s(L, x, \lambda^{-1}, m), \tag{C29}$$

$$v^{(m)}|_m = g_1(L, x, \lambda^{-1}, m)g_{-1}(L, x, \lambda^{-1}, m), \tag{C30}$$

$$v^{(m)}|_{j_-} = g_{-1}(L, x, \lambda^{-1}, m)\cosh\left(\frac{L-1}{2} + j_-\right)x, \tag{C31}$$

$$v^{(m)}|_{j_+} = g_1(L, x, \lambda^{-1}, m)\cosh\left(\frac{L-1}{2} - j_+\right)x, \tag{C32}$$

where $x \in \mathbb{R}$ is a free parameter. In this case, the following equation holds.

$$\left[\hat{A}^{(m)} - \frac{\lambda(\cosh x - 1)}{2}\hat{I}\right] \cdot v^{(m)}|_j = -\frac{\lambda}{4}\delta_{j,m}F\left(L, x, \lambda^{-1}, \frac{2m}{L-3}\right). \tag{C33}$$

Here we recall that $g_s(L, x, \lambda^{-1}, m)$ and $F(L, x, \lambda^{-1}, \frac{2m}{L-3})$ are defined in Eqs. (C18) and (C1), respectively. In the following, we set $x = x_{\max}(L, \lambda^{-1}, \frac{2m}{L-3})$. From its definition in Eq. (C9), we have that the rhs of Eq. (C33) is zero, which leads to

$$\left[\hat{A}^{(m)} - \frac{\lambda(\cosh x_{\max}(L, \lambda^{-1}, \frac{2m}{L-3}) - 1)}{2}\hat{I}\right] \cdot v^{(m)}|_j = 0. \tag{C34}$$

Moreover, thanks to Property 1, we find that all the elements of $v^{(m)}$ never become zero simultaneously, and therefore we conclude that $v^{(m)}$ and $\frac{\lambda}{2}(\cosh x_{\max}(L, \lambda^{-1}, \frac{2m}{L-3}) - 1)$ represent the eigenvector and the eigenvalue of $\hat{A}^{(m)}$, respectively. In particular, if $|m| \leq \frac{L-5}{2}$, all the elements of $v^{(m)}$ are guaranteed to be positive due to Eq. (C19) in Property 1. By combining this fact and the fact that $\hat{A}^{(m)}$ is an Hermite operator with non-negarive off-diagonal elements, we conclude that the eigenvalue $\frac{\lambda}{2}(\cosh x_{\max}(L, \lambda^{-1}, \frac{2m}{L-3}) - 1)$ is the largest eigenvalue of $\hat{A}^{(m)}$ if $|m| \leq \frac{L-5}{2}$. Finally, from Eq. (C16), we have that

$$\frac{\lambda}{2}\left[\cosh x_{\max}\left(L, \lambda^{-1}, \frac{2m}{L-3}\right) - 1\right] \leq \frac{\lambda}{2}(\cosh x_{\max}(L, \lambda^{-1}, 1) - 1). \tag{C35}$$

Since the rhs represents the eigenvalue of $\hat{A}^{(\frac{L-3}{2})}$, we conclude that $\hat{A}^{(\frac{L-3}{2})}$ has an eigenvalue that is no smaller than the largest eigenvalue of $\hat{A}^{(m)}$ with $|m| \leq \frac{L-5}{2}$.

[1] C. H. Bennett and G. Brassard, In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing p. 175 (1984).

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991), URL http://link.aps.org/doi/10.1103/PhysRevLett.67.661.

[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992), URL http://link.aps.org/doi/10.1103/PhysRevLett.68.3121.

[4] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998), URL http://link.aps.org/doi/10.1103/PhysRevLett.81.3018.

[5] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004), URL http://link.aps.org/doi/10.1103/PhysRevLett.92.057901.

[6] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Applied Physics Letters **87**, 194108 (2005), http://dx.doi.org/10.1063/1.2126792, URL http://dx.doi.org/10.1063/1.2126792.

[7] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002), URL http://link.aps.org/doi/10.1103/PhysRevLett.89.037902.

[8] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003), URL http://link.aps.org/doi/10.1103/PhysRevA.68.022317.

[9] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002), URL http://link.aps.org/doi/10.1103/PhysRevLett.88.057902.

[10] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al., Opt. Express **19**, 10387 (2011), URL http://www.opticsexpress.org/abstract.cfm?URI=oe-19-11-10387.

[11] K. Wen, K. Tamaki, and Y. Yamamoto, Phys. Rev. Lett. **103**, 170503 (2009), URL http://link.aps.org/doi/10.1103/PhysRevLett.103.170503.

[12] K. Tamaki, G. Kato, and M. Koashi, arXiv:1208.1995v1 (2012).

[13] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000), URL http://link.aps.org/doi/10.1103/PhysRevLett.85.441.

[14] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003), URL http://link.aps.org/doi/10.1103/PhysRevLett.90.057902.

[15] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003), URL http://link.aps.org/doi/10.1103/PhysRevLett.90.167904.

[16] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004), URL http://link.aps.org/doi/10.1103/PhysRevLett.93.120501.

[17] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005), URL http://link.aps.org/doi/10.1103/PhysRevLett.94.040503.

[18] K. Tamaki and H.-K. Lo, Phys. Rev. A **73**, 010302 (2006), URL http://link.aps.org/doi/10.1103/PhysRevA.73.010302.

[19] M. Koashi, arXiv:0704.3661 (2007).

[20] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[21] M. Koashi, New Journal of Physics **11**, 045018 (2009), URL http://stacks.iop.org/1367-2630/11/i=4/a=045018.

[22] R. Canetti, In Proc. IEEE Int. Conf. on Cluster Comput. pp. 136–145 (2001).

[23] Y. Hatakeyama, A. Mizutani, G. Kato, N. Imoto, and K. Tamaki, Phys. Rev. A **95**, 042301 (2017), URL https://link.aps.org/doi/10.1103/PhysRevA.95.042301.