Commun. Math. Phys. 333, 335–350 (2015)
Digital Object Identifier (DOI) 10.1007/s00220-014-2174-y

Communications in
Mathematical
Physics

Precise Evaluation of Leaked Information with Secure Randomness Extraction in the Presence of Quantum Attacker

Masahito Hayashi[1,2]

[1] Graduate School of Mathematics, Nagoya University, Nagoya, Japan.
E-mail: masahito@math.nagoya-u.ac.jp
[2] Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore

Received: 1 December 2012 / Accepted: 9 August 2014
Published online: 11 November 2014 – © Springer-Verlag Berlin Heidelberg 2014

Abstract: We treat secret key extraction when the eavesdropper has correlated quantum states. We propose quantum privacy amplification theorems different from Renner's, which are based on quantum conditional Rényi entropy of order $1 + s$. Using those theorems, we derive an exponential rate of decrease for leaked information and the asymptotic equivocation rate, which have not been derived hitherto in the quantum setting.

1. Introduction

Extracting secret random numbers in the presence of a quantum attacker is one of the important topics in quantum information theory. The classical version of this topic was discussed by [1–5]. The quantum version is mainly treated by Renner [6] and his collaborators by using a universal$_2$ hash function. Indeed, a universal$_2$ hash function can be implemented efficiently, i.e., with a small amount of calculation. When the classical random variable is correlated with the eavesdropper's quantum state, the existence of a deterministic secure hash function is guaranteed by the privacy amplification theorem shown by Renner [6].

When the size of the generated final random variable is sufficiently small, the final bits are almost independent of the eavesdropper's quantum state. Then, one needs to evaluate the leaked information of the protocol using a universal$_2$ hash function. In order to evaluate the secrecy, Renner [6] showed the privacy amplification theorem under the trace norm distance with the conditional Rényi entropy of order 2. Combining this theorem with the smoothing method, he provided the evaluation for the secrecy of the final random variable. Then, he proved the strong security in the asymptotic setting when the extracted key rate is less than the conditional entropy. However, it is difficult to calculate the exact value of the smoothed conditional Rényi entropy of order 2 with a large system size. Furthermore, he did not provide the speed of the convergence of the security parameter, e.g., the trace norm distance, explicitly. In order to prove the strong

security in the asymptotic setting, he also employed the several properties of symmetric states. In this paper, we derive another type of privacy amplification theorem by using the conditional Rényi entropy of order $1+s$. Then, we can directly show the strong security without use of smoothing nor several properties of symmetric states when the final key size is smaller than the conditional entropy. That is, our method is more direct and gives the speed of convergence of the security measure, whose detail will be explained as follows.

In this paper, we employ the difference of the conditional entropy from the entropy of the uniform random number, which can be regarded as a modification of the quantum mutual information (See (9)). Indeed, the conditional entropy is more suitable for describing the conditional uncertainty of the given system from the physical viewpoint although the trace norm distance is more appropriate from the cryptography viewpoint. Both quantities can describe the conditional uncertainty of the system when the conditional entropy is close to the uniform case. However, when the conditional entropy is far from the uniform case, this quantity can describe the conditional uncertainty of the system properly while the trace norm distance cannot. In order to address both cases uniformly, we use this quantity as our security measure for leaked information.

Using the conditional Rényi entropy of order $1+s$, we propose other types of privacy amplification theorems under the above security measure. For this purpose, a fundamental theorem is derived by extending classical privacy amplification theorems obtained by [5,7]. Using the theorem, we derive an exponential rate of decrease of the security measure. That is, when the extracted key rate is less than the conditional entropy, the security measure goes to zero exponentially. Then, we derive an exponential rate of decrease for leaked information, whose commutative case is the same as that by [5]. Our derivation deviates from [8] in the point that our method does not employ smoothing method. Our exponent is better than that given in [8] under our security measure. Indeed, as is numerically discussed with the classical case in [9], the exponential approach sometimes has an advantage over the second order asymptotics [10,11] when the allowable leaked information is too small. Hence, we focus on the exponent. Furthermore, using the Pinsker inequality, we apply our result to the trace norm distance.

When the extracted key rate is larger than the conditional entropy, the leaked information does not go to zero. In this case, we focus on the maximum conditional entropy rate, which was proposed by Wyner [12] and is called the equivocation rate. After Wyner's proposal [12], the concept has been actively studied and accepted by so many researchers in classical information and communication theory from a more applied view point [13–23]. However, the quantum version has not been treated until now; hence, it was desirable to derive the quantum version. We derive the equivocation rate by treating the minimum leaked information rate. The smoothing method cannot evaluate the leaked information rate in this case while the smoothing method can derive lower bounds for exponential rate decrease [8]. Since our method directly evaluates the information amount leaked to the eavesdropper, it enables us to derive the equivocation rate.

This paper is organized as follows. In Sect. 2, we prepare quantum versions of information quantities. In Sect. 3, we formulate our setting and derive the exponents of leaked information when the key generation rate is less than the conditional entropy rate. In Sect. 4, we compare our exponents with the exponents given by the smoothing method in [8]. In Sect. 5, we derive the equivocation rate as the minimum conditional entropy for a given key generation rate. The proofs for Theorems 1 and 2 are given in the appendix.

2. Information Quantities

In order to treat leaked information after an application of a hash function in the quantum setting, 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 this paper, we denote the state on $\mathcal{H}_E$ by ρ_E^a when the classical information of $\mathcal{H}_A$ is a. When the classical information a is generated with probability $P(a)$, the state of the composite system $\mathcal{H}_A \otimes \mathcal{H}_E$ is $\rho_{AE} = \sum_a P(a)|a\rangle\langle a| \otimes \rho_E^a$. In the following, when the density matrix concerns the composite system $\mathcal{H}_A \otimes \mathcal{H}_E$, we abbreviate the subscript because there is no possibility for confusion. Then, the von Neumann entropies and Rényi entropies are given as[1]

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

with $s \in \mathbb{R}$ and $\rho_E = \mathrm{Tr}_A \rho$. When we focus on the total system of a given density ρ, $H(A, E|\rho)$ and $H_{1+s}(A, E|\rho)$ are simplified to $H(\rho)$ and $H_{1+s}(\rho)$.

We consider two kinds of quantum versions of the conditional entropy for $s \in \mathbb{R}$:

$$\begin{aligned} H(A|E|\rho) &:= H(A, E|\rho) - H(E|\rho) \\ \overline{H}(A|E|\rho) &:= -\mathrm{Tr}\, \rho \log(\rho_E^{-1/2} \rho \rho_E^{-1/2}), \end{aligned}$$

and two kinds of quantum versions of the conditional Rényi entropy for $s \in \mathbb{R}$ [34,35]:

$$\tilde{H}_{1+s}(A|E|\rho) := \frac{-1}{s} \log \mathrm{Tr}\, (\rho_E^{-\frac{s}{2(1+s)}} \rho \rho_E^{-\frac{s}{2(1+s)}})^{1+s}$$

and

$$\overline{H}^*_{1+s}(A|E|\rho) := \frac{-1}{s} \log \mathrm{Tr}\, \rho (\rho_E^{-1/2} \rho \rho_E^{-1/2})^s,$$

where $I_A \otimes \rho_E$ is abbreviated to ρ_E. This abbreviation will be applied in the following discussion. The quantity $\tilde{H}_{1+s}(A|E|\rho)$ is used for the exponential rate of decrease for the security measure in Sect. 3 while $\overline{H}^*_{1+s}(A|E|\rho)$ is used for our derivation of the equivocation rate in Sect. 4. Indeed, while the quantity $\overline{H}^*_2(A|E|\rho) = \tilde{H}_2(A|E|\rho)$ is the same as the quantity $H_2(A|E|\rho)$ given in [6] and the quantity $\overline{H}_2(A|E|\rho)$ given in [8], the quantity $\overline{H}^*_{1+s}(A|E|\rho)$ and $\tilde{H}_{1+s}(A|E|\rho)$ are different from the quantity $\overline{H}_{1+s}(A|E|\rho)$ given in [8] with $0 < s < 1$.

Indeed, our result holds by replacing $\tilde{H}_{1+s}(A|E|\rho)$ by

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

[1] With the relation to the conditional entropies, we describe the information quantity by identifying the quantum system. Hence, we introduce these notations. Indeed, when we fix a state ρ, it is be easily understandable to treat information quantities by identifying the quantum systems.

However, we only discuss $\tilde{H}_{1+s}(A|E|\rho)$. This is because $\tilde{H}_{1+s}(A|E|\rho)$ gives a better evaluation due to the relation $H_{1+s}(A|E|\rho) \le \tilde{H}_{1+s}(A|E|\rho)$ [34, Proposition 4] [35, (13)].

Since the second derivatives of the function $s \mapsto s\overline{H}^*_{1+s}(A|E|\rho)$ is positive, it is concave. Hence, as $0\overline{H}_1(A|E|\rho) = 0$, $\overline{H}^*_{1+s}(A|E|\rho)$ is monotone decreasing for $s \in \mathbb{R}$. Since $\lim_{s\to\infty} \overline{H}^*_{1+s}(A|E|\rho)$ coincides with the min entropy $H_{\min}(A|E|\rho) := -\log \|\rho_E^{-1/2}\rho\rho_E^{-1/2}\|$, $\overline{H}^*_{1+s}(A|E|\rho) \ge H_{\min}(A|E|\rho)$. Furthermore, since the derivative at $s = 0$ of the function $s \mapsto s\overline{H}^*_{1+s}(A|E|\rho)$ is $\overline{H}(A|E|\rho)$, we have the relation $\lim_{s\to 0} \overline{H}^*_{1+s}(A|E|\rho) = \overline{H}(A|E|\rho)$. Hence, this relation and the monotone decreasing property of $\overline{H}^*_{1+s}(A|E|\rho)$ yield

$$\overline{H}(A|E|\rho) \ge \overline{H}^*_{1+s}(A|E|\rho) \tag{2}$$

for $s \in (0, 1]$.

Similar properties hold for $\tilde{H}_{1+s}(A|E|\rho)$. Calculating the derivative at $s = 0$, we have $\lim_{s\to 0} \tilde{H}_{1+s}(A|E|\rho) = H(A|E|\rho)$. As is shown in Appendix C, $\tilde{H}_{1+s}(A|E|\rho)$ is monotone decreasing for s. Then, we have

$$\begin{aligned} H(A|E|\rho) &\ge \tilde{H}_{1+s}(A|E|\rho) \ge \lim_{s\to\infty} \tilde{H}_{1+s}(A|E|\rho) \\ &= -\log \|\rho_E^{-1/2}\rho\rho_E^{-1/2}\| = H_{\min}(A|E|\rho) \end{aligned} \tag{3}$$

for $s > 0$.

Then, the correlation between A and $\mathcal{H}_E$ can be evaluated by two kinds of quantum versions of the mutual information

$$I(A : E|\rho) := D(\rho\|\rho_A \otimes \rho_E) \tag{4}$$

$$\underline{I}(A : E|\rho) := \underline{D}(\rho\|\rho_A \otimes \rho_E) \tag{5}$$

$$D(\rho\|\sigma) := \mathrm{Tr}\, \rho(\log \rho - \log \sigma) \tag{6}$$

$$\underline{D}(\rho\|\sigma) := \mathrm{Tr}\, \rho \log(\sigma^{-1/2}\rho\sigma^{-1/2}). \tag{7}$$

Note that $\rho^{1/2}\log(\sigma^{-1/2}\rho\sigma^{-1/2})\rho^{1/2}$ is called Fujii–Kamei operator relative entropy [24]. As is shown in [8, Lemma 7], we have

$$D(\rho\|\sigma) \ge \underline{D}(\rho\|\sigma). \tag{8}$$

Furthermore, $\underline{D}(\rho\|\sigma)$ is different from Belavkin Staszewski relative entropy $\mathrm{Tr}\, \rho \log (\rho^{1/2}\sigma^{-1}\rho^{1/2})$[25], which is not less than $D(\rho\|\sigma)$ [26, Corollary 2.6.]. Indeed, an opposite inequality of (8) will be also shown as (23) latter. Thanks to both inequalities, the trace version $\underline{D}(\rho\|\sigma)$ of Fujii–Kamei operator relative entropy is close to the usual quantum relative entropy $D(\rho\|\sigma)$ in a special case even in the non-commutative case. The quantity $\underline{D}(\rho\|\sigma)$ plays an important role for resolving the non-commutative difficulty in the following way. A modification of mutual information is defined in (10) by using $\underline{D}(\rho\|\sigma)$, and a variant of privacy amplification theorem is shown with this modification as Theorem 2. Combining Theorem 2 and (23), we derive the minimum leaked information rate based on the usual quantum relative entropy as well as the equivocation rate, e.g., the maximum conditional entropy rate of the extracted keys, which is one of the main results.

By using the completely mixed state $\rho_{\mathrm{mix},A}$ on $\mathcal{A}$, two kinds of quantum versions of the mutual information can be modified to

$$\begin{aligned} I'(A:E|\rho) &:= D(\rho\|\rho_{\mathrm{mix},A}\otimes\rho_E) = I(A:E|\rho) + D(\rho_A\|\rho_{\mathrm{mix},A}) \\ &= I(A:E|\rho)+H(A|\rho_{\mathrm{mix},A})-H(A|\rho_A)=H(A|\rho_{\mathrm{mix},A})-H(A|E|\rho_A), \end{aligned} \tag{9}$$

$$\underline{I}'(A:E|\rho) := \underline{D}(\rho\|\rho_{\mathrm{mix},A}\otimes\rho_E), \tag{10}$$

which satisfy

$$\begin{aligned} I(A:E|\rho) &\le I'(A:E|\rho) \\ \underline{I}(A:E|\rho) &\le \underline{I}'(A:E|\rho) \end{aligned}$$

and

$$H(A|E|\rho) = -I'(A:E|\rho) + \log|\mathcal{A}| \tag{11}$$

$$\overline{H}(A|E|\rho) = -\underline{I}'(A:E|\rho) + \log|\mathcal{A}|. \tag{12}$$

Indeed, the quantity $I(A:E|\rho)$ represents the amount of information leaked to E, and the remaining quantity $D(\rho_A\|\rho_{\mathrm{mix},A})$ describes the difference of the random number A from the uniform random number. So, if the quantity $I'(A:E|\rho)$ is small, we can conclude that the random number A has less correlation with E and is close to the uniform random number. In particular, if the quantity $I'(A:E|\rho)$ goes to zero, the mutual information $I(A:E|\rho)$ goes to zero, and the state ρ_A goes to the completely mixed state $\rho_{\mathrm{mix},A}$. Hence, we can adopt the quantity $I'(A:E|\rho)$ as a measure for qualifying the secret random number.

Using the trace norm, we can evaluate the secrecy for the state ρ as follows:

$$d_1(A:E|\rho) := \|\rho - \rho_A\otimes\rho_E\|_1. \tag{13}$$

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

$$d_1'(A:E|\rho) := \|\rho - \rho_{\mathrm{mix},A}\otimes\rho_E\|_1. \tag{14}$$

Using the quantum version of Pinsker inequality, we obtain

$$d_1(A:E|\rho)^2 \le I(A:E|\rho) \tag{15}$$

$$d_1'(A:E|\rho)^2 \le I'(A:E|\rho). \tag{16}$$

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.,

$$H(f(A)|E|\rho) \le H(A|E|\rho). \tag{17}$$

As is shown in [33, Theirem 1], when we apply a quantum operation $\mathcal{E}$ on $\mathcal{H}_E$, since it does not act on the classical system $\mathcal{A}$,

$$H(A|E|\mathcal{E}(\rho)) \ge H(A|E|\rho) \tag{18}$$

$$\tilde{H}_{1+s}(A|E|\mathcal{E}(\rho)) \ge \tilde{H}_{1+s}(A|E|\rho). \tag{19}$$

When the state σ has the spectral decomposition $\sigma = \sum_i s_i E_i$, the pinching map $\mathcal{E}_\sigma$ is defined as

$$\mathcal{E}_\sigma(\rho) := \sum_i E_i \rho E_i. \tag{20}$$

When v is the number of the distinct eigenvalues of σ, the inequality

$$\rho \le v \mathcal{E}_\sigma(\rho) \tag{21}$$

holds [27, Lemma 3.8], [28]. As $x \mapsto \log x$ is matrix monotone,

$$\log \rho \le \log v + \log \mathcal{E}_\sigma(\rho). \tag{22}$$

Thus,

$$\begin{aligned} D(\rho\|\sigma) &= \mathrm{Tr}\, \rho \log \rho - \mathrm{Tr}\, \rho \log \sigma \le \log v + \mathrm{Tr}\, \rho \log \mathcal{E}_\sigma(\rho) - \mathrm{Tr}\, \rho \log \sigma \\ &= \log v + \mathrm{Tr}\, \mathcal{E}_\sigma(\rho) \log \mathcal{E}_\sigma(\rho) - \mathrm{Tr}\, \mathcal{E}_\sigma(\rho) \log \sigma \\ &= \log v + D(\mathcal{E}_\sigma(\rho)\|\sigma) = \underline{D}(\mathcal{E}_\sigma(\rho)\|\sigma) + \log v. \end{aligned} \tag{23}$$

Therefore, when v is the number of distinct eigenvalues of $\rho_E := \sum_a p(a)\rho_E^a$, an inequality

$$\begin{aligned} I(A:E|\rho) &\le I(A:E|\mathcal{E}_{\rho_E}(\rho)) + \log v \\ &= \underline{I}(A:E|\mathcal{E}_{\rho_E}(\rho)) + \log v \end{aligned} \tag{24}$$

holds.

Using these relations, we can show the following lemma.

Lemma 1.

$$\overline{H}^*_{1+s}(A|E|\rho) \ge \tilde{H}_{1+s}(A|E|\rho). \tag{25}$$

Proof. Applying (21) to the case of $\sigma = \rho_E$, we obtain

$$\rho \le v \mathcal{E}_{\rho_E}(\rho).$$

Hence,

$$\rho_E^{-1/2} \rho \rho_E^{-1/2} \le v \rho_E^{-1/2} \mathcal{E}_{\rho_E}(\rho) \rho_E^{-1/2}.$$

Since $x \to x^s$ is matrix monotone, we obtain

$$[\rho_E^{-1/2} \rho \rho_E^{-1/2}]^s \le v^s [\rho_E^{-1/2} \mathcal{E}_{\rho_E}(\rho) \rho_E^{-1/2}]^s.$$

Hence,

$$\begin{aligned} e^{-s\overline{H}^*_{1+s}(A|E|\rho)} &= \mathrm{Tr}\, \rho [\rho_E^{-1/2} \rho \rho_E^{-1/2}]^s \le v^s \mathrm{Tr}\, \rho [\rho_E^{-1/2} \mathcal{E}_{\rho_E}(\rho) \rho_E^{-1/2}]^s \\ &= v^s \mathrm{Tr}\, \mathcal{E}_{\rho_E}(\rho) [\rho_E^{-1/2} \mathcal{E}_{\rho_E}(\rho) \rho_E^{-1/2}]^s = v^s e^{-s\overline{H}^*_{1+s}(A|E|\mathcal{E}_{\rho_E}(\rho))} \\ &= v^s e^{-s\tilde{H}_{1+s}(A|E|\mathcal{E}_{\rho_E}(\rho))} \le v^s e^{-s\tilde{H}_{1+s}(A|E|\rho)}, \end{aligned} \tag{26}$$

where (19) is used in the final inequality. By letting v_n be the number of distinct eigenvalues of $\rho_E^{\otimes n}$, the logarithm of (26) yields

$$\begin{aligned} n\overline{H}^*_{1+s}(A|E|\rho) + \frac{\log v_n^s}{s} &= \overline{H}^*_{1+s}(A|E|\rho^{\otimes n}) + \log v_n \\ &\ge \tilde{H}_{1+s}(A|E|\rho^{\otimes n}) = n\tilde{H}_{1+s}(A|E|\rho), \end{aligned}$$

Taking the limit $n \to \infty$, we obtain (25).

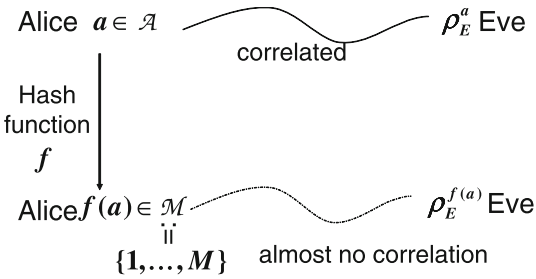

Fig. 1. Application of hash function

3. Formulation and Exponential Rate of Decrease

We consider the secure key extraction problem from a common classical random number $a \in \mathcal{A}$ which has been partially eavesdropped as quantum states by Eve. For this problem, it is assumed that Alice and Bob share a common classical random number $a \in \mathcal{A}$, and Eve has a quantum state ρ_E^a in the quantum system $\mathcal{H}_E$, which is correlated to the random number a. The task is to extract a common random number $f(a)$ from the random number $a \in \mathcal{A}$, which is almost independent of Eve's quantum state. Here, Alice and Bob are only allowed to apply the same function f to the common random number $a \in \mathcal{A}$ as Fig. 1. Now, we focus on an ensemble of the functions $f_{\mathbf{X}}$ from $\mathcal{A}$ to $\{1, \ldots, M\}$, where $\mathbf{X}$ denotes a random variable describing the stochastic behavior of the function f. An ensemble of the functions $f_{\mathbf{X}}$ is called universal$_2$ when it satisfies the following condition [29]:

Condition 1. $\forall (a_1, a_2) \in \mathcal{A}^2$ *with* $a_1 \neq a_2$, *the probability that* $f_{\mathbf{X}}(a_1) = f_{\mathbf{X}}(a_2)$ *is at most* $\frac{1}{M}$.

Indeed, when the cardinality $|\mathcal{A}|$ is a power of a prime power q and M is another power of the same prime power q, an ensemble $\{f_{\mathbf{X}}\}$ satisfying both conditions is given by the the concatenation of Toeplitz matrix and the identity $(\mathbf{X}, I)$ [30] only with $\log_q |\mathcal{A}| - 1$ random variables taking values in the finite filed $\mathbb{F}_q$. That is, the matrix $(\mathbf{X}, I)$ be efficiently constructed.

Theorem 1. *When the ensemble of the functions* $\{f_{\mathbf{X}}\}$ *is universal*$_2$, *it satisfies*

$$\begin{aligned} I(f_{\mathbf{X}}(A) : E, \mathbf{X}|\rho, P^{\mathbf{X}}) &\le I'(f_{\mathbf{X}}(A) : E, \mathbf{X}|\rho, P^{\mathbf{X}}) = \mathrm{E}_{\mathbf{X}} I'(f_{\mathbf{X}}(A) : E|\rho) \\ &\le \frac{v^s M^s}{s} e^{-s\tilde{H}_{1+s}(A|E|\rho)} = v^s \frac{e^{s(\log M - \tilde{H}_{1+s}(A|E|\rho))}}{s}, \end{aligned} \tag{27}$$

where v *is the number of distinct eigenvalues of* ρ_E.

That is, there exists a function $f : \mathcal{A} \to \{1, \ldots, M\}$ such that

$$I'(f(A) : E|\rho) \le v^s \frac{e^{s(\log M - \tilde{H}_{1+s}(A|E|\rho))}}{s}. \tag{28}$$

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

$$\begin{aligned} G(\rho) :=& \sup_{\{(f_n,M_n)\}} \left\{ \lim_{n\to\infty} \frac{\log M_n}{n} \left| \begin{array}{l} \lim_{n\to\infty} \frac{1}{n} I(f_n(A):E|\rho^{\otimes n}) = 0 \\ \lim_{n\to\infty} \frac{H(f_n(A)|\rho^{\otimes n})}{\log M_n} = 1 \end{array} \right. \right\} \\ =& \sup_{\{(f_n,M_n)\}} \left\{ \lim_{n\to\infty} \frac{\log M_n}{n} \left| \lim_{n\to\infty} \frac{I'(f_n(A):E|\rho^{\otimes n})}{n} = 0 \right. \right\}, \end{aligned}$$

whose classical version is treated by [1]. The second equation holds as follows. the condition $\lim_{n\to\infty} \frac{H(f_n(A)|\rho^{\otimes n})}{\log M_n} = 1$ is equivalent with $\lim_{n\to\infty} \frac{D(\rho_{f_n(A)}\|\rho_{\mathrm{mix},f_n(A)})}{n} = 0$. Hence, $\lim_{n\to\infty} \frac{I(f_n(A):E|\rho^{\otimes n})}{n} = 0$ and $\lim_{n\to\infty} \frac{H(f_n(A)|\rho^{\otimes n})}{\log M_n} = 1$ if and only if $\lim_{n\to\infty} \frac{I'(f_n(A):E|\rho^{\otimes n})}{n} = 0$.

When the generation rate $R = \lim_{n\to\infty} \frac{\log M_n}{n}$ is smaller than $H(A|E)$, there exists a sequence of functions $f_n : \mathcal{A}^n \to \{1,\ldots,e^{nR}\}$ such that

$$I'(f_n(A):E|\rho^{\otimes n}) \le v_n^s \frac{e^{s(R-\tilde{H}_{1+s}(A|E|\rho^{\otimes n}))}}{s}, \tag{29}$$

where v_n is the number of distinct eigenvalues of $\rho_E^{\otimes n}$, which is polynomially increasing for n. Since $\lim_{s\to 0} \tilde{H}_{1+s}(A|E|\rho) = H(A|E|\rho)$, there exists a number $s \in (0,1]$ such that $s(R - \tilde{H}_{1+s}(A|E|\rho)) > 0$. Thus, the right hand side of (29) goes to zero exponentially. Conversely, due to (17), any sequence of functions $f_n : \mathcal{A}^n \mapsto \{1,\ldots,e^{nR}\}$ satisfies that

$$\lim_{n\to\infty} \frac{H(f_n(A)|E|\rho^{\otimes n})}{n} \le \frac{H(A|E|\rho^{\otimes n})}{n} = H(A|E|\rho). \tag{30}$$

When $\lim_{n\to\infty} \frac{H(f_n(A)|\rho^{\otimes n})}{nR} = 1$,

$$\begin{aligned} \lim_{n\to\infty} \frac{I(f_n(A):E|\rho^{\otimes n})}{n} &= R - \lim_{n\to\infty} \frac{H(f_n(A)|E|\rho^{\otimes n})}{n} \\ &\ge R - H(A|E|\rho). \end{aligned} \tag{31}$$

That is, when $R > H(A|E|\rho)$, $\frac{I(f_n(A):E|\rho^{\otimes n})}{n}$ does not go to zero. Hence, we reproduce the known result [6,31]:

$$G(\rho) = H(A|E|\rho). \tag{32}$$

In order to treat the speed of this convergence, we focus on the supremum of the *exponential rate (exponent)* of decrease of $I'(f_n(A):E|\rho^{\otimes n})$ for a given R

$$e_I(\rho|R) := \sup_{\{(f_n,M_n)\}} \left\{ \lim_{n\to\infty} \frac{-\log I'(f_n(A):E|\rho^{\otimes n})}{n} \left| \lim_{n\to\infty} \frac{-\log M_n}{n} \le R \right. \right\}.$$

Since the relation $s\tilde{H}_{1+s}(A|E|\rho^{\otimes n}) = ns\tilde{H}_{1+s}(A|E|\rho)$ holds, the inequality (29) implies that

$$\begin{aligned} e_I(\rho|R) \geq e_H(\rho|R) &:= \max_{0\leq s\leq 1} s\tilde{H}_{1+s}(A|E|\rho) - sR \\ &= \max_{0\leq s\leq 1} s(\tilde{H}_{1+s}(A|E|\rho) - R), \end{aligned} \tag{33}$$

whose commutative version coincides with the bound given in [5].

Next, we apply our evaluation to the measure $d_1'(A : E|\rho)$. When $\{f_{\mathbf{X}}\}$ satisfies Condition 1, combining (16) and (27), we obtain

$$\begin{aligned} \mathrm{E}_{\mathbf{X}} d_1'(f_{\mathbf{X}}(A) : E|\rho) &\leq \sqrt{\mathrm{E}_{\mathbf{X}} d_1'(f_{\mathbf{X}}(A) : E|\rho)^2} \\ &\leq \frac{v^{s/2}M^{s/2}}{\sqrt{s}} e^{-\frac{s}{2}\tilde{H}_{1+s}(A|E|\rho)}. \end{aligned} \tag{34}$$

That is, in the n-fold asymptotic setting, when the generation key rate is R, we focus on the supremum of the *exponential rate (exponent)* of decrease of $I(f_n(A) : E|\rho^{\otimes n})$ for a given R

$$e_d(\rho|R) := \sup_{\{(f_n, M_n)\}} \left\{ \lim_{n\to\infty} \frac{-\log d_1'(f_n(A) : E|\rho^{\otimes n})}{n} \middle| \lim_{n\to\infty} \frac{-\log M_n}{n} \leq R \right\}.$$

Then, the inequality (34) implies that $e_d(\rho|R) \geq \frac{e_H(\rho|R)}{2}$. However, when ρ is commutative, the paper [32] gave another lower bound of $e_d(\rho|R)$, which is tighter than $\frac{e_H(\rho|R)}{2}$.

4. Comparison with Smoothing Method

The paper [8] derived lower bounds for $e_I(\rho|R)$ and $e_d(\rho|R)$. In order to describe them, we introduce an information quantity $\phi(s|A|E|\rho)$:

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

This quantity satisfies the following lemma.

Lemma 2. [8, Lemma 11] *The inequalities*

$$sH_{1+s}(A|E|\rho) \geq -\phi(s|A|E|\rho) \tag{35}$$

$$sH_{1+s}(A|E|\rho) \leq -(1+s)\phi(\frac{s}{1+s}|A|E|\rho) \tag{36}$$

hold for $0 \leq s \leq 1$.

Then, the paper [8] showed that

$$e_d(\rho|R) \geq e_{\phi,q}(\rho|R) \tag{37}$$

$$e_I(\rho|R) \geq e_{H,q}(\rho|R) \tag{38}$$

$$e_I(\rho|R) \geq e_{\phi,q}(\rho|R), \tag{39}$$

where

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

As a relation, we obtain the following lemma.

Lemma 3. *The quantity $e_H(\rho|R)$ defined in (33) satisfies that*

$$e_H(\rho|R) \ge e_{H,q}(\rho|R) \tag{40}$$
$$e_H(\rho|R) \ge e_{\phi,q}(\rho|R). \tag{41}$$

In fact, when the maximum in (33) is not realized by $s = 1$, Inequality (40) is strict. When the maximum in (33) is not realized by $s \in [0, \frac{1}{2}]$, Inequality (41) is strict.

Hence, when the maximum in (33) is realized only by $s \in (\frac{1}{2}, 1)$, our lower bound $e_H(\rho|R)$ for $e_I(\rho|R)$ is strictly better than those given in [8]. This fact implies that our method is better than the smoothing method used in [8] under the modified mutual information measure.

Proof. We have

$$\begin{aligned} e_H(\rho|R) &= \max_{0\le s\le 1} s(\tilde{H}_{1+s}(A|E|\rho) - R) \\ &\ge \max_{0\le s\le 1} s(H_{1+s}(A|E|\rho) - R) \\ &\ge \max_{0\le s\le 1} \frac{s}{2-s}(H_{1+s}(A|E|\rho) - R) = e_{H,q}(\rho|R), \end{aligned}$$

which implies (40). From the above derivation, we can find that Inequality (40) is strict when the maximum in (33) is not realized by $s = 1$.

Furthermore, (35) yields that

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

which implies (41). From the above derivation, we can find that Inequality (41) is strict when the maximum in (33) is not realized by $s \in [0, \frac{1}{2}]$.

5. Equivocation Rate

Next, we consider the case when $\log M$ is larger than $H(A|E|\rho)$.

Theorem 2. *When the ensemble of the functions $\{f_{\mathbf{X}}\}$ is universal$_2$, it satisfies*

$$\begin{aligned} \mathrm{E}_{\mathbf{X}} e^{s\underline{I}'(f_{\mathbf{X}}(A):E|\rho)} &\le 1 + M^s e^{-s\overline{H}^*_{1+s}(A|E|\rho)} \\ &= 1 + e^{s(\log M - \overline{H}^*_{1+s}(A|E|\rho))}. \end{aligned} \tag{42}$$

Using (42) and the concavity of $x \mapsto \log x$, we obtain

$$\begin{aligned} s\mathrm{E}_{\mathbf{X}} \underline{I}'(f_{\mathbf{X}}(A) : E|\rho) &\le \log \mathrm{E}_{\mathbf{X}} e^{s\underline{I}'(f_{\mathbf{X}}(A):E|\rho)} \\ &\le \log(1 + e^{s(\log M - \overline{H}^*_{1+s}(A|E|\rho))}) \le e^{s(\log M - \overline{H}^*_{1+s}(A|E|\rho))}, \end{aligned}$$

which can be regarded as another version of (27).

Hence, (24), (42), and (19) guarantee that

$$\begin{aligned} \mathrm{E}_{\mathbf{X}} e^{sI'(f_{\mathbf{X}}(A):E|\rho)} &\le v^s \mathrm{E}_{\mathbf{X}} e^{sI'(f_{\mathbf{X}}(A):E|\mathcal{E}_{\rho_E}(\rho))} \\ &\le v^s (1 + M^s e^{-s\overline{H}^*_{1+s}(A|E|\mathcal{E}_{\rho_E}(\rho))}) \\ &= v^s (1 + M^s e^{-s\tilde{H}_{1+s}(A|E|\mathcal{E}_{\rho_E}(\rho))}) \\ &\le v^s (1 + M^s e^{-s\tilde{H}_{1+s}(A|E|\rho)}) = v^s (1 + e^{s(\log M - \tilde{H}_{1+s}(A|E|\rho))}), \end{aligned}$$

where v is the number of distinct eigenvalues of ρ_E. Since

$$\begin{aligned} &\log v^s (1 + e^{s(\log M - \tilde{H}_{1+s}(A|E|\rho))}) \\ &= s \log v + \log(1 + e^{s(\log M - \tilde{H}_{1+s}(A|E|\rho))}) \\ &\le s \log v + \log 2 + \log \max\{1, e^{s(\log M - \tilde{H}_{1+s}(A|E|\rho))}\} \\ &= s \log v + \log 2 + \max\{0, s(\log M - \tilde{H}_{1+s}(A|E|\rho))\}, \end{aligned}$$

using (11), we obtain the following theorem:

Theorem 3. *There exists a function $f : \mathcal{A} \mapsto \{1, \ldots, M\}$ such that*

$$\begin{aligned} \log M - H(f(A)|E|\rho) &= I'(f(A) : E|\rho) \\ &\le \log v + \frac{\log 2}{s} + \max\{0, \log M - \tilde{H}_{1+s}(A|E|\rho)\}. \end{aligned}$$

for $s \in (0, 1]$.

Next, we consider the case when our state is given by the n-fold independent and identical state ρ, i.e., $\rho^{\otimes n}$. Then, we define the *equivocation rate* as the maximum Eve's ambiguity rate for the given key generation rate R:

$$\mathcal{R}(R|\rho) := \sup_{\{f_n\}} \{ \lim_{n\to\infty} \frac{H(f_n(A)|E|\rho^{\otimes n})}{n} | \lim_{n\to\infty} \frac{H(f_n(A)|\rho^{\otimes n})}{nR} = 1\},$$

where the supremum takes the map f_n that maps from $\mathcal{A}^n$ to $\{1, \ldots, e^{nR}\}$. Then, we obtain the following theorem.

Theorem 4. *When the key generation rate R is greater than $H(A|E|\rho)$,*

$$\mathcal{R}(R|\rho) = H(A|E|\rho). \tag{43}$$

Indeed, using the above theorem, we can calculate the minimum information rate for the given key generation rate R as follows.

$$\begin{aligned}&\inf_{\{f_n\}}\{\lim_{n\to\infty}\frac{I(E:f_n(A)|\rho^{\otimes n})}{n}|\lim_{n\to\infty}\frac{H(f_n(A)|\rho^{\otimes n})}{nR}=1\}\\ &=\max\{R-H(A|E|\rho),0\}.\end{aligned}$$

Proof. When the key generation rate R, i.e., $M_n = e^{nR}$, there exists a sequence of functions $f_n : \mathcal{A}^n \mapsto \{1,\ldots,M_n\}$ such that

$$R - \lim_{n\to\infty}\frac{H(E|f_n(A)|\rho^{\otimes n})}{n} \le \max\{0, R - \tilde{H}_{1+s}(A|E|\rho)\}$$

for $s \in (0, 1]$. Then, taking the limit $s \to 0$, we obtain

$$R - \lim_{n\to\infty}\frac{H(E|f_n(A)|\rho^{\otimes n})}{n} \le \max\{0, R - H(A|E|\rho)\},$$

which implies the part $\le$ of (43). Converse inequality $\ge$ of (43) follows from (30).

6. Conclusion

We have derived an upper bound of information leaked to a quantum attacker in the modified quantum mutual information measure when we apply universal$_2$ hash functions. In the commutative case, our lower bound coincides with the bound given in [5]. In the non-commutative case, our bound is different from Renner's [6] two universal hashing lemma even in $s = 1$ because Renner's [6] result is based on $\tilde{H}_2(A|E|\rho) = \overline{H}^*_2(A|E|\rho)$ but ours is based on $\tilde{H}_{1+s}(A|E|\rho)$.

Applying our bound to the i.i.d. case, we have obtained a lower bound for the exponential rate of decrease for information leaked to a quantum attacker under the modified mutual information measure. Our lower bound is better than lower bounds derived by the smoothing method in [8].

Furthermore, we have derived the asymptotic equivocation rate. In order to show it, we have derived a quantum version of privacy amplification theorems, whose classical version is given in [5,7]. In this quantum version, we have employed $\overline{H}^*_{1+s}(A|E|\rho)$ instead of $H_{1+s}(A|E|\rho)$. In the second step for the derivation, we have employed $\tilde{H}_{1+s}(A|E|\rho)$. Then, the asymptotic equivocation rate can be characterized by $\tilde{H}(A|E|\rho)$, which is given by the limit $\lim_{s\to 0}\tilde{H}_{1+s}(A|E|\rho)$.

Acknowledgements. The author is grateful to the referee for his helpful comments. He 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.

A. Proof of Theorem 1

In order to show Theorem 1, we prepare the following two lemmas.

Lemma 4. *The matrix inequality* $(I + X)^s \le I + X^s$ *holds with a non-negative matrix* X *and* $s \in (0, 1]$.

Proof. Since I is commutative with X, it is sufficient to show that $(1 + x)^s \le 1 + x^s$ for $x \ge 0$. This inequality is trivial.

Lemma 5. *The matrix inequality* $\log(I + X) \le \frac{1}{s} X^s$ *holds with a non-negative matrix* X *and* $s \in (0, 1]$.

Proof. Since I is commutative with X, it is sufficient to show that $\log(1 + x) \le \frac{x^s}{s}$ for $x \ge 0$. Since the inequalities $(1 + x)^s \le 1 + x^s$ and $\log(1 + x) \le x$ hold for $x \ge 0$ and $0 < s \le 1$, the inequalities

$$\log(1 + x) = \frac{\log(1 + x)^s}{s} \le \frac{\log(1 + x^s)}{s} \le \frac{x^s}{s} \tag{44}$$

hold.

Now, we prove Theorem 1.

$$\begin{aligned}
&\mathrm{E}_{\mathbf{X}} I'(f_{\mathbf{X}}(A) : E|\rho) \\
&= \mathrm{E}_{\mathbf{X}} D(\sum_{i=1}^{M} |i\rangle\langle i| \otimes \sum_{a: f_{\mathbf{X}}(a)=i} P(a)\rho_E^a \| \frac{1}{M} I \otimes \rho_E) \\
&= \mathrm{E}_{\mathbf{X}} \sum_a \mathrm{Tr}\, P(a)\rho_E^a (\log(\sum_{a': f_{\mathbf{X}}(a')=f_{\mathbf{X}}(a)} P(a')\rho_{a'}^E) - \log \frac{1}{M}\rho_E) \\
&\le \sum_a P(a)\mathrm{Tr}\, \rho_E^a (\log(\mathrm{E}_{\mathbf{X}} \sum_{a': f_{\mathbf{X}}(a')=f_{\mathbf{X}}(a)} P(a')\rho_{a'}^E) - \log \frac{1}{M}\rho_E) \qquad (45) \\
&= \sum_a P(a)\mathrm{Tr}\, \rho_E^a (\log(P(a)\rho_E^a + \mathrm{E}_{\mathbf{X}} \sum_{a': f_{\mathbf{X}}(a')=f_{\mathbf{X}}(a), a'\neq a} P(a')\rho_{a'}^E) - \log \frac{1}{M}\rho_E) \\
&\le \sum_a P(a)\mathrm{Tr}\, \rho_E^a (\log(P(a)\rho_E^a + \frac{1}{M} \sum_{a': a'\neq a} P(a')\rho_{a'}^E) - \log \frac{1}{M}\rho_E) \qquad (46) \\
&\le \sum_a P(a)\mathrm{Tr}\, \rho_E^a (\log(P(a)\rho_E^a + \frac{1}{M}\rho_E) - \log \frac{1}{M}\rho_E) \\
&\le \sum_a P(a)\mathrm{Tr}\, \rho_E^a (\log(vP(a)\mathcal{E}_{\rho_E}(\rho_E^a) + \frac{1}{M}\rho_E) - \log \frac{1}{M}\rho_E) \qquad (47) \\
&= \sum_a P(a)\mathrm{Tr}\, \rho_E^a \log(vMP(a)\mathcal{E}_{\rho_E}(\rho_E^a)\rho_E^{-1} + I), \qquad (48)
\end{aligned}$$

where (45) follows from the matrix convexity of $x \mapsto \log x$, (46) follows from Condition 1 and the matrix monotonicity of $x \mapsto \log x$, (47) follows from (21) and the matrix monotonicity of $x \mapsto \log x$, and (48) follows from the commutativity of $\mathcal{E}_{\rho_E}(\rho_E^a)$ and ρ_E.

Using Lemma 5, we obtain

$$\begin{aligned}
&\sum_a P(a)\mathrm{Tr}\,\rho_E^a \log(vMP(a)\mathcal{E}_{\rho_E}(\rho_E^a)\rho_E^{-1}+I)\\
&\le \frac{1}{s}\sum_a P(a)\mathrm{Tr}\,\rho_E^a (vMP(a)\mathcal{E}_{\rho_E}(\rho_E^a)\rho_E^{-1})^s\\
&= \frac{v^s M^s}{s}\sum_a P(a)^{1+s}\mathrm{Tr}\,\mathcal{E}_{\rho_E}(\rho_E^a)^{1+s}(\rho_E)^{-s}\\
&= \frac{v^s M^s}{s} e^{-s\tilde{H}_{1+s}(A|E|\mathcal{E}_{\rho_E}(\rho))} \le \frac{v^s M^s}{s} e^{-s\tilde{H}_{1+s}(A|E|\rho)}, \qquad (49)
\end{aligned}$$

where (49) follows from (19).

B. Proof of Theorem 2

The relations (2) and (12) imply

$$s\underline{I}'(B:E|\rho) \le \log \sum_b P(b)\mathrm{Tr}\,\rho_E^b (|\mathcal{B}|P(b)\rho_E^{-1/2}\rho_E^b\rho_E^{-1/2})^s.$$

Substituting $f(A)$ into B, we have

$$\begin{aligned}
&\mathrm{E}_{\mathbf{X}} e^{s\underline{I}'(f_{\mathbf{X}}(A):E|\rho)}\\
&\le \mathrm{E}_{\mathbf{X}} \sum_a P(a)\mathrm{Tr}\,\rho_E^a (M\rho_E^{-1/2}(\sum_{a':f_{\mathbf{X}}(a')=f_{\mathbf{X}}(a)} P(a')\rho_{a'}^E)\rho_E^{-1/2})^s\\
&\le \sum_a P(a)\mathrm{Tr}\,\rho_E^a (M\rho_E^{-1/2}\mathrm{E}_{\mathbf{X}}(\sum_{a':f_{\mathbf{X}}(a')=f_{\mathbf{X}}(a)} P(a')\rho_{a'}^E)\rho_E^{-1/2})^s \qquad (50)\\
&= \sum_a P(a)\mathrm{Tr}\,\rho_E^a (M\rho_E^{-1/2}(P(a)\rho_E^a + \mathrm{E}_{\mathbf{X}}(\sum_{a':f_{\mathbf{X}}(a')=f_{\mathbf{X}}(a),a\neq a'} P(a')\rho_{a'}^E))\rho_E^{-1/2})^s\\
&\le \sum_a P(a)\mathrm{Tr}\,\rho_E^a (M\rho_E^{-1/2}(P(a)\rho_E^a + \frac{1}{M}(\sum_{a':a\neq a'} P(a')\rho_{a'}^E))\rho_E^{-1/2})^s \qquad (51)\\
&\le \sum_a P(a)\mathrm{Tr}\,\rho_E^a (M\rho_E^{-1/2}(P(a)\rho_E^a + \frac{1}{M}\rho_E)\rho_E^{-1/2})^s\\
&= \sum_a P(a)\mathrm{Tr}\,\rho_E^a (I + MP(a)\rho_E^{-1/2}\rho_E^a\rho_E^{-1/2})^s\\
&\le \sum_a P(a)\mathrm{Tr}\,\rho_E^a (I + M^s P(a)^s(\rho_E^{-1/2}\rho_E^a\rho_E^{-1/2})^s) \qquad (52)\\
&= 1 + M^s \sum_a P(a)^{1+s}\mathrm{Tr}\,\rho_E^a(\rho_E^{-1/2}\rho_E^a\rho_E^{-1/2})^s\\
&= 1 + M^s e^{-s\overline{H}^*_{1+s}(A|E|\rho)}
\end{aligned}$$

where (50) follows from the matrix convexity of $x \mapsto x^s$, and (51) follows from Condition 1 and the matrix monotonicity of $x \mapsto x^s$, and (52) follows from Lemma 4.

C. Monotone Decreasing Property of $\widetilde{H}_{1+s}(A|E|\rho)$

First, as shown in [36, Corollary III.8], we notice that

$$\tilde{H}_{1+s}(A|E|\rho) = \lim_{n\to\infty} \frac{1}{n} \tilde{H}_{1+s}(A|E|\mathcal{E}_{\rho_E^{\otimes n}}(\rho^{\otimes n})). \tag{53}$$

Since $\tilde{H}_{1+s}(A|E|\mathcal{E}_{\rho_E^{\otimes n}}(\rho^{\otimes n})) = \overline{H}^{*}_{1+s}(A|E|\mathcal{E}_{\rho_E^{\otimes n}}(\rho^{\otimes n}))$, $\tilde{H}_{1+s}(A|E|\mathcal{E}_{\rho_E^{\otimes n}}(\rho^{\otimes n}))$ is monotone decreasing for s. Thus, $\tilde{H}_{1+s}(A|E|\rho)$ is also monotone decreasing for s.

References

1. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography part 1: Secret sharing. IEEE Trans. Inform. Theory **39**(4), 1121–1132 (1993)
2. Bennett, C.H., Brassard, G., Crepeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inform. Theory **41**, 1915–1923 (1995)
3. Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. SIAM J. Comput **28**, 1364 (1999)
4. Renner, R., Wolf, S.: Simple and Tight Bounds for Information Reconciliation and Privacy Amplification, ASIACRYPT 2005, Lecture Notes in Computer Science, vol. 3788: SIAM J. Comput. pp. 199–216 (2005)
5. Hayashi, M.: Exponential decreasing rate of leaked information in universal random privacy amplification. IEEE Trans. Inf. Theory **57**(6), 3989–4001 (2011)
6. Renner, R.: Security of Quantum Key Distribution, Ph.D. thesis, Dipl. Phys. ETH, Switzerland (2005). arXiv:quantph/0512258
7. Matsumoto, R., Hayashi, M.: Universal Strongly Secure Network Coding with Dependent and Non-Uniform Messages (2011). arXiv:1111.4174
8. Hayashi, M.: Large deviation analysis for classical and quantum security via approximate smoothing (2012). arXiv:1202.0322. Accepted for IEEE Transactions on Information Theory
9. Watanabe, S., Hayashi, M.: Non-Asymptotic Analysis of Privacy Amplification via Renyi Entropy and Inf-Spectral Entropy. In: 2013 IEEE International Symposium on Information Theory (ISIT 2013) Istanbul, Turkey, pp. 2715–2719. 7–12 July 2013
10. Hayashi, M.: Second-order asymptotics in fixed-length source coding and intrinsic randomness. IEEE Trans. Inf. Theory **54**, 4619–4637 (2008)
11. Tomamichel, M., Hayashi, M.: A hierarchy of information quantities for finite block length analysis of quantum tasks. IEEE Trans. Inf. Theory **59**(11), 7693–7710 (2013)
12. Wyner, A.D.: The wire-tap channel. Bell. Syst. Tech. J. **54**, 1355–1387 (1975)
13. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. IEEE Trans. Inform. Theory **24**(3), 339–348 (1978)
14. Marina, N., Yagi, H., Poor, H.V.: Improved Rate-Equivocation Regions for Secure Cooperative Communication. arXiv:1102.3500. In: Proceedings of the 2011 IEEE ISIT St. Petersburg, Russia, July 2011, pp. 2871–2875
15. Shafee, S., Ulukus, S.: Achievable Rates in Gaussian MISO Channels with Secrecy Constraints. In: Proceedings of the 2007 IEEE ISIT, Nice, France, June. pp. 2466–2470 (2007)
16. Xu, J., Chen, B.: An outer bound to the rate equivocation region of broadcast channels with two confidential messages. In: Proceedings of the Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. New Orleans, LA, USA, pp. 1–5, Nov–Dec 2008
17. Liang, Y., Poor, H.V.: Multiple-access channels with confidential messages. IEEE Trans. Inform. Theory **54**(3), 976–1002 (2008)
18. Oggier, F., Hassibi, B.: The secrecy capacity of the MIMO wiretap channel. In: Proceedings of the 2008 IEEE ISIT Toronto, Canada, pp. 524–528. July 2008
19. Ozel, O., Ulukus, S.: Rate-equivocation region of cyclic shift symmetric wiretap channels. In: Proceedings of the 49th Annual Allerton Conf. Allerton House, Monticello, IL, USA, pp. 1120–1127 (2011)
20. Andersson, M., Rathi, V., Thobaben, R., Kliewer, J., Skoglund, M.: Nested polar codes for wiretap and relay channels. IEEE Commun. Lett. **14**(8), 752–754 (2010)
21. Hayashi, M., Matsumoto, R.: Universally attainable error and information exponents, and equivocation rate for the broadcast channels with confidential messages. In: Proceedings of the 49th Annual Allerton Conf. Allerton House, Monticello, IL, USA, pp. 439–444 (2011)
22. Choo, L.-C., Ling, C., Wong, K.-K.: Achievable rates for lattice coded gaussian wiretap channels. In: Proceedings of the IEEE International Conference on Communications Workshops (ICC), pp. 1–5. June 2011

23. Rathi, V., Urbanke, R., Andersson, M., Skoglund, M.: Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel. In: Proceedings of the 2011 IEEE ISIT Saint-Petersburg, Russia, pp. 2393–2397, Aug 2011)
24. Fujii, J.I., Kamei, E.: Relative operator entropy in noncommutative information theory. Math. Japon. **34**, 341–348 (1989)
25. Belavkin, V.P., Staszewski, P.: C^*-algebraic generalization of relative entropy and entropy. Ann. Inst. Henri Poincaré, Sec. A **37**, 51–58 (1982)
26. Hiai, F., Petz, D.: The proper formula for relative entropy and its asymptotics in quantum probability. Commun. Math. Phys. **143**, 99–114 (1991)
27. Hayashi, M.: Quantum Information: An Introduction. Springer, Berlin (2006)
28. Hayashi, M.: Optimal sequence of POVMs in the sense of Stein's lemma in quantum hypothesis. J. Phys. A: Math. Gen. **35**, 10759–10773 (2002)
29. Carter, L., Wegman, M.: Universal classes of hash functions. J. Comput. Syst. Sci. **18**(2), 143–154 (1979)
30. Krawczyk, H.: LFSR-based hashing and authentication. Advances in Cryptology—CRYPTO '94 Lecture Notes in Computer Science, vol. 839, pp. 129–139. Springer, Berlin (1994)
31. Devetak, I., Winter, A.: Distillation of secret key and entanglement from quantum states. Proc. R. Soc. Lond. A **461**, 207–235 (2005)
32. Hayashi, M.: Tight exponential analysis of universally composable privacy amplification and its applications. IEEE Trans. Inf. Theory **59**(11), 7728–7746 (2013)
33. Frank, R.L., Lieb, E.H.: Monotonicity of a relative Renyi entropy. J. Math. Phys. **54**(12), 122201 (2013)
34. Muller-Lennert, M., Dupuis, F., Szehr, O., Fehr, S., Tomamichel, M.: On quantum Renyi entropies: a new generalization and some properties. J. Math. Phys. **54**, 122203 (2013)
35. Wilde, M.M., Winter, A., Yang, D.: Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Renyi relative entropy. Commun. Math. Phys. **331**(2), 593–622 (2014)
36. Mosonyi, M., Ogawa, T.: Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies. arXiv:1309.3228

Communicated by A. Winter