Equivalence of three classical algorithms with quantum side information: Privacy amplification, error correction, and data compression

Toyohiro Tsurumaru

Abstract—Privacy amplification (PA) is an indispensable component in classical and quantum cryptography. Error correction (EC) and data compression (DC) algorithms are also indispensable in classical and quantum information theory. We here study these three algorithms (PA, EC, and DC) in the presence of quantum side information, and show that they all become equivalent in the one-shot scenario. As an application of this equivalence, we take previously known security bounds of PA, and translate them into coding theorems for EC and DC which have not been obtained previously. Further, we apply these results to simplify and improve our previous result that the two prevalent approaches to the security proof of quantum key distribution (QKD) are equivalent. We also propose a new method to simplify the security proof of QKD.

Index Terms—Data compression, error correction, privacy amplification, quantum cryptography, quantum information theory.

I. Introduction

Privacy amplification (PA) algorithms is an indispensable component in classical and quantum cryptography [1], [2], [3], [4]. The goal of PA is to generate a random bit string that is completely unknown to outside, from a bit string which may be partially leaked to outside. On the other hand, error correction (EC) and data compression (DC) algorithms are also indispensable in classical and quantum information theory [5].

We here study these three algorithms (PA, EC, and DC), in the presence of quantum side information, and show that they all become equivalent in the one-shot scenario.

The equivalence here means that the following two conditions are satisfied: 1) If one chooses any one of the three algorithms (PA, EC and DC) and its input, the remaining two algorithms and their inputs are also determined uniquely and automatically, and 2) The security or the performance indices of the three algorithms thus determined are all equal (see Sec. IV for the rigorous statements). This means that these three algorithms are in fact a single algorithm viewed from different angles.

Also, by generalizing this result to randomized algorithms, we show the equivalence between a security evaluation method for PA (called the leftover hashing lemma, LHL), and the coding theorems for EC and DC. From a practical viewpoint,

The author is with Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa, 247-8501, Japan (e-mail: Tsurumaru.Toyohiro@da.MitsubishiElectric.co.jp). This paper was presented in part at the 43rd Quantum Information Technology Symposium (QIT43), held online, Dec. 10-11, 2020, and at a poster session of QCrypt 2021 Conference, held online, Aug. 23-27, 2021.

this means, e.g., that if one wishes to improve PA algorithms used for quantum cryptography, it suffices to improve DC or EC algorithms instead, and vice versa.

The equivalence is made possible by modifying these three algorithms in the following three points:

First, we consider the generalized cases where there is quantum side information: In PA, information leaked to the eavesdropper is not necessarily classical but quantum [1], [6]. In EC and in DC, the decoder can use an auxiliary quantum state, in addition to the classical codeword or the usual classical compressed data [7], [8].

Second, in order to evaluate the security of PA, we use a relatively new security index put forward by König et al. [9] based on the purified distance [10], while most literature use the conventional criterion called the ε-security (see e.g. Ref. [1]), based on the trace distance. We stress that we do not lose the security essentially by using this new criterion; see Section III-A3 for details.

Third, we restrict hash functions used for PA, and codes used for PA and EC to be linear.

We also demonstrate the usefulness of this equivalence with two applications:

First, we take previously known security bounds (i.e., LHLs) of PA, and convert them into new coding theorems for EC and DC with quantum side information. Specifically, we consider three types of hash functions F which are widely used for PA, namely, the universal$_2$ [11], the *almost* universal$_2$ [12], and the *almost dual* universal$_2$ functions [13], [14]. Then we convert their LHLs into the coding theorems of EC and DC using the dual function of F. To the best of our knowledge, these coding theorems are new results that have not been obtained previously.

Second, we apply these results to the security proof of quantum key distribution (QKD) [15]. In the field of QKD, there are two major approaches to the security proof, called the leftover hashing lemma (LHL)-based approach [1], and the phase error correction (PEC)-based approach [16], [17], [18], [19], [20]. Previously, we have shown that these two approaches are in fact equivalent mathematically [8]. In this paper, we simplify and improve this proof by exploiting the equivalence of the three algorithms (PA, EC, and DC). The proof here is improved in that it is valid for a larger class of hash functions; that is, the equivalence holds for the case where the random function F for PA is *almost* universal$_2$ and *almost dual* universal$_2$, while previously we treated only the case of universal$_2$ [8].

Further, utilizing the knowledge gained in this new proof, we propose a method to simplify the PEC-based proof. That is, we propose to evaluate the randomness of Alice's phase degrees of freedom by the smooth max-entropy, rather than by the phase error rate. This method has an additional merit that every step of the proof becomes equivalent to that of the corresponding LHL-based proof. As a result, one is guaranteed to reach exactly the same security bound as in the LHL-based approach, without any extra factor.

The relations between results of the present manuscript and the existing literature are as follows:

In Refs. [21], [22], Renes and coauthors studied PA and DC in the independent and identically distributed (i.i.d.) setting, not in the one-shot scenario, and showed that their asymptotic rates are equal. Renes refined these results in more recent papers [23], [24], and showed that PA and DC are equivalent in the one-shot scenario using a fixed (not randomized) code (Ref. [23], Corollary 11). This corresponds to a limited case of Theorem 1 of the present manuscript. In comparison, our contributions here are the extension of this equivalence that includes EC (Theorem 1), and all the results after that, such as (i) we generalized Theorem 1 further to random codes, and showed the equivalence of LHL for PA and the coding theorems for DC and EC (Theorems 2 and 3), (ii) obtained explicit forms of equivalent pairs of an LHL and a coding theorem for practical cases including the universal$_2$ hash function (Section V), and (iii) showed how these results can simplify and improve the security proof of QKD (Section VI).

We also note that our main result here can be considered as a refinement of the results of our previous paper [8]. Previously, we have shown the leftover hashing lemmas (LHLs) can be derived from a coding theorem of EC with quantum side information [8]. On the other hand, in the present manuscript, we demonstrate that PA and EC are not only directly connected, but are in fact equivalent, if we define the security of PA using the purified distance, instead of the trace distance which has been widely used. In addition, we also prove that DC with quantum side information is also equivalent to these two algorithms.

II. NOTATION

All the rules below apply to alphabets besides A, U and V.

A. Random variables and the Hilbert spaces

We denote random variables by a capital letter, such as A. The same capital letter will also be used to denote the Hilbert space where the random variable is stored, unless otherwise specified. For example, if a random variable, A, is already defined and if we speak of Hilbert space A, it means that random variable A is stored in Hilbert space A (for examples of this notation, see Refs. [1], [10]).

B. Use of tilde

If a random variable A takes value a, and if it is stored in the z basis, we write the situation as $|a\rangle_A$ without tilde; and if stored in the x basis, we write it as $|\tilde{a}\rangle_A$ with tilde.

To put it more precisely: We denote the Pauli matrices in the z and the x bases by σ_Z and σ_X respectively[1]. We denote eigenstates of σ_Z and σ_X in a qubit space by $|z\rangle$ and $|\tilde{x}\rangle$ respectively; i.e., $\sigma_Z |z\rangle = (-1)^z |z\rangle$ and $\sigma_X |\tilde{x}\rangle = (-1)^x |\tilde{x}\rangle$ with $z, x \in \{0,1\}$. We also extend this notation to multi-qubit space with length l, and write $|z\rangle = |z_1\rangle \otimes \cdots \otimes |z_l\rangle$ and $|\tilde{x}\rangle = |\widetilde{x_1}\rangle \otimes \cdots \otimes |\widetilde{x_l}\rangle$ for $z = (z_1, \ldots, z_l), x = (x_1, \cdots, x_l) \in \{0,1\}^l$.

C. Classical states

Given any quantum state ρ_U in a space U, we denote by Z^U the random variable that results from the z-basis measurement in U, and by ρ_{Z^U} the resulting state; see, e.g., Ref. [7].

In this notation, when given a state ρ_{UV}, the result of z basis measurement on space U takes the form

$$\rho_{Z^U V} = \sum_z (|z\rangle \langle z|_U \otimes \mathbb{I}_V) \rho_{UV} (|z\rangle \langle z|_U \otimes \mathbb{I}_V), \quad (1)$$

with $\mathbb{I}$ being the identity operator. We say that ρ_{UV} is *classical in Z^U* if $\rho_{UV} = \rho_{Z^U V}$, i.e., if ρ_{UV} is invariant under the Z^U-measurement (or informally, if U is already measured in the z basis).

We also use the same notation for the x basis; e.g., ρ_{UV} is classical in X^U if $\rho_{UV} = \rho_{X^U V}$.

D. Distance measures and entropies

A state ρ is called sub-normalized if $\text{Tr}(\rho) \leq 1$. The L_1 norm of a matrix A is $\|A\|_1 := \text{Tr}(\sqrt{AA^\dagger})$. For two sub-normalized states ρ, σ, the generalized fidelity is $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1 + \sqrt{(1 - \text{Tr}(\rho))(1 - \text{Tr}(\sigma))}$, and the purified distance is $P(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2}$. We say that ρ, σ are ε-close and write $\rho \approx_\varepsilon \sigma$, if $P(\rho, \sigma) \leq \varepsilon$ (see e.g. Ref. [10]).

The conditional min- and max-entropies of a sub-normalized state ρ_{UV} are

$$H_{\min}(U|V)_\rho$$
$$:= -\log \min_{\sigma \geq 0} \{\text{Tr}(\sigma) : \rho_{UV} \leq \mathbb{I}_U \otimes \sigma_V\}, \quad (2)$$

$$H_{\max}(U|V)_\rho$$
$$:= \max_{\sigma \geq 0, \text{Tr}(\sigma)=1} \log_2(|\mathcal{U}| F(\rho_{UV}, |\mathcal{U}|^{-1} \mathbb{I}_U \otimes \sigma_V)^2), \quad (3)$$

where $\mathcal{U}$ denotes the domain (alphabets) of random variable U, and $|\mathcal{U}|$ its cardinality. Their smoothed versions are

$$H_{\min}(U|V)_\rho^\varepsilon := \max_{\bar{\rho}} H_{\min}(U|V)_{\bar{\rho}}, \quad (4)$$

$$H_{\max}(U|V)_\rho^\varepsilon := \min_{\bar{\rho}} H_{\max}(U|V)_{\bar{\rho}}, \quad (5)$$

where the maximum and the minimum are evaluated for sub-normalized states $\bar{\rho}_{UV} \approx_\varepsilon \rho_{UV}$ (see e.g. Ref. [10]).

III. THREE ALGORITHMS TO BE CONSIDERED

In this section, we specify three algorithms to be considered in this paper: Privacy amplification (PA), error correction (EC), and data compression (DC). In the next section, these three algorithms will be shown equivalent to each other.

---

[1]It is straightforward to generalize all our results below to the mutually unbiased bases (MUB) in prime power dimensions. However for the sake of simplicity, in this paper we limit ourselves with the case of qubits.
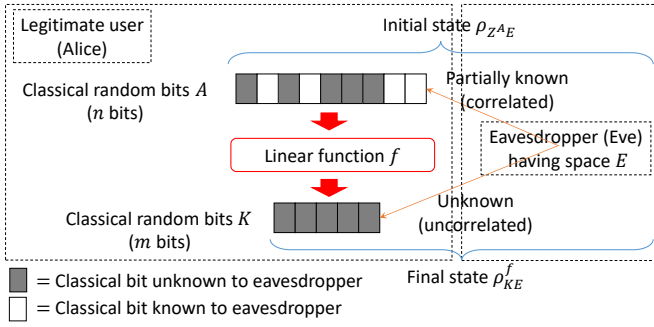
Fig. 1. Privacy amplification (PA) against quantum side information. Initially, Alice's bit string Z^A is partially known to the Eve; i.e., Eve has a quantum side information in space E, which is correlated with Z^A. By applying a linear function f, Alice attempts to convert Z^A into a bit string K, which is unknown to Eve.

A. Privacy amplification (PA) against quantum side information

Privacy amplification (PA) is an algorithm for extracting a secret random bits, from a bit string which may be partially leaked outside (Fig. 1) [1], [6], [2], [3].

1) Description of the algorithm: By definition, A PA algorithm starts with a situation where the legitimate user, Alice, has a classical information $z \in \{0,1\}^n$, and the eavesdropper, Eve, has a quantum state (quantum side information) ρ^z correlated with z. That is, there is initially a classical-quantum (cq) state,

$$\rho_{Z^A E} = \sum_z |z\rangle \langle z|_A \otimes \rho_E^z, \qquad (6)$$

where Hilbert spaces A and E describe Alice's and Eve's degrees of freedom, respectively. Then Alice applies a linear function $f : \{0,1\}^n \to \{0,1\}^m$ to z and generates a random bits $k = f(z)$. The function f used in this context of PA is often called a *hash function*. As a result, random bits K and Eve end up in a state

$$\rho_{KE}^f := \rho_{f(Z^A)E} = \sum_k |k\rangle \langle k|_K \otimes \sum_{z \in f^{-1}(k)} \rho_E^z, \qquad (7)$$

where k is the output of function f, and K is the Hilbert space for storing k.

2) Security criteria of PA: We say that random bits K is ideally secure, if it is uniformly distributed and completely unknown to Eve, i.e., if $\rho_{KE}^f = 2^{-m}\mathbb{I}_K \otimes \sigma_E$ for a normalized state σ. However, such ideal state is unrealistic in practice. Thus it is customary to define the security by the distance between the actual state ρ_{KE}^f and the ideal state $2^{-m}\mathbb{I}_K \otimes \sigma_E$.

In this paper, we particularly follow König et al. [9] and measure the security by an index

$$
\begin{aligned}
Q^{\mathrm{PA},f}(\rho_{Z^A E}) &:= \mathrm{Tr}(\rho_{Z^A E}) - 2^{H_{\max}(f(Z^A)|E)_\rho - m} \\
&= \mathrm{Tr}(\rho_{KE}^f) - 2^{H_{\max}(K|E)_{\rho^f} - m}. \qquad (8)
\end{aligned}
$$

The idea here is to measure the distance between the actual and ideal states by the square of the purified distance. Note that if $\rho_{Z^A E}$ is normalized, $Q^{\mathrm{PA},f}(\rho_{Z^A E})$ indeed equals the squared purified distance between the two states. For the general case where $\rho_{Z^A E}$ is not necessarily normalized, $Q^{\mathrm{PA},f}(\rho_{Z^A E})$ is defined to scale proportionally to $\mathrm{Tr}(\rho_{Z^A E})$.

3) Justification for using the new index $Q^{\mathrm{PA},f}$:

a) Conventional criterion: On the other hand, in fact, most existing literature on PA do not use the security index $Q^{\mathrm{PA},f}$ of (8). They rather use an alternative index

$$d_1(\rho_{KE}^f) := \left\| \rho_{KE}^f - 2^{-m}\mathbb{I}_K \otimes \rho_E \right\|_1 \qquad (9)$$

based on the trace distance, and say that random number K is ε-secure if $\frac{1}{2}d_1(\rho_{KE}^f) \leq \varepsilon$ (e.g. Ref. [1]). This criterion, ε-security, is prevalent because it is explicitly shown to satisfy a desirable property called the universal composability [25].

Even so, our use of a rather new criterion, $Q^{\mathrm{PA},f}$, can be justified by the following two observations.

b) ε-security using the new index $Q^{\mathrm{PA},f}$: The ε-security can also be guaranteed by using $Q^{\mathrm{PA},f}(\rho_{Z^A E})$. This is because $Q^{\mathrm{PA},f}(\rho_{Z^A E})$ bounds $d_1(\rho_{KE}^f)$ as

$$d_1(\rho_{KE}^f) \leq 4\sqrt{\mathrm{Tr}(\rho)}\sqrt{Q^{\mathrm{PA},f}(\rho_{Z^A E})} \qquad (10)$$

(see Appendix B for the proof).

c) Tightness of security bounds: Bounds on $Q^{\mathrm{PA},f}$ thus obtained are nearly as tight as previously obtained bounds on $d_1(\rho_{KE}^f)$ in many practical situations.

For example, if we let function f be a random function called the universal$_2$ function [11], and denote it by capital letter F (see Section IV-B for details of this notation), then we have

$$\mathrm{E}_F \, Q^{\mathrm{PA},F}(\rho_{Z^A E}) \leq 2^{m - H_{\min}(Z^A|E)_\rho}, \qquad (11)$$

where the expected value E_F is taken on the ensemble of random function F (Lemma 12 of Ref. [8], or Lemma 4 of the present paper). If we further apply (10) and Jensen's inequality to (11), we obtain

$$\mathrm{E}_F \, d_1(\rho_{KE}^F) \leq 4\sqrt{\mathrm{Tr}(\rho)}\sqrt{2^{m - H_{\min}(Z^A|E)_\rho}}, \quad (12)$$

which differs only by a factor of 4 from the well-known bound called the leftover hashing lemma (LHL, or Theorem 5.5.1 of Ref. [1]. Later, we will derive it again as Eq. (49)). Note that this factor 4 is harmless in practice, since it can be compensated for by reducing the length of random bits m only by 4 bits.

In Section V, we will also show that similarly tight bounds can be obtained for almost universal$_2$ [12] and almost *dual* universal$_2$ hash functions [13], [14].

4) LHLs of the conventional type and of the new type: In the past literature, an LHL always meant a bound on an average of the conventional security index, $\mathrm{E}_F \, d_1(\rho_{KE}^F)$. In this paper, we extend this terminology and use the word LHL to also mean a bound on an average of the new security index, $\mathrm{E}_F \, Q^{\mathrm{PA},F}(\rho_{Z^A E})$ (e.g. (11)). When we need to distinguish between these two types, we call the former an LHL of the conventional type, and the latter the new type.

We do not claim that the new security index based on $Q^{\mathrm{PA},F}$ is either best or proper. The main motivation for using this index here is to clarify the equivalence of PA and other two algorithms, EC and DC, defined below.

B. Error correction (EC) with quantum side information

Next we introduce a generalized form of classical error correction (EC), which we call *EC with quantum side information* (Fig. 2). This is identical to what we called the *generalized error correction* in Ref. [8], but in this paper we will use the name above to clarify the relation with the data compression algorithm to be discussed in the next subsection. From now on, whenever we say EC, we mean this generalized form.

In a conventional classical EC algorithm [5], the sender chooses a message $t \in \{0,1\}^m$ and generates the corresponding codeword $c(t) \in \{0,1\}^n$. The string $c(t)$ is then sent through a noisy channel, and output as a string x, which is $c(t)$ with bit flips applied probabilistically. The receiver then decodes x to recover $c(t)$.

On the other hand, in our EC with quantum side information, codeword $c(t)$ is sent through a noisy quantum channel and output as a cq state $\rho^{c(t)} = \sum_x |\tilde{x}\rangle \langle \tilde{x}| \otimes \tilde{\rho}^{c(t),x}$; see Fig. 2. Or equivalently as a classical string x *plus* an auxiliary quantum state (quantum side information) $\tilde{\rho}^{c(t),x}$, where the tilde indicates that it is an expansion of $\rho^{c(t)}$ with respect to $|\tilde{x}\rangle$. Hence, it is possible that the decoding succeeds with a higher probability, due to information (i.e. hint) obtained by measuring $\tilde{\rho}^{c(t),x}$. Details are as follows.

1) Description of the algorithm: For the sake of similicity, we assume that the channel is symmetric under bit flips (i.e., binary symmetric channel). We also assume that the error correcting code $C \subset \{0,1\}^n$ is linear, i.e., a linear $[n,m]$ code. We denote its linear syndrome function by $g : \{0,1\}^n \to \{0,1\}^{n-m}$.

a) Encoding and sending: The sender chooses an message $m \in \{0,1\}^m$, and the classical codeword $c(t) \in C$ that corresponds to it.

b) Quantum channel: The codeword $c(t)$ is input to the quantum channel and then output as a cq state $\rho^{c(t)} = \sum_x |\tilde{x}\rangle \langle \tilde{x}| \otimes \tilde{\rho}^{c(t),x}$. Or equivalently it is output as a classical string x plus an auxiliary quantum state $\tilde{\rho}^{c(t),x}$.

c) Decoding: The receiver performs the following decoding algorithm using x and $\tilde{\rho}^{c(t),x}$.

1) Calculate the syndrome $s = g(x) \in \{0,1\}^{n-m}$.
2) Measure $\tilde{\rho}^{c(t),x}$ using positive operator valued measures (POVMs) which depend on s; that is, $M^s = \{M^{s,e} \mid e \in \{0,1\}^n\}$ satisfying $\sum_e M^{s,e} = \mathbb{I}$. The result e is the estimated error pattern.
3) Output $y = x + e$ as the estimated codeword.

2) Performance index: We say that the decoding is successful when its output y equals the correct codeword $c(t)$; i.e., $\Pr[\text{EC succeeds}] := \Pr[Y = c(T)]$. We then define the performance index of our EC to be its failure probability (block error rate) when using the best decoder,

$$Q^{\text{EC},g} := \min_{\{M^s\}} \Pr[Y \neq c(T)]. \qquad (13)$$

As we here limit ourselves with a BSC, we have

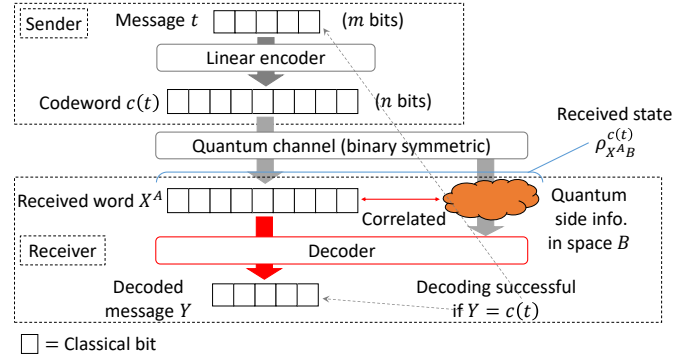$$\tilde{\rho}^{c(t)+\Delta,x+\Delta} = \tilde{\rho}^{c(t),x} \qquad (14)$$

Fig. 2. Error correction (EC) with quantum side information. The sender uses a linear classical error correcting code C, and we denote its syndrome function by g. Note that the situation becomes the same as in the conventional classical error correction, if the quantum side information (orange cloud) is absent.

for any $\Delta \in \{0,1\}^n$. Hence, as we also limit ourselves with a linear code C, it suffices to consider $Q^{\text{EC},g}$ for conditioned on message $t = 0$ and the codeword $c(0) = 0$; that is,

$$
\begin{aligned}
Q^{\text{EC},g}(\rho^0_{X^A B}) &= \min_{\{M^s\}} \Pr[Y \neq 0 \mid T = 0] \\
&= \min_{\{M^s\}} \Pr[Y \neq 0 \mid \rho^0_{X^A B}], \qquad (15)
\end{aligned}
$$

where

$$\rho^0_{X^A B} = \sum_x |\tilde{x}\rangle \langle \tilde{x}|_A \otimes \tilde{\rho}^{0,x}_B \qquad (16)$$

denotes the output of the quantum channel on input $c(0) = 0$. As remarked in Section II-B, $|\tilde{x}\rangle$ appearing in (16) means that the channel output x is encoded in the x basis. We stress that we lose no generality by using this particular choice of the basis; see Section III-D.

In what follows, for ease of notation, we will often omit superscript 0 of $\rho^0_{X^A B}$ and $\tilde{\rho}^{0,x}_B$, and write

$$\rho_{X^A B} = \rho^0_{X^A B}, \quad \tilde{\rho}^x_B = \tilde{\rho}^{0,x}_B. \qquad (17)$$

In this notation, Eq. (16) is rewritten as

$$\rho_{X^A B} = \sum_x |\tilde{x}\rangle \langle \tilde{x}|_A \otimes \tilde{\rho}^x_B, \qquad (18)$$

and the performance index (15) can also regarded a function of $\rho_{X^A B}$,

$$Q^{\text{EC},g}(\rho_{X^A B}) = Q^{\text{EC},g}(\rho^0_{X^A B}). \qquad (19)$$

3) Relation with classical EC with quantum decoder in the past literature: The EC defined above is a limitation of classical EC with quantum decoder, which has been discussed in various literatures (see e.g. Ref. [15], Section 12.3 for the asymptotic case, and [26] for non-asymptotic cases). The past literature and this paper are the same up to the point where the quantum channel receives codeword $c(t)$ and outputs a quantum state $\rho^{c(t)}$. On the other hand, while $\rho^{c(t)}$ are general quantum state in the past literature, we here assume that $\rho^{c(t)}$ are cq states satisfying BSC condition (14).

The main motivation for considering such restricted form of EC is its application to the security proof of QKD, whose details will be given in Section VI. A. 4. To give a quick
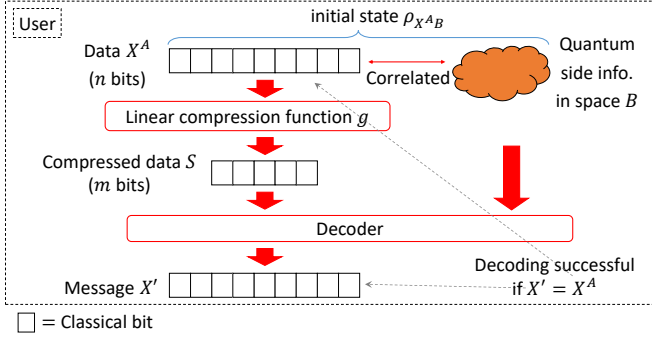
Fig. 3. Data compression (DC) with quantum side information. Note that the situation becomes the same as in the conventional classical data compression using compression function g, if the quantum side information (orange cloud) is absent.

overview: In the phase error correction (PEC)-based approach of the QKD security proof, one can benefit by considering EC on a purification $|\rho\rangle_{ABE}$ (virtual state) of the actual state $\rho_{Z^A E}$, instead of dealing with $\rho_{Z^A E}$ directly. This naturally gives rise to EC as defined above, where the additional information from the (virtual) ancilla space B improves the performance of EC (and thus also improve the security of QKD).

C. Data compression (DC) with quantum side information

Similarly, a generalization of classical data compression (DC) is known, called *DC with quantum side information* (Fig. 3); see Ref. [27] for the original definition, and Refs. [7], [10], [22], [23], [28] for recent results on one-shot and non-asymptotic cases. From now on, whenever we say DC, we mean this generalized type.

In a conventional classical DC algorithm [5], given a classical data $x \in \{0,1\}^n$, one generates the corresponding compressed data $g(x) \in \{0,1\}^m$, using a compression function g, and stores it. After some time passes, one decodes $g(x)$ to restore x.

On the other hand, in DC with quantum side information (Fig. 3) [27], [7], [10], [23], [22], [28], there is an additional set of sub-normalized quantum states (quantum side information) $\tilde{\rho}^x$ which correspond to x and satisfy $\sum_x \operatorname{Tr}\tilde{\rho}^x = 1$. The user can store $\tilde{\rho}^x$ along with the classical compressed data $g(x)$, and also use it for decoding. Thus, as in the EC algorithm of the previous subsection, it is possible that the decoding succeeds with a higher probability, due to information (i.e. hint) obtained by measuring $\tilde{\rho}^x$. Details are as follows.

1) Description of the algorithm: For the sake of simplicity, we assume that the compression function $g : \{0,1\}^n \to \{0,1\}^m$ is linear.

a) Encoding: Choose variable x with probability $\Pr[X^A = x] = \operatorname{Tr}(\tilde{\rho}^x)$. Then output the compressed data $s = g(x)$ of x, along with the corresponding quantum side information $\tilde{\rho}^x$.

b) Decoding: Receive $s \in \{0,1\}^{n-m}$ and state $\tilde{\rho}_B^x$ as inputs. Measure $\tilde{\rho}_B^x$ using a POVM $M^s = \{M^{s,e} \mid e \in \{0,1\}^n\}$, and output $x' = e$ as the estimated value of x.

2) Performance index: We say that the decoding is successful when its output x' equals the correct data x; $\Pr[\text{DC succeeds}] = \Pr[X' = X^A]$. We then define the performance index of DC with quantum side information to be its failure probability when using the best decoder,

$$Q^{\mathrm{DC},g}(\{\tilde{\rho}^x\}) := \min_{\{M^s\}} \Pr[X' \neq X^A \mid \{\tilde{\rho}^x\}] \qquad (20)$$

If we particularly choose to encode the classical data x in the x basis, then the correlation between x and $\tilde{\rho}^x$ can be represented by a single quantum state $\rho_{X^A B} = \sum_x |\tilde{x}\rangle \langle \tilde{x}| \otimes \tilde{\rho}^x$, which has the identical form to the state $\rho_{X^A B}$ of (18), which is used in EC. That is, though $\rho_{X^A B}$ was originally introduced to describe the quantum channel of EC, it can also be regarded as describing the initial state of DC. In this notation, the probability $Q^{\mathrm{DC},g}$ of (20) can be considered as a function of $\rho_{X^A B}$,

$$\begin{aligned} Q^{\mathrm{DC},g}(\{\tilde{\rho}^x\}) &= Q^{\mathrm{DC},g}(\rho_{X^A B}) \\ &= \min_{\{M^s\}} \Pr[X' \neq X^A \mid \rho_{X^A B}]. \end{aligned} \qquad (21)$$

D. Note on the basis choices of the classical information

In the specification of algorithms above, for each algorithm we assigned different orthogonal bases for encoding the classical variable z or x: Variable z in PA is encoded in the z basis (without tilde), whereas variable x in EC and DC is encoded in the x basis (with tilde).

We note that we chose these particular bases solely for the purpose of simplifying the discussion of the following sections, where we prove the equivalence of the three algorithms. We stress that we have no other reason for these particular choices. For example, when one implements any one of the three algorithms in practice, one can use an arbitrary orthogonal basis for encoding classical variables, even besides the z and the x bases.

IV. MAIN RESULTS

Next we present the two main results of this paper.

The first result is that all three algorithms described above are actually equivalent. That is, if any one of the three is specified, the other two can also be defined uniquely, and in addition, their indices, Q^{PA}, Q^{EC}, Q^{DC}, are all equal.

The second result is that an leftover hashing lemma (LHL) for PA and coding theorems for EC and DC with quantum side information, are also equivalent. That is, given either an LHL for PA, or a coding theorem for EC or DC, one can also derive the other two propositions (LHL or coding theorem) uniquely, and the three propositions thus obtained are all equivalent.

A. Equivalence of the three algorithms

1) Definition of the equivalence: By the equivalence of the three algorithms, we mean the following two conditions:

I. **Correspondence between the three types of algorithms:** If one specifies any one of the three algorithms (PA, EC and DC) and its input, the other two algorithms and their inputs are also specified uniquely and automatically.

Here, to "specify an algorithm" means to fix the function f or g, which is used for the classical data processing[2]. To "specify the input to an algorithm" is to fix the state $\rho_{Z^A E}$ or $\rho_{X^A B}$, which determines the initial state or the environment of the algorithm.

II. **Equality of three indices:** The indices of the three algorithms thus specified (i.e., $Q^{\mathrm{PA},f}(\rho_{Z^A E})$, $Q^{\mathrm{EC},g}(\rho_{X^A B})$, and $Q^{\mathrm{DC},g}(\rho_{X^A B})$) are all equal.

Condition I says that, once the hash function f and the input $\rho_{Z^A E}$ for PA are fixed, then the function g and the input $\rho_{X^A B}$ for EC (or for DC) are also fixed automatically; and vice versa. This correspondence will be defined explicitly in Section IV-A2.

Condition II says that once the analysis is finished for the security or the failure probability of any one of the three algorithms, then analyses for the other two algorithms become no longer necessary, since we know that they always give the same result. From a practical viewpoint, this means, for example, that if one wishes to improve PA algorithms used for quantum cryptography, it suffices to improve DC or EC algorithms instead; and vice versa. This equality will be shown in Section IV-A3.

In short, there is a correspondence between the three types of algorithms, and the triplet of algorithms connected by this correspondence share the same value of indices Q. This means that the triplet of algorithms are in fact a single algorithm viewed from different angles. Thus we call it the the equivalence of the three types of algorithms.

2) Correspondence between the three types of algorithms (Condition I): Here we explicitly define the correspondence mentioned in Condition I above. That is, we show that if one specifies the classical function (i.e., f or g) and the input (i.e., ($\rho_{Z^A E}$ or $\rho_{X^A B}$) for any one of the three algorithms (PA, EC and DC), then the function and the input for the other two algorithms are also specified uniquely and automatically.

a) Correspondence between f and g (dual functions): Given either one of functions f and g, one can choose the other function to be the *dual* function in the following sense.

Definition 1 (Dual function pair [14], [29]). *Suppose a pair of linear functions $f : \{0,1\}^n \to \{0,1\}^m$ and $g : \{0,1\}^n \to \{0,1\}^{n-m}$ is given, and can be written $f(x) = fx^T$, $g(x) = gx^T$ using $m \times n$ matrices f, g. Also suppose that functions f, g are both surjective (i.e., matrices f, g are of full rank). We say that functions f, g are dual, if the corresponding matrices f, g satisfy $fg^T = 0$.*

We will often write $f \perp g$ or $g = f^\perp$ or $f = g^\perp$, to say that f, g are dual.

Note that we do not lose generality by restricting f and g to be surjective. A non-surjective f or g can always be modified to be surjective by discarding some of its output bits, and this modification does not affect the indices of the corresponding algorithm, Q^{PA}, Q^{EC}, and Q^{DC}.
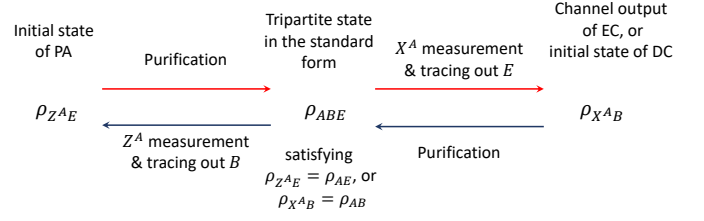

Fig. 4. Standard form of tripartite states: The state $\rho_{Z^A E}$ that specifies the PA algorithm, and the state $\rho_{X^A B}$ that specifies EC and DC can be converted to each other uniquely, as shown above (cf. Section IV-A2). In these processes, one also obtains a pure tripartite state ρ_{ABE} satisfying the condition $\rho_{AE} = \rho_{Z^A E}$ or $\rho_{AB} = \rho_{X^A B}$. For later convenience, we call this type of ρ_{ABE} the standard form (see Definition 2).

b) Correspondence between $\rho_{Z^A E}$ and $\rho_{X^A B}$ (standard form of tripartite states): Given either one of states $\rho_{Z^A E}$ and $\rho_{X^A B}$, one can always define the other state uniquely by the following procedure (Fig. 4).

1) Define a tripartite pure state ρ_{ABE} by purifying $\rho_{Z^A E}$ or $\rho_{X^A B}$.
   (E.g., if $\rho_{Z^A E}$ is given, introduce ancilla space B and let ρ_{ABE} such that $\rho_{Z^A E} = \mathrm{Tr}_B(|\rho\rangle \langle\rho|_{ABE})$.)
2) Trace out the unnecessary one of spaces B and E.
3) Measure space A in the appropriate basis, of the z and x bases.
   (E.g., in order to obtain $\rho_{X^A B}$, perform the X^A-measurement on $\rho_{AB} = \mathrm{Tr}_E(|\rho\rangle \langle\rho|_{ABE})$.)

In what follows, we will often refer to this procedure as T [3]. The pure state ρ_{ABE} obtained in this procedure satisfies $\rho_{AE} = \rho_{Z^A E}$ or $\rho_{AB} = \rho_{X^A B}$ by definition. For later convenience, we call this type of ρ_{ABE} the *standard form*.

Definition 2 (Standard form of tripartite states; Fig. 4). *We say that a sub-normalized tripartite state ρ_{ABE} is in the standard form, if it is pure, and satisfies either one of the conditions below,*

- ρ_{AE} is classical in Z^A (i.e., $\rho_{AE} = \rho_{Z^A E}$),
- ρ_{AB} is classical in X^A (i.e., $\rho_{AB} = \rho_{X^A B}$).

3) Equality of three indices (Condition II): Next we prove the equality of the indices of the three algorithms thus specified (Condition II of Section IV-A1). We also show that they can all be expressed by the conditional min- and max-entropies.

Theorem 1 (Equality of the indices; Fig. 5.). *For a dual pair of functions, f and g ($= f^\perp$), and for a sub-normalized state ρ_{ABE} in the standard form,*

$$
\begin{aligned}
Q^{\mathrm{PA},f}(\rho_{Z^A E}) &= Q^{\mathrm{EC},g}(\rho_{X^A B}) = Q^{\mathrm{DC},g}(\rho_{X^A B}) \\
&= \mathrm{Tr}(\rho) - 2^{H_{\max}(f(Z^A)|E)_\rho - m} \\
&= \mathrm{Tr}(\rho) - 2^{-H_{\min}(X^A|B, g(X^A))_\rho}. \quad (22)
\end{aligned}
$$

---

[2]It is straightforward to see that an PA algorithm can be specified uniquely by fixing the function f; and that an DC algorithm can be specified by g. An EC algorithm can also be specified uniquely by the linear syndrome function g, as g determines the corresponding linear error correcting code C, up to unessential linear transformations on input variable x

[3]In fact, applying T twice in a row does not output the original state, e.g. $T(T(\rho_{Z^A E})) \neq \rho_{Z^A E}$, but this fact does not compromise our correspondence of the states. This is because the state $T(T(\rho_{Z^A E}))$ and $\rho_{Z^A E}$ can be regarded equivalent as long as PA is concerned, and similarly, $T(T(\rho_{X^A B}))$ and $\rho_{X^A B}$ are equivalent as long as DC or EC is concerned. Details are given in Appendix C.
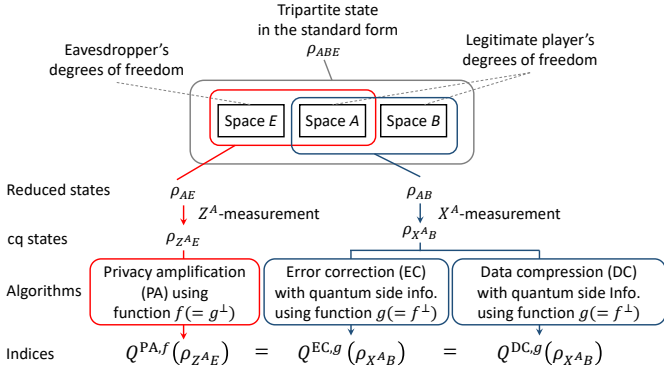
Fig. 5. Equality of three indices: The indices Q^{PA}, Q^{EC}, Q^{DC} of the three algorithms are equal (Section IV-A3), if their inputs $\rho_{Z^A E}$ and $\rho_{X^A E}$ are related via tripartite state ρ_{ABE} in the standard form (cf. Fig. 4), and if functions f and g are dual (cf. Definition 1).

In other words, evaluating the security of PA is equivalent to evaluating the performances of EC and DC. The proof of this theorem is given in Appendix A.

We note that Renes has already shown part of Theorem 1, the equivalence of PA and DC (Ref. [23], Corollary 11). Thus our contribution in Theorem 1 is that we extended the equivalence to also include EC.

B. Random functions F, G

Next suppose that one chooses function f (or g) randomly from a given set $\mathcal{F}$ (or $\mathcal{G}$) with a given probability $p(f)$ (or $q(g)$), every time one executes the algorithm. This corresponds to the case where one uses a random hash function in PA, or a random code in EC and DC.

Even in this setting, Theorem 1 is true, as long as f and g are randomized in such a way that their duality is maintained. Details are as follows.

In order to simplify the notation of these random functions f, g, from now on, we will consider them as random variables and write them in uppercase F, G. In this notation, the occurrence probability of f, for example, is denoted $\Pr[F = f] = p(f)$, and the expected value of $r(f)$, a function r of f, is $\mathrm{E}_F r(F) = \sum_{f \in \mathcal{F}} p(f) r(f)$. The same is true for function g.

Then we say that a pair of random functions F, G is dual, if they are chosen randomly with their duality (in the sense of Definition 1) maintained; that is,

Definition 3. *We say that a pair of random functions F, G is dual, if they are chosen from sets of the same size, $\mathcal{F} = \{f_1, f_2, \dots\}$, $\mathcal{G} = \{g_1, g_2, \dots\}$, respectively, and if each function pair f_i, g_i is dual (in the sense of Definition 1) and is chosen with the same probability, i.e.,*

$$f_i \perp g_i \text{ and } \Pr[F = f_i] = \Pr[G = g_i] \text{ for } \forall i. \quad (23)$$

We also write $F \perp G$ or $G = F^\perp$ or $F = G^\perp$, if F, G are dual.

By using this notation, we can state an averaged version of Theorem 1 as follows.

Corollary 1. *Let F, G be a pair of dual random functions, and ρ_{ABE} be a sub-normalized state in the standard form, then*

$$
\begin{aligned}
& \mathrm{E}_F \, Q^{\mathrm{PA},F}(\rho_{Z^A E}) \\
&= \mathrm{E}_G \, Q^{\mathrm{EC},G}(\rho_{X^A B}) = \mathrm{E}_G \, Q^{\mathrm{DC},G}(\rho_{X^A B}) \\
&= \mathrm{Tr}(\rho) - \mathrm{E}_F \, 2^{H_{\max}(F(Z^A)|E)_\rho - m} \\
&= \mathrm{Tr}(\rho) - \mathrm{E}_G \, 2^{-H_{\min}(X^A|B, G(X^A))_\rho}. \quad (24)
\end{aligned}
$$

C. Equivalence of leftover hashing lemmas (LHL) and coding theorems

1) Equivalence of LHLs and coding theorems: If the average security index $\mathrm{E}_F \, Q^{\mathrm{PA},F}(\rho_{Z^A E})$, appearing in Corollary 1, can be bounded by some function of the initial state $\rho_{Z^A E}$, it will be called a leftover hashing lemma (LHL). Similarly, if the average failure probability $\mathrm{E}_G \, Q^{\mathrm{EC},G}(\rho_{X^A B})$ of EC (or $\mathrm{E}_G \, Q^{\mathrm{DC},G}(\rho_{X^A B})$ of DC) can be bounded by some function of the environment state $\rho_{X^A E}$, it will be called a coding theorem.

We can show that these LHLs and coding theorems are equivalent, if we combine Corollary 1 and the duality of min- and max-entropies (Lemma 1 below).

Theorem 2 (Equivalence of an LHL and coding theorems)**.** *Let F, G be a pair of dual random functions, r be an arbitrary function, and $\rho_{Z^A E}$ and $\rho_{X^A B}$ be normalized states. Then the following three inequalities are equivalent; that is, if any one of them is true, then all of them are true.*

- *An LHL for PA using $F \, (= G^\perp)$,*

$$\mathrm{E}_F \, Q^{\mathrm{PA},F}(\rho_{Z^A E}) \le r(H_{\min}(Z^A|E)_\rho). \quad (25)$$

- *Coding theorem for EC using $G \, (= F^\perp)$,*

$$\mathrm{E}_G \, Q^{\mathrm{EC},G}(\rho_{X^A B}) \le r(n - H_{\max}(X^A|B)_\rho). \quad (26)$$

- *Coding theorem for DC using $G \, (= F^\perp)$,*

$$\mathrm{E}_G \, Q^{\mathrm{DC},G}(\rho_{X^A B}) \le r(n - H_{\max}(X^A|B)_\rho). \quad (27)$$

This theorem is a direct consequence of Corollary 1 above, and Lemma 1 below. The left hand sides of (25), (26), (27) are equal due to Corollary 1, and the right hands are also equal due to Lemma 1.

Lemma 1 (Entropic uncertainty relation [30], and its equality condition [31])**.** *Let A be an n-qubit space and ρ_{ABE} be a sub-normalized pure state. Then for $\varepsilon \ge 0$, we have [30]*

$$H_{\max}^\varepsilon(X^A|B)_\rho + H_{\min}^\varepsilon(Z^A|E)_\rho \ge n. \quad (28)$$

The inequality holds if ρ_{ABE} is in the standard form [31].

2) Equivalence of the generalized bounds: We note that Theorem 2 above can also be generalized in a straightforward way.

In Theorem 2, we implicitly assumed that the average security index $\mathrm{E}_F \, Q^{\mathrm{PA},F}(\rho_{Z^A E})$ of PA should be bounded by a function of its initial state $\rho_{Z^A E}$, and also that the failure probability $\mathrm{E}_G \, Q^{\mathrm{EC},G}(\rho_{X^A B})$ of EC (or $\mathrm{E}_G \, Q^{\mathrm{DC},G}(\rho_{X^A B})$ of DC) should be bounded by its environment state $\rho_{X^A B}$. However, as one can see from the proof of Theorem 2, such

restriction is not in fact essential in our formalism. Rather, we may consider bounds of the generalized forms by removing such restriction, and prove their equivalence.

Theorem 3 (Generalization of Theorem 2). *Let F, G be a pair of dual random functions, r be a function, and ρ_{ABE} be a normalized state in the standard form. Then the six inequalities of the form*

$$a \le r(b) \tag{29}$$

are all equivalent, where

$$
\begin{aligned}
a &\in \{\mathrm{E}_F\, Q^{\mathrm{PA},F}(\rho_{Z^A E}),\ \mathrm{E}_G\, Q^{\mathrm{EC},G}(\rho_{X^A B}), \\
&\qquad \mathrm{E}_G\, Q^{\mathrm{DC},G}(\rho_{X^A B})\}, \\
b &\in \{H_{\min}(Z^A|E)_\rho,\ n - H_{\max}(X^A|B)_\rho\}.
\end{aligned}
$$

That is, if one inequality of the form (29) is true, then all the six are true.

V. APPLICATION 1: LEFTOVER HASHING LEMMAS FOR (DUAL) UNIVERSAL$_2$ FUNCTIONS F, AND THE CORRESPONDING CODING THEOREMS

Next we apply our main results of the previous section, Theorem 3 in particular, to explicit examples of dual random function pair, F and $G\ (= F^\perp)$.

Specifically, we choose F be the three classes of hash functions that are commonly used for PA: the universal$_2$ [11], the almost universal$_2$ [12], and the dual universal$_2$ functions [13], [14]. Then we prove LHLs of the new type (i.e. bounds on $\mathrm{E}_F\, Q^{\mathrm{PA},F}$; cf. III-A4) for these F.

Further, we apply Theorem 3 to the new LHLs thus obtained, and demonstrate that the coding theorems for EC and DC using the dual random function $F^\perp$ follows automatically.

To the best of our knowledge, most of the LHLs and the coding theorems obtained below are new results that have not been obtained previously (also see the first paragraph of Section V-B).

A. Basic strategy

The basic strategy here is to borrow previous results related with LHLs of the conventional form (i.e. bounds on the standard security index $\mathrm{E}_F\, d_1(\rho_{KE}^F)$) [1], [6], [13], [14], and convert them to LHLs of the new type. The actual procedure is as follows.

1) Previous derivation of LHLs of the conventional form: First we review the previous results of Refs. [1], [6], [13], [14]. In these papers, LHLs of the conventional form were obtained by the following two steps.

1) Prove a bound of the form

$$\mathrm{E}_F\, d_2(\rho_{KE}^F|\sigma_E) \le 2^{-m} r(H_2(\rho_{Z^A E}|\sigma_E)), \tag{30}$$

where $r(\cdot)$ is a non-increasing function, and $d_2(\cdot)$ and $H_2(\cdot|\cdot)$ are defined by

$$
\begin{aligned}
&d_2(\rho_{KE}|\sigma_E) \\
&:= \mathrm{Tr}\left\{\left(\left(\rho_{KB} - 2^{-m}\mathbb{I}_K \otimes \rho_E\right)\left(\mathbb{I}_K \otimes \sigma_E^{-1/2}\right)\right)^2\right\},
\end{aligned} \tag{31}
$$

$$H_2(\rho_{Z^A E}|\sigma_E) := -\log \mathrm{Tr}\left\{\left(\rho_{Z^A E}\left(\mathbb{I}_A \otimes \sigma_E^{-1/2}\right)\right)^2\right\} \tag{32}$$

for a normalized σ (see, e.g., [1]).

2) By using relations

$$d_1(\rho_{KE}^f) \le \sqrt{2^m d_2(\rho_{KE}^f|\sigma_E)}, \tag{33}$$

$$H_{\min}(Z^A|E)_\rho \le H_2(\rho_{Z^A E}|\sigma_E) \tag{34}$$

which hold for a normalized σ (see Ref. [1] for the proofs), and by using Jensen's inequality, one obtains an LHL of the conventional form,

$$\mathrm{E}_F\, d_1(\rho_{KE}^F) \le \sqrt{r(H_{\min}(Z^A|E)_\rho)}. \tag{35}$$

2) How to derive the new type of LHLs: As we have seen above, bounds of the form (30) have already been proved for some random functions F [1], [6], [13], [14]. These bounds can readily be converted to the new type of LHLs (i.e. bounds on $\mathrm{E}_F\, Q^{\mathrm{PA},F}(\rho_{Z^A E})$) by using the following theorem.

Theorem 4. *Let $\rho_{Z^A E}$ be a normalized state, F be a random function, and r be a non-increasing function. If we have a bound of the form*

$$\mathrm{E}_F\, d_2(\rho_{KE}^F|\rho_E) \le 2^{-m} r(H_2(\rho_{Z^A E}|\rho_E)) \tag{36}$$

(i.e., Inequality (30) with $\sigma_E = \rho_E$), then we have an LHL for PA using F,

$$\mathrm{E}_F\, Q^{\mathrm{PA},F}(\rho_{Z^A E}) \le r(H_{\min}(Z^A|E)_\rho), \tag{37}$$

and coding theorems for EC and DC using $G = F^\perp$,

$$
\begin{aligned}
\mathrm{E}_F\, Q^{\mathrm{EC},F^\perp}(\rho_{X^A B}) &= \mathrm{E}_F\, Q^{\mathrm{DC},F^\perp}(\rho_{X^A B}) \\
&\le r(n - H_{\max}(X^A|B)_\rho),
\end{aligned} \tag{38}
$$

which holds for a normalized state $\rho_{X^A B}$.

Note here that if we apply (10) and Jensen's inequality to Inequality (37), we again derive an LHL of the conventional type

$$\mathrm{E}_F\, d_1(\rho_{KE}) \le 4\sqrt{r(H_{\min}(Z^A|E)_\rho)}. \tag{39}$$

Also note that this inequality differs only by the factor of four from the previous result (35), which was obtained without using (37). In this sense we say that the new bound (37) is nearly as tight as the previous bound (35).

3) Proof of Theorem 4: Theorem 4 can be proved by using Theorem 2 and the following two lemmas.

Lemma 2. *For any random hash function F, and for a normalized state $\rho_{Z^A E}$,*

$$Q^{\mathrm{PA},f}(\rho_{Z^A E}) \leq 2^m d_2(\rho_{KE}^f|\rho_E). \tag{40}$$

Proof. According to Ref. [32], we have

$$\widetilde{H}_{1/2}^{\downarrow}(K|E)_\rho \geq \widetilde{H}_2^{\downarrow}(K|E)_\rho, \tag{41}$$

where

$$\widetilde{H}_{1/2}^{\downarrow}(K|E)_\rho := 2\log_2 F(\mathbb{I}_K \otimes \rho_E, \rho_{KE}), \tag{42}$$

$$\widetilde{H}_2^{\downarrow}(K|E)_\rho := -\log_2 \mathrm{Tr}\left\{\left(\rho_{KE}\left(\mathbb{I}_K \otimes \rho_E^{-1/2}\right)\right)^2\right\}. \tag{43}$$

Also by definition of $H_{\max}(K|E)_\rho$ and $\widetilde{H}_{1/2}^{\downarrow}(K|E)_\rho$, we have $H_{\max}(K|E)_\rho \geq \widetilde{H}_{1/2}^{\downarrow}(K|E)_\rho$. Thus

$$
\begin{aligned}
Q^{\mathrm{PA},f}(\rho) &\leq 1 - 2^{-m+\widetilde{H}_{1/2}^{\downarrow}(K|E)_\rho} \\
&\leq 1 - 2^{-m+\widetilde{H}_2^{\downarrow}(K|E)_\rho} \leq 2^{m-\widetilde{H}_2^{\downarrow}(K|E)_\rho} - 1 \\
&= 2^m \mathrm{Tr}\left\{\left(\rho_{KE}\left(\mathbb{I}_K \otimes \rho_E^{-1/2}\right)\right)^2\right\} - 1 \\
&= 2^m d_2(\rho_{KE}|\rho_E),
\end{aligned}
\tag{44}
$$

where in the second line we used $1 - 1/x \leq x - 1$ for $x > 0$. $\square$

Lemma 3. *For any random hash function F, and for a normalized state $\rho_{Z^A E}$,*

$$H_{\min}(Z^A|E)_\rho \leq H_2(\rho_{Z^A E}|\rho_E). \tag{45}$$

Proof. $H_2(\rho_{Z^A E}|\rho_E)$ equals the quantity $\widetilde{H}_2^{\downarrow}(Z^A|E)_\rho$ defined in Ref. [32], and $H_{\min}(Z^A|E)_\rho$ equals $\widetilde{H}_\infty^{\uparrow}(Z^A|E)_\rho$ also defined in the same paper. Hence it suffices to show

$$\widetilde{H}_\infty^{\uparrow}(Z^A|E)_\rho \leq \widetilde{H}_2^{\downarrow}(Z^A|E)_\rho. \tag{46}$$

This inequality follows by substituting $\alpha = \infty$ in Eq. (48), Corollary 4, Ref. [32]. $\square$

B. Explicit examples of an LHL and the corresponding coding theorems

Next we apply Theorem 4 above to three examples of random functions F. To the best of our knowledge, all lemmas in this subsection, except Lemma 4, are new results that have not been obtained previously.

1) Case where F is universal$_2$: The first example of F is the universal$_2$ function. This is the most commonly used random functions for PA.

Definition 4 (Linear universal$_2$ function [11]). *A linear random function $F : \{0,1\}^n \to \{0,1\}^m$ is universal$_2$ if*

$$\Pr[F(x) = 0] \leq 2^{-m} \text{ for } \forall x \neq 0. \tag{47}$$

a) Leftover hashing lemma: For this type of F, an inequality of the type of (30) is already known, which takes the form

$$\mathrm{E}_F d_2(\rho_{KE}|\sigma_E) \leq 2^{-H_2(\rho_{Z^A E}|\sigma_E)} \tag{48}$$

for a normalized $\rho_{Z^A E}$ (Lemma 5.4.3, Ref. [1]). If one applies relations (33) and (34) to this inequality, one obtains an LHL of the conventional form,

$$\mathrm{E}_F d_1(\rho_{KE}^F) \leq \sqrt{\mathrm{Tr}(\rho)}\sqrt{2^{m-H_{\min}(Z^A|E)_\rho}} \tag{49}$$

for a sub-normalized $\rho_{Z^A E}$ (Theorem 5.5.1 of Ref. [1]).

On the other hand, if we instead apply the former half of Theorem 4 to (48), we obtain an LHL of the new type.

Lemma 4 (LHL for PA using a universal$_2$ hash function, in terms of Q^{PA} (Lemma 12, Ref. [8])). *For a universal$_2$ function F, and for a sub-normalized state $\rho_{Z^A E}$,*

$$\mathrm{E}_F Q^{\mathrm{PA},F}(\rho_{Z^A E}) \leq 2^{m-H_{\min}(Z^A|E)_\rho}. \tag{50}$$

As noted in Section III-A3a, this LHL of the new type is nearly as tight as the LHL (49) of the conventional type, which has been obtained previously for the same type of F.

b) Coding theorems: On the other hand, if we apply Theorem 2 to Lemma 4, we readily obtain coding theorems for EC and DC using G ($= F^\perp$), with F being universal$_2$.

Lemma 5 (Coding theorems for EC and DC using a dual universal$_2$ function (Lemma 12, Ref. [8])). *Let G be a random function whose dual $G^\perp$ is universal$_2$ (or equivalently, let G be a dual universal$_2$ function; see Definition 6). Then for a sub-normalized state $\rho_{X^A B}$,*

$$
\begin{aligned}
\mathrm{E}_G Q^{\mathrm{EC},G}(\rho_{X^A B}) &= \mathrm{E}_G Q^{\mathrm{DC},G}(\rho_{X^A B}) \\
&\leq 2^{H_{\max}(X^A|B)_\rho - (n-m)}.
\end{aligned}
\tag{51}
$$

2) Case where F is almost universal$_2$: The second example of F is a generalization of the universal$_2$ function above, which is defined as follows.

Definition 5 (Linear almost universal$_2$ function [12]). *Let $\delta \in \mathbb{R}$ be a parameter. A linear random function $F : \{0,1\}^n \to \{0,1\}^m$ is δ-almost universal$_2$ if*

$$\Pr[F(x) = 0] \leq 2^{-m}\delta \text{ for } \forall x \neq 0. \tag{52}$$

We note that δ must satisfy $(2^n - 2^m)/(2^n - 1) \leq \delta$, as can be shown by a simple argument [12]. Note that the universal$_2$ case of the previous subsection corresponds to $\delta = 1$, near the minimum value.

a) Leftover hashing lemma: For this type of F as well, an inequality of the type of (30) is already known,

$$\mathrm{E}_F d_2(\rho_{KE}^F|\rho_E) \leq 2^{-m}(\delta - 1) + 2^{-H_2(\rho_{Z^A E}|\rho_E)} \tag{53}$$

for a normalized $\rho_{Z^A E}$ (Lemma 5 of Ref. [6]), as well as an LHL of the conventional type

$$
\begin{aligned}
&\mathrm{E}_F d_1(\rho_{KE}^F) \\
&\leq \inf_{\varepsilon > 0} \frac{1}{2}\sqrt{\delta - 1 + 2^{m-H_2(\rho_{Z^A E}|\rho_E)+\log(2/\varepsilon^2+1)}} + \varepsilon
\end{aligned}
\tag{54}
$$

(Lemma 2 of Ref. [6]).

By applying the former half of Theorem 4 to (53), we obtain an LHL of the new type.

Lemma 6 (LHL for PA using an almost universal$_2$ hash function, in terms of Q^{PA})**.** *For a universal$_2$ hash function F and for a sub-normalized state $\rho_{Z^A E}$,*

$$\mathrm{E}_F \, Q^{\mathrm{PA},F}(\rho_{Z^A E}) \leq (\delta - 1)\mathrm{Tr}(\rho) + 2^{m - H_{\min}(Z^A|E)_\rho}. \quad (55)$$

Note that if we set $\delta = 1$, we again obtain Lemma 4. Also note that the bound (55) loses its meaning for $2 < \delta$, where its right hand exceeds one. Therefore, PA using this type of F can only be secure when δ is confined within a relatively small region, $1 \simeq (2^n - 2^m)/(2^n - 1) \leq \delta < 2$ (see Section VIII.B of Ref. [14] for a more detailed argument). This seems to reflect the fact that this type of F was originally conceived for information theoretically secure authentication [12], and not for PA.

b) Coding theorems: As in the previous subsection, if we apply Theorem 2 to Lemma 6, we readily obtain coding theorems for EC and DC using a dual random function G ($= F^\perp$).

Lemma 7 (Coding theorems for EC and DC using an almost dual universal$_2$ function)**.** *Let G be a random function whose dual function $G^\perp$ is δ-almost universal$_2$ (or equivalently, let G be a δ-almost dual universal$_2$ function; see Definition 6). Then for a sub-normalized state $\rho_{X^A B}$,*

$$\mathrm{E}_G \, Q^{\mathrm{EC},G}(\rho_{X^A B}) = \mathrm{E}_G \, Q^{\mathrm{DC},G}(\rho_{X^A B})$$
$$\leq (\delta - 1)\mathrm{Tr}(\rho) + 2^{H_{\max}(X^A|B)_\rho - (n-m)}. \quad (56)$$

3) Case where G is almost universal$_2$, or equivalently, where F is almost dual universal$_2$: In the third example of random functions, we switch properties of F and G, and let G ($= F^\perp$) be an almost universal$_2$ function, instead of F. In this case, F is said to be an almost *dual* universal$_2$ function.

Definition 6 (Almost dual universal$_2$ function [13], [14])**.** *A random function F is called δ-almost dual universal$_2$, if its dual random function $F^\perp$ is δ-almost universal$_2$.*

We note that for this type of F, parameter δ must satisfy $(2^n - 2^{n-m})/(2^n - 1) \leq \delta$ [14]. We also note that this type of F is $2(1 - 2^{-m}\delta) + (\delta - 1)2^{n-m}$-almost universal$_2$ simultaneously [14][4].

a) Leftover hashing lemma: For this type of F as well, an inequality of the type of (30) is known [13], [14],

$$\mathrm{E}_F \, d_2(\rho^F_{KE}|\sigma_E) \leq 2^{-H_2(\rho_{Z^A E}|\sigma_E)}\delta, \quad (57)$$

for a normalized $\rho_{Z^A E}$.

If one applies relations (33) and (34) to this inequality, one obtains an LHL of the conventional form,

$$\mathrm{E}_F \, d_1(\rho^F_{KE}) \leq \sqrt{\mathrm{Tr}(\rho)} \sqrt{2^{m - H_{\min}(Z^A|E)_\rho}} \sqrt{\delta} \quad (58)$$

for a sub-normalized $\rho_{Z^A E}$ [13], [14].

On the other hand, if we instead apply the former half of Theorem 4 to (57), we obtain an LHL of the new type.

---

[4]Conversely, the type of random function F that is defined in Definition 5 is also $2(1 - 2^{-m}\delta) + (\delta - 1)2^{n-m}$-almost *dual* universal$_2$ [14].

Lemma 8 (LHL for PA using an almost dual universal$_2$ hash function, in terms of Q^{PA})**.** *For a δ-almost dual universal$_2$ hash function F, and for a sub-normalized state $\rho_{Z^A E}$,*

$$\mathrm{E}_F \, Q^{\mathrm{PA},F}(\rho_{Z^A E}) \leq 2^{m - H_{\min}(Z^A|E)_\rho}\delta. \quad (59)$$

Unlike the δ-almost universal$_2$ function of the previous subsection (see the paragraph below Lemma 6), PA using this type of F is secure even for δ exponentially larger than one. Hence, this type of F provides a much larger class of secure functions for PA. Exploiting this property, in Ref. [29] we proposed many useful examples of F, such as, efficiently computable hash functions requiring a small random seed.

b) Coding theorems: Again by applying Theorem 2 to Lemma 8, we readily obtain the following lemma.

Lemma 9 (Coding theorems for EC and DC using an almost universal$_2$ function)**.** *For a δ-almost universal$_2$ function G, and for a sub-normalized state $\rho_{X^A B}$,*

$$\mathrm{E}_G \, Q^{\mathrm{EC},G}(\rho_{X^A B}) = \mathrm{E}_G \, Q^{\mathrm{DC},G}(\rho_{X^A B}) \quad (60)$$
$$\leq 2^{H_{\max}(X^A|B)_\rho - (n-m)}\delta.$$

This lemma generalizes and improves the first inequality given in Theorem 1 of Ref. [22], which essentially says, in our notation,

$$\mathrm{E}_G \, Q^{\mathrm{DC},G}(\rho_{X^A B}) \leq 4\sqrt{2^{H_{\max}(X^A|B)_\rho - (n-m)}} \quad (61)$$

for normalized $\rho_{X^A B}$ and for $\delta = 1$.

VI. APPLICATION 2: EQUIVALENCE OF THE TWO APPROACHES TO THE SECURITY PROOF OF QUANTUM KEY DISTRIBUTION

There are two major approaches for the security proof of quantum key distribution (QKD):
- **Leftover hashing lemma (LHL)-based approach**, where one makes use of an LHL [1].
- **Phase error correction (PEC)-based approach** [16], [17], [18], [19], [20], where one transforms a given QKD protocol mathematically to a EC algorithm on the phase degree of freedom of its sifted key.

Previously we have proved that these two approaches are equivalent, in the sense that a proof of one approach can always be converted to the one of the other approach without affecting the resulting security bound [8].

Below, we will apply the results obtained in this paper to simplify and improve our previous proof in Ref. [8]. The proof below is improved in that it is valid for a larger classes of hash functions. That is, the equivalence holds for the case where the random function F for PA is *almost* universal$_2$ [12] and *almost dual* universal$_2$ [13], [14], while previously [8] we treated only the case where F is universal$_2$ [11].

Further, utilizing the knowledge gained in this new proof, we propose a method to simplify the PEC-based proof. That is, we propose to evaluate the randomness of Alice's phase degrees of freedom by the smooth max-entropy, rather than by the phase error rate. This method has an additional merit that every step of the proof becomes equivalent to that of the corresponding LHL-based proof. As a result, one is guaranteed to reach exactly the same security bound as in the LHL-based approach, without any extra factor.

A. Quick review of the two approaches

We begin by reviewing these approaches concentrating on typical cases, though not completely general.

1) Typical QKD protocol: First, we specify what we mean by a typical QKD protocol.

a) Participants and their degrees of freedom: There are two legitimate users, Alice and Bob, who want to share a secure key, and an eavesdropper Eve.

We let space A be Alice's n-qubit space for storing her sifted key, and B be all other degrees of freedom of the legitimate users. Note here that space B generally includes Alice's degrees of freedom, besides Bob's.

We also let space E be all degrees of freedom of Eve.

b) Protocol: For the sake of simplicity we limit ourselves with entanglement-based protocol. We note that we do not lose generality here, since a prepare-and-measure protocols can always be transformed to an entanglement-based protocol by introducing ancillary spaces appropriately.

Initially, Alice, Bob, and Eve are in a state μ_{ABE}. Alice and Bob then perform the following protocol.

1. **Sample measurement** Alice and Bob measure their reduced state μ_{AB}, and determine whether they abort the protocol or not.
2. **Corrected key generation** Alice and Bob each performs a measurement in space AB independently. They then perform information reconciliation together, and generate their corrected keys $z \in \{0,1\}^n$ for Alice, and $z' \in \{0,1\}^n$ for Bob respectively.

   We assume that Alice stores her corrected key z in space A in the z basis, or in Z^A basis. We denote by $\rho_{Z^A E}$ the sub-normalized state after this step of Alice's z and Eve's degree of freedom E.
3. **Secret key generation** Alice and Bob each applies PA using a random function F to their sifted keys z, z' respectively, and generates their secret keys k, k'.

2) Security criterion of QKD: In order to show the security of a QKD protocol as a whole, it suffices to bound the sum of the failure probability of IR, $\varepsilon_{\mathrm{IR}} = \Pr[Z \neq Z']$ ($\geq \Pr[K \neq K']$), and the security index of Alice' secret key $\mathrm{E}_F\, d_1(\rho_{KE}^F)$ (see e.g. Remark 6.1.3 of Ref. [1]).

The probability $\varepsilon_{\mathrm{IR}}$ can easily be bounded using the theory of classical error correcting codes.

As a result, the security analysis of QKD is reduced to that of Alice's secret key, i.e., to bounding $\mathrm{E}_F\, d_1(\rho_{KE}^F)$.

3) Leftover hashing lemma (LHL)-based approach: For a QKD protocol of the above type, a typical LHL-based proof proceeds as follows.

a) Assumption: One assumes that the sample measurement is designed so that the resulting sub-normalized state $\rho_{Z^A E}$ satisfies

$$H_{\min}^{\mathrm{th}} \leq H_{\min}^{\varepsilon}(Z^A|E)_\rho \qquad (62)$$

with $H_{\min}^{\mathrm{th}}$ being a predetermined constant.

One also assumes that an LHL for the random function F has already been proved. In practice, it suffices to assume that Alice and Bob use one of the examples of F that we studied in Section V, i.e., universal$_2$, δ-almost universal$_2$ (with δ sufficiently small), and δ-almost dual universal$_2$ functions.

b) Security proof: As mentioned in Section VI-A2, in order to prove the security of the QKD protocol, one needs to bound the security index of Alice's secret key, $\mathrm{E}_F\, d_1(\rho_{KE}^F)$. For this purpose, one uses an LHL.

For example, if F is universal$_2$, $\mathrm{E}_F\, d_1(\rho_{KE}^F)$ can be bound by using an LHL (49). By substituting (62) to (49), one obtains a security bound

$$\mathrm{E}_F\, d_1(\rho_{KE}^F) \leq 2\varepsilon + \sqrt{2^{m-H_{\min}^{\mathrm{th}}}}. \qquad (63)$$

Also for the case where F is δ-almost universal$_2$, one can obtain a similar security bounds using an LHL (54). For the case of δ-almost universal$_2$, one can use (58).

4) Phase error correction (PEC)-based approach: On the other hand, a typical PEC-based proof proceeds as follows.

a) Assumption: This approach starts by deriving a *virtual state* $\rho_{X^A B}$. That is, one applies to state $\rho_{Z^A E}$ (defined in step 2 of Section VI-A1b) the procedure given in Section IV-A and Fig. 4, and generates $\rho_{X^A B}$ along with a tripartite state ρ_{ABE} in the standard form.

Then one supposes that Alice and Bob together perform EC, with $\rho_{X^A B}$ regarded as the quantum channel on input Alice's codeword $c(t) = 0$ and message $t = 0$[5]. One also assumes that the sample measurement step and the random function F are designed, so that the EC using the dual random function $F^\perp$ fails with a probability,

$$\mathrm{E}_F\, Q^{\mathrm{EC},F^\perp}(\rho_{X^A B}) \leq Q^{\mathrm{EC,th}}, \qquad (64)$$

where $Q^{\mathrm{EC,th}}$ is a predetermined constant.

b) Security proof: As mentioned in Section VI-A2, one needs to bound the security index of Alice's secret key, $\mathrm{E}_F\, d_1(\rho_{KE}^F)$. For this purpose, one uses an inequality

$$d_1(\rho_{KE}^f) \leq 2\sqrt{2}\sqrt{Q^{\mathrm{EC},f^\perp}(\rho_{X^A B})}, \qquad (65)$$

which has been known previously (see e.g. Refs. [33], [8]). By substituting condition (64) to (65), one obtains a security bound

$$\begin{aligned} \mathrm{E}_F\, d_1(\rho_{KE}^F) &\leq 2\sqrt{2}\sqrt{\mathrm{E}_F\, Q^{\mathrm{EC},F^\perp}(\rho_{X^A B})} \\ &\leq 2\sqrt{2}\sqrt{Q^{\mathrm{EC,th}}}, \end{aligned} \qquad (66)$$

where used Jensen's inequality is used in the first line.

c) Typical method for satisfying the assumption: In most literature of the PEC-based approach, one designs the sample measurement step and determines the upper bound $Q^{\mathrm{EC,th}}$ on the average failure probability of the virtual EC, as follows.

1) One chooses a POVM $N = \{N^e \mid \sum_e N^e = \mathbb{I}_B\}$ in space B, and calculates the classical distribution $p(x,e) := \mathrm{Tr}\{\rho_{X^A B}(|\tilde{x}\rangle\langle\tilde{x}|_A \otimes N^e)\}$.
2) One designs the sample measurement step such that the randomness of x seen in $p(x,e)$ becomes sufficiently small, for example, such that the phase error rate $e_{\mathrm{ph}} := \sum_{x \neq 0, e} p(x,e)$ becomes sufficiently small.

---

[5]This corresponds to the situation where Alice always sends out $c(t) = 0$, and Bob's goal is always to recover $y = 0$. If this setting seems unnatural, one may rewrite the situation such that the quantum channel is binary symmetric (see Section III-B) by "twirling" or by randomizing the EC with bit flips in the X basis (randomization by the Pauli Z operators). Such randomization is always possible since $\rho_{Z^A E}$ is invariant under the Pauli Z operators.

3) Using the theory of classical EC, one obtains an upper bound on the average failure probability of the EC. This bound serves as $Q^{\mathrm{EC,th}}$.

The POVM N here plays the same role as M^s of Section III-B1c; i.e., they both provide a hint to boost the performance of the decoder (cf. 3rd paragraph, Section III-B). The difference is that unlike M^s, N does not depend on the syndrome $s = f^\perp(x)$.

d) Remarks: There are two remarks regarding the above procedure.

First, in the context of the QKD, state $\rho_{X^A B}$ is often called a virtual state since it is not necessarily realized in the actual QKD protocol, unlike $\rho_{Z^A E}$. It is rather a mathematical artifact introduced for simplifying security proofs. For the same reason, the EC on the phase error correction considered above is often called the *virtual* EC.

Second, while the bound (65) has been known previously, it can alternatively be regarded as a consequence of the equivalence of EC and PA, which we have shown in Section IV. Indeed, if we combine (10) and Theorem 1, we obtain a slightly weaker inequality $d_1(\rho_{KE}^f) \le 4\sqrt{Q^{\mathrm{EC},f^\perp}(\rho_{X^A B})}$.

B. How to convert one approach to the other

By using our results of Section IV, one can always convert proofs of these two approaches to each other, while keeping the bounds (63) and (66) essentially the same.

1) Conversion from the LHL-based to the PEC-based: When given a LHL-based proof, one can always convert it to an alternative proof of the PEC-based approach.

The basic idea is as follows. When given $\rho_{Z^A E}$, one can always reconstruct the (sub-normalized) virtual state $\rho_{X^A B}$, by using the procedure of Fig. 4. If one applies EC to $\rho_{X^A B}$ thus obtained, the situation now becomes equivalent to the PEC-based approach. In addition, the failure probability of the EC there equals the security of PA in the original LHL-based proof,

$$\mathrm{E}_F\, Q^{\mathrm{PA},F}(\rho_{Z^A E}) = \mathrm{E}_F\, Q^{\mathrm{EC},F^\perp}(\rho_{X^A B}). \tag{67}$$

This is because, by definition, $\rho_{Z^A E}$ and $\rho_{X^A B}$ here are related via a standard form ρ_{ABE}, and Corollary 1 can be applied. If one further applies (65), one can recover essentially the same bound as the original LHL approach, though one is working in the PEC-based approach.

We will see this procedure in detail for the case where F is universal$_2$. (For the case where F is almost universal$_2$ or almost dual universal$_2$, one also can perform a similar procedure using Lemma 6 or 8).

By the definition of the smooth min-entropy, there exists a sub-normalized state $\bar{\rho}_{Z^A E}$ which is ε-close to $\rho_{Z^A E}$ and satisfies $H_{\min}(Z^A|E)_{\bar{\rho}} = H_{\min}^\varepsilon(Z^A|E)_\rho$. Let $\bar{\rho}_{X^A B}$ be the virtual sub-normalized state corresponding to $\bar{\rho}_{Z^A E}$. Then by applying Corollary 1 and Lemma 4, one obtains

$$
\begin{aligned}
\mathrm{E}_F\, Q^{\mathrm{EC},F^\perp}(\bar{\rho}_{X^A B}) &= \mathrm{E}_F\, Q^{\mathrm{PA},F}(\bar{\rho}_{Z^A E}) \\
&= 2^{m-H_{\min}(Z^A|E)_{\bar{\rho}}} = 2^{m-H_{\min}^\varepsilon(Z^A|E)_\rho} \\
&\le 2^{m-H_{\min}^{\mathrm{th}}}.
\end{aligned}
\tag{68}
$$

This means that the situation is now equivalent to that of the PEC-based approach where assumption (64) holds for $\bar{\rho}_{X^A B}$ with $Q^{\mathrm{EC,th}} = 2^{m-H_{\min}^{\mathrm{th}}}$. Therefore by applying (66), one obtains a bound,

$$\mathrm{E}_F\, d_1(\bar{\rho}_{KB}^F) \le 2\sqrt{2}\sqrt{2^{\frac{1}{2}(m-H_{\min}^{\mathrm{th}})}}, \tag{69}$$

and also the security bound for the actual state ρ_{KB}^F,

$$\mathrm{E}_F\, d_1(\rho_{KB}^F) \le 2\varepsilon + 2\sqrt{2}\sqrt{2^{\frac{1}{2}(m-H_{\min}^{\mathrm{th}})}}, \tag{70}$$

which is identical to (63), except for the presence of the factor of $2\sqrt{2}$.

2) Conversion from the PEC-based to the LHL-based approach: Conversely, when given a security proof of the PEC-based approach, one can always convert it to a proof of the LHL-based approach.

To this end, one repeats the the reasoning of the first two paragraph of Section VI-B1, and reaches Eq. (67). Then by substituting condition (64) to (67), one obtains a LHL of the new type (see Section III-A4),

$$\mathrm{E}_F\, Q^{\mathrm{PA},F}(\rho_{Z^A E}) \le Q^{\mathrm{EC,th}}. \tag{71}$$

The situation is now equivalent to that of the LHL-based approach. If one further applies (10) to (71), one obtains

$$
\begin{aligned}
\mathrm{E}_F\, d_1(\rho_{KE}) &\le 4\sqrt{\mathrm{Tr}\rho}\sqrt{\mathrm{E}_F\, Q^{\mathrm{PA},F}(\rho_{Z^A E})} \\
&\le 4\sqrt{Q^{\mathrm{EC,th}}},
\end{aligned}
\tag{72}
$$

which is the same as (66), except that it is looser by the factor of $\sqrt{2}$.

C. Evaluating the phase randomness by the smooth max-entropy

In Section VI-A4c, we explained a typical method used in the PEC-based approach for designing the sample measurement step and for determining the bound $Q^{\mathrm{EC,th}}$ on the average failure probability of the virtual EC.

However, this method has a problem that there is no fixed methodology for finding the appropriate POVM N.

We here propose a method to avoid this problem. Namely, we point out that it is convenient to evaluate the randomness of the phase degrees of freedom X^A by the conditional max-entropy $H_{\max}^\varepsilon(X^A|B)_\rho$, rather than by the phase error rate e_{ph} mentioned in Section VI-A4c. In this method one can exploit the coding theorems for EC (e.g. those derived in Section V-B) to determine $Q^{\mathrm{EC,th}}$, without being bothered by the choice of the POVN N.

This method has an additional merit that every step of the proof becomes equivalent to that of the LHL-based approach of Section VI-A3. As a result, one is guaranteed to reach exactly the same security bound as in the LHL-based approach, without any extra factor.

1) PEC-based approach using the smooth max-entropy:

a) Assumptions: As in Section VI-A4a, we derive the (sub-normalized) virtual state $\rho_{X^A B}$ by the procedure given in Section IV-A and Fig. 4. Then we assume the following two items.

1) The sample measurement step is designed such that the virtual (sub-normalized) state $\rho_{X^A B}$ ends up having the smooth min-entropy bounded as

$$H_{\max}^\varepsilon(X^A|B)_\rho \le n - H_{\min}^{\text{th}}. \tag{73}$$

2) The random hash function F is universal$_2$.

These two assumptions together guarantee that there exists a *approximate* virtual (sub-normalized) state $\bar\rho_{X^A B}$ ($\approx_\varepsilon \rho_{X^A B}$) which satisfies condition (64) of the PEC-based approach, with the parameter

$$Q^{\text{EC,th}} = 2^{m-H_{\min}^{\text{th}}}. \tag{74}$$

To see this, note that by the definition of the smooth max-entropy, there exists a sub-normalized state $\bar\rho_{X^A B}$ ($\approx_\varepsilon \rho_{X^A B}$) satisfying $H_{\max}(X^A|B)_{\bar\rho} = H_{\max}^\varepsilon(X^A|B)_\rho$. Then by applying the coding theorem for EC using $F^\perp$ (Lemma 5) to this $\bar\rho_{X^A B}$,

$$
\begin{aligned}
\mathrm{E}_F\, Q^{\text{EC},F^\perp}(\bar\rho_{X^A B}) &\le 2^{H_{\max}(X^A|B)_{\bar\rho}-(n-m)} \\
&= 2^{H_{\max}^\varepsilon(X^A|B)_\rho-(n-m)} \\
&\le 2^{m-H_{\min}^{\text{th}}}.
\end{aligned} \tag{75}
$$

b) Security proof: Hence we can apply the PEC-based proof of Section VI-A4 to the approximate virtual (sub-normalized) state $\bar\rho_{X^A B}$. By substituting (75) to (65), we obtain

$$\mathrm{E}_F\, d_1(\bar\rho_{KE}^F) \le 2\sqrt{2}\sqrt{2^{H_{\max}^\varepsilon(X^A|B)_\rho-(n-m)}}. \tag{76}$$

Since $\bar\rho_{KE}^f \approx_\varepsilon \rho_{KE}^f$, we then have an LHL which is expressed in terms of Alice's phase degree of freedom X^A,

$$\mathrm{E}_F\, d_1(\rho_{KE}^F) \le 2\varepsilon + 2\sqrt{2}\sqrt{2^{H_{\max}^\varepsilon(X^A|B)_\rho-(n-m)}}. \tag{77}$$

By substituting condition (73) to (77), we obtain

$$\mathrm{E}_F\, d_1(\rho_{KE}^F) \le 2\varepsilon + 2\sqrt{2}\sqrt{2^{m-H_{\min}^{\text{th}}}}. \tag{78}$$

2) Equivalence with the LHL-based approach: The final result (78) of the PEC-based proof above is the same as (63) of the LHL-based proof, except for the presence of the factor of $2\sqrt{2}$. This is because we are in fact using the same assumption and the same inequality as in the LHL-based approach of Section VI-A2:

- Condition (73) is equivalent to condition (62) of the LHL-based approach.
  This is because in the current situation, we have

  $$H_{\min}^\varepsilon(Z^A|E)_\rho + H_{\max}^\varepsilon(X^A|B)_\rho = n \tag{79}$$

  due to Lemma 1.
- The coding theorem (Lemma 5) that we used to derive (75) is essentially equivalent to the LHL (49), which is used in the LHL-based approach.

To see this, we apply Theorem 2 (the equivalence of PA and EC) to Lemma 5, and obtain an LHL of the new type,

$$
\begin{aligned}
\mathrm{E}_F\, Q^{\text{EC},F^\perp}(\rho_{X^A B}) &= \mathrm{E}_F\, Q^{\text{PA},F}(\rho_{Z^A E}) \\
&\le 2^{H_{\max}(X^A|B)_\rho-(n-m)} \\
&= 2^{m-H_{\min}(Z^A|E)_\rho}
\end{aligned} \tag{80}
$$

If we then apply (10) to these inequalities, we obtain an LHL of the conventional type, which differs from (49) by a factor of 4.

Thus, in fact our proof method here is essentially the same as the LHL-based approach that was specified in Section VI-A2. The difference is that ours is re-formalized within the PEC-based approach.

3) Advantages of our method: From the standpoint of the PEC-based approach, we believe that this stronger version of the equivalence is an additional merit of our method. As a result, the advantages of our method against the typical PEC-based approach can be summarized as follows.

1) It admits the use of the smoothing parameter ε.
2) The analysis is simple: One need not specify POVM N, which was mentioned in Section VI-A4c. Once one finishes evaluating Alice's phase randomness in terms of $H_{\max}^\varepsilon(X^A|B)_\rho$, the security bound readily follows from the LHL (77).
3) The bound thus obtained is guaranteed to be the same as in the corresponding LHL-based proof.

4) Improved bound using the uncertainty relation: Finally, we note that the LHL expressed in terms of Alice's phase degree of freedom, (77), is not by itself a new result (though we believe that our interpretation in the PEC-based approach is). It is rather a direct consequence of the entropic uncertainty relation (the former half of Lemma 1 of this paper), which was shown previously by Tomamichel and coauthors [30], [34], [10]. Moreover, (77) can be improved by using their result.

If we substitute (28) to (49), we obtain an LHL

$$\mathrm{E}_F\, d_1(\rho_{KE}^F) \le 2\varepsilon + \sqrt{\mathrm{Tr}(\rho)}\sqrt{2^{H_{\max}^\varepsilon(X^A|B)_\rho-(n-m)}}, \tag{81}$$

which improves (77) by a factor of $2\sqrt{2}$. If we then substitute condition (73) to (81), we obtain a security bound

$$\mathrm{E}_F\, d_1(\rho_{KE}^F) \le 2\varepsilon + \sqrt{2^{m-H_{\min}^{\text{th}}}}, \tag{82}$$

which again improves (78) by a factor of $2\sqrt{2}$, and equals (63) of the LHL-based proof exactly.

VII. Summary and Outlook

We showed that quantum algorithms of privacy amplification (PA), error correction (EC), and data compression (DC) are equivalent, if we define the security of PA by using the purified distance and if we generalize EC and DC by adding quantum side information.

As an application of this equivalence, we took previously known security bounds of PA, and converted them into coding theorems for EC and DC that have not been obtained previously. We applied these results to simplify and improve our previous result that the two prevalent approaches to

the security proof of quantum key distribution (QKD) are equivalent. We also propose a method to simplify the security proof of QKD by using the insight gained in this analysis.

An interesting future direction is to generalize the equivalence by using a dual pair of K-entropies [31] for defining the indices Q for the three algorithms. For example, if we use the von Neumann entropy to define the index Q for any one of the three algorithms, and if we can still prove the equivalence, then all the three algorithms will share the same definition for their indices Q. Therefore, the equivalence in a stronger sense will be established, and the three algorithms will become truly indistinguishable.

APPENDIX A
PROOF OF THEOREM 1

In this section we will prove Theorem 1.

Since all terms in (22) are proportional to $\mathrm{Tr}(\rho_{ABE})$, it suffices to consider the case where ρ_{ABE} is normalized. In this case, Theorem 1 follows immediately by combining Eq. (8) and the following three lemmas.

Lemma 10. *For a normalized state $\rho_{X^A B}$ and for a function g, we have*

$$
\begin{aligned}
Q^{\mathrm{EC},g}(\rho_{X^A B}) &= Q^{\mathrm{DC},g}(\rho_{X^A B}) \\
&= 1 - 2^{-H_{\min}(X^A|B,g(X^A))_\rho}.
\end{aligned} \tag{83}
$$

Proof. From the definitions of EC and DC, it is evident that their indices $Q^{\mathrm{EC},g}(\rho_{X^A B})$ and $Q^{\mathrm{DC},g}(\rho_{X^A B})$ can both be rewritten as

$$
\begin{aligned}
Q^{\mathrm{EC},g}(\rho_{X^A B}) &= Q^{\mathrm{DC},g}(\rho_{X^A B}) \\
&= \min_{\{M^s\}} \left(1 - \sum_x \mathrm{tr}(\tilde{\rho}^x M^{g(x),x}) \right).
\end{aligned} \tag{84}
$$

Next note that the decoding of DC is equivalent to the situation where, given a state

$$
\tau = \sum_x |\tilde{x}\rangle \langle \tilde{x}|_A \otimes \tilde{\rho}_B^x \otimes |g(x)\rangle \langle g(x)|_D \tag{85}
$$

(with D being a new ancillary space), one estimates x by measuring spaces B, D. According to Ref. [9], the success probability of this estimation equals $2^{H_{\min}(X^A|B,D)_\tau}$. Then, by noting $H_{\min}(X^A|B,D)_\tau = H_{\min}(X^A|B,g(X^A))_\rho$, we obtain the lemma. $\qquad\square$

Lemma 11. *For a dual pair of functions f, g, and for a normalized state ρ_{ABE}, we have*

$$
Q^{\mathrm{PA},f}(\rho_{Z^A E}) \leq Q^{\mathrm{EC},g}(\rho_{X^A B}). \tag{86}
$$

Proof. We begin by introducing a new notation: We denote the i-th row of a matrix f (appearing in Definition 1) by f_i, and components of f_i by $f_{i1}, \ldots, f_{in}$. In this notation, for example, the duality condition $f g^T = 0$ can be written $f_i \cdot g_j = \sum_k f_{ik} g_{jk} = 0$ for $\forall i, j$.

Next we note that the security index $Q^{\mathrm{PA},f}$ for PA can be rewritten as

$$
\begin{aligned}
&Q^{\mathrm{PA},f}(\rho_{Z^A E}) \\
&= 1 - \max_{\sigma \geq 0, \mathrm{Tr}\sigma=1} F(\Pi^{\mathrm{PA},f}(\rho_{ABE})_{KE}, 2^{-m}\mathbb{I}_K \otimes \sigma_E)^2.
\end{aligned} \tag{87}
$$

by using the algorithm $\Pi^{\mathrm{PA},f}$ below, which is designed to affect spaces A, E in the same way as the actual PA.

- **Equivalent algorithm for PA ($\Pi^{\mathrm{PA},f}$):** Measure space A using the operator $Z^{f_i} = Z^{f_{i1}} \otimes \cdots \otimes Z^{f_{in}}$ ($i = 1, \ldots, m$), and store the result $k \in \{0,1\}^m$ in space K.

Similarly, we also note that the performance index $Q^{\mathrm{EC},g}(\rho_{X^A B})$ of EC can be rewritten as

$$
\begin{aligned}
&Q^{\mathrm{EC},g}(\rho_{X^A B}) \\
&= 1 - \max_{\{M^s\}} F(|\tilde{0}\rangle \langle \tilde{0}|_A, \Pi^{\mathrm{EC},g}(\rho_{ABE})_A)^2.
\end{aligned} \tag{88}
$$

by using the algorithm $\Pi^{\mathrm{EC},g}$ below.

- **Equivalent decoding algorithm for EC ($\Pi^{\mathrm{EC},g}$):**
  1) **Syndrome measurement:** Measure space A using an operator $X^{g_i} = X^{g_{i1}} \otimes \cdots \otimes X^{g_{in}}$ ($i = 1, \ldots, n-m$), and record the result as the syndrome $s = (s_1, \ldots, s_{n-m}) \in \{0,1\}^{n-m}$.
  2) **Side information measurement:** Measure space B using the POVM $M^s = \{M^{s,e}\}_{x' \in \{0,1\}^n}$, and obtain the estimated error pattern e.
  3) **Bit flip:** Apply the operator Z^e in space A.

The state $|\tilde{0}\rangle \langle \tilde{0}|_A$ appearing in Eq. (88) must take the form $|\tilde{0}\rangle \langle \tilde{0}|_A \otimes \sigma_E$ for some σ, when it is extended to spaces A, E. Thus Eq. (88) can be rewritten further as

$$
\begin{aligned}
&Q^{\mathrm{EC},g}(\rho_{X^A B}) = \\
&1 - \max_{\{M^s\}, \sigma \geq 0, \sigma, \mathrm{Tr}\sigma=1} F\left(|\tilde{0}\rangle \langle \tilde{0}|_A \otimes \sigma_E, \Pi^{\mathrm{EC},g}(\rho_{ABE})_{AE}\right)^2.
\end{aligned} \tag{89}
$$

Further, if functions f, g are dual, the operator Z^{f_i} of $\Pi^{\mathrm{PA},f}$, commutes with X^{g_i} and with $Z^{z'}$ of $\Pi^{\mathrm{EC},g}$. Thus algorithms $\Pi^{\mathrm{PA},f}$ and $\Pi^{\mathrm{EC},g}$ also commute with each other. Therefore we have $\Pi^{\mathrm{PA},f}(\Pi^{\mathrm{EC},g}(\rho))_{KE} = \Pi^{\mathrm{EC},g}(\Pi^{\mathrm{PA},f}(\rho))_{KE} = \Pi^{\mathrm{PA},f}(\rho)_{KE}$, and

$$
\begin{aligned}
&1 - Q^{\mathrm{EC},g}(\rho_{X^A B}) \\
&\leq \max_{\{M^s\}, \sigma \geq 0, \mathrm{Tr}\sigma=1} \\
&\quad F\left(\Pi^{\mathrm{PA},f}(|\tilde{0}\rangle \langle \tilde{0}|_A \otimes \sigma_E)_{KE}, \Pi^{\mathrm{PA},f}(\Pi^{\mathrm{EC},g}(\rho)_{AE})_{KE}\right)^2 \\
&= \max_{\sigma \geq 0, \mathrm{Tr}\sigma=1} F\left(\Pi^{\mathrm{PA},f}(|\tilde{0}\rangle \langle \tilde{0}|_A \otimes \sigma_E)_{KE}, \Pi^{\mathrm{PA},f}(\rho)_{KE}\right)^2 \\
&= \max_{\sigma \geq 0, \mathrm{Tr}\sigma=1} F\left(\mathbb{I}_K \otimes \sigma_E, \rho_{KE}^f\right)^2 = 1 - Q^{\mathrm{PA},f}(\rho_{AE}).
\end{aligned} \tag{90}
$$

$\qquad\square$

Lemma 12. *For a dual pair of functions f, g, and for a normalized state ρ_{ABE} in the standard form, we have*

$$
H_{\max}(f(Z^A)|E)_\rho + H_{\min}(X^A|B,g(X^A))_\rho = m. \tag{91}
$$

Proof. We continue to use the notation introduced in the proof of Lemma 11. In this notation, the random number $K = f(Z^A)$ in PA corresponds to measurement result by operators $(Z^{f_i})_A$, and the syndrome $S = g(X^A)$ in EC corresponds to that by $(X^{g_j})_A$. Since these operators, $(Z^{f_i})_A$ and $(X^{g_j})_A$, commutes with each other for a dual pair f, g, we can decompose space A into $A = A_1 A_2$, such that random variable K equals the result of the z basis measurement in the m-qubit space A_1, and S equals the result of the

x basis measurement in the $n - m$ qubit space A_2, i.e., $Z^{A_1} = K = f(Z^A)$ and $X^{A_2} = g(X^A)$.

In this case, $H_{\min}(X|B, X^{A_2})_\rho = H_{\min}(X^{A_1}|B, X^{A_2})_\rho$ holds, and the relation (91), which we need to prove, takes the form

$$H_{\max}(Z^{A_1}|E)_\rho + H_{\min}(X^{A_1}|B, X^{A_2})_\rho = m. \qquad (92)$$

(i) Suppose that $\rho_{AE} = \rho_{Z^A E}$. In this case, if we measure $|\rho\rangle_{ABE} = |\rho\rangle_{A_1 A_2 BE}$ in the X^{A_2} basis, we obtain

$$\rho_{A_1 X^{A_2} BE} = 2^{-(n-m)} \sum_t |\tilde{s}\rangle \langle \tilde{s}|_{A_2} \otimes |\tau^s\rangle \langle \tau^s|_{A_1 BE}. \qquad (93)$$

Alternatively, if we measure $\rho_{A_1 A_2 E} = \rho_{Z^{A_1} Z^{A_2} E}$ in the X^{A_2} basis, we obtain

$$\rho_{Z^{A_1} X^{A_2} E} = 2^{-(n-m)} \mathbb{I}_{A_2} \otimes \rho_{Z^{A_1} E}. \qquad (94)$$

Then if we further trace out B from (93), it should equal (94) by construction. Thus all $|\tau^s\rangle$ are a purification of $\rho_{Z^{A_1} E}$. Hence by applying Lemma 1 to $|\tau^s\rangle$ and space A_1, we see that $H_{\min}(X^{A_1}|B)_{\tau^s} = m - H_{\max}(Z^{A_1}|E)_{\tau^s} = m - H_{\max}(Z^{A_1}|E)_\rho$. Also by applying Proposition 4.6 of Ref. [10], we obtain $2^{H_{\min}(X^{A_1}|X^{A_2}, B)_\rho} = 2^{-(n-m)} \sum_s 2^{H_{\min}(X^{A_1}|B)_{\tau^s}} = 2^{H_{\max}(Z^{A_1}|E)_\rho}$, which proves (92).

(ii) Suppose that $\rho_{AB} = \rho_{X^A B}$. Then we have $\rho_{A_1 A_2 B} = \rho_{A_1 X^{A_2} B} = \rho_{X^{A_1} X^{A_2} B}$, with ρ_{ABE} being the purification of all these states. By applying Lemma 1 to ρ_{ABE} and space A_1, we obtain (92). $\square$

APPENDIX B
RELATION BETWEEN SECURITY CRITERIA OF PRIVACY AMPLIFICATION

In section III-A, we introduced quantities $Q^{\mathrm{PA},f}(\rho_{Z^A E})$ and $d_1(\rho_{KE}^f)$ as the security index for random number $K = f(Z^A)$ in PA. Besides these two quantities, some literature also use security index for K,

$$d_1'(\rho_{KE}^f) := \min_{\sigma \geq 0, \mathrm{Tr}(\sigma)=1} \left\| \rho_{KE}^f - 2^{-m} \mathbb{I}_K \otimes \sigma_E \right\|_1. \qquad (95)$$

It is straightforward to show that this quantity can be bounded by $Q^{\mathrm{PA},f}(\rho_{Z^A E})$ as

$$1 - \sqrt{1 - Q^{\mathrm{PA},f}(\rho_{Z^A E})} \leq \frac{1}{2} d_1'(\rho_{KE}^f) \leq \sqrt{Q^{\mathrm{PA},f}(\rho_{Z^A E})}, \qquad (96)$$

if ρ is normalized (see from Eq. (9.110) of Ref. [15]).

It can also be shown that $d_1'(\rho_{KE}^f)$ bounds the conventional security index $d_1(\rho_{KE}^f)$ as

$$d_1'(\rho_{KE}^f) \leq d_1(\rho_{KE}^f) \leq 2d_1'(\rho_{KE}^f), \qquad (97)$$

if ρ is normalized. The first inequality is immediate from the definitions of $d_1(\rho_{KE}^f)$ and $d_1'(\rho_{KE}^f)$. The second inequality can be shown as

$$
\begin{aligned}
& \left\| \rho_{KE}^f - 2^{-m} \mathbb{I}_K \otimes \rho_E \right\| \\
& \leq \left\| \rho_{KE}^f - 2^{-m} \mathbb{I}_K \otimes \sigma_E \right\| \\
& \quad + \left\| 2^{-m} \mathbb{I}_K \otimes \sigma_E - 2^{-m} \mathbb{I}_K \otimes \rho_E \right\| \\
& = \left\| \rho_{KE}^f - 2^{-m} \mathbb{I}_K \otimes \sigma_E \right\| + \left\| \rho_E - \sigma_E \right\| \\
& \leq 2 \left\| \rho_{KE}^f - 2^{-m} \mathbb{I}_K \otimes \sigma_E \right\|, \qquad (98)
\end{aligned}
$$

where the last inequality holds from the monotonicity of the trace distance.

Inequality (10) of section III-A follows from Eqs. (96) and (97).

APPENDIX C
A NOTE ON THE CORRESPONDENCE OF STATES

In Sec. IV-A2b, we introduced the procedure T in order to define the correspondence between the input state $\rho_{Z^A E}$ of PA, and $\rho_{X^A B}$ of EC and DC. However, contrary to our naive expectation, repeating this procedure T twice does not in fact yield the original state: A straightforward calculation gives

$$
\begin{aligned}
T(T(\rho_{Z^A E})) &= \mathrm{XOR}_{E' \to A}^z(\rho_{Z^A E} \otimes 2^{-n} \mathbb{I}_{E'}), & (99) \\
T(T(\rho_{X^A B})) &= \mathrm{XOR}_{B' \to A}^x(\rho_{X^A B} \otimes 2^{-n} \mathbb{I}_{B'}), & (100)
\end{aligned}
$$

where the Hilbert spaces E' and B' are of the same size as A, and $\mathrm{XOR}_{C \to A}^b$ denotes XORing variable C on variable A in basis $b \in \{z, x\}$. Note that $T(T(\rho_{Z^A E})) \neq \rho_{Z^A E}$ and $T(T(\rho_{X^A B})) \neq \rho_{X^A B}$.

Here we demonstrate that this fact does not compromise the correspondence of the two types of states. The basic observation is that states $T(T(\rho_{Z^A E}))$ and $\rho_{Z^A E}$ are equivalent as long as one is concerned with the security of PA; and $T(T(\rho_{X^A B}))$ and $\rho_{X^A B}$ are equivalent as long as the performance of DC or EC is concerned.

To see this for the case of $\rho_{Z^A E}$, note that the state $\mathrm{XOR}_{E' \to A}^z(\rho_{Z^A E} \otimes 2^{-n} \mathbb{I}_{E'})$ appearing in (99) describes a classical ensemble of $\rho_{Z^A E}$ where Alice's classical variable Z^A is shifted (XORed) by a publicly known random variable E'. Hence performing PA on this state is equivalent to performing it on $\rho_{Z^A E}$ in parallel, where Alice's random bits k is shifted by a public constant value $f(e')$. Since the security of k cannot be affected by such shift, this situation is clearly equivalent to PA on $\rho_{Z^A E}$.

We note that essentially the same argument also holds for the case of $\rho_{X^A B}$ in DC and EC.

REFERENCES

[1] R. Renner, "Security of quantum key distribution," Ph.D. dissertation, Diss. ETH No. 16242, 2005.

[2] G. V. Assche, *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, 2006.

[3] P. Tuyls, B. Škoric, and T. Kevenaar, *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, ser. Security with noisy data. Springer London, 2007. [Online]. Available: https://books.google.co.jp/books?id=psWUQ5cDsI0C

[4] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *Npj Quantum Information*, vol. 2, p. 16021, Jun 2016. [Online]. Available: https://doi.org/10.1038/npjqi.2016.21

[5] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. USA: Wiley-Interscience, 2006.

[6] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5524–5535, 2011.

[7] J. M. Renes, "Duality of privacy amplification against quantum adversaries and data compression with quantum side information," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 467, no. 2130, pp. 1604–1623, 2011. [Online]. Available: https://royalsocietypublishing.org/doi/abs/10.1098/rspa.2010.0445

[8] T. Tsurumaru, "Leftover hashing from quantum error correction: Unifying the two approaches to the security proof of quantum key distribution," *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3465–3484, 2020.

[9] R. König, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4337–4347, 2009.

[10] M. Tomamichel, "A framework for non-asymptotic quantum information theory," Ph.D. dissertation, Diss. ETH No. 20213, 2012.

[11] J. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143 – 154, 1979. [Online]. Available: http://www.sciencedirect.com/science/article/pii/0022000079900448

[12] M. N. Wegman and J. Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences*, vol. 22, no. 3, pp. 265 – 279, 1981. [Online]. Available: http://www.sciencedirect.com/science/article/pii/0022000081900337

[13] S. Fehr and C. Schaffner, "Randomness extraction via delta-biased masking in the presence of a quantum attacker," *Theory of Cryptography Fifth Theory of Cryptography Conference, TCC 2008 New York, USA, March 19-21, Lecture Notes in Computer Science*, vol. 4948, pp. 465–481, 2008.

[14] T. Tsurumaru and M. Hayashi, "Dual universality of hash functions and its applications to quantum cryptography," *IEEE Transactions on Information Theory*, vol. 59, no. 7, pp. 4700–4717, 2013.

[15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. New York, NY, USA: Cambridge University Press, 2011.

[16] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, May 2001. [Online]. Available: http://doi.acm.org/10.1145/382780.382781

[17] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999. [Online]. Available: https://science.sciencemag.org/content/283/5410/2050

[18] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.85.441

[19] M. Koashi, "Complementarity, distillable secret key, and distillable entanglement," *arXiv:0704.3661 [quant-ph]*, 2007.

[20] M. Hayashi, "Upper bounds of eavesdropper's performances in finite-length code with the decoy method," *Phys. Rev. A*, vol. 76, p. 012329, Jul 2007. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.76.012329

[21] J. M. Renes and J.-C. Boileau, "Physical underpinnings of privacy," *Phys. Rev. A*, vol. 78, p. 032335, Sep 2008, (preprints arXiv:quant-ph/0702187v1 and arXiv:0803.3096v2 [quant-ph]). [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.78.032335

[22] J. M. Renes and R. Renner, "One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys," *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1985–1991, 2012.

[23] J. M. Renes, "Duality of channels and codes," *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 577–592, 2018.

[24] ——, "On privacy amplification, lossy compression, and their duality to channel coding," *IEEE Transactions on Information Theory*, vol. 64, no. 12, pp. 7792–7801, 2018.

[25] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, "The universal composable security of quantum key distribution," in *Theory of Cryptography*, J. Kilian, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 386–406.

[26] H.-C. Cheng, E. P. Hanson, N. Datta, and M.-H. Hsieh, "Duality between source coding with quantum side information and c-q channel coding," *arXiv e-prints*, p. arXiv:1809.11143, Sep. 2018.

[27] I. Devetak and A. Winter, "Classical data compression with quantum side information," *Phys. Rev. A*, vol. 68, p. 042301, Oct 2003. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.68.042301

[28] H.-C. Cheng, E. P. Hanson, N. Datta, and M.-H. Hsieh, "Non-asymptotic classical data compression with quantum side information," *IEEE Transactions on Information Theory*, vol. 67, no. 2, pp. 902–930, 2021.

[29] M. Hayashi and T. Tsurumaru, "More efficient privacy amplification with less random seeds via dual universal hash function," *IEEE Transactions on Information Theory*, vol. 62, no. 4, pp. 2213–2232, 2016.

[30] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," *Phys. Rev. Lett.*, vol. 106, p. 110506, Mar 2011. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.106.110506

[31] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, "Uncertainty relations from simple entropic properties," *Phys. Rev. Lett.*, vol. 108, p. 210405, May 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.108.210405

[32] M. Tomamichel, M. Berta, and M. Hayashi, "Relating different quantum generalizations of the conditional Rényi entropy," *Journal of Mathematical Physics*, vol. 55, no. 8, p. 082206, 2014. [Online]. Available: https://doi.org/10.1063/1.4892761

[33] M. Hayashi and T. Tsurumaru, "Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths," *New Journal of Physics*, vol. 14, no. 9, p. 093014, 2012. [Online]. Available: http://stacks.iop.org/1367-2630/14/i=9/a=093014

[34] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Communications*, vol. 3, p. 634, Jan. 2012.

Toyohiro Tsurumaru was born in Japan in 1973. He received the B.S. degree from the Faculty of Science, University of Tokyo, Japan in 1996, and the M.S. and Ph.D. degrees in physics from the Graduate School of Science, University of Tokyo, Japan in 1998 and 2001, respectively. Then he joined Mitsubishi Electric Corporation in 2001. His research interests include theoretical aspects of quantum cryptography, as well as modern cryptography.