




Security proof for round-robin differential-quadrature-phase-shift quantum key distribution

Yang-Guang Shan , Zhen-Qiang Yin*, Hang Liu, Shuang Wang , Wei Chen, De-Yong He, Guang-Can Guo, and Zheng-Fu Han 

CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, China;
CAS Center for Excellence in Quantum Information and Quantum Physics,
University of Science and Technology of China, Hefei, Anhui 230026, China;
and State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China



(Received 20 January 2022; revised 6 March 2022; accepted 8 March 2022; published 24 March 2022)

By introducing four-phase modulations into round-robin-differential-phase-shift (RRDPS) quantum key distribution (QKD) protocol, the round-robin-differential-quadrature-phase-shift (RRDQPS) protocol is proposed. According to the security proof of RRDQPS protocol, it is able to tolerate a higher error rate of key bits. However, its performance with a practical weak coherent source is still unknown since that security proof only applies to a single photon source. In this article, we give the security proof for the general n -photon RRDQPS protocol, by which RRDQPS with a practical weak coherent source becomes feasible in the experiment. Through numerical simulation, it is verified that RRDQPS protocol has an advantage over RRDPS protocol on transmission distance, especially when the pulse number is small.

DOI: [10.1103/PhysRevA.105.032441](https://doi.org/10.1103/PhysRevA.105.032441)

I. INTRODUCTION

Quantum key distribution (QKD) promises proven unconditional secure key distribution between two distant parties (usually called Alice and Bob). Since the first QKD protocol BB84 protocol [1] was proposed by Bennett and Brassard, a lot of ingenious protocols [2–9] have been put forward. Among them, the round-robin-differential-phase-shift (RRDPS) protocol [8] has attracted attention because of its distinctive characteristics. First, signal disturbance monitoring is not indispensable in RRDPS. Due to this characteristic, decoy states [10–12] and even error-rate monitoring are not needed, which may reduce some potential loopholes of intensity modulators. The simplification of devices and postprocessing could reduce the practical difficulty of implementing real-life QKD systems. Second, as a high-dimensional protocol [13], RRDPS may tolerate a higher error rate compared to the well-known BB84 protocol, which can be useful in some particular channels. For instance, the well-known BB84 cannot generate any secret key if the error rate is larger than 11% [14], while this value in RRDPS can be substantially increased. Since the invention and the first security proof given in [8], improved security proofs [15–19] have been given to further enhance its performance. Several experimental realizations [20–23] showed its practicability.

It is beneficial to briefly review the flow of RRDPS. Alice first prepares packets of L ($3 \leq L \leq 100$ typically) coherent pulses and the phase of each pulse is encoded from $\{0, \pi\}$ randomly corresponding to her raw key bit. Then the packets are sent from Alice to Bob through an insecure channel. Bob will randomly select two pulses in each packet and conduct

a phase differential measurement on them to acquire his key bit. Through authentic classical communications, Bob tells the indices of the pulses he selected to Alice, who can determine her sifted key then. One can see the main difference between RRDPS and the well-known phase-encoding BB84 is that the former prepares L -pulse states instead of 2-pulse states in BB84. Indeed, the random selection of two pulses among the L pulses made by Bob plays an essential role in the security of RRDPS. On the other hand, BB84 modulates four phases, i.e., $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$, while RRDPS just employs $\{0, \pi\}$. So an intuitive idea to improve the security of RRDPS is introducing four-phase modulation like BB84 into RRDPS, which is the very idea of the round-robin-differential-quadrature-phase-shift (RRDQPS) protocol [24]. In the RRDQPS protocol, Alice sends packets of L pulses to Bob like RRDPS. Differently, the phase of each pulse is modulated randomly from $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ like phase-encoding BB84. Then Bob will perform a differential phase measurement on X -basis $\{0, \pi\}$ or Y -basis $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$ uniformly at random, which is also quite like phase-encoding BB84 except that the two pulses are randomly chosen from the L pulses. RRDPS can be seen as an X -basis case of RRDQPS. More interestingly, the phase-encoding BB84 can be viewed as a special case of RRDQPS with $L = 2$. In [25], the security proof for the RRDQPS protocol in the single-photon case was given and significant improvement on error tolerance compared to single-photon RRDPS can be seen. However, without a security proof for the general n -photon case, the RRDQPS protocol cannot be applied to weak coherent-state pulse (WCP) sources.

In this article, we will give an asymptotic security proof for the n -photon RRDQPS protocol, and then we apply our result to RRDQPS with WCP source to see its improvement in practice. Numerical simulation shows that, when the bit error rate is monitored, larger error rates can be tolerated

*yinzq@ustc.edu.cn

by the RRDQPS protocol than the RRDPS protocol. More importantly, a longer transmission distance can be achieved. This article is organized as follows. In Sec. II, the flow of the RRDQPS protocol is listed. In Sec. III, we give the sketch of the security proof (see a detailed proof in the Appendixes). Some discussions of our result and a comparison between RRDQPS and RRDPS with WCP sources are given in Sec. IV. Finally, we come to the conclusion in Sec. V.

II. PROTOCOL DESCRIPTION

The RRDQPS protocol with a WCP source is described below.

(1) Alice prepares packets of L pulses and the phase of each pulse is modulated from $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ randomly. Since the pulses are produced from a WCP source and phase randomization is conducted between packets, the quantum state of each packet is a mixed state of pure Fock states, and the mixed state ratios follow a Poisson distribution. So the state of a packet is shown as

$$|\psi\rangle\langle\psi| = \sum_{n=0}^{\infty} \frac{(L\mu)^n e^{-L\mu}}{n!} |\psi_n\rangle\langle\psi_n|, \quad (1)$$

where μ is the average photon number per pulse and $|\psi_n\rangle$ is the state when there are n photons in a packet. For example, we have

$$|\psi_1\rangle = \frac{1}{\sqrt{L}} \sum_{m=1}^L i^{k_m} |m\rangle, \quad (2)$$

$$|\psi_2\rangle = \frac{1}{L} \left(\sum_{m=1}^L i^{2k_m} |mm\rangle + \sqrt{2} \sum_{1 \leq m < p \leq L} i^{k_m+k_p} |mp\rangle \right), \quad (3)$$

where i is the imaginary unit, $k_m \in \{0, 1, 2, 3\}$ means that Alice modulates phase $k_m\pi/2$ for the m th pulse in this packet, and $|m\rangle$ means that the single photon in this packet is in the m th pulse. Similarly, $|mp\rangle$ means that there are two photons in the packet and they are in the m th and p th pulses, respectively.

(2) Packets of pulses are sent from Alice to Bob through an insecure channel where the eavesdropper (usually called Eve) can conduct attacks. Bob selects a pulse delay value $r \in \{1, 2, \dots, L-1\}$ and detects the X basis or Y basis randomly for each packet. When the X basis is selected, Bob conducts the detection projecting to $(|a\rangle \pm |b\rangle)/\sqrt{2}$, where $b-a=r$ for all $a, b \in \{1, 2, \dots, L\}$. When the Y basis is selected, Bob projects the state into $(|a\rangle \pm i|b\rangle)/\sqrt{2}$, ($b-a=r$). In experimental realization, this kind of detection can be realized by a Mach-Zehnder interferometer with a phase modulator and a variable delay [24]. We assume that the detectors of Bob could discriminate between single-photon clicks from two or more photon clicks. Only when there is one single-photon click in a packet can the detecting result be recorded as a successful click.

(3) After the transmission of sufficient packets, Bob publicly discloses the two time-bins a, b and the detecting bases for each packet with successful click. Alice also claims the $X(Y)$ basis if $|k_a - k_b|$ is even (odd). Then Alice and Bob discard the events with mismatched encoding and detecting bases. Encoding and detecting events associated with $(|a\rangle +$

$|b\rangle)/\sqrt{2}$ and $(|a\rangle + i|b\rangle)/\sqrt{2}$ are recorded as bit 0, while $(|a\rangle - |b\rangle)/\sqrt{2}$ and $(|a\rangle - i|b\rangle)/\sqrt{2}$ are recorded as bit 1. Finally, classical postprocessing is conducted to obtain the final key.

III. SECURITY PROOF

The essential of the security proof is to bound Eve's information on the key bits. In the main text, we only give the sketch of the proof, but leave the detailed proof in our Appendixes. To sketch the security proof for the n -photon case, we begin from the single-photon case for the ease of reading, though a proof for this case has been given in [25]. In the single-photon case the state sent from Alice is $|\psi_1\rangle = \sum_{m=1}^L i^{k_m} |m\rangle$. The general collective attack can be given as $U_{\text{Eve}} |m\rangle |e_{0|0}\rangle = \sum_{j=1}^L c_{m|j} |j\rangle |e_{m|j}\rangle$, where the state of Eve's ancilla $|e_{m|j}\rangle$ corresponds to Eve's transformation from $|m\rangle$ to $|j\rangle$ which will be sent to Bob. After Bob's projection to the a th and b th pulses, the terms of $|e_{m|j}\rangle$ ($j \neq a, b$) become irrelevant for guessing the key bit. It is worth noting that Eve cannot get any information from the terms of $|e_{m|a}\rangle$ ($|e_{m|b}\rangle$) for $m \neq a, b$ because the phase encoding bits $k_{m \neq a, b} \in \{0, 1, 2, 3\}$ are randomly selected and never disclosed by Alice. After the disclosing of bases, Eve's information can be estimated by a Holevo bound for the X and Y bases, respectively. Then the average information Eve can get is the mean of the information for the X and Y bases, which is

$$I_{AE} \leq \varphi[(L-1)x_1, x_2]/(L-1), \quad (4)$$

where $\varphi(x, y) = -x \log_2 x - y \log_2 y + (x+y) \log_2(x+y)$. Here $x_1 = \sum_m c_{m|m}^2$, $x_2 = \sum_{m \neq n} c_{m|n}^2$ satisfying $0 \leq x_1 \leq 1$, $0 \leq x_2 \leq 1$ and $x_1 + x_2 = 1$. x_1 and x_2 depend on the attack Eve conducts. So for all attacks we have the upper bound of Eve's information $I_{AE}^U = \max_{x_1, x_2} \varphi[(L-1)x_1, x_2]/(L-1)$. Furthermore, the bit error rate of key bits E can also be related to x 's, namely $E \geq \frac{1}{2}x_2$. Then we can get the information of Eve at the condition of error rate E . The detailed security proof can be seen in Appendix A.

With a similar method we can get the security proof of the two-photon case, which is present in Appendix B. The key point is that the variables $c_{m|j}$ in the single-photon case become $c_{mm|j}$ because we must analyze Eve's transformation from $|mn\rangle$ to $|j\rangle$ in the two-photon case. Of course, this leads to a complicated form of I_{AE} , namely,

$$I_{AE} \leq \frac{\varphi[(L-1)x_1 + x_2, x_3] + \varphi[(L-2)x_3, 2x_4]}{L-1}, \quad (5)$$

$$E \geq \frac{(\sqrt{(L-1)x_1} - \sqrt{x_3})^2 + (L-1)x_2 + (L-1)x_4}{2(L-1)}. \quad (6)$$

Here $x_1 = \sum_m c_{mm|m}^2$, $x_2 = \sum_{m \neq n} c_{mm|n}^2$, $x_3 = \sum_{m \neq n} c_{mn|m}^2$, and $x_4 = \sum_{m < n; p \neq m, n} c_{mn|p}^2$. The nonnegative x 's satisfy $x_1 + x_2 + x_3 + x_4 = 1$.

According to the examples of the single-photon and two-photon cases, it is easy to see that I_{AE} and E can be fully characterized by a set of variables x 's, and its size becomes larger when the photon number increases. Actually, in Appendix C we give the security proof for the three-photon case and seven x 's should be used.

Finally, we give the security proof for the n -photon case in Appendix E. The result is complex and we only give the form here, which is shown as

$$I_{AE} \leq \frac{1}{L-1} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 < n}} f_\varphi(M, n), \quad (7)$$

$$E \geq \frac{1}{2(L-1)} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n}} f_E(M, n). \quad (8)$$

Here f_φ and f_E are expressions about the x 's (please see Appendix E for details). $M = [M_1, M_2, M_3]$ means that there are M_i pulses containing $i + 4p$ ($p = 0, 1, 2, \dots$) photons in the $L - 2$ pulses (the a th and the b th pulses are excluded). Though the photon number n_j of the j th pulse can be larger than 3, the phase modulation $i^{n_j k_j}$ equals $i^{(n_j-4)k_j}$. So the behaviors of 5, 9, 13, ... photon pulses are the same as the behavior of the one-photon pulses. Therefore, the three elements of M are enough to represent the pulses of any photon number.

To calculate the upper bound of Eve's information, one can refer to Eqs. (E37) and (E51) in Appendix E to see the expression of f_φ and f_E . Then, for a given photon number n , Eqs. (7) and (8) become expressions about x 's. The parameters named as x have three restrictions. First, the summation of all x 's equals 1. Second, for a given error rate E , Eq. (8) should be satisfied. Third, the x 's are all nonnegative. Under these three restrictions, one can find a group of x 's reaching the maximum of Eq. (7).

IV. DISCUSSION

In this discussion, we first compare our results with the existing security proof to check the validity of the results and then focus on the performance of RRDQPS with practical WCP.

As a generalized security proof, it is natural to compare our results with the existing proof for the single-photon case in [25]. Eve's information and the bit error rate obtained in [25] are shown as $I_{AE} \leq \max_{x_{1,2,3,4}} [\varphi(x_1, x_2/(L-1)) + \varphi(x_3/(L-1), x_4)]$ and $E = (x_2 + x_3)/2 + x_4$ for the single-photon case. Here nonnegative x_1, x_2, x_3 , and x_4 satisfy $x_1 + x_2 + x_3 + x_4 = 1$. Though our result has different forms, these results are equivalent because the maximum of I_{AE} , i.e., I_{AE}^U always holds when $x_3 = x_4 = 0$ (if E is involved) or $x_2/x_3 = x_1/x_4$ (if E is not involved or E is large enough to have no restriction on the x 's). When $x_2/x_3 = x_1/x_4$, I_{AE} in [25] is given by

$$\begin{aligned} & \varphi[x_1, x_2/(L-1)] + \varphi[x_3/(L-1), x_4] \\ &= \varphi[x_1 + x_4, (x_2 + x_3)/(L-1)] \\ &= \varphi[(L-1)(x_1 + x_4), x_2 + x_3]/(L-1), \end{aligned} \quad (9)$$

which equals our result when E is not involved. When E is involved, we have $x_3 = x_4 = 0$, so our results are also the same.

In the following, with our security proof, a detailed comparison between RRDPS and RRDQPS can be made.

First, when E is not used to get I_{AE} , our result shows that RRDPS and RRDQPS protocols have a same upper bound I_{AE}^U .

TABLE I. Maximum error rate when only n -photon packets are used and $L = 8$.

n	RRDPS without E	RRDPS with E	RRDQPS with E
1	17.63%	19.13%	19.93%
2	8.58%	9.69%	10.56%
3	3.92%	4.73%	6.08%
4	1.51%	2.02%	3.80%

So there is no advantage for RRDQPS protocol without error monitoring. In the following, we will discuss the difference when E is involved.

Let us begin with the maximum tolerable error rate E_{\max} , defined by $I_{AE}^U(E_{\max}) = 1 - H_2(E_{\max})$, where $H_2(x) = -x \log_2 x - (1-x) \log_2(1-x)$ is the binary Shannon entropy function. In Table I, we list E_{\max} for each protocol when only n -photon packets are used and when $L = 8$. We can see the RRDQPS protocol has an advantage over the RRDPS protocol, especially when photon number n is large.

Then we will use our result on the WCP source QKD scheme to show its improvement. For a WCP source with phase randomization between packets, the probability of producing an n -photon packet is shown as

$$p(n) = \frac{(L\mu)^n e^{-L\mu}}{n!}, \quad (10)$$

where μ is the average photon number of a pulse.

When the pulse delay r is selected, only $(L-r)$ detecting windows are opened, so the counting rate is

$$Q^{(r)} = (1-d)^{2(L-r)-1} e^{-(L-r)\eta\mu} [(L-r)\eta\mu + 2(L-r)d], \quad (11)$$

where d is the dark counting rate of two detectors of Bob. η is the transmission efficiency from Alice to Bob, and the detecting efficiency is also included in it. For all $r \in \{1, 2, \dots, L-1\}$, the total counting rate is $Q = \sum_{r=1}^{L-1} Q^{(r)}/(L-1)$.

The bit error rate E is shown as

$$\begin{aligned} EQ &= \sum_{r=1}^{L-1} \frac{1}{L-1} (1-d)^{2(L-r)-1} e^{-(L-r)\eta\mu} \\ &\quad \times [(L-r)\eta\mu e_{\text{mis}} + (L-r)d], \end{aligned} \quad (12)$$

where e_{mis} is the probability that an incident photon clicks an erroneous detector due to interferometer misalignment.

If Bob knows the ratio of his clicks from single-photon packets, from two-photon packets, and so on, the secret key rate per pulse R is given by

$$2RL = Q[1 - H_2(E)] - [Q_1 I_{AE_1}^U(E_1) + Q_2 I_{AE_2}^U(E_2) + \dots], \quad (13)$$

where $H_2(x) = -x \log_2 x - (1-x) \log_2(1-x)$ is the binary Shannon entropy function. Q_n is the counting rate and E_n is the error rate for the n -photon packet. $I_{AE_n}^U$ means the maximum of I_{AE} when the photon number is n . However, Q_n and E_n are unknown to Alice and Bob.

We assume that when the photon number is larger than ν_{th} , no security key can be produced, so the optimal attack for Eve is that all packets with photon number larger than ν_{th} are sent

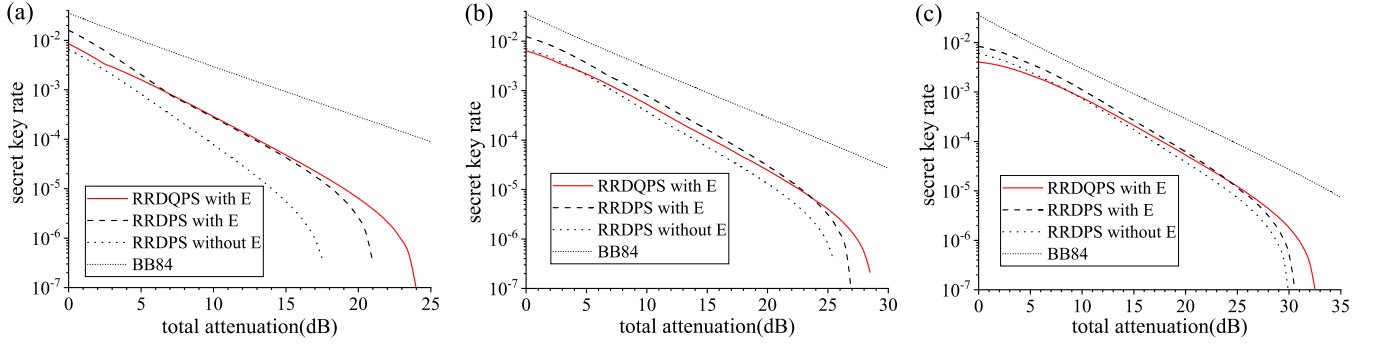


FIG. 1. The simulation results of secret key rate when $e_{\text{mis}} = 0.015$, $d = 10^{-6}$. And for (a), (b) and (c), $L = 4, 8, 16$ separately.

to Bob without attenuation, which means

$$\sum_{k=1}^{\infty} Q_{v_{th}+k} I_{AE_{v_{th}+k}}^U(E_{v_{th}+k}) \leq e_{\text{src}}, \quad (14)$$

where $e_{\text{src}} = 1 - \sum_{n=0}^{v_{th}} \frac{e^{-L\mu} (L\mu)^n}{n!}$. When the equality holds we have

$$\sum_{n=0}^{v_{th}} Q_n = Q - e_{\text{src}}. \quad (15)$$

Then we can obtain

$$\begin{aligned} \sum_{n=1}^{\infty} Q_n I_{AE_n}^U(E_n) &\leq \sum_{n=1}^{v_{th}} Q_n I_{AE_n}^U(E_n) + e_{\text{src}} \\ &\leq \sum_{n=0}^{v_{th}} Q_n I_{AE_{v_{th}}}^U(E_n) + e_{\text{src}} \\ &\leq \left(\sum_{n=0}^{v_{th}} Q_n \right) I_{AE_{v_{th}}}^U \left(\frac{\sum_{n=0}^{v_{th}} Q_n E_n}{\sum_{n=0}^{v_{th}} Q_n} \right) + e_{\text{src}} \\ &\leq (Q - e_{\text{src}}) I_{AE_{v_{th}}}^U \left(\frac{QE}{Q - e_{\text{src}}} \right) + e_{\text{src}}. \end{aligned} \quad (16)$$

Here we used the concavity of $I_{AE_{v_{th}}}^U(E)$, which is proven in Appendix F. When $m \leq n$, $I_{AE_m}^U(E) \leq I_{AE_n}^U(E)$ is obvious.

So we have

$$2RL \geq Q[1 - H_2(E)] - e_{\text{src}} - (Q - e_{\text{src}}) I_{AE_{v_{th}}}^U \left(\frac{QE}{Q - e_{\text{src}}} \right). \quad (17)$$

Then we can optimize μ and v_{th} to get the largest R .

We simulated the key rates (per pulse) when $L = 4, 8, 16$, which are shown in Fig. 1. We use the method in [16] to calculate the key rates of the RRDPS protocol. The key rates for phase-encoding BB84 are also simulated for comparison. In the simulation, we set $e_{\text{mis}} = 0.015$ and $d = 10^{-6}$. When attenuation is small, the RRDQPS protocol has no advantage because of the $1/2$ coefficient from bases correcting. But when attenuation is large, the RRDQPS protocol overwhelms RRDPS and has a longer transmission distance. We can see that RRDQPS protocol has more advantage when L is small.

We also simulated the key rate under high error rate, which is shown in Fig. 2. The parameters are set to be $L = 8$, $e_{\text{mis}} = 0.175$, and $d = 10^{-6}$. No keys can be produced under this error rate by the BB84 protocol, while RRDPS and RRDQPS can still work. Larger key rates can be achieved by the RRDQPS protocol on this condition, which means the RRDQPS protocol has a higher error tolerance than the RRDPS protocol.

Compared with the well-known BB84 protocol, we can see that higher error tolerance is a distinct advantage for the RRDQPS protocol. The BB84 protocol must use decoy states to have a long transmission distance. However, decoy states are not needed in the RRDQPS protocol. Thus high speed intensity modulators are not needed. Some potential loopholes might be avoided. Therefore, in some high noise channels, the RRDQPS protocol can be a good alternative.

Finally, we must stress that it is not restrictive to extend the proof to be against coherent attack, though it is present at the condition of collective attack. Indeed, with the quantum de Finetti theorem [26,27] or postselection technique [28], the security proof for a discrete-variable QKD protocol against collective attack can also hold when coherent attacks are conducted, provided an additional reduction of the key size is performed.

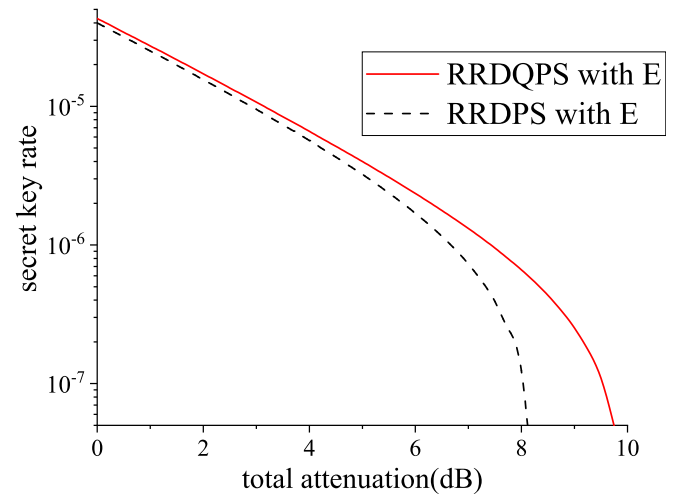


FIG. 2. The simulation results of secret key rate when $L = 8$, $e_{\text{mis}} = 0.175$, and $d = 10^{-6}$. BB84 protocol and RRDPS protocol without monitoring error rate cannot work on this condition.

V. SUMMARY

To summarize, we give a security proof for the RRDQPS protocol and conduct a simulation to show its improvement.

The RRDQPS and RRDPS protocols can run without monitoring error rates, but RRDQPS has no advantage on this condition. When error rate is considered, the RRDQPS and RRDPS protocols can also run without decoy states. On this condition, a longer transmission distance can be achieved by the RRDQPS protocol.

In our simulation, we show that at long distance, the RRDQPS protocol has a higher key rate than RRDPS. The advantage is more notable when L is small. While in exper-

iment RRDPS or RRDQPS protocols with large L are hard to realize and the phase modulation from two phases to four phases is easy to achieve, RRDQPS could be a good method to improve transmission distance.

ACKNOWLEDGMENTS

This work was supported by the National Key Research and Development Program of China (Grant No. 2018YFA0306400), the National Natural Science Foundation of China (Grants No. 62171424, No. 61961136004, No. 61775207, and No. 61627820), and Anhui Initiative in Quantum Information Technologies.

APPENDIX A: SECURITY PROOF IN THE SINGLE-PHOTON CASE

Alice randomly prepares the single photon state $|\psi\rangle = \sum_{m=1}^L i^{k_m} |m\rangle$, where i is the imaginary unit, $k_m \in \{0, 1, 2, 3\}$ is Alice's random phase modulation, and $|m\rangle$ ($m \in \{1, \dots, L\}$) represents that a single photon is in the m th time bin. Eve's general collective attack can be given by

$$U_{\text{Eve}} |m\rangle |e_{0|0}\rangle = \sum_j^L c_{m|j} |j\rangle |e_{m|j}\rangle = \sum_j^L \tilde{C}_{m|j} |j\rangle, \tag{A1}$$

where $|e_{m|j}\rangle$ is the quantum state of Eve's ancilla. We denote $c_{m|j} |e_{m|j}\rangle$ as $\tilde{C}_{m|j}$.

After the measurement of Bob, Bob's state will be projected to $(|a\rangle \pm |b\rangle)/\sqrt{2}$ (X basis) or $(|a\rangle \pm i|b\rangle)/\sqrt{2}$ (Y basis). Eve can know Bob's basis information which is disclosed after Bob's measurement. Thus we can analyze the X -basis and Y -basis cases separately.

If Bob projects the state into the a th and b th time bins, the state of Eve's ancilla and Bob's photon will become

$$U_{\text{Eve}} |\psi\rangle |e_{0|0}\rangle \longrightarrow i^{k_a} (\tilde{C}_{a|a} |a\rangle + \tilde{C}_{b|a} |b\rangle) + i^{k_b} (\tilde{C}_{b|a} |a\rangle + \tilde{C}_{b|b} |b\rangle) + \sum_{m \neq a,b} i^{k_m} (\tilde{C}_{m|a} |a\rangle + \tilde{C}_{m|b} |b\rangle). \tag{A2}$$

If Bob projects to the X basis, the state of Eve is a mixed state of two states when Alice prepares $(|a\rangle + |b\rangle)/\sqrt{2}$ or $(|a\rangle - |b\rangle)/\sqrt{2}$. Eve's state of $(|a\rangle + |b\rangle)/\sqrt{2}$ is from the state Eq. (A2) when $k_a = k_b$ and we calculate the mean for $k_m = 0, 1, 2, 3$ ($m \neq a, b$), which are randomly selected and unknown to Eve:

$$\rho_{xs} = \left[P\{\tilde{C}_{a|a} + \tilde{C}_{b|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{m|a}\} \right] + \left[P\{\tilde{C}_{a|b} + \tilde{C}_{b|b}\} + \sum_{m \neq a,b} P\{\tilde{C}_{m|b}\} \right] = P\{\tilde{C}_{a|a} + \tilde{C}_{b|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{m|a}\} + \text{Part}\{b\}. \tag{A3}$$

We see two similar parts with the only difference of the last subscript a and b of \tilde{C} . So we denote the second part with subscript b as $\text{Part}\{b\}$. We also define $P\{|a\rangle\} = |a\rangle \langle a|$.

Eve's state of $(|a\rangle - |b\rangle)/\sqrt{2}$ is

$$\rho_{xd} = P\{\tilde{C}_{a|a} - \tilde{C}_{b|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{m|a}\} + \text{Part}\{b\}. \tag{A4}$$

For the Y basis, Eve's state of $(|a\rangle + i|b\rangle)/\sqrt{2}$ is

$$\rho_{ys} = P\{\tilde{C}_{a|a} + i\tilde{C}_{b|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{m|a}\} + \text{Part}\{b\}. \tag{A5}$$

In addition, Eve's state of $(|a\rangle - i|b\rangle)/\sqrt{2}$ is

$$\rho_{yd} = P\{\tilde{C}_{a|a} - i\tilde{C}_{b|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{m|a}\} + \text{Part}\{b\}. \tag{A6}$$

Without compromising the security, we assume that $\langle e_{k|m} | e_{l|n} \rangle = \delta_{kl} \delta_{mn}$. Then Eve's information of the X basis can be given by the Holevo bound, which is

$$\begin{aligned} Q_x^{(a,b)} I_{AE_x}^{(a,b)} &\leq S\left(\frac{1}{2}\rho_{xs} + \frac{1}{2}\rho_{xd}\right) - \left(\frac{1}{2}S(\rho_{xs}) + \frac{1}{2}S(\rho_{xd})\right) \\ &= -c_{a|a}^2 \log_2 c_{a|a}^2 - c_{b|a}^2 \log_2 c_{b|a}^2 + (c_{a|a}^2 + c_{b|a}^2) \log_2 (c_{a|a}^2 + c_{b|a}^2) + \text{Part}\{b\} \\ &= \varphi(c_{a|a}^2, c_{b|a}^2) + \varphi(c_{a|b}^2, c_{b|b}^2), \end{aligned} \tag{A7}$$

where $S(\rho)$ is the von Neumann entropy of state ρ and $\varphi(x, y) = -x \log_2 x - y \log_2 y + (x + y) \log_2(x + y)$. $Q_x^{(a,b)}$ is the yield when Bob uses the X basis and projects to the a th and b th time bins.

Similarly, we have $Q_y^{(a,b)} I_{AE_y}^{(a,b)} \leq \varphi(c_{a|a}^2, c_{b|a}^2) + \varphi(c_{a|b}^2, c_{b|b}^2)$ and here $\frac{1}{2}(Q_x^{(a,b)} + Q_y^{(a,b)}) = \sum_m (c_{m|a}^2 + c_{m|b}^2)$.

Then we can get the ratio of Eve's information,

$$\begin{aligned} I_{AE} &= \frac{\frac{1}{2} \sum_{a<b} (Q_x^{(a,b)} I_{AE_x}^{(a,b)} + Q_y^{(a,b)} I_{AE_y}^{(a,b)})}{\frac{1}{2} \sum_{a<b} (Q_x^{(a,b)} + Q_y^{(a,b)})} \leq \frac{\sum_{a<b} [\varphi(c_{a|a}^2, c_{b|a}^2) + \varphi(c_{a|b}^2, c_{b|b}^2)]}{\sum_{a<b} \sum_m (c_{m|a}^2 + c_{m|b}^2)} \\ &\leq \frac{\varphi(\sum_{a<b} (c_{a|a}^2 + c_{b|b}^2), \sum_{a<b} (c_{b|a}^2 + c_{a|b}^2))}{\sum_{a<b} \sum_m (c_{m|a}^2 + c_{m|b}^2)} = \frac{\varphi[(L-1)x_1, x_2]}{L-1}. \end{aligned} \quad (\text{A8})$$

Here we used the inequality $\varphi(a, b) + \varphi(c, d) \leq \varphi(a + c, b + d)$, which is because $\varphi(x, y) = (x + y)H_2(\frac{x}{x+y})$ where $H_2(x) = -x \log_2 x - (1-x) \log_2(1-x)$ is the binary entropy function and H_2 is concave. Because $\varphi(ax, ay) = (ax + ay)H_2(\frac{x}{x+y}) = a\varphi(x, y)$, we can set $\sum_{m,n} c_{m|n}^2 = 1$ without loss of generality.

Here $x_1 = \sum_m c_{m|m}^2$, $x_2 = \sum_{m \neq n} c_{m|n}^2$, $x_1 + x_2 = 1$. The x 's are nonnegative. The x 's are also restricted by the error rate of the sifted keys. Then we give the error rate.

From Eq. (A2), we can obtain the rates that Bob gets $(|a\rangle - |b\rangle)/\sqrt{2}$ when $k_a = k_b$ and gets $(|a\rangle + |b\rangle)/\sqrt{2}$ when $k_a = k_b + 2 \pmod{4}$. They are errors of the X basis, which are

$$Q_{xs}^{(a,b)} E_{xs}^{(a,b)} = \frac{1}{2} \left(|\tilde{C}_{a|a} - \tilde{C}_{a|b} + \tilde{C}_{b|a} - \tilde{C}_{b|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{m|a} - \tilde{C}_{m|b}|^2 \right), \quad (\text{A9})$$

$$Q_{xd}^{(a,b)} E_{xd}^{(a,b)} = \frac{1}{2} \left(|\tilde{C}_{a|a} + \tilde{C}_{a|b} - \tilde{C}_{b|a} - \tilde{C}_{b|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{m|a} + \tilde{C}_{m|b}|^2 \right). \quad (\text{A10})$$

Here we calculated the mean for $k_m = 0, 1, 2, 3$ ($m \neq a, b$).

We can also get the errors that Bob gets $(|a\rangle - i|b\rangle)/\sqrt{2}$ when $k_b = k_a + 1 \pmod{4}$ and gets $(|a\rangle + i|b\rangle)/\sqrt{2}$ when $k_b = k_a + 3 \pmod{4}$. They are

$$Q_{ys}^{(a,b)} E_{ys}^{(a,b)} = \frac{1}{2} \left(|\tilde{C}_{a|a} + i\tilde{C}_{a|b} + i\tilde{C}_{b|a} - \tilde{C}_{b|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{m|a} + i\tilde{C}_{m|b}|^2 \right), \quad (\text{A11})$$

$$Q_{yd}^{(a,b)} E_{yd}^{(a,b)} = \frac{1}{2} \left(|\tilde{C}_{a|a} - i\tilde{C}_{a|b} - i\tilde{C}_{b|a} - \tilde{C}_{b|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{m|a} - i\tilde{C}_{m|b}|^2 \right). \quad (\text{A12})$$

The overall error is the mean from Eqs. (A9) to (A12) for all a and b , which is

$$EQ = \sum_{a<b} \frac{1}{2} \left[|\tilde{C}_{a|a} - \tilde{C}_{b|b}|^2 + |\tilde{C}_{a|b}|^2 + |\tilde{C}_{b|a}|^2 + \sum_{m \neq a,b} (|\tilde{C}_{m|a}|^2 + |\tilde{C}_{m|b}|^2) \right] \geq \frac{1}{2} [0 + x_2 + (L-2)x_2] = \frac{1}{2} (L-1)x_2. \quad (\text{A13})$$

Here $Q = \frac{1}{2} \sum_{a<b} (Q_x^{(a,b)} + Q_y^{(a,b)}) = L-1$, so we can get

$$E \geq \frac{1}{2} x_2. \quad (\text{A14})$$

Finally, we can get a bound of I_{AE} with Eq. (A8), Eq. (A14), and $x_1 + x_2 = 1$, $x_1 \geq 0$, $x_2 \geq 0$.

APPENDIX B: SECURITY PROOF IN THE TWO-PHOTON CASE

Alice randomly prepares the two-photon state $|\psi\rangle = \sum_{m=1}^L (-1)^{k_m} |mm\rangle + \sum_{1 \leq m < n \leq L} i^{k_m+k_n} |mn\rangle$, where $k_m, k_n \in \{0, 1, 2, 3\}$ are Alice's random phase modulations and $|mn\rangle$ represents that there are two photons in a packet; they are in the m th and n th time bins, respectively. Eve's general collective attack can be shown as

$$U_{\text{Eve}} |mn\rangle |e_{00}\rangle = \sum_{l=1}^L c_{mn|l} |l\rangle |e_{mn|l}\rangle = \sum_{l=1}^L \tilde{C}_{mn|l} |l\rangle. \quad (\text{B1})$$

Note that the realistic state should be $|\psi\rangle = \sum_m^L (-1)^m |mm\rangle + \sqrt{2} \sum_{1 \leq m < n \leq L} i^{k_m+k_n} |mn\rangle$. But the constant coefficients can be absorbed into $c_{mn|l}$ s, so we just ignore them (the same for our three-photon case and the n -photon case).

If Bob projects the state into the a th and b th time bins, the state of Eve’s ancilla and Bob’s photon will become

$$\begin{aligned}
 U_{\text{Eve}} |\psi\rangle |e_{00}\rangle &\longrightarrow (-1)^{k_a} (\tilde{C}_{aa|a} |a\rangle + \tilde{C}_{aa|b} |b\rangle) + (-1)^{k_b} (\tilde{C}_{bb|a} |a\rangle + \tilde{C}_{bb|b} |b\rangle) \\
 &+ \sum_{m \neq a,b} (-1)^{k_m} (\tilde{C}_{mm|a} |a\rangle + \tilde{C}_{mm|b} |b\rangle) + i^{k_a+k_b} (\tilde{C}_{ab|a} |a\rangle + \tilde{C}_{ab|b} |b\rangle) \\
 &+ \sum_{m < n; m,n \neq a,b} i^{k_m+k_n} (\tilde{C}_{mn|a} |a\rangle + \tilde{C}_{mn|b} |b\rangle) + \sum_{m \neq a,b} i^{k_m} [i^{k_a} (\tilde{C}_{ma|a} |a\rangle + \tilde{C}_{ma|b} |b\rangle) + i^{k_b} (\tilde{C}_{mb|a} |a\rangle + \tilde{C}_{mb|b} |b\rangle)].
 \end{aligned} \tag{B2}$$

If Bob projects to the X basis, the state of Eve is a mixed state of two states when Alice prepares $(|a\rangle + |b\rangle)/\sqrt{2}$ or $(|a\rangle - |b\rangle)/\sqrt{2}$. Eve’s state of $(|a\rangle + |b\rangle)/\sqrt{2}$ is

$$\rho_{xs} = P\{\tilde{C}_{aa|a} + \tilde{C}_{bb|a} + \tilde{C}_{ab|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{mm|a}\} + \sum_{m < n; m,n \neq a,b} P\{\tilde{C}_{mn|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{ma|a} + \tilde{C}_{mb|a}\} + \text{Part}\{b\}. \tag{B3}$$

Here we calculated the mean for $k_m = 0, 1, 2, 3$ ($m \neq a, b$).

Eve’s state of $(|a\rangle - |b\rangle)/\sqrt{2}$ is

$$\rho_{xd} = P\{\tilde{C}_{aa|a} + \tilde{C}_{bb|a} - \tilde{C}_{ab|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{mm|a}\} + \sum_{m < n; m,n \neq a,b} P\{\tilde{C}_{mn|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{ma|a} - \tilde{C}_{mb|a}\} + \text{Part}\{b\}. \tag{B4}$$

For the Y basis, Eve’s state of $(|a\rangle + i|b\rangle)/\sqrt{2}$ is

$$\rho_{ys} = P\{\tilde{C}_{aa|a} - \tilde{C}_{bb|a} + i\tilde{C}_{ab|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{mm|a}\} + \sum_{m < n; m,n \neq a,b} P\{\tilde{C}_{mn|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{ma|a} + i\tilde{C}_{mb|a}\} + \text{Part}\{b\}. \tag{B5}$$

Also Eve’s state of $(|a\rangle - i|b\rangle)/\sqrt{2}$ is

$$\rho_{yd} = P\{\tilde{C}_{aa|a} - \tilde{C}_{bb|a} - i\tilde{C}_{ab|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{mm|a}\} + \sum_{m < n; m,n \neq a,b} P\{\tilde{C}_{mn|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{ma|a} - i\tilde{C}_{mb|a}\} + \text{Part}\{b\}. \tag{B6}$$

For the X basis, the Holevo bound of Eve’s information is

$$Q_x^{(a,b)} I_{AE_x}^{(a,b)} \leq \varphi(|\tilde{C}_{aa|a} + \tilde{C}_{bb|a}|^2, |\tilde{C}_{ab|a}|^2) + \varphi(|\tilde{C}_{aa|b} + \tilde{C}_{bb|b}|^2, |\tilde{C}_{ab|b}|^2) + \sum_{m \neq a,b} [\varphi(|\tilde{C}_{ma|a}|^2, |\tilde{C}_{mb|a}|^2) + \varphi(|\tilde{C}_{ma|b}|^2, |\tilde{C}_{mb|b}|^2)]. \tag{B7}$$

In addition, for the Y basis, the Holevo bound of Eve’s information is

$$Q_y^{(a,b)} I_{AE_y}^{(a,b)} \leq \varphi(|\tilde{C}_{aa|a} - \tilde{C}_{bb|a}|^2, |\tilde{C}_{ab|a}|^2) + \varphi(|\tilde{C}_{aa|b} - \tilde{C}_{bb|b}|^2, |\tilde{C}_{ab|b}|^2) + \sum_{m \neq a,b} [\varphi(|\tilde{C}_{ma|a}|^2, |\tilde{C}_{mb|a}|^2) + \varphi(|\tilde{C}_{ma|b}|^2, |\tilde{C}_{mb|b}|^2)]. \tag{B8}$$

Then Eve’s information is

$$\begin{aligned}
 Q_{I_{AE}} &= \sum_{a < b} \frac{1}{2} (Q_x^{(a,b)} I_{AE_x}^{(a,b)} + Q_y^{(a,b)} I_{AE_y}^{(a,b)}) \\
 &\leq \sum_{a < b} \left(\varphi(c_{aa|a}^2 + c_{bb|a}^2 + c_{aa|b}^2 + c_{bb|b}^2, c_{ab|a}^2 + c_{ab|b}^2) + \sum_{m \neq a,b} \varphi(c_{ma|a}^2 + c_{mb|b}^2, c_{mb|a}^2 + c_{ma|b}^2) \right) \\
 &\leq \varphi \left(\sum_{a < b} c_{aa|a}^2 + c_{bb|a}^2 + c_{aa|b}^2 + c_{bb|b}^2, \sum_{a < b} c_{ab|a}^2 + c_{ab|b}^2 \right) + \varphi \left(\sum_{a < b} \sum_{m \neq a,b} c_{ma|a}^2 + c_{mb|b}^2, \sum_{a < b} \sum_{m \neq a,b} c_{mb|a}^2 + c_{ma|b}^2 \right) \\
 &= \varphi((L-1)x_1 + x_2, x_3) + \varphi((L-2)x_3, 2x_4).
 \end{aligned} \tag{B9}$$

Here we have

$$x_1 = \sum_m c_{mm|m}^2, \quad x_2 = \sum_{m \neq n} c_{mm|n}^2, \quad x_3 = \sum_{m \neq n} c_{mn|m}^2, \quad x_4 = \sum_{m < n; p \neq m,n} c_{mn|p}^2. \tag{B10}$$

And here

$$Q = \sum_{a < b} \sum_{m \leq n} (c_{mn|a}^2 + c_{mn|b}^2) = (L-1)(x_1 + x_2 + x_3 + x_4) = L-1. \tag{B11}$$

We have

$$I_{AE} \leq \frac{\varphi[(L-1)x_1 + x_2, x_3] + \varphi[(L-2)x_3, 2x_4]}{L-1}. \tag{B12}$$

Then we give the error rate from Eq. (B2).

We can get the rates that Bob gets $(|a\rangle - |b\rangle)/\sqrt{2}$ when $k_a = k_b$ and gets $(|a\rangle + |b\rangle)/\sqrt{2}$ when $k_a = k_b + 2 \pmod{4}$, which are

$$Q_{xs}^{(a,b)} E_{xs}^{(a,b)} = \frac{1}{2} \left\{ |\tilde{C}_{aa|a} - \tilde{C}_{aa|b} + \tilde{C}_{bb|a} - \tilde{C}_{bb|b} + \tilde{C}_{ab|a} - \tilde{C}_{ab|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{mm|a} - \tilde{C}_{mm|b}|^2 \right. \\ \left. + \sum_{m < n, m, n \neq a,b} |\tilde{C}_{mn|a} - \tilde{C}_{mn|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{ma|a} - \tilde{C}_{ma|b} + \tilde{C}_{mb|a} - \tilde{C}_{mb|b}|^2 \right\}, \tag{B13}$$

$$Q_{xd}^{(a,b)} E_{xd}^{(a,b)} = \frac{1}{2} \left\{ |\tilde{C}_{aa|a} + \tilde{C}_{aa|b} + \tilde{C}_{bb|a} + \tilde{C}_{bb|b} - \tilde{C}_{ab|a} - \tilde{C}_{ab|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{mm|a} + \tilde{C}_{mm|b}|^2 \right. \\ \left. + \sum_{m < n, m, n \neq a,b} |\tilde{C}_{mn|a} + \tilde{C}_{mn|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{ma|a} + \tilde{C}_{ma|b} - \tilde{C}_{mb|a} - \tilde{C}_{mb|b}|^2 \right\}. \tag{B14}$$

Here we calculated the mean for $k_m = 0, 1, 2, 3$ ($m \neq a, b$).

We can also get the errors that Bob gets $(|a\rangle - i|b\rangle)/\sqrt{2}$ when $k_b = k_a + 1 \pmod{4}$ and gets $(|a\rangle + i|b\rangle)/\sqrt{2}$ when $k_b = k_a + 3 \pmod{4}$, which are

$$Q_{ys}^{(a,b)} E_{ys}^{(a,b)} = \frac{1}{2} \left\{ |\tilde{C}_{aa|a} + i\tilde{C}_{aa|b} - \tilde{C}_{bb|a} - i\tilde{C}_{bb|b} + i\tilde{C}_{ab|a} - \tilde{C}_{ab|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{mm|a} + i\tilde{C}_{mm|b}|^2 \right. \\ \left. + \sum_{m < n, m, n \neq a,b} |\tilde{C}_{mn|a} + i\tilde{C}_{mn|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{ma|a} + i\tilde{C}_{ma|b} + i\tilde{C}_{mb|a} - \tilde{C}_{mb|b}|^2 \right\}. \tag{B15}$$

$$Q_{yd}^{(a,b)} E_{yd}^{(a,b)} = \frac{1}{2} \left\{ |\tilde{C}_{aa|a} - i\tilde{C}_{aa|b} - \tilde{C}_{bb|a} + i\tilde{C}_{bb|b} - i\tilde{C}_{ab|a} - \tilde{C}_{ab|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{mm|a} - i\tilde{C}_{mm|b}|^2 \right. \\ \left. + \sum_{m < n, m, n \neq a,b} |\tilde{C}_{mn|a} - i\tilde{C}_{mn|b}|^2 + \sum_{m \neq a,b} |\tilde{C}_{ma|a} - i\tilde{C}_{ma|b} - i\tilde{C}_{mb|a} - \tilde{C}_{mb|b}|^2 \right\}. \tag{B16}$$

The overall error is the mean from Eqs. (B13) to (B16) for all a and b , which is

$$EQ = \frac{1}{2} \sum_{a < b} \left\{ |\tilde{C}_{aa|a} - \tilde{C}_{ab|b}|^2 + |\tilde{C}_{bb|b} - \tilde{C}_{ab|a}|^2 + |\tilde{C}_{bb|a}|^2 + |\tilde{C}_{aa|b}|^2 \right. \\ \left. + \sum_{m \neq a,b} (|\tilde{C}_{mm|a}|^2 + |\tilde{C}_{mm|b}|^2) + \sum_{m < n, m, n \neq a,b} (|\tilde{C}_{mn|a}|^2 + |\tilde{C}_{mn|b}|^2) \right. \\ \left. + \sum_{m \neq a,b} (|\tilde{C}_{ma|a} - \tilde{C}_{mb|b}|^2 + |\tilde{C}_{ma|b}|^2 + |\tilde{C}_{mb|a}|^2) \right\}. \tag{B17}$$

Then we use the inequalities that $|\tilde{a} - \tilde{b}|^2 + |\tilde{x} - \tilde{y}|^2 \geq (\sqrt{a^2 + x^2} - \sqrt{b^2 + y^2})^2$ and $(\sqrt{a} - \sqrt{b})^2 + (\sqrt{x} - \sqrt{y})^2 \geq (\sqrt{a+x} - \sqrt{b+y})^2$. We have

$$EQ \geq \frac{1}{2} \left\{ \left(\sqrt{\sum_{a < b} (c_{aa|a}^2 + c_{bb|b}^2)} - \sqrt{\sum_{a < b} (c_{ab|b}^2 + c_{ab|a}^2)} \right)^2 + \sum_{a < b} (c_{bb|a}^2 + c_{aa|b}^2) \right. \\ \left. + \sum_{a < b} \sum_{m \neq a,b} (c_{mm|a}^2 + c_{mm|b}^2) + \sum_{a < b} \sum_{m < n, m, n \neq a,b} (c_{mn|a}^2 + c_{mn|b}^2) + \sum_{a < b} \sum_{m \neq a,b} (0 + c_{ma|b}^2 + c_{mb|a}^2) \right\} \\ = \frac{1}{2} [(\sqrt{(L-1)x_1} - \sqrt{x_3})^2 + x_2 + (L-2)x_2 + (L-3)x_4 + 2x_4] \\ = \frac{1}{2} [(\sqrt{(L-1)x_1} - \sqrt{x_3})^2 + (L-1)x_2 + (L-1)x_4]. \tag{B18}$$

Then

$$E \geq \frac{(\sqrt{(L-1)x_1} - \sqrt{x_3})^2 + (L-1)x_2 + (L-1)x_4}{2(L-1)}. \quad (\text{B19})$$

APPENDIX C: SECURITY PROOF IN THE THREE-PHOTON CASE

Alice randomly prepares the three-photon state $|\psi\rangle = \sum_{m=1}^L i^{3k_m} |mmm\rangle + \sum_{1 \leq m, n \leq L; m \neq n} i^{2k_m+k_n} |mmn\rangle + \sum_{1 \leq m < n < p \leq L} i^{k_m+k_n+k_p} |mnp\rangle$, where $k_m, k_n, k_p \in \{0, 1, 2, 3\}$ are Alice's random phase modulations and $|mnp\rangle$ represents that there are three photons in a packet, and they are in the m th, n th, and the p th time bins, respectively. Eve's general collective attack can be shown as

$$U_{\text{Eve}} |mnp\rangle |e_{000}\rangle = \sum_{l=1}^L c_{mnp|l} |l\rangle |e_{mnp|l}\rangle = \sum_{l=1}^L \tilde{C}_{mnp|l} |l\rangle. \quad (\text{C1})$$

If Bob projects the state into the a th and b th time bins, the state of Eve's ancilla and Bob's photon will become

$$\begin{aligned} U_{\text{Eve}} |\psi\rangle |e_{000}\rangle &\longrightarrow i^{3k_a} (\tilde{C}_{aaa|a} |a\rangle + \tilde{C}_{aaa|b} |b\rangle) + i^{3k_b} (\tilde{C}_{bbb|a} |a\rangle + \tilde{C}_{bbb|b} |b\rangle) + \sum_{m \neq a, b} i^{3k_m} (\tilde{C}_{mmm|a} |a\rangle + \tilde{C}_{mmm|b} |b\rangle) \\ &+ i^{2k_a+k_b} (\tilde{C}_{aab|a} |a\rangle + \tilde{C}_{aab|b} |b\rangle) + i^{k_a+2k_b} (\tilde{C}_{abb|a} |a\rangle + \tilde{C}_{abb|b} |b\rangle) \\ &+ \sum_{m \neq a, b} i^{2k_m} [i^{k_a} (\tilde{C}_{amm|a} |a\rangle + \tilde{C}_{amm|b} |b\rangle) + i^{k_b} (\tilde{C}_{bmm|a} |a\rangle + \tilde{C}_{bmm|b} |b\rangle)] \\ &+ \sum_{m \neq a, b} i^{k_m} [i^{2k_a} (\tilde{C}_{aam|a} |a\rangle + \tilde{C}_{aam|b} |b\rangle) + i^{2k_b} (\tilde{C}_{bbm|a} |a\rangle + \tilde{C}_{bbm|b} |b\rangle)] \\ &+ \sum_{m, n \neq a, b; m \neq n} i^{2k_m+k_n} (\tilde{C}_{mmn|a} |a\rangle + \tilde{C}_{mmn|b} |b\rangle) + \sum_{m \neq a, b} i^{k_m+k_a+k_b} (\tilde{C}_{mab|a} |a\rangle + \tilde{C}_{mab|b} |b\rangle) \\ &+ \sum_{m, n \neq a, b; m < n} i^{k_m+k_n} [i^{k_a} (\tilde{C}_{mna|a} |a\rangle + \tilde{C}_{mna|b} |b\rangle) + i^{k_b} (\tilde{C}_{mnb|a} |a\rangle + \tilde{C}_{mnb|b} |b\rangle)] \\ &+ \sum_{m < n < p; m, n, p \neq a, b} i^{k_m+k_n+k_p} (\tilde{C}_{mnp|a} |a\rangle + \tilde{C}_{mnp|b} |b\rangle). \end{aligned} \quad (\text{C2})$$

If Bob projects to the X basis, the state of Eve is a mixed state of two states when Alice prepares $(|a\rangle + |b\rangle)/\sqrt{2}$ or $(|a\rangle - |b\rangle)/\sqrt{2}$. Eve's state of $(|a\rangle + |b\rangle)/\sqrt{2}$ is

$$\begin{aligned} \rho_{xs} &= P\{\tilde{C}_{aaa|a} + \tilde{C}_{bbb|a} + \tilde{C}_{aab|a} + \tilde{C}_{abb|a}\} + \sum_{m \neq a, b} P\{\tilde{C}_{mmm|a}\} + \sum_{m \neq a, b} P\{\tilde{C}_{amm|a} + \tilde{C}_{bmm|a}\} \\ &+ \sum_{m \neq a, b} P\{\tilde{C}_{aam|a} + \tilde{C}_{bbm|a} + \tilde{C}_{mab|a}\} + \sum_{m, n \neq a, b; m \neq n} P\{\tilde{C}_{mmn|a}\} \\ &+ \sum_{m < n; m, n \neq a, b} P\{\tilde{C}_{mna|a} + \tilde{C}_{mnb|a}\} + \sum_{m < n < p; m, n, p \neq a, b} \{\tilde{C}_{mnp|a}\} + \text{Part}\{b\}. \end{aligned} \quad (\text{C3})$$

Here we calculated the mean for $k_m = 0, 1, 2, 3$ ($m \neq a, b$).

And Eve's state of $(|a\rangle - |b\rangle)/\sqrt{2}$ is

$$\begin{aligned} \rho_{xd} &= P\{\tilde{C}_{aaa|a} - \tilde{C}_{bbb|a} - \tilde{C}_{aab|a} + \tilde{C}_{abb|a}\} + \sum_{m \neq a, b} P\{\tilde{C}_{mmm|a}\} + \sum_{m \neq a, b} P\{\tilde{C}_{amm|a} - \tilde{C}_{bmm|a}\} \\ &+ \sum_{m \neq a, b} P\{\tilde{C}_{aam|a} + \tilde{C}_{bbm|a} - \tilde{C}_{mab|a}\} + \sum_{m, n \neq a, b; m \neq n} P\{\tilde{C}_{mmn|a}\} \\ &+ \sum_{m < n; m, n \neq a, b} P\{\tilde{C}_{mna|a} - \tilde{C}_{mnb|a}\} + \sum_{m < n < p; m, n, p \neq a, b} \{\tilde{C}_{mnp|a}\} + \text{Part}\{b\}. \end{aligned} \quad (\text{C4})$$

For the Y basis, Eve's state of $(|a\rangle + i|b\rangle)/\sqrt{2}$ is

$$\begin{aligned} \rho_{ys} = & P\{\tilde{C}_{aaa|a} - i\tilde{C}_{bbb|a} + i\tilde{C}_{aab|a} - \tilde{C}_{abb|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{mmm|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{amm|a} + i\tilde{C}_{bmm|a}\} \\ & + \sum_{m \neq a,b} P\{\tilde{C}_{aam|a} - \tilde{C}_{bbm|a} + i\tilde{C}_{mab|a}\} + \sum_{m,n \neq a,b; m \neq n} P\{\tilde{C}_{mmn|a}\} \\ & + \sum_{m < n; m, n \neq a,b} P\{\tilde{C}_{mna|a} + i\tilde{C}_{mnb|a}\} + \sum_{m < n < p; m, n, p \neq a,b} \{\tilde{C}_{mnp|a}\} + \text{Part}\{b\}. \end{aligned} \quad (C5)$$

And Eve's state of $(|a\rangle - i|b\rangle)/\sqrt{2}$ is

$$\begin{aligned} \rho_{yd} = & P\{\tilde{C}_{aaa|a} + i\tilde{C}_{bbb|a} - i\tilde{C}_{aab|a} - \tilde{C}_{abb|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{mmm|a}\} + \sum_{m \neq a,b} P\{\tilde{C}_{amm|a} - i\tilde{C}_{bmm|a}\} \\ & + \sum_{m \neq a,b} P\{\tilde{C}_{aam|a} - \tilde{C}_{bbm|a} - i\tilde{C}_{mab|a}\} + \sum_{m,n \neq a,b; m \neq n} P\{\tilde{C}_{mmn|a}\} \\ & + \sum_{m < n; m, n \neq a,b} P\{\tilde{C}_{mna|a} - i\tilde{C}_{mnb|a}\} + \sum_{m < n < p; m, n, p \neq a,b} \{\tilde{C}_{mnp|a}\} + \text{Part}\{b\}. \end{aligned} \quad (C6)$$

For the X basis, the Holevo bound of Eve's information is

$$\begin{aligned} Q_x^{(a,b)} I_{AE_x}^{(a,b)} \leq & \varphi(|\tilde{C}_{aaa|a} + \tilde{C}_{abb|a}|^2, |\tilde{C}_{bbb|a} + \tilde{C}_{aab|a}|^2) + \sum_{m \neq a,b} \varphi(\tilde{C}_{amm|a}^2, \tilde{C}_{bmm|a}^2) \\ & + \sum_{m \neq a,b} \varphi(|\tilde{C}_{aam|a} + \tilde{C}_{bbm|a}|^2, \tilde{C}_{mab|a}^2) + \sum_{m < n; m, n \neq a,b} \varphi(\tilde{C}_{mna|a}^2, \tilde{C}_{mnb|a}^2) + \text{Part}\{b\}. \end{aligned} \quad (C7)$$

And for the Y basis, the Holevo bound of Eve's information is

$$\begin{aligned} Q_y^{(a,b)} I_{AE_y}^{(a,b)} \leq & \varphi(|\tilde{C}_{aaa|a} - \tilde{C}_{abb|a}|^2, |\tilde{C}_{bbb|a} - \tilde{C}_{aab|a}|^2) + \sum_{m \neq a,b} \varphi(\tilde{C}_{amm|a}^2, \tilde{C}_{bmm|a}^2) \\ & + \sum_{m \neq a,b} \varphi(|\tilde{C}_{aam|a} - \tilde{C}_{bbm|a}|^2, \tilde{C}_{mab|a}^2) + \sum_{m < n; m, n \neq a,b} \varphi(\tilde{C}_{mna|a}^2, \tilde{C}_{mnb|a}^2) + \text{Part}\{b\}. \end{aligned} \quad (C8)$$

Then Eve's information is

$$\begin{aligned} Q_{IAE} = & \sum_{a < b} \frac{1}{2} (Q_x^{(a,b)} I_{AE_x}^{(a,b)} + Q_y^{(a,b)} I_{AE_y}^{(a,b)}) \\ \leq & \sum_{a < b} \left[\varphi(c_{aaa|a}^2 + c_{bbb|b}^2 + c_{abb|a}^2 + c_{aab|b}^2, c_{bbb|a}^2 + c_{aaa|b}^2 + c_{aab|a}^2 + c_{abb|b}^2) + \sum_{m \neq a,b} \varphi(c_{amm|a}^2 + c_{bmm|b}^2, c_{bmm|a}^2 + c_{amm|b}^2) \right. \\ & \left. + \sum_{m \neq a,b} \varphi(c_{aam|a}^2 + c_{bbm|b}^2 + c_{bbm|a}^2 + c_{aam|b}^2, c_{mab|a}^2 + c_{mab|b}^2) + \sum_{m < n; m, n \neq a,b} \varphi(c_{mna|a}^2 + c_{mnb|b}^2, c_{mnb|a}^2 + c_{mna|b}^2) \right] \\ \leq & \varphi[(L-1)x_{(0,0,1,3)} + x_{(1,1,0,1)} + x_{(0,0,1,0)} + x_{(1,1,0,2)}] + \varphi[(L-2)x_{(1,1,0,1)} + x_{(1,1,0,0)}] \\ & + \varphi[(L-2)x_{(1,1,0,2)} + x_{(1,1,0,0)} + 2x_{(3,0,1,1)}] + \varphi[(L-3)x_{(3,0,1,1)} + 3x_{(3,0,0,0)}]. \end{aligned} \quad (C9)$$

Here we have

$$\begin{aligned} x_1 = & \sum_m c_{mmm|m}^2 = x_{(0,0,1,3)}, \quad x_2 = \sum_{m \neq n} c_{mmm|n}^2 = x_{(0,0,1,0)}, \quad x_3 = \sum_{m \neq n} c_{mmn|n}^2 = x_{(1,1,0,1)}, \\ x_4 = & \sum_{m \neq n} c_{mmn|m}^2 = x_{(1,1,0,2)}, \quad x_5 = \sum_{p \neq q; m \neq p, q} c_{pmm|q}^2 = x_{(1,1,0,0)}, \quad x_6 = \sum_{m < n; p \neq m, n} c_{mnp|p}^2 = x_{(3,0,0,1)}, \\ x_7 = & \sum_{m < n < p; q \neq m, n, p} c_{mnp|q}^2 = x_{(3,0,0,0)}. \end{aligned} \quad (C10)$$

The subscripts will be explained in Appendix D.

We have

$$I_{AE} \leq \frac{1}{L-1} (\varphi[(L-1)x_{([0,0,1],3)} + x_{([1,1,0],1)}, x_{([0,0,1],0)} + x_{([1,1,0],2)}] + \varphi[(L-2)x_{([1,1,0],1)}, x_{([1,1,0],0)}] + \varphi[(L-2)x_{([1,1,0],2)} + x_{([1,1,0],0)}, 2x_{([3,0,0],1)}] + \varphi[(L-3)x_{([3,0,0],1)}, 3x_{([3,0,0],0)}]). \quad (C11)$$

Then the error rate can also be given, which is

$$E \geq \frac{1}{2(L-1)} [(\sqrt{(L-1)x_{([0,0,1],3)}} - \sqrt{x_{([1,1,0],1)}})^2 + (\sqrt{(L-2)x_{([1,1,0],2)}} - \sqrt{2x_{([3,0,0],1)}})^2 + (L-2)x_{([0,0,1],0)} + (L-1)x_{([1,1,0],0)} + (L-1)x_{([3,0,0],0)}]. \quad (C12)$$

APPENDIX D: EXPLANATION OF SYMBOLS

In the next Appendix, we will give the security proof in the n -photon case. This section will describe the symbols we will use.

(1) We used the forms “ $\sum_{m<n;p \neq m,n} c_{mm|p}^2$ ” in Appendix B and “ $\sum_{m \neq n} c_{mmn|m}^2$ ” in Appendix C. We can forecast that we will use something like “ $\sum_{p<q;p,q \neq a} c_{ppqq|a}^2$ ” in the four-photon case. We denote “ $c_{mmn|m}$ ” as “ $c_{m_2 n|m}$ ”. Then we define $M = [M_1, M_2, M_3]$, where M_i means there are M_i pulses containing i photons. We define that $\sum_{M/a,b}$ means the summation of cases that the M_i 's traverse all combinations of L pulses except the a th and b th pulses. For example,

$$\sum_{\substack{q < r \\ p \neq q, r, s \\ s \neq q, r}}^L c_{p_3 q_2 r_2 s|a}^2 = \sum_M c_{M|a}^2, \quad (M = [1, 2, 1]), \quad (D1)$$

$$\sum_{\substack{q < r \\ p, q, r, s \neq a, b \\ p \neq q, r, s \\ s \neq q, r}}^L c_{p_3 q_2 r_2 s|a}^2 = \sum_{M/a,b} c_{M|a}^2, \quad (M = [1, 2, 1]), \quad (D2)$$

and, for example,

$$\sum_{\substack{p < q < r \\ p, q, r, s \neq a, b \\ s \neq p, q, r}}^L c_{p_2 q_2 r_2 s a_2 b|a}^2 = \sum_{M/a,b} c_{M a_2 b|a}^2, \quad (M = [1, 3, 0]). \quad (D3)$$

Similarly, we define

$$\sum_{p < q < r; s \neq p, q, r}^L i^{2k_p + 2k_q + 2k_r + k_s} |ppqrrs\rangle = \sum_M i^{k_M} |M\rangle, \quad (M = [1, 3, 0]). \quad (D4)$$

(2) We find that in the state vector the phase of $\tilde{C}_{p_5|a}$ is $i^{5k_p} = i^{k_p}$, where $k_p \in \{0, 1, 2, 3\}$ is Alice's phase modulation. It has a same phase as $\tilde{C}_{p_1|a}$ because $i^4 = 1$. So we use $\tilde{C}_{p_j|a}$, $j \in \{0, 1, 2, 3\}$ representing all $\tilde{C}_{p_{j+4n}|a}$, $l = 0, 1, 2, 3 \dots$ states. It is also the reason that we only define M_1, M_2 , and M_3 three elements in M .

(3) We used some x 's as some summation of c^2 's such as Eq. (B10), and now we rename them. We define

$$x_{[(M+m_k),k]} = \sum_{M/q} \sum_q c_{M q_k|q}^2, \quad (D5)$$

where the summation $\sum_{M/q}$ means M_i 's traverse all combinations of L pulses except the q th pulse. $M' = (M + m_k)$ means $M'_k = M_k + 1$ and $M'_i = M_i$ ($i \neq k$), i.e., $m_k = [\delta_{1k}, \delta_{2k}, \delta_{3k}]$.

For example, see Eq. (C10) which is

$$\begin{aligned} x_1 &= \sum_m c_{mmn|m}^2 = x_{([0,0,1],3)}, & x_2 &= \sum_{m \neq n} c_{mmn|n}^2 = x_{([0,0,1],0)}, & x_3 &= \sum_{m \neq n} c_{mmn|n}^2 = x_{([1,1,0],1)}, \\ x_4 &= \sum_{m \neq n} c_{mmn|m}^2 = x_{([1,1,0],2)}, & x_5 &= \sum_{p \neq q; m \neq p, q} c_{pmm|q}^2 = x_{([1,1,0],0)}, & x_6 &= \sum_{m < n; p \neq m, n} c_{mnp|p}^2 = x_{([3,0,0],1)}, \\ x_7 &= \sum_{m < n < p; q \neq m, n, p} c_{mnp|q}^2 = x_{([3,0,0],0)}. \end{aligned} \quad (D6)$$

(4) Define $z = n - (M_1 + 2M_2 + 3M_3)$, where n is the number of photons in a packet of L pulses.

APPENDIX E: SECURITY PROOF IN THE n -PHOTON CASE

First, we give the state Alice prepares, which is

$$|\psi\rangle = \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n \\ n - (M_1 + 2M_2 + 3M_3) = 0 \pmod{4}}} \sum_M i^{K_M} |M\rangle. \tag{E1}$$

Here $M = [M_1, M_2, M_3]$. There are $(L - M_1 - M_2 - M_3)$ pulses containing no photons or their photon numbers are multiples of 4.

Then we give the state of Eve’s ancilla and Bob’s photon after Eve’s attack and Bob’s projecting to the a th and b th time bins, which is

$$U_{\text{Eve}} |\psi\rangle |e_{0|0}\rangle \longrightarrow \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n}} \sum_{M/a,b} i^{K_M} \sum_{\substack{t=0 \\ z-t \geq 0}}^3 i^{k_a+(z-t)k_b} \tilde{C}_{M_a, b_{z-t}|a} |a\rangle + \text{Part}\{b\}. \tag{E2}$$

Here $z = n - (M_1 + 2M_2 + 3M_3)$.

For example, when $n = 2$, we have

$$\begin{aligned} M = [0, 0, 0], t = 0 &: i^{2k_b} (\tilde{C}_{bb|a} |a\rangle + \tilde{C}_{bb|b} |b\rangle), & M = [0, 0, 0], t = 1 &: i^{k_a+k_b} (\tilde{C}_{ab|a} |a\rangle + \tilde{C}_{ab|b} |b\rangle), \\ M = [0, 0, 0], t = 2 &: i^{2k_a} (\tilde{C}_{aa|a} |a\rangle + \tilde{C}_{aa|b} |b\rangle), & M = [1, 0, 0], t = 0 &: \sum_{p \neq a,b} i^{k_p} i^{k_b} (\tilde{C}_{pb|a} |a\rangle + \tilde{C}_{pb|b} |b\rangle), \\ M = [1, 0, 0], t = 1 &: \sum_{p \neq a,b} i^{k_p} i^{k_a} (\tilde{C}_{pa|a} |a\rangle + \tilde{C}_{pa|b} |b\rangle), & M = [0, 1, 0], t = 0 &: \sum_{p \neq a,b} i^{2k_p} (\tilde{C}_{pp|a} |a\rangle + \tilde{C}_{pp|b} |b\rangle), \\ M = [2, 0, 0], t = 0 &: \sum_{p < q, p, q \neq a,b} i^{k_p+k_q} (\tilde{C}_{pq|a} |a\rangle + \tilde{C}_{pq|b} |b\rangle), \end{aligned} \tag{E3}$$

which is the same as Eq. (B2).

1. I_{AE}

We can see that the $M_1 + 2M_2 + 3M_3 = n$ terms have no contributions to I_{AE} because no information about the a th and b th pulses is included in these terms. For example, from Eqs. (B3) to (B6), the terms “ $\tilde{C}_{mm|a}$ ” and “ $\tilde{C}_{mn|a}$ ” are not shown in I_{AE} . So we use an abbreviation in the following, which is

$$\sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n}} \longrightarrow \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 < n}} \equiv \sum_{C(M)}. \tag{E4}$$

If Bob declares that his photon has been projected to the X basis, Eve’s ancilla state is a mixed state of two states when Alice prepares $(|a\rangle + |b\rangle)/\sqrt{2}$ or $(|a\rangle - |b\rangle)/\sqrt{2}$. They are

$$\sum_{C(M)} \sum_{M/a,b} P \left\{ \sum_{\substack{t=0 \\ z-t \geq 0}}^3 \tilde{C}_{M_a, b_{z-t}|a} \right\} + \text{Part}\{b\}, \tag{E5}$$

and

$$\sum_{C(M)} \sum_{M/a,b} P \left\{ \sum_{\substack{t=0 \\ z-t \geq 0}}^3 (-1)^{z-t} \tilde{C}_{M_a, b_{z-t}|a} \right\} + \text{Part}\{b\}. \tag{E6}$$

Here we have gotten the mean for all K_M . So the cross terms are not shown in the two equations above.

Similarly in the Y basis, Eve's ancilla is a mixed state of the following two states:

$$\sum_{C(M)} \sum_{M/a,b} P \left\{ \sum_{\substack{t=0 \\ z-t \geq 0}}^3 i^{z-t} \tilde{C}_{Ma,b_{z-t}|a} \right\} + \text{Part}\{b\}, \tag{E7}$$

$$\sum_{C(M)} \sum_{M/a,b} P \left\{ \sum_{\substack{t=0 \\ z-t \geq 0}}^3 (-i)^{z-t} \tilde{C}_{Ma,b_{z-t}|a} \right\} + \text{Part}\{b\}. \tag{E8}$$

Then we can get the Holevo bound of Eve's information. For the X basis, it is

$$Q_x^{(a,b)} I_{AE_x}^{(a,b)} \leq \sum_{C(M)} \sum_{M/a,b} \varphi [(\tilde{C}_{Ma_z b_0|a} + \tilde{C}_{Ma_{z-2} b_2|a})^2, (\tilde{C}_{Ma_{z-1} b_1|a} + \tilde{C}_{Ma_{z-3} b_3|a})^2] + \text{Part}\{b\}. \tag{E9}$$

For the Y basis, it is

$$Q_y^{(a,b)} I_{AE_y}^{(a,b)} \leq \sum_{C(M)} \sum_{M/a,b} \varphi [(\tilde{C}_{Ma_z b_0|a} - \tilde{C}_{Ma_{z-2} b_2|a})^2, (\tilde{C}_{Ma_{z-1} b_1|a} - \tilde{C}_{Ma_{z-3} b_3|a})^2] + \text{Part}\{b\}. \tag{E10}$$

The overall information Eve can get is the mean of $Q_x^{(a,b)} I_{AE_x}^{(a,b)}$ and $Q_y^{(a,b)} I_{AE_y}^{(a,b)}$. It is

$$Q^{(a,b)} I_{AE}^{(a,b)} \leq \sum_{C(M)} \sum_{M/a,b} \varphi [c_{Ma_z b_0|a}^2 + c_{Ma_{z-2} b_2|a}^2, c_{Ma_{z-1} b_1|a}^2 + c_{Ma_{z-3} b_3|a}^2] + \text{Part}\{b\}. \tag{E11}$$

So

$$Q I_{AE} \leq \sum_{a < b} \sum_{C(M)} \sum_{M/a,b} \varphi [c_{Ma_z b_0|a}^2 + c_{Ma_{z-2} b_2|a}^2, c_{Ma_{z-1} b_1|a}^2 + c_{Ma_{z-3} b_3|a}^2] + \text{Part}\{b\} \leq \sum_{C(M)} f_\varphi(M, n). \tag{E12}$$

We will give f_φ below.

(1) If $z = 1$,

$$\begin{aligned} & \sum_{a < b} \sum_{M/a,b} \varphi [c_{Ma_z b_0|a}^2 + c_{Ma_{z-2} b_2|a}^2, c_{Ma_{z-1} b_1|a}^2 + c_{Ma_{z-3} b_3|a}^2] + \text{Part}\{b\} \\ &= \sum_{a < b} \sum_{M/a,b} \varphi (c_{Ma_1|a}^2, c_{Mb_1|a}^2) + \varphi (c_{Ma_1|b}^2, c_{Mb_1|b}^2) \leq \varphi \left(\sum_{a < b} \sum_{M/a,b} c_{Ma_1|a}^2 + c_{Mb_1|b}^2, \sum_{a < b} \sum_{M/a,b} c_{Mb_1|a}^2 + c_{Ma_1|b}^2 \right) \\ &= \varphi((L - \sum M - 1)x_{[(M+m_1),1]}, (M_1 + 1)x_{[(M+m_1),0]}). \end{aligned} \tag{E13}$$

Here $\sum M = M_1 + M_2 + M_3$.

$$x_{[(M+m_1),1]} = \sum_{M'/q} \sum_q c_{M'q|q}^2, \tag{E14}$$

$$x_{[(M+m_1),0]} = \sum_{M'/q} \sum_q c_{M'q}^2 \quad (M' = M + m_1). \tag{E15}$$

(2) If $z = 1 \pmod 4$ and $z \neq 1$,

$$\begin{aligned} & \sum_{a < b} \sum_{M/a,b} \varphi (c_{Ma_1|a}^2 + c_{Ma_3 b_2|a}^2, c_{Mb_1|a}^2 + c_{Ma_2 b_3|a}^2) + \varphi (c_{Ma_1|b}^2 + c_{Ma_3 b_2|b}^2, c_{Mb_1|b}^2 + c_{Ma_2 b_3|b}^2) \\ & \leq \varphi \left(\sum_{a < b} \sum_{M/a,b} c_{Ma_1|a}^2 + c_{Mb_1|b}^2 + c_{Ma_3 b_2|a}^2 + c_{Ma_2 b_3|b}^2, \sum_{a < b} \sum_{M/a,b} c_{Mb_1|a}^2 + c_{Ma_1|b}^2 + c_{Ma_2 b_3|a}^2 + c_{Ma_3 b_2|b}^2 \right) \\ &= \varphi[(L - \sum M - 1)x_{[(M+m_1),1]} + (M_2 + 1)x_{[(M+m_2+m_3),3]}, (M_1 + 1)x_{[(M+m_1),0]} + (M_3 + 1)x_{[(M+m_2+m_3),2]}]. \end{aligned} \tag{E16}$$

Here,

$$x_{[(M+m_2+m_3),3]} = \sum_{M'/q} \sum_q c_{M'qq|q}^2 \quad (M' = M + m_2), \tag{E17}$$

$$x_{[(M+m_2+m_3),2]} = \sum_{M'/q} \sum_q c_{M'qq|q}^2 \quad (M' = M + m_3). \tag{E18}$$

(3) If $z = 2$,

$$\begin{aligned} & \sum_{a < b} \sum_{M/a, b} \varphi(c_{Ma_2|a}^2 + c_{Mb_2|a}^2, c_{Ma_1b_1|a}^2) + \varphi(c_{Ma_2|b}^2 + c_{Mb_2|b}^2, c_{Ma_1b_1|b}^2) \\ & \leq \varphi\left(\sum_{a < b} \sum_{M/a, b} c_{Ma_2|a}^2 + c_{Mb_2|b}^2 + c_{Mb_2|a}^2 + c_{Ma_2|b}^2, \sum_{a < b} \sum_{M/a, b} c_{Ma_1b_1|a}^2 + c_{Ma_1b_1|b}^2\right) \\ & = \varphi\left[(L - \sum M - 1)x_{[(M+m_2), 2]} + (M_2 + 1)x_{[(M+m_2), 0]} + (M_1 + 1)x_{[(M+m_1+m_1), 1]}\right]. \end{aligned} \quad (E19)$$

Here,

$$x_{[(M+m_2), 2]} = \sum_{M'/q} \sum_q c_{M'q|q}^2, \quad (E20)$$

$$x_{[(M+m_2), 0]} = \sum_{M'/q} \sum_q c_{M'|q}^2 \quad (M' = M + m_2), \quad (E21)$$

$$x_{[(M+m_1+m_1), 1]} = \sum_{M'/q} \sum_q c_{M'q|q}^2 \quad (M' = M + m_1). \quad (E22)$$

(4) If $z = 2 \pmod 4$ and $z \neq 2$,

$$\begin{aligned} & \sum_{a < b} \sum_M \varphi(c_{Ma_2|a}^2 + c_{Mb_2|a}^2, c_{Ma_1b_1|a}^2 + c_{Ma_3b_3|a}^2) + \varphi(c_{Ma_2|b}^2 + c_{Mb_2|b}^2, c_{Ma_1b_1|b}^2 + c_{Ma_3b_3|b}^2) \\ & \leq \varphi\left[(L - \sum M - 1)x_{[(M+m_2), 2]} + (M_2 + 1)x_{[(M+m_2), 0]} + (M_1 + 1)x_{[(M+m_1+m_1), 1]} + (M_3 + 1)x_{[(M+m_3+m_3), 3]}\right]. \end{aligned} \quad (E23)$$

Here,

$$x_{[(M+m_3+m_3), 3]} = \sum_{M'/q} \sum_q c_{M'qq|q}^2 \quad (M' = M + m_3). \quad (E24)$$

(5) If $z = 3 \pmod 4$,

$$\begin{aligned} & \sum_{a < b} \sum_M \varphi(c_{Ma_3|a}^2 + c_{Ma_1b_2|a}^2, c_{Ma_2b_1|a}^2 + c_{Mb_3|a}^2) + \varphi(c_{Ma_3|b}^2 + c_{Ma_1b_2|b}^2, c_{Ma_2b_1|b}^2 + c_{Mb_3|b}^2) \\ & \leq \varphi\left[(L - \sum M - 1)x_{[(M+m_3), 3]} + (M_2 + 1)x_{[(M+m_1+m_2), 1]} + (M_1 + 1)x_{[(M+m_1+m_2), 2]} + (M_3 + 1)x_{[(M+m_3), 0]}\right]. \end{aligned} \quad (E25)$$

Here,

$$x_{[(M+m_3), 3]} = \sum_{M'/q} \sum_q c_{M'qq|q}^2, \quad (E26)$$

$$x_{[(M+m_1+m_2), 1]} = \sum_{M'/q} \sum_q c_{M'q|q}^2 \quad (M' = M + m_2), \quad (E27)$$

$$x_{[(M+m_1+m_2), 2]} = \sum_{M'/q} \sum_q c_{M'q|q}^2 \quad (M' = M + m_1), \quad (E28)$$

$$x_{[(M+m_3), 0]} = \sum_{M'/q} \sum_q c_{M'|q}^2 \quad (M' = M + m_3). \quad (E29)$$

(6) If $z = 0 \pmod 4$ and $z \neq 0$,

$$\begin{aligned} & \sum_{a < b} \sum_M \varphi(c_{M|a}^2 + c_{Ma_2b_2|a}^2, c_{Ma_3b_1|a}^2 + c_{Ma_1b_3|a}^2) + \varphi(c_{M|b}^2 + c_{Ma_2b_2|b}^2, c_{Ma_3b_1|b}^2 + c_{Ma_1b_3|b}^2) \\ & \leq \varphi\left[(L - \sum M - 1)x_{(M, 0)} + (M_2 + 1)x_{[(M+m_2+m_2), 2]} + (M_1 + 1)x_{[(M+m_1+m_3), 3]} + (M_3 + 1)x_{[(M+m_1+m_3), 1]}\right]. \end{aligned} \quad (E30)$$

Here,

$$x_{(M, 0)} = \sum_{M'/q} \sum_q c_{M'|q}^2, \quad (E31)$$

$$x_{[(M+m_2+m_2), 2]} = \sum_{M'/q} \sum_q c_{M'qq|q}^2 \quad (M' = M + m_2), \quad (E32)$$

$$x_{[(M+m_1+m_3), 3]} = \sum_{M'/q} \sum_q c_{M'qq|q}^2 \quad (M' = M + m_1), \quad (E33)$$

$$x_{[(M+m_1+m_3), 1]} = \sum_{M'/q} \sum_q c_{M'q|q}^2 \quad (M' = M + m_3). \quad (E34)$$

The yield Q is

$$Q = \sum_{a < b} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n \\ n - (M_1 + 2M_2 + 3M_3) = 0 \pmod{4}}} \sum_M (c_{M|a}^2 + c_{M|b}^2) = (L - 1) \sum x = L - 1. \tag{E35}$$

So we get

$$I_{AE} = \frac{Q_{IAE}}{Q} \leq \frac{1}{L - 1} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 < n}} f_\varphi(M, n), \tag{E36}$$

$$f_\varphi = \begin{cases} \varphi[(L - \sum M - 1)x_{(M+m_1),1}, (M_1 + 1)x_{(M+m_1),0}] & z = 1, \\ \varphi[(L - \sum M - 1)x_{(M+m_1),1} + (M_2 + 1)x_{(M+m_2+m_3),3}, (M_1 + 1)x_{(M+m_1),0} + (M_3 + 1)x_{(M+m_2+m_3),2}] & z = 1 \pmod{4}, \text{ and } z \neq 1, \\ \varphi[(L - \sum M - 1)x_{(M+m_2),2} + (M_2 + 1)x_{(M+m_2),0}, (M_1 + 1)x_{(M+m_1+m_1),1}] & z = 2, \\ \varphi[(L - \sum M - 1)x_{(M+m_2),2} + (M_2 + 1)x_{(M+m_2),0}, (M_1 + 1)x_{(M+m_1+m_1),1} + (M_3 + 1)x_{(M+m_3+m_3),3}] & z = 2 \pmod{4}, \text{ and } z \neq 2, \\ \varphi[(L - \sum M - 1)x_{(M+m_3),3} + (M_2 + 1)x_{(M+m_1+m_2),1}, (M_1 + 1)x_{(M+m_1+m_2),2} + (M_3 + 1)x_{(M+m_3),0}] & z = 3 \pmod{4}, \\ \varphi[(L - \sum M - 1)x_{(M,0)} + (M_2 + 1)x_{(M+m_2+m_2),2}, (M_1 + 1)x_{(M+m_1+m_3),3} + (M_3 + 1)x_{(M+m_1+m_3),1}] & z = 0 \pmod{4}, \text{ and } z \neq 0. \end{cases} \tag{E37}$$

Here $z = n - (M_1 + 2M_2 + 3M_3)$.

2. Error

In this part we will give the relationship between the error rate and x 's.

The errors when Alice sends $(|a\rangle + |b\rangle)/\sqrt{2}$ can be given by multiplying $(\langle a| - \langle b|)/\sqrt{2}$ to Eq. (E2) and getting its square, which is

$$Q_{xs}^{a,b} E_{xs}^{a,b} = \frac{1}{2} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n}} \sum_{M/a,b} \left| \sum_{\substack{t=0 \\ z-t \geq 0}}^3 (\tilde{C}_{Ma_t b_{z-t}|a} - \tilde{C}_{Ma_t b_{z-t}|b}) \right|^2. \tag{E38}$$

Here sending $(|a\rangle + |b\rangle)/\sqrt{2}$ means $k_a = k_b$, and we have calculated the mean for all K_M . So the cross terms are not shown.

Then we can get the errors when Alice sends $(|a\rangle - |b\rangle)/\sqrt{2}$, which is

$$Q_{xd}^{a,b} E_{xd}^{a,b} = \frac{1}{2} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n}} \sum_{M/a,b} \left| \sum_{\substack{t=0 \\ z-t \geq 0}}^3 (-1)^{z-t} (\tilde{C}_{Ma_t b_{z-t}|a} + \tilde{C}_{Ma_t b_{z-t}|b}) \right|^2. \tag{E39}$$

Here sending $(|a\rangle - |b\rangle)/\sqrt{2}$ means $k_b = k_a + 2 \pmod{4}$, and we have gotten the mean for all K_M .

When Alice sends $(|a\rangle + i|b\rangle)$, errors can be obtained by multiplying $(\langle a| - i\langle b|)/\sqrt{2}$ to Eq. (E2) and getting its square, which is

$$Q_{ys}^{a,b} E_{ys}^{a,b} = \frac{1}{2} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n}} \sum_{M/a,b} \left| \sum_{\substack{t=0 \\ z-t \geq 0}}^3 i^{z-t} (\tilde{C}_{Ma_t b_{z-t}|a} + i\tilde{C}_{Ma_t b_{z-t}|b}) \right|^2. \tag{E40}$$

Here sending $(|a\rangle + i|b\rangle)/\sqrt{2}$ means $k_b = k_a + 1 \pmod{4}$.

When Alice sends $(|a\rangle - i|b\rangle)$, the errors are

$$Q_{yd}^{a,b} E_{yd}^{a,b} = \frac{1}{2} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n}} \sum_{M/a,b} \left| \sum_{\substack{t=0 \\ z-t \geq 0}}^3 (-i)^{z-t} (\tilde{C}_{Ma_t b_{z-t}|a} - i\tilde{C}_{Ma_t b_{z-t}|b}) \right|^2. \tag{E41}$$

Here sending $(|a\rangle - i|b\rangle)/\sqrt{2}$ means $k_b = k_a + 3 \pmod{4}$.

We calculate the mean of these four cases from Eqs. (E38) to (E41) and get its summation for a and b . We get

$$\begin{aligned}
 QE &= \frac{1}{2} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n}} \sum_{a < b} \sum_{M/a, b} \{ |\tilde{C}_{Ma_z b_0|a} - \tilde{C}_{Ma_{z-1} b_1|b}|^2 + |\tilde{C}_{Ma_{z-2} b_2|a} - \tilde{C}_{Ma_{z-3} b_3|b}|^2 \\
 &\quad + |\tilde{C}_{Ma_{z-1} b_1|a} - \tilde{C}_{Ma_{z-2} b_2|b}|^2 + |\tilde{C}_{Ma_{z-3} b_3|a} - \tilde{C}_{Ma_z b_0|b}|^2 \} \\
 &\geq \frac{1}{2} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n}} f_E(M, n).
 \end{aligned} \tag{E42}$$

Then we will give f_E . And in the following we will use the inequalities that $|\tilde{a} - \tilde{b}|^2 + |\tilde{x} - \tilde{y}|^2 \geq (\sqrt{a^2 + x^2} - \sqrt{b^2 + y^2})^2$ and $(\sqrt{a} - \sqrt{b})^2 + (\sqrt{x} - \sqrt{y})^2 \geq (\sqrt{a+x} - \sqrt{b+y})^2$.

(1) If $z = 1$,

$$\sum_{a < b} \sum_{M/a, b} \{ |\tilde{C}_{Ma_1|a} - \tilde{C}_{Mb_1|b}|^2 + |\tilde{C}_{Mb_1|a}|^2 + |\tilde{C}_{Ma_1|b}|^2 \} \geq (M_1 + 1)x_{[(M+m_1), 0]}. \tag{E43}$$

(2) If $z = 1 \pmod{4}$ and $z \neq 1$,

$$\begin{aligned}
 &\sum_{a < b} \sum_{M/a, b} \{ |\tilde{C}_{Ma_1|a} - \tilde{C}_{Mb_1|b}|^2 + |\tilde{C}_{Ma_3 b_2|a} - \tilde{C}_{Ma_2 b_3|b}|^2 + |\tilde{C}_{Mb_1|a} - \tilde{C}_{Ma_3 b_2|b}|^2 + |\tilde{C}_{Ma_2 b_3|a} - \tilde{C}_{Ma_1|b}|^2 \} \\
 &\geq \left(\sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Mb|a}^2 + c_{Ma|b}^2)} - \sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_2 b_3|a}^2 + c_{Ma_3 b_2|b}^2)} \right)^2 = (\sqrt{(M_1 + 1)x_{[(M+m_1), 0]}} - \sqrt{(M_3 + 1)x_{[(M+m_2+m_3), 2]}})^2.
 \end{aligned} \tag{E44}$$

(3) If $z = 2$,

$$\begin{aligned}
 &\sum_{a < b} \sum_{M/a, b} \{ |\tilde{C}_{Ma_2|a} - \tilde{C}_{Ma_1 b_1|b}|^2 + |\tilde{C}_{Mb_2|a}|^2 + |\tilde{C}_{Ma_1 b_1|a} - \tilde{C}_{Mb_2|b}|^2 + |\tilde{C}_{Ma_2|b}|^2 \} \\
 &\geq \left\{ \sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_2|a}^2 + c_{Mb_2|b}^2)} - \sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_1 b_1|a}^2 + c_{Ma_1 b_1|b}^2)} \right\}^2 + \sum_{\substack{a < b \\ M/a, b}} (c_{Mb_2|a}^2 + c_{Ma_2|b}^2) \\
 &= \left(\sqrt{(L - \sum M - 1)x_{[(M+m_2), 2]}} - \sqrt{(M_1 + 1)x_{[(M+m_1+m_1), 1]}} \right)^2 + (M_2 + 1)x_{[(M+m_2), 0]}.
 \end{aligned} \tag{E45}$$

(4) If $z = 2 \pmod{4}$ and $z \neq 2$,

$$\begin{aligned}
 &\sum_{a < b} \sum_{M/a, b} \{ |\tilde{C}_{Ma_2|a} - \tilde{C}_{Ma_1 b_1|b}|^2 + |\tilde{C}_{Mb_2|a} - \tilde{C}_{Ma_3 b_3|b}|^2 + |\tilde{C}_{Ma_1 b_1|a} - \tilde{C}_{Mb_2|b}|^2 + |\tilde{C}_{Ma_3 b_3|a} - \tilde{C}_{Ma_2|b}|^2 \} \\
 &\geq \left(\sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_2|a}^2 + c_{Mb_2|b}^2)} - \sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_1 b_1|a}^2 + c_{Ma_1 b_1|b}^2)} \right)^2 \\
 &\quad + \left(\sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Mb_2|a}^2 + c_{Ma_2|b}^2)} - \sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_3 b_3|a}^2 + c_{Ma_3 b_3|b}^2)} \right)^2 \\
 &= \left(\sqrt{(L - \sum M - 1)x_{[(M+m_2), 2]}} - \sqrt{(M_1 + 1)x_{[(M+m_1+m_1), 1]}} \right)^2 + (\sqrt{(M_2 + 1)x_{[(M+m_2), 0]}} - \sqrt{(M_3 + 1)x_{[(M+m_3+m_3), 3]}})^2.
 \end{aligned} \tag{E46}$$

(5) If $z = 3 \pmod 4$,

$$\begin{aligned} & \sum_{a < b} \sum_{M/a, b} \{ |\tilde{C}_{Ma_3|a} - \tilde{C}_{Ma_2b_1|b}|^2 + |\tilde{C}_{Ma_1b_2|a} - \tilde{C}_{Mb_3|b}|^2 + |\tilde{C}_{Ma_2b_1|a} - \tilde{C}_{Ma_1b_2|b}|^2 + |\tilde{C}_{Mb_3|a} - \tilde{C}_{Ma_3|b}|^2 \} \\ & \geq \left(\sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_3|a}^2 + c_{Mb_3|b}^2)} - \sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_1b_2|a}^2 + c_{Ma_2b_1|b}^2)} \right)^2 \\ & = \left(\sqrt{(L - \sum M - 1)x_{[(M+m_3), 3]}} - \sqrt{(M_2 + 1)x_{[(M+m_1+m_2), 1]}} \right)^2. \end{aligned} \tag{E47}$$

(6) If $z = 0$,

$$\sum_{a < b} \sum_{M/a, b} \{ |\tilde{C}_{M|a}|^2 + |\tilde{C}_{M|b}|^2 \} = (L - \sum M - 1)x_{(M, 0)}. \tag{E48}$$

(7) If $z = 0 \pmod 4$ and $z \neq 0$,

$$\begin{aligned} & \sum_{a < b} \sum_{M/a, b} \{ |\tilde{C}_{M|a} - \tilde{C}_{Ma_3b_1|b}|^2 + |\tilde{C}_{Ma_2b_2|a} - \tilde{C}_{Ma_1b_3|b}|^2 + |\tilde{C}_{Ma_3b_1|a} - \tilde{C}_{Ma_2b_2|b}|^2 + |\tilde{C}_{Ma_1b_3|a} - \tilde{C}_{M|b}|^2 \} \\ & \geq \left(\sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{M|a}^2 + c_{M|b}^2)} - \sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_1b_3|a}^2 + c_{Ma_3b_1|b}^2)} \right)^2 \\ & \quad + \left(\sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_2b_2|a}^2 + c_{Ma_2b_2|b}^2)} - \sqrt{\sum_{\substack{a < b \\ M/a, b}} (c_{Ma_3b_1|a}^2 + c_{Ma_1b_3|b}^2)} \right)^2 \\ & = \left(\sqrt{(L - \sum M - 1)x_{(M, 0)}} - \sqrt{(M_3 + 1)x_{[(M+m_1+m_3), 1]}} \right)^2 + \left(\sqrt{(M_2 + 1)x_{[(M+m_2+m_2), 2]}} - \sqrt{(M_1 + 1)x_{[(M+m_1+m_3), 3]}} \right)^2. \end{aligned} \tag{E49}$$

So we get

$$E = \frac{QE}{Q} \geq \frac{1}{2(L - 1)} \sum_{\substack{M_1, M_2, M_3 \geq 0 \\ M_1 + 2M_2 + 3M_3 \leq n}} f_E(M, n). \tag{E50}$$

$$f_E = \begin{cases} (M_1 + 1)x_{[(M+m_1), 0]} & z = 1, \\ (\sqrt{(M_1 + 1)x_{[(M+m_1), 0]}} - \sqrt{(M_3 + 1)x_{[(M+m_2+m_3), 2]}})^2 & z = 1 \pmod 4, \text{ and } z \neq 1, \\ (\sqrt{(L - \sum M - 1)x_{[(M+m_2), 2]}} - \sqrt{(M_1 + 1)x_{[(M+m_1+m_1), 1]}})^2 + (M_2 + 1)x_{[(M+m_2), 0]} & z = 2, \\ (\sqrt{(L - \sum M - 1)x_{[(M+m_2), 2]}} - \sqrt{(M_1 + 1)x_{[(M+m_1+m_1), 1]}})^2 + (\sqrt{(M_2 + 1)x_{[(M+m_2), 0]}} - \sqrt{(M_3 + 1)x_{[(M+m_3+m_3), 3]}})^2 & z = 2 \pmod 4, \text{ and } z \neq 2, \\ (\sqrt{(L - \sum M - 1)x_{[(M+m_3), 3]}} - \sqrt{(M_2 + 1)x_{[(M+m_1+m_2), 1]}})^2 & z = 3 \pmod 4, \\ (L - \sum M - 1)x_{(M, 0)} & z = 0, \\ (\sqrt{(L - \sum M - 1)x_{(M, 0)}} - \sqrt{(M_3 + 1)x_{[(M+m_1+m_3), 1]}})^2 + (\sqrt{(M_2 + 1)x_{[(M+m_2+m_2), 2]}} - \sqrt{(M_1 + 1)x_{[(M+m_1+m_3), 3]}})^2 & z = 0 \pmod 4, \text{ and } z \neq 0. \end{cases} \tag{E51}$$

APPENDIX F: PROOF FOR THE CONCAVITY OF I_{AE}^U

In this section, we will give the proof that I_{AE}^U is a concave function for variable E . From Eqs. (E36) and (E37), we can see that I_{AE}^U has a form like

$$I_{AE} \leq \varphi(k_1x_1 + k_2x_2, k_3x_3 + k_4x_4) + \dots \quad (F1)$$

We assume that if error rate is E , I_{AE} gets its maximum I_{AE}^U when the x 's are x_1, x_2, \dots , and if the error rate is E' , I_{AE} gets its maximum I_{AE}^U when the x 's are x'_1, x'_2, \dots , which means

$$I_{AE}^U(E) = \varphi(k_1x_1 + k_2x_2, k_3x_3 + k_4x_4) + \dots, \quad (F2)$$

$$I_{AE}^U(E') = \varphi(k_1x'_1 + k_2x'_2, k_3x'_3 + k_4x'_4) + \dots \quad (F3)$$

Then we have

$$\begin{aligned} \alpha I_{AE}^U(E) + (1 - \alpha)I_{AE}^U(E') &= \alpha\varphi(k_1x_1 + k_2x_2, k_3x_3 + k_4x_4) + (1 - \alpha)\varphi(k_1x'_1 + k_2x'_2, k_3x'_3 + k_4x'_4) + \dots \\ &\leq \varphi\{k_1[\alpha x_1 + (1 - \alpha)x'_1] + k_2[\alpha x_2 + (1 - \alpha)x'_2], k_3[\alpha x_3 + (1 - \alpha)x'_3] \\ &\quad + k_4[\alpha x_4 + (1 - \alpha)x'_4]\} + \dots \end{aligned} \quad (F4)$$

Here $\alpha \in [0, 1]$. Then if we can prove that $I_{AE}^U[\alpha E + (1 - \alpha)E'] \geq \alpha I_{AE}^U(E) + (1 - \alpha)I_{AE}^U(E')$, the concavity will be proven.

We define that $X_i = \alpha x_i + (1 - \alpha)x'_i$ for $i = 1, 2, \dots$. Then we can get that $\sum_i X_i = \alpha \sum_i x_i + (1 - \alpha) \sum_i x'_i = 1$ and $X_i \geq 0$. So the X 's are a legitimate group of variables for I_{AE} . From Eq. (F4) we can see $I_{AE}[\alpha E + (1 - \alpha)E', X] \geq \alpha I_{AE}^U(E) + (1 - \alpha)I_{AE}^U(E')$ if the X 's meet the error rate requirement of $\alpha E + (1 - \alpha)E'$, which will be proven in the following.

From Eq. (E50), E has a form like

$$E \geq t_1x_1 + t_2x_2 + (\sqrt{w_1x_1} - \sqrt{w_2x_2})^2 + \dots \quad (F5)$$

So we have

$$E' \geq t_1x'_1 + t_2x'_2 + (\sqrt{w_1x'_1} - \sqrt{w_2x'_2})^2 + \dots \quad (F6)$$

$$\alpha E + (1 - \alpha)E' \geq t_1X_1 + t_2X_2 + w_1X_1 + w_2X_2 - 2\alpha\sqrt{w_1x_1w_2x_2} - 2(1 - \alpha)\sqrt{w_1x'_1w_2x'_2} \dots \quad (F7)$$

What we should prove is

$$\alpha E + (1 - \alpha)E' \geq t_1X_1 + t_2X_2 + (\sqrt{w_1X_1} - \sqrt{w_2X_2})^2 + \dots = t_1X_1 + t_2X_2 + w_1X_1 + w_2X_2 - 2\sqrt{w_1X_1w_2X_2} \dots \quad (F8)$$

Here $-\sqrt{w_1X_1w_2X_2} \leq -\alpha\sqrt{w_1x_1w_2x_2} - (1 - \alpha)\sqrt{w_1x'_1w_2x'_2}$ is easy to prove. So Eq. (F8) is correct.

To summarize, the X 's is a group of variables satisfying $I_{AE}[\alpha E + (1 - \alpha)E', X] \geq \alpha I_{AE}^U(E) + (1 - \alpha)I_{AE}^U(E')$. And $I_{AE}^U[\alpha E + (1 - \alpha)E'] \geq I_{AE}[\alpha E + (1 - \alpha)E', X]$. So the function I_{AE}^U is concave.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 10-12 December 1984* (IEEE, New York, 1984), p. 175.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).

[3] C. H. Bennett, Quantum Cryptography Using Any Two Nonorthogonal States, *Phys. Rev. Lett.* **68**, 3121 (1992).

[4] K. Inoue, E. Waks, and Y. Yamamoto, Differential Phase Shift Quantum Key Distribution, *Phys. Rev. Lett.* **89**, 037902 (2002).

[5] K. Boström and T. Felbinger, Deterministic Secure Direct Communication Using Entanglement, *Phys. Rev. Lett.* **89**, 187902 (2002).

[6] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, *Phys. Rev. Lett.* **98**, 230501 (2007).

[7] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).

[8] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, *Nature (London)* **509**, 475 (2014).

[9] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, *Nature (London)* **557**, 400 (2018).

[10] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.* **91**, 057901 (2003).

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

[12] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).

- [13] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d -Level Systems, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [14] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
- [15] Z. Zhang, X. Yuan, Z. Cao, and X. Ma, Practical round-robin differential-phase-shift quantum key distribution, *New J. Phys.* **19**, 033013 (2017).
- [16] Z.-Q. Yin, S. Wang, W. Chen, Y.-G. Han, R. Wang, G.-C. Guo, and Z.-F. Han, Improved security bound for the round-robin-differential-phase-shift quantum key distribution, *Nat. Commun.* **9**, 457 (2018).
- [17] R. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Round-robin-differential-phase-shift quantum key distribution with monitoring signal disturbance, *Opt. Lett.* **43**, 4228 (2018).
- [18] T. Matsuura, T. Sasaki, and M. Koashi, Refined security proof of the round-robin differential-phase-shift quantum key distribution and its improved performance in the finite-sized case, *Phys. Rev. A* **99**, 042303 (2019).
- [19] H. Liu, Z.-Q. Yin, R. Wang, Z.-H. Wang, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Tight finite-key analysis for quantum key distribution without monitoring signal disturbance, *npj Quantum Inf.* **7**, 95 (2021).
- [20] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Experimental quantum key distribution without monitoring signal disturbance, *Nat. Photonics* **9**, 827 (2015).
- [21] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, Experimental demonstration of a quantum key distribution without signal disturbance monitoring, *Nat. Photonics* **9**, 832 (2015).
- [22] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution, *Phys. Rev. Lett.* **114**, 180502 (2015).
- [23] Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, W. Chen, Y. Xu, J.-Y. Guan, S.-K. Liao, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng, and J.-W. Pan, Experimental round-robin differential phase-shift quantum key distribution, *Phys. Rev. A* **93**, 030302(R) (2016).
- [24] C. Zhou, Y.-Y. Zhang, W.-S. Bao, H.-W. Li, Y. Wang, and M.-S. Jiang, Round-robin differential quadrature phase-shift quantum key distribution, *Chin. Phys. B* **26**, 020303 (2017).
- [25] R. Wang, Z.-Q. Yin, C.-H. Cui, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Security proof for single-photon round-robin differential-quadrature-phase-shift quantum key distribution, *Phys. Rev. A* **98**, 062331 (2018).
- [26] C. M. Caves, C. A. Fuchs, and R. Schack, Unknown quantum states: The quantum de finetti representation, *J. Math. Phys.* **43**, 4537 (2002).
- [27] C. A. Fuchs, R. Schack, and P. F. Scudo, De finetti representation theorem for quantum-process tomography, *Phys. Rev. A* **69**, 062305 (2004).
- [28] M. Christandl, R. König, and R. Renner, Postselection Technique for Quantum Channels with Applications to Quantum Cryptography, *Phys. Rev. Lett.* **102**, 020504 (2009).