Key rate of quantum key distribution with hashed two-way classical communication

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

Yasuhito Kawano§
NTT Communication Science Laboratories, NTT Corporation, 3-1, Wakamiya, Morinosato, Atsugishi, Kanagawa Prefecture, 243-0198, Japan

(Received 3 June 2007; published 12 September 2007)

We propose an information reconciliation protocol that uses two-way classical communication. The key rates of quantum key distribution (QKD) protocols that use our protocol are higher than those using previously known protocols for a wide range of error rates for the Bennett-Brassard 1984 and six-state protocols. We also clarify the relation between the proposed and known QKD protocols, and the relation between the proposed protocol and entanglement distillation protocols.

DOI: 10.1103/PhysRevA.76.032312 PACS number(s): 03.67.Dd, 89.70.+c

I. INTRODUCTION

Quantum key distribution (QKD) protocols provide a way for two parties, a sender, Alice, and a receiver, Bob, to share an unconditionally secure key in the presence of an eavesdropper, Eve. Unlike conventional schemes of key distribution that rely on unproven computational assumptions, the security of QKD protocols is guaranteed by the principles of quantum mechanics.

QKD protocols usually consist of two parts, a quantum and a classical part. Alice sends a binary sequence to Bob in the quantum part by encoding it into quantum states that are randomly chosen from a set of nonorthogonal states. Since unknown nonorthogonal states cannot be cloned perfectly, any eavesdropping attempt by Eve will disturb the transmitted quantum states. Thus, by estimating the error rate of the transmitted quantum states, Alice and Bob can estimate the amount of information that Eve has gained. For the sequence that remains after the error estimation phase, which is usually called the raw key, Alice and Bob first carry out an information reconciliation (IR) protocol [1,2] to share the same bit sequence. Alice and Bob then distill the final secure key by conducting a privacy amplification (PA) protocol [2,3].

The best-known QKD protocols are the Bennett-Brassard 1984 (BB84) protocol [4] and the six-state protocol [5]. The unconditional security of the BB84 protocol has been proved [6–8]. Shor and Preskill [9] presented a simple proof of the BB84 protocol by showing that the QKD protocol that uses the entanglement distillation protocol (EDP) [10,11] can be converted into the BB84 protocol. After that, the unconditional security of the six-state protocol was proved [12] using the same technique as in [9]. Recently, the security of generic QKD protocols that include the BB84 protocol and the six-state protocol has been proved [13–15], based on information-theoretical techniques instead of Shor and Preskill's technique.

In addition to the security of QKD protocols, the key rates of QKD protocols are also important, where the key rate is defined by the ratio of the length of the final secure key to the length of the raw key. Gottesman and Lo [16] converted EDPs that use two-way classical communication into QKD protocols that use the same communication. More specifically, they proposed preprocessing that uses two-way classical communication. By inserting this two-way preprocessing before the conventional one-way IR protocol, the key rates of QKD protocols are increased when the error rate of a channel expressed as a percentage is higher than about 9%. Indeed, the tolerable error rate of the BB84 protocol is increased from 11% to 18.9%, and that of the six-state protocol is increased from 12.7% to 26.4%, where the tolerable error rate is the error rate at which the key rate becomes zero. Chau later showed that the two-way BB84 protocol can tolerate 20.0% error rate, and that the two-way six-state protocol can tolerate 27.6% error rate [17]. Recently, this kind of two-way preprocessing has been applied to QKD protocols with weak coherent pulses [18,19]. It should be noted that this preprocessing is also known within the classical key agreement context, in which it is usually called an advantage distillation protocol [20]. Bae and Acín and Acín *et al.* [21,22] extensively studied the tolerable error rate of QKD protocols with advantage distillation protocols; on the other hand, we are interested in the key rates of QKD protocols in this paper.

Vollbrecht and Vestraete proposed a new type of two-way EDP [23]. This protocol uses previously shared Einstein-Podolsky-Rosen (EPR) pairs as an assistant resource (two-way breeding EDP), and the distillation rate of this EDP exceeds that of one-way EDPs for a whole range of fidelities, where the fidelity is that between the initial mixed state and the EPR pair. Using the fact that a breeding EDP can be converted into a QKD protocol assisted by one-time pad encryption with a preshared secret key [24], Vollbrecht and Vestraete's two-way breeding EDP [23] was converted into a

*shun-wata@it.ss.titech.ac.jp
†ryutaroh@rmatsumoto.org; URL: http://www.rmatsumoto.org/research.html
‡uyematsu@ieee.org
§kawano@theory.brl.ntt.co.jp

two-way QKD protocol assisted by one-time pad encryption [18,25]. The key rate of the converted QKD protocol is higher than that of one-way QKD protocols [9,12] for a whole range of error rates. It should be noted that the use of a preshared secret key is not the basis of their improvement, because any QKD protocol that makes use of a preshared key can be transformed into an equally efficient protocol that does not need a preshared secret key [26].

We propose an IR protocol that uses two-way classical communication in this paper. Our proposed protocol is based on Vollbrecht and Vestraete's idea of a two-way breeding EDP [23], but does not require any preshared secret keys. Furthermore, our protocol does not leak information that is redundantly leaked to Eve in [18,25]. More precisely, in these protocols [18,25], Alice sends a redundant message that is useless to Bob, but is useful to Eve. However, in the proposed protocol, Alice does not send that redundant information. As a result, for the BB84 and six-state protocols, the key rates of the QKD protocols that use our IR protocol are higher than those of previously known protocols for a wide range of error rates. In particular, the key rate of our protocol is higher than those of known protocols [9,12,14,25] for the whole range of error rates. We also show the relation between the proposed protocol and the advantage distillation protocol, i.e., the *B* step of Gottesman and Lo [16] (Remark 4). We also show the relation between the proposed QKD protocol and Vollbrecht and Vestraete's EDP. As a result, it turns out that there does not seem to be any EDP that corresponds to our proposed protocol (Remark 5).

The rest of this paper is organized as follows. Section II proposes a two-way IR protocol. Section III presents the key rate formula of the QKD protocol that uses our proposed IR protocol. We present a proof of the key rate formula in the supplementary material [27], because the proof is involved and techniques used in the proof are not new. Section IV presents the key rate formula as a function of error rate.

II. TWO-WAY INFORMATION RECONCILIATION PROTOCOL

We propose an IR protocol that uses two-way classical communication (called a two-way IR protocol after this) in this section. When Alice and Bob have correlated classical sequences, $\mathbf{x},\mathbf{y}\in\mathbb{F}_2^{2n}$, the purpose of IR protocols for Alice and Bob is to share the same classical sequence by exchanging messages over a public authenticated channel, where $\mathbb{F}_2$ is a field of order 2. Here, we assume that the pair of sequences $(\mathbf{x},\mathbf{y})$ is independently identically distributed (i.i.d) according to a joint probability distribution P_{XY} on $\mathbb{F}_2\times\mathbb{F}_2$.

Let us review some notations for a linear code to describe our IR protocol. An $[n,n-m]$ classical linear code $\mathcal{C}_{n,m}$ is an $(n-m)$-dimensional linear subspace of $\mathbb{F}_2^n$. Then a parity check matrix $M_{\mathcal{C}_{n,m}}$ of code $\mathcal{C}_{n,m}$ is an $m\times n$ matrix of rank m with 0,1 entries such that $\mathbf{c}M_{\mathcal{C}_{n,m}}^T=\mathbf{0}$ for any $\mathbf{c}\in\mathcal{C}_{n,m}$, where $M_{\mathcal{C}_{n,m}}^T$ is the transpose matrix of $M_{\mathcal{C}_{n,m}}$. A decoder $g_{\mathcal{C}_{n,m}}$ of code $\mathcal{C}_{n,m}$ is a map from a syndrome $\mathbf{t}\in\mathbb{F}_2^m$ to an error $\mathbf{e}\in\mathcal{D}(\mathbf{t})$, where $\mathcal{D}(\mathbf{t})\coloneqq\{\mathbf{e}\in\mathbb{F}_2^n|\mathbf{e}M_{\mathcal{C}_{n,m}}^T=\mathbf{t}\}$ is the set of errors whose syndromes are $\mathbf{t}$. After this, we will assume that a linear code is implicitly specified with a parity check matrix and a decoder.

We need to define some auxiliary random variables to describe our IR protocol. Let $\xi_1:\mathbb{F}_2^2\to\mathbb{F}_2$ be a function defined as $\xi_1(a_1,a_2)\coloneqq a_1+a_2$ for $a_1,a_2\in\mathbb{F}_2$, and let $\xi_2:\mathbb{F}_2^2\to\mathbb{F}_2$ be a function defined as $\xi_2(a,0)\coloneqq a$ and $\xi_2(a,1)\coloneqq 0$ for $a\in\mathbb{F}_2$. For a pair of joint random variables $((X_1,Y_1),(X_2,Y_2))$ with a distribution P_{XY}^2, define random variables $U_1\coloneqq\xi_1(X_1,X_2)$, $V_1\coloneqq\xi_1(Y_1,Y_2)$, and $W_1\coloneqq U_1+V_1$. Furthermore, define random variables $U_2\coloneqq\xi_2(X_2,W_1)$, $V_2\coloneqq\xi_2(Y_2,W_1)$ and $W_2\coloneqq U_2+V_2$. For the pair of sequences $\mathbf{x}=(x_{11},x_{12},\ldots,x_{n1},x_{n2})$ and $\mathbf{y}=(y_{11},y_{12},\ldots,y_{n1},y_{n2})$, which is distributed according to the product distribution P_{XY}^{2n}, let $\mathbf{u}$, $\mathbf{v}$, and $\mathbf{w}$ be $2n$-bit sequences such that

$$u_{i1}\coloneqq\xi_1(x_{i1},x_{i2}),\quad v_{i1}\coloneqq\xi_1(y_{i1},y_{i2}),\quad w_{i1}\coloneqq u_{i1}+v_{i1}$$

and

$$u_{i2}\coloneqq\xi_2(x_{i2},w_{i1}),\quad v_{i2}\coloneqq\xi_2(y_{i2},w_{i1}),\quad w_{i2}\coloneqq u_{i2}+v_{i2}$$

for $1\leqslant i\leqslant n$. Then, the pair $(\mathbf{u},\mathbf{v})$ is distributed according to the distribution $P_{U_1U_2V_1V_2}^n$, and the discrepancy $\mathbf{w}$ between $\mathbf{u}$ and $\mathbf{v}$ is distributed according to the distribution $P_{W_1W_2}^n$. For sequence $\mathbf{w}$, let $\mathsf{T}_b\coloneqq\{j|1\leqslant j\leqslant n,w_{j1}=b\}$ be the set of indices of blocks such that the parities of the discrepancies are $b\in\{0,1\}$. For the subsequence $\mathbf{u}_2\coloneqq(u_{12},\ldots,u_{n2})$, let $\mathbf{u}_{2,\mathsf{T}_b}$ be the subsequence that consists of the ith bit of $\mathbf{u}_2$ such that $i\in\mathsf{T}_b$.

The first step of well-known methods [16,20,23] of two-way processing within the key distillation context is to classify blocks of length 2 according to the parity w_{i1} of the discrepancies in each block. In conventional two-way processing of key distillation protocols [16,20], the so-called advantage distillation protocols, Alice sends the parity sequence $\mathbf{u}_1\coloneqq(u_{11},\ldots,u_{n1})$ to Bob so that he can identify the parity sequence $\mathbf{w}_1\coloneqq(w_{11},\ldots,w_{n1})$ of the discrepancies. Then, Alice and Bob discard $\mathbf{u}_1$ and $\mathbf{v}_1\coloneqq(v_{11},\ldots,v_{n1})$, respectively, because $\mathbf{u}_1$ is revealed to Eve. Furthermore, Alice and Bob discard the second bit of the ith block, if the parity of the discrepancies is 1, i.e., $i\in\mathsf{T}_1$. Finally, Alice and Bob undertake an error correction procedure for the subsequences $(\mathbf{u}_{2,\mathsf{T}_0},\mathbf{v}_{2,\mathsf{T}_0})$. More precisely, Alice sends the syndrome $\mathbf{t}_2\coloneqq\mathbf{u}_{2,\mathsf{T}_0}M_{\mathcal{C}_{n_0,m_0}}^T$ for the prescribed $[n_0,m_0]$ linear code, and then Bob decodes $\hat{\mathbf{w}}_{2,\mathsf{T}_0}\coloneqq g_{\mathcal{C}_{n_0,m_0}}(\mathbf{t}_2+\mathbf{v}_{2,\mathsf{T}_0}M_{\mathcal{C}_{n_0,m_0}}^T)$ and obtains $\mathbf{v}_{2,\mathsf{T}_0}+\hat{\mathbf{w}}_{2,\mathsf{T}_0}$, where $n_0\coloneqq|\mathsf{T}_0|$ is the cardinality of the set T_0.

Our two-way IR protocol, which is based on Vollbrecht and Vestraete's idea of two-way EDP [23], is quite similar to the previously described two-way processing except for one significant change. As is usual in information theory, if we allow negligible error probability, Alice does not need to send the parity sequence $\mathbf{u}_1$ to Bob to identify parity sequence $\mathbf{w}_1$. More precisely, Bob can decode $\mathbf{w}_1$ with negligible decoding error probability if Alice sends a syndrome $\mathbf{t}_1\coloneqq\mathbf{u}_1M_{\mathcal{C}_{n,m}}^T$ for a linear code such that the rate is $m/n\simeq H(P_{W_1})$ ([28], Corollary 2). Since Eve's available information from syndrome $\mathbf{t}_1$ is often much smaller than that from the sequence $\mathbf{u}_1$ itself, our IR protocol is more efficient than the above-mentioned two-way processing in most cases, as

will be discussed in Sec. IV. Our IR protocol is formally executed as follows, where the tilde and caret on a sequence, a set, or a number indicate that they are guessed versions of those without these diacritics. Note that the inputs of the IR protocol are Alice's bit sequence $\mathbf{x}$ and Bob's bit sequence $\mathbf{y}$, and the outputs of the IR protocol are a sequence $\hat{\mathbf{u}}$ guessed by Alice and a sequence $\tilde{\mathbf{u}}$ guessed by Bob.

(i) Alice locally computes $\mathbf{u}_1$ and Bob does the same for $\mathbf{v}_1$.

(ii) For a prescribed $[n,n-m]$ linear code $\mathcal{C}_{n,m}$, Alice sends syndrome $\mathbf{t}_1=\mathbf{u}_1 M_{\mathcal{C}_{n,m}}^T$ to Bob.

(iii) Bob decodes $\hat{\mathbf{w}}_1 := g_{\mathcal{C}_{n,m}}(\mathbf{t}_1+\mathbf{v}_1 M_{\mathcal{C}_{n,m}}^T)$ and sends $\hat{\mathbf{w}}_1$ to Alice.

(iv) Alice computes $\hat{\mathbf{u}}_2$. If the number $\hat{n}_0 := |\{i|\hat{w}_{i1}=0\}|$ of blocks such that the guessed parity $\hat{w}_{i1}$ of the discrepancies is 0 does not satisfy $\underline{n}_0 \leqslant \hat{n}_0 \leqslant \bar{n}_0$ for prescribed integers $\underline{n}_0$ and $\bar{n}_0$, then Bob randomly guesses $\hat{\mathbf{u}}_{2,\hat{\mathsf{T}}_0}$. Otherwise, Alice sends the syndrome $\hat{\mathbf{t}}_2 := \hat{\mathbf{u}}_{2,\hat{\mathsf{T}}_0} M_{\mathcal{C}_{\hat{n}_0,\hat{m}_0}}$ for a prescribed $[\hat{n}_0,\hat{n}_0-\hat{m}_0]$ linear code $\mathcal{C}_{\hat{n}_0,\hat{m}_0}$.

(v) Bob decodes $\tilde{\mathbf{w}}_{2,\hat{\mathsf{T}}_0} := g_{\mathcal{C}_{\hat{n}_0,\hat{m}_0}}(\hat{\mathbf{t}}_2+\hat{\mathbf{v}}_{2,\hat{\mathsf{T}}_0} M_{\mathcal{C}_{\hat{n}_0,\hat{m}_0}}^T)$, and obtains $\tilde{\mathbf{u}}_{2,\hat{\mathsf{T}}_0} := \hat{\mathbf{v}}_{2,\hat{\mathsf{T}}_0}+\tilde{\mathbf{w}}_{2,\hat{\mathsf{T}}_0}$.

Note that $\hat{\mathbf{u}}_{2,\hat{\mathsf{T}}_1}$ and $\hat{\mathbf{v}}_{2,\hat{\mathsf{T}}_1}$ are set to all 0's in our protocol, which is mathematically equivalent to discarding them.

According to the universal channel coding theorem for the linear code ([28], Corollary 2), rates $m/n=H(P_{W_1})+\delta$ and $\hat{m}_0/\hat{n}_0=H(P_{W_2|W_1=0})+\delta$ for small $\delta>0$ are sufficient for Bob to decode $\mathbf{w}_1$ and $\mathbf{w}_{2,\mathsf{T}_0}$ with negligible decoding error probability. Furthermore, we set $\underline{n}_0 := n[P_{W_1}(0)-\delta]$ and $\bar{n}_0 := n[P_{W_1}(1)+\delta]$ to satisfy the condition $\underline{n}_0 \leqslant \hat{n}_0 \leqslant \bar{n}_0$, in step (iv) with high probability.

Remark 1. Since we cannot estimate the probability distribution of error exactly in QKD protocols and the actual distribution fluctuates around the estimated error distribution, universality of codes is required. Even though the distribution of errors in the QKD protocols are not necessarily i.i.d., it is sufficient to consider a universality condition on codes for the i.i.d. case. More precisely, it is sufficient to use a linear code such that the decoding error probability of the linear code is universally small for any binary symmetric channel whose crossover probability is close to the estimated error rate. Such observations were first pointed out by Hamada [29]. Efficiently decodeable linear codes such as the low-density parity check matrix code [30] and the turbo code [31] satisfy this condition.

III. SECURITY OF QKD AND KEY RATE

This section presents the asymptotic key rate of a QKD protocol that employs the IR protocol proposed in Sec. II. The asymptotic key rate is derived by the security proof method [13–15].

We implement a prepare and measure scheme in a practical QKD protocol. However, when we analyze the security of a QKD protocol, it is usually more convenient to consider its entanglement-based version. Without compromising security, we can assume that Alice and Bob's raw keys and bit sequences for error estimation are obtained by measuring a bipartite state $\rho_{A^N B^N}$ on an N pair of bipartite systems $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes N}$, that $\rho_{A^N B^N}$ is invariant under the permutation of the systems,[1] and that Eve can access $\mathrm{Tr}_{A^N B^N}(\rho_{A^N B^N E^N})$ for a purification $\rho_{A^N B^N E^N}$ of $\rho_{A^N B^N}$ (see also [13,14]). The specific form of $\rho_{A^N B^N}$ depends on which scheme Alice and Bob employ to transmit a binary sequence, noise in the channel, and Eve's attack. From ([15], Lemma 4.2.2), without loss of generality, we can assume that purification $\rho_{A^N B^N E^N}$ lies on the symmetric subspace of $(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)^{\otimes N}$, because any purification can be transformed into another purification using Eve's local operation.

Before the protocol is started, Alice and Bob discard the last k subsystems $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B^{\otimes k}$ for technical reasons of security proof. More specifically, k subsystems are discarded to apply the de Finetti style representation theorem ([15], Theorem 4.3.2) (see also [32]) in the security proof. Therefore, we set $N := 2n+m+k$. Then, Alice and Bob conduct the protocol for the state, $\rho_{A^{2n+m}B^{2n+m}} := \mathrm{Tr}_k(\rho_{A^N B^N})$, where k is the number of discarded systems, m is the number of systems for parameter estimation, and $2n$ is the number of systems that are used for key distillation.

First, Alice and Bob undertake the following parameter estimation protocol for the last m subsystems of the state $\rho_{A^{2n+m}B^{2n+m}}$. The parameter estimation protocol is conducted to estimate the number of discrepancies between Alice and Bob's raw keys, and the amount of information that Eve has gained by eavesdropping.

(i) Alice and Bob carry out a measurement that corresponds to a positive-operator-valued measure (POVM), $\mathcal{M} := \{M_a\}_{a\in\mathcal{A}}$, for each system $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{A}$ is the set of measurement outcomes. The specific form of $\mathcal{M}$ depends on which scheme we use.

(ii) If the type $P_{\mathbf{a}}$ of the measurement outcomes $\mathbf{a}=(a_1,\ldots,a_m)$ satisfies $P_{\mathbf{a}} \in \mathcal{Q}$ for a prescribed set $\mathcal{Q}$, the protocol outputs the type $Q := P_{\mathbf{a}}$, and Alice and Bob conduct the key distillation protocol according to Q, where the type of sequence $\mathbf{a}=(a_1,\ldots,a_m)$ is the frequency distribution defined by

$$P_{\mathbf{a}}(a) := \frac{|\{i|1 \leqslant i \leqslant m, a_i = a\}|}{m} \quad \text{for } a \in \mathcal{A}$$

(for more details on the type, see [[33], Chap. 11]). Otherwise, it outputs "abort."

It is convenient to describe the parameter estimation protocol using a completely positive (CP) map as follows. Let $\mathcal{M}^{\otimes m} := \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathcal{A}^m}$ be a product POVM on $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes m}$, where $M_{\mathbf{a}} = M_{a_1} \otimes \cdots \otimes M_{a_m}$. Then, we can define a CP map $\mathcal{E}_Q$ by

$$\mathcal{E}_Q : \rho_m \mapsto \sum_{\mathbf{a}\in\mathcal{T}_Q^n(\mathcal{A})} \mathrm{Tr} M_{\mathbf{a}} \rho_m, \tag{1}$$

which maps the density operator to the probability such that the parameter estimation protocol outputs Q, where $\mathcal{T}_Q^m(\mathcal{A})$ is a set of all sequences on $\mathcal{A}^m$ with type Q.

[1] By applying the random permutation after the transmission phase of QKD protocols, we can assume that Alice's and Bob's bit sequences are invariant under the permutation without any compromise of the security.

When the output of the parameter estimation protocol is $Q \in \mathcal{Q}$, Alice, Bob, and Eve's tripartite state is given by

$$\rho^{Q}_{A^{2n}B^{2n}E^{N}} := \frac{1}{P_{\mathrm{PE}}(Q)} \times (\mathrm{id}_{A^{2n}B^{2n}} \otimes \mathcal{E}_{Q} \otimes \mathrm{id}_{E^{N}})(\rho_{A^{2n+m}B^{2n+m}E^{N}}),$$

where $P_{\mathrm{PE}}(Q)$ is the probability that the parameter estimation protocol outputs Q, and id denotes the identity map on each system.

Alice and Bob apply a measurement $\mathcal{M}_{XY} := \{M_x \otimes M_y\}_{(x,y)\in \mathbb{F}_2\times\mathbb{F}_2}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ to the remaining $2n$ systems to obtain classical data (raw keys). Then, Alice and Bob's measurement results, $(\mathbf{x},\mathbf{y}) \in \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n}$, and Eve's available information is described by a $\{ccq\}$ state[2]

$$\rho^{Q}_{\mathbf{XY}E^{N}} := (\mathcal{E}^{\otimes 2n}_{XY} \otimes \mathrm{id}_{E^{N}})(\rho^{Q}_{A^{2n}B^{2n}E^{N}}),$$

where we introduce a CP map $\mathcal{E}_{XY}$ that describes the measurement procedure for convenience.

According to output Q of the parameter estimation protocol, Alice and Bob decide the parameters of the IR protocol: the rate $R(Q) := m/n$ of the linear code $\mathcal{C}_{n,m}$, the numbers $\underline{n}_0(Q)$ and $\bar{n}_0(Q)$ that are used in step (iv), and the rate $R_0(Q) := m_0/n_0$ of the linear code $\mathcal{C}_{n_0,m_0}$ for $\underline{n}_0(Q) \leqslant n_0 \leqslant \bar{n}_0(Q)$. Furthermore, Alice and Bob also decide the length $\ell(Q)$ of the finally distilled key according to Q. According to the determined parameters, a final secure key pair is distilled as follows.

(i) Alice and Bob undertake the two-way IR protocol in Sec. II, and Alice obtains $\hat{\mathbf{u}}$ and Bob obtains $\tilde{\mathbf{u}}$.

(ii) Alice and Bob carry out a privacy amplification protocol to distill a key pair (s_A, s_B) such that Eve has little information about it. Alice first randomly chooses a hash function $f: \mathbb{F}_2^{2n} \to \{0,1\}^{\ell(Q)}$ from a family of two-universal hash functions (refer to ([15], Definition 5.2.1) for a formal definition of a family of two-universal hash functions), and sends the choice of f to Bob over the public channel. Then, Alice's distilled key is $s_A = f(\hat{\mathbf{u}})$ and Bob's distilled key is $s_B = f(\tilde{\mathbf{u}})$.

The distilled key pair and Eve's available information can be described by a $\{cccq\}$ state, $\rho^{Q}_{S_A S_B C E^{N}}$, where the classical system C consists of random variables $(\mathbf{T}_1, \hat{\mathbf{T}}_2, \hat{\mathbf{W}}_1)$ that describe the exchanged messages $(\mathbf{t}_1, \hat{\mathbf{t}}_2, \hat{\mathbf{w}}_1)$ in the IR protocol and a random variable F that describes the choice of the hash function in the PA protocol. To define the security of the distilled key pair (S_A, S_B), we use the universally composable security definition [34,35], which is defined by the trace distance between the actual key pair and the ideal key pair. We cannot state security in QKD protocols in the sense that the distilled key pair (S_A, S_B) is secure for a particular output Q of the parameter estimation protocol, because there is a slight possibility that the parameter estimation protocol will not output "abort" even though Eve has so much information. The QKD protocol is said to be ε secure (in the sense of the average over the outputs of the parameter estimation protocol) if

$$\sum_{Q\in\mathcal{Q}} P_{\mathrm{PE}}(Q) \frac{1}{2} \left\| \rho^{Q}_{S_A S_B C E^{N}} - \rho^{Q,\mathrm{mix}}_{S_A S_B} \otimes \rho_{C E^{N}} \right\| \leqslant \varepsilon, \tag{2}$$

where $\rho^{Q,\mathrm{mix}}_{S_A S_B} := \sum_{s\in\mathcal{S}_Q} (1/|\mathcal{S}_Q|) |s,s\rangle\langle s,s|$ is the uniformly distributed key on the key space $\mathcal{S}_Q := \{0,1\}^{\ell(Q)}$.

To state the relation between the security and the asymptotic key rate of the previously mentioned QKD protocol, define

$$\Gamma(Q) := \{\sigma_{AB} | P^{\sigma_{AB}}_{A} = Q\}$$

as the set of two-qubit density operators that are compatible with output Q of the parameter estimation protocol, where $P^{\sigma_{AB}}_{A}$ denotes the probability distribution of the outcomes when measuring σ_{AB} with POVM $\mathcal{M}$, i.e., $P^{\sigma_{AB}}_{A}(a) := \mathrm{Tr}(M_a \sigma_{AB})$. For a purification σ_{ABE} of a density operator $\sigma_{AB} \in \Gamma(Q)$, let $\sigma_{X_1X_2Y_1Y_2E_1E_2} := (\mathcal{E}^{\otimes 2}_{XY} \otimes \mathrm{id}^{\otimes 2}_{E})(\sigma^{\otimes 2}_{ABE})$ be a $\{ccq\}$ state that consists of two-bit pairs $((X_1,X_2),(Y_1,Y_2))$ and environment systems E_1, E_2. By using functions ξ_1 and ξ_2, define random variables (U_1, U_2, W_1, W_2) for the pair of bits $((X_1,X_2),(Y_1,Y_2))$ in the same way as in Sec. II. Then, let $\sigma_{U_1U_2W_1E_1E_2}$ and $\sigma_{U_1U_2W_1U_1E_1E_2}$ be density operators that respectively describe the classical random variables (U_1, U_2, W_1) and (U_1, U_2, W_1, U_1) with the environment systems E_1, E_2.

Theorem 1. For $Q \in \mathcal{Q}$, i.e., the output of the parameter estimation protocol such that the QKD protocol does not abort, let $\ell(Q)/2n$ be the key rate of the protocol. For any $\varepsilon > 0$, if the key rate satisfies

$$\begin{aligned} \frac{\ell(Q)}{2n} < \frac{1}{2} \min_{\sigma_{AB}\in\Gamma(Q)} \max[& H_{\sigma}(U_1U_2|W_1E_1E_2) - H(P_{W_1}) \\ & - P_{W_1}(0) H(P_{W_2|W_1=0}), H_{\sigma}(U_2|W_1U_1E_1E_2) \\ & - P_{W_1}(0) H(P_{W_2|W_1=0})], \end{aligned} \tag{3}$$

then there exists a protocol that is ε secure in the sense of Eq. (2) for sufficiently large n, where $H_{\rho}(A|B) := H(\rho_{AB}) - H(\rho_B)$ is the conditional von Neumann entropy [36], and $H(P)$ is the Shannon entropy [33].

The meaning of the two arguments of the maximum in Eq. (3) should be noted. The first argument states that the key rate is given by the difference between Eve's ambiguity $H_{\sigma}(U_1U_2|W_1E_1E_2)$ about Alice's reconciled key and the amount $H(P_{W_1}) + P_{W_1}(0) H(P_{W_2|W_1=0})$ of information leaked in the IR protocol. On the other hand, since information leaked from the syndrome $\mathbf{t}_1 = \mathbf{u}_1 M^{T}_{\mathcal{C}_{n,m}}$ cannot be more than $\mathbf{u}_1$ itself, we can evaluate the key rate under the condition that Eve can access $\mathbf{u}_1$ itself, i.e., Eve's ambiguity $H_{\sigma}(U_2|W_1U_1E_1E_2)$ about Alice's reconciled key and the amount $P_{W_1}(0) H(P_{W_2|W_1=0})$ of information leaked in the IR protocol. If either of them is omitted, the key rate is underestimated, as will be discussed in Section IV.

[2] A $\{ccq\}$ state is a tripartite state such that the first and second systems are classical and the third system is quantum. See [39] for details of this notation.

Theorem 1 is proved by demonstrating the above intuition formally, where we use a security proof method [13–15]. More precisely, we use the techniques of privacy amplification and minimum entropy, and the de Finetti style representation theorem and the property of symmetric states (see [15]). Since the proof is involved and techniques used in the proof are not new, we give the proof for Theorem 2 in the supplementary material [27].

IV. ANALYSIS OF KEY RATE

Here, we analyze the asymptotic key rate formula in Theorem 1. More precisely, we derive a specific form of the key rate formulas as functions of the error rates for the six-state [5] and BB84 protocols [4].

Before analyzing the key rate, let us define some notations. For $\mathsf{x},\mathsf{z}\in\mathbb{F}_2$, let

$$|\psi(\mathsf{x},\mathsf{z})\rangle := \frac{1}{\sqrt{2}}[|0\rangle|0+\mathsf{x}\rangle + (-1)^{\mathsf{z}}|1\rangle|1+\mathsf{x}\rangle]$$

be the Bell states on the two-qubit system $\mathcal{H}_A\otimes\mathcal{H}_B$. For a probability distribution P_{XZ} on $\mathbb{F}_2\times\mathbb{F}_2$, a state of the form

$$\sum_{\mathsf{x},\mathsf{z}\in\mathbb{F}_2} P_{\mathsf{XZ}}(\mathsf{x},\mathsf{z})|\psi(\mathsf{x},\mathsf{z})\rangle\langle\psi(\mathsf{x},\mathsf{z})|$$

is called a Bell diagonal state. We occasionally abbreviate $P_{\mathsf{XZ}}(\mathsf{x},\mathsf{z})$ as p_{xz}.

Theorem 2. For a Bell diagonal state $\sigma_{AB}=\Sigma_{\mathsf{x},\mathsf{z}\in\mathbb{F}_2}P_{\mathsf{XZ}}(\mathsf{x},\mathsf{z})|\psi(\mathsf{x},\mathsf{z})\rangle\langle\psi(\mathsf{x},\mathsf{z})|$, we have

$$\begin{aligned}&\frac{1}{2}\max[H_\sigma(U_1U_2|W_1E_1E_2)-H(P_{W_1})-P_{W_1}(0)H(P_{W_2|W_1=0}),\\&\quad H_\sigma(U_2|W_1U_1E_1E_2)-P_{W_1}(0)H(P_{W_2|W_1=0})]\\&=\max\left[1-H(P_{\mathsf{XZ}})+\frac{P_{\bar{\mathsf{X}}}(1)}{2}h\left(\frac{p_{00}p_{10}+p_{01}p_{11}}{(p_{00}+p_{01})(p_{10}+p_{11})}\right),\right.\\&\left.\frac{P_{\bar{\mathsf{X}}}(0)}{2}[1-H(P'_{\mathsf{XZ}})]\right],\end{aligned}\tag{4}$$

where $h(p):=-p\log p-(1-p)\log(1-p)$ is the binary entropy function,

$$P_{\bar{\mathsf{X}}}(0) := (p_{00}+p_{01})^2+(p_{10}+p_{11})^2,$$

$$P_{\bar{\mathsf{X}}}(1) := 2(p_{00}+p_{01})(p_{10}+p_{11}),$$

and

$$P'_{\mathsf{XZ}}(0,0) := \frac{p_{00}^2+p_{01}^2}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2},$$

$$P'_{\mathsf{XZ}}(1,0) := \frac{2p_{00}p_{01}}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2},$$

$$P'_{\mathsf{XZ}}(0,1) := \frac{p_{10}^2+p_{11}^2}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2},$$

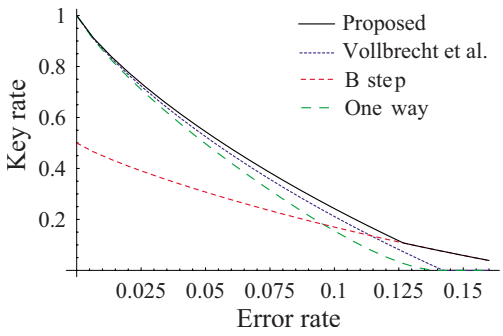

FIG. 1. (Color online) Comparison of the key rates of the six-state protocols. "Proposed" is the key rate of the six-state protocol that uses the proposed IR protocol. "Vollbrecht *et al.*" is the key rate of the two-way six-state protocol of [18,25]. "*B* step" is the key rate of the two-way six-state protocol of [16]. "One way" is the key rate of the one-way six-state protocol with noisy preprocessing [14]. It should be noted that the key rates of two-way six-state protocols of [15–17] are slightly higher than that of the proposed protocol for error rates higher than about 15%. For error rates higher than 15%, the best protocol among known protocols is the protocol presented by Renner [15], which involves the advantage distillation and the noisy preprocessing proposed by Renner *et al.* [13,14].

$$P'_{\mathsf{XZ}}(1,1) := \frac{2p_{10}p_{11}}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}.$$

The theorem is proved by a straightforward calculation. Thus, the proof is presented in the supplementary material [27].

The six-state protocol [5] uses three different bases defined by the z basis $\{|0_z\rangle,|1_z\rangle\}$, x basis $\{1/\sqrt{2}(|0_z\rangle\pm|1_z\rangle)\}$, and y basis $\{1/\sqrt{2}(|0_z\rangle\pm i|1_z\rangle)\}$. When Alice and Bob obtain an error rate e, the set $\Gamma(Q)$ consists of states whose Bell diagonal entries $p_{00},p_{10},p_{01},p_{11}$ satisfy the conditions $p_{10}+p_{11}=e$, $p_{01}+p_{11}=e$, and $p_{01}+p_{10}=e$. Together with the normalization condition, we find $p_{00}=1-3e/2$ and $p_{10}=p_{01}=p_{11}=e/2$. Since it is sufficient only to minimize over the Bell diagonal states in Eq. (3) (see the supplementary material [27] for a proof), the key rate of the six-state protocol for the error rate e is given by substituting $p_{00}=1-3e/2$ and $p_{10}=p_{01}=p_{11}=e/2$ into Eq. (4). The key rate of the six-state protocol that uses the proposed IR protocol is plotted in Fig. 1.

The BB84 protocol is similar to the six-state protocol, but uses only the z basis and the x basis to transmit a bit sequence. Thus, we obtain only two conditions on the four coefficients $p_{00},p_{10},p_{01},p_{11}$, and the set $\Gamma(Q)$ consists of states whose Bell diagonal entries satisfy the conditions $p_{10}+p_{11}=e$ and $p_{01}+p_{11}=e$. The resulting candidates for Bell diagonal states in $\Gamma(Q)$ have coefficients $p_{00}=1-2e+p_{11}$, $p_{10}=p_{01}=e-p_{11}$, and $p_{11}\in[0,e]$, and we have to minimize the key rate formula of Eq. (4) over the free parameter $p_{11}\in[0,e]$. The key rate of the BB84 protocol that uses the proposed IR protocol is plotted in Fig. 2.

Remark 2. By using the chain rule of von Neumann entropy, we can rewrite the left-hand side (LHS) of Eq. (4) as

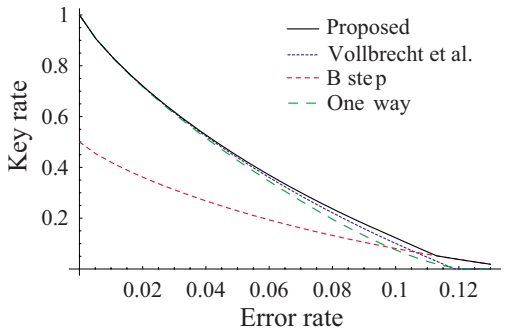

FIG. 2. (Color online) Comparison of the key rates of the BB84 protocols. "Proposed" is the key rate of the BB84 protocol that uses the proposed IR protocol. "Vollbrecht *et al.*" is the key rate of the two-way BB84 protocol of [18,25]. "*B* step" is the key rate of the two-way BB84 protocol of [16]. "One way" is the key rate of the one-way BB84 protocol with noisy preprocessing [14].

$$\frac{1}{2}\{\max[H_\sigma(U_1|W_1E_1E_2)-H(P_{W_1}),0]+H_\sigma(U_2|W_1U_1E_1E_2) - P_{W_1}(0)H(P_{W_2|W_1=0})\}. \tag{5}$$

We can interpret this formula as follows. If Bob's ambiguity $H(P_{W_1})$ about bit U_1, i.e., the amount of transmitted syndrome per bit, is smaller than Eve's ambiguity $H_\sigma(U_1|W_1E_1E_2)$ about bit U_1, then Eve cannot decode sequence $\mathbf{U}_1$ [37,38], and there exists some remaining ambiguity about bit U_1 for Eve. We can thus distill some secure key from bit U_1. On the other hand, if Bob's ambiguity $H(P_{W_1})$ about bit U_1, i.e., the amount of transmitted syndrome per bit, is larger than Eve's ambiguity $H_\sigma(U_1|W_1E_1E_2)$ about U_1, then Eve might be able to decode sequence $\mathbf{U}_1$ from her side information W_1, E_1, E_2, and the transmitted syndrome [37,38]. Thus, there exists the possibility that Eve can completely know bit U_1, and we can distill no secure key from bit U_1, because we have to consider the worst case in a cryptographic scenario. Consequently, sending the hashed version (syndrome) of sequence $\mathbf{U}_1$ instead of $\mathbf{U}_1$ itself is not always effective, and the slopes of the key rate curves in Figs. 1 and 2 change when Eve becomes able to decode $\mathbf{U}_1$.

The second and third terms of Eq. (5) are the same as the key rate formula of the protocol that uses Gottesman and Lo's *B* step [16] followed by error correction and privacy amplification. Even though Alice sends the sequence $\mathbf{U}_1$ itself instead of its hashed version in the *B* step, the key rate of the protocol with the *B* step is equal to that of the proposed protocol for high error rates, because Eve can decode sequence $\mathbf{U}_1$ from her side information and the transmitted syndrome.

Remark 3. The yield of Vollbrecht and Vestraete's EDP [23] and the key rate of the QKD protocols [18,25] are given by

$$1-H(P_{XZ})+\frac{P_{\bar{X}}(1)}{4}\left\{h\left(\frac{p_{01}}{p_{00}+p_{01}}\right)+h\left(\frac{p_{11}}{p_{10}+p_{11}}\right)\right\}. \tag{6}$$

We can find by the concavity of the binary entropy function that the first argument in the maximum of the RHS of Eq. (4) is larger than the value in Eq. (6). To explain why the key rate of the proposed protocol is higher than that of [18,25], we need to review the EDP [23] by using the notations in Sec. II. Assume that Alice and Bob share Bell diagonal states $\sigma_{AB}^{\otimes 2n}$. First, Alice and Bob divide $2n$ pairs into n blocks of length 2, and locally carry out a controlled-NOT CNOT operation on each block, where the $2i$th pair is the source and the $(2i-1)$th pair is the target. Then, Alice and Bob undertake the breeding protocol [10] to guess bit-flip errors in the $(2i-1)$th pair for all i. The guessed bit-flip errors can be described by a sequence $\hat{\mathbf{w}}_1$. Note that two-way communication is used in this step. According to sequence $\hat{\mathbf{w}}_1$, Alice and Bob classify indices of blocks into two sets $\hat{\mathsf{T}}_0$ and $\hat{\mathsf{T}}_1$. For a collection of $2i$th pairs such that $i\in\hat{\mathsf{T}}_0$, Alice and Bob conduct the breeding protocol to correct bit-flip errors. For a collection of $2i$th pairs such that $i\in\hat{\mathsf{T}}_1$, Alice and Bob perform measurements in the $\{|0_z\rangle,|1_z\rangle\}$ basis, and obtain measurement results $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ and $\mathbf{y}_{2,\hat{\mathsf{T}}_1}$. Alice sends $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ to Bob. Alice and Bob correct the phase errors for the remaining pairs by using information $\hat{\mathsf{T}}_0$ and $\hat{\mathsf{T}}_1$ and bit-flip error $\mathbf{x}_{2,\hat{\mathsf{T}}_1}+\mathbf{y}_{2,\hat{\mathsf{T}}_1}$.

If we convert this EDP into a QKD protocol, the difference between that QKD protocol and ours is as follows. In the protocol converted from [23], after step (iii), Alice reveals the sequence $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$, which consists of the second bit x_{i2} of the ith block such that the parity of discrepancies $\hat{w}_{i1}$ is 1. However, Alice discards $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ in the proposed IR protocol of Sec. II. Since the sequence $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ has some correlation to the sequence $\mathbf{u}_1$ from the viewpoint of Eve, Alice should not reveal $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ to achieve a higher key rate.

In the EDP context, on the other hand, since the bit flip error $\mathbf{x}_{2,\hat{\mathsf{T}}_1}+\mathbf{y}_{2,\hat{\mathsf{T}}_1}$ has some correlation to the phase-flip errors in the $(2i-1)$th pair with $i\in\hat{\mathsf{T}}_1$, Alice should send the measurement results $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ to Bob. If Alice discards measurement results $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ without telling Bob what the result is, then the yield of the resulting EDP is worse than Eq. (6). Consequently, there seems to be no correspondence between the EDP and our proposed classical processing.

V. CONCLUSION

We proposed an information reconciliation protocol that uses two-way classical communication. For the BB84 and six-state protocols, the key rates of QKD protocols that use our information reconciliation protocol are higher than previously known protocols for a wide range of error rates. Furthermore, we showed the relation between the proposed protocol and the *B* step of [16] (Remark 2). We clarified why the key rate of our protocol is higher than those of [18,23,25] (Remark 3), and found that there does not seem to be any EDP that corresponds to our proposed QKD protocol.

ACKNOWLEDGMENTS

We would like to thank Dr. Manabu Hagiwara, Dr. Kentaro Imafuku, Professor Hideki Imai, Dr. Mitsugu Iwamoto, Dr. Takayuki Miyadera, Dr. Jun Muramatsu, Professor Hiroshi Nagaoka, Dr. Tomohiro Ogawa, and Professor Stefan Wolf for valuable discussions. This research was also partly supported by the Japan Society for the Promotion of Science under Grants-in-Aid No. 18760266 and No. 00197137.

[1] G. Brassard and L. Salvail, in *Advances of Cryptology—EUROCRYPT'93*, edited by T. Helleseth, Lecture Notes in Computer Science, Vol. 765 (Springer, Berlin, 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. Crepeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[4] C. H. Bennett and G. Brassard, in *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), pp. 175–179.
[5] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[6] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings on the 32nd Annual ACM Symposium of the Theory of Computing*, 2000 (unpublished), pp. 715–724.
[7] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, J. Cryptology **19**, 381 (2006).
[8] D. Mayers, J. ACM **48**, 351 (2001).
[9] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[10] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[11] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[12] H. K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
[13] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (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, e-print arXiv:quant-ph/0512258.
[16] D. Gottesman and H. K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[17] H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).
[18] X. Ma, C. H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H. K. Lo, Phys. Rev. A **74**, 032330 (2006).
[19] B. Kraus, C. Branciard, and R. Renner, Phys. Rev. A **75**, 012316 (2007).
[20] U. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[21] J. Bae and A. Acín, Phys. Rev. A **75**, 012334 (2007).
[22] A. Acín, J. Bae, E. Bagan, M. Baig, L. Masanes, and R. Munöz-Tapia, Phys. Rev. A **73**, 012327 (2006).
[23] Karl-Gerd H. Vollbrecht and F. Vestraete, Phys. Rev. A **71**, 062325 (2005).
[24] H. K. Lo, New J. Phys. **5**, 36 (2003).
[25] S. Watanabe, R. Matsumoto, and T. Uyematsu, in Proceedings of AQIS 2006, Beijing, China, 2006 (unpublished), pp. 11–12.
[26] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, in *Proceedings of the Fourth Theory of Cryptography Conference, Amsterdam, The Netherlands, 2007*, edited by P. Vadhan, Lecture Notes in Computer Science, Vol. 4392 (Springer, Berlin, 2007), pp. 456–478.
[27] See EPAPS Document No. E-PLRAAN-76-169708 for the proofs of Theorems 1 and 2. For more information on EPAPS, see http://www.aip.org/pubservs/epaps.html.
[28] I. Csiszár, IEEE Trans. Inf. Theory **28**, 585 (1982).
[29] M. Hamada, J. Phys. A **37**, 8303 (2004).
[30] R. G. Gallager, *Low Density Parity Check Codes* (MIT Press, Cambridge, MA, 1963).
[31] C. Berrou and A. Glavieux, IEEE Trans. Commun. **44**, 1261 (1996).
[32] R. Renner, e-print arXiv:quant-ph/0703069.
[33] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (John Wiley & Sons, New York, 2006).
[34] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Second Theory of Cryptography Conference TCC, Cambridge, MA, 2005*, edited by J. Kilian, Lecture Notes in Computer Science, Vol. 3378 (Springer, Berlin, 2005), pp. 386–406.
[35] R. Renner and R. Konig, in *Second Theory of Cryptography Conference TCC, Cambridge, MA 2005* (Ref. [34]), pp. 407–425.
[36] M. Hayashi, *Quantum Information: An Introduction* (Springer, Berlin, 2006).
[37] D. Slepian and J. K. Wolf, IEEE Trans. Inf. Theory **19**, 471 (1973).
[38] I. Devetak and A. Winter, Phys. Rev. A **68**, 042301 (2003).
[39] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2004).