Optimum ratio between two bases in the Bennett-Brassard 1984 protocol with second-order analysis

Masahito Hayashi [*]

Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Nanshan District, Shenzhen 518055, China;

International Quantum Academy (SIQA), Futian District, Shenzhen 518048, China;

Guangdong Provincial Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Nanshan District, Shenzhen 518055, China;

and Graduate School of Mathematics, Nagoya University, Furocho, Chikusa-ku, Nagoya 464-8602, Japan

(Received 30 January 2022; accepted 25 March 2022; published 11 April 2022)

In the Bennett-Brassard 1984 protocol, we optimize the ratio of the choice of two bases, the bit basis and the phase basis, by using the second-order expansion for the length of the generation keys under the coherent attack. This optimization addresses the trade-off between the loss of transmitted bits due to the disagreement of their bases and the estimation error of the error rate in the phase basis. Then, we derive the optimum ratio and the optimum length of the generation keys with the second-order asymptotics. Surprisingly, the second order has the order $n^{\frac{3}{4}}$, which is much larger than the second-order $n^{\frac{1}{2}}$ in the conventional setting when n is the number of quantum communication. This fact shows that our setting has much larger importance for the second-order analysis than the conventional problem. To illustrate this importance, we numerically plot the effect of the second-order correction.

DOI: 10.1103/PhysRevA.105.042603

I. INTRODUCTION

The Bennett-Brassard 1984 (BB84) protocol [1] is a standard protocol for quantum key distribution. The key point of this protocol is the evaluation of the amount of information leakage on the bit basis via the estimation of the error rate in the phase basis. Due to this reason, the sender, Alice, and the receiver, Bob, choose their basis independently with equal probability in the conventional setting. In this method, a half of the transmitted bits are discarded due to the disagreement of their bases. However, since the aim is the estimation for the error rate, it is sufficient to assign the phase basis to a limited number of transmitted pulses that enables Alice and Bob to estimate the error rate in the phase basis [2]. In this situation, we need to address the trade-off between the loss of transmitted bits due to the disagreement of their bases and the estimation error of the error rate in the phase basis. To address this problem, we need to clarify the effect of the estimation error to the key generation rate. The existing study [3] treated the estimation error in the large deviation framework. While the large deviation method addresses the speed of convergence of the amount of information leakage, it cannot directly address the fixed amount of information leakage. Due to this reason, people in the community of quantum information are interested in the latter formulation rather than the large deviation theory. Fortunately, the existing studies [4,5] investigated this trade-off problem in the security proof under the coherent attack by using the second-order analysis while the preceding studies [6–10] address only the first-order analysis in the asymptotic regime for the security proofs. These studies [4,5] clarified that the order of the second order in the length of the key generation is $n^{\frac{1}{2}}$ when n expresses the number of quantum communications.

The second-order theory was initiated by Strassen [11] and addresses the fixed amount of the error probability. Then, the paper in [4] applied it to the asymptotic regime of the security proof of QKD and the paper in [12] did it to the classical source coding and uniform random number generation. However, this approach did not attract attention sufficiently until the papers in [13,14] applied it to the classical channel coding. After the papers in [13,14], the papers in [15,16] applied this approach to other topics in quantum information. In particular, the paper in [16] studied the secure random number extraction and the data compression with quantum side information in this framework. While the paper in [17] studied the finite-length regime for the security proofs, the paper in [5] established the bride between the finite-length and second-order regimes for the security proofs. That is, it derived the finite-length bound for key generation and recovered the second-order asymptotics as its limit. Later, the papers in [18,19] considered the second-order analysis for QKD under the collective attack, but they assumed that the error of the channel estimation is zero. Overall, the order of the second order is $n^{\frac{1}{2}}$ when n is the order of the first order.

In this paper, using the second-order analysis under the coherent attack by [4,5], we address the trade-off between the loss of transmitted bits due to the disagreement of Alice's and Bob's bases and the estimation error of the error rate in the phase basis. Then, we optimize the ratio of the phase basis depending on the observed error rates. As a result, we find that the order of the second order in the length of the key generation is $n^{\frac{3}{4}}$, while n expresses the number of quantum communications. Comparing the above existing studies, no

[*]hayashi@sustech.edu.cn

preceding study derived the order $n^{\frac{3}{4}}$ as the second order. Further, our second-order $n^{\frac{3}{4}}$ is much larger than the conventional second order. This fact shows that our problem has a larger effect by the second-order correction, i.e., the second-order analysis in our setting is more important than the second-order analysis in other problem settings. To clarify this importance, we numerically plot the effect of the second-order correction.

The remaining part of this paper is organized as follows. Section II states our problem setting. Section III shows the concrete protocol for our analysis by combining the error verification. Section IV states the optimum key generation length and makes its numerical plot. Section V gives the detail derivation for our obtained result.

II. FORMULATION

In BB84 protocol, for each transmission, the sender, Alice, randomly chooses one of two bases, the bit basis $\{|0\rangle, |1\rangle\}$ and the phase basis $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. The receiver, Bob, measures each received state by choosing one of these two bases. While these choices are done with equal probability in the usual case, we assume that Alice and Bob choose the bit basis with probability $1 - r_0$. After their quantum communication, Alice and Bob find which quantum transmission is done in the matched basis by exchanging their basis choice via public communication. While they keep the data in the matched basis, they exchange a part of them to estimate the error rate. Here, we denote the ratio of data used for estimation in the bit basis (the phase basis) by r_1 (r_2).

When the quantum channel is noisy, we need information reconciliation and privacy amplification after quantum communication. Privacy amplification can be done by applying a typical type of hash function with calculation complexity $O(n \log_2 n)$, where n is the block length. Hence we can choose the hash function depending on the error rate of the channel. In contrast, for a practical setting for BB84 protocol, we often fix our code with coding rate β for information reconciliation because it is not so easy to construct an error correcting code depending on the error rate of the channel. In this paper, we adopt the following security criterion. We denote Alice's and Bob's final keys by K and $\hat{K}$, respectively, and denote Eve's system by E. Also, we denote the public information and the length of final keys by G and L. In this situation, the ideal state $\rho^{\rm ideal}_{LGK\hat{K}E}$ is given by using $\vec{\sigma}_{E|LG} = (\sigma_{E|L=l,G=g})_{l,g}$ as follows:

$$\rho^{\rm ideal}_{LGK\hat{K}E}(\vec{\sigma}_{E|LG}) := \sum_{l=0}^{l_{\rm m}} \sum_{g} P_{LG}(l,g)|l,g\rangle\langle l,g| \otimes \sum_{k=1}^{2^l} \frac{1}{2^l}|k,k\rangle\langle k,k| \otimes \sigma_{E|L=l,G=g}, \quad (1)$$

where $l_{\rm m}$ expresses the maximum length of final keys. Therefore, our security criterion for our final state $\rho^{\rm real}_{LGK\hat{K}E}$ is given as the difference between the ideal state $\rho^{\rm ideal}_{LGK\hat{K}E}$ and the real state $\rho^{\rm real}_{LGK\hat{K}E}$ as

$$\mathcal{C}\big(\rho^{\rm real}_{LGK\hat{K}E}\big) := \min_{\vec{\sigma}_E} \frac{1}{2}\big\|\rho^{\rm ideal}_{LGK\hat{K}E}(\vec{\sigma}_{E|LG}) - \rho^{\rm real}_{LGK\hat{K}E}\big\|_1. \quad (2)$$

If $\vec{\sigma}_E$ is fixed to the state $\vec{\rho}_{E|LG} = (\rho_{E|L=l,G=g})_{l,g}$, the above value is the same as the criterion defined in [20]. When we attach the error verification step, we can guarantee the correctness of our final keys without caring about the estimation error of the error rate of the channel [21, Sec. VIII].

We denote the final states for the part generated by the bit basis (the phase basis) by $\rho^{\rm real,1}_{LGK\hat{K}E}$ ($\rho^{\rm real,2}_{LGK\hat{K}E}$). Now, we impose our protocol to the condition under the coherent attack:

$$\mathcal{C}\big(\rho^{\rm real,1}_{LGK\hat{K}E}\big) \leqslant \epsilon + o\Big(\frac{1}{\sqrt{n}}\Big), \quad \mathcal{C}\big(\rho^{\rm real,2}_{LGK\hat{K}E}\big) \leqslant \epsilon + o\Big(\frac{1}{\sqrt{n}}\Big). \quad (3)$$

III. DESCRIPTION OF OUR PROTOCOL

Before presenting our main result, we state our protocol. This protocol uses modified Toeplitz matrices in privacy amplification. A randomized function f_S with random seeds S is called a modified Toeplitz matrix from $\mathbb{F}_2^{l_1}$ to $\mathbb{F}_2^{l_2}$ with $l_1 \geqslant l_2$ when S takes values in $\mathbb{F}_2^{l_1-1}$ and f_S is given as the matrix $[I, T(S)]$, where $T(S)$ is the $l_2 \times (l_1 - l_2)$ Toeplitz matrix, whose components are defined as $T(S)_{i,j} = S_{j-i+l_1}$. In fact, a modified Toeplitz matrix f_S is an example of universal2 hash functions [22, Appendix II]. Here, a randomized function f_S from $\mathcal{X}$ to $\mathcal{Y}$ with random seed S is called a universal2 hash function when the condition

$$\Pr[f_S(x) = f_S(x')] \leqslant \frac{1}{|\mathcal{Y}|} \quad (4)$$

holds for any $x \neq x' \in \mathcal{X}$ [23].

Also, based on [4, Secs. II-B and III-B] and [24, Eq. (4)], we define the small value

$$\delta(p, \epsilon, m_1, m_2) := \sqrt{\frac{p(1-p)(m_1+m_2)}{m_1 m_2}}\Phi^{-1}(\epsilon_{du}), \quad (5)$$

with $\epsilon = \sqrt{\epsilon_{du}}$. That is, $\delta(p, \epsilon, m_1, m_2)$ is given as

$$\delta(p, \epsilon, m_1, m_2) = \sqrt{\frac{p(1-p)(m_1+m_2)}{m_1 m_2}}\Phi^{-1}(\epsilon^2). \quad (6)$$

Then, our protocol is given as Protocol 1.

Protocol 1.

Quantum communication. Alice randomly chooses the bit basis or the phase basis with the ratio $1 - r_0 : r_0$ and sends n qubits and Bob measures the n receiving qubits by choosing the bit basis or the phase basis with the ratio $1 - r_0 : r_0$. Here, Alice chooses her bits subject to the uniform distribution. After quantum communication, they exchange the choice of bases via public channel. Then, they obtain $N_1 = n_1$ bits with the bit basis and $N_2 = n_2$ bits with the phase basis.

Error estimation. They randomly choose check bits in the bit basis (the phase basis) with ratio r_1 (r_2), and obtain the estimate p_1 (p_2) by exchanging their information. Then, they decide the sacrificed lengths $m_1(n_1, p_2) := (1 - r_1)n_1\{h[p_2 + \delta(p_2, \epsilon, (1-r_1)n_1, r_2 n_2)]\}$ and $m_2(n_2, p_1) := (1 - r_2)n_2\{h[p_1 + \delta(p_1, \epsilon, (1-r_2)n_2, r_1 n_1)]\}$.

Information reconciliation. They apply error correction with the linear code C_1 (C_2) of the rate β in the remaining bits in the bit basis (the phase basis). That is, Alice sends

her syndrome of the linear code C_1 (C_2) of $(1-r_1)n_1$ bits with the bit basis [$(1-r_2)n_2$ bits with the phase basis] to Bob via public channel. Bob corrects his error. Then, Alice (Bob) obtains $\beta(1-r_1)n_1$ bits X_1 ($\hat{X}_1$) with the bit basis and $\beta(1-r_2)n_2$ bits X_2 ($\hat{X}_2$) with the phase basis.

Privacy amplification. Alice randomly chooses two modified Toeplitz matrices f_{1,S_1} from $\beta(1-r_1)n_1$ bits to $\beta(1-r_1)n_1-m_1$ bits and f_{2,S_2} from $\beta(1-r_2)n_2$ bits to $\beta(1-r_2)n_1-m_2$ bits, and sends the choices of S_1 and S_2 to Bob via public channel. Then, Alice [Bob] obtains $f_{1,S_1}(X_1)$ [$f_{1,S_1}(\hat{X}_1)$] with the bit basis and $f_{2,S_2}(X_2)$ [$f_{2,S_2}(\hat{X}_2)$] with the phase basis.

Error verification. Alice sets m_3 to be $\log_2 n$. Alice randomly chooses two modified Toeplitz matrices f_{3,S_3} from $\beta(1-r_1)n_1-m_1$ bits to m_3 bits and f_{4,S_4} from $\beta(1-r_2)n_2-m_2$ bits to m_3 bits, and sends the choices of S_3, S_4 and $f_{3,S_3}[f_{1,S_1}(X_1)]$, $f_{4,S_4}[f_{2,S_2}(X_2)]$ to Bob via public channel. If the relation $f_{3,S_3}[f_{1,S_1}(X_1)] = f_{3,S_3}[f_{1,S_1}(\hat{X}_1)]$ ($f_{4,S_4}[f_{2,S_2}(X_2)] = f_{4,S_4}[f_{2,S_2}(\hat{X}_2)]$) holds, they keep their bits $f_{1,S_1}(X_1)$ and $f_{1,S_1}(\hat{X}_1)$ [$f_{2,S_2}(X_2)$ and $f_{2,S_2}(\hat{X}_2)$] by discarding initial m_3 bits of $f_{1,S_1}(X_1)$ and $f_{1,S_1}(\hat{X}_1)$ [$f_{2,S_2}(X_2)$ and $f_{2,S_2}(\hat{X}_2)$]. Otherwise, they discard their obtained keys, i.e., set the length L to be zero.

IV. OUR RESULT

To discuss the length of the generated keys, we employ the second-order asymptotics for the generated key length [4, Secs. II-B and III-B] and [5, Eq. (53)]. When the observed error rates in the bit basis (the phase basis) are given as p_1 (p_2) and the error verification is passed, the averaged length of generated keys can be approximated by

$$n(A(p_1)(1-r_0)^2(1-r_1)+A(p_2)r_0^2(1-r_2))-\sqrt{n}\Bigg(B(p_2,\epsilon)\sqrt{\frac{(1-r_0)^2(1-r_1)\big[(1-r_0)^2(1-r_1)+r_0^2r_2\big]}{r_0^2r_2}}$$
$$+B(p_1,\epsilon)\sqrt{\frac{r_0^2(1-r_2)\big[r_0^2(1-r_2)+(1-r_0)^2r_1\big]}{(1-r_0)^2r_1}}\Bigg)+o(\sqrt{n}), \tag{7}$$

where

$$A(p):=\beta-h(p),\quad B(p,\epsilon):=h'(p)\sqrt{p(1-p)}\Phi^{-1}(\epsilon^2), \tag{8}$$

and $\Phi(x):=\int_x^\infty \frac{1}{\sqrt{2\pi}}e^{-t^2/2}dt$. Here, $h(p)$ expresses the binary entropy $-p\log_2 p-(1-p)\log_2(1-p)$ and $h'(p)$ expresses its derivative.

When $h(p_2)\leqslant h(p_1)$, the optimal choices of r_0, r_1, r_2 are $\sqrt{\frac{B(p_2,\epsilon)}{2A(p_2)}}n^{-\frac{1}{4}}$, 0, 1. The maximum averaged length of the generated keys is

$$nA(p_2)-n^{\frac{3}{4}}2\sqrt{2A(p_2)B(p_2,\epsilon)}+O(n^{\frac{1}{2}})$$
$$=nA(p_2)\left(1-n^{-\frac{1}{4}}2\sqrt{\frac{2B(p_2,\epsilon)}{A(p_2)}}+O(n^{-\frac{1}{2}})\right). \tag{9}$$

After this optimization, the second order has the order $n^{\frac{3}{4}}$, which is a larger order than the second order in (7). Figure 1 shows the optimum key generation rate with the second-order correction when $p_2=0.05$. Since the second-order $n^{\frac{1}{4}}$ appears in the rate, its effect is not negligible up to $n=10^{10}$. This phenomena is surprising in comparison with the conventional second-order analysis because the second-order $n^{\frac{1}{2}}$ appears in the rate in the conventional setting so that its effect vanishes around $n=10^5$. This fact shows that the second-order correction is more important when we optimize the ratios r_0, r_1, r_2 in our modified BB84 protocol given as Protocol 1 than the conventional case.

V. DERIVATION OF OUR EVALUATION

For our security analysis under the coherent attack, we define the state

$$\rho^{\mathrm{mid},i}_{LGK\hat{K}E}:=\sum_{l=0}^{l_{\mathrm{m}}}\sum_g P^i_{LG}(l,g)|l,g\rangle\langle l,g|$$
$$\otimes\sum_{k=1}^{2^l}\frac{1}{2^l}|k,k\rangle\langle k,k|\otimes\rho^i_{E|K=k,L=l,G=g} \tag{10}$$

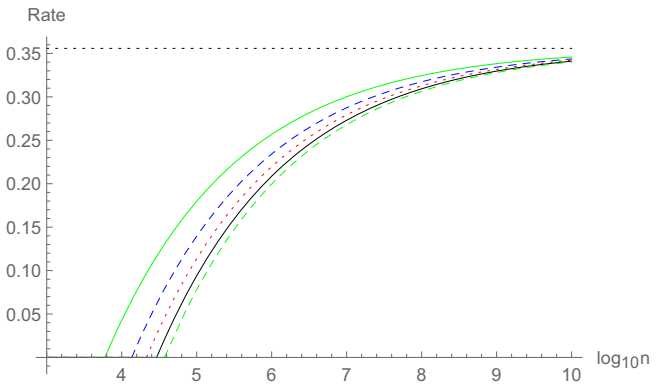

FIG. 1. Numerical plot of the key generation rate $A(p_2)(1-n^{-\frac{1}{4}}2\sqrt{\frac{2B(p_2,\epsilon)}{A(p_2)}})$ with $p_2=0.05$ and $\beta=0.9[1-h(0.05)]=0.642\,243$. The rate is dimensionless because it is given as the length divided by n. The vertical axis expresses the rate and the horizontal axis expresses the $\log_{10} n$. The top black dotted line expresses the first-order rate, i.e., $A(0.05)=0.355\,846$. The green normal line expresses the case with $\epsilon=10^{-2}$. The blue dashed line expresses the case with $\epsilon=10^{-4}$. The red dotted line expresses the case with $\epsilon=10^{-6}$. The black normal line expresses the case with $\epsilon=10^{-8}$. The green dashed line expresses the case with $\epsilon=10^{-10}$.

for $i=1,2$. As explained in Appendix A, using the property (4), we can show

$$\frac{1}{2}\left\|\rho^{\mathrm{mid},i}_{LGK\hat{K}E}-\rho^{\mathrm{real},i}_{LGK\hat{K}E}\right\|_1\leqslant\frac{1}{2^{m_3}}=\frac{1}{n} \tag{11}$$

for $i=1,2$. Thus we expand the security criterion $\mathcal{C}(\rho^{\mathrm{real},i}_{LGK\hat{K}E})$ as

$$\begin{aligned}\mathcal{C}\big(\rho^{\mathrm{real},i}_{LGK\hat{K}E}\big)\leqslant&\frac{1}{2}\left\|\rho^{\mathrm{ideal},i}_{LGK\hat{K}E}(\vec{\sigma}_{E|LG})-\rho^{\mathrm{mid},i}_{LGK\hat{K}E}\right\|_1\\&+\min_{\vec{\sigma}_{E|LG}}\frac{1}{2}\left\|\rho^{\mathrm{mid},i}_{LGK\hat{K}E}-\rho^{\mathrm{real},i}_{LGK\hat{K}E}\right\|_1\\\leqslant&\min_{\vec{\sigma}_{E|LG}}\frac{1}{2}\left\|\rho^{\mathrm{ideal},i}_{LGKE}(\vec{\sigma}_{E|LG})-\rho^{\mathrm{real},i}_{LGKE}\right\|_1+\frac{1}{n}.\end{aligned} \tag{12}$$

The papers in [4,5,25] considered the virtual decoding error probability in the dual basis, which is denoted by P^i_{du} for $i=1,2$. As shown in Appendix B, we have

$$\min_{\vec{\sigma}_{E|LG}}\frac{1}{2}\left\|\rho^{\mathrm{ideal},i}_{LGKE}(\vec{\sigma}_{E|LG})-\rho^{\mathrm{real},i}_{LGKE}\right\|_1\leqslant\sqrt{P^i_{du}}. \tag{13}$$

Now, we recall the result for the second-order analysis by [4, Secs. II-B and III-B] and [24, Eq. (4)], which is the corrected version of [5, Eq. (53)]. Due to the choices of m_1 and m_2, the above-mentioned second-order analysis guarantees that

$$P^i_{du}\leqslant\epsilon_{du}+o\left(\frac{1}{\sqrt{n}}\right) \tag{14}$$

under the coherent attack. Since $\epsilon^2=\epsilon_{du}$, combining (12), (13), and (14), we have

$$\mathcal{C}\big(\rho^{\mathrm{real},i}_{LGK\hat{K}E}\big)\leqslant\epsilon+o\left(\frac{1}{\sqrt{n}}\right), \tag{15}$$

which guarantees (3). That is, we find that Protocol 1 satisfies the condition (3).

As shown in Appendix D, by using the definition of $\delta(p,\epsilon,m_1,m_2)$ given in (5) the length of the generated keys is calculated as

$$\begin{aligned}&\beta(1-r_1)n_1-m_1(n_1,p_2)-m_3\\&\quad+\beta(1-r_2)n_2-m_2(n_2,p_1)-m_3\\&=(1-r_1)[\beta-h(p_2)]n_1+(1-r_2)[\beta-h(p_1)]n_2\\&\quad-B(p_2,\epsilon)\sqrt{\frac{[(1-r_1)n_1+r_2n_2](1-r_1)n_1}{r_2n_2}}\\&\quad-B(p_1,\epsilon)\sqrt{\frac{[(1-r_2)n_2+r_1n_1](1-r_2)n_2}{r_1n_1}}+o(\sqrt{n}).\end{aligned} \tag{16}$$

Since n_1 and n_2 are the realizations of the random variables N_1 and N_2, we consider the average with respect to these variables. Since the averages of N_1 and N_2 are $n(1-r_0)^2$ and nr_0^2, we have

$$\begin{aligned}&\mathbb{E}_{N_1,N_2}\big[\beta(1-r_1)N_1-m_1(N_1,p_2)-m_3\\&\quad+\beta(1-r_2)N_2-m_2(N_2,p_1)-m_3\big]\\&=\mathbb{E}_{N_1,N_2}\Bigg[(1-r_1)[\beta-h(p_2)]N_1+(1-r_2)[\beta-h(p_1)]N_2\\&\quad-(1-r_1)B(p_2,\epsilon)\sqrt{\frac{[(1-r_1)N_1+r_2N_2](1-r_1)N_1}{r_2N_2}}\\&\quad-(1-r_2)B(p_1,\epsilon)\sqrt{\frac{[(1-r_2)N_2+r_1N_1](1-r_2)N_2}{r_1N_1}}\Bigg]\\&\quad+o(\sqrt{n})\\&=(1-r_1)[\beta-h(p_2)](1-r_0)^2n+(1-r_2)[\beta-h(p_1)]r_0^2n\\&\quad-B(p_2,\epsilon)\sqrt{\frac{\big[(1-r_1)(1-r_0)^2+r_2r_0^2\big](1-r_1)(1-r_0)^2}{r_2r_0^2}}\\&\quad\times\sqrt{n}\\&\quad-B(p_1,\epsilon)\sqrt{\frac{[(1-r_2)r_0^2+r_1(1-r_0)^2](1-r_2)r_0^2}{r_1(1-r_0)^2}}\sqrt{n}\\&\quad+o(\sqrt{n}),\end{aligned} \tag{17}$$

which implies (7).

Next, we optimize the ratios r_0,r_1,r_2 under the condition $h(p_2)\leqslant h(p_1)$. In this case, the optimal rate in the first-order coefficient is $[\beta-h(p_2)]$. To achieve this rate, the ratio r_0 needs to approach to zero. We set r_0 to be $\alpha_1 n^{-\frac{1}{4}}\kappa_n$ with a sequence κ_n. Then, the above value is calculated as

$$\begin{aligned}&(1-r_1)A(p_2)n-2(1-r_1)A(p_2)\alpha_1 n^{\frac{3}{4}}\kappa_n\\&\quad-B(p_2,\epsilon)\sqrt{\frac{(1-r_1)^2}{r_2\alpha_1^2}}n^{\frac{3}{4}}\kappa_n^{-1}+O\big(n^{\frac{1}{2}}\big(1+\kappa_n^2\big)\big).\end{aligned} \tag{18}$$

Since coefficients of the orders $n^{\frac{3}{4}}\kappa_n$ and $n^{\frac{3}{4}}\kappa_n^{-1}$ are negative, the maximization of the above value is realized when the order of the second term coincides with the order of the third term, i.e., κ_n is a constant term. In the following, we choose κ_n to be 1. Then, the above value is calculated as

$$\begin{aligned}&(1-r_1)A(p_2)n-\Bigg(2(1-r_1)A(p_2)\alpha_1\\&\quad+B(p_2,\epsilon)\frac{(1-r_1)}{r_2^{1/2}\alpha_1}\Bigg)n^{3/4}+O(\sqrt{n}).\end{aligned} \tag{19}$$

To maximize the first-order coefficient, r_1 needs to be zero. The maximum of $-(2A(p_2)\alpha_1+B(p_2,\epsilon)\frac{1}{r_2^{1/2}\alpha_1})$ is realized when $r_2=1$ and $\alpha_1=\sqrt{\frac{B(p_2,\epsilon)}{2A(p_2)}}$. Under this choice, the above value equals (9).

When $r_1=0$, Alice and Bob cannot estimate the error rate p_1. However, they can check whether their final shared keys are matched by using the error verification. That is, once the error verification test passed, we can guarantee the correctness of our final keys without caring about the estimation error of the error rate of the channel [21, Sec. VIII]. The recent papers in [26, Appendix E] and [27, Sec. VI] discussed the detail evaluation for the performance of the error verification. In the realistic situation, we have a prior

knowledge for the expected value of the error rate p_1. Hence we design our protocol by using this prior knowledge. If an unexpected event does not happen, the error verification passes. Therefore, the choice with $r_1 = 0$ is allowed in our protocol.

VI. DISCUSSION AND CONCLUSION

We have derived the optimum key generate rate when we optimize the ratios of basis choices. Then, we clarified the second-order effect under this optimization. While the second order has the order $n^{\frac{1}{2}}$ under the conventional setting [4,5], the second order has the order $n^{\frac{3}{4}}$ in our setting. That is, when we focus on the generation rate, our second-order effect has the order $n^{-\frac{1}{4}}$, while the second-order effect in the conventional case has the order $n^{-\frac{1}{2}}$. Since the vanishing speed of the second-order effect is quite slow in our setting, we need to be careful for the effect by the second-order correction. Overall, our result has clarified that the order of the second order becomes large after the optimization for the ratio of the choices of the bases. Since the second-order coefficient is a negative value, the second-order effect is negative. That is, the key generation can be improved by removing the second-order effect. In other words, the key generation can be improved by increasing the block length n. Further, we can expect similar phenomena in a problem with a certain optimization. That is, this result suggests a possibility that an optimization makes the order of the second order larger than the original order of the second order.

Our model assumes a single-photon source. Many reports for implementation of quantum key distribution used weak coherent sources. Unfortunately, our result cannot be applied to such practical systems while decoy BB84 methods and the continuous-variable method can be used for such practical systems [28–34]. For practical use, we need to expand our analysis to the above two methods. In our result, one basis is used to generate the sifted keys and the other basis is used to estimate the quantum channel. This idea can be generalized to the following: we optimize the ratio among the pulses to generate the sifted keys and the pulses to estimate the quantum channel. Therefore, we need to apply the above optimization to the above practical settings. An interesting future study would be to clarify the order of the second order larger after the above optimization in such practical settings.

Next, in order to improve the key generation rate, we discuss how to increase the block length n. For this aim, we discuss the implementation cost for our protocol in the software part. The numerical plots in Fig. 1 show that the block length n needs to be chosen as 10^{10} to attain the rate $A(p_2)$. However, it does not require one to prepare an error correcting code with such a long block length. It is sufficient to prepare modified Toeplitz matrices with such a long block length. This construction can be done only with the calculation complexity $O(n \log_2 n)$ Reference [35, Appendices C and D] explains how to implement the multiplication of the Toeplitz matrix. Indeed, Ref. [35, Appendix E-A] reported its actual implementation for key length 10^8 using a typical personal computer equipped with a 64-bit CPU (Intel Core i7) with 16 GByte memory, and using a publicly available software library. Therefore, we can expect to implement the privacy amplification with $n = 10^{10}$ in a current technology.

Here, we should remark on the relation between our method for privacy amplification and the method by [9,17,36]. Our method is based on the method by [4,5,25] and the paper in [36] clarified what condition for hash functions is essential for this method. To clarify the point, the paper in [36] introduced the concept of dual universal2 hash functions and explained the difference between dual universal2 hash functions and universal2 hash functions, which are used in the method by [9,17,36]. While the privacy amplification in our method [4,5,25] requires a surjectivity and linearity, the privacy amplification in [9,17,36] works with a general universal2 hash function, i.e., the linearity is not needed in [9,17,36]. However, as explained in [35, Sec. III-C], our method has a better robustness than the method by [9,17,36].

ACKNOWLEDGMENTS

The author was supported in part by the National Natural Science Foundation of China (Grant No. 62171212) and Guangdong Provincial Key Laboratory (Grant No. 2019B121203002).

APPENDIX A: PROOF OF (11)

The relation (11) is shown as follows:

$$\frac{1}{2}\left\|\rho^{\mathrm{mid},i}_{LGK\hat{K}E} - \rho^{\mathrm{real},i}_{LGK\hat{K}E}\right\|_1 = \frac{1}{2}\left\| \sum_{l=0}^{l_{\mathrm{m}}} \sum_{g} P^i_{LG}(l,g)|l,g\rangle\langle l,g| \otimes \sum_{k=1}^{2^l} \frac{1}{2^l}\left(|k,k\rangle\langle k,k| - \sum_{\hat{k}=1}^{2^l} P^i_{\hat{K}|K,L=l}(\hat{k}|k)|k,\hat{k}\rangle\langle k,\hat{k}|\right)\right.$$

$$\left. \otimes \rho^i_{E|K=k,L=l,G=g}\right\|_1$$

$$= \frac{1}{2}\sum_{l=0}^{l_{\mathrm{m}}} P^i_L(l)\left\| \sum_{k=1}^{2^l} \frac{1}{2^l}\left(|k,k\rangle\langle k,k| - \sum_{\hat{k}=1}^{2^l} P^i_{\hat{K}|K,L=l}(\hat{k}|k)|k,\hat{k}\rangle\langle k,\hat{k}|\right)\right\|_1$$

$$= P^i_{K,\hat{K}}(\hat{K} \neq K)$$

$$\begin{aligned}
&\leqslant \Pr(f_{i,S_i}(X_i) \neq f_{i,S_i}(\hat{X}_i),\ f_{2+i,S_{2+i}}[f_{i,S_i}(X_i)] = f_{2+i,S_{2+i}}[f_{i,S_i}(\hat{X}_i)]) \\
&= \Pr(f_{i,S_i}(X_i) \neq f_{i,S_i}(\hat{X}_i)) \Pr(f_{2+i,S_{2+i}}[f_{i,S_i}(X_i)] = f_{2+i,S_{2+i}}[f_{i,S_i}(\hat{X}_i)] | f_{i,S_i}(X_i) \neq f_{i,S_i}(\hat{X}_i)) \\
&\overset{(a)}{\leqslant} \Pr(f_{i,S_i}(X_i) \neq f_{i,S_i}(\hat{X}_i)) \frac{1}{2^{m_3}} \leqslant \frac{1}{2^{m_3}} = \frac{1}{n},
\end{aligned} \tag{A1}$$

where (a) follows from (11).

APPENDIX B: PROOF OF (13)

To show (13), we divide the public information G into two parts G_1 and G_2. G_1 is the public information except for $f_{2+i,S_{2+i}}[f_{2+i,S_{2+i}}(X_i)]$ and G_2 is the public information $f_{2+i,S_{2+i}}[f_{2+i,S_{2+i}}(X_i)]$. Also, we denote keys after privacy amplification and its length by $K_* = (K_1, K_2)$ and L_1, respectively, where K_1 is the initial m_3 bits and K_2 is the remaining bits. Since $K_1 \mapsto f_{2+i}(K_1 k_2)$ is bijective for every k_2, (K_1, K_2) and (G_2, K_2) have a one-to-one relation. Now, we say that the phase basis (the bit basis) is the dual basis when we focus on the information on the bit basis (the phase basis). That is, when $i = 1$ ($i = 2$), the dual basis is the phase basis (the bit basis).

Now, we focus on the fidelity $F(\rho^{\mathrm{ideal},i}_{L_1G_1K_*E}(\vec{\sigma}_{E|L_1G_1}), \rho^{\mathrm{real},i}_{L_1G_1K_*E})$ between $\rho^{\mathrm{ideal},i}_{L_1G_1K_*E}(\vec{\sigma}_{E|L_1G_1})$ and $\rho^{\mathrm{real},i}_{L_1G_1K_*E}$. We define the virtual decoding error probability $P^i_{du|L_1=l}$ in the dual basis for $i = 1, 2$ depending on $L_1 = l$. As shown in Appendix C, the relation

$$\begin{aligned}
&\max_{\vec{\sigma}_{E|G_1}} F\left(\rho^{\mathrm{ideal},i}_{G_1K_*E|L_1=l}(\vec{\sigma}_{E|G_1}), \rho^{\mathrm{real},i}_{G_1K_*E|L_1=l}\right) \\
&\quad \geqslant \sqrt{1 - P^i_{du|L_1=l}}
\end{aligned} \tag{B1}$$

holds. Hence we have

$$\begin{aligned}
&\max_{\vec{\sigma}_{E|L_1G_1}} F\left(\rho^{\mathrm{ideal},i}_{L_1G_1K_*E}(\vec{\sigma}_{E|L_1G_1}), \rho^{\mathrm{real},i}_{L_1G_1K_*E}\right) \\
&= \sum_l P_{L_1}(l) \max_{\vec{\sigma}_{E|G_1}} F\left(\rho^{\mathrm{ideal},i}_{G_1K_*E|L_1=l}(\vec{\sigma}_{E|G_1}), \rho^{\mathrm{real},i}_{G_1K_*E|L_1=l}\right) \\
&\overset{(a)}{\geqslant} \sum_l P_{L_1}(l) \sqrt{1 - P^i_{du|L_1=l}} \\
&\overset{(b)}{\geqslant} \sqrt{\sum_l P_{L_1}(l)\left(1 - P^i_{du|L_1=l}\right)} = \sqrt{1 - P^i_{du}},
\end{aligned} \tag{B2}$$

where (a) follows from (B1) and (b) follows from the concavity of the function $x \mapsto \sqrt{x}$. Thus we have

$$\begin{aligned}
&\min_{\vec{\sigma}_{E|LG}} \frac{1}{2} \left\| \rho^{\mathrm{ideal},i}_{LGKE}(\vec{\sigma}_{E|LG}) - \rho^{\mathrm{real},i}_{LGKE} \right\|_1 \\
&\overset{(a)}{\leqslant} \min_{\vec{\sigma}_{E|L_1G}} \frac{1}{2} \left\| \rho^{\mathrm{ideal},i}_{L_1GK_2E}(\vec{\sigma}_{E|L_1G}) - \rho^{\mathrm{real},i}_{L_1GK_2E} \right\|_1 \\
&\overset{(b)}{=} \min_{\vec{\sigma}_{E|L_1G_1G_2}} \frac{1}{2} \left\| \rho^{\mathrm{ideal},i}_{L_1G_1G_2K_2E}(\vec{\sigma}_{E|L_1G_1G_2}) - \rho^{\mathrm{real},i}_{L_1G_1G_2K_2E} \right\|_1 \\
&\leqslant \min_{\vec{\sigma}_{E|L_1G_1}} \frac{1}{2} \left\| \rho^{\mathrm{ideal},i}_{L_1G_1G_2K_2E}(\vec{\sigma}_{E|L_1G_1}) - \rho^{\mathrm{real},i}_{L_1G_1G_2K_2E} \right\|_1 \\
&\overset{(c)}{=} \min_{\vec{\sigma}_{E|L_1G_1}} \frac{1}{2} \left\| \rho^{\mathrm{ideal},i}_{L_1G_1K_1K_2E}(\vec{\sigma}_{E|L_1G_1}) - \rho^{\mathrm{real},i}_{L_1G_1K_1K_2E} \right\|_1 \\
&\overset{(d)}{\leqslant} \min_{\vec{\sigma}_{E|L_1G_1}} \sqrt{1 - F\left(\rho^{\mathrm{ideal},i}_{L_1G_1K_1K_2E}(\vec{\sigma}_{E|L_1G_1}), \rho^{\mathrm{real},i}_{L_1G_1K_1K_2E}\right)^2} \\
&= \sqrt{1 - \max_{\vec{\sigma}_{E|L_1G_1}} F\left(\rho^{\mathrm{ideal},i}_{L_1G_1K_1K_2E}(\vec{\sigma}_{E|L_1G_1}), \rho^{\mathrm{real},i}_{L_1G_1K_1K_2E}\right)^2} \\
&\overset{(e)}{\leqslant} \sqrt{1 - \left(1 - P^i_{du}\right)} = \sqrt{P^i_{du}},
\end{aligned} \tag{B3}$$

where (a) follows from the fact that K_2 is a part of K, (b) follows from the relation $G = (G_1G_2)$, (c) follows from the one-to-one relation between (K_1, K_2) and (G_2, K_2), (d) follows from the general inequality $\frac{1}{2}\|\rho - \sigma\| \leqslant \sqrt{1 - F(\rho, \sigma)^2}$ [37, (6.106)], and (e) follows from (B2). Hence we obtain (13).

APPENDIX C: PROOF OF (B1)

For simplicity, we show (B1) only for the case with $i = 1$. Since L_1 is fixed to l, we omit $L_1 = l$ in the following discussion. For $s, t \in \mathbb{F}_2^l$, we define operators on the l-qubit system as

$$W(s,t) := \left(\sum_{x' \in \mathbb{F}_2^l} |x' + s\rangle\langle x'|\right)\left(\sum_{x \in \mathbb{F}_2^l} (-1)^{t \cdot x} |x\rangle\langle x|\right), \tag{C1}$$

where $t \cdot x := \sum_{j=1}^l t_j x_j$. Then, by using a distribution P_{XZ} on $\mathbb{F}_2^{2l}$, a generalized Pauli channel $\Lambda[P_{XZ}]$ is written as

$$\Lambda[P_{XZ}](\rho) := \sum_{(s,t) \in \mathbb{F}_2^{2l}} P_{XZ}(s,t) W(s,t) \rho W(s,t)^\dagger. \tag{C2}$$

As shown in [25, Sec. V-B], the noisy channel can be considered as a generalized Pauli channel by considering the virtual application of discrete twirling. Also, the virtual application of discrete twirling does not change the joint state on Alice and Bob. Hence we can consider that Alice and Bob made the virtual application of discrete twirling. That is, we can consider that the obtained keys K_* and $\hat{K}_*$ are obtained via quantum communication via a generalized Pauli channel. In this case, as shown in [25, Appendix B], Eve's state $\rho_{E|K_*=k}$ with public information G is given as

$$\rho_{E|K_*=k} = \sum_{x \in \mathbb{F}_2^l} P_X(x) |P_{XZ}, k, x\rangle\langle P_{XZ}, k, x|, \tag{C3}$$

where

$$|P_{XZ}, y, x\rangle := \sum_{z \in \mathbb{F}_2^l} (-1)^{z \cdot y} \sqrt{P_{Z|X}(z|x)} |x, z\rangle. \tag{C4}$$

While the system E is composed of $2l$ qubits, the first l qubits do not have off-diagonal elements. When the first and second l qubits in E are written by E_1 and E_2, E_1 can be considered as a classical system.

We have

$$\rho_{K_* E} = \sum_{k\in\mathbb{F}_2^l} \frac{1}{2^l} |k\rangle\langle k| \otimes \rho_{E|K_*=k}. \tag{C5}$$

Then,

$$\begin{aligned}\max_{\sigma_E} F(\rho_{K_* E}, \rho_{K^*}\otimes\sigma_E) &= \max_{\sigma_E} F\left(\sum_{k\in\mathbb{F}_2^l} \frac{1}{2^l}|k\rangle\langle k| \otimes \sum_{x\in\mathbb{F}_2^l} P_X(x)|P_{XZ},k,x\rangle\langle P_{XZ},k,x|, \sum_{k\in\mathbb{F}_2^l}\frac{1}{2^l}|k\rangle\langle k|\otimes\sigma_{E_1E_2}\right)\\ &= \max_{\sigma_{E_2|E_1=x}} F\left(\sum_{k\in\mathbb{F}_2^l} \frac{1}{2^l}|k\rangle\langle k| \otimes \sum_{x\in\mathbb{F}_2^l} P_X(x)|P_{XZ},k,x\rangle\langle P_{XZ},k,x|, \sum_{k\in\mathbb{F}_2^l}\frac{1}{2^l}|k\rangle\langle k|\otimes\sigma_{E_1E_2}\right).\end{aligned} \tag{C6}$$

Since

$$\begin{aligned}&[I\otimes I\otimes W(0,t)]\sum_{k\in\mathbb{F}_2^l}\frac{1}{2^l}|k\rangle\langle k|\otimes\sum_{x\in\mathbb{F}_2^l}P_X(x)|P_{XZ},k,x\rangle\langle P_{XZ},k,x|[I\otimes I\otimes W(0,t)]^\dagger\\ &= \sum_{k\in\mathbb{F}_2^l}\frac{1}{2^l}|k\rangle\langle k|\otimes|P_{XZ},k,x\rangle\langle P_{XZ},k,x|\end{aligned} \tag{C7}$$

for $t\in\mathbb{F}_2^l$, the minimizer for $\sigma_{E_1E_2}$ can be assumed to be invariant for $I\otimes W(0,t)$. That is, $\sigma_{E_1E_2}$ has the form $\sum_{x,z\in\mathbb{F}_2^l} Q_{XZ}(x,z)|x,z\rangle\langle x,z|$. Hence

$$\begin{aligned}&\max_{\sigma_{E_1E_2}} F\left(\sum_{k\in\mathbb{F}_2^l} \frac{1}{2^l}|k\rangle\langle k| \otimes \sum_{x\in\mathbb{F}_2^l} P_X(x)|P_{XZ},k,x\rangle\langle P_{XZ},k,x|, \sum_{k\in\mathbb{F}_2^l}\frac{1}{2^l}|k\rangle\langle k|\otimes\sigma_{E_1E_2}\right)\\ &= \max_{\sigma_{E_1E_2}}\sum_{k\in\mathbb{F}_2^l}\frac{1}{2^l}F\left(\sum_{x\in\mathbb{F}_2^l}P_X(x)|P_{XZ},k,x\rangle\langle P_{XZ},k,x|,\sigma_{E_1E_2}\right)\\ &= \max_{Q_{XZ}}\sum_{k\in\mathbb{F}_2^l}\frac{1}{2^l}\sum_{x\in\mathbb{F}_2^l}\sqrt{P_X(x)Q_X(x)}F\left(|P_{XZ},k,x\rangle\langle P_{XZ},k,x|,\sum_{z\in\mathbf{1}_2}Q_{Z|X}(z|x)|x,z\rangle\langle x,z|\right)\\ &= \max_{Q_{XZ}}\sum_{k\in\mathbb{F}_2^l}\frac{1}{2^l}\sum_{x\in\mathbb{F}_2^l}\sqrt{P_X(x)Q_X(x)\left\langle P_{XZ},k,x\right|\sum_{z\in\mathbf{1}_2}Q_{Z|X}(z|x)|x,z\rangle\langle x,z|\left|P_{XZ},k,x\right\rangle}\\ &= \max_{Q_{XZ}}\sum_{k\in\mathbb{F}_2^l}\frac{1}{2^l}\sum_{x\in\mathbb{F}_2^l}\sqrt{P_X(x)Q_X(x)\sum_{z\in\mathbb{F}_2^l}P_{Z|X=x}(z)Q_{Z|X=x}(z)}\\ &= \max_{Q_X}\sum_{k\in\mathbb{F}_2^l}\frac{1}{2^l}\sum_{x\in\mathbb{F}_2^l}\sqrt{P_X(x)Q_X(x)\max_{z\in\mathbb{F}_2^l}P_{Z|X=x}(z)}\\ &= \max_{Q_X}\sum_{x\in\mathbb{F}_2^l}\sqrt{P_X(x)Q_X(x)\max_{z\in\mathbb{F}_2^l}P_{Z|X=x}(z)}\overset{(a)}{=}\sqrt{\sum_{x\in\mathbb{F}_2^l}P_X(x)\max_{z\in\mathbb{F}_2^l}P_{Z|X=x}(z)}\\ &\geqslant\sqrt{\max_{z\in\mathbb{F}_2^l}P_Z(z)}\geqslant\sqrt{1-P_{du}^1},\end{aligned} \tag{C8}$$

where (a) follows from the following relation: let $\{\alpha_i\}$ be general non-negative real numbers. We have the following minimization for probability distribution q_i:

$$\max_{q_i}\sum_i\sqrt{\alpha_i q_i} = \sqrt{\sum_i\alpha_i}, \tag{C9}$$

where the maximum is attained when $q_i = \frac{\alpha_i}{\sum_{i'}\alpha_{i'}}$. Therefore, we obtain (B1).

APPENDIX D: PROOF OF (16)

Using the definition of $\delta(p,\epsilon,m_1,m_2)$ given in (5), we calculate the length of the generated keys as follows:

$$\begin{aligned}
&\beta(1-r_1)n_1 - m_1(n_1,p_2) - m_3 + \beta(1-r_2)n_2 - m_2(n_2,p_1) - m_3 \\
&= \beta(1-r_1)n_1 - (1-r_1)n_1\{h[p_2+\delta(p_2,\epsilon,(1-r_1)n_1,r_2n_2)]\} \\
&\quad + \beta(1-r_2)n_2 - (1-r_2)n_2\{h[p_1+\delta(p_1,\epsilon,(1-r_2)n_2,r_1n_1)]\} - 2\log_2 n \\
&= \beta(1-r_1)n_1 - (1-r_1)n_1\left[h(p_2)+h'(p_2)\delta(p_2,\epsilon,(1-r_1)n_1,r_2n_2)+o\left(\frac{1}{\sqrt{n}}\right)\right] \\
&\quad + \beta(1-r_2)n_2 - (1-r_2)n_2\left[h(p_1)+h'(p_1)\delta(p_1,\epsilon,(1-r_2)n_2,r_1n_1)+o\left(\frac{1}{\sqrt{n}}\right)\right] - 2\log_2 n \\
&= (1-r_1)[\beta-h(p_2)]n_1 + (1-r_2)[\beta-h(p_1)]n_2 \\
&\quad - (1-r_1)h'(p_2)\delta(p_2,\epsilon,(1-r_1)n_1,r_2n_2)n_1 - (1-r_2)h'(p_1)\delta(p_1,\epsilon,(1-r_2)n_2,r_1n_1)n_2 + o(\sqrt{n}) \\
&= (1-r_1)[\beta-h(p_2)]n_1 + (1-r_2)[\beta-h(p_1)]n_2 \\
&\quad - B(p_2,\epsilon)\sqrt{\frac{[(1-r_1)n_1+r_2n_2](1-r_1)n_1}{r_2n_2}} - B(p_1,\epsilon)\sqrt{\frac{[(1-r_2)n_2+r_1n_1](1-r_2)n_2}{r_1n_1}} + o(\sqrt{n}).
\end{aligned} \tag{D1}$$

Hence we obtain (16).

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computing Systems and Signal Processing*, Bangalore, India, 1984 (IEEE, New York, 1984), pp. 175–179.

[2] H.-K. Lo, H. F. Chau, and M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, J. Cryptol. **18**, 133 (2005).

[3] M. Hayashi, Optimal ratio between phase basis and bit basis in quantum key distributions, Phys. Rev. A **79**, 020303(R) (2009).

[4] M. Hayashi, Practical evaluation of security for quantum key distribution, Phys. Rev. A **74**, 022307 (2006).

[5] M. Hayashi and T. Tsurumaru, Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths, New J. Phys. **14**, 093014 (2012).

[6] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[7] D. Mayers, in *Advances in Cryptology Proceedings of Crypto'96*, edited by N. Koblitz, Lecture Notes in Computer Science Vol. 1109 (Springer-Verlag, New York, 1996), p. 343; D. Mayers, J. ACM **48**, 351 (2001).

[8] M. Hamada, Reliability of Calderbank-Shor-Steane codes and security of quantum key distribution, J. Phys. A: Math. Gen. **37**, 8303 (2004).

[9] R. Renner, Security of quantum key distribution, Ph.D. dissertation, Dipl. Phys. ETH, Zurich, Switzerland, 2005.

[10] S. Watanabe, R. Matsumoto, and T. Uyematsu, Noise tolerance of the BB84 protocol with random privacy amplification, Int. J. Quantum Inf. **04**, 935 (2006).

[11] V. Strassen, Asymptotische abschätzungen in Shannons informationstheorie, in Transactions of the Third Prague Conference on Information Theory, Prague, 1962, pp. 689–723, http://www.math.cornell.edu/.

[12] M. Hayashi, Second-order asymptotics in fixed-length source coding and intrinsic randomness, IEEE Trans. Inf. Theory **54**, 4619 (2008).

[13] M. Hayashi, Information spectrum approach to second-order coding rate in channel coding, IEEE Trans. Inf. Theory **55**, 4947 (2009).

[14] Y. Polyanskiy, H. V. Poor, and S. Verdú, Channel coding rate in the finite blocklength regime, IEEE Trans. Inf. Theory **56**, 2307 (2010).

[15] K. Li, Second order asymptotics for quantum hypothesis testing, Ann. Statist. **42**, 171 (2014).

[16] M. Tomamichel and M. Hayashi, A hierarchy of information quantities for finite block length analysis of quantum tasks, IEEE Trans. Inf. Theory **59**, 7693 (2013).

[17] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[18] K. Bradler, M. Mirhosseini, R. Fickler, A. Broadbent, and R. Boyd, Finite-key security analysis for multilevel quantum key distribution, New J. Phys. **18**, 073030 (2016).

[19] S. Khatri, E. Kaur, S. Guha, and M. M. Wilde, Second-order coding rates for key distillation in quantum key distribution, arXiv:1910.03883.

[20] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *The Universal Composable Security of Quantum Key Distribution, Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005*, edited by J. Kilian, Lecture Notes in Computer Science Vol. 3378 (Springer-Verlag, Berlin, 2005), pp. 386–406.

[21] C. H. F. Fung, X. Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, Phys. Rev. A **81**, 012318 (2010).

[22] M. Hayashi, Exponential decreasing rate of leaked information in universal random privacy amplification, IEEE Trans. Inf. Theory **57**, 3989 (2011).

[23] J. L. Carter and M. N. Wegman, Universal classes of hash functions, J. Comput. Syst. Sci. **18**, 143 (1979).

[24] M. Hayashi and T. Tsurumaru, Corrigendum: Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths (2012 New J. Phys. 14 093014), New J. Phys. **23**, 129504 (2021).

[25] M. Hayashi, Upper bounds of eavesdropper's performances in finite-length code with the decoy method, Phys. Rev. A **76**, 012329 (2007); **79**, 019901(E) (2009).

[26] M. Hayashi, Quantum-inspired secure wireless communication protocol under spatial and local Gaussian noise assumptions, IEEE Access **10**, 29040 (2022).

[27] J. Wu, G.-L. Long, and M. Hayashi, Quantum secure direct communication with private dense coding using general preshared quantum state, arXiv:2112.15113.

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

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

[30] X.-F. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[31] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005); Decoy-state protocol for quantum cryptography with four different intensities of coherent light, Phys. Rev. A **72**, 012322 (2005).

[32] T. C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A **61**, 010303(R) (1999).

[33] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (2000).

[34] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[35] M. Hayashi and T. Tsurumaru, More efficient privacy amplification with less random seeds via dual universal hash function, IEEE Trans. Inf. Theory **62**, 2213 (2016).

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

[37] M. Hayashi, S. Ishizaka, A. Kawachi, G. Kimura, and T. Ogawa, *Introduction to Quantum Information Science*, Graduate Texts in Physics (Springer, Berlin, 2014) (Originally published from Kyoritsu Shuppan in 2012 with Japanese.).