Tomography increases key rates of quantum-key-distribution protocols

Shun Watanabe,* Ryutaroh Matsumoto,† and Tomohiko Uyematsu‡
Department of Communications and Integrated Systems, Tokyo Institute of Technology, 2-12-1, Oookayama, Meguro-ku, Tokyo, 152-8552, Japan

(Received 18 February 2008; revised manuscript received 16 July 2008; published 17 October 2008)

We construct a practically implementable classical processing for the Bennett-Brassard 1984 (BB84) protocol and the six-state protocol that fully utilizes the accurate channel estimation method, which is also known as the quantum tomography. Our proposed processing yields at least as high a key rate as the standard processing by Shor and Preskill. We show two examples of quantum channels over which the key rate of our proposed processing is strictly higher than the standard processing. In the second example, the BB84 protocol with our proposed processing yields a positive key rate even though the so-called error rate is higher than the 25% limit.

DOI: 10.1103/PhysRevA.78.042316 PACS number(s): 03.67.Dd, 89.70.−a, 03.65.Wj

I. INTRODUCTION

Quantum key distribution (QKD) has attracted great attention as an unconditionally secure key distribution scheme. The fundamental feature of QKD protocols is that the amount of information gained by an eavesdropper, usually referred to as Eve, can be estimated from the channel between the legitimate sender and the receiver, usually referred to as Alice and Bob, respectively. Such a task cannot be conducted in classical key distribution schemes. If the estimated amount is lower than a threshold, then Alice and Bob determine the length of a secret key from the estimated amount of Eve's information, and can share a secret key by performing the information reconciliation (error correction) [1,2] and the privacy amplification [2,3]. Since the key rate, which is the length of securely sharable key per channel use, is one of the most important criteria for the efficiency of QKD protocols, the estimation of the channel is of primary importance.

In this paper, we only treat the Bennett-Brassard 1984 (BB84) protocol [4] and the six-state protocol [5], and we mean the BB84 protocol and the six-state protocol by the QKD protocols throughout the paper. Furthermore, a classical processing consists of a procedure to determine a key rate from a channel estimate and a procedure for the information reconciliation and the privacy amplification.

Mathematically, quantum channels are described by trace preserving completely positive (TPCP) maps [6]. Conventionally in the QKD protocols, we only use the statistics of matched measurement outcomes, which are transmitted and received by the same basis, to estimate the TPCP map describing the quantum channel; mismatched measurement outcomes, which are transmitted and received by different bases, are discarded in the conventionally used channel estimation methods. By using the statistics of mismatched measurement outcomes in addition to that of matched measurement outcomes, we can estimate the TPCP map more accurately than the conventional estimation method. Such an accurate channel estimation method is also known as the quantum tomography [7,8]. In the early 1990s, Barnett *et al.* [9] showed that the use of mismatched measurement outcomes enables Alice and Bob to detect the presence of Eve with higher probability for the so-called intercept and resend attack. Furthermore, some literature uses the accurate estimation method to ensure the channel to be a Pauli channel [10–13], where a Pauli channel is a channel over which four kinds of Pauli errors (including the identity) occur probabilistically. However, the channel is not necessarily a Pauli channel.

The use of the accurate channel estimation method in a classical processing has a potential to improve the key rates of previously known classical processing. However, there is no proposed practically implementable classical processing that fully utilizes the accurate estimation method. Recently, Renner *et al.* [14–16] developed information theoretical techniques to prove the security of the QKD protocols. Their proof techniques can be used to prove the security of the QKD protocols with a classical processing that fully utilizes the accurate estimation method. However, they only considered Pauli channels or partial twirled channels.[1] For Pauli channels, the accurate estimation method and the conventional estimation method make no difference.

In this paper, we construct a practically implementable classical processing that fully utilizes the accurate channel estimation method. More precisely, we present a procedure to determine a key rate based on the accurate channel estimate for the BB84 protocol and the six-state protocol, respectively. Then we also present a practically implementable procedure for the information reconciliation and the privacy amplification in which we can share a secret key at the determined key rate. Note that we only change the classical processing of the QKD protocols, and the method of the transmission and reception of quantum systems in the QKD protocols remains unchanged.

Although it is straightforward to determine a key rate from the accurate channel estimate for the six-state protocol,

*shun-wata@it.ss.titech.ac.jp
†ryutaroh@rmatsumoto.org
http://www.rmatsumoto.org/research.html
‡uyematsu@ieee.org

[1] By the partial twirling (discrete twirling) [17], any channel becomes a Pauli channel.

it is subtle how to determine a key rate from the accurate channel estimate for the BB84 protocol. More specifically, we can obtain only partial parameters describing the channel, and there remain some free parameters. Thus we have to consider the worst case, i.e., the key rate that is minimized over the free parameters. We shall show an explicit procedure to determine the minimized key rate.

Our proposed processing yields at least as high a key rate as the standard processing by Shor and Preskill [18]. As examples, we show that the key rate of our proposed classical processing is strictly higher than that of the standard processing for the amplitude damping channel and the rotation channel, which are unitary channels that rotate the Bloch sphere in the z-x plane. In the example of the amplitude damping channel, we show that the key rate of the so-called reverse reconciliation,[2] in which the key is generated based on Bob's bit sequence, is higher than the key rate of the direct reconciliation, in which the key is generated based on Alice's bit sequence.[3] In the example of the rotation channel, we solve a problem left open in [Ref. [22], Sec. V]—the problem of whether it is possible to obtain positive key rates from both matched measurement outcomes and mismatched measurement outcomes for the BB84 protocol.

It is believed that we cannot share any secret key if the so-called error rate is higher than the 25% limit in the BB84 protocol [23]. However, Curty *et al.* [24] suggested that, for some asymmetric error patterns, it might be possible to share a secret key even for the error rates above the 25% limit. In the example of the rotation channel, we show that we can actually obtain a positive key rate even though the error rate is higher than the 25% limit.

Devetak and Winter [25] also showed the key rate formula that coincides with the key rate formula shown by Renner *et al.* [14–16] if we know the channel exactly. By combining our proposed procedure to determine a key rate based on the accurate channel estimate and Devetak and Winter's procedure for the information reconciliation and the privacy amplification, we can obtain the same key rate as in this paper. However, the procedure for the information reconciliation and the privacy amplification shown by Devetak and Winter is not practically implementable.

Our proposed information reconciliation can be implemented by any efficiently decodable linear code for the Slepian-Wolf coding [26]. For example, we can use the low density parity check matrix (LDPC) code [27].

The rest of this paper is organized as follows: We first present a procedure for the information reconciliation and the privacy amplification in Sec. II. Then we present a procedure to determine a key rate from the estimate of the channel in Sec. III. We consider the amplitude damping channel, the unital channel, and the rotation channel as examples, and show that the key rate of our proposed processing is higher than the standard processing in Sec. IV. We state the conclusion in Sec. V.

[2]The reverse reconciliation was originally proposed by Maurer [19] in the classical key agreement.

[3]For QKD protocols with weak coherent states, literature [20,21] already pointed out that the key rate of the direct reconciliation and the reverse reconciliation are different.

In this paper, we mainly consider standard procedures for the information reconciliation and the privacy amplification with one-way classical communication, i.e., we do not treat, except in Remarks 9 and 10, the noisy preprocessing [14,16] nor procedures with two-way classical communication [23,28]. However, our results in this paper can be easily extended to procedures with the noisy preprocessing and two-way classical communication (see Remark 11).

II. INFORMATION RECONCILIATION AND PRIVACY AMPLIFICATION

We construct a practical procedure for the information reconciliation and the privacy amplification in this section. We first describe our proposed procedure with general linear codes and the maximum *a posteriori* probability (MAP) decoding. Then as an example of efficiently decodable linear code, we show how to apply the sum-product algorithm of the low density parity check matrix (LDPC) code[4] to our proposed procedure in Remark 5.

For simplicity we assume that Eve's attack is the collective attack,[5] i.e., the channel connecting Alice and Bob is given by tensor products of a channel $\mathcal{E}_B$ from a qubit density matrix to itself. As is usual in QKD literature, we assume that Eve can access all the environment of channel $\mathcal{E}_B$; the channel to the environment is denoted by $\mathcal{E}_E$.

In the six-state protocol, Alice randomly sends bit 0 or 1 to Bob by modulating it into a transmission basis that is randomly chosen from the z basis $\{|0_z\rangle,|1_z\rangle\}$, the x basis $\{|0_x\rangle,|1_x\rangle\}$, or the y basis $\{|0_y\rangle,|1_y\rangle\}$, where $|0_a\rangle,|1_a\rangle$ are eigenstates of the Pauli matrix σ_a for $a\in\{x,y,z\}$, respectively. Then Bob randomly chooses one of the measurement observables σ_x, σ_y, and σ_z, and converts a measurement result +1 or −1 into a bit 0 or 1, respectively. After a sufficient number of transmissions, Alice and Bob publicly announce their transmission bases and measurement observables. They also announce a part of their bit sequences for estimating channel $\mathcal{E}_B$. Note that Alice and Bob do not discard mismatched measurement outcomes, which are transmitted and received by different bases, to estimate the channel accurately.

In the BB84 protocol, Alice uses only z basis and x basis to transmit the bit sequence, and Bob uses only observable σ_z and σ_x to receive the bit sequence.

Henceforth, we treat only Alice's bit sequence $\mathbf{x}\in\mathbb{F}_2^n$ that is transmitted in z basis and corresponding Bob's bit sequence $\mathbf{y}\in\mathbb{F}_2^n$ that is received in σ_z measurement, where $\mathbb{F}_2$ is the finite field of order 2. Furthermore, we occasionally omit the subscripts $\{x,y,z\}$ of bases, and the basis $\{|0\rangle,|1\rangle\}$ is regarded as z basis unless otherwise stated. Since the pair of sequences $(\mathbf{x},\mathbf{y})$ is transmitted and received in z basis, they

[4]It should be noted that the application of the LDPC codes for classical key agreement protocols has been considered by Muramatsu [29], in which he uses the LDPC code as the Slepian-Wolf source coding.

[5]This assumption is not essential. By using the de Finetti representation arguments [15,30], our result can be extended to the coherent attack.

are independently identically distributed according to

$$P_{XY}(x,y) := \frac{1}{2}\langle y_{\mathsf{z}}|\mathcal{E}_B(|x_{\mathsf{z}}\rangle\langle x_{\mathsf{z}}|)|y_{\mathsf{z}}\rangle. \tag{1}$$

Note that the distribution P_{XY} can be estimated from the statistics of the sample bits that are transmitted by z basis and received by σ_{z} observable.

Before describing our proposed procedure, we should review the basic facts of linear codes. An $[n,n-m]$ classical linear code $\mathcal{C}$ is an $(n-m)$-dimensional linear subspace of $\mathbb{F}_2^n$, and its parity check matrix M is an $m\times n$ matrix of rank m with 0,1 entries such that $M\mathbf{c}=\mathbf{0}$ for any code word $\mathbf{c}\in\mathcal{C}$. By using these preparations, our proposed procedure is described as follows:

(i) Alice calculates syndrome $\mathbf{t}:=M\mathbf{x}$, and sends it to Bob over the public channel.

(ii) Bob decodes $(\mathbf{y},\mathbf{t})$ into estimate $\hat{\mathbf{x}}$ of $\mathbf{x}$ by using the maximum *a posteriori* probability (MAP) decoding. More precisely, Bob selects $\hat{\mathbf{x}}\in\mathbb{F}_2^n$ such that $M\hat{\mathbf{x}}=\mathbf{t}$ and *a posteriori* probability $P_{X|Y}^n(\hat{\mathbf{x}}|\mathbf{y})$ is maximized (if there are tied sequences, then he selects the smallest one with respect to the lexicographic order), where $P_{X|Y}^n$ is the nth product distribution of $P_{X|Y}$.

(iii) Alice randomly chooses a hash function $f:\mathbb{F}_2^n\to\mathcal{S}_n$ from a set of universal hash functions [31], and sends the choice to Bob over the public channel. Then Alice and Bob's final keys are $s_A:=f(\mathbf{x})$ and $s_B:=f(\hat{\mathbf{x}})$, respectively.

If we set the rate of syndrome as

$$\frac{m}{n} > H(X|Y), \tag{2}$$

then there is a linear code in the LDPC codes such that Bob's decoding error probability is arbitrarily small for sufficiently large n [Ref. [32], Theorem 2], where $H(X|Y)$ is the conditional entropy with respect to the joint probability distribution P_{XY} [33]. Note that the base of a logarithm and a (conditional) entropy are 2 throughout the paper.

The key rate, $\frac{1}{n}\log_2|\mathcal{S}_n|$, is determined according to the results of privacy amplification [[15], Corollary 3.3.7 and Lemma 6.4.1]. Let

$$H_\rho(X|E) := H(\rho_{XE}) - H(\rho_E)$$

be the conditional von Neumann entropy with respect to density matrix $\rho_{XE}:=\Sigma_{x\in\mathbb{F}_2}\frac{1}{2}|x\rangle\langle x|\otimes\mathcal{E}_E(|x\rangle\langle x|)$, where $H(\rho)$ is the von Neumann entropy for a density matrix ρ. If the key rate satisfies

$$\frac{1}{n}\log_2|\mathcal{S}_n| < H_\rho(X|E) - \frac{m}{n}, \tag{3}$$

then the final key S_A is secure in the sense of the trace distance.[6] More precisely, the density matrix $\rho_{S_A\mathbf{T}FE^n}$, which describes Alice's final key S_A, the publicly transmitted syndrome $\mathbf{T}$ and hash function F, and the state in Eve's system E^n, satisfies

$$\|\rho_{S_A\mathbf{T}FE^n} - \rho_S\otimes\rho_{\mathbf{T}FE^n}\| \leqslant \varepsilon$$

for arbitrarily small ε and sufficiently large n, where $\rho_S:=\Sigma_{s\in\mathcal{S}_n}\frac{1}{|\mathcal{S}_n|}|s\rangle\langle s|$ is the density matrix that describes the uniformly distributed key on $\mathcal{S}_n$. From Eqs. (2) and (3), we find that

$$H_\rho(X|E) - H(X|Y) \tag{4}$$

is a secure key rate.

Note that the conditional von Neumann entropy $H_\rho(X|E)$ can be calculated from the channel $\mathcal{E}_B$ as follows. Since system X is classical, we can rewrite $H(\rho_{XE})=H(X)+\Sigma_{x\in\mathbb{F}_2}\frac{1}{2}H(\mathcal{E}_E(|x\rangle\langle x|))$. Noting that $H(\mathcal{E}_E(|x\rangle\langle x|))=H(\mathcal{E}_B(|x\rangle\langle x|))$ and $H(\rho_E)=H((\mathrm{id}\otimes\mathcal{E}_B)(\psi))$ for the maximally entangled state $|\psi\rangle:=\Sigma_{x\in\mathbb{F}_2}\frac{1}{\sqrt{2}}|x\rangle|x\rangle$, Eve's ambiguity for Alice's bit, $H_\rho(X|E)$, can be calculated from the channel $\mathcal{E}_B$. How to determine Eve's ambiguity $H_\rho(X|E)$ from an estimate of the channel $\mathcal{E}_B$ is discussed in the next section.

Remark 1. If we use the conventionally used method [18,34] for decoding $\hat{\mathbf{x}}$, the rate of syndrome $\frac{m}{n}$ cannot be as small as the right-hand side of Eq. (2). Thus, the key rate in Eq. (4) cannot be achieved. Define a probability distribution on $\mathbb{F}_2$ as

$$P_W(w) := \sum_{y\in\mathbb{F}_2} P_Y(y)P_{X|Y}(y+w|y). \tag{5}$$

Then the error $\mathbf{w}:=\mathbf{x}+\mathbf{y}$ between Alice and Bob's sequence is distributed according to P_W^n. In the conventional method, Bob calculates the difference of syndromes, $\mathbf{t}+M\mathbf{y}$, and selects the error $\hat{\mathbf{w}}$ such that $M\hat{\mathbf{w}}=\mathbf{t}+M\mathbf{y}$ and the likelihood of the error $P_W^n(\hat{\mathbf{w}})$ is maximized. Then, the estimate for Alice's sequence is $\hat{\mathbf{x}}=\mathbf{y}+\hat{\mathbf{w}}$. The rate of syndrome has to be larger than $H(W)$ for the decoding error probability to be small. By the log-sum inequality [33] and Eq. (5), we have

$$\begin{aligned} H(X|Y) &= \sum_{x,y\in\mathbb{F}_2} P_Y(y)P_{X|Y}(x|y)\log_2\frac{1}{P_{X|Y}(x|y)} \\ &= \sum_{w,y\in\mathbb{F}_2} P_Y(y)P_{X|Y}(y+w|y)\log_2\frac{P_Y(y)}{P_Y(y)P_{X|Y}(y+w|y)} \\ &\leqslant \sum_{w\in\mathbb{F}_2} P_W(w)\log_2\frac{1}{P_W(w)} = H(W). \end{aligned}$$

Thus, the key rate in Eq. (4) cannot be achieved by the conventional decoding method unless $P_{X|Y}(w|0)$ equals $P_{X|Y}(1+w|1)$ for any $w\in\mathbb{F}_2$.

Remark 2. By switching the role of Alice and Bob, we obtain a classical processing that achieves the key rate

$$H_\rho(Y|E) - H(Y|X). \tag{6}$$

Such a procedure is usually called the reverse reconciliation. On the other hand, the original procedure is usually called the direct reconciliation. The reverse reconciliation was originally proposed by Maurer in the classical key agreement context [19].

[6] The trace norm of a matrix A is defined by $\|A\| := \mathrm{Tr}\sqrt{A^*A}$. Then the trace distance between two matrices A and B is defined by $\|A-B\|$.

Note that we can calculate the conditional von Neumann entropy $H_\rho(Y|E)=H(\rho_{YE})-H(\rho_E)$ from the channel $\mathcal{E}_B$ as follows. Let ψ_{ABE} be a purification of $(\mathrm{id}\otimes\mathcal{E}_B)(\psi)$, and let $\rho_{BE}:=\mathrm{Tr}_A[\psi_{ABE}]$. Then, the density matrix ρ_{YE} is derived by measurement on Bob's system, i.e.,

$$\rho_{YE}=\sum_{y\in\mathbb{F}_2}(|y\rangle\langle y|\otimes I)\rho_{BE}(|y\rangle\langle y|\otimes I).$$

In Sec. IV A, we will show that the key rate of the reverse reconciliation can be higher than that of the direct reconciliation. The fact that the key rate of the direct reconciliation and the reverse reconciliation are different is already pointed out for QKD protocols with weak coherent states [20,21].

Remark 3. We used the MAP decoding instead of the maximum likelihood (ML) decoding in our procedure, because the MAP decoding minimizes the decoding error probability, and the MAP decoding is different from the ML decoding for the reverse reconciliation. In the ML decoding for the reverse reconciliation, Alice selects $\hat{\mathbf{y}}\in\mathbb{F}_2^n$ such that $M\hat{\mathbf{y}}$ equals the syndrome $\mathbf{t}=M\mathbf{y}$, and that the likelihood $P^n_{X|Y}(\mathbf{x}|\hat{\mathbf{y}})$ is maximized. Since the prior probability of Bob's sequence $\mathbf{y}$ is not necessarily the uniform distribution, the ML decoding and the MAP decoding are not necessarily equivalent, i.e.,

$$\operatorname*{argmax}_{\hat{\mathbf{y}}:\ M\hat{\mathbf{y}}=\mathbf{t}} P^n_{X|Y}(\mathbf{x}|\hat{\mathbf{y}})=\operatorname*{argmax}_{\hat{\mathbf{y}}:\ M\hat{\mathbf{y}}=\mathbf{t}} P^n_{Y|X}(\hat{\mathbf{y}}|\mathbf{x})$$

does not hold in general.

Remark 4. By modifying our proposed procedure as follows, we obtain a procedure in which Alice and Bob can share a secret key from Alice's sequence $\mathbf{x}$ that is transmitted by z basis and corresponding Bob's sequence $\mathbf{y}$ that is received by σ_{x} measurement. Since $(\mathbf{x},\mathbf{y})$ are independently identically distributed according to

$$P_{XY'}(x,y):=\frac{1}{2}\langle y_{\mathsf{x}}|\mathcal{E}_B(|x_{\mathsf{z}}\rangle\langle x_{\mathsf{z}}|)|y_{\mathsf{x}}\rangle, \tag{7}$$

we replace $P^n_{X|Y}$ in step (ii) with $P^n_{X|Y'}$. By a similar argument as in the original procedure, the secure key rate of the modified procedure is given by

$$H_\rho(X|E)-H(X|Y'). \tag{8}$$

In Sec. IV B, we shall show an example in which Alice and Bob can share secret keys both from matched measurement outcomes and mismatched measurement outcomes, i.e., both Eqs. (4) and (8) are positive.

Remark 5. The sum-product algorithm can be used in step (ii) of our proposed procedure as follows. For a given sequence $\mathbf{y}\in\mathbb{F}_2^n$, and a syndrome $\mathbf{t}\in\mathbb{F}_2^m$, define a function

$$P^*(\hat{\mathbf{x}}):=\prod_{j=1}^n P_{X|Y}(\hat{x}_j|y_j)\prod_{k=1}^m \mathbf{1}\left[\sum_{\ell\in N(k)}\hat{x}_\ell=t_k\right], \tag{9}$$

where $N(k):=\{j|M_{kj}=1\}$ for the parity check matrix M, and $\mathbf{1}[\ ]$ is the indicator function. The function $P^*(\hat{\mathbf{x}})$ is the nonnormalized *a posteriori* probability distribution on $\mathbb{F}_2^n$ given $\mathbf{y}$ and $\mathbf{t}$. The sum-product algorithm is a method to (approximately) calculate the marginal *a posteriori* probability, i.e.,

$$P^*_j(\hat{x}_j):=\sum_{\hat{x}_\ell,\ell\neq j}P^*(\hat{\mathbf{x}}).$$

The definition of *a posteriori* probability in Eq. (9) is the only difference between the decoding for the Slepian-Wolf source coding and that for the channel coding. More precisely, we replace [[35], Eq. (47.6)], with Eq. (9) and use the algorithm in [[35], Sec. 47.3]. The above procedure is a generalization of [36], and a special case of [37].

In QKD protocols we should minimize the block error probability rather than the bit error probability, because a bit error might propagate to other bits after the privacy amplification. Although the sum-product algorithm is designed to minimize the bit error probability, it is known by computer simulations that the algorithm makes the block error probability small [35].

III. PROCEDURE FOR CHANNEL ESTIMATION

In this section we show procedures to estimate Eve's ambiguity $H_\rho(X|E)$ for the six-state protocol and the BB84 protocol. We first present general preliminaries in Sec. III A. Then we show procedures for the six-state protocol and the BB84 protocol in Secs. III B and III C, respectively. In Sec. III D, we clarify the relation between our proposed procedures for estimating $H_\rho(X|E)$ and the conventional ones.

Although we explain the procedures to estimate $H_\rho(X|E)$ for the direct reconciliation, the estimation of $H_\rho(Y|E)$ for the reverse reconciliation can be done in a similar manner.

A. Preliminaries

In the Stokes parametrization, the qubit channel $\mathcal{E}_B$ can be described by the affine map parametrized by 12 real parameters [38,39] as follows:

$$\begin{bmatrix}\theta_{\mathsf{z}}\\ \theta_{\mathsf{x}}\\ \theta_{\mathsf{y}}\end{bmatrix}\mapsto\begin{bmatrix}R_{\mathsf{zz}} & R_{\mathsf{zx}} & R_{\mathsf{zy}}\\ R_{\mathsf{xz}} & R_{\mathsf{xx}} & R_{\mathsf{xy}}\\ R_{\mathsf{yz}} & R_{\mathsf{yx}} & R_{\mathsf{yy}}\end{bmatrix}\begin{bmatrix}\theta_{\mathsf{z}}\\ \theta_{\mathsf{x}}\\ \theta_{\mathsf{y}}\end{bmatrix}+\begin{bmatrix}t_{\mathsf{z}}\\ t_{\mathsf{x}}\\ t_{\mathsf{y}}\end{bmatrix}, \tag{10}$$

where $(\theta_{\mathsf{z}},\theta_{\mathsf{x}},\theta_{\mathsf{y}})$ describes a vector in the Bloch sphere [6]. For the channel $\mathcal{E}_B$ and each pair of bases $(\mathsf{a},\mathsf{b})\in\{\mathsf{z},\mathsf{x},\mathsf{y}\}^2$, define the biases of the outputs as

$$Q_{\mathsf{ab}0}:=\langle 0_{\mathsf{b}}|\mathcal{E}_B(|0_{\mathsf{a}}\rangle\langle 0_{\mathsf{a}}|)|0_{\mathsf{b}}\rangle-\langle 1_{\mathsf{b}}|\mathcal{E}_B(|0_{\mathsf{a}}\rangle\langle 0_{\mathsf{a}}|)|1_{\mathsf{b}}\rangle,$$

$$Q_{\mathsf{ab}1}:=\langle 1_{\mathsf{b}}|\mathcal{E}_B(|1_{\mathsf{a}}\rangle\langle 1_{\mathsf{a}}|)|1_{\mathsf{b}}\rangle-\langle 0_{\mathsf{b}}|\mathcal{E}_B(|1_{\mathsf{a}}\rangle\langle 1_{\mathsf{a}}|)|0_{\mathsf{b}}\rangle.$$

Then, a straightforward calculation shows the relations

$$R_{\mathsf{ba}}=\frac{1}{2}(Q_{\mathsf{ab}0}+Q_{\mathsf{ab}1}),\quad t_{\mathsf{b}}=\frac{1}{2}(Q_{\mathsf{ab}0}-Q_{\mathsf{ab}1}). \tag{11}$$

The qubit channel $\mathcal{E}_B$ can be also described by the Choi matrix $\rho_{AB}:=(\mathrm{id}\otimes\mathcal{E}_B)(\psi)$ [40] for the maximally entangled state $|\psi\rangle=\frac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|1\rangle)$. By using the parameters in Eq. (10), we can write the Choi matrix ρ_{AB} as

$$\frac{1}{4}\begin{bmatrix} 1+R_{zz}+t_z & R_{xz}+t_x+\mathbf{i}R_{yz}+\mathbf{i}t_y & R_{zx}-\mathbf{i}R_{zy} & R_{xx}+R_{yy}+\mathbf{i}R_{yx}-\mathbf{i}R_{xy} \\ R_{xz}+t_x-\mathbf{i}R_{yz}-\mathbf{i}t_y & 1-R_{zz}-t_z & R_{xx}-R_{yy}-\mathbf{i}R_{yx}-\mathbf{i}R_{xy} & -R_{zx}+\mathbf{i}R_{zy} \\ R_{zx}+\mathbf{i}R_{zy} & R_{xx}-R_{yy}+\mathbf{i}R_{yx}+\mathbf{i}R_{xy} & 1-R_{zz}+t_z & -R_{xy}+t_x-\mathbf{i}R_{yz}+\mathbf{i}t_y \\ R_{xx}+R_{yy}-\mathbf{i}R_{yx}+\mathbf{i}R_{xy} & -R_{zx}-\mathbf{i}R_{zy} & -R_{xz}+t_x+\mathbf{i}R_{yz}-\mathbf{i}t_y & 1+R_{zz}-t_z \end{bmatrix}, \tag{12}$$

where **i** is the imaginary unit.

B. Six-state protocol

An *ad hoc* approach to estimate Eve's ambiguity in the six-state protocol is very simple, because all parameters can be estimated from the statistics of sampled bits [7,8].

(i) By using the statistics of sampled bits and the relation in Eq. (11), Alice and Bob calculate the estimate $(\tilde{R},\tilde{t})$ for the parameters of the channel $\mathcal{E}_B$.

(ii) By using Eq. (12), Alice and Bob calculate the corresponding matrix $\tilde{\rho}_{AB}$. If the resulting matrix $\tilde{\rho}_{AB}$ is not a Choi matrix, Alice and Bob select a Choi matrix $\hat{\rho}_{AB}$ such that the Frobenius norm between $\hat{\rho}_{AB}$ and $\tilde{\rho}_{AB}$ is minimized.[7]

(iii) Alice and Bob calculate an estimator $H_{\hat{\rho}}(X|E)$ for Eve's ambiguity $H_\rho(X|E)$.

The validity of this estimation procedure is shown as follows. Since the estimators in step (i) converge to the true parameters in probability as the number of sampled bits goes to the infinity, the matrix $\tilde{\rho}_{AB}$ also converges[8] to ρ_{AB}. Then the Choi matrix $\hat{\rho}_{AB}$ also converges to the ρ_{AB}. Since the conditional entropy is a continuous function, the estimator $H_{\hat{\rho}}(X|E)$ in step (iii) also converges to $H_\rho(X|E)$ in probability as the number of sampled bits goes to the infinity.

C. BB84 protocol

The estimation of $H_\rho(X|E)$ in the BB84 protocol is much more complicated. When Alice and Bob only use z basis and x basis, the statistics of the input and the output are irrelevant to the parameters $(R_{zy},R_{xy},R_{yz},R_{yx},R_{yy},t_y)$. Thus, we can only estimate the parameters $\omega=(R_{zz},R_{zx},R_{xz},R_{xx},t_z,t_x)$, and we have to consider the worst case for the parameters ω, i.e.,

$$F(\omega) := \min_{\tau\in\mathcal{P}'(\omega)} H_{\rho_\tau}(X|E), \tag{13}$$

where $\mathcal{P}'(\omega)$ is the set of all parameters $\tau=(R_{zy},R_{xy},R_{yz},R_{yx},R_{yy},t_y)$ such that the parameters ω and τ constitute a qubit channel, and ρ_τ is the Choi matrix corresponding to the parameter τ.[9]

By using the following proposition, which is proved in Appendix B, we can make the desired function $F(\omega)$ into a simpler form.

Proposition 1. The minimization in Eq. (13) is achieved when the parameters R_{zy}, R_{xy}, R_{yz}, R_{yx}, and t_y are 0.

The number of free parameters has been reduced to 1 by Proposition 1. Thus the problem is rewritten as looking for an estimator of

$$F(\omega) = \min_{R_{yy}\in\mathcal{P}(\omega)} H_{\rho_{R_{yy}}}(X|E), \tag{14}$$

where $\mathcal{P}(\omega)$ is the set of parameters R_{yy} such that the parameters ω and R_{yy} constitute a qubit channel when other parameters are all 0, and $\rho_{R_{yy}}$ is the Choi matrix corresponding to the parameter R_{yy}. Since the range $\mathcal{P}(\omega)$ of the remaining free parameter R_{yy} is a closed interval and $H_\rho(X|E)$ is a convex function (see Lemma 2), the minimization in $F(\omega)$ is achieved at the boundary points of the range of R_{yy} or at the zero point of the derivative of $H_\rho(X|E)$ with respect to R_{yy}.

An *ad hoc* approach to find an estimator is as follows:

(i) By using the statistics of sampled bits and the relation in Eq. (11), Alice and Bob calculate the estimate $\tilde{\omega}$ for the parameters ω.

(ii) If $\mathcal{P}(\tilde{\omega})$ is the empty set, then Alice and Bob find the point $\hat{\omega}$ such that $\hat{\omega}$ is closest (in Euclidean distance) to $\tilde{\omega}$ and $\mathcal{P}(\hat{\omega})$ is not an empty set.[10]

(iii) Alice and Bob calculate an estimator $F(\hat{\omega})$ for Eve's (worst-case) ambiguity $F(\omega)$.

The validity of this estimation procedure can be shown as follows. The estimator $\tilde{\omega}$ converges to the true value ω in probability. The estimator $\hat{\omega}$ also converges to ω, because $\|\hat{\omega}-\tilde{\omega}\|\leq\|\tilde{\omega}-\omega\|$, which implies $\|\hat{\omega}-\omega\|\leq 2\|\tilde{\omega}-\omega\|$ by the triangle inequality. Thus the following lemma, which is proved in Appendix C, guarantees that the estimator $F(\hat{\omega})$ converges to the desired quantity $F(\omega)$ in probability as the number of sampled bits goes to the infinity.

Lemma 1. The function $F(\omega)$ is a continuous function of ω.

[7]This step can be implemented, for example, by the convex optimization [41] because the set of all Choi matrices is a closed convex set. For more detail, see Appendix E.

[8]When we consider a convergence of a density matrix, the convergence is with respect to the trace distance. On the other hand, when we consider a convergence of parameters, we use the Euclidean distance. If estimated parameters converges to the true values, then the resulting matrix also converges to the true one, because the convergence of the Frobenius norm and that of the trace norm are equivalent.

[9]It should be noted that there are some other papers [42–44] that consider the situation in which we have to estimate a channel from partially estimated parameters as above. However, the methods in these papers cannot be used in our problem.

[10]This step can be implemented, for example, by the convex optimization [41] because the set of all $\hat{\omega}$'s such that $\mathcal{P}(\hat{\omega})$ is not empty is a closed convex set. For more detail, see Appendix E.

Although we showed a procedure to exactly estimate Eve's worst-case ambiguity so far, it is worthwhile to show a closed form lower bound on Eve's worst-case ambiguity, which will be proved in Appendix D.

Proposition 2. Let d_z and d_x be the singular values of the matrix

$$\begin{bmatrix} R_{zz} & R_{zx} \\ R_{xz} & R_{xx} \end{bmatrix}. \tag{15}$$

Then, we have

$$F(\omega) \geqslant 1 - h\left(\frac{1+d_z}{2}\right) - h\left(\frac{1+d_x}{2}\right) + h\left(\frac{1+\sqrt{R_{zz}^2+R_{xz}^2}}{2}\right), \tag{16}$$

where $h(\ )$ is the binary entropy function. The equality holds if $t_z=t_x=0$.

Remark 6. For the reverse reconciliation, the worst case of Eve's ambiguity $H_\rho(Y|E)$ is lower bounded by the right-hand side of Eq. (16) in which R_{xz} is replaced by R_{zx}.

Remark 7. The right-hand side of Eq. (16) is further lower bounded by $1-h((1-R_{xx})/2)$. Since $(1-R_{xx})/2$ is equal to the so-called phase error rate P_x [see Eq. (17)], the right-hand side of Eq. (16) is a lower bound on Eve's worst-case ambiguity that is tighter than the well-known bound $1-h(P_x)$ [14].

Remark 8. We described estimation methods for Eve's ambiguity $H_\rho(X|E)$ based on the channel estimation method so-called linear inversion [45] in Sec. III B and in this section. It is well known that the maximum likelihood (ML) channel estimator has smaller estimation error than the linear inversion [45]. An algorithm for ML channel estimation has been proposed [45–47], however, its convergence as a numerical algorithm has not been proved. The absence of a convergence proof prevents us from using that algorithm in the QKD protocols that require a rigorous proof of the convergence of an estimator.

The computation of the ML channel estimate in the six-state protocol is a convex optimization problem. Because the set of Choi matrices is a closed convex set defined by equality constraints and generalized inequality constraints [41] and the log-likelihood function is a concave function of Choi matrices for given measurement outcomes. Therefore, the interior point method [41], for example, can compute the ML estimate with convergence guarantee. For the BB84 protocol, the domain of log-likelihood function is narrowed to real Choi matrices by Proposition 1 that is also a closed convex set, and the parameter R_{yy} remains undetermined as well as the linear inversion because the log-likelihood function is independent of R_{yy}. The rest of the parameters can be computed by a convex optimization algorithm. If we are allowed to use enough computation time for sophisticated channel estimation procedures, then it may be better to use the ML channel estimation.

D. Relation to the conventional estimation procedure

In this section, we show the relation between Eve's ambiguity $H_\rho(X|E)$ that is estimated by our proposed procedures and that is estimated by the conventional procedures.

In the conventional procedure to estimate $H_\rho(X|E)$ in the six-state protocol [14], we first estimate the so-called error rate for each basis as follows:

$$P_z := \frac{\langle 1_z|\mathcal{E}_B(|0_z\rangle\langle 0_z|)|1_z\rangle + \langle 0_z|\mathcal{E}_B(|1_z\rangle\langle 1_z|)|0_z\rangle}{2},$$

$$P_x := \frac{\langle 1_x|\mathcal{E}_B(|0_x\rangle\langle 0_x|)|1_x\rangle + \langle 0_x|\mathcal{E}_B(|1_x\rangle\langle 1_x|)|0_x\rangle}{2},$$

$$P_y := \frac{\langle 1_y|\mathcal{E}_B(|0_y\rangle\langle 0_y|)|1_y\rangle + \langle 0_y|\mathcal{E}_B(|1_y\rangle\langle 1_y|)|0_y\rangle}{2}. \tag{17}$$

Then, we calculate the worst case of Eve's ambiguity $\min H_\rho(X|E)$ in which the minimization is taken over the set of all channels that are compatible with the estimates of the error rates (P_z,P_x,P_y). Since we estimate the actual channel instead of the worst case, Eve's ambiguity estimated by our procedure is at least as large as that estimated by the conventional one.

In the conventional procedure to estimate $H_\rho(X|E)$ in the BB84 protocol, we first estimate P_z and P_x. Then we calculate the worst case of Eve's ambiguity $\min H_\rho(X|E)$ in which the minimization is taken over the set of all channels that are compatible with the estimates of the error rates (P_z,P_x). The minimum is given by the well-known value $1-h(P_x)$ [14]. Since the error rates (P_z,P_x) are a degraded version of the parameters ω, the range of minimization in the conventional procedure is larger than $\mathcal{P}(\omega)$ in our proposed procedure. Thus, Eve's worst-case ambiguity estimated by our proposed procedure is at least as large as that estimated by the conventional one.

For both the six-state protocol and the BB84 protocol, a sufficient condition such that Eve's worst-case ambiguity estimated by our proposed procedure and that estimated by the conventional one coincide is that the channel $\mathcal{E}_B$ is a Pauli channel. However, it is not clear whether the condition is also a necessary condition or not.

Combining the arguments in this section and Remark 1, we find that our proposed classical processing yields at least as high a key rate as the standard processing by Shor and Preskill [18] for the QKD protocols.

IV. EXAMPLES

In this section, we calculate the key rates of the BB84 protocol and the six-state protocol with our proposed classical processing for the amplitude damping channel, the unital channel, and the rotation channel, and clarify that the key rate of our proposed classical processing is higher than previously known ones.

A. Amplitude damping channel

In the Stokes parametrization, the amplitude damping channel $\mathcal{E}_p$ is given by the affine map

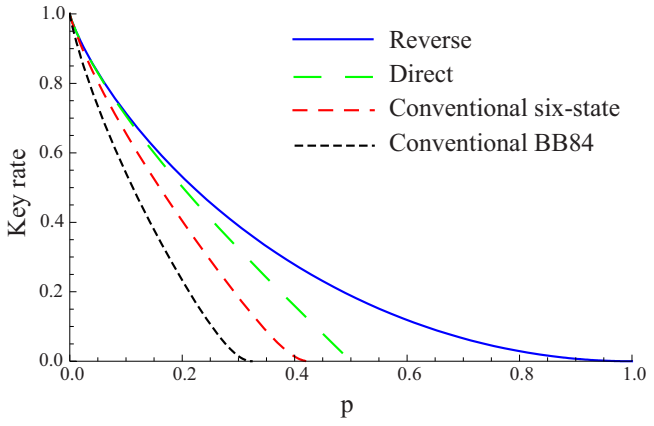

FIG. 1. (Color online) Comparison of the key rates against the parameter p of the amplitude damping channel (see Eq. (18)). "Reverse" and "Direct" are the key rates when we use the reverse reconciliation and the direct reconciliation in our proposed classical processing respectively. "Conventional six-state" and "Conventional BB84" are the key rates of the six-state protocol and the BB84 protocol with the conventional classical processing. Note that the conventional classical processing involves the noisy preprocessing [14,16].

$$\begin{bmatrix} \theta_z \\ \theta_x \\ \theta_y \end{bmatrix} \mapsto \begin{bmatrix} 1-p & 0 & 0 \\ 0 & \sqrt{1-p} & 0 \\ 0 & 0 & \sqrt{1-p} \end{bmatrix} \begin{bmatrix} \theta_z \\ \theta_x \\ \theta_y \end{bmatrix} + \begin{bmatrix} p \\ 0 \\ 0 \end{bmatrix} \tag{18}$$

parametrized by a real parameter $0 \leqslant p \leqslant 1$.

We first calculate the key rate for the BB84 protocol. In the BB84 protocol, we can estimate the parameters $R_{zz}=1-p$, $R_{zx}=0$, $R_{xz}=0$, $R_{xx}=\sqrt{1-p}$, $t_z=p$, and $t_x=0$. By Proposition 1, we can set $R_{zy}=R_{xy}=R_{yz}=R_{yx}=t_y=0$. Furthermore, by the condition on the TPCP map [39]

$$(R_{xx}-R_{yy})^2 \leqslant (1-R_{zz})^2 - t_z^2,$$

we can decide the remaining parameter as $R_{yy}=\sqrt{1-p}$. Thus, Eve's (worst-case) ambiguity $F(\omega)$ for the BB84 protocol coincides with the true value $H_\rho(X|E)$, which means that the BB84 protocol can achieve the same key rate as the six-state protocol.

By straightforward calculations, the key rates of the direct reconciliation and reverse reconciliation are calculated as

$$1+\frac{1}{2}h(p)-h\left(\frac{p}{2}\right)-\frac{1+p}{2}h\left(\frac{1}{1+p}\right),$$

and

$$h\left(\frac{1+p}{2}\right)+\frac{1+p}{2}h\left(\frac{1}{1+p}\right)-h\left(\frac{1}{2}\right)-\frac{1}{2}h(p),$$

respectively. These key rates are plotted in Fig. 1.

The Bell diagonal entries of the Choi matrix $(\mathrm{id}\otimes\mathcal{E}_p)(\psi)$ are $\frac{1}{4}(2+2\sqrt{1-p}-p)$, $\frac{1}{4}p$, $\frac{1}{4}(2-2\sqrt{1-p}-p)$, and $\frac{1}{4}p$. The key rate of the six-state protocol and the BB84 protocol with the conventional processing can be calculated only from the Bell diagonal entries, and are also plotted in Fig. 1.

We find that the key rates of our proposed classical processing are higher than those of the conventional processing. Furthermore, we find that the key rate of the reverse reconciliation is higher than that of the direct reconciliation.

Remark 9. When the channel is degradable [48], i.e., there exists a channel $\mathcal{D}$ such that $\mathcal{E}_E(\rho)=\mathcal{D}\circ\mathcal{E}_B(\rho)$ for any input ρ, the quantum wire-tap channel capacity [49] is known to be achievable without any auxiliary random variable [50,61].

For the one-way key agreement from a degradable (from Alice to Bob and Eve) $\{ccq\}$ state, which is a state $\rho_{XYE}=\Sigma_{x,y}P_{XY}(x,y)|x\rangle\langle x|\otimes|y\rangle\langle y|\otimes\rho_E^{x,y}$ such that there exist states $\{\hat{\rho}_E^y\}_y$ satisfying $\Sigma_y P_{Y|X}(y|x)\hat{\rho}_E^y=\rho_E^x:=\Sigma_y P_{Y|X}(y|x)\rho_E^{x,y}$, a similar statement also holds, namely, the key rate in Eq. (4) cannot be improved with any auxiliary random variable. The use of auxiliary random variable for the key agreement corresponds to the noisy preprocessing [14,16].

The above statement is proved as follows. Since we are considering the information reconciliation and the privacy amplification with one-way classical communication, key rates only depend on distribution P_{XY} and $\{cq\}$ state ρ_{XE}. Thus the maximum key rate for ρ_{XYE} is equal to that for a degraded version of it, $\hat{\rho}_{XYE}:=\Sigma_{x,y}P_{XY}(x,y)|x\rangle\langle x|\otimes|y\rangle\langle y|\otimes\hat{\rho}_E^y$. On the other hand the (quantum) intrinsic information

$$I_\rho(X;Y\downarrow E) := \inf I_\rho(X;Y|E')$$

is an upper bound on the maximum key rate [51], where $I_\rho(X;Y|E):=H_\rho(XE)+H_\rho(YE)-H_\rho(XYE)-H_\rho(E)$ is the quantum conditional mutual information, and the infimum is taken over all $\{ccq\}$ states $\rho_{XYE'}=(\mathrm{id}\otimes\mathcal{N}_{E\to E'})(\rho_{XYE})$ for CPTP maps $\mathcal{N}_{E\to E'}$ from system E to E'. Taking the identity map id_E, the quantum conditional mutual information $I_\rho(X;Y|E)$ itself is an upper bound on the maximum key rate. Applying this fact for the degraded $\{ccq\}$ state, $\hat{\rho}_{XYE}$, the maximum key rate is upper bounded by

$$\begin{aligned} I_{\hat{\rho}}(X;Y|E) &= I_{\hat{\rho}}(X;YE) - I_{\hat{\rho}}(X;E) \\ &= H_{\hat{\rho}}(X|E) - H(X|Y) + I_{\hat{\rho}}(X;E|Y) \\ &= H_\rho(X|E) - H(X|Y), \end{aligned}$$

which is the desired upper bound, and is equal to Eq. (4).

When Alice randomly sends $\{|0_z\rangle,|1_z\rangle\}$ over the amplitude damping channel and Bob measures the received state by σ_z observable, the resulting $\{ccq\}$ state is degradable,[11] which implies the key rate of direct reconciliation cannot be improved by the noisy preprocessing. It is not clear whether the $\{ccq\}$ state for the amplitude damping channel is degradable in reverse order; there exists a possibility to improve the key rate of reverse reconciliation by the noisy preprocessing.

B. Unital channel and rotation channel

A channel $\mathcal{E}_B$ is called a unital channel if the vector (t_z,t_x,t_y) is the zero vector in the Stokes parametrization [see Eq. (10)], or equivalently if the channel $\mathcal{E}_B$ maps the completely mixed state $I/2$ to itself. The unital channel has the

[11]The fact that the amplitude damping channel is degradable has been shown in [52].

following physical meaning in QKD protocols. When Eve conducts the Pauli cloning [53] with respect to an orthonormal basis that is a rotated version of $\{|0_z\rangle,|1_z\rangle\}$, the quantum channel from Alice to Bob is not a Pauli channel but a unital channel. It is natural to assume that Eve cannot determine the direction of the basis $\{|0_z\rangle,|1_z\rangle\}$ accurately, and the unital channel deserves consideration in the QKD research as well as the Pauli channel.

By the singular value decomposition, we can decompose the matrix R in Eq. (10) as

$$O_2\begin{bmatrix} e_z & 0 & 0 \\ 0 & e_x & 0 \\ 0 & 0 & e_y \end{bmatrix}O_1, \tag{19}$$

where O_1 and O_2 are some rotation matrices,[12] and $|e_z|$, $|e_x|$, and $|e_y|$ are the singular value of the matrix R.[13] Thus, we can consider the unital channel $\mathcal{E}_B$ as the composition of the unitary channel $\mathcal{E}_{O_1}$, the Pauli channel

$$\varrho \mapsto q_i\varrho + q_z\sigma_z\varrho\sigma_z + q_x\sigma_x\varrho\sigma_x + q_y\sigma_y\varrho\sigma_y,$$

and the unitary channel $\mathcal{E}_{O_2}$ [54], where

$$q_i = \frac{1+e_z+e_x+e_y}{4},$$

$$q_z = \frac{1+e_z-e_x-e_y}{4},$$

$$q_x = \frac{1-e_z+e_x-e_y}{4},$$

$$q_y = \frac{1-e_z-e_x+e_y}{4}.$$

For the unital channel, we have $H(X|Y)=H(Y|X)=h((1+R_{zz})/2)$. For the six-state protocol, we can calculate Eve's ambiguity $H_\rho(X|E)$ as

$$1 - H[q_i,q_z,q_x,q_y] + h\left(\frac{1+\sqrt{R_{zz}^2+R_{xz}^2+R_{yz}^2}}{2}\right) \tag{20}$$

because (q_i,q_z,q_x,q_y) are the eigenvalues of the Choi matrix ρ_{AB}. For the reverse reconciliation, Eve's ambiguity $H_\rho(Y|E)$ is given by Eq. (20) in which R_{xz} and R_{yz} are replaced by R_{zx} and R_{zy} respectively. Thus, $R_{xz}^2+R_{yz}^2=R_{zx}^2+R_{zy}^2$ is the necessary and sufficient condition for $H_\rho(X|E)=H_\rho(Y|E)$. For the BB84 protocol, we can calculate Eve's worst case ambiguity $F(\omega)$ by Proposition 2 because $t_z=t_x=0$ for the unital channel. Note that the singular values (d_z,d_x) in Proposition 2 are different from the singular values $(|e_z|,|e_x|)$ in general because there exist off-diagonal elements $(R_{zy},R_{xy},R_{yz},R_{yx})$.

From Remark 6, $R_{xz}^2=R_{zx}^2$ is the necessary and sufficient condition for that Eve's worst-case ambiguity for the direct reconciliation and that for the reverse reconciliation coincide.

In the rest of this section, we analyze a special class of the unital channel, the rotation channel. We define the rotation channel from Alice to Bob as

$$\begin{bmatrix} \theta_z \\ \theta_x \\ \theta_y \end{bmatrix} \mapsto \begin{bmatrix} \cos\vartheta & -\sin\vartheta & 0 \\ \sin\vartheta & \cos\vartheta & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \theta_z \\ \theta_x \\ \theta_y \end{bmatrix}.$$

The rotation channels occur, for example, when the directions of the transmitter and the receiver are not properly aligned.

For the rotation channel, Eq. (16) gives $F(\omega)=1$, which implies that Eve gained no information. Thus, Eve's (worst-case) ambiguity for the BB84 protocol coincides with the true value $H_\rho(X|E)$, and the BB84 protocol with our proposed classical processing can achieve the same key rate as the six-state protocol.

There are two reasons why we show this example—the rotation channel. The first one is that we can obtain secret keys, in the BB84 protocol, both from matched measurement outcomes, which are transmitted and received by the same basis (say z basis), and mismatched measurement outcomes, which are transmitted and received by different bases (say z basis and x basis respectively). The probability distributions of Alice and Bob's bit for each case are given by $P_{X|Y}(1|0)=P_{X|Y}(0|1)=\sin^2(\vartheta/2)$ and $P_{X|Y'}(1|0)=P_{X|Y'}(0|1)=\sin^2(\vartheta/2-\pi/4)$, respectively [see Eqs. (1) and (7) for the definitions of P_{XY} and $P_{XY'}$]. If the channel is biased, i.e., $\vartheta\neq 0,\pi/2,\pi,3\pi/2$, then we can obtain secret keys with positive key rates both from matched measurement outcomes and mismatched measurement outcomes. This fact solves an open problem discussed in [Ref. [22], Sec. V].

The second reason is that we can obtain a secret key from matched measurement outcomes even though the so-called error rate is higher than the 25% limit [23] in the BB84 protocol. The Bell diagonal entries of the Choi matrix ρ_ϑ are $\cos^2(\vartheta/2)$, 0, 0, and $\sin^2(\vartheta/2)$. Thus the error rate is $\sin^2(\vartheta/2)$. For $\pi/3\leqslant\vartheta\leqslant 5\pi/3$, the error rate is higher than 25%, but we can obtain the positive key rate, $1-h(\sin^2(\vartheta/2))$ except $\vartheta=\pi/2,3\pi/2$. Note that the key rate of the standard processing by Shor and Preskill [18] is $1-2h(\sin^2(\vartheta/2))$. This fact verifies Curty *et al.*'s suggestion [24] that key agreement might be possible even for the error rates higher than 25% limits.

Remark 10. If the $\{ccq\}$ state ρ_{XYE} is degraded (from Alice to Bob and Eve), i.e., the $\{ccq\}$ state is of the form $\rho_{XYE}=\Sigma_{x,y}P_{XY}(x,y)|x\rangle\langle x|\otimes|y\rangle\langle y|\otimes\rho_E^{xy}$, then we can prove that the key rate in Eq. (4) cannot be improved even if we use any noisy preprocessing or two-way processing. The reason is that the upper bound $I_\rho(X;Y|E)$ and the lower bound in Eq. (4) coincide for the degraded $\{ccq\}$ state in a similar manner to Remark 9. For the rotation channel $\mathcal{E}_\vartheta$, the resulting $\{ccq\}$ state is obviously degraded. Thus the key rate $1-h(\sin^2(\vartheta/2))$ cannot be improved anymore.

[12]The rotation matrix is the real orthogonal matrix with determinant 1.

[13]The decomposition is not unique because we can change the order of (e_z,e_x,e_y) or the sign of them by adjusting the rotation matrices O_1 and O_2. However, the result in this paper does not depend on a choice of the decomposition.

V. CONCLUSION

In this paper, we constructed a practically implementable classical processing for the BB84 protocol and the six-state protocol that fully utilizes the accurate channel estimation method. A consequence of our result is that we should not discard mismatched measurement outcomes in the QKD protocols; those measurement outcomes can be used to estimate the channel accurately, and increase key rates.

There is a problem that was not treated in this paper. Although we only treated the asymptotically secure key rate in this paper, the final goal is the nonasymptotic analysis of eavesdropper's information, i.e., evaluate eavesdropper's information as a function of the length of the raw key, the key rate, and the length of sample bits as in the literature [15,34,54–60]. This topic is a future research agenda.

ACKNOWLEDGMENTS

We would like to thank Dr. Jean-Christian Boileau, Professor Akio Fujiwara, Dr. Manabu Hagiwara, Dr. Kentaro Imafuku, Professor Hideki Imai, Professor Hoi-Kwong Lo and members of his group, Professor Masahito Hayashi, Dr. Takayuki Miyadera, Professor Hiroshi Nagaoka, Professor Renato Renner and members of his group, Mr. Yutaka Shikano, Professor Tadashi Wadayama, Professor Stefan Wolf and members of his group, and Professor Isao Yamada for valuable discussions and comments. We are grateful to one of the referees for informing us of Ref. [11], and to the other for pointing out an error during the review process. This research was partly supported by the Japan Society for the Promotion of Science under Grants-in-Aid No. 18760266 and No. 00197137.

APPENDIX A: CONVEXITY OF EVE'S AMBIGUITY

In this Appendix, we show a lemma that will be used in the rest of the appendices.

Lemma 2. For two channels $\mathcal{E}_B^1$ and $\mathcal{E}_B^2$, and a probabilistically mixed channel $\mathcal{E}_B' := \lambda\mathcal{E}_B^1 + (1-\lambda)\mathcal{E}_B^2$, Eve's ambiguity is convex, i.e., we have

$$H_{\rho'}(X|E) \leqslant \lambda H_{\rho^1}(X|E) + (1-\lambda)H_{\rho^2}(X|E),$$

where $\rho_{XE}' := \sum_{x\in\mathbb{F}_2}\frac{1}{2}|x\rangle\langle x| \otimes \mathcal{E}_E'(|x\rangle\langle x|)$ for channel $\mathcal{E}_E'$ to all the environment of $\mathcal{E}_B'$, and $\rho_{XE}^r := \sum_{x\in\mathbb{F}_2}\frac{1}{2}|x\rangle\langle x| \otimes \mathcal{E}_E^r(|x\rangle\langle x|)$ for channel $\mathcal{E}_E^r$ to all the environment of $\mathcal{E}_B^r$ and for $r \in \{1,2\}$.

Proof. For $r=1$ and 2, let ψ_{ABE}^r be a purification of the Choi matrix $\rho_{AB}^r := (\mathrm{id}\otimes\mathcal{E}_B^r)(\psi)$. Then the density matrix ρ_{XE}^r is derived by Alice's measurement by z basis and the partial trace over Bob's system, i.e.,

$$\rho_{XE}^r = \mathrm{Tr}_B\left[\sum_x (|x\rangle\langle x| \otimes I)\psi_{ABE}^r(|x\rangle\langle x| \otimes I)\right]. \quad \text{(A1)}$$

Let

$$|\psi_{ABER}'\rangle := \sqrt{\lambda}|\psi_{ABE}^1\rangle|1\rangle + \sqrt{1-\lambda}|\psi_{ABE}^2\rangle|2\rangle$$

be a purification of $\rho_{AB}' := (\mathrm{id}\otimes\mathcal{E}_B')(\psi)$, where $\mathcal{H}_R$ is the reference system, and $\{|1\rangle,|2\rangle\}$ is an orthonormal basis of $\mathcal{H}_R$. Let

$$\rho_{XER}' := \mathrm{Tr}_B\left[\sum_x (|x\rangle\langle x| \otimes I)\psi_{ABER}'(|x\rangle\langle x| \otimes I)\right], \quad \text{(A2)}$$

and let

$$\rho_{XER}^* := \sum_{r\in\{1,2\}} (I\otimes|r\rangle\langle r|)\rho_{XER}'(I\otimes|r\rangle\langle r|)$$
$$= \lambda\rho_{XE}^1 \otimes |1\rangle\langle 1| + (1-\lambda)\rho_{XE}^2 \otimes |2\rangle\langle 2|$$

be the density matrix such that the system $\mathcal{H}_R$ is measured by the $\{|1\rangle,|2\rangle\}$ basis. Then we have

$$H_{\rho'}(X|ER) = H(X) - I_{\rho'}(X;ER) \leqslant H(X) - I_{\rho^*}(X;ER)$$
$$= H_{\rho^*}(X|ER) = \lambda H_{\rho^1}(X|E) + (1-\lambda)H_{\rho^2}(X|E),$$

where the inequality follows from the monotonicity of the quantum mutual information for measurements (data processing inequality) [61]. By renaming the systems ER to E, we have the assertion of the lemma. ■

Remark 11. By switching the role of Alice and Bob, we can show that the assertion in Lemma 2 and thus Proposition 1 hold for the reverse reconciliation. Furthermore, the statements also hold for the information reconciliation and the privacy amplification with k-blockwise two-way processing [23,28] (including one-way noisy preprocessing [14,16]). More precisely, let $\mathcal{N}_{X^kY^k\to UV}$ be the TPCP map that represents a two-way processing. Then for the density matrix

$$\rho_{UVE^k} := (\mathcal{N}_{X^kY^k\to UV}\otimes \mathrm{id}_{E^k})(\rho_{XYE}^{\otimes k}),$$

we can obtain the inequality

$$H_{\rho'}(U|VE^k) \leqslant \lambda H_{\rho^1}(U|VE^k) + (1-\lambda)H_{\rho^2}(U|VE^k).$$

The modifications of the proof are to replace ψ_{ABE}' and ψ_{ABER}' with $(\psi_{ABE}')^{\otimes k}$ and $(\psi_{ABER}')^{\otimes k}$ in Eqs. (A1) and (A2), to replace the partial trace over Bob's system with Bob's measurement, to append a map $\mathcal{N}_{X^kY^k\to UV}$, and to replace the measurement on the system $\mathcal{H}_R$ with the measurements on $\mathcal{H}_R^{\otimes k}$.

APPENDIX B: PROOF OF PROPOSITION 1

The statement of Proposition 1 easily follows from Lemma 2. For any channel $\mathcal{E}_B$, let $\bar{\mathcal{E}}_B$ be the channel whose Choi matrix is the complex conjugate of that for $\mathcal{E}_B$. Note that eigenvalues of density matrices are unchanged by the complex conjugate, and thus Eve's ambiguity $H_{\bar{\rho}}(X|E)$ for $\bar{\mathcal{E}}_B$ is equal to $H_\rho(X|E)$. By applying Lemma 2 for $\mathcal{E}_B^1=\mathcal{E}_B$, $\mathcal{E}_B^2=\bar{\mathcal{E}}_B$, and $\lambda=\frac{1}{2}$, we have

$$H_{\rho'}(X|E) \leqslant \frac{1}{2}H_\rho(X|E) + \frac{1}{2}H_{\bar{\rho}}(X|E),$$

where $\rho_{AB}' = \frac{1}{2}\rho_{AB} + \frac{1}{2}\bar{\rho}_{AB}$. Note that ρ_{AB}' is a real density matrix whose entries are equal to the real components of ρ_{AB}, which implies that the parameters R_{zy}, R_{xy}, R_{yz}, R_{yx}, and t_{y}, are 0 by Eq. (12). Since the channel $\mathcal{E}_B$ was arbitrary, we have the assertion of the proposition. ■

APPENDIX C: PROOF OF LEMMA 1

Since the conditional entropy is a continuous function, the following statement will suffice for proving that $F(\omega)$ is a continuous function at any $\omega_0 \in \mathcal{P}$, where $\mathcal{P}$ is the set of all ω such that $\mathcal{P}(\omega)$ is not empty. For any $\omega \in \mathcal{P}$ such that $\|\omega - \omega_0\| \leqslant \varepsilon$, there exist $\varepsilon', \varepsilon'' > 0$ such that

$$\mathcal{P}(\omega) \subset \mathcal{B}_{\varepsilon'}(\mathcal{P}(\omega_0)), \tag{C1}$$

$$\mathcal{P}(\omega_0) \subset \mathcal{B}_{\varepsilon''}(\mathcal{P}(\omega)), \tag{C2}$$

and ε' and ε'' converge to 0 as ε goes to 0, where $\mathcal{B}_{\varepsilon'}(\mathcal{P}(\omega_0))$ is the ε' neighbor of the set $\mathcal{P}(\omega_0)$.

Define the set $\mathcal{Q} := \{(\omega, R_{yy}) \mid \omega \in \mathcal{P}, R_{yy} \in \mathcal{P}(\omega)\}$, which is a closed convex set. Define functions

$$U(\omega) := \max_{R_{yy} \in \mathcal{P}(\omega)} R_{yy},$$

$$L(\omega) := \min_{R_{yy} \in \mathcal{P}(\omega)} R_{yy}$$

as the upper surface and the lower surface of the set $\mathcal{Q}$, respectively. Then $U(\omega)$ and $L(\omega)$ are concave and convex functions, respectively, because $\mathcal{Q}$ is a convex set. Thus $U(\omega)$ and $L(\omega)$ are continuous functions except the extreme points of $\mathcal{P}$. For any extreme point ω' and for any interior point ω, we have $U(\omega) \geqslant U(\omega')$ and $L(\omega) \leqslant L(\omega')$, because $\mathcal{Q}$ is a convex set. Since $\mathcal{Q}$ is a closed set, we have $\lim_{\omega \to \omega'} U(\omega) \in \mathcal{P}(\omega')$ and $\lim_{\omega \to \omega'} L(\omega) \in \mathcal{P}(\omega')$, which implies that $U(\omega') = \lim_{\omega \to \omega'} U(\omega)$ and $L(\omega') = \lim_{\omega \to \omega'} L(\omega)$. Thus $U(\omega)$ and $L(\omega)$ are also continuous at the extreme points. Since $\mathcal{P}(\omega)$ is a convex set, the continuity of $U(\omega)$ and $L(\omega)$ implies that Eqs. (C1) and (C2) hold for some $\varepsilon', \varepsilon'' > 0$, and ε' and ε'' converge to 0 as ε goes to 0. ■

APPENDIX D: PROOF OF PROPOSITION 2

By Proposition 1, it suffices to consider the channel $\mathcal{E}_B$ of the form

$$\begin{bmatrix} \theta_z \\ \theta_x \\ \theta_y \end{bmatrix} \mapsto \begin{bmatrix} R_{zz} & R_{zx} & 0 \\ R_{xz} & R_{xx} & 0 \\ 0 & 0 & R_{yy} \end{bmatrix} \begin{bmatrix} \theta_z \\ \theta_x \\ \theta_y \end{bmatrix} + \begin{bmatrix} t_z \\ t_x \\ 0 \end{bmatrix}.$$

Define the channel $\mathcal{E}_B^-(\varrho) := \sigma_y[\mathcal{E}_B(\sigma_y \varrho \sigma_y)]\sigma_y$ and the mixed channel $\mathcal{E}_B' := \frac{1}{2}\mathcal{E}_B + \frac{1}{2}\mathcal{E}_B^-$. Since the channel $\mathcal{E}_B^-$ is given by

$$\begin{bmatrix} \theta_z \\ \theta_x \\ \theta_y \end{bmatrix} \mapsto \begin{bmatrix} R_{zz} & R_{zx} & 0 \\ R_{xz} & R_{xx} & 0 \\ 0 & 0 & R_{yy} \end{bmatrix} \begin{bmatrix} \theta_z \\ \theta_x \\ \theta_y \end{bmatrix} + \begin{bmatrix} -t_z \\ -t_x \\ 0 \end{bmatrix},$$

$\mathcal{E}_B'$ is a unital channel and the matrix part of $\mathcal{E}_B$ and $\mathcal{E}_B'$ are the same. Furthermore, since $H_\rho(X|E)$ for $\mathcal{E}_B$ is equal to $H_{\rho^-}(X|E)$ for $\mathcal{E}_B^-$, by using Lemma 2, we have

$$H_\rho(X|E) \geqslant H_{\rho'}(X|E).$$

The rest of the proof is to calculate the minimization of $H_{\rho'}(X|E)$ with respect to R_{yy}. By the singular value decomposition, we can decompose the matrix R' corresponding to the channel $\mathcal{E}_B'$ as

$$O_2 \begin{bmatrix} \tilde{d}_z & 0 & 0 \\ 0 & \tilde{d}_x & 0 \\ 0 & 0 & R_{yy} \end{bmatrix} O_1,$$

where O_1 and O_2 are some rotation matrices within the z-x plane, and $|\tilde{d}_z|$ and $|\tilde{d}_x|$ are the singular value of the matrix in Eq. (15). Then, we have

$$\begin{aligned} \min_{R_{yy}} H_{\rho'}(X|E) &= \min_{R_{yy}} \left[1 - H(\rho_{AB}') + \sum_{x \in \mathbb{F}_2} \frac{1}{2} H(\mathcal{E}_B'(|x\rangle\langle x|)) \right] \\ &= 1 - \max_{R_{yy}} H[q_i, q_z, q_x, q_y] + h\left(\frac{1 + \sqrt{R_{zz}^2 + R_{xz}^2}}{2} \right) \\ &= 1 - h(q_i + q_z) - h(q_i + q_x) \\ &\quad + h\left(\frac{1 + \sqrt{R_{zz}^2 + R_{xz}^2}}{2} \right), \end{aligned}$$

where (q_i, q_z, q_x, q_y) are the eigenvalues of the Choi matrix ρ_{AB}'. By noting that $q_i + q_z = \frac{1+\tilde{d}_z}{2}$ and $q_i + q_x = \frac{1+\tilde{d}_x}{2}$ (see Sec. IV B), we have assertion of the proposition. ■

APPENDIX E: CONVEX OPTIMIZATION

In this appendix, we briefly explain how to apply a convex optimization method, the interior-point method, to the channel estimation in the BB84 protocol. In a similar manner, we can apply the interior-point method to the channel estimation in the six-state protocol. For more details, see the textbook [[41], Sec. 11.6].

First, we define a generalized inequality. Since the set $K \subset \mathbb{R}^{4\times 4}$ of (real) semidefinite matrices is a proper cone (see [41, Sec. 2.4.1] for the definition of the proper cone), we can define a generalized inequality $\leqslant_K$ as

$$M \leqslant_K N \Leftrightarrow N - M \in K.$$

For a given parameter $(\omega, R_{yy}) \in \mathbb{R}^7$, we define the real matrix $\rho(\omega, R_{yy}) \in \mathbb{R}^{4\times 4}$ by using the relation in Eq. (12), where we set other parameters $(R_{zy}, R_{xy}, R_{yz}, R_{yx}, t_y)$ to be all 0. Then, the function $\rho: \mathbb{R}^7 \to \mathbb{R}^{4\times 4}$ is a K-concave function (see [[41], Sec. 3.6.2] for the definition of the K-concave function).

We can formulate our optimization problem as follows:

$$\begin{aligned} \text{minimize} \quad & \|\hat{\omega} - \tilde{\omega}\|^2 \\ \text{subject to} \quad & \rho(\hat{\omega}, R_{yy}) \geqslant_K 0, \\ & \mathrm{Tr}_B[\rho(\hat{\omega}, R_{yy})] = I, \end{aligned}$$

where $\| \|^2$ is the square Euclidean norm, which is a convex function, and I is the 2×2 identity matrix. This optimization problem can be solved by the interior-point method. Note that we can use $\log\det \rho(\hat{\omega}, R_{yy})$ as a logarithmic barrier function (see [[41], Example 11.7]).

[1] G. Brassard and L. Salvail, in *Advances of Cryptology—EUROCRYPT '93*, edited by T. Helleseth, Lecture Notes in Computer Science, Vol. 765 (Lofthus, Norway, 1994), pp. 410–423.
[2] C. H. Bennett, G. Brassard, and J. M. Robert, SIAM J. Comput. **17**, 210 (1988).
[3] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[4] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing* (Bangalore, India, 1984), pp. 175–179.
[5] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[7] I. L. Chuang and M. A. Nielsen, J. Mod. Opt. **44**, 2455 (1997).
[8] J. F. Poyatos, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **78**, 390 (1997).
[9] S. M. Barnett, B. Huttner, and S. J. D. Phoenix, J. Mod. Opt. **40**, 2501 (1993).
[10] D. Bruß, M. Christandl, A. Ekert, B. G. Englert, D. Kaszlikowski, and C. Macchiavello, Phys. Rev. Lett. **91**, 097901 (2003).
[11] Y. C. Liang, D. Kaszlikowski, B. G. Englert, L. C. Kwek, and C. H. Oh, Phys. Rev. A **68**, 022324 (2003).
[12] D. Kaszlikowski, J. Y. Lim, D. K. L. Oi, F. H. Willeboordse, A. Gopinathan, and L. C. Kwek, Phys. Rev. A **71**, 012309 (2005).
[13] D. Kaszlikowski, J. Y. Lim, L. C. Kwek, and B. G. Englert, Phys. Rev. A **72**, 042315 (2005).
[14] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[15] R. Renner, Ph.D thesis, Dipl. Phys. ETH, Switzerland (2005).
[16] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[17] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[18] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[19] U. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[20] J. C. Boileau, J. Batuwantudawe, and R. Laflamme, Phys. Rev. A **72**, 032321 (2005).
[21] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).
[22] R. Matsumoto and S. Watanabe, IEICE Trans. Fundamentals **E91-A**, 2870 (2008).
[23] D. Gottesman and H. K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[24] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[25] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2004).
[26] D. Slepian and J. K. Wolf, IEEE Trans. Inf. Theory **19**, 471 (1973).
[27] R. G. Gallager, *Low Density Parity Check Codes* (M.I.T. Press, Cambridge, MA, 1963).
[28] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, Phys. Rev. A **76**, 032312 (2007).
[29] J. Muramatsu, IEICE Trans. Fundamentals **E89-A**, 2036 (2006).
[30] R. Renner, Nat. Phys. **3**, 645 (2007).
[31] J. L. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).
[32] J. Muramatsu, T. Uyematsu, and T. Wadayama, IEEE Trans. Inf. Theory **51**, 3645 (2005).
[33] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (John Wiley & Sons, New York, 2006).
[34] D. Mayers, J. ACM **48**, 351 (2001).
[35] D. J. C. MacKay, *Information Theory, Inference, and Learning Algorithms* (Cambridge University Press, Cambridge, MA, 2003).
[36] A. D. Liveris, Z. Xiong, and C. N. Georghiades, IEEE Commun. Lett. **6**, 440 (2002).
[37] T. P. Coleman, A. H. Lee, M. Médard, and M. Effros, IEEE Trans. Inf. Theory **52**, 3546 (2006).
[38] A. Fujiwara and H. Nagaoka, IEEE Trans. Inf. Theory **44**, 1071 (1998).
[39] A. Fujiwara and P. Algoet, Phys. Rev. A **59**, 3290 (1999).
[40] M. D. Choi, Linear Algebr. Appl. **10**, 285 (1975).
[41] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, MA, 2004); URL http://www.stanford.edu/boyd/cvxbook/.
[42] M. Ziman, M. Plesch, and V. Bužek, Eur. Phys. J. D **32**, 215 (2005).
[43] M. Ziman, M. Plesch, and V. Bužek, Found. Phys. **36**, 127 (2006).
[44] M. Ziman, Phys. Rev. A **78**, 032118 (2008).
[45] Z. Hradil, J. Řeháăek, and J. Fiurášek, in *Quantum State Estimation*, edited by M. Paris and J. Řeháăek, Lecture Notes in Physics, Vol. 649 (Springer, New York, 2004), pp. 59–112.
[46] J. Fiurášek and Z. Hradil, Phys. Rev. A **63**, 020101(R) (2001).
[47] M. Ježek, J. Fiurášek, and Z. Hradil, Phys. Rev. A **68**, 012305 (2003).
[48] I. Devetak and P. W. Shor, Commun. Math. Phys. **256**, 287 (2005).
[49] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[50] G. Smith, Phys. Rev. A **78**, 022306 (2008).
[51] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, in *Proceedings of the 4th Theory of Cryptography Conference*, edited by S. P. Vadhan, Lecture Notes in Computer Science, Vol. 4392 (Amsterdam, The Netherlands, 2007), pp. 456–478.
[52] V. Giovannetti and R. Fazio, Phys. Rev. A **71**, 032314 (2005).
[53] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[54] P. S. Bourdon and H. T. Williams, Phys. Rev. A **69**, 022314 (2004).
[55] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, J. Cryptology **19**, 381 (2006).
[56] S. Watanabe, R. Matsumoto, and T. Uyematsu, e-print id arXiv:quant-ph/0412070.
[57] M. Hayashi, Phys. Rev. A **74**, 022307 (2006).
[58] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[59] V. Scarani and R. Renner, e-print arXiv:0806.0120.
[60] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß, Phys. Rev. A **74**, 042340 (2006).
[61] M. Hayashi, *Quantum Information: An Introduction* (Springer, New York, 2006).