Quantum Security Analysis via Smoothing of Renyi Entropy of Order 2

Masahito Hayashi[1,2]

[1] Graduate School of Mathematics, Nagoya University
[2] Centre for Quantum Technologies, National University of Singapore
masahito@math.nagoya-u.ac.jp
http://www.math.nagoya-u.ac.jp/~masahito/index_e.html

Abstract. It is known that the security evaluation can be done by smoothing of Rényi entropy of order 2 in the quantum setting when we apply universal$_2$ hash functions. This fact can be extended to the case when we apply ε-almost dual universal$_2$ hash functions, which is a generalized concept of universal$_2$ hash functions. Demonstrating the smoothing of Rényi entropy of order 2, we derived security bounds for universal composability and mutual information criterion under the condition in the quantum setting.

1 Introduction

Evaluation of secrecy is one of important topics in classical and quantum information theory. In order to increase the secrecy, we apply a hash function. Bennett et al. [4] and Håstad et al. [14] proposed to use universal$_2$ hash functions for privacy amplification and derived two universal hashing lemma, which provides an upper bound for the universal composability based on Rényi entropy of order 2. Renner [6] extended their idea to the quantum case and evaluated the secrecy with universal$_2$ hash functions based on a quantum version of conditional Rényi entropy order 2.

In order to apply Renner's two universal hashing lemma to a realistic setting, Renner [6] attached the smoothing to min entropy, which is smaller than the above quantum version of conditional Rényi entropy order 2 in the classical case. That is, he proposed the application of universal hashing lemma to a state approximating the true state. In this method, it is not easy to find a suitable approximating state. Hayashi [11] found such a suitable approximating state in the sense of Rényi entropy order 2. That is, he applied the smoothing to Rényi entropy order 2. Then, he evaluated the universal composability criterion after universal$_2$ hash functions based on Rényi entropy order $1+s$. Since Rényi entropy order 2 gives a tighter security bound than the min entropy, the smoothing for Rényi entropy order 2 yields a better security bound than the min entropy. Indeed, it has been showed that the method [11] yields the optimal exponential decreasing rate in the n-fold independent and identical case.

However, in other cases (quantum case and classical case with the mutual information criterion), no study attached the smoothing to the quantum version

K. Iwama, Y. Kawano, and M. Murao (Eds.): TQC 2012, LNCS 7582, pp. 128–140, 2013.

of conditional Rényi entropy order 2. The purpose of this paper is to attach the smoothing to the quantum version of conditional Rényi entropy order 2. and to obtain an evaluation for secret key generation from correlated random number in two kinds of criteria (universal composability and the modified mutual information) in the quantum settings. As our result, first, we obtain a lower bound of the exponential decreasing rate with the quantum i.i.d. settings for secret key generation when Alice and Bob share the same random number and Eve has a correlated random number, i.e., the secret key generation without error correction.

Indeed, the obtained evaluation can be applied to a more general case. Recently, Tsurumaru et al [13] proposed the concept "ε-almost dual universal hash functions" as a generalization of linear universal hash functions. This concept is defined for a family of hash functions. On the other hand, Dodis and Smith [7] proposed the concept "δ-biased family" for a family of random variables. The concept "ε-almost dual universal hash functions" can be converted to a part of "δ-biased family"[7,13]. Indeed, Dodis et al.[7] and Fehr et al.[8] showed a security lemma (9). Employing this conversion and the above security lemma, Tsurumaru et al [13] obtained a variant of two universal hashing lemma for "ε-almost dual universal hash functions". This lemma can be regarded as a kind of generalization of two universal hashing lemma by Renner [6]. Therefore, our evaluation can be applied to the class of "ε-almost dual universal hash functions", which is a wider class of hash function.

The remaining part of this paper is the following. In section 2, we introduce the information quantities for evaluating the security and derive several useful inequalities. We also give a clear definition for security criteria. In section 3, according to Tsurumaru et al [13], we introduce several class of hash functions (universal$_2$ hash functions and ε-almost dual universal$_2$ hash functions). We clarify the relation between ε-almost dual universal$_2$ hash functions and δ-biased family. We also explain an ε-almost dual universal$_2$ version of Renner's two universal hashing lemma [6, Lemma 5.4.3](Lemma 10) based on Lemma for δ-biased family given by Dodis et al.[7] and Fehr et al.[8].

In section 4, we attach the smoothing to the obtained upper bound and obtain a security upper bound under the universal composability criterion, which is the main result of this paper. In section 5, we derive an exponential decreasing rate when we simply apply hash functions and there is no error between Alice and Bob. All proofs are omitted and are given in [16]. Further analysis are also presented in [16].

2 Preparation

2.1 Information Quantities for Single System

In order to discuss the quantum case, we prepare several useful properties of information quantities in single quantum system: First, we define the following quantities:

$$D(\rho\|\sigma) := \mathrm{Tr}\,\rho(\log\rho - \log\sigma) \tag{1}$$
$$\psi(s|\rho\|\sigma) := \log \mathrm{Tr}\,\rho^{1+s}\sigma^{-s} \tag{2}$$
$$\underline{\psi}(s|\rho\|\sigma) := \log \mathrm{Tr}\,\rho^{\frac{1+s}{2}}\sigma^{-s/2}\rho^{\frac{1+s}{2}}\sigma^{-s/2} \tag{3}$$

with $s \in \mathbb{R}$. Then, we obtain the following lemma:

Lemma 1. *The functions $s \mapsto \psi(s|\rho\|\sigma), \underline{\psi}(s|\rho\|\sigma)$ are convex.*

For a proof for $\psi(s|\rho\|\sigma)$, see Hayashi [9, Exercises 2.24]. For $\underline{\psi}(s|\rho\|\sigma)$, see Hayashi [16].

Since $\lim_{s\to 0}\frac{1}{s}\psi(s|\rho\|\sigma) = D(\rho\|\sigma)$, and $\lim_{s\to 0}\frac{1}{s}\underline{\psi}(s|\rho\|\sigma) = D(\rho\|\sigma)$, we obtain the following lemma.

Lemma 2. *$\frac{\psi(s|\rho\|\sigma)}{s}$ and $\frac{\underline{\psi}(s|\rho\|\sigma)}{s}$ are monotone increasing concerning $s \in \mathbb{R}$. In particular,*

$$sD(\rho\|\sigma) \le \psi(s|\rho\|\sigma) \tag{4}$$
$$sD(\rho\|\sigma) \le \underline{\psi}(s|\rho\|\sigma) \tag{5}$$

for $s > 0$.

For any quantum operation Λ, the following information processing inequalities

$$D(\Lambda(\rho)\|\Lambda(\sigma)) \le D(\rho\|\sigma), \quad \psi(s|\Lambda(\rho)\|\Lambda(\sigma)) \le \psi(s|\rho\|\sigma) \tag{6}$$

hold for $s \in (0,1]$[9, (5,30),(5.41)]. However, this kind of inequality does not fold for $\underline{\psi}(s|\rho\|\sigma)$ in general.

2.2 Information Quantities in Composite System

Next, we prepare several information quantities in a composite system $\mathcal{H}_A \otimes \mathcal{H}_E$, in which, $\mathcal{H}_A$ is a classical system spanned by the basis $\{|a\rangle\}$. In the following, a sub-state ρ is not necessarily normalized and is assumed to satisfy $\mathrm{Tr}\,\rho \le 1$. A composite sub-state ρ is called a *c-q* state when it has a form $\rho = \rho^{A,E} = \sum_a P^A(a)|a\rangle\langle a| \otimes \rho_a^E$ with $P^A(a) \ge 0$, in which the conditional state ρ_a^E is normalized. Then, the von Neumann entropies and Renyi entropies are given as

$$H(A,E|\rho^{A,E}) := -\mathrm{Tr}\,\rho^{A,E}\log\rho^{A,E}$$
$$H(E|\rho^E) := -\mathrm{Tr}\,\rho^E\log\rho^E$$
$$H_{1+s}(A,E|\rho^{A,E}) := \frac{-1}{s}\log \mathrm{Tr}\,(\rho^{A,E})^{1+s}$$
$$H_{1+s}(E|\rho^E) := \frac{-1}{s}\log \mathrm{Tr}\,(\rho^E)^{1+s}$$

with $s \in \mathbb{R}$. When we focus on the total system of a given density $\rho^{A,E}$ and the density matrix ρ describes the state on the composite system $\mathcal{H}_A \otimes \mathcal{H}_E$, $H(A,E|\rho^{A,E})$ and $H_{1+s}(A,E|\rho)$ are simplified to $H(\rho)$ and $H_{1+s}(\rho)$.

A quantum version of the conditional entropy and two kinds of quantum versions of conditional Renyi entropy are given for $s \in \mathbb{R}$:

$$\begin{aligned} H(A|E|\rho) &:= H(A,E|\rho) - H(E|\rho^E) \\ H_{1+s}(A|E|\rho) &:= \frac{-1}{s} \log \mathrm{Tr}\, \rho^{1+s} (I_A \otimes (\rho^E)^{-s}) \\ \overline{H}_{1+s}(A|E|\rho) &:= \frac{-1}{s} \log \mathrm{Tr}\, \rho^{\frac{1+s}{2}} (I_A \otimes (\rho^E)^{-s/2}) \rho^{\frac{1+s}{2}} (I_A \otimes (\rho^E)^{-s/2}). \end{aligned}$$

These quantities can be written in the following way:

$$H(A|E|\rho) = \log |\mathcal{A}| - D(\rho \| \rho^A_{\mathrm{mix}} \otimes \rho^E) \tag{7}$$

$$H_{1+s}(A|E|\rho) = \log |\mathcal{A}| - \frac{1}{s} \psi(s|\rho \| \rho^A_{\mathrm{mix}} \otimes \rho^E) \tag{8}$$

$$\overline{H}_{1+s}(A|E|\rho) = \log |\mathcal{A}| - \frac{1}{s} \underline{\psi}(s|\rho \| \rho^A_{\mathrm{mix}} \otimes \rho^E). \tag{9}$$

When we replace ρ^E by another normalized state σ^E on $\mathcal{H}_E$, we obtain the following generalizations:

$$\begin{aligned} H(A|E|\rho\|\sigma^E) &:= \log |\mathcal{A}| - D(\rho \| \rho^A_{\mathrm{mix}} \otimes \sigma^E) \\ H_{1+s}(A|E|\rho\|\sigma^E) &:= \log |\mathcal{A}| - \frac{1}{s} \psi(s|\rho \| \rho^A_{\mathrm{mix}} \otimes \sigma^E) \\ \overline{H}_{1+s}(A|E|\rho\|\sigma^E) &:= \log |\mathcal{A}| - \frac{1}{s} \underline{\psi}(s|\rho \| \rho^A_{\mathrm{mix}} \otimes \sigma^E). \end{aligned}$$

Then, we obtain

$$H(A|E|\rho\|\sigma^E) = H(A|E|\rho) + D(\rho^E \| \sigma^E) \ge H(A|E|\rho). \tag{10}$$

Using Lemma 2, we obtain the following lemma.

Lemma 3. *$H_{1+s}(A|E|\rho\|\sigma^E)$ and $\overline{H}_{1+s}(A|E|\rho\|\sigma^E)$ are monotone decreasing concerning $s \in \mathbb{R}$. In particular,*

$$H(A|E|\rho\|\sigma^E) \ge H_{1+s}(A|E|\rho\|\sigma^E), \tag{11}$$

$$H(A|E|\rho\|\sigma^E) \ge \overline{H}_{1+s}(A|E|\rho\|\sigma^E) \tag{12}$$

and

$$H_{1+s}(A|E|\rho\|\sigma^E) \le \overline{H}_{1+s}(A|E|\rho\|\sigma^E) \tag{13}$$

for $s > 0$.

When we apply a quantum operation Λ on $\mathcal{H}_E$, since it does not act on the classical system $\mathcal{A}$, (6) implies that

$$H(A|E||\Lambda(\rho)\|\Lambda(\sigma^E)) \ge H(A|E|\rho\|\sigma^E) \tag{14}$$

$$H_{1+s}(A|E|\Lambda(\rho)\|\Lambda(\sigma^E)) \ge H_{1+s}(A|E|\rho\|\sigma^E). \tag{15}$$

When we apply the function f to the classical random number $a \in \mathcal{A}$, $H(f(A), E|\rho) \le H(A, E|\rho)$, i.e.,

$$H(f(A)|E|\rho) \le H(A|E|\rho). \tag{16}$$

For a deeper analysis, we introduce another information quantity $\phi(s|A|E|\rho^{A,E})$:

$$\begin{aligned}\phi(s|A|E|\rho^{A,E}) &:= \log \mathrm{Tr}_E(\mathrm{Tr}_A(\rho^{A,E})^{1/(1-s)})^{1-s} \\ &= \log \mathrm{Tr}_E(\sum_a P^A(a)^{1/(1-s)}\rho_a^{1/(1-s)})^{1-s}.\end{aligned} \tag{17}$$

Taking the limit $s \to 0$, we obtain

$$\begin{aligned}&\frac{d\phi(s|A|E|\rho^{A,E})}{ds}|_{s=0} = \lim_{s\to 0}\frac{\phi(s|A|E|\rho^{A,E})}{s} \\ =&H(E|A|\rho^{A,E}) - H(E|\rho^{A,E}) + H(A|\rho^{A,E}) = -H(A|E|\rho^{A,E}).\end{aligned} \tag{18}$$

Then, we obtain the following lemma:

Lemma 4. *The relation*

$$\max_\sigma sH_{1+s}(A|E|\rho^{A,E}\|\sigma^E) = -(1+s)\phi(\frac{s}{1+s}|A|E|\rho^{A,E}) \tag{19}$$

holds for $s \in (0,\infty)$. The maximum can be realized when $\sigma^E = (\mathrm{Tr}_A(\rho^{A,E})^{1+s})^{1/(1+s)}/\mathrm{Tr}_E(\mathrm{Tr}_A(\rho^{A,E})^{1+s})^{1/(1+s)}$.

For a proof, see Hayashi [16].

2.3 Criteria for Secret Random Numbers

Next, we introduce criteria for quantifying information leaked to the system $\mathcal{H}_E$. Using the trace norm, we can evaluate the secrecy for the state $\rho^{A,E}$ as follows:

$$d_1(A:E|\rho^{A,E}) := \|\rho^{A,E} - \rho^A \otimes \rho^E\|_1. \tag{20}$$

Taking into account the randomness, Renner [6] defined the following criteria for security of a secret random number:

$$d_1'(A|E|\rho^{A,E}) := \|\rho^{A,E} - \rho^A_{\mathrm{mix}} \otimes \rho^E\|_1, \tag{21}$$

which is called the universal composability.

Renner[6] defined the conditional L_2-distance from uniform of ρ relative to a state σ on $\mathcal{H}_E$:

$$\begin{aligned} & d_2(A:E|\rho\|\sigma) \\ :=& \mathrm{Tr}\left((I\otimes\sigma^{-1/4})(\rho-\rho^A_{\mathrm{mix}}\otimes\rho^E)(I\otimes\sigma^{-1/4})\right)^2 \\ =& \mathrm{Tr}\left((I\otimes\sigma^{-1/4})\rho(I\otimes\sigma^{-1/4})\right)^2-\frac{1}{|\mathcal{A}|}\mathrm{Tr}\left(\sigma^{-1/4}\rho^E\sigma^{-1/4}\right)^2 \\ =& e^{-\overline{H}_2(A|E|\rho\|\sigma)}-\frac{1}{|\mathcal{A}|}\mathrm{Tr}\left(\sigma^{-1/4}\rho^E\sigma^{-1/4}\right)^2 \end{aligned}$$

Using this value, we can evaluate $d'_1(A:E|\rho)$ as follows [6, Lemma 5.2.3] when the state σ is a normalized state on $\mathcal{H}_E$:

$$d'_1(A:E|\rho)\le\sqrt{|\mathcal{A}|}\sqrt{d_2(A:E|\rho|\sigma)}. \tag{22}$$

3 Ensemble of Hash Functions

3.1 Ensemble of General Hash Functions

In this section, we focus on an ensemble $\{f_{\mathbf{X}}\}$ of hash functions $f_{\mathbf{X}}$ from $\mathcal{A}$ to $\mathcal{B}$, where $\mathbf{X}$ is a random variable identifying the function $f_{\mathbf{X}}$. In this case, the total information of Eve's system is written as $(E,\mathbf{X})$. Then, by using $\rho^{f_{\mathbf{X}}(A),E,\mathbf{X}}:=\sum_{a\in f_{\mathbf{X}}^{-1}(b),x}P^{\mathbf{X}}(x)|b\rangle\langle b|\otimes\rho^E_a\otimes|x\rangle\langle x|$, the universal composability is written as

$$\begin{aligned} d'_1(f_{\mathbf{X}}(A)|E,\mathbf{X}|\rho^{f_{\mathbf{X}}(A),E,\mathbf{X}}) =& \|\rho^{f_{\mathbf{X}}(A),E,\mathbf{X}}-\rho^B_{\mathrm{mix}}\otimes\rho^{E,\mathbf{X}}\|_1 \\ =& \sum_x P^{\mathbf{X}}(x)\|\rho^{f_{\mathbf{X}=x}(A),E}-\rho^B_{\mathrm{mix}}\otimes\rho^E\|_1 \\ =& \mathrm{E}_{\mathbf{X}}\|\rho^{f_{\mathbf{X}}(A),E}-\rho^B_{\mathrm{mix}}\otimes\rho^E\|_1. \end{aligned} \tag{23}$$

We say that a function ensemble $\mathcal{F}$ is ε-*almost universal*$_2$ [1,2,13], if, for any pair of different inputs a_1,a_2, the collision probability of their outputs is upper bounded as

$$\Pr\left[f_{\mathbf{X}}(a_1)=f_{\mathbf{X}}(a_2)\right]\le\frac{\varepsilon}{|\mathcal{B}|}. \tag{24}$$

The parameter ε appearing in (24) is shown to be confined in the region

$$\varepsilon\ge\frac{|\mathcal{A}|-|\mathcal{B}|}{|\mathcal{A}|-1}, \tag{25}$$

and in particular, an ensemble $\{f_{\mathbf{X}}\}$ with $\varepsilon=1$ is simply called a *universal*$_2$ function ensemble.

Two important examples of universal$_2$ hash function ensembles are the Toeplitz matrices (see, e.g., [3]), and multiplications over a finite field (see, e.g., [1,4]). A modified form of the Toeplitz matrices is also shown to be universal$_2$, which is given by a concatenation (X,I) of the Toeplitz matrix X and the identity matrix I [12]. The (modified) Toeplitz matrices are particularly useful in

practice, because there exists an efficient multiplication algorithm using the fast Fourier transform algorithm with complexity $O(n \log n)$ (see, e.g., [5]).

The following lemma holds for any *universal*$_2$ function ensemble.

Lemma 5 (Renner [6, Lemma 5.4.3]). *Given any composite c-q sub-state $\rho^{A,E}$ on $\mathcal{H}_A \otimes \mathcal{H}_E$ and any normalized state σ^E on $\mathcal{H}_E$. Any universal$_2$ ensemble of hash functions $f_{\mathbf{X}}$ from $\mathcal{A}$ to $\{1, \ldots, M\}$ satisfies*

$$\mathrm{E}_{\mathbf{X}} d_2(f_{\mathbf{X}}(A) : E|\rho^{A,E}\|\sigma^E) \le e^{-\overline{H}_2(A|E|\rho^{A,E}\|\sigma^E)}. \tag{26}$$

More precisely, the inequality

$$\begin{aligned} &\mathrm{E}_{\mathbf{X}} e^{-\overline{H}_2(f_{C_{\mathbf{X}}}(A)|E|\rho^{A,E}\|\sigma^E)} \\ \le &(1 - \frac{1}{M}) e^{-\overline{H}_2(A|E|\rho^{A,E}\|\sigma^E)} + \frac{1}{M} e^{\underline{\psi}(1|\rho^{A,E}\|\sigma^E)} \end{aligned} \tag{27}$$

holds.

3.2 Ensemble of Linear Hash Functions

Tsurumaru and Hayashi[13] focused on linear functions over the finite field $\mathbb{F}_2$. Now, we treat the case of linear functions over a finite field $\mathbb{F}_q$, where q is a power of a prime number p. We assume that sets $\mathcal{A}$, $\mathcal{B}$ are $\mathbb{F}_q^n$, $\mathbb{F}_q^m$ respectively with $n \ge m$, and f are linear functions over $\mathbb{F}_q$. Note that, in this case, there is a kernel C corresponding to a given linear function f, which is a vector space of $n - m$ dimensions or more. Conversely, when given a vector subspace $C \subset \mathbb{F}_q^n$ of $n - m$ dimensions or more, we can always construct a linear function

$$f_C : \mathbb{F}_q^n \to \mathbb{F}_q^n / C \cong \mathbb{F}_q^l, \quad l \le m. \tag{28}$$

That is, we can always identify a linear hash function f_C and a code C.

When $C_{\mathbf{X}} = \mathrm{Ker}\, f_{\mathbf{X}}$, the definition of ε-universal$_2$ function ensemble of (24) takes the form

$$\forall x \in \mathbb{F}_q^n \setminus \{0\}, \quad \Pr[f_{\mathbf{X}}(x) = 0] \le q^{-m}\varepsilon, \tag{29}$$

which is equivalent with

$$\forall x \in \mathbb{F}_q^n \setminus \{0\}, \quad \Pr[x \in C_{\mathbf{X}}] \le q^{-m}\varepsilon. \tag{30}$$

This shows that the ensemble of kernel $\{C_{\mathbf{X}}\}$ contains sufficient information for determining if a function ensemble $\{f_{\mathbf{X}}\}$ is ε-almost universal$_2$ or not.

For a given ensemble of codes $\{C_{\mathbf{X}}\}$, we define its minimum (respectively, maximum) dimension as $t_{\min} := \min_{\mathbf{X}} \dim C_{\mathbf{X}}$ (respectively, $t_{\max} := \max_{r \in I} \dim C_{\mathbf{X}}$). Then, we say that a linear code ensemble $\{C_{\mathbf{X}}\}$ of minimum (or maximum) dimension t is an *ε-almost universal$_2$* code ensemble, if the following condition is satisfied

$$\forall x \in \mathbb{F}_q^n \setminus \{0\}, \quad \Pr[x \in C_{\mathbf{X}}] \le q^{t-n}\varepsilon. \tag{31}$$

In particular, if $\varepsilon = 1$, we call $\{C_{\mathbf{X}}\}$ a *universal$_2$* code ensemble.

3.3 Dual Universality of a Code Ensemble

Based on Tsurumaru and Hayashi[13], we define several variations of the universality of an ensemble of error-correcting codes and the linear functions as follows.

First, we define the dual code ensemble $\{C_{\mathbf{X}}\}^{\perp}$ of a given linear code ensemble $\{C_{\mathbf{X}}\}$ as the set of all dual codes of $C_{\mathbf{X}}$. That is, $\{C_{\mathbf{X}}\}^{\perp} = \{C_{\mathbf{X}}^{\perp}\}$. We also introduce the notion of dual universality as follows. We say that a code ensemble $\{C_{\mathbf{X}}\}$ is *ε-almost dual universal$_2$*, if the dual ensemble $\mathcal{C}^{\perp}$ is ε-almost universal$_2$. Hence, a linear function ensemble $\{f_{\mathbf{X}}\}$ is ε-almost dual universal$_2$, if the kernels $C_{\mathbf{X}}$ of $f_{\mathbf{X}}$ form an ε-almost dual universal$_2$ code ensemble.

An explicit example of a dual universal$_2$ function ensemble (with $\varepsilon = 1$) can be given by the modified Toeplitz matrices mentioned earlier [10], i.e., a concatenation (X, I) of the Toeplitz matrix X and the identity matrix I. This example is particularly useful in practice because it is both universal$_2$ and dual universal$_2$, and also because there exists an efficient algorithm with complexity $O(n \log n)$.

With these preliminaries, we can present the following theorem as an extension of [13, Theorem 2] to the case of the finite field $\mathbb{F}_q$:

Theorem 1. *Any universal$_2$ linear function ensemble $\{f_{\mathbf{X}}\}$ over the finite field $\mathbb{F}_q$ is q-almost dual universal$_2$ function ensemble.*

3.4 Permuted Code Ensemble

In order to treat an example of ε-almost universal$_2$ functions, we consider the case when the distribution is invariant under permutations of the order in $\mathbb{F}_q^n$. Now, S_n denotes the symmetric group of degree n, and $\sigma(i) = j$ means that $\sigma \in S_n$ maps i to j, where $i, j \in \{1, \ldots, n\}$. The code $\sigma(C)$ is defined by $\{x^{\sigma} := (x_{\sigma(1)}, \ldots, x_{\sigma(n)}) | x = (x_1, \ldots, x_n) \in C\}$. Then, we introduce the permuted code ensemble $\{\sigma(C)\}_{\sigma \in S_n}$ of a code C. In this ensemble, σ obeys the uniform distribution on S_n

For an element $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, we can define the empirical distribution p_x on $\mathbb{F}_q$ as $p_x(a) := \#\{i | x_i = a\}/n$. So, we denote the set of the empirical distributions on $\mathbb{F}_q^n$ by $T_{q,n}$. The cardinality $|T_{q,n}|$ is bounded by $(n+1)^{q-1}$. Similarly, we define $T_{q,n}^{+} := T_{q,n} \setminus \{1_0\}$, where 1_0 is the deterministic distribution on $0 \in \mathbb{F}_q$. For given a code $C \subset \mathbb{F}_q^n$, we define

$$\varepsilon_p(C) := \frac{q^n \#\{x \in C | p_x = p\}}{|C| \#\{x \in \mathbb{F}_q^n | p_x = p\}}. \tag{32}$$

and

$$\varepsilon(C) := \max_{p \in T_{q,n}^{+}} \varepsilon_p(C). \tag{33}$$

Then, we obtain the following lemmas, which are generalization of lemmas in [13] to the case of the finite field $\mathbb{F}_q$.

Lemma 6. *The permuted code ensemble* $\{\sigma(C)\}_{\sigma\in S_n}$ *of a code* C *is* $\varepsilon(C)$*-almost universal*$_2$*.*

Proof. For any non-zero element $x' \in \mathbb{F}_q^n$, we fix an empirical distribution $p := p_{x'}$. Then, x' belongs to $\sigma(C)$ with the probability $\frac{\#\{x\in C|p_x=p\}}{\#\{x\in\mathbb{F}_q^n|p_x=p\}}$. That is, the probability that x' belongs to $\sigma(C)$ is less than $\frac{\varepsilon(C)|C|}{q^n}$.

Lemma 7. *For any* $t \le n$*, there exists a* t*-dimensional code* $C \in \mathbb{F}_q^n$ *such that*

$$\varepsilon(C) < (n+1)^{q-1}. \tag{34}$$

Proof. Let $\{C_{\mathbf{X}}\}_{\mathbf{X}}$ be a universal$_2$ code ensemble. Then, any $p \in T_{q,n}^+$ satisfies $\mathrm{E}_{\mathbf{X}}\varepsilon_p(C_{\mathbf{X}}) \le 1$. The Markov inequality yields

$$\Pr\{\varepsilon_p(C_{\mathbf{X}}) \ge |T_{q,n}|\} \le \frac{1}{|T_{q,n}|} \tag{35}$$

and thus

$$\Pr\{\exists p \in T_{q,n}^+,\ \varepsilon_p(C_{\mathbf{X}}) \ge |T_{q,n}|\} \le \frac{|T_{q,n}|-1}{|T_{q,n}|}. \tag{36}$$

Hence,

$$\Pr\{\forall p \in T_{q,n}^+,\ \varepsilon_p(C_{\mathbf{X}}) < |T_{q,n}|\} \ge \frac{1}{|T_{q,n}|}. \tag{37}$$

Therefore, there exists a code C satisfying the desired condition (34).

3.5 δ-Biased Ensemble: Classical Case

Although the contents of this section has a overlap with Tsurumaru and Hayashi[13], we explain the relation with δ-biased ensemble of random variables $\{W_{\mathbf{X}}\}$, which has been introduced by Dodis and Smith[7] because the relation is too complicated. For a given $\delta > 0$, an ensemble of random variables $\{W_{\mathbf{X}}\}$ on $\mathbb{F}_q^n$ is called δ*-biased* when the inequality

$$\mathrm{E}_{\mathbf{X}}(\mathrm{E}_{W_{\mathbf{X}}}(-1)^{x\cdot W_{\mathbf{X}}})^2 \le \delta^2 \tag{38}$$

holds for any $x \in \mathbb{F}_q^n$.

We denote the random variable subject to the uniform distribution on a code $C \in \mathbb{F}_q^n$, by W_C. Then,

$$\mathrm{E}_{W_C}(-1)^{x\cdot W_C} = \begin{cases} 0 & \text{if } x \notin C^\perp \\ 1 & \text{if } x \in C^\perp. \end{cases} \tag{39}$$

Using the above relation, as is suggested in [7, Case 2], we obtain the following lemma.

Lemma 8. *When the l-dimensional code ensemble $\{C_{\mathbf{X}}\}$ is ε-almost dual universal, the ensemble of random variables $\{W_{C_{\mathbf{X}}}\}$ on $\mathbb{F}_q^n$ is $\sqrt{\varepsilon q^{-m}}$-biased.*

In the following, we treat the case of $\mathcal{A} = \mathbb{F}_q^n$. Given a composite state $\rho^{A,E}$ on $\mathcal{H}_A \otimes \mathcal{H}_E$ and a distribution P^W on $\mathcal{A}$, we define another composite state $\rho^{A,E} * P^W := \sum_w P^W(w) \sum_a P^A(a) |a+w\rangle\langle a+w| \otimes \rho_a^E$. Then, we obtain the following.

Lemma 9 ([8, Theorem 3.2]). *For any c-q sub-state $\rho^{A,E}$ on $\mathcal{H}_A \otimes \mathcal{H}_E$ and any normalized state σ^E on $\mathcal{H}_E$, a δ-biased ensemble of random variables $\{W_{\mathbf{X}}\}$ on $\mathcal{A}$ satisfies*

$$\mathrm{E}_{\mathbf{X}} d_2(A:E|\rho^{A,E} * P^{W_{\mathbf{X}}} \|\sigma^E) \le \delta^2 e^{-\overline{H}_2(A|E|\rho^{A,E}\|\sigma^E)}. \tag{40}$$

More precisely,

$$\mathrm{E}_{\mathbf{X}} d_2(A:E|\rho^{A,E} * P^{W_{\mathbf{X}}} \|\sigma^E) \le \delta^2 (1 - \frac{1}{M}) e^{-\overline{H}_2(A|E|\rho^{A,E}\|\sigma^E)}. \tag{41}$$

Indeed, applying Lemma 9 to the concept of "ε-almost dual universal", we obtain the following lemma.

Lemma 10. *Given a c-q sub-state $\rho^{A,E}$ on $\mathcal{H}_A \otimes \mathcal{H}_E$ and a normalized state σ^E on $\mathcal{H}_E$. When $\{C_{\mathbf{X}}\}$ is an m-dimensional and ε-almost dual universal$_2$ code ensemble, the ensemble of hash functions $\{f_{C_{\mathbf{X}}}\}_{C\in\mathcal{C}}$ satisfies*

$$\mathrm{E}_{\mathbf{X}} d_2(f_{C_{\mathbf{X}}}(A):E|\rho^{A,E}\|\sigma^E) \le \varepsilon e^{-\overline{H}_2(A|E|\rho^{A,E}\|\sigma^E)}. \tag{42}$$

More precisely,

$$\begin{aligned} &\mathrm{E}_{\mathbf{X}} e^{-\overline{H}_2(f_{C_{\mathbf{X}}}(A)|E|\rho^{A,E}\|\sigma^E)} \\ \le& \varepsilon (1 - \frac{1}{M}) e^{-\overline{H}_2(A|E|\rho^{A,E}\|\sigma^E)} + \frac{1}{M} e^{\underline{\psi}(1|\rho^{A,E}\|\sigma^E)}. \end{aligned} \tag{43}$$

For a proof for the binary case, see Tsurumaru and Hayashi [13], and for the general case, see Hayashi [16].

Lemma 10 essentially coincides with Lemma 9. However, the concept "δ-biased" does not concern a family of linear hash functions while the concept "ε-almost dual universal$_2$" does it because the former is defined for the family of random variables. That is, the latter is a generalization of universal$_2$ linear hash functions while the former does not. Hence, Lemma 9 cannot directly provide the performance of linear hash functions. Lemma 10 gives how small the leaked information is after the privacy amplification by linear hash functions. Therefore, in the following section, using Lemma 10 we treat the exponential decreasing rate when we apply the privacy amplification by ε-almost dual universal$_2$ linear hash functions.

4 Security Bounds with Rényi Entropy

Similar to Renner [6], combining (22) and Lemma 10, we obtain the following security bound based on the Renyi entropy order 2. Indeed, Renner [6] showed the following inequality with $\varepsilon = 1$ when the ensemble of linear hash functions $\{f_{\mathbf{X}}\}_{\mathbf{X}}$ is universal$_2$.

Lemma 11. *Given a normalized state σ on $\mathcal{H}_E$ and c-q sub-states $\rho^{A,E}$ and $\rho'^{A,E}$ on $\mathcal{H}_A \otimes \mathcal{H}_E$. When an ensemble of linear hash functions $\{f_{\mathbf{X}}\}_{\mathbf{X}}$ from $\mathcal{A}$ to $\{1, \ldots, M\}$ is ε-almost dual universal$_2$, we obtain*

$$\mathrm{E}_{\mathbf{X}} d_1'(f_{\mathbf{X}}(A) : E|\rho^{A,E}) \le \sqrt{\varepsilon} M^{\frac{1}{2}} e^{-\frac{1}{2}\overline{H}_2(A|E|\rho^{A,E}\|\sigma^E)} \tag{44}$$

$$\mathrm{E}_{\mathbf{X}} d_1'(f_{\mathbf{X}}(A) : E|\rho^{A,E}) \le 2\|\rho - \rho'\|_1 + \sqrt{\varepsilon} M^{\frac{1}{2}} e^{-\frac{1}{2}\overline{H}_2(A|E|\rho'^{A,E}\|\sigma^E)}. \tag{45}$$

For a proof, see Hayashi [16].

In order to obtain a better upper bound for $\mathrm{E}_{\mathbf{X}} d_1'(f_{\mathbf{X}}(A) : E|\rho^{A,E})$, we have to choose a suitable ρ' in (45). Choosing a suitable state ρ' with the condition $\|\rho - \rho'\|_1 \le c$ is called smoothing. Renner [6] applies smoothing to min-entropy $H_{\min}(A|E|\rho^{A,E}\|\sigma^E) := -\log \|(I_A \otimes \sigma^E)^{-1/2} \rho^{A,E} (I_A \otimes \sigma^E)^{-1/2}\|$. However, $\overline{H}_2(A|E|\rho^{A,E}\|\sigma^E)$ is larger than $H_{\min}(A|E|\rho^{A,E}\|\sigma^E)$. Hence, the smoothing for $\overline{H}_2(A|E|\rho^{A,E}\|\sigma^E)$ yields a better bound for $\mathrm{E}_{\mathbf{X}} d_1'(f_{\mathbf{X}}(A) : E|\rho^{A,E})$ than the smooth min entropy. In fact, Hayashi [11] applies the smoothing to $\overline{H}_2(A|E|\rho^{A,E}\|\sigma^E)$ in the classical case. In the following, applying the same kind of smoothing to the quantum case, we obtain the following lemma.

Lemma 12. *Given any c-q sub-state $\rho^{A,E}$ on $\mathcal{A}$ and $\mathcal{H}_E$ and any normalized state σ^E on $\mathcal{H}_E$. When an ensemble of linear hash functions $\{f_{\mathbf{X}}\}_{\mathbf{X}}$ from $\mathcal{A}$ to $\{1, \ldots, M\}$ is ε-almost dual universal$_2$, we obtain*

$$\mathrm{E}_{\mathbf{X}} d_1'(f_{\mathbf{X}}(A) : E|\rho^{A,E}) \le (4 + \sqrt{v}\sqrt{\varepsilon}) M^{s/2} e^{-\frac{s}{2} H_{1+s}(A|E|\rho^{A,E}\|\sigma^E)}, \tag{46}$$

for $s \in (0, 1]$, where v is the number of eigenvalues of σ.

Further, the inequalities with $\varepsilon = 1$ hold when the ensemble of linear hash functions $\{f_{\mathbf{X}}\}_{\mathbf{X}}$ is universal$_2$.

The next step is the choice of a suitable σ^E. The optimal σ^E is given in Lemma 4. Hence, the combination of Lemmas 4 and 12 yields the following lemma.

Lemma 13. *Further, when $\rho^{A,E}$ is normalized,*

$$\mathrm{E}_{\mathbf{X}} d_1'(f_{\mathbf{X}}(A) : E|\rho^{A,E}) \le (4 + \sqrt{v'}\sqrt{\varepsilon}) M^{s/2} e^{\frac{1+s}{2}\phi(\frac{s}{1+s}|A|E|\rho^{A,E})} \tag{47}$$

for $s \in (0, 1]$, where v' is the number of eigenvalues of $\mathrm{Tr}_A \rho^{1+s}$.

5 Asymptotic Evaluation

Next, we consider the case when our state is given by the n-fold independent and identical state ρ, i.e., $\rho^{\otimes n}$. In this case, we focus on the optimal generation rate

$$G(\rho^{A,E})$$
$$:= \sup_{\{(f_n,M_n)\}} \left\{ \lim_{n\to\infty} \frac{\log M_n}{n} \Big| \lim_{n\to\infty} d_1'(f_n(A_n) : E_n|(\rho^{A,E})^n) = 0 \right\}.$$

As is shown in [15,6], the amount is calculated to

$$G(\rho) = H(A|E|\rho). \tag{48}$$

In order to treat the speed of this convergence, we focus on the *exponentially decreasing rate (exponent)* of $d_1'(f_n(A) : E|\rho^{\otimes n})$ for a given R. Due to Lemma 12, when a function ensemble $f_{\mathbf{X}^n}$ from $\mathcal{A}^n$ to $\{1,\ldots,\lfloor e^{nR}\rfloor\}$ is $\varepsilon(n)$-almost universal$_2$ and $\varepsilon(n)$ increases polynomially at most,

$$\liminf_{n\to\infty} \frac{-1}{n} \log \mathrm{E}_{\mathbf{X}_n} d_1'(f_{\mathbf{X}^n}(A_n) : E_n|(\rho^{A,E})^{\otimes n}) \ge e_{\phi,q}(\rho^{A,E}|R), \tag{49}$$

where

$$\begin{aligned} e_{\phi,q}(\rho^{A,E}|R) &:= \max_{0\le s\le 1} -\frac{1+s}{2}\phi(\frac{s}{1+s}|\rho^{A,E}) - \frac{s}{2}R \\ &= \max_{0\le t\le \frac{1}{2}} -\frac{1}{2(1-t)}\phi(t|\rho^{A,E}) - \frac{t}{2(1-t)}R. \end{aligned}$$

6 Conclusion

We have derived an upper bound of exponential decreasing rate for the leaked information in the mutual information criterion and the universal composability in the quantum case when we apply a family of ε-almost dual univeresal$_2$ hash functions for privacy amplification. Although the class of families of ε-almost dual univeresal$_2$ hash functions larger than the class of families of univeresal$_2$ linear hash functions, our bounds is quite similar to the known bound [11,12]. Hence, the obtained result suggests a possibility of the existence of an effective privacy amplification protocol with a smaller complexity than known privacy amplification protocols.

Acknowledgments. The author is grateful to Dr. Toyohiro Tsurumaru for a helpful comments. He is also grateful to the referee of the first version of [13] for informing the literatures [7,8]. He also is partially supported by a MEXT Grant-in-Aid for Young Scientists (A) No. 20686026 and Grant-in-Aid for Scientific Research (A) No. 23246071. He is partially supported by the National Institute of Information and Communication Technolgy (NICT), Japan. The Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme.

References

1. Carter, J.L., Wegman, M.N.: Universal Classes of Hash Functions. J. Comput. System Sci. 18, 143–154 (1979)
2. Wegman, M.N., Carter, J.L.: New Hash Functions and Their Use in Authentication and Set Inequality. J. Comput. System Sci. 22, 265–279 (1981)
3. Mansour, Y., Nisan, N., Tiwari, P.: The Computational Complexity of Universal Hashing. In: STOC 1990, Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing, pp. 235–243 (1990)
4. Bennett, C.H., Brassard, G., Crepeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Transactions on Information Theory 41, 1915–1923 (1995)
5. Golub, G.H., Van Loan, C.F.: Matrix Computation, 3rd edn. The John Hopkins University Press (1996)
6. Renner, R.: Security of Quantum Key Distribution. PhD thesis, Dipl. Phys. ETH, Switzerland, 2005; arXiv:quantph/0512258 (2005)
7. Dodis, Y., Smith, A.: Correcting Errors Without Leaking Partial Information. In: STOC 2005, pp. 654–663 (2005)
8. Fehr, S., Schaffner, C.: Randomness Extraction Via δ-Biased Masking in the Presence of a Quantum Attacker. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 465–481. Springer, Heidelberg (2008)
9. Hayashi, M.: Quantum Information: An Introduction. Springer (2006)
10. Hayashi, M.: Upper bounds of eavesdropper's performances in finite-length code with the decoy method. Physical Review A 76, 012329 (2007); Physical Review A 79, 019901(E) (2009)
11. Hayashi, M.: Tight exponential evaluation for universal composablity with privacy amplification and its applications. arXiv:1010.1358 (2010)
12. Hayashi, M.: Exponential decreasing rate of leaked information in universal random privacy amplification. IEEE Transactions on Information Theory 57(6), 3989–4001 (2011)
13. Tsurumaru, T., Hayashi, M.: Dual universality of hash functions and its applications to quantum cryptography. arXiv:1101.0064 (2011)
14. Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A Pseudorandom Generator from any One-way Function. SIAM J. Comput. 28, 1364 (1999)
15. Devetak, I., Winter, A.: Distillation of secret key and entanglement from quantum states. Proc. R. Soc. Lond. A, 461, 207–235 (2005)
16. Hayashi, M.: Classical and quantum security analysis via smoothing of Renyi entropy of order 2. arXiv:1202.0322 (2012)