Non-Asymptotic Analysis of Privacy Amplification via Rényi Entropy and Inf-Spectral Entropy

Shun Watanabe* and Masahito Hayashi†
*Department of Information Science and Intelligent Systems, University of Tokushima, Japan,
and Institute for System Research, University of Maryland, College Park.
Email: shun-wata@is.tokushima-u.ac.jp
†Graduate School of Mathematics, Nagoya University, Japan,
and Centre for Quantum Technologies, National University of Singapore, Singapore.
E-mail: masahito@math.nagoya-u.ac.jp

Abstract—**This paper investigates the privacy amplification problem, and compares the existing two bounds: the exponential bound derived by one of the authors and the min-entropy bound derived by Renner. It turns out that the exponential bound is better than the min-entropy bound when a security parameter is rather small for a block length, and that the min-entropy bound is better than the exponential bound when a security parameter is rather large for a block length. Furthermore, we present another bound that interpolates the exponential bound and the min-entropy bound by a hybrid use of the Rényi entropy and the inf-spectral entropy.**

I. Introduction

The privacy amplification [1] is a technique to distill a secret key from a source that is partially known to an eavesdropper, usually referred to as Eve. The privacy amplification is regarded as an indispensable tool in the information theoretic security, and it has been studied in many literatures (eg. [2], [3], [4], [5], [6], [7], [8]).

Recently, the non-asymptotic analysis of coding problems has attracted considerable attention [9], [10]. Especially for the channel coding problem, the relation between various types of non-asymptotic bounds are extensively compared in [10].

The performance of the privacy amplification is typically characterized by the smooth minimum entropy or the inf-spectral entropy [2], [11], [8]. There is also another approach, the exponential bound, which has been investigated by one of the authors [7]. So far, the relation between non-asymptotic bounds derived by these two approaches has not been clarified. The first purpose of this paper is to compare the min-entropy bound, which is derived by the smooth minimum entropy framework, and the exponential bound. Actually, it turns out that the exponential bound is better than the min-entropy bound when a security parameter is rather small for a block length. In the following, we explain a reason for this result.

In the achievability part of the smooth entropy framework [2] or the information spectrum approach [12], a performance criterion of a problem, such as an error probability or a security parameter, is usually upper bounded by a formula consisting of two terms. One of the terms is caused by the smoothing error, which corresponds to a tail probability of atypical outcomes. The other is caused by typical outcomes. In the following, let us call the former one the type 1 error term and the latter one the type 2 error term respectively.

To derive a tight bound in total, we need to tightly bound both the type 1 and type 2 error terms. This fact has been recognized in literatures. Indeed, one of the authors derived the state-of-the-art error exponent for the classical-quantum channel coding by tightly bounding both types of error terms [13]. In [10], Polyanskiy *et. al.* derived a non-asymptotic bound of the channel coding, which is called the DT bound, by tightly bounding both types of error terms. The DT bound remarkably improves on the so-called Feinstein bound because the type 2 error term is loosely bounded in the Feinstein bound. The improvement is especially remarkable when a required error probability is rather small for a block length.

For the privacy amplification problem, one of the authors derived the state-of-the-art exponent of the variational distance by tightly bounding both types of error terms [7]. On the other hand, the type 2 error term is loosely bounded in the bound derived via the smooth minimum entropy [2].

As is expected from the above argument, the exponential bound turns out to be better than the min-entropy bound when a security parameter is rather small for a block length. For rather large security parameters, the min-entropy bound is better than the exponential bound. This is because we derive the exponential bound by using the large deviation technique [14]. The large deviation technique is only tight when a threshold of a tail probability is away from the average, and this is not the case when a security parameter is rather large for a block length. As the second purpose of this paper, we derive a bound that interpolates the exponential bound and the min-entropy bound. This is done by a hybrid use of the Rényi entropy and the inf-spectral entropy. It turns out that the hybrid bound is better than both the exponential bound and the min-entropy bound for whole ranges of security parameters.

The rest of the paper is organized as follows. In Section II, we summarize known bounds on the privacy amplification. In Section III, we propose a novel bound by using the Rényi entropy and the inf-spectral entropy. In Section IV, we compare the bounds numerically. Proofs of some technical lemmas can be found in [15].

II. Preliminaries

In this section, we review the problem setting and known results on the privacy amplification. Although most of results in this section were stated explicitly or implicitly in literatures, we restate them for reader's convenience. Especially, Theorem 1, Theorem 2, and Theorem 3 are classical analogue of those obtained in [8] for the quantum setting, where the distance to evaluate the smoothing is different.

A. Problem Formulation

For a set $\mathcal{A}$, let $\mathcal{P}(\mathcal{A})$ be the set of all probability distribution on $\mathcal{A}$. It is also convenient to introduce the set $\bar{\mathcal{P}}(\mathcal{A})$ of all sub-normalized non-negative functions.

Let $P_{XZ} \in \bar{\mathcal{P}}(\mathcal{X} \times \mathcal{Z})$ be a sub-normalized non-negative function. For a function $f : \mathcal{X} \to \mathcal{S}$ and the key $S = f(X)$, let

$$P_{SZ}(s,z) = \sum_{x \in f^{-1}(s)} P_{XZ}(x,z).$$

We define the security by

$$d(f|P_{XZ}) = d(P_{SZ}, P_{\bar{S}} \times P_Z),$$

where $P_{\bar{S}}$ is the uniform distribution on $\mathcal{S}$ and

$$d(P,Q) := \frac{1}{2} \sum_a |P(a) - Q(a)| \tag{1}$$

for $P, Q \in \bar{\mathcal{P}}(\mathcal{A})$.

Although the quantity $d(f|P_{XZ})$ has no operational meaning for unnormalized P_{XZ}, it will be used to derive bounds on $d(f|P_{XZ})$ for normalized P_{XZ}. For distribution $P_{XZ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$ and security parameter $\varepsilon \geq 0$, we are interested in characterizing

$$\ell(P_{XZ}, \varepsilon) = \sup\{\log |\mathcal{S}| : \exists f : \mathcal{X} \to \mathcal{S} \text{ s.t. } d(f|P_{XZ}) \leq \varepsilon\}.$$

B. Min Entropy Framework

In this section, we review the smooth minimum entropy framework that was mainly introduced and developed by Renner and his collaborators [2], [3], [16], [17], [4]. Throughout the paper, we assume that the base of the logarithm is 2.

Definition 1: For $P_{XZ} \in \bar{\mathcal{P}}(\mathcal{X} \times \mathcal{Z})$ and a normalized $R_Z \in \mathcal{P}(\mathcal{Z})$, we define

$$H_{\min}(P_{XZ}|R_Z) = -\log \max_{\substack{x \in \mathcal{X} \\ z \in \mathrm{supp}(R_Z)}} \frac{P_{XZ}(x,z)}{R_Z(z)}.$$

Then, we define

$$\bar{H}^{\varepsilon}_{\min}(P_{XZ}|R_Z) = \max_{Q_{XZ} \in \bar{\mathcal{B}}^{\varepsilon}(P_{XZ})} H_{\min}(Q_{XZ}|R_Z),$$

where

$$\bar{\mathcal{B}}^{\varepsilon}(P_{XZ}) = \left\{ Q_{XZ} \in \bar{\mathcal{P}}(\mathcal{X} \times \mathcal{Z}) : d(P_{XZ}, Q_{XZ}) \leq \varepsilon \right\}.$$

We also define

$$H^{\varepsilon}_{\min}(P_{XZ}|R_Z) = \max_{Q_{XZ} \in \mathcal{B}^{\varepsilon}(P_{XZ})} H_{\min}(Q_{XZ}|R_Z),$$

where

$$\mathcal{B}^{\varepsilon}(P_{XZ}) = \{ Q_{XZ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Z}) : d(P_{XZ}, Q_{XZ}) \leq \varepsilon \}.$$

The following is a key lemma to derive every lower bound on $\ell(P_{XZ}, \varepsilon)$.

Lemma 1 (Leftover Hash:[2]): Let F be the uniform random variable on a set of universal 2 hash family $\mathcal{F}$. Then, for $P_{XZ} \in \bar{\mathcal{P}}(\mathcal{X} \times \mathcal{Z})$ and $R_Z \in \mathcal{P}(\mathcal{Z})$, we have[1]

$$\mathbb{E}_F[d(F|P_{XZ})] \leq \frac{1}{2} \sqrt{|\mathcal{S}| 2^{-H_2(P_{XZ}|R_Z)}},$$

where

$$H_2(P_{XZ}|R_Z) = -\log \sum_{\substack{x \in \mathcal{X} \\ z \in \mathrm{supp}(R_Z)}} \frac{P_{XZ}(x,z)^2}{R_Z(z)}$$

is the conditional Rényi entropy of order 2 relative to R_Z.

Since $H_2(P_{XZ}|R_Z) \geq H_{\min}(P_{XZ}|R_Z)$, we have the following.

Corollary 1: For $P_{XZ} \in \bar{\mathcal{P}}(\mathcal{X} \times \mathcal{Z})$ and $R_Z \in \mathcal{P}(\mathcal{Z})$, we have

$$\mathbb{E}_F[d(F|P_{XZ})] \leq \frac{1}{2} \sqrt{|\mathcal{S}| 2^{-H_{\min}(P_{XZ}|R_Z)}}.$$

Furthermore, since

$$d(P_{XZ}|f) \leq 2\varepsilon + d(\bar{P}_{XZ}|f)$$

holds for $\bar{P}_{XZ} \in \bar{\mathcal{B}}^{\varepsilon}(P_{XZ})$ by the triangular inequality, we have the following.

Corollary 2: For $P_{XZ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$ and $R_Z \in \mathcal{P}(\mathcal{Z})$, we have

$$\mathbb{E}_F[d(F|P_{XZ})] \leq 2\varepsilon + \frac{1}{2} \sqrt{|\mathcal{S}| 2^{-\bar{H}^{\varepsilon}_{\min}(P_{XZ}|R_Z)}}.$$

The following is a key lemma to derive a upper bound on $\ell(P_{XZ}, \varepsilon)$.

Lemma 2 (Monotonicity): For any function $f : \mathcal{X} \to \mathcal{S}$, $P_{XZ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$, and $R_Z \in \mathcal{P}(\mathcal{Z})$, we have

$$H^{\varepsilon}_{\min}(P_{SZ}|R_Z) \leq H^{\varepsilon}_{\min}(P_{XZ}|R_Z).$$

Remark 1: When Eve's side-information is the quantum density operator instead of the random variable, the monotonicity of the smooth minimum entropy was proved in [8, Proposition 3], where the smoothing is evaluated by the so-called purified distance instead of the trace distance. For the quantum setting and the trace distance, it is not clear whether the monotonicity holds or not because we cannot apply Uhlmann's theorem to the trace distance directly.

From Corollary 2 and Lemma 2, we get the following lower and upper bounds on $\ell(P_{XZ}, \varepsilon)$.

Theorem 1: For any $0 < \eta \leq \varepsilon$, we have

$$\begin{aligned} &\max_{R_Z \in \mathcal{P}(\mathcal{Z})} \bar{H}^{(\varepsilon-\eta)/2}_{\min}(P_{XZ}|R_Z) + \log 4\eta^2 - 1 \\ &\quad \leq \ \ell(P_{XZ}, \varepsilon) \\ &\quad \leq \ H^{\varepsilon}_{\min}(P_{XZ}|P_Z). \end{aligned}$$

C. Information Spectrum Approach

In this section, we introduce the inf-spectral entropy. The quantity is used to calculate the lower and upper bounds in Theorem 1.

Definition 2: For $P_{XZ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$ and $0 \leq \varepsilon \leq 1$, let

$$\begin{aligned} &H^{\varepsilon}_{\mathrm{s}}(P_{XZ}|R_Z) \\ &\quad := \ \sup\left\{ r : P_{XZ}\left\{ -\log \frac{P_{XZ}(x,z)}{R_Z(z)} \leq r \right\} \leq \varepsilon \right\} \end{aligned}$$

be the conditional inf-spectral entropy relative to $R_Z \in \mathcal{P}(\mathcal{Z})$.

The following two lemmas relate the quantities $H^{\varepsilon}_{\min}(P_{XZ}|R_Z)$ and $H^{\varepsilon}_{\mathrm{s}}(P_{XZ}|R_Z)$.

[1] Technically, R_Z must be such that $\mathrm{supp}(P_Z) \subset \mathrm{supp}(R_Z)$.

Lemma 3: For $P_{XZ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$ and $R_Z \in \mathcal{P}(\mathcal{Z})$, we have

$$\bar{H}_{\min}^{\varepsilon/2}(P_{XZ}|R_Z) \ge H_{\mathrm{s}}^{\varepsilon}(P_{XZ}|R_Z).$$

Lemma 4: For $P_{XZ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$, we have

$$H_{\min}^{\varepsilon}(P_{XZ}|P_Z) \le H_{\mathrm{s}}^{\varepsilon+\zeta}(P_{XZ}|P_Z) - \log \zeta$$

for any $0 < \zeta \le 1 - \varepsilon$.

From Theorem 1, Lemma 3 and Lemma 4, we have the following.

Theorem 2: For any $0 < \eta \le \varepsilon$ and $0 < \zeta \le 1 - \varepsilon$, we have

$$\begin{aligned} &\max_{R_Z \in \mathcal{P}(\mathcal{Z})} H_{\mathrm{s}}^{\varepsilon-\eta}(P_{XZ}|R_Z) + \log 4\eta^2 - 1 \\ &\le \ \ell(P_{XZ}, \varepsilon) \\ &\le \ H_{\mathrm{s}}^{\varepsilon+\zeta}(P_{XZ}|P_Z) - \log \zeta. \end{aligned}$$

D. Gaussian Approximation

In this section, we consider the asymptotic setting. By applying the Berry-Esséen theorem to Theorem 2, we have the following Gaussian approximation of $\ell(P_{XZ}^n, \varepsilon)$.

Theorem 3: Let

$$V(X|Z) := \sum_{x,z} P_{XZ}(x,z) \left(\log \frac{1}{P_{X|Z}(x|z)} - H(X|Z) \right)^2$$

be the dispersion of the conditional log likelihood. Then, we have

$$\ell(P_{XZ}^n, \varepsilon) = nH(X|Z) + \sqrt{nV(X|Z)}\Phi^{-1}(\varepsilon) + O(\log n),$$

where $\Phi(\cdot)$ is the cumulative distribution function of the standard Gaussian random variable.

E. Exponential Bound

In this section, we review the exponential bounds.

Definition 3: For $P_{XZ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$, let

$$\phi(\rho|P_{XZ}) = \log \sum_z P_Z(z) \left(\sum_x P_{X|Z}(x|z)^{\frac{1}{1-\rho}} \right)^{1-\rho}.$$

We have the following.

Theorem 4 ([7]): For any $0 < \rho \le \frac{1}{2}$, we have

$$\mathbb{E}_F[d(F|P_{XZ})] \le \frac{3}{2}|\mathcal{S}|^{\rho} 2^{\phi(\rho|P_{XZ})}.$$

Definition 4: For $\theta > 0$, $P_{XZ} \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$, and $R_Z \in \mathcal{P}(\mathcal{Z})$, let

$$H_{1+\theta}(P_{XZ}|R_Z) := -\frac{1}{\theta} \log \sum_{x,z} R_Z(z) \left(\frac{P_{XZ}(x,z)}{R_Z(z)} \right)^{1+\theta}$$

be the conditional Rényi entropy of order $1+\theta$ relative to R_Z. For $\theta = 0$, we define

$$\begin{aligned} H_1(P_{XZ}|R_Z) \ &:= \ \lim_{\theta \to 0} H_{1+\theta}(P_{XZ}|R_Z) \\ &= \ H(X|Z) - D(P_Z \| R_Z). \end{aligned}$$

By using Jensen's inequality and by setting $\rho = \frac{\theta}{1+\theta}$, we have

$$\phi(\rho|P_{XZ}) \le -\frac{\theta}{1+\theta} H_{1+\theta}(P_{XZ}|P_Z).$$

Thus, we have the following slightly looser bound.

Corollary 3: For $0 < \theta \le 1$, we have

$$\mathbb{E}_F[d(F|P_{XZ})] \le \frac{3}{2}|\mathcal{S}|^{\frac{\theta}{1+\theta}} 2^{-\frac{\theta}{1+\theta} H_{1+\theta}(P_{XZ}|P_Z)}.$$

From Theorem 4 and Corollary 3, we have the following.

Theorem 5: We have

$$\begin{aligned} &\ell(P_{XZ}, \varepsilon) \\ &\ge \sup_{0 < \rho \le \frac{1}{2}} \frac{-\phi(\rho|P_{XZ}) + \log(2\varepsilon/3)}{\rho} - 1 \qquad (2) \\ &\ge \sup_{0 < \theta \le 1} \frac{\theta H_{1+\theta}(P_{XZ}|P_Z) + (1+\theta)\log(2\varepsilon/3)}{\theta} - 1. \qquad (3) \end{aligned}$$

III. Hybrid Bound

In this section, we derive another bound from the leftover hash lemma (Lemma 1). A basic idea is to use the smoothing in a similar manner as in the derivation of Theorem 4. However, we do not use the large deviation bound.

Theorem 6: For any $0 < \eta \le \varepsilon$, we have

$$\begin{aligned} &\ell(P_{XZ}, \varepsilon) \\ &\ge \max_{0 \le \theta \le 1} \max_{R_Z} [\theta H_{1+\theta}(P_{XZ}|R_Z) \\ &\qquad + (1-\theta) H_{\mathrm{s}}^{\varepsilon-\eta}(P_{XZ}|R_Z)] + \log 4\eta^2 - 1. \qquad (4) \end{aligned}$$

Proof: We define the smoothed probability

$$\bar{P}_{XZ}(x,z) = P_{XZ}(x,z) \mathbf{1}\left[-\log \frac{P_{XZ}(x,z)}{R_Z(z)} > r \right]. \qquad (5)$$

From Lemma 1, we have

$$\begin{aligned} &\mathbb{E}_F\left[d(F|\bar{P}_{XZ}) \right] \\ &\le \sqrt{|\mathcal{S}| 2^{-H_2(\bar{P}_{XZ}|R_z)}} \\ &= \sqrt{|\mathcal{S}| \sum_{x,z} \frac{\bar{P}_{XZ}(x,z)^2}{R_Z(z)}} \\ &\le \sqrt{|\mathcal{S}| \sum_{x,z} \frac{P_{XZ}(x,z)^{1+\theta}}{R_Z(z)^{\theta}} 2^{-(1-\theta)r}} \\ &= \sqrt{|\mathcal{S}| \sum_{x,z} 2^{-\theta H_{1+\theta}(P_{XZ}|R_Z) - (1-\theta)r}}. \end{aligned}$$

By the triangular inequality, we have

$$\begin{aligned} &\mathbb{E}_F\left[d(F|\bar{P}_{XZ}) \right] \\ &\le 2d(P_{XZ}, \bar{P}_{XZ}) + \frac{1}{2}\sqrt{|\mathcal{S}| 2^{-\theta H_{1+\theta}(P_{XZ}|R_Z) - (1-\theta)r}} \\ &= P_{XZ}\left\{ -\log \frac{P_{XZ}(x,z)}{R_Z(z)} \le r \right\} \\ &\qquad + \frac{1}{2}\sqrt{|\mathcal{S}| 2^{-\theta H_{1+\theta}(P_{XZ}|R_Z) - (1-\theta)r}}. \end{aligned}$$

Thus, by setting $r = H_{\mathrm{s}}^{\varepsilon-\eta}(P_{XZ}|R_Z)$ and by taking $|\mathcal{S}|$ so that

$$\frac{1}{2}\sqrt{|\mathcal{S}| 2^{-\theta H_{1+\theta}(P_{XZ}|R_Z) - (1-\theta)r}} \le \eta,$$

we have the statement of the theorem. ■

Note that the bound in Theorem 6 interpolates the lower bound in Theorem 2 and the bound in (2) and (3) of Theorem 5. More specifically, when the supremum in (4) is achieved by $\theta = 0$, then the bound in (4) reduces to the bound in Theorem 2. To derive the bounds in (2) and (3), we need some large deviation calculation. By using Markov's inequality, we have

$$\begin{aligned} & P_{XZ}\left\{ -\log \frac{P_{XZ}(x,z)}{R_Z(z)} \le r \right\} \\ &= P_{XZ}\left\{ \theta \log \frac{P_{XZ}(x,z)}{R_Z(z)} \ge -\theta r \right\} \\ &\le \exp\left\{ \theta r - \theta H_{1+\theta}(P_{XZ}|R_Z) \right\}. \end{aligned}$$

Thus, we have

$$H_{\mathrm{s}}^{\varepsilon-\eta}(P_{XZ}|R_Z) \ge H_{1+\theta}(P_{XZ}|R_Z) + \frac{1}{\theta}\log(\varepsilon - \eta). \tag{6}$$

In [18], it was shown that

$$\max_{R_Z \in \mathcal{P}(\mathcal{Z})} H_{1+\theta}(P_{XZ}|R_Z) = -\frac{1+\theta}{\theta}\phi\left(\frac{\theta}{1+\theta}|P_{XZ}\right)$$

and the optimal choice of R_Z was shown to be

$$R_Z^*(z) = \frac{\left(\sum_x P_{XZ}(x,z)^{1+\theta}\right)^{\frac{1}{1+\theta}}}{\sum_z \left(\sum_x P_{XZ}(x,z)^{1+\theta}\right)^{\frac{1}{1+\theta}}}. \tag{7}$$

By setting $\eta = \frac{\varepsilon}{3}$ and $R_Z = R_Z^*$, by substituting (6) into (4), and by changing the variables $\rho = \frac{\theta}{1+\theta}$, we have the bound in (2). Similarly, by setting $\eta = \frac{\varepsilon}{3}$ and $R_Z = P_Z$, and by substituting (6) into (4), we have the bound in (3).

IV. Numerical Calculation

In this section, we consider the i.i.d. setting. We consider the case such that Z is obtained from X throughout BSC, i.e.,

$$P_{XZ}(x,x) = \frac{1-q}{2}, \quad P_{XZ}(x,x+1) = \frac{q}{2}. \tag{8}$$

In this case, since P_Z is the uniform distribution on $\{0,1\}$, from (7), the optimal choice of R_Z is $R_Z = P_Z$. We have

$$P_{XZ}^n\left\{ \log \frac{1}{P_{X|Z}^n(x^n|z^n)} \le r \right\} = B\left(n, q, \frac{r + n\log(1-q)}{\log\frac{1-q}{q}}\right),$$

where $B(n,q,k)$ is the cumulative density function of the binomial trial. Thus, the lower and upper bounds in Theorem 2 can be described as $\ell_{\mathrm{s,low}}(\varepsilon) \le \ell(P_{XZ}^n, \varepsilon) \le \ell_{\mathrm{s,up}}(\varepsilon)$, where

$$\begin{aligned} \ell_{\mathrm{s,low}}(\varepsilon) &= B^{-1}(n,q,\varepsilon-\eta) \times \log\frac{1-q}{q} \\ &\qquad - n\log(1-q) + \log 4\eta^2 - 1 \quad (9) \\ \ell_{\mathrm{s,up}}(\varepsilon) &= B^{-1}(n,q,\varepsilon+\zeta) \times \log\frac{1-q}{q} \\ &\qquad - n\log(1-q) - \log\zeta \quad (10) \end{aligned}$$

For the distribution of the form in (8), the bound in (2) and (3) coincide. We have

$$H_{1+\theta}(P_{XZ}|P_Z) = -\frac{1}{\theta}\log\left(q^{1+\theta} + (1-q)^{1+\theta}\right).$$

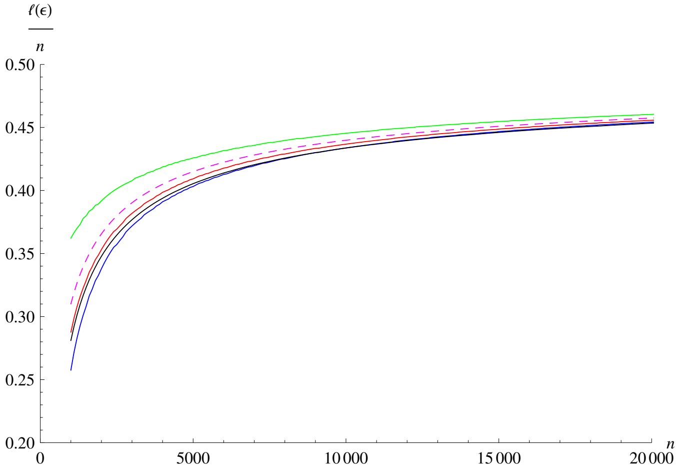

Fig. 1. A comparison among the bounds for $\varepsilon = 10^{-10}$ and $q = 0.11$. The blue curve is the min-entropy bound $\ell_{\mathrm{s,low}}(\varepsilon)$. The black curve is the exponential bound $\ell_{\mathrm{e,low}}(\varepsilon)$. The red curve is the hybrid bound $\ell_{\mathrm{h,low}}(\varepsilon)$. The dashed pink curve is the Gaussian approximation. The green curve is the upper bound $\ell_{\mathrm{s,up}}(\varepsilon)$.

Thus, the bounds in Theorem 5 can be described as $\ell(P_{XZ}^n, \varepsilon) \ge \ell_{\mathrm{e,low}}(\varepsilon)$, where

$$\begin{aligned} \ell_{\mathrm{e,low}}(\varepsilon) &= \sup_{0<\theta\le 1} \frac{-n\log\left(q^{1+\theta} + (1-q)^{1+\theta}\right)}{\theta} \\ &\qquad + \frac{(1-\theta)}{\theta}\log(2\varepsilon/3) - 1 \quad (11) \end{aligned}$$

Similarly, the bound in Theorem 6 can be described as $\ell(P_{XZ}^n, \varepsilon) \ge \ell_{\mathrm{h,low}}(\varepsilon)$, where

$$\begin{aligned} &\ell_{\mathrm{h,low}}(\varepsilon) \\ &= \max_{0\le\theta\le 1}\left[-n\log\left(q^{1+\theta} + (1-q)^{1+\theta}\right) + (1-\theta) \right. \\ &\quad \left. \times \left\{ B^{-1}(n,q,\varepsilon-\eta) \times \log\frac{1-q}{q} - n\log(1-q) \right\} \right] \\ &\quad + \log 4\eta^2 - 1. \qquad (12) \end{aligned}$$

For $\varepsilon = 10^{-10}$ and $q = 0.11$, we plot $\ell_{\mathrm{s,low}}(\varepsilon)$, $\ell_{\mathrm{s,up}}(\varepsilon)$, $\ell_{\mathrm{e,low}}(\varepsilon)$, $\ell_{\mathrm{h,low}}(\varepsilon)$, and Gaussian approximation derived by Theorem 3 in Fig. 1, where we set $\eta = \zeta = \frac{\varepsilon}{2}$. From the figure, we can find that the exponential bound is better than the min-entropy bound up to about $n = 10000$. The hybrid bound is better than both the exponential bound and the min-entropy bound. The Gaussian approximation overestimate the lower bounds, but it is sandwiched by the lower bounds and the upper bound.

In Figs. 2, 3 and 4, the bounds are compared from a different perspective, i.e., for fixed n and varying ε. From the figures, we can find that the exponential bound and the hybrid bound become much better than the min-entropy bound as ε becomes small. When ε is rather large for n, the min-entropy bound is better than the exponential bound. The hybrid bound is better than both the exponential bound and the min-entropy bound for whole ranges of ε.

V. Conclusions

In this paper, we have compared the exponential bound and the min-entropy bound. It turned out that the exponential

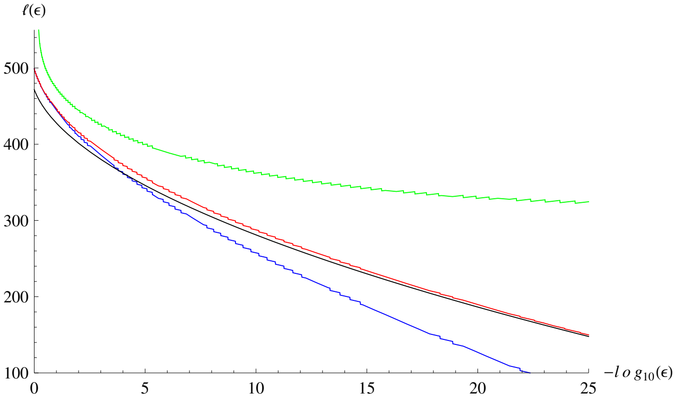

Fig. 2. A comparison among the bounds for $n = 1000$ and $q = 0.11$. The blue curve is the min-entropy bound $\ell_{\mathrm{s,low}}(\varepsilon)$. The black curve is the exponential bound $\ell_{\mathrm{e,low}}(\varepsilon)$. The red curve is the hybrid bound $\ell_{\mathrm{h,low}}(\varepsilon)$. The green curve is the upper bound $\ell_{\mathrm{s,up}}(\varepsilon)$.

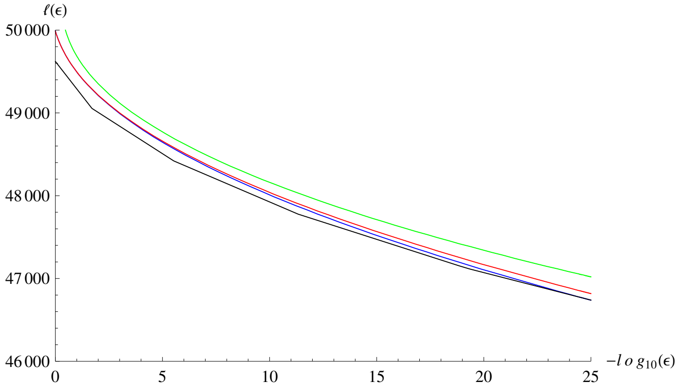

Fig. 4. A comparison among the bounds for $n = 100000$ and $q = 0.11$. The blue curve is the min-entropy bound $\ell_{\mathrm{s,low}}(\varepsilon)$. The black curve is the exponential bound $\ell_{\mathrm{e,low}}(\varepsilon)$. The red curve is the hybrid bound $\ell_{\mathrm{h,low}}(\varepsilon)$. The green curve is the upper bound $\ell_{\mathrm{s,up}}(\varepsilon)$.

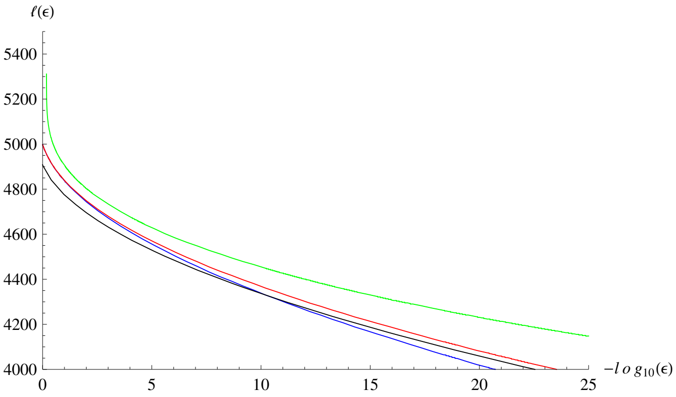

Fig. 3. A comparison among the bounds for $n = 10000$ and $q = 0.11$. The blue curve is the min-entropy bound $\ell_{\mathrm{s,low}}(\varepsilon)$. The black curve is the exponential bound $\ell_{\mathrm{e,low}}(\varepsilon)$. The red curve is the hybrid bound $\ell_{\mathrm{h,low}}(\varepsilon)$. The green curve is the upper bound $\ell_{\mathrm{s,up}}(\varepsilon)$.

bound is better than the min-entropy bound when ε is rather small for n. When ε is rather large for n, the min-entropy bound is better than the exponential bound. We also presented the hybrid bound that interpolates the exponential bound and the min-entropy bound.

Although we only treated the privacy amplification in this paper, we believe that the observation that the dominance relationships of non-asymptotic bounds may depend on ε is also important for other problems in the information theory. For the channel coding problem as an example, from the numerical comparisons in [10], we can find that the dominance relationship between the DT bound and the Gallager bound depends on ε for fixed n. Thus, the Gallager bound should be more appreciated in the context of the non-asymptotic analysis. Further investigation in this direction will be treated in our forthcoming paper.

For a future research agenda, it is also important to extend the results in this paper to the quantum setting or other information theoretic security tasks such as the wire-tap channel.

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized Privacy Amplification," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[2] R. Renner, "Security of Quantum Key Distribution," Ph.D. dissertation, Dipl. Phys. ETH, Switzerland, February 2005, arXiv:quant-ph/0512258, also available from International Journal of Quantum Information, vol. 6, no. 1, pp. 1–127, February 2008.

[3] R. Renner and S. Wolf, "Simple and Tight Bound for Information Reconciliation and Privacy Amplification," in *Advances in Cryptology – ASIACRYPT 2005*, ser. Lecture Notes in Computer Science, vol. 3788. Springer-Verlag, 2005, pp. 199–216.

[4] M. Tomamichel, "A Framework for Non-Asymptotic Quantum Information Theory," Ph.D. dissertation, Dipl. Phys. ETH, Switzerland, 2012, arXiv:1203.2142.

[5] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover Hashing Against Quantum Side-Information," *IEEE Trans. Inform. Theory*, vol. 57, no. 8, pp. 5524–5535, August 2011, arXiv:1002.2436.

[6] M. Hayashi, "Exponential Decreasing Rate of Leaked Information in Universal Random Privacy Amplification," *IEEE Trans. Inform. Theory*, vol. 57, no. 6, pp. 3989–4001, June 2011, arXiv:0904.0308.

[7] ——, "Tight Exponential Evaluation for Information Theoretical Secrecy Based on L_1 Distance," arXiv:1010.1358.

[8] M. Tomamichel and M. Hayashi, "A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks," 2012, arXiv:1208.1478.

[9] M. Hayashi, "Information Spectrum Approach to Second-Order Coding Rate in Channel Coding," *IEEE Trans. Inform. Theory*, vol. 55, no. 11, pp. 4947–4966, November 2009.

[10] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel Coding Rate in The Finite Blocklength Regime," *IEEE Trans. Inform. Theory*, vol. 57, no. 5, pp. 2307–2359, May 2010.

[11] N. Datta and R. Renner, "Smooth Entropies and The Quantum Information Spectrum," *IEEE Trans. Inform. Theory*, vol. 55, no. 6, pp. 2807–2815, June 2009.

[12] T. S. Han, *Information-Spectrum Methods in Information Theory*. Springer, 2003.

[13] M. Hayashi, "Error Exponent in Asymmetric Quantum Hypothesis Testing and Its Application to Classical-Quantum Channel Coding," *Phys. Rev. A*, vol. 76, no. 6, p. 062301, December 2007, arXiv:quant-ph/0611013.

[14] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications*, 2nd ed. Springer, 1998.

[15] S. Watanabe and M. Hayashi, "Non-Asymptotic Analysis of Privacy Amplification via Rényi Entropy and Inf-Spectral Entropy," 2012, arXiv:1211.5252.

[16] M. Tomamichel, R. Colbeck, and R. Renner, "A Fully Quantum Asymptotic Equipartition Property," *IEEE Trans. Inform. Theory*, vol. 55, no. 12, pp. 5840–5847, December 2009, arXiv:0811.1221.

[17] ——, "Duality Between Smooth Min- and Max-Entropies," *IEEE Trans. Inform. Theory*, vol. 56, no. 9, pp. 4674–4681, September 2010, arXiv:0907.5238.

[18] M. Hayashi, "Large Deviation Analysis for Classical and Quantum Security via Approximate Smoothing," 2012, arXiv:1202.0322.