Refined security proof of the round-robin differential-phase-shift quantum key distribution and its improved performance in the finite-sized case

Takaya Matsuura, Toshihiko Sasaki, and Masato Koashi

Phys. Rev. A **99**, 042303 — Published 1 April 2019

DOI: 10.1103/PhysRevA.99.042303

Refined security proof of the round-robin differential phase shift quantum key distribution and its improved performance in the finite-sized case

Takaya Matsuura,[1,*] Toshihiko Sasaki,[1,2] and Masato Koashi[1,2]

[1]*Department of Applied Physics, Graduate School of Engineering,*
The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan
[2]*Photon Science Center, Graduate School of Engineering,*
The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan

(Dated: March 5, 2019)

Among many quantum key distribution (QKD) protocols, the round-robin differential phase shift (RRDPS) protocol is unique in that it can upper-bound the amount of the information leakage without monitoring signal disturbance. To expedite implementation of the protocol, however, the number of pulses forming a single block should be kept small, which significantly decreases the key rates in the original security proof. In the present paper, we refine the security proof of the RRDPS protocol in the finite-sized regime and achieve a tighter estimation for the information leakage with neither monitoring signal disturbance nor changing the original experimental setups. As a consequence, we obtain better key rates in both asymptotic and finite-sized cases while keeping the preferable features of the protocol, such as omission of phase randomization.

I. INTRODUCTION

One of the most important implications of the quantum information theory is that information-theoretically secure communication is possible by the quantum key distribution (QKD). After the first proposal of the BB84 protocol [1], many researches have been made in the field. In recent years, the real world implementation of the QKD is attracting much attention. For the real world implementation, we need careful consideration about the finite-sized effect of the key and the imperfections of the experimental devices because communications in the real world are often done in limited time and with imperfect devices. The finite-sized key rate of the QKD protocol is especially important when we consider the communication between the ground and the satellite [2, 3] for which the communication time is limited and therefore only a small number of bits can be sent at a time.

The round-robin differential phase shift (RRDPS) protocol [4] is a QKD protocol which has a special property that the required amount of privacy amplification is determined only by the protocol parameters and independent of the bit error rates. Due to this property, the protocol is expected to be able to generate the key even when the number of communication rounds is small, because it does not suffer from the convoluted statistical estimation of the information leakage. The protocol can be implemented with a light source producing a coherent laser pulse train at the sender, and a variable-delay interferometer followed by photon detection at the receiver. A number of experimental demonstrations have already been made [5–8]. Especially, the apparatus for the sender can be made very simple with only binary phase modulation, and the security can be proved without phase randomization of the optical pulses. Fewer assumptions on the light source in the RRDPS protocol also lead to the robustness against the source imperfection [9].

On the other hand, the RRDPS protocol also has a few undesirable features. The protocol assumes a variable delay interferometer which should be switched among L different delays actively or passively for each pulse block. Implementing such an interferometer is costly especially for large L. Furthermore, the asymptotic key rate of the RRDPS protocol even with relatively large block size ($L \sim 128$) is about one-tenth of that of the decoy BB84 protocol [10], which is a widely used and the most studied practical QKD protocol. The key rate gets even worse when we decrease L to simplify the implementation. Therefore, it is desired to improve the key rate of the RRDPS protocol especially for relatively small L. There have been intensive researches to mitigate or to get over these problems both in theory [11–18] and experiment [7, 19].

Very recently, Yin *et al.* shows that by directly evaluating Eve's collective attacks, one can improve the key rate of the RRDPS protocol with block-wise phase randomization without any change in the protocol [18]. It also implies that we can decrease L to achieve the same key rate. Unfortunately, the analysis in [18] cannot directly be extended to the finite-sized case, and thus its usage is limited.

In this paper, we refine the security proof of the RRDPS protocol with a different approach and obtain better key rates in both asymptotic and finite-sized case without the aid of the block-wise phase randomization. The main idea of our analysis is to utilize the information disregarded in the original security proof, which leads to a tighter estimation for the amount of the information leakage, and thus neither monitoring signal disturbance nor changing experimental setups is required. Our analysis developed here is based on the technique used in the security proof of the differential quadrature phase shift protocol [20], and it may be applicable to other high dimensional QKD protocols including other DPS-type pro-

[*] matsuura@qi.t.u-tokyo.ac.jp

tocols. The obtained key rate in the asymptotic limit with our analysis is comparable to that in [18], but we do not require the block-wise phase randomization, and we can also explicitly give the key rate formula in the finite-sized case. Furthermore, we show that the RRDPS protocol outperforms decoy BB84 protocol when the number of communication rounds is small.

The paper is organized as follows. In Section II, we develop the refined security proof of the RRDPS protocol, which is the main part of this paper. We give the definition of the protocol and subsequently construct a compatible virtual protocol which includes a crucial difference from the original one. We further introduce another auxiliary protocol which reproduces the statistics of the phase errors in the virtual protocol, and by analyzing it, we derive the main theorem, which gives the required amount of the privacy amplification. In Section III, we numerically simulate the key rates of the RRDPS protocol with our refined analysis in both asymptotic and finite-sized case, illustrating how we determine the parameters which appear in the key rate formula. Finally, in Section IV, we wrap up our analysis, discuss the comparison between the techniques developed here and the existing ones, and refer to some remaining problems.

II. SECURITY PROOF

In what follows, $h(x) := -x\log x - (1-x)\log(1-x)$ denotes binary entropy function, $H(X|Y)_P$ denotes the conditional entropy with the joint probability distribution P, and $D(P\|Q)$ denotes the Kullback-Leibler divergence. $\mathbb{E}_{X\sim P}[f(X)]$ denotes the expectation value of $f(X)$ when the random variable X obeys the probability distribution P. $\|\rho-\sigma\|_1 = \mathrm{Tr}|\rho-\sigma|$ is the trace norm distance and $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ is the fidelity between the density matrices ρ and σ. We call $\{|0\rangle, |1\rangle\}$ as the bit basis of the qubit, and $\{|0_X\rangle = (|0\rangle+|1\rangle)/\sqrt{2}, |1_X\rangle = (|0\rangle-|1\rangle)/\sqrt{2}\}$ as the phase basis. The controlled-NOT (CNOT) operation between control qubit 1 and target qubit 2 is defined as $|0\rangle\langle 0|_1 \otimes I_2 + |1\rangle\langle 1|_1 \otimes X_2 = I_1 \otimes |0_X\rangle\langle 0_X|_2 + Z_1 \otimes |1_X\rangle\langle 1_X|_2$, where I denotes the identity operator, $X = |0\rangle\langle 1| + |1\rangle\langle 0|$, and $Z = |0_X\rangle\langle 1_X| + |1_X\rangle\langle 0_X|$. $\boldsymbol{I}_N$ denotes $N\times N$ identity matrix, and $\oplus$ denotes the summation modulo 2. The base of the logarithm is taken to be 2.

A. The definition of the protocol

We first give the actual procedure of the RRDPS protocol [4] and the assumptions for the analysis in this paper.

Setups and assumptions: The sender Alice has a $0/\pi$ phase modulator and an i.i.d. source of weak coherent optical pulses. The quantum state of each optical pulse is represented by a density operator σ, which has no correlation with any other system. The probability that the source emits odd numbers of photons is upper-bounded by a known parameter p_{src} (e.g. $p_{\mathrm{src}} = 1 - \langle 0|\,\sigma\,|0\rangle$). Bob has a variable delay interferometer whose delay can be switched according to randomly generated numbers. The photon detector can distinguish zero, one, and two or more photons. The inefficiency and the dark counting of the photon detectors can be included in the channel loss. They share a public channel for announcement as well as a quantum channel. The eavesdropper Eve can perform arbitrary attacks allowed in the law of quantum mechanics on the quantum channel and listen to all the announcements of Alice and Bob made over the public channel.

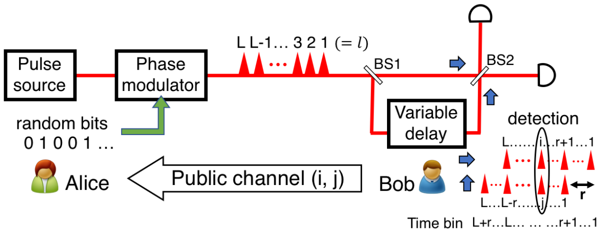

FIG. 1. Schematics of the RRDPS protocol

Protocol 1 (actual protocol):

Before the commencement of the protocol, Alice and Bob agree on constants L and N_{em} as well as a function $N_{\mathrm{fin}}(N)$ and probabilities $p'(C|N, N_{\mathrm{fin}})$ over full-rank $N\times N_{\mathrm{fin}}$ binary matrices C.

(i) Alice and Bob repeat the following procedures for N_{em} rounds.

- Alice generates a sequence of random bits $s^{(1)}, ..., s^{(L)}$, and encode them to L optical pulses by modulating the optical phase of the l-th pulse with $\mathrm{e}^{\pi i s^{(l)}}$ ($l = 1, ..., L$). She sends Bob the L optical pulses through the quantum channel.
- Bob randomly selects the delay $r \in \{1, ..., L-1\}$ and feeds the received L pulses to the delayed interferometer as shown in Figure 1. He detects photons with the two detectors at time bins 1 through $L + r$.
  - If Bob detects only one photon from the $(r+1)$-th to the L-th time bin, and observes no detection at the other bins, he records a sifted key bit $z_B \in \{0, 1\}$ according to which photon detector has reported the detection. He also records the unordered pair (i, j), which are the positions of the pulse pair arriving at the detected time bin ($i, j \in \{1, ..., L\}$, $|i-j| = r$). He announces "success", and Alice records

her random bit sequence $(s^{(1)},...,s^{(L)})$. [Success round]

- If the above condition is not satisfied, Bob announces "failure" and Alice discards her random bits. [Failure round]

(ii) Let N be the number of the success rounds. By proper indexing, Alice's records are represented by $(s_1^{(1)},...,s_1^{(L)}),...,(s_N^{(1)},...,s_N^{(L)})$, and Bob's sifted key by $\boldsymbol{z}_B = (z_{B1} \cdots z_{BN})$ and his unordered pairs by $(i_1,j_1),...,(i_N,j_N)$.

(iii) Bob announces the sequence of the unordered pairs $(i_1,j_1),...,(i_N,j_N)$.

(iv) Alice defines her sifted key $\boldsymbol{z}_A = (z_{A1} \cdots z_{AN})$ by $z_{Ak} := s_k^{(i_k)} \oplus s_k^{(j_k)}$ for $k = 1,...,N$.

(v) (Bit error correction) Alice chooses and announces a bit error correcting code. She calculates the N_{EC}-bit syndrome for $\boldsymbol{z}_A$ and encrypts it by consuming N_{EC} bits of the pre-shared secret key before she sends it to Bob. With the syndrome, Bob performs bit error correction on his sifted key $\boldsymbol{z}_B$ and obtains the reconciled key $\boldsymbol{z}_B^{\mathrm{rec}}$ of N bits.

(vi) (Privacy amplification) Let $N_{\mathrm{fin}} := N_{\mathrm{fin}}(N)$. Alice draws a full-rank $N \times N_{\mathrm{fin}}$ binary matrix C_{PA} with the probability $p'(C_{PA}|N, N_{\mathrm{fin}})$ and announces it. Alice and Bob computes the final keys as $\boldsymbol{z}_A^{\mathrm{fin}} = \boldsymbol{z}_A C_{PA}$ and $\boldsymbol{z}_B^{\mathrm{fin}} = \boldsymbol{z}_B^{\mathrm{rec}} C_{PA}$, respectively.

For simplicity, we omitted the bit error sampling rounds in the above protocol. In order to estimate an upper-bound on the bit error rate e_{bit}, Alice randomly inserts N_{smp} sampling rounds among N_{em} rounds, and according to e_{bit}, she decides whether she aborts the protocol or not. Here we assume that N_{smp} is negligibly small compared to N_{em}. The required amount of the error syndrome Alice sends to Bob in the bit error correction, N_{EC}, depends on the error correction method; here we assume $N_{EC} = N f_{EC} h(e_{\mathrm{bit}})$, where f_{EC} is an error correction efficiency to satisfy the required correctness. The net key gain per pulse of the protocol is therefore given by $(N_{\mathrm{fin}} - N_{EC})/(N_{\mathrm{em}} L) = (N_{\mathrm{fin}} - N f_{EC} h(e_{\mathrm{bit}}))/(N_{\mathrm{em}} L)$.

We evaluate the secrecy of Protocol 1 by the $\varepsilon_{\mathrm{sec}}$-secrecy condition for Alice's final key defined as

$$\frac{1}{2} \sum_{N_{\mathrm{fin}} \geq 1} \Pr(N_{\mathrm{fin}}) \left\| \rho_{AE|N_{\mathrm{fin}}}^{\mathrm{fin}} - \rho_{AE|N_{\mathrm{fin}}}^{\mathrm{ideal}} \right\|_1 \leq \varepsilon_{\mathrm{sec}}. \qquad (1)$$

Here $\Pr(N_{\mathrm{fin}})$ is the probability of obtaining N_{fin}, where aborting the protocol is interpreted as $N_{\mathrm{fin}} = 0$. The density operator $\rho_{AE|N_{\mathrm{fin}}}^{\mathrm{fin}}$ represents the state of Alice's final key and Eve's quantum system, which takes the form of

$$\rho_{AE|N_{\mathrm{fin}}}^{\mathrm{fin}} = \sum_{\boldsymbol{z}_A^{\mathrm{fin}} \in \{0,1\}^{N_{\mathrm{fin}}}} \Pr(\boldsymbol{z}_A^{\mathrm{fin}}) \left| \boldsymbol{z}_A^{\mathrm{fin}} \right\rangle \left\langle \boldsymbol{z}_A^{\mathrm{fin}} \right|_A \otimes \rho_{E|N_{\mathrm{fin}}}(\boldsymbol{z}_A^{\mathrm{fin}}). \qquad (2)$$

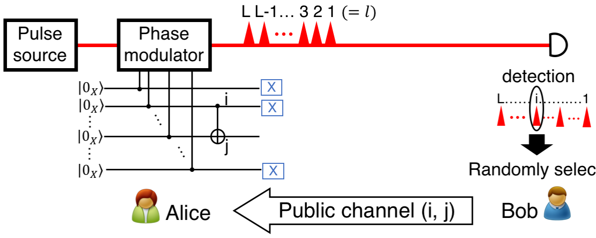

FIG. 2. Virtual protocol of the RRDPS. In contrast to the original security proof, here we assume that Alice measures all but j-th of the L qubits in the phase basis.

The ideal state $\rho_{AE|N_{\mathrm{fin}}}^{\mathrm{ideal}}$ is defined as

$$\rho_{AE|N_{\mathrm{fin}}}^{\mathrm{ideal}} := \left(\sum_{\boldsymbol{z}_A^{\mathrm{fin}} \in \{0,1\}^{N_{\mathrm{fin}}}} \frac{1}{2^{N_{\mathrm{fin}}}} \left| \boldsymbol{z}_A^{\mathrm{fin}} \right\rangle \left\langle \boldsymbol{z}_A^{\mathrm{fin}} \right|_A \right) \otimes \mathrm{Tr}_A \left(\rho_{AE|N_{\mathrm{fin}}}^{\mathrm{fin}} \right). \qquad (3)$$

B. The reduction of the protocol

We prove the secrecy condition (1) of the protocol based on complementarity [21]. In this way of the security proof, we introduce a virtual protocol (Protocol 2) in which Alice's N_{fin}-bit final key is obtained by a bit basis measurement on N_{fin} register qubits. Protocol 2 should be related to Protocol 1 such that for every attack on Protocol 1, there exists an attack on Protocol 2 resulting in the same final state ($\Pr(N_{\mathrm{fin}})$ and $\rho_{AE|N_{\mathrm{fin}}}^{\mathrm{fin}}$). While the original proof [4] followed the same technique, our construction of Protocol 2 below (see also Figure 2) includes a modification (shown in bold fonts) which is crucial to an improvement of the key rate.

Protocol 2 (virtual protocol):
Before the commencement of the protocol, Alice and Bob agree on constants L and N_{em} as well as functions $N_{\mathrm{fin}}(N)$, $\boldsymbol{x}^*(N, y^N, N_{\mathrm{fin}}, \boldsymbol{t})$, and probabilities $p(C|N, N_{\mathrm{fin}})$ over full-rank $N \times N$ binary matrices C.

(i) Alice and Bob repeat the following procedures for N_{em} rounds.

- Alice prepares an L-qubit register $A^{(1)},...,A^{(L)}$, a reference $R := R^{(1)},...,R^{(L)}$, and L optical pulses (system $1,...,L$) in the following state:

$$2^{-L/2} \bigotimes_{l=1}^{L} \sum_{s^{(l)}=0,1} \left| s^{(l)} \right\rangle_{A^{(l)}} \mathrm{e}^{\pi \mathrm{i} s^{(l)} \hat{n}_l} \left| \Psi_\sigma \right\rangle_{lR^{(l)}}, \qquad (4)$$

where $\mathrm{Tr}_R \left(\bigotimes_{l=1}^{L} \left| \Psi_\sigma \right\rangle \left\langle \Psi_\sigma \right|_{lR^{(l)}} \right) = \sigma \otimes \cdots \otimes \sigma$, and $\hat{n}_l$ is the photon number operator for the

l-th pulse. She sends Bob the L optical pulses through the quantum channel.

- Bob measures the photon number of each of the received pulses. He also generates a uniformly random binary number q.
  - If Bob detects only one photon in the block and the generated random number q is 0, he announces "success" and Alice keeps her register qubits $(A^{(1)},...,A^{(L)})$. Let i be the position of the pulse with the detection. Bob randomly selects $j \in \{1,...,L\}\backslash\{i\}$ and records the ordered pair $(i \to j)$. [Success round]
  - If the above condition is not satisfied, Bob announces "failure" and Alice discards her qubits. [Failure round]

(ii) Let N be the number of the success rounds. By proper indexing, Alice's qubit registers are represented by $(A_1^{(1)},...,A_1^{(L)}),...,(A_N^{(1)},...,A_N^{(L)})$ and Bob's records of ordered pairs are represented by $(i_1 \to j_1),...,(i_N \to j_N)$.

(iii) Bob announces the sequence of unordered pairs $(i_1,j_1),...,(i_N,j_N)$. He additionally announces the ordered pairs $(i_1 \to j_1),...,(i_N \to j_N)$.

(iv) According to the ordered pairs $(i_k \to j_k)$ $(k \in \{1,...,N\})$, Alice applies a CNOT operation between qubits $A_k^{(i_k)}$ and $A_k^{(j_k)}$ with $A_k^{(i_k)}$ being control and $A_k^{(j_k)}$ being target. She stores qubit $A_k^{(j_k)}$ as the kth sifted key qubit, which she renames as A_k. **She then measures qubit $A_k^{(i_k)}$ in the phase basis to obtain a binary outcome b_k. She also performs phase-basis measurement on each of the $L-2$ qubits $A_k^{(l)}$ $(l \in \{1,...,L\} \setminus \{i_k,j_k\})$ to count the number $a_k \in \{0,...,L-2\}$ of the qubits with outcome 1. Alice records $y_k = (a_k,b_k)$.** At the end, she has N sifted key qubits $A' := A_1,...,A_N$, and the sequence $y^N := y_1,...,y_N$.

(v) Alice chooses and announces a bit error correcting code.

(vi) Let $N_{\rm fin} := N_{\rm fin}(N)$. Alice draws a full-rank $N \times N$ binary matrix C with the probability $p(C|N,N_{\rm fin})$ and announces $N \times N_{\rm fin}$ matrix $C_{PA} := C\,(\boldsymbol{I}_{N_{\rm fin}}\ \boldsymbol{O})^T$. She acts a unitary $U(C) = \sum_{\boldsymbol{z}\in\{0,1\}^N} |\boldsymbol{z}C\rangle\langle\boldsymbol{z}|_{A'} = \sum_{\boldsymbol{x}\in\{0,1\}^N} |\boldsymbol{x}(C^{-1})^T{}_X\rangle\langle\boldsymbol{x}_X|_{A'}$ on her sifted key qubits, and performs phase basis measurement on the subsystem $A_{N_{\rm fin}+1},...,A_N$ to obtain $(N-N_{\rm fin})$-bit sequence $\boldsymbol{t}$. **Using y^N and $\boldsymbol{t}$, Alice computes $\boldsymbol{x}^* := \boldsymbol{x}^*(N,y^N,N_{\rm fin},\boldsymbol{t})$** and acts a unitary $U'(\boldsymbol{x}^*) = \sum_{\boldsymbol{x}'\in\{0,1\}^{N_{\rm fin}}} |(\boldsymbol{x}'\oplus\boldsymbol{x}^*\tilde{H}^T)_X\rangle\langle\boldsymbol{x}'_X|_A$ on the remaining $N_{\rm fin}$ qubits $A := A_1,...,A_{N_{\rm fin}}$ (final key qubits), where $\tilde{H}$ is the $N_{\rm fin} \times N$ matrix $(\boldsymbol{I}_{N_{\rm fin}}\ \boldsymbol{O})\,C^{-1}$.

(vii) She performs bit basis measurement on the final key qubits A and obtains the final key $\boldsymbol{z}_A^{\rm fin}$.

We choose the parameters in Protocol 2 according to those of Protocol 1 as follows. The constants L and $N_{\rm em}$ and the function $N_{\rm fin}(N)$ are the same as those of Protocol 1. The probability $p(C|N,N_{\rm fin})$ is chosen to satisfy

$$\sum_{C:C(\boldsymbol{I}_{N_{\rm fin}}\ \boldsymbol{O})^T=C_{PA}} p(C|N,N_{\rm fin}) = p'(C_{PA}|N,N_{\rm fin}). \quad (5)$$

If Alice performed bit basis measurement on her register qubits of (4), she obtains the random bit sequence $s^{(1)},...,s^{(L)}$ with the same probability and the L optical pulses in the same state as those in Protocol 1. In addition, all the quantum operations of Alice in Protocol 2, which are composed of permutations of the bit basis, are equivalent to the classical information processing in Protocol 1. (Note that $U'(\boldsymbol{x}^*)$ dose not change the bit basis of the qubits.) Furthermore, as shown in the original paper [4], Bob announces unordered pairs (i_k,j_k) in Protocol 2 with the same probability as in Protocol 1. Therefore, for every attack of Eve in Protocol 1, we can define a corresponding attack in Protocol 2 by letting Eve ignore the ordered pairs $(i_k \to j_k)$. Then, by setting the parameters as mentioned above and with the attack by Eve as defined above, we can conclude that the final state of Alice and Eve at the end of (vii) in Protocol 2 is equal to $\rho^{\rm fin}_{AE|N_{\rm fin}}$ in Protocol 1.

On the other hand, let $\rho^{\rm virt}_{AE|N_{\rm fin}}$ be the quantum state on the Alice's final key qubits A and Eve's system E at the end of (vi) in Protocol 2. If $\rho^{\rm virt}_{AE|N_{\rm fin}}$ satisfies

$$\sum_{N_{\rm fin}\geq 1} \Pr(N_{\rm fin})\left(1-F\left(\rho^{\rm virt}_{A|N_{\rm fin}}, |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A\right)\right) \leq \eta', \quad (6)$$

where $|\mathbf{0}_X\rangle := |0_X\rangle^{\otimes N_{\rm fin}}$ and $\rho^{\rm virt}_{A|N_{\rm fin}} := {\rm Tr}_E(\rho^{\rm virt}_{AE|N_{\rm fin}})$, and Eve performs the attack as defined above, the left-hand side of (1) is proved to satisfy

$$\frac{1}{2}\sum_{N_{\rm fin}\geq 1} \Pr(N_{\rm fin})\left\|\rho^{\rm fin}_{AE|N_{\rm fin}} - \rho^{\rm ideal}_{AE|N_{\rm fin}}\right\|_1 \leq \sqrt{1-(1-\eta')^2} \leq \sqrt{2\eta'}, \quad (7)$$

and thus Protocol 1 is $\sqrt{2\eta'}$-secret [21, 22].

The fidelity in the left-hand side of (6) is equal to the probability that Alice obtains $N_{\rm fin}$-bit sequence $\mathbf{0} := (0\cdots0)$ when she measures $\rho^{\rm virt}_{AE|N_{\rm fin}}$ in the phase basis. We therefore consider the alternative procedure (vii)' after (vi) in Protocol 2 as follows:

(vii)' She performs phase basis measurement on the final key qubits A and obtains the final-phase key $\boldsymbol{x}_A^{\rm fin}$.

Using $\boldsymbol{x}_A^{\rm fin}$, the fidelity in (6) is given by

$$F\left(\rho^{\rm virt}_{A|N_{\rm fin}}, |\mathbf{0}_X\rangle\langle\mathbf{0}_X|_A\right) = \Pr(\boldsymbol{x}_A^{\rm fin} = \mathbf{0}|N_{\rm fin}). \tag{8}$$

In order to evaluate the right-hand side, we introduce a third protocol which faithfully simulates the statistics of $\boldsymbol{x}_A^{\rm fin}$ as follows.

Protocol 3 (estimation protocol):

(i) Alice and Bob follow the step (i) of Protocol 2 except that Alice measures the L qubits in the phase basis immediately after its preparation, and obtains a bit sequence $\mathfrak{s}^{(1)},...,\mathfrak{s}^{(L)}$. She records $m = \sum_{l=1}^{L}\mathfrak{s}^{(l)}$ $(\in \{0,...,L\})$ for every round. In the success rounds, Alice records the sequence $(\mathfrak{s}_k^{(1)},...,\mathfrak{s}_k^{(L)})$. Let v_M be the number of rounds with $m = M$, where $\sum_M v_M = N_{\rm em}$.

(ii) By proper indexing, Alice has the bit sequences $(\mathfrak{s}_1^{(1)},...,\mathfrak{s}_1^{(L)}),...,(\mathfrak{s}_N^{(1)},...,\mathfrak{s}_N^{(L)})$. Bob has the sequence of ordered pairs, $(i_1 \to j_1),...,(i_N \to j_N)$.

(iii) Bob announces the sequence of unordered pairs $(i_1, j_1),...,(i_N, j_N)$. He additionally announces the ordered pairs $(i_1 \to j_1),...,(i_N \to j_N)$.

(iv) With the ordered pairs $(i_k \to j_k)$ $(k \in \{1,...,N\})$, Alice computes the following variables for $k \in \{1,...,N\}$.

$$x_k := \mathfrak{s}_k^{(j_k)} \tag{9}$$

$$m_k := \sum_{l\in\{1,...,L\}} \mathfrak{s}_k^{(l)} \tag{10}$$

$$u_k := \mathfrak{s}_k^{(i_k)} \tag{11}$$

$$a_k := \sum_{l\in\{1,...,L\}\backslash\{i_k,j_k\}} \mathfrak{s}_k^{(l)} = m_k - u_k - x_k \tag{12}$$

$$b_k := \mathfrak{s}_k^{(i_k)} \oplus \mathfrak{s}_k^{(j_k)} = u_k \oplus x_k \tag{13}$$

$$y_k := (a_k, b_k) \tag{14}$$

At the end, she has a sifted-phase key $\boldsymbol{x}_A := (x_1\cdots x_N)(= x^N)$ and the sequence $y^N := y_1,...,y_N$ as well as the sequences $m^N := m_1,...,m_N$ and $u^N := u_1,...,u_N$.

(vi) She draws a full-rank $N \times N$ binary matrix C with probability $p(C|N, N_{\rm fin})$. She computes $H := (\boldsymbol{O}\ \boldsymbol{I}_{N-N_{\rm fin}})C^{-1}$, $\tilde{H} := (\boldsymbol{I}_{N_{\rm fin}}\ \boldsymbol{O})C^{-1}$, and $\boldsymbol{t} := \boldsymbol{x}_A H^T$. Using y^N and $\boldsymbol{t}$, she computes $\boldsymbol{x}^* := \boldsymbol{x}^*(N, y^N, N_{\rm fin}, \boldsymbol{t})$ and obtains the final-phase key $\boldsymbol{x}_A^{\rm fin} = (\boldsymbol{x}_A \oplus \boldsymbol{x}^*)\tilde{H}^T$.

Since all the quantum operations of Alice in Protocol 2 are composed of permutations of the phase basis states, Alice's procedures of determining $\boldsymbol{x}_A^{\rm fin}$ in Protocol 2 with (vii)' and those in Protocol 3 are equivalent. (We used the property of CNOT operation to derive (9) and (13).)

It is clear in Protocol 3 that the following inequality always holds:

$$\Pr(N_{\rm fin} \geq 1, \boldsymbol{x}_A^{\rm fin} \neq \mathbf{0}) \leq \Pr(N_{\rm fin} \geq 1, \boldsymbol{x}_A \neq \boldsymbol{x}^*). \tag{15}$$

With (8), the left-hand side of the above inequality is identified as the left-hand side of (6). Therefore, if we can ensure

$$\Pr(N_{\rm fin} \geq 1, \boldsymbol{x}_A \neq \boldsymbol{x}^*) \leq \eta', \tag{16}$$

the condition (6) is satisfied. The parameter η' in (16) can be regarded as an upper-bound on the probability that Alice misidentifies the sequence $\boldsymbol{x}_A$ (phase error patterns) and computes the wrong sequence $\boldsymbol{x}^*$ when given the sequence y^N and the syndrome $\boldsymbol{t}$.

The bound η' can be further related to the number of candidates of $\boldsymbol{x}_A$, given N and y^N. Suppose that a family of sets $T(N, y^N)$ satisfies

$$\Pr(N \geq 1, \boldsymbol{x}_A \notin T(N, y^N)) \leq \eta. \tag{17}$$

Suppose further that a function $H_{PA}(N)$ which depends only on N satisfies,

$$NH_{PA}(N) \geq \log\left|T(N, y^N)\right| \text{ for all } y^N, \tag{18}$$

where $\left|T(N, y^N)\right|$ is the cardinality of $T(N, y^N)$. We assume that the selection of H^T with probability $p(C|N, N_{\rm fin})$ in Protocol 3 is equivalent to universal$_2$ hashing, i.e.

$$\begin{aligned}&\forall \boldsymbol{x}_1, \boldsymbol{x}_2 \in \{0,1\}^N\\ &\quad \Pr(\boldsymbol{x}_1 H^T = \boldsymbol{x}_2 H^T|N, N_{\rm fin}) \leq 2^{-(N-N_{\rm fin})},\end{aligned} \tag{19}$$

which amounts to require $p'(C|N, N_{\rm fin})$ in Protocol 1 to be dual universal$_2$ hashing [23]. Then, by setting

$$N_{\rm fin}(N) = \max\{N(1 - H_{PA}(N) - s/N), 0\}, \tag{20}$$

we obtain, from the union bound,

$$\Pr(N_{\rm fin} \geq 1, \boldsymbol{x}_A \neq \boldsymbol{x}^*) \leq \eta + 2^{-s}, \tag{21}$$

because learning $\boldsymbol{t} = \boldsymbol{x}_A H^T$ eliminates all the wrong candidates in $T(N, y^N)$ except probability no more than 2^{-s}. Then, from (6), (7), (21), and by identifying $\eta' = \eta + 2^{-s}$, Protocol 1 is $\sqrt{2(\eta + 2^{-s})}$-secret.

The conclusion of this subsection is as follows. If we can define a family of sets $T(N, y^N)$ which satisfies

$$\Pr(N \geq 1, \boldsymbol{x}_A \notin T(N, y^N)) \leq \eta \tag{22}$$

in Protocol 3 and

$$\forall y^N, \ \ \log\left|T(N, y^N)\right| \leq NH_{PA}(N), \tag{23}$$

for a function $H_{PA}(N)$ which depends only on N, then by setting

$$N_{\rm fin}(N) = \max\{N(1 - H_{PA}(N) - s/N), 0\}, \tag{24}$$

Protocol 1 can be made $\sqrt{2(\eta + 2^{-s})}$-secret.

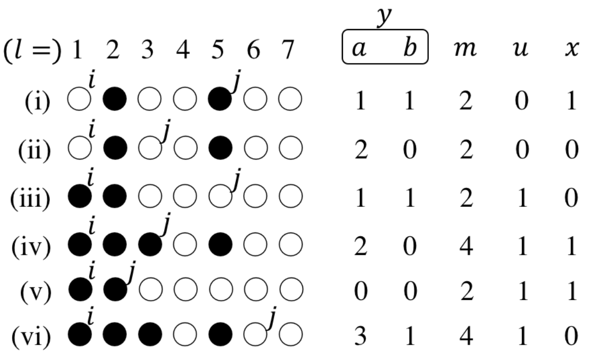

FIG. 3. The illustration of how additional information $y = (a, b)$ works when $L = 7$. The white circle denotes $\mathfrak{s}^{(l)} = 0$ and the black circle denotes $\mathfrak{s}^{(l)} = 1$. The pairs {(i), (ii)}, {(iii), (v)}, and {(iv), (vi)} correspond to the cases in which Eve's attacks are the same but different positions are chosen for j due to the random selection by Bob.

C. The origin of the improvement

Here we give a crude explanation of why we expect an improvement of the key rate from the introduction of additional information $y_k = (a_k, b_k)$ collected by Alice in Protocol 2. In the asymptotic limit, the ratio $N_{\rm fin}/N$ is given by $N_{\rm fin}/N = 1 - H_{PA}$, where H_{PA} is the fraction for the shortening in privacy amplification, representing an upper-bound on the amount of leaked information. In the original security proof, for the implementation without phase randomization, it is simply given by $H_{PA} = \max h(e_{\rm ph})$, where $e_{\rm ph}$ is the average phase error probability of a sifted key qubit. In this framework, the best strategy by Eve is to make $e_{\rm ph}$ as high as possible. It is simply achieved by her measuring all the photon number parities $\mathfrak{s}^{(1)}, ..., \mathfrak{s}^{(L)}$, followed by choosing the index i such that $\mathfrak{s}^{(i)} = 0$, as illustrated in Figure 3, (i) and (ii). Since the index j is chosen randomly, phase error occurs (like (i)) with probability $m/(L-1)$ for a round, resulting in $e_{\rm ph} = (\sum_k m_k/(L-1))/N$. Hence, Eve will only have to choose N rounds with higher values of $m = \sum_l \mathfrak{s}^{(l)}$.

The introduction of $y_k = (a_k, b_k)$ drastically changes Eve's strategy. In this case, the asymptotic fraction will be given by a conditional entropy as $H_{PA} = \max \sum_y p(y) h(e_{\rm ph}(y))$, where $e_{\rm ph}(y)$ is the phase error probability conditioned on $y = (a, b)$. As seen in Figure 3, case (i) and case (ii) have distinct values of y, and thus no longer contributes to H_{PA}. In order to increase the conditional entropy, Eve must mix the case with the same values of y, such as cases (iii) and (iv). Due to the randomness of index j, these inevitably lead to occurrence of other cases like (v) and (vi), and this continues. Notice that these cases involve different values of $m = \sum_l \mathfrak{s}^{(l)}$. Hence simply choosing higher values of m no longer works for Eve, and she must find an appropriate balance over the values of m to make the conditional entropy higher.

We emphasize here that the above constraint for Eve is quite natural once we notice that her true objective is not to increase the phase error probability but to learn the optical phase difference $s^{(i)} \oplus s^{(j)}$ between the pair of pulses. The value of $s^{(i)} \oplus s^{(j)}$ is encoded on the relative phase of superposition states of (i) and (iii), and on that of (ii) and (iv), for example. In this sense, the introduction of $y_k = (a_k, b_k)$ can be interpreted as providing more precise evaluation of Eve's ability to learn Alice's sifted key bits. The reduction to Protocol 3 in the previous subsection is essentially regarded as reducing the evaluation to a problem on classical random variables possessed by Alice alone. It is nonetheless convoluted and involves many variables and constraints, but it will be efficiently solved by introducing Lagrange multipliers in the next subsection.

D. The estimation of the number of phase error patterns

In this subsection, we give an explicit construction of $T(N, y^N)$, a family of the set of likely phase error patterns. The construction has free parameters $\boldsymbol{\nu}$ and $\boldsymbol{\xi}$ served as Lagrange multipliers, which will be defined later. While any proper choice of the parameters makes Protocol 1 secure, the key length will depend on the choice.

In what follows, we adopt the following notations. For a finite set $\mathcal{W}$, we define $\mathcal{P}_{\mathcal{W}}$ as the set of all the probability mass functions on $\mathcal{W}$. When a set Γ is associated with $\mathcal{W}$ uniquely by a function $f_\Gamma : \mathcal{W} \to \Gamma$, we denote the distribution on Γ induced from $P \in \mathcal{P}_{\mathcal{W}}$ by P_Γ, which satisfies

$$P_\Gamma(g) = \sum_{w \in \mathcal{W}: f_\Gamma(w) = g} P(w) \tag{25}$$

for $g \in \Gamma$. For a finite set Ω, the type $\tilde{P}_{\omega^n} \in \mathcal{P}_\Omega$ for $\omega^n = (\omega_1, ..., \omega_n) \in \Omega^n$ is defined by

$$\tilde{P}_{\omega^n}(\omega) = \frac{1}{n} \left| \{ i \in \{1, ..., n\} : \omega_i = \omega \} \right| \tag{26}$$

for $\omega \in \Omega$.

Let $\mathcal{M} = \{0, ..., L\}$, $\mathcal{U} = \mathcal{X} = \{0, 1\}$ and $\mathcal{Y} = \{(a, b) | a \in \{0, ..., L-2\},\ b \in \{0, 1\}\}$ be the set of all the possible values of m_k, u_k, x_k, and y_k in Protocol 3, respectively. Let $\mathcal{W}$ be the finite set defined as follows:

$$\mathcal{W} = \{(M, U, X) \in \mathcal{M} \times \mathcal{U} \times \mathcal{X} : 0 \le M - U - X \le L - 2\}. \tag{27}$$

Let $f_{\mathcal{M}} : \mathcal{W} \to \mathcal{M}$, $f_{\mathcal{M} \times \mathcal{U}} : \mathcal{W} \to \mathcal{M} \times \mathcal{U}$, and $f_{\mathcal{X}} : \mathcal{W} \to \mathcal{X}$ be the projections from the Cartesian product $\mathcal{M} \times \mathcal{U} \times \mathcal{X}$ restricted on $\mathcal{W}$. Let $f_{\mathcal{Y}} : \mathcal{W} \to \mathcal{Y}$ be the function defined by

$$f_{\mathcal{Y}}(M, U, X) := (M - U - X, U \oplus X). \tag{28}$$

In Protocol 3, x_k, u_k, and m_k are related to y_k by

$$y_k = f_{\mathcal{Y}}(m_k, u_k, x_k), \tag{29}$$

and hence y^N is uniquely determined once sequences x^N, m^N, and u^N are given. We denote the binomial distribution with L trials by $\mathfrak{b}_{L,p} \in \mathcal{P}_{\mathcal{M}}$, where

$$\mathfrak{b}_{L,p}(M) := \binom{L}{M} p^M (1-p)^{L-M}. \tag{30}$$

When Eve's attack is fixed in Protocol 3, the joint probability distribution of $\boldsymbol{v} := (v_0, ..., v_L), N, x^N, m^N$, and u^N, denoted by $\mathfrak{P}$, is determined. In what follows, $\Pr\{\cdot\}$ denotes the probability under $\mathfrak{P}$. Regardless of Eve's attacks, the following three conditions hold for $\mathfrak{P}$.

1. The variable $\boldsymbol{v} = (v_0, ..., v_L)$ obeys multinomial distribution

$$\Pr\{\boldsymbol{v}\} = \frac{N_{\mathrm{em}}!}{\prod_{M=0}^{L} v_M!} \prod_{M=0}^{L} \left(\mathfrak{b}_{L,p_{\mathrm{odd}}}(M)\right)^{v_M} \tag{31}$$

with p_{odd} satisfying

$$p_{\mathrm{odd}} \leq p_{\mathrm{src}}. \tag{32}$$

This property can be confirmed if we rewrite the initial state of Protocol 3, given by (4), as

$$\begin{aligned} &2^{-L/2} \bigotimes_{l=1}^{L} \sum_{s^{(l)}=0,1} |s^{(l)}\rangle_{A^{(l)}} \, \mathrm{e}^{\pi \mathrm{i} s^{(l)} \hat{n}_l} \, |\Psi_\sigma\rangle_{lR^{(l)}} \\ &= \bigotimes_{l=1}^{L} \Bigg(|0_X^{(l)}\rangle_{A^{(l)}} \frac{1+(-1)^{\hat{n}_l}}{2} |\Psi_\sigma\rangle_{lR^{(l)}} \\ &\qquad\qquad + |1_X^{(l)}\rangle_{A^{(l)}} \frac{1-(-1)^{\hat{n}_l}}{2} |\Psi_\sigma\rangle_{lR^{(l)}} \Bigg) \\ &= \bigotimes_{l=1}^{L} \left(|0_X^{(l)}\rangle_{A^{(l)}} \, \Pi_l^{\mathrm{even}} \, |\Psi_\sigma\rangle_{lR^{(l)}} + |1_X^{(l)}\rangle_{A^{(l)}} \, \Pi_l^{\mathrm{odd}} \, |\Psi_\sigma\rangle_{lR^{(l)}} \right), \end{aligned} \tag{33}$$

where $\Pi_l^{\mathrm{even(odd)}}$ is the projection operator onto the even (odd) photon number subspace. The probability of obtaining $\mathfrak{s}^{(l)} = 1$ when measuring the l-th qubit of (33) in phase basis, denoted by p_{odd}, is given by

$$\begin{aligned} p_{\mathrm{odd}} &:= \mathrm{Tr}\left(\Pi_l^{\mathrm{odd}} \, |\Psi_\sigma\rangle \, \langle\Psi_\sigma|_{lR^{(l)}} \, \Pi_l^{\mathrm{odd}}\right) \\ &= \mathrm{Tr}\left(\Pi_l^{\mathrm{odd}} \sigma\right). \end{aligned} \tag{34}$$

Hence the number $M = \sum_l \mathfrak{s}^{(l)}$ follows the probability $\mathfrak{b}_{L,p_{\mathrm{odd}}}(M)$. Since p_{odd} is equal to the probability of emitting odd number of photons in a pulse, (32) holds by definition.

2. For the type $\tilde{P}_{m^N}$ of the random variable m^N,

$$^\forall M \in \mathcal{M}, \ \Pr\left\{ N\tilde{P}_{m^N}(M) \leq v_M \,\middle|\, N \geq 1 \right\} = 1 \tag{35}$$

holds, which is obvious from the definition of the type.

3. Since Bob randomly chooses j_k out of $\{1, ..., L\} \setminus \{i_k\}$ in each success round, the probability of obtaining $x_k = 1$ in the kth success round given m_k and u_k is $(m_k - u_k)/(L-1)$. Therefore,

$$\Pr\left\{ x^N \,\middle|\, N, m^N, u^N \right\} = \prod_{k=1}^{N} [c(m_k, u_k)]^{x_k} [1 - c(m_k, u_k)]^{1-x_k} \tag{36}$$

holds for $N \geq 1$, where

$$c(M, U) := \frac{M - U}{L - 1}. \tag{37}$$

Let $\boldsymbol{\nu} = \{\nu_0, ..., \nu_L\}$ be the set of real non-negative constants which satisfy $\nu_M = 0$ for all $M < Lp_{\mathrm{src}}$. Let $\mathcal{P}^{N,\boldsymbol{\nu},\delta_1} \subseteq \mathcal{P}_{\mathcal{W}}$ be the set of the probability mass functions defined by

$$\begin{aligned} \mathcal{P}^{N,\boldsymbol{\nu},\delta_1} := \Bigg\{ P \in \mathcal{P}_{\mathcal{W}} : &\ \mathbb{E}_{M \sim P_{\mathcal{M}}}[\nu_M] \\ &\leq \frac{N_{\mathrm{em}}}{N} \left(\mathbb{E}_{M \sim \mathfrak{b}_{L,p_{\mathrm{src}}}}[\nu_M] + \delta_1 \right) \Bigg\}. \end{aligned} \tag{38}$$

From the conditions 1 and 2 of $\mathfrak{P}$, the type $\tilde{P}_{m^N,u^N,x^N} \in \mathcal{P}_{\mathcal{W}}$ in Protocol 3 belongs to $\mathcal{P}^{N,\boldsymbol{\nu},\delta_1}$ with a high probability. More precisely, we have the following proposition with its proof given in Appendix A.

Proposition 1. *Let $\boldsymbol{\nu} = \{\nu_0, ..., \nu_L\}$ be the set of non-negative constants which satisfy $\nu_M = 0$ for all $M < Lp_{\mathrm{src}}$. Suppose that η_1 and δ_1 satisfy*

$$\max_{Q \in \mathcal{Q}} 2^{-N_{\mathrm{em}} D(Q \| \mathfrak{b}_{L,p_{\mathrm{src}}})} \leq \eta_1, \tag{39}$$

where the convex set $\mathcal{Q}$ is defined as

$$\mathcal{Q} = \left\{ Q \in \mathcal{P}_{\mathcal{M}} : \mathbb{E}_{M \sim Q}[\nu_M] \geq \mathbb{E}_{M \sim \mathfrak{b}_{L,p_{\mathrm{src}}}}[\nu_M] + \delta_1 \right\}. \tag{40}$$

When the random variables $(\boldsymbol{v}, N, m^N, u^N, x^N)$ satisfy (31) and (35), the following inequality holds:

$$\Pr\{N \geq 1, \tilde{P}_{m^N,u^N,x^N} \notin \mathcal{P}^{N,\boldsymbol{\nu},\delta_1}\} \leq \eta_1. \tag{41}$$

Let $\boldsymbol{\xi} = \{\xi_{M,U} : (M,U) \in \mathcal{M} \times \mathcal{U}, \ 0 \leq c(M,U) \leq 1\}$ be the set of real constants satisfying $\left|\xi_{M,U}\right| \leq 1$. Let $\mathcal{P}^{\boldsymbol{\xi},\delta_2} \subseteq \mathcal{P}_{\mathcal{W}}$ be the set of the probability mass functions defined as

$$\mathcal{P}^{\boldsymbol{\xi},\delta_2} := \Big\{P \in \mathcal{P}_{\mathcal{W}} : \mathbb{E}_{(M,U,X)\sim P}\left[(X - c(M,U))\,\xi_{M,U}\right] \le \frac{\delta_2}{3} + \left[\left(\frac{\delta_2}{3}\right)^2 + 2\delta_2 \mathbb{E}_{(M,U)\sim P_{\mathcal{M}\times\mathcal{U}}}\left[c(M,U)\,(1 - c(M,U))\,\xi_{M,U}^2\right]\right]^{\frac{1}{2}}\Bigg\}. \tag{42}$$

Since the right-hand side of the inequality is a concave function with respect to P, $\mathcal{P}^{\boldsymbol{\xi},\delta_2}$ is a convex subset of $\mathcal{P}_{\mathcal{W}}$. From the condition 3 of $\mathfrak{P}$, the type $\tilde{P}_{m^N,u^N,x^N} \in \mathcal{P}_{\mathcal{W}}$ in Protocol 3 belongs to $\mathcal{P}^{\boldsymbol{\xi},\delta_2(N)}$ with a high probability. More precisely, we have the following proposition with its proof given in Appendix B.

Proposition 2. *Let $\boldsymbol{\xi} = \{\xi_{M,U} : (M,U) \in \mathcal{M}\times\mathcal{U},\ 0 \le c(M,U) \le 1\}$ be the set of real constants which satisfy $\left|\xi_{M,U}\right| \le 1$. Suppose that η_2 and $\{\delta_2(N)\}_{N=1,2,\dots}$ satisfy*

$$\exp\left[-N\delta_2(N)\right] \le \eta_2. \tag{43}$$

When the random variables (N, m^N, u^N, x^N) satisfy the condition (36), the following inequality holds:

$$\Pr\left\{N \ge 1, \tilde{P}_{m^N,u^N,x^N} \notin \mathcal{P}^{\boldsymbol{\xi},\delta_2(N)}\right\} \le \eta_2. \tag{44}$$

We define the following convex set of probability mass functions over $\mathcal{W}$,

$$\mathcal{E} := \left\{P : P \in \mathcal{P}^{N,\boldsymbol{\nu},\delta_1} \cap \mathcal{P}^{\boldsymbol{\xi},\delta_2(N)}\right\}, \tag{45}$$

which satisfies

$$\Pr\{N \ge 1, \tilde{P}_{m^N,u^N,x^N} \notin \mathcal{E}\} \le \eta_1 + \eta_2, \tag{46}$$

if (η_1, δ_1) and $(\eta_2, \{\delta_2(N)\}_{N=1,\dots})$ satisfy (39) and (43), respectively (union bound). With $\mathcal{E} \subseteq \mathcal{P}_{\mathcal{W}}$, we define the family of the set of likely phase error patterns $T(N, y^N)$ as follows:

$$T(N, y^N) := \{x^N \in \mathcal{X}^N : {}^{\exists}P \in \mathcal{E}, P_{\mathcal{X}\times\mathcal{Y}} = \tilde{P}_{x^N,y^N}\}. \tag{47}$$

If $\tilde{P}_{m^N,u^N,x^N} \in \mathcal{E}$, by setting $P = \tilde{P}_{m^N,u^N,x^N}$, we have $P_{\mathcal{X}\times\mathcal{Y}} = \tilde{P}_{x^N,y^N}$, and thus $x^N \in T(N, y^N)$. Therefore, from (46), we also have

$$\Pr\{N \ge 1, x^N \notin T(N, y^N)\} \le \eta_1 + \eta_2. \tag{48}$$

Here, the upper-bound of $\left|T(N, y^N)\right|$ is obtained by using the following lemma.

Lemma 1 (The upper bound on the number of distinct patterns compatible to a joint probability distribution)**.** *Let $\mathcal{W}$ be a finite set, and $\mathcal{E}$ be a closed convex subset of $\mathcal{P}_{\mathcal{W}}$. Let $\mathcal{X}$ and $\mathcal{Y}$ be sets associated with $\mathcal{W}$ by functions $f_{\mathcal{X}} : \mathcal{W} \to \mathcal{X}$ and $f_{\mathcal{Y}} : \mathcal{W} \to \mathcal{Y}$. For $y^N \in \mathcal{Y}^N$, define the set*

$$T(y^N) := \{x^N \in \mathcal{X}^N : {}^{\exists}P \in \mathcal{E}, P_{\mathcal{X}\times\mathcal{Y}} = \tilde{P}_{x^N,y^N}\}. \tag{49}$$

Then the cardinality of the set $T(y^N)$ satisfies

$$\left|T(y^N)\right| \le \max_{P\in\mathcal{E}:P_{\mathcal{Y}}=\tilde{P}_{y^N}} 2^{NH(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}}}. \tag{50}$$

Although we have assumed specific choices of $\mathcal{W}, f_{\mathcal{X}}, f_{\mathcal{Y}}$, and $\mathcal{E}$, we can generally prove Lemma 1 without such specification, as shown in Appendix C. Since what we need is a bound on $\left|T(N, y^N)\right|$ independent of y^N as in (23), we use Lemma 1 with $T(y^N) = T(N, y^N)$ and take the maximum with all the possible sequence y^N as follows:

$$\begin{aligned}
&\max_{y^N} \log\left|T(N, y^N)\right| \\
&\le \max_{y^N} \max_{P\in\mathcal{E}:P_{\mathcal{Y}}=\tilde{P}_{y^N}} NH(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}} \\
&\le \max_{P\in\mathcal{E}} NH(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}}.
\end{aligned} \tag{51}$$

Combining Proposition 1 and 2, (45), (47), (48), and (51), we arrive at the following theorem.

Theorem 1 (The main result)**.** *Let $\boldsymbol{\nu} = \{\nu_M : M \in \mathcal{M}\}$ be the set of non-negative constants which satisfy $\nu_M = 0$ for all $M < Lp_{\mathrm{src}}$. Let $\boldsymbol{\xi} = \{\xi_{M,U} : (M,U) \in \mathcal{M}\times\mathcal{U},\ 0 \le c(M,U) \le 1\}$ be the set of real constants which satisfy $\left|\xi_{M,U}\right| \le 1$. Let η_1 and δ_1 be non-negative numbers which satisfy*

$$\max_{Q\in\mathcal{P}_{\mathcal{M}}:\mathbb{E}_{M\sim Q}[\nu_M]\ge\mathbb{E}_{M\sim\mathfrak{b}}[\nu_M]+\delta_1} 2^{-N_{\mathrm{em}}D(Q\|\mathfrak{b})} \le \eta_1, \tag{52}$$

where $\mathfrak{b} := \mathfrak{b}_{L,p_{\mathrm{src}}}$. Let η_2 and $\{\delta_2(N)\}_{N=1,\dots}$ be non-negative numbers which satisfy

$$\exp\left[-N\delta_2(N)\right] \le \eta_2. \tag{53}$$

Let $H_{PA}(N)$ be a function of N which satisfies

$$\max_{P\in\mathcal{E}} H(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}} \le H_{PA}(N), \tag{54}$$

where $\mathcal{E}$ is given in (45). Then, if the three conditions (31), (35), and (36) are satisfied, there exists $T(N, y^N)$ which satisfies

$$\Pr\{N \ge 1, x^N \notin T(N, y^N)\} \le \eta_1 + \eta_2 \tag{55}$$

in Protocol 3, and

$$\forall y^N,\ \ \log\left|T(N, y^N)\right| \le NH_{PA}(N). \tag{56}$$

Combining this and the conclusion of the section II B, we conclude that Protocol 1 can be made $\sqrt{2(\eta_1 + \eta_2 + 2^{-s})}$-secret by setting $N_{\mathrm{fin}}(N)$ as in (24).

III. NUMERICAL SIMULATIONS

We numerically simulate the net key gain per pulse $(N_{\mathrm{fin}} - N_{EC})/N_{\mathrm{em}}L = N(1 - H_{PA}(N) - s/N -$

$f_{EC}h(e_{\rm bit}))/N_{\rm em}L$ of the RRDPS protocol using Theorem 1. We set

$$NH_{PA}(N) = \lceil \max_{P\in\mathcal{E}} NH(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}} \rceil, \tag{57}$$

where $\lceil\cdot\rceil$ denotes the ceiling function. Since the conditional entropy function is concave with respect to the joint probability distribution P, what we need is to solve the following constrained convex optimization problem:

$$\begin{aligned} \underset{P\in\mathcal{P}_{\mathcal{W}}}{\text{maximize}} \quad & H(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}}, \\ \text{subject to} \quad & \mathbb{E}_{M\sim P_{\mathcal{M}}}[\nu_M] \le \frac{N_{\rm em}}{N}\left(\mathbb{E}_{M\sim\mathfrak{b}_{L,p_{\rm src}}}[\nu_M] + \delta_1\right), \\ & \mathbb{E}_{(M,U,X)\sim P}\left[(X - c(M,U))\,\xi_{M,U}\right] \\ & \qquad \le \frac{\delta_2(N)}{3} + \left[\left(\frac{\delta_2(N)}{3}\right)^2 + 2\delta_2(N)\mathbb{E}_{(M,U)\sim P_{\mathcal{M}\times\mathcal{U}}}\left[c(M,U)\left(1-c(M,U)\right)\xi^2_{M,U}\right]\right]^{\frac{1}{2}}, \end{aligned} \tag{58}$$

with a proper choice of the constants $\boldsymbol{\nu}$ and $\boldsymbol{\xi}$.

First, we consider the asymptotic limit $N_{\rm em}, N \to \infty$ while the block detection rate $R := N/N_{\rm em}$ remains constant. In this case, we can neglect δ_1 and $\delta_2(N)$, and the optimization problem (58) is reduced to the following simple form:

$$\begin{aligned} \underset{P\in\mathcal{P}_{\mathcal{W}}}{\text{maximize}} \quad & H(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}}, \\ \text{subject to} \quad & \mathbb{E}_{M\sim P_{\mathcal{M}}}[\nu_M] \le \frac{\mathbb{E}_{M\sim\mathfrak{b}_{L,p_{\rm src}}}[\nu_M]}{R}, \\ & \mathbb{E}_{(M,U,X)\sim P}\left[(X - c(M,U))\,\xi_{M,U}\right] = 0. \end{aligned} \tag{59}$$

Here the equality of the second constraint comes from the fact that $\xi_{M,U}$ can be both positive and negative. Finding the best bound on $H(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}}$ by adjusting $\boldsymbol{\nu}$ and $\boldsymbol{\xi}$ is equivalent to solving the following convex optimization problem with the affine constraints:

$$\begin{aligned} \underset{P\in\mathcal{P}_{\mathcal{W}}}{\text{maximize}} \quad & H(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}}, \\ \text{subject to} \quad & P_{\mathcal{M}}(M) \le \frac{\mathfrak{b}_{L,p_{\rm src}}(M)}{R}, \\ & \qquad \forall M\in\mathcal{M},\ M \ge Lp_{\rm src}, \\ & P(M,U,X=1) - c(M,U)P_{\mathcal{M}\times\mathcal{U}}(M,U) = 0, \\ & \qquad \forall (M,U)\in\mathcal{M}\times\mathcal{U},\ 0\le c(M,U)\le 1. \end{aligned} \tag{60}$$

Since the problem is convex, if we can find $P^*(M,U,X) > 0, \boldsymbol{\nu}^*, \boldsymbol{\xi}^*$, and λ^* that satisfy the following Karush-Kuhn-Tucker (KKT) condition, the maximum of $H(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}}$ in the problem (60) is achieved at $P = P^*$.

$$\begin{cases} \nabla_P \Bigg[H(X|Y)_{P_{\mathcal{X}\times\mathcal{Y}}} - \lambda^* \displaystyle\sum_{(M,U,X)\in\mathcal{W}} P(M,U,X) - \sum_{M\in\mathcal{M}} \nu^*_M P_{\mathcal{M}}(M) \\ \qquad\qquad - \displaystyle\sum_{\substack{(M,U)\in\mathcal{M}\times\mathcal{U} \\ 0\le c(M,U)\le 1}} \xi^*_{M,U}\left[P(M,U,X=1) - c(M,U)P_{\mathcal{M}\times\mathcal{U}}(M,U)\right] \Bigg]_{P=P^*} = \mathbf{0}, \\ \qquad\qquad \nu^*_M = 0, \quad \forall M\in\mathcal{M},\ M < Lp_{\rm src}, \\ \nu^*_M \ge 0, \quad \dfrac{\mathfrak{b}_{L,p_{\rm src}}(M)}{R} \ge P^*_{\mathcal{M}}(M), \quad \nu^*_M\left(\dfrac{\mathfrak{b}_{L,p_{\rm src}}(M)}{R} - P^*_{\mathcal{M}}(M)\right) = 0, \quad \forall M\in\mathcal{M},\ M \ge Lp_{\rm src}, \\ \qquad P^*(M,U,X=1) - c(M,U)P^*_{\mathcal{M}\times\mathcal{U}}(M,U) = 0, \quad \forall (M,U)\in\mathcal{M}\times\mathcal{U},\ 0\le c(M,U)\le 1, \\ \qquad \displaystyle\sum_{(M,U,X)\in\mathcal{W}} P^*(M,U,X) = 1. \end{cases} \tag{61}$$

The asymptotic limit H_{PA} of the amount of privacy amplification $H_{PA}(N)$ is then given by

$$H_{PA} = H(X|Y)_{P^*_{\mathcal{X}\times\mathcal{Y}}}. \tag{62}$$

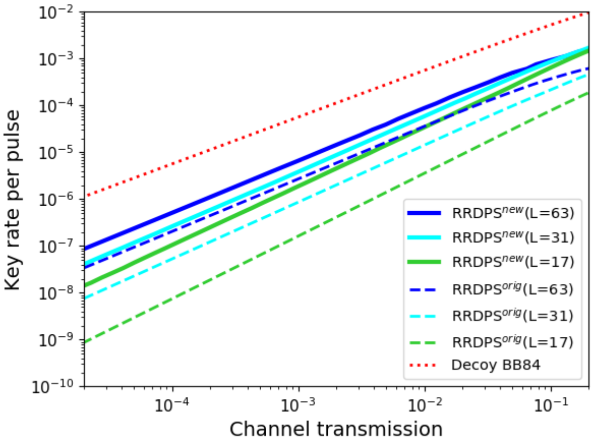

FIG. 4. The asymptotic key rates of the RRDPS protocol by our new analysis (RRDPS^{new}, solid lines) and by the original analysis (RRDPS^{orig}, broken lines). The mean photon number μ of the light source is optimized for each transmission rate. The bit error rate is set to 3%. The dotted line is the rate of the ideal decoy-state BB84 protocol with time-bin implementation, assuming the same bit error rate.

For the numerical simulation of the key rate, we assume that the block detection rate R is given by

$$R = \frac{1}{2}\eta\mu L \exp(-\eta\mu L), \tag{63}$$

where η is an overall transmission rate of the channel and μ is the mean photon number of each pulse from the source. (This rate is equal to the probability of detecting single photon in a block with efficiency 1/2 [4].) We neglect the dark count rate. In addition, we assume that the photon number distribution of each pulse is Poissonian with mean μ. From (34), $p_{\rm odd}$ in this case is given by

$$p_{\rm odd} = {\rm e}^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^{2n+1}}{(2n+1)!} = {\rm e}^{-\mu} \sinh\mu. \tag{64}$$

We set $p_{\rm src} = p_{\rm odd} = {\rm e}^{-\mu}\sinh\mu$. The error correction efficiency f_{EC} is set to 1. We numerically solved (61) and always found a solution. Figure 4 shows the key rates vs. transmission rates by our new analysis and by the original analysis with the key rate of the decoy BB84 protocol with time-bin implementation when $e_{\rm bit} = 3\%$. One can see that our new analysis improves the key rates of the RRDPS protocol for all L compared to the original one. Moreover, we obtain an improvement of more than one order of magnitude in the key rate with relatively small L, which may improve the practicality of the protocol. The improved key rates with our analysis are comparable to that obtained in [18], but our analysis does not require the optical phase randomization.

Next we simulated the key rates in the finite-sized case by solving (58) with a heuristic choice of $\boldsymbol{\nu}$ and $\boldsymbol{\xi}$. Regardless of $N_{\rm em}$, we used $\{\nu_M^* : M \in \mathcal{M}\}$ and $\{\xi_{M,U}^* : (M,U) \in \mathcal{M}\times\mathcal{U},\ 0 \le c(M,U) \le 1\}$, which are obtained as the solutions of (61), to define

$$\boldsymbol{\nu} := \{\nu_M^* : M \in \mathcal{M}\},$$
$$\boldsymbol{\xi} := \left\{ \frac{\xi_{M,U}^*}{\xi_{\max}} : (M,U) \in \mathcal{M}\times\mathcal{U},\ 0 \le c(M,U) \le 1 \right\}, \tag{65}$$

where $\xi_{\max}$ is defined as

$$\xi_{\max} := \max\{ \left|\xi_{M,U}^*\right| : (M,U) \in \mathcal{M}\times\mathcal{U},\ 0 \le c(M,U) \le 1\}. \tag{66}$$

This heuristic choice of $\boldsymbol{\nu}$ and $\boldsymbol{\xi}$ becomes optimal when $N_{\rm em}, N \to \infty$, i.e. in the asymptotic limit. We set the required correctness $\varepsilon_{\rm cor}$ and the required secrecy $\varepsilon_{\rm sec}$ to $\varepsilon_{\rm cor} = \varepsilon_{\rm sec} = 10^{-15}$. We assumed that the bit error correction efficiency $f_{EC} = 1.2$. Furthermore, for simplicity, we set

$$\eta_1 = \eta_2 = 2^{-s} = \frac{\varepsilon_{\rm sec}^2}{6}, \tag{67}$$

in order to satisfy $\varepsilon_{\rm sec} = \sqrt{2(\eta_1 + \eta_2 + 2^{-s})}$. We determined the values of δ_1 and $\{\delta_2(N)\}_{N=1,\ldots}$ by numerically solving

$$\eta_1 = \max_{Q\in\mathcal{P}_{\mathcal{M}}:\mathbb{E}_{M\sim Q}[\nu_M]\ge\mathbb{E}_{M\sim\mathfrak{b}}[\nu_M]+\delta_1} 2^{-N_{\rm em}D(Q\|\mathfrak{b})}, \tag{68}$$
$$\eta_2 = \exp\left[-N\delta_2(N)\right], \tag{69}$$

where $\mathfrak{b} := \mathfrak{b}_{L,p_{\rm src}}$. When we solved the optimization problem, we used the "minimize" function of the scipy

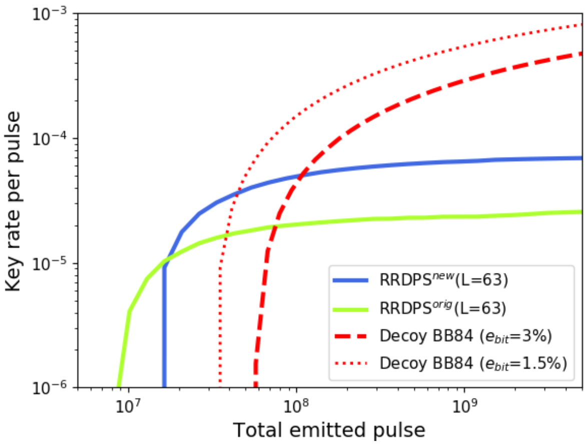

FIG. 5. The key rates of the RRDPS protocol in finite-sized case with block length $L = 63$. The horizontal axis shows the total number of pulses which Alice emits. The transmission rate is set to be 10^{-2}, and $e_{\rm bit} = 3\%$. The mean photon number of the light source is optimized for each number of pulses. The red broken line is the rate of the three-state decoy BB84 protocol with time-bin implementation under the same condition [24], and the dotted line is that under the bit error rate 1.5%.

library in Python with the "SLSQP" method. Figure 5 shows the key rates vs. the total emitted pulses of the RRDPS protocol with our analysis and with the original analysis, and of the decoy BB84 protocol. (The number of total emitted pulses is given by $N_{\rm em}L$ in the case of the RRDPS protocol.) Since the sampling cost $N_{\rm smp}$ is negligible only when we allow a margin for the estimation of $e_{\rm bit}$, we expect that the actual bit error rate should be lower than 3%. For this reason, we have also plotted the rate with $e_{\rm bit} = 1.5\%$ for the decoy BB84 protocol. Comparison of these rates shows that the improvement of the key rates over the original proof survives up to fairly small number of total emitted pulses at which the decoy BB84 protocol fails to produce a key.

IV. DISCUSSION

In this paper, we proposed a refined security proof of the RRDPS protocol, which improves the key generation rate without any change in the protocol itself. The crux of the improvement is an observation that the estimation of the phase error pattern in the virtual protocol can be aided by additional information y^N, which was ignored in the original security analysis. The pair of parameters $y_k = (a_k, b_k)$ are related to the parity of the number of emitted photons in each of the L pulses forming the k-th block (see (9)-(14)). The parameter b_k is associated with the pulse pair from which the sifted key bit is extracted, while the parameter a_k is with the rest of $L-2$ pulses. It is interesting that not only b_k but also a_k contributes to the improvement of the key rate.

The use of additional information related to the emitted numbers may look similar to the tagging technique [25] used for the (decoy) BB84 protocols with a practical source, where the latter uses the information whether the each pulse contains multiple photons (tagged) or not (untagged). There are, however, a couple of differences. One is the conceptual difference arising from the timing at which the tag is defined. In the case of the BB84 protocols, a tag is defined when the optical phase randomization is applied to the pulse before it leaves the sender. As a result, we can easily analyze the statistical properties of the tags without regard to the Eve's attack. In contrast, $y_k = (a_k, b_k)$ in our case should be dubbed an *ex post facto* tag, because it is defined only after the positions of the pair of pulses are announced by Bob. The analysis on the statistical properties of the *ex post facto* tags are not straightforward and often requires special techniques to extract a property that is independent of Eve's attack [20]. In our case, it is solved by introducing a third protocol (Protocol 3) solely for this purpose. From the viewpoint of implementation, the *ex post facto* tag has an advantage that it does not require optical phase randomization.

Another difference is a rather technical one that becomes significant in analyzing the finite-sized case. In contrast to the tag for the BB84 protocols which takes two values (multiple photons or not) or three values (multiple photons, single photons, or vacuum), our tag y_k takes $\left|\mathcal{Y}\right| = 2(L-1)$ values. As a result, the number of rounds with a specific value $y \in \mathcal{Y}$ of tag, $N\tilde{P}_{y^N}(y)$, is much smaller than N. In addition, the constraint (36) essentially dictates connection between the events whose tags take different values. In such a case, it is not wise to derive a statistical bound separately for each value of $y \in \mathcal{Y}$ and then to combine those bounds by using the union bound. Instead, here we introduced Lagrange multipliers and derived an inequality for a combined property directly, as in Proposition 1 and 2. For counting the number of phase error patterns, the bound in Lemma 1 that is independent of the size $\left|\mathcal{Y}\right|$ will be quite useful for mitigating finite-sized effects.

Although the above strategy succeeded in showing that the improvement persists up to a relatively small total number of emitted pulses, we see in Figure 5 that the rate is eventually surpassed by the original analysis when the total number is further decreased. We may ascribe it to either or both of the following two reasons. One is the fact that we did not optimize the values of the Lagrange multipliers and substituted the values in the asymptotic limit instead. The other is the use of a Bernstein's inequality in the proof of Proposition 2, which affects the key rate through the definition of $\mathcal{P}^{\boldsymbol{\xi},\delta_2(N)}$ in (42). It remains to be open whether we can replace it with a tighter bound while keeping the convexity of $\mathcal{P}^{\boldsymbol{\xi},\delta_2(N)}$.

We emphasize here that our focus in the present paper was on the simplest implementation of the sender's apparatus, namely, the use of the protocol without block-wise phase randomization in the original proposal, as it is. A natural question is that how the situation changes if we combine block-wise phase randomization with our analysis. On one hand, the aid of block-wise phase randomization does not seem to change the key rate so much considering that the key rate with our analysis is comparable to that with [18] in which the block-wise phase randomization is used. On the other hand, $\mathcal{P}^{N,\boldsymbol{\nu},\delta_1}$ may be significantly narrowed by the additional photon number constraint which is the consequence of the block-wise phase randomization. We leave it for the future research.

ACKNOWLEDGMENTS

This work was funded in part by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan), Photon Frontier Network Program (Ministry of Education, Culture, Sports, Science and Technology), CREST (Japan Science and Technology Agency), Research and Development of the Quantum Cryptography Technology for Satellite Communications in "Research and Development of Information and Communications Technology" (Ministry of Internal Affairs and Communication, Japan), and JSPS KAKENHI Grant Number JP18K13469.

Appendix A: Proof of Proposition 1

Let $P_{\boldsymbol{v}} \in \mathcal{P}_{\mathcal{M}}$ be defined as $P_{\boldsymbol{v}}(M) := v_M / N_{\rm em}$. From the condition (31) and the fact that $\mathcal{Q}$ is a convex set, we can apply the special case of the Sanov's theorem [26, 27] to $P_{\boldsymbol{v}}$ as follows:

$$\Pr\left\{P_{\boldsymbol{v}} \in \mathcal{Q}\right\} \le \max_{Q \in \mathcal{Q}} 2^{-N_{\rm em} D(Q \| \mathfrak{b}_{L,p_{\rm odd}})}. \tag{A1}$$

Let $b_{\rm norm}$ be the constant given by

$$b_{\rm norm} := \sum_{M : M < Lp_{\rm src}} \mathfrak{b}_{L,p_{\rm odd}}(M). \tag{A2}$$

Let $q \in \mathcal{P}_{\mathcal{M}}$ be the probability mass function which is defined as

$$q(M) := \begin{cases} \dfrac{\mathfrak{b}_{L,p_{\rm src}}(M)}{b_{\rm norm}} & \forall M < Lp_{\rm src} \\ \dfrac{\mathfrak{b}_{L,p_{\rm src}}(M) - \mathfrak{b}_{L,p_{\rm odd}}(M)}{b_{\rm norm}} & \forall M \ge Lp_{\rm src}, \end{cases} \tag{A3}$$

which is well-defined since $\mathfrak{b}_{L,p_{\rm src}}(M) \ge \mathfrak{b}_{L,p_{\rm odd}}(M)$ holds for all $M \ge Lp_{\rm src}$, and $\sum_{M \in \mathcal{M}} q(M) = 1$. We define the stochastic map $S : \mathcal{P}_{\mathcal{M}} \to \mathcal{P}_{\mathcal{M}}$ as follows:

$$\forall P \in \mathcal{P}_{\mathcal{M}}, \quad S(P)(M') := \sum_{M \in \mathcal{M}} \Pr(M'|M) P(M), \tag{A4}$$

where

$$\Pr(M'|M) := \begin{cases} q(M') & \forall M < Lp_{\rm src} \\ \delta_{M'M} & \forall M \ge Lp_{\rm src}. \end{cases} \tag{A5}$$

It is easy to observe that

$$\mathfrak{b}_{L,p_{\rm src}} = S(\mathfrak{b}_{L,p_{\rm odd}}). \tag{A6}$$

Furthermore, since (i) $S(P)(M) \ge P(M)$ and $\nu_M \ge 0$ for all $M \ge Lp_{\rm src}$, and (ii) $\nu_M = 0$ for all $M < Lp_{\rm src}$, we have

$$\forall P \in \mathcal{P}_{\mathcal{M}}, \quad \mathbb{E}_{M \sim S(P)}[\nu_M] \ge \mathbb{E}_{M \sim P}[\nu_M]. \tag{A7}$$

Therefore, from the definition of $\mathcal{Q}$ in (40), we have

$$\forall Q \in \mathcal{Q}, \quad S(Q) \in \mathcal{Q}. \tag{A8}$$

Combining (A6) and (A8) with the monotonicity property of the Kullback-Leibler divergence under the stochastic map [28], we have

$$\begin{aligned} \min_{Q \in \mathcal{Q}} D(Q \| \mathfrak{b}_{L,p_{\rm odd}}) &\ge \min_{Q \in \mathcal{Q}} D\left(S(Q) \| S(\mathfrak{b}_{L,p_{\rm odd}})\right) \\ &\ge \min_{Q \in \mathcal{Q}} D(Q \| \mathfrak{b}_{L,p_{\rm src}}). \end{aligned} \tag{A9}$$

From (A1) and (A9), we have

$$\Pr\left\{P_{\boldsymbol{v}} \in \mathcal{Q}\right\} \le \max_{Q \in \mathcal{Q}} 2^{-N_{\rm em} D(Q \| \mathfrak{b}_{L,p_{\rm src}})}. \tag{A10}$$

On the other hand, since the random variables $(\boldsymbol{v}, N, m^N)$ obey (35) and ν_M $(M \in \mathcal{M})$ are non-negative, we have

$$\begin{aligned} &\forall M \in \mathcal{M}, \\ &\quad \Pr\left\{ \nu_M \tilde{P}_{m^N}(M) \le \nu_M \frac{N_{\rm em}}{N} P_{\boldsymbol{v}}(M) \middle| N \ge 1 \right\} = 1, \end{aligned} \tag{A11}$$

and hence

$$\Pr\left\{ \mathbb{E}_{M \sim \tilde{P}_{m^N}}[\nu_M] \le \frac{N_{\rm em}}{N} \mathbb{E}_{M \sim P_{\boldsymbol{v}}}[\nu_M] \middle| N \ge 1 \right\} = 1. \tag{A12}$$

Combining (A12) with the definition of $\mathcal{Q}$, we have

$$\begin{aligned} &\Pr\Big\{ N \ge 1, \mathbb{E}_{M \sim \tilde{P}_{m^N}}[\nu_M] \\ &\qquad\qquad \ge \frac{N_{\rm em}}{N} (\mathbb{E}_{M \sim \mathfrak{b}_{L,p_{\rm src}}}[\nu_M] + \delta_1) \Big\} \\ &\le \Pr\Big\{ N \ge 1, \frac{N_{\rm em}}{N} \mathbb{E}_{M \sim P_{\boldsymbol{v}}}[\nu_M] \\ &\qquad\qquad \ge \frac{N_{\rm em}}{N} (\mathbb{E}_{M \sim \mathfrak{b}_{L,p_{\rm src}}}[\nu_M] + \delta_1) \Big\} \\ &\le \Pr\{P_{\boldsymbol{v}} \in \mathcal{Q}\}, \end{aligned} \tag{A13}$$

where the first inequality follows from (A12). Combining this with (A10), we have

$$\begin{aligned} \Pr\left\{ N \ge 1, \mathbb{E}_{M \sim \tilde{P}_{m^N}}[\nu_M] \ge \frac{N_{\rm em}}{N} (\mathbb{E}_{M \sim \mathfrak{b}_{L,p_{\rm src}}}[\nu_M] + \delta_1) \right\} \\ \le \max_{Q \in \mathcal{Q}} 2^{-N_{\rm em} D(Q \| \mathfrak{b}_{L,p_{\rm src}})}. \end{aligned} \tag{A14}$$

Then (39) implies (41).

Appendix B: Proof of Proposition 2

We use one of the Bernstein's inequalities [29], which is stated as follows. Let $X_1, ..., X_N$ be independent zero-mean random variables. Suppose that $|X_k| \le 1$ for all k. Then, for all non-negative t,

$$\Pr\left(\frac{1}{N} \sum_{k=1}^{N} X_k \ge t \right) \le \exp\left[-\frac{N t^2}{\frac{2}{N} \sum_k \mathbb{E}[X_k^2] + \frac{2}{3} t} \right] \tag{B1}$$

holds.

For fixed values of $N (\ge 1), m^N, u^N$, the condition (36) determines the conditional statistics of N variables $\{X_k := (x_k - c(m_k, u_k))\, \xi(m_k, u_k)\}_{k=1,...,N}$, where $\xi(M, U) := \xi_{M,U}$. They are independent and zero-mean. Furthermore, since $|\xi(m_k, u_k)| \le 1$ and $0 \le c(m_k, u_k) \le 1$ hold, $|X_k| \le 1$ also holds for all k. Thus, (B1) holds if we interpret $\Pr(\cdot)$ and $\mathbb{E}[\cdot]$ as the conditional probability and the conditional mean. Using the definition of the type, we can rewrite the sums over index k as

$$\begin{aligned}\sum_{k=1}^{N} X_k &= \sum_{(M,U,X)\in\mathcal{W}} (X - c(M,U))\,\xi_{M,U} N\tilde{P}_{m^N,u^N,x^N}(M,U,X) \\ &= N\mathbb{E}_{(M,U,X)\sim\tilde{P}_{m^N,u^N,x^N}}\left[(X-c(M,U))\,\xi_{M,U}\right],\end{aligned} \tag{B2}$$

and

$$\begin{aligned}&\sum_{k=1}^{N}\mathbb{E}[X_k^2] \\ &= \sum_{(M,U)\in\mathcal{M}\times\mathcal{U}} \Big\{\left[(0-c(M,U))\,\xi_{M,U}\right]^2(1-c(M,U)) + \left[(1-c(M,U))\,\xi_{M,U}\right]^2 c(M,U)\Big\} N\tilde{P}_{m^N,u^N}(M,U) \\ &= \sum_{(M,U)\in\mathcal{M}\times\mathcal{U}} c(M,U)\,(1-c(M,U))\,\xi_{M,U}^2 N\tilde{P}_{m^N,u^N}(M,U) \\ &= N\mathbb{E}_{(M,U)\sim\tilde{P}_{m^N,u^N}}[c(M,U)(1-c(M,U))\xi_{M,U}^2].\end{aligned} \tag{B3}$$

We choose t to be

$$t = \frac{\delta_2(N)}{3} + \left[\left(\frac{\delta_2(N)}{3}\right)^2 + \frac{2\delta_2(N)}{N}\sum_i \mathbb{E}[X_k^2]\right]^{\frac{1}{2}}, \tag{B4}$$

which satisfies

$$t^2 = \delta_2(N)\left(\frac{2}{N}\sum_i \mathbb{E}[X_k^2] + \frac{2}{3}t\right). \tag{B5}$$

Substituting (B2), (B3), (B4) to (B1), we obtain the following:

$$\begin{aligned}\Pr\Bigg\{&\mathbb{E}_{(M,U,X)\sim\tilde{P}_{m^N,u^N,x^N}}\left[(X-c(M,U))\,\xi_{M,U}\right] \\ &\geq \frac{\delta_2(N)}{3} + \left[\left(\frac{\delta_2(N)}{3}\right)^2 + 2\delta_2(N)\mathbb{E}_{(M,U)\sim\tilde{P}_{m^N,u^N}}\left[c(M,U)\,(1-c(M,U))\,\xi_{M,U}^2\right]\right]^{\frac{1}{2}}\Bigg\} \leq \exp\left[-N\delta_2(N)\right].\end{aligned} \tag{B6}$$

Then (43) implies (44).

Appendix C: Proof of Lemma 1

For $y^N \in \mathcal{Y}^N$, define a set

$$\mathcal{E}_{\mathcal{X}\times\mathcal{Y}}(y^N) := \{P_{\mathcal{X}\times\mathcal{Y}} : P \in \mathcal{E}, P_{\mathcal{Y}} = \tilde{P}_{y^N}\}. \tag{C1}$$

Since $\mathcal{E}$ is a closed convex set, $\mathcal{E}_{\mathcal{X}\times\mathcal{Y}}(y^N)$ is also a closed convex set. Using the set, we can rewrite $T(y^N)$ as

$$T(y^N) := \{x^N \in \mathcal{X}^N : \tilde{P}_{x^N,y^N} \in \mathcal{E}_{\mathcal{X}\times\mathcal{Y}}(y^N)\}. \tag{C2}$$

Consider a probability mass function $Q(x,y)$ given by

$$Q(x,y) := |\mathcal{X}|^{-1}\tilde{P}_{y^N}(y). \tag{C3}$$

Then we have

$$\sum_{x^N\in T(y^N)} Q^N(x^N,y^N) = |\mathcal{X}|^{-N}\tilde{P}_{y^N}^N(y^N)|T(y^N)| \tag{C4}$$

Let

$$P^* := \arg\min_{P\in\mathcal{E}_{\mathcal{X}\times\mathcal{Y}}(y^N)} D(P\|Q). \tag{C5}$$

Then, we have (Pythagorean theorem [28])

$$D(P\|Q) \geq D(P\|P^*) + D(P^*\|Q) \text{ for } {}^{\forall}P \in \mathcal{E}_{\mathcal{X}\times\mathcal{Y}}(y^N). \tag{C6}$$

For $(x^N,y^N) \in \mathcal{X}^N \times \mathcal{Y}^N$ with $\tilde{P}_{x^N,y^N} \in \mathcal{E}_{\mathcal{X}\times\mathcal{Y}}$, we have

$$\begin{aligned}&\log Q^N(x^N,y^N) - \log P^{*N}(x^N,y^N) \\ &= -ND(\tilde{P}_{x^N,y^N}\|Q) + ND(\tilde{P}_{x^N,y^N}\|P^*) \\ &\leq -ND(P^*\|Q),\end{aligned} \tag{C7}$$

and hence

$$\begin{aligned}&\sum_{x^N\in T(y^N)} Q^N(x^N,y^N) \\ &\leq 2^{-ND(P^*\|Q)}\sum_{x^N\in T(y^N)} P^{*N}(x^N,y^N) \\ &\leq 2^{-ND(P^*\|Q)}\sum_{x^N\in \mathcal{X}^N} P^{*N}(x^N,y^N) \\ &= 2^{-ND(P^*\|Q)}\tilde{P}_{y^N}^N(y^N).\end{aligned} \tag{C8}$$

Combined with (C4), we have

$$|T(y^N)| \le 2^{-ND(P^*\|Q)+N\log|\mathcal{X}|}. \tag{C9}$$

On the other hand, for $P \in \mathcal{E}_{\mathcal{X}\times\mathcal{Y}}(y^N)$,

$$\begin{aligned} D(P\|Q) &= \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} P(x,y)\log\frac{P(x,y)}{Q(x,y)} \\ &= \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} P(x,y)\log\frac{P(x|y)}{Q(x|y)} \\ &= \log|\mathcal{X}| - H(X|Y)_P, \end{aligned} \tag{C10}$$

and hence

$$\begin{aligned} D(P^*\|Q) &= \min_{P\in\mathcal{E}_{\mathcal{X}\times\mathcal{Y}}(y^N)} D(P\|Q) \\ &= \log|\mathcal{X}| - \max_{P\in\mathcal{E}_{\mathcal{X}\times\mathcal{Y}}(y^N)} H(X|Y)_P. \end{aligned} \tag{C11}$$

Combining (C1), (C9), and (C11) leads to (50).

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

[2] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, Experimental satellite quantum communications, Phys. Rev. Lett. **115**, 040502 (2015).

[3] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, and Z.-P. Li, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).

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

[5] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Experimental quantum key distribution without monitoring signal disturbance, Nature Photonics **9**, 827 (2015).

[6] 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, Nature Photonics **9**, 832 (2015).

[7] 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).

[8] 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 (2016).

[9] A. Mizutani, N. Imoto, and K. Tamaki, Robustness of the round-robin differential-phase-shift quantum-key-distribution protocol against source flaws, Phys. Rev. A **92**, 060303 (2015).

[10] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Phys. Rev. Lett. **91**, 057901 (2003).

[11] H.-L. Yin, Y. Fu, Y. Mao, and Z.-B. Chen, Detector-decoy quantum key distribution without monitoring signal disturbance, Phys. Rev. A **93**, 022330 (2016).

[12] Z. Zhang, X. Yuan, Z. Cao, and X. Ma, Practical round-robin differential-phase-shift quantum key distribution, New Journal of Physics **19**, 033013 (2017).

[13] T. Sasaki and M. Koashi, A security proof of the round-robin differential phase shift quantum key distribution protocol based on the signal disturbance, Quantum Science and Technology **2**, 024006 (2017).

[14] Y. Hatakeyama, A. Mizutani, G. Kato, N. Imoto, and K. Tamaki, Differential-phase-shift quantum-key-distribution protocol with a small number of random delays, Phys. Rev. A **95**, 042301 (2017).

[15] L. Wang and S. Zhao, Round-robin differential-phase-shift quantum key distribution with heralded pair-coherent sources, Quantum Information Processing **16**, 100 (2017).

[16] L. Liu, F.-Z. Guo, S.-J. Qin, and Q.-Y. Wen, Round-robin differential-phase-shift quantum key distribution with a passive decoy state method, Scientific Reports **7**, 42261 (2017).

[17] D. Leermakers and B. Skoric, Security proof for round robin differential phase shift qkd, arXiv preprint arXiv:1709.00552 (2017).

[18] 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, Nature communications **9**, 457 (2018).

[19] F. Bouchard, A. Sit, K. Heshami, R. Fickler, and E. Karimi, Round-robin differential-phase-shift quantum key distribution with twisted photons, Phys. Rev. A **98**, 010301 (2018).

[20] S. Kawakami, T. Sasaki, and M. Koashi, Security of the differential-quadrature-phase-shift quantum key distribution, Phys. Rev. A **94**, 022332 (2016).

[21] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New Journal of Physics **11**, 045018 (2009).

[22] M. Hayashi and T. Tsurumaru, Concise and tight security analysis of the bennettbrassard 1984 protocol with finite key lengths, New Journal of Physics **14**, 093014 (2012).

[23] T. Tsurumaru and M. Hayashi, Dual universality of hash functions and its applications to quantum cryptography, IEEE Trans. Inf. Theory **59**, 4700 (2013).

[24] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[25] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on* (IEEE, 2004) p. 136.

[26] I. Csiszár, Sanov property, generalized i-projection and a conditional limit theorem, The Annals of Probability **12**, 768 (1984).

[27] I. N. Sanov, On the probability of large deviations of random magnitudes, Mat. Sb. (NS), **42(84)**, 11 (1957).

[28] T. M. Cover and J. A. Thomas, *Elements of information theory* (John Wiley & Sons, 2012).

[29] S. Bernstein, On a modification of chebyshevs inequality and of the error formula of laplace, Ann. Sci. Inst. Sav. Ukraine, Sect. Math **1**, 38 (1924).