Bit Security Estimation Using Various Information-Theoretic Measures*

Dong-Hoon Lee (scott814@ccl.snu.ac.kr)[1], Young-Sik Kim[2], and Jong-Seon No[1]

[1] Seoul National University, Seoul, South Korea
[2] Chosun University, Gwangju, South Korea

Abstract. In this paper, various quantitative information-theoretic security reductions which correlate statistical difference between two probability distributions with security level's gap between two cryptographic schemes are proposed. Security is the most important prerequisite for cryptographic primitives. In general, there are two kinds of security; one is computational security, and the other is information-theoretic security. We focus on latter one in this paper, especially the view point of bit security which is a convenient notion to indicate the quantitative security level. We propose tighter and more generalized version of information-theoretic security reductions than those of the previous works [1,2]. More specifically, we obtain about 2.5-bit tighter security reduction than that in previous work [2], and we devise a further generalized version of security reduction in the previous work [1] by relaxing the constraint on the upper bound of the information-theoretic measure, that is, λ-efficient. Through this work, we propose the methodology to estimate the affects on security level when κ-bit secure original scheme is implemented on p-bit precision system. (Here, p can be set to any value as long as certain condition is satisfied.) In the previous work [1], p was fixed as $\frac{\kappa}{2}$, but our result is generalized to make it possible to security level κ and precision p variate independently. Moreover, we provide diverse types of security reduction formulas for the five kinds of information-theoretic measures. We are expecting that our results could provide an information-theoretic guideline for how much the two identical cryptographic schemes (i.e., the only difference is probability distribution) may show the difference in their security level when extracting their randomness from two different probability distributions. Especially, our results can be used to obtain the quantitative estimation of how much the statistical difference between the ideal distribution and the real distribution affects the security level.

Keywords: bit security · information-theoretic measures · security reduction · Rényi divergence · statistical distance · max-log distance · λ-efficient measure.

* This research was supported by Samsung Research Funding and Incubation Center for Future Technology of Samsung Electronics under Project SRFC-IT1801-08.

1 Introduction

Nowadays, almost every modern cryptographic primitive depends their security on some randomness value, which is extracted from a specific probability distribution (e.g., lattice-based cryptographic scheme which extracts its randomness from discrete Gaussian distribution). In other words, probability distribution of the cryptographic scheme has an important influence on its security. From this point of view, a lot of research has been conducted to analyze how security level changes when the probability distribution for the randomness of the cryptographic scheme is replaced by another probability distribution. Traditionally, 'probability preservation property (PPP)' [4,6] has been widely used to correlate difference between two statistical distributions with adversary's attack success probability. This kind of security reduction enables us to compare relative security level among cryptographic schemes. However only with PPP, we cannot have any detailed quantitative information for security level. With this motivation, several researchers have conducted studies to enable quantitative security analysis. Micciancio and Walter [1,2] deserve to be considered as leaders in this field. They suggested various quantitative security reductions by way of information-theoretic measures and they expressed the security reductions in terms of bit security. However, we could notice that their reduction results could be further improved and their results are informative only for limited cases.

In this paper, our contributions are as follows. First, we derive tighter security reduction bounds than those of Micciancio and Walter. Second, we propose a further generalized version of Micciancio and Walter's security reduction result by relaxing the constraint on the upper bound of the measure, that is, λ-efficient. Through this work, we manage to propose the methodology to estimate the affects on security level when κ-bit secure original scheme is implemented on p-bit precision system. (p can be set to any value as long as certain condition is satisfied.) Third, we provide various types of security reduction formulas for the five kinds of information-theoretic measures; statistical distance, Rényi divergence, Kullback-Leibler divergence, max-log distance, and relative error. These measures are often used in cryptography for security reduction analysis.

This paper is organized as follows. In Section II, we briefly introduce some essential concepts which are necessary to understand our results. Next, in Section III, we provide our three main results. Finally, in Section IV, we conclude the paper and present the future research directions.

2 Preliminaries

2.1 Information-Theoretic Measures

There are several widely known information-theoretic measures which are used to analyze security reduction as follows.

i) Statistical Distance (Δ_{SD})

For any two discrete probability distributions P and Q, the statistical distance between P and Q is defined as

$$\Delta_{SD}(P,Q) = \frac{1}{2} \sum_{x \in Supp(P) \cup Supp(Q)} |P(x) - Q(x)|,$$

where $Supp(\cdot)$ denotes the support set of probability distribution.

ii) Rényi Divergence (RD_α)

For any two discrete probability distributions P and Q such that $Supp(Q) \subseteq Supp(P)$, the Rényi divergence of order α between P and Q is defined as

a) $\alpha \in (1,\infty)$: $RD_\alpha(Q||P) = (\sum_{x \in Supp(Q)} \frac{Q(x)^\alpha}{P(x)^{\alpha-1}})^{\frac{1}{\alpha-1}}$

b) $\alpha = 1$: $RD_1(Q||P) = \exp(\sum_{x \in Supp(Q)} Q(x) \log \frac{Q(x)}{P(x)})$

c) $\alpha = \infty$: $RD_\infty(Q||P) = \max_{x \in Supp(Q)} \frac{Q(x)}{P(x)}$.

RD_α satisfies many attractive features such as probability preservation property, multiplicative property, data processing inequality, etc [4,5].

iii) Kullback-Leibler Divergence (Δ_{KL})

For any two discrete probability distributions P and Q such that $Supp(Q) \subseteq Supp(P)$, the Kullback-Leibler divergence between P and Q is defined as

$$\Delta_{KL}(Q||P) = \sum_{x \in Supp(Q)} Q(x) \log \frac{Q(x)}{P(x)}.$$

iv) Max-Log Distance (Δ_{ML})

For any two discrete probability distributions P and Q over the same support (i.e., $Supp(P) = Supp(Q)$), the max-log distance between P and Q is defined as

$$\Delta_{ML}(P,Q) = \max_{x \in Supp(Q)} |\ln P(x) - \ln Q(x)|.$$

Note that we should apply Δ_{ML} only in case when the support of two distributions are same.

v) Relative Error (δ_{RE})

For any two discrete probability distributions P and Q, the relative error between P and Q is defined as

$$\delta_{RE}(P,Q) = \max_{x \in Supp(P)} \frac{|P(x) - Q(X)|}{P(x)}.$$

2.2 Special Kinds of Measures

Micciancio and Walter defined two special kinds of measures in their paper [1]. Those are 'useful measure' and 'λ-efficient measure'. We will reuse their definitions.

i) Useful Measure

Any measure δ that satisfies the following three properties is called useful measure:

a) Probability preservation property: For any event E over the random variable X, we have $\Pr_{X \leftarrow P}[E] \geq \Pr_{X \leftarrow Q}[E] - \delta(P, Q)$, where $X \leftarrow P$ (respectively, $X \leftarrow Q$) denotes that X is sampled from probability distribution P (respectively, Q). This property makes it possible to bound the probability of an event occurring under distribution P in terms of the probability of the same event occurring under distribution Q and the measure value $\delta(P, Q)$. It is not hard to prove that this property is equivalent to the bound $\Delta_{SD}(P, Q) \leq \delta(P, Q)$. This fact implies that $\delta = \Delta_{SD}$ satisfies this property for sure.

b) Sub-additivity for joint distributions: Let $(X_i)_i$ and $(Y_i)_i$ be two lists of discrete random variables over the support $\prod_i S_i$ and let's define $X_{<i} = (X_1, ..., X_{i-1})$ (and similar for $Y_{<i}$). Then

$$\delta((X_i)_i, (Y_i)_i) \leq \sum_i \max_a \delta([X_i | X_{<i} = a], [Y_i | Y_{<i} = a]),$$

where the maximum value is taken over $a \in \prod_{j<i} S_j$.

c) Data processing inequality: $\delta(f(P), f(Q)) \leq \delta(P, Q)$ for any two probability distributions P, Q and function $f(\cdot)$, i.e., the measure δ does not increase under additional function application.

ii) λ-Efficient Measure

Consider a measure δ which satisfies the above two properties b) and c). We call it 'λ-efficient measure' if it satisfies the following property d) instead of property a):

d) Pythagorean probability preservation property (with parameter λ): For any joint distributions $(P_i)_i$ and $(Q_i)_i$ over support $\prod_i S_i$, if $\delta(P_i|a_i, Q_i|a_i) \leq \lambda$ is enjoyed for all i and $a_i \in \prod_{j<i} S_j$, then

$$\Delta_{SD}((P_i)_i, (Q_i)_i) \leq ||(\max_{a_i} \delta(P_i|a_i, Q_i|a_i))_i||_2.$$

2.3 New Notion of Bit Security

For long time, bit security has widely played a role to measure and estimate the quantitative security level of cryptographic primitives. The traditional definition of bit security is pretty simple. It is defined as $\min_A\{\log_2 \frac{T_A}{\epsilon_A}\}$, where for an

arbitrary adversary A, T_A and ϵ_A are adversary's resources and attack success probability, respectively. Micciancio and Walter designed a new concept of security game and they defined new notion of bit security in their work [2]. With their newly devised security game, they redefined the adversary's advantage. They provided adversary's advantage in terms of information-theoretic quantities. We will cite their definitions as follows.

Definition 1 [Definition 5, [2]] An n-bit security game is played by an adversary A who is interacting with a challenger C. At the beginning of the game, the challenger chooses a secret c, which is represented by the random variable $\mathcal{C} \in \{0,1\}^n$, from some distribution $D_{\mathcal{C}}$. At the end of the game, A outputs some value, which is represented by the random variable $\mathcal{A}$. The goal of the adversary is to output a value a such that $R(c,a)$, where R is some relation. A may output a special symbol $\perp$ such that $R(c,\perp)$ and $R^c(c,\perp)$ are both false.

Definition 2 [Definition 7, [2]] For any security game with corresponding random variable $\mathcal{C}$ and $\mathcal{A}(\mathcal{C})$, the adversary's advantage is $adv^A = \frac{I(\mathcal{C};\mathcal{Y})}{H(\mathcal{C})} = 1 - \frac{H(\mathcal{C}|\mathcal{Y})}{H(\mathcal{C})}$, where $I(\cdot;\cdot)$ is the mutual information between two random variables, $H(\cdot)$ is the Shannon entropy of a random variable, and $\mathcal{Y}(\mathcal{C},\mathcal{A})$ is the random variable with marginal distributions $\mathcal{Y}_{c,a} = \{y|\mathcal{C}=c, \mathcal{A}=a\}$ defined as follows:

a) $\mathcal{Y}_{c,\perp} = \perp$, for all c
b) $\mathcal{Y}_{c,a} = c$, for all $(c,a) \in R$
c) $\mathcal{Y}_{c,a} = \{c' \leftarrow D_{\mathcal{C}} | c' \neq c\}$, for all $(c,a) \in R^c$.

Definition 3 [Definition 10, [2]] For a search game, the advantage of the adversary A is $adv^A = \alpha^A \beta^A$ and for a decision game, it is $adv^A = \alpha^A (2\beta^A - 1)^2$, where $\alpha^A = \Pr[\mathcal{A} \neq \perp]$ is output probability, and $\beta^A = \Pr[R(\mathcal{C},\mathcal{A})|\mathcal{A} \neq \perp]$ is conditional success probability.

3 Main Results

Micciancio and Walter found out quantitative security reductions between two identical cryptographic schemes with all other conditions equal and differing only in the probability distributions for which the schemes extract the randomness [1,2]. Their works made it possible to guess how much security loss would occur when the defined probability distribution is replaced by another distribution. In other words, their works have provided information-theoretic guideline of security level (i.e., how statistical difference of two distribution affects on security level of cryptographic scheme). However, problems have been raised that their results may not be tight enough and their results are informative only in limited cases (i.e., their results give information only when the information-theoretic measure values between two distributions are upper bounded by specific fixed value, and the upper bound cannot be freely controllable). Due to these problems, it is necessary to bring out the tighter and the more generalized security

reduction. Our first work is tighter version of Lemma 3 in [1] that is proved by using similar approach to that of [1] as follows.

Theorem 1. Let S^P and S^Q be standard cryptographic schemes with black-box access to probability distribution ensembles P_θ and Q_θ, respectively. If S^P is κ-bit secure and $\delta(P_\theta, Q_\theta) \leq 2^{-\frac{\kappa}{2}}$ for some $2^{-\frac{\kappa}{2}}$-efficient measure δ, then S^Q is $(\kappa - \log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}) \approx (\kappa - 2.374)$-bit secure.

Proof. Suppose that $\frac{T_A}{\epsilon_A^Q} < 2^{\kappa - \log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}$ is satisfied when an adversary A satisfies $\frac{T_A}{\epsilon_A^P} \geq 2^\kappa$. Now, let's define some notations:

a) $G_{S,A}^P$ (respectively, $G_{S,A}^Q$): event that an adversary A succeeds in breaking the scheme S^P (respectively, S^Q) with the probability $\epsilon_A^P = \Pr(G_{S,A}^P)$ (respectively, $\epsilon_A^Q = \Pr(G_{S,A}^Q)$)
b) $[G_{S,A}^P]^n$ (respectively, $[G_{S,A}^Q]^n$): independent n copies of $G_{S,A}^P$ (respectively, $G_{S,A}^Q$)
c) $\epsilon_{A^n}^P$ (respectively, $\epsilon_{A^n}^Q$): probability that A wins the security game $[G_{S,A}^P]^n$ (respectively, $[G_{S,A}^Q]^n$) at least once
d) T_{A^n}: required resources that A wins the security game $[G_{S,A}^P]^n$ (respectively, $[G_{S,A}^Q]^n$) at least once
e) q: adversary A's number of queries

Applying probability preservation property and data processing inequality of Δ_{SD}, we have

$$\begin{aligned}\epsilon_{A^n}^P &\geq \epsilon_{A^n}^Q - \Delta_{SD}([G_{S,A}^P]^n, [G_{S,A}^Q]^n) \\ &\geq \epsilon_{A^n}^Q - \Delta_{SD}((\theta_i, P_{\theta_i})_i, (\theta_i', Q_{\theta_i'})_i).\end{aligned}$$

Here, $(\theta_i)_i$(respectively, $(\theta'_i)_i$) is the sequence of queries made during the game $[G_{S,A}^P]^n$(respectively, $[G_{S,A}^Q]^n$). Note that at any point during the game, conditioned on the event E_i that $(\theta_j, P_{\theta_j})_{j<i}$ and $(\theta_j', Q_{\theta_j'})_{j<i}$ take some specific and the same value, the adversary behaves identically in the two games up to the point that it makes the i-th query. Especially, the conditional distributions $(\theta_i|E_i)$ and $(\theta_i'|E_i)$ are the same and $\delta((\theta_i|E_i), (\theta_i'|E_i)) = 0$. This fact follows by sub-additivity for joint distributions that

$$\begin{aligned}\delta((\theta_i, P_{\theta_i}|E_i), (\theta_i', Q_{\theta_i'}|E_i)) &\leq \delta((\theta_i|E_i), (\theta_i'|E_i)) + \delta(P_\theta, Q_\theta) \\ &\leq 0 + 2^{-\frac{\kappa}{2}} = 2^{-\frac{\kappa}{2}}.\end{aligned}$$

This ensures that we can apply Pythagorean probability preservation property, and thus we can guarantee that the following inequalities are also true.

$$\begin{aligned}\epsilon^P_{A^n} &\geq \epsilon^Q_{A^n} - \Delta_{SD}((\theta_i, P_{\theta_i})_i, (\theta'_i, Q_{\theta'_i})_i) \\ &\geq \epsilon^Q_{A^n} - \sqrt{q \times \delta(P_\theta, Q_\theta)^2} \\ &\geq \epsilon^Q_{A^n} - \sqrt{T_{A^n} \times \delta(P_\theta, Q_\theta)^2} \\ &\geq \epsilon^Q_{A^n} - \sqrt{T_{A^n}} \times 2^{-\frac{\kappa}{2}}.\end{aligned}$$

At this point, without loss of generality, we suppose $q \leq T_{A^n}$. Now we set $\epsilon^Q_A = \frac{1}{n}$ and note that $T_{A^n} \leq n \times T_A$, and then we have

$$\begin{aligned}\epsilon^Q_{A^n} - \sqrt{T_{A^n}} \times 2^{\frac{-\kappa}{2}} &\geq \epsilon^Q_{A^n} - \sqrt{\frac{nT_A}{2^\kappa}} \\ &= \epsilon^Q_{A^n} - \sqrt{\frac{T_A}{2^\kappa \epsilon^Q_A}}.\end{aligned}$$

From the first assumption in the proof, the following inequalities are satisfied as

$$\begin{aligned}\epsilon^P_{A^n} &\geq \epsilon^Q_{A^n} - \sqrt{\frac{T_A}{2^\kappa \epsilon^Q_A}} \\ &> \epsilon^Q_{A^n} - \sqrt{2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}} \\ &= 1 - (1-\epsilon^Q_A)^n - \sqrt{2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}} \\ &> 1 - e^{-1} - \sqrt{2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}} \\ &= 0.1929...\end{aligned}$$

from $\epsilon^Q_A = \frac{1}{n}$ and $(1-\epsilon^Q_A)^n = (1-\frac{1}{n})^n < e^{-1}$.

Meanwhile, considering union bound, we can notice $\epsilon^P_{A^n} \leq n \times \epsilon^P_A$ and reminding initial assumption $\epsilon^P_A \leq \frac{T_A}{2^\kappa}$, we have

$$\begin{aligned}\epsilon^P_{A^n} &\leq \frac{nT_A}{2^\kappa} = \frac{T_A}{2^\kappa \epsilon^Q_A} \\ &< 2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}} \\ &= 0.1929...\end{aligned}$$

Summarizing the above results, we obtain

$$1 - e^{-1} - \sqrt{2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}} < \epsilon^P_{A^n}$$

$$< 2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}.$$

After simple computing verification process, we can conclude that the upper and lower bounds of $\epsilon^P_{A^n}$ are exactly the same. This is definitely a contradiction. This contradiction must be from the first wrong assumption. Thus finally, we have

$$\frac{T_A}{\epsilon^Q_A} \geq 2^{\kappa - \log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}$$

i.e., we show S^Q preserves at least $(\kappa - \log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}})$-bit security. □

Remark. In the previous work [1], Micciancio and Walter suggested $(\kappa - 3)$-bit security preserving security reduction. We propose $(\kappa - 2.374)$-bit security preserving security reduction in the above theorem. Our result is almost 1-bit tighter than that of the previous reduction. This improvement will be enhanced in the following results.

It is well known that Δ_{ML} is λ-efficient measure for $\lambda \leq \frac{1}{3}$ [1,2]. Thus we could derive the following corollary easily from Theorem 1.

Corollary 1. If S^P is κ-bit secure and $\Delta_{ML}(P_\theta, Q_\theta) \leq 2^{-\frac{\kappa}{2}}$ $(\leq 1/3)$, then S^Q is $(\kappa - 2.374)$-bit secure.

Also, from Lemma 6 in [1], we can naturally derive the following corollary.

Corollary 2. If S^P is κ-bit secure and $\delta_{RE}(P_\theta, Q_\theta) \leq 1 - e^{-2^{-\frac{\kappa}{2}}} (\leq 1 - e^{-\frac{1}{3}})$, then S^Q is $(\kappa - 2.374)$-bit secure.

In [2], Micciancio and Walter supported and justified their new "bit security" definition by proving a number of technical results, including an application to the security analysis of indistinguishability primitives (e.g., encryption schemes) making use of (approximate) floating point numbers (refer to Section 5.3 in [2]). Corollary 2 and Theorem 8 in [2] are their main results. In this paper, we make both of them further tighter than those in [2]. Following lemma is an improved version of Corollary 2 in [2].

Lemma 1. For any adversary A with resource T attacking S^P and any event E over A's output, the probability of E is denoted by γ_P. The probability of E over A's output when attacking S^Q is also denoted by γ_Q. If the efficient measure δ is $\sqrt{\frac{\gamma_Q}{T}}\sqrt{(\frac{2\times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}})^{-1}}$-efficient and $\delta(P_\theta, Q_\theta) \leq \sqrt{\frac{\gamma_Q}{T}}\sqrt{(\frac{2\times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}})^{-1}}$, then $\gamma_Q \leq \frac{2\times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}} \times \gamma_P \approx 5.184 \times \gamma_P$, where y is sufficiently small positive real number, i.e., $y \to 0^+$.

Proof. Let's consider the contraposition of Theorem 1, i.e., introduce k that satisfies the following equation

$$2^{k-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}-y} = \frac{T}{\gamma_Q} (< 2^{k-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}),$$

where y is sufficiently small positive real number.

For proof by contradiction, suppose

$$\gamma_Q > \frac{2 \times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}} \times \gamma_P.$$

Then we have

$$\begin{aligned} 2^{k-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}-y} &= \frac{T}{\gamma_Q} \\ &< T/(\frac{2 \times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}} \times \gamma_P) \end{aligned}$$

and it implies

$$2^k < \frac{T}{\gamma_P}. \tag{1}$$

Meanwhile, according to the contraposition of Theorem 1, if

$$\frac{T}{\gamma_Q} < 2^{k-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}$$

is hold, then at least one of $2^k > \frac{T}{\gamma_P}$ or $\delta(P_\theta, Q_\theta) > 2^{-\frac{k}{2}}$ should be true. Now, let's remind the original condition of Lemma 1 such that δ satisfies

$$\delta(P_\theta, Q_\theta) \leq \sqrt{\frac{\gamma_Q}{T}} \sqrt{(\frac{2 \times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}})^{-1}}$$

and the value k also satisfies

$$2^{k-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}-y} = \frac{T}{\gamma_Q}.$$

These facts imply that $\delta(P_\theta, Q_\theta) \leq 2^{-\frac{k}{2}}$ holds for the selected k. Therefore, by the contraposition of Theorem 1, $2^k > \frac{T}{\gamma_P}$ should be held but it is contradiction to (1). It means that the initial assumption must be false. Thus, we have

$$\gamma_Q \leq \frac{2 \times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}} \times \gamma_P.$$

□

Remark. Corollary 2 in [2] suggested the relation between γ_P and γ_Q as $\gamma_Q \leq 16 \times \gamma_P$ if efficient measure δ satisfies $\delta(P_\theta, Q_\theta) \leq \sqrt{\frac{\gamma_Q}{16T}} (= \sqrt{\frac{\gamma_Q}{T}} \times 0.25)$. Our Lemma 1 proposes the relation between γ_P and γ_Q as $\gamma_Q \leq 5.184 \times \gamma_P$ if efficient measure δ satisfies $\delta(P_\theta, Q_\theta) \leq \sqrt{\frac{\gamma_Q}{T}} \sqrt{(\frac{2 \times 2^y}{3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}})^{-1}} (\approx \sqrt{\frac{\gamma_Q}{T}} \times 0.44)$. We manage to derive more than 3 times tighter relation between γ_P and γ_Q, even though the upper bound of $\delta(P_\theta, Q_\theta)$ is larger than that of Corollary 2 in [2]. This fact implies that Corollary 2 in [2] provides us somewhat loose reduction.

Using Lemma 1, we could derive the following theorem which gives tighter $(\kappa - 5.54)$-bit security reduction than $(\kappa - 8)$-bit security reduction of Theorem 8 in [2]. The proof is similar to that in [2].

Theorem 2. Let S^P and S^Q be 1-bit secrecy games with black-box access to probability ensembles $(P_\theta)_\theta$ and $(Q_\theta)_\theta$, respectively, and δ be a λ-efficient measure for any $\lambda \leq \sqrt{(\frac{2}{3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}})^{-1}} (\approx 0.44)$. If S^P is κ-bit secure and $\delta(P_\theta, Q_\theta) \leq 2^{-\frac{\kappa}{2}}$, then S^Q is $(\kappa - \log_2 \frac{18}{3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}} - y) \approx (\kappa - 5.544)$-bit secure, where y is sufficiently small positive real number, i.e., $y \to 0^+$.

Proof. Consider an arbitrary adversary A of S^P, whose resource is upper bounded by T^A. Define A's output probability as α_P^A, and its conditional success probability as β_P^A. From the κ-bit security of S^P, the inequality $\alpha_P^A (2\beta_P^A - 1)^2 \leq \frac{T^A}{2^\kappa}$ is satisfied. For proof by contradiction, suppose

$$\alpha_Q^A (2\beta_Q^A - 1)^2 > T^A / 2^{\kappa - \log_2 \frac{18}{3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}} - y}.$$

From Lemma 1, we have

$$\alpha_P^A \geq (\frac{2 \times 2^y}{3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}})^{-1} \times \alpha_Q^A.$$

The reason why we can apply Lemma 1 is that δ is $\sqrt{\frac{\gamma_Q}{T^A}} \sqrt{(\frac{2 \times 2^y}{3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}})^{-1}}$-efficient measure, because the following inequalities are satisfied as

$$
\begin{aligned}
&\sqrt{\left(\frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}\right)^{-1}} \\
&> \sqrt{\left(\frac{2\times 2^{y}}{3-2e^{-1}-\sqrt{5-4e^{-1}}}\right)^{-1}} \\
&> \sqrt{\frac{\alpha_Q^A}{T^A}}\sqrt{\left(\frac{2\times 2^{y}}{3-2e^{-1}-\sqrt{5-4e^{-1}}}\right)^{-1}} \\
&\geq \sqrt{\frac{\alpha_Q^A(2\beta_Q^A-1)^2}{T^A}}\sqrt{\left(\frac{2\times 2^{y}}{3-2e^{-1}-\sqrt{5-4e^{-1}}}\right)^{-1}} \\
&= \sqrt{\frac{\gamma_Q^A}{T^A}}\sqrt{\left(\frac{2\times 2^{y}}{3-2e^{-1}-\sqrt{5-4e^{-1}}}\right)^{-1}} \\
&> \sqrt{2^{\log_2 \frac{18\times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}} \times 2^{-\frac{\kappa}{2}} \times \sqrt{\left(\frac{2\times 2^{y}}{3-2e^{-1}-\sqrt{5-4e^{-1}}}\right)^{-1}} \\
&= 3\times 2^{-\frac{\kappa}{2}} > 2^{-\frac{\kappa}{2}} \geq \delta(P_\theta, Q_\theta).
\end{aligned}
$$

Now, consider $\hat{S}^P$ and $\hat{S}^Q$ which are somewhat modified version of S^P and S^Q. They are almost the same with S^P and S^Q but the only difference is that adversary A can restart the game with totally fresh randomness whenever it wants. Consider an adversary B against $\hat{S}$ that simply runs A until $\mathcal{A} \neq \perp$ (restarting the game if $\mathcal{A} = \perp$) and outputs whatever A returns. If we define α as $\alpha = \min(\alpha_P^A, \alpha_Q^A)$, then adversary B's resource T^B satisfies $T^B < T^A/\alpha$. B's output probability is $\alpha_P^B = \alpha_Q^B = 1$, and the conditional success probability, i.e., the case that successfully solve distinguish problem is $\beta_P^B = \beta_P^A$ (or $\beta_Q^B = \beta_Q^A$) for $\hat{S^P}$ (or $\hat{S^Q}$, respectively). By the properties of λ-efficient measure δ and Δ_{SD}, we have

$$\beta_P^B \geq \beta_Q^B - \sqrt{T^B}\delta(P_\theta, Q_\theta) \geq \beta_Q^B - \sqrt{\frac{T^B}{2^\kappa}}.$$

Thus, we can have

$$2\beta_P^B - 1 \geq 2\beta_Q^B - 1 - 2\sqrt{\frac{T^B}{2^\kappa}}.$$

From the given condition in the theorem, we also have

$$2\beta_P^A - 1 \leq \sqrt{\frac{T^A}{\alpha_P^A \times 2^\kappa}}$$

i.e.,

$$\sqrt{\frac{T^A}{\alpha \times 2^\kappa}} \geq \sqrt{\frac{T^A}{\alpha_P^A \times 2^\kappa}} \geq 2\beta_P^A - 1$$

$$\geq 2\beta_Q^B - 1 - 2\sqrt{\frac{T^B}{2^\kappa}} > 2\beta_Q^B - 1 - 2\sqrt{\frac{T^A}{\alpha \times 2^\kappa}}$$

$$\Rightarrow 3\sqrt{\frac{T^A}{\alpha \times 2^\kappa}} > 2\beta_Q^B - 1 = 2\beta_Q^A - 1.$$

If $\alpha_Q^A \leq \alpha_P^A$, then we have $\alpha = \alpha_Q^A$. Considering our proof by contradiction assumption, we have

$$2^\kappa < \frac{9T^A}{\alpha_Q^A(2\beta_Q^A - 1)^2} < 9 \times 2^{\kappa - \log_2 \frac{18 \times 2^y}{3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}}}.$$

After some computation, we can simplify the above inequality to

$$1 < y + 1 < \log_2(3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}) < -1.374.$$

This is definitely a contradiction. If $\alpha_Q^A > \alpha_P^A$, then we have $\alpha = \alpha_P^A$ and we know that the following inequalities are valid as

$$\left(\frac{2 \times 2^y}{3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}}\right)^{-1} \times \alpha_Q^A \leq \alpha_P^A$$

$$< \frac{9T^A}{2^\kappa(2\beta_Q^A - 1)^2} < \frac{\alpha_Q^A(3 - 2e^{-1} - \sqrt{5 - 4e^{-1}})}{2^{y+1}}.$$

By observation, we can notice that the upper bound and the lower bound of α_P^A are exactly the same. This fact implies that the inequalities can be reduced to $1 < 1$, and thus this case is also a contradiction. Above process tells us that our initial assumption is false and finally we have

$$\alpha_Q^A(2\beta_Q^A - 1)^2 \leq T^A / 2^{\kappa - \log_2 \frac{18}{3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}} - y}$$

and theorem is clearly proven. □

Remark. From Theorem 8 in [2], we propose 2.5-bit tighter security reduction than that of Theorem 8 in [2]. We not only improve the tightness of security reduction, but also extend the possible ranges of λ value. Theorem 8 in [2] can be applied for λ which satisfies $\lambda \leq \frac{1}{4}$, but we extend its allowed ranges to $\lambda \leq 0.44$.

Theorem 1 improves the work in [1]. However, it still has significant limitations for its universal use, because we can apply Theorem 1 only in case when efficient measure δ satisfies $\delta(P_\theta, Q_\theta) \leq 2^{-\frac{\kappa}{2}}$. In other words, we cannot apply Theorem 1 to more general situations. There are many practical situations that $\delta(P_\theta, Q_\theta)$ is much smaller or bigger than $2^{-\frac{\kappa}{2}}$. We need more general criteria and general methodology which give us theoretic guideline how statistical difference affects on security level of cryptographic primitives. This motivation enables us

to come up with the following theorem.

Theorem 3. [Generalization of Theorem 1] Let S^P and S^Q be standard cryptographic schemes with black-box access to probability distribution ensembles P_θ and Q_θ, respectively. If S^P is κ-bit secure and $\delta(P_\theta, Q_\theta) \leq 2^{-\frac{f(\kappa)}{2}}$ for some $2^{-\frac{f(\kappa)}{2}}$-efficient measure δ, then S^Q is $(2\log_2(\sqrt{1+2^{f(\kappa)-\kappa+2}(1-e^{-1})}-1)-f(\kappa)+2\kappa-2)$-bit secure. Here, $f(\kappa)$ should satisfy $f(\kappa) \geq -2\log_2(1-e^{-1}-2^{-\kappa})$, where κ is security level of S^P.

Proof. The overall flow of proof is similar to that of Theorem 1. Considering an arbitrary adversary A, suppose that if $\frac{T_A}{\epsilon^P_A} \geq 2^\kappa$ is satisfied, then $\frac{T_A}{\epsilon^Q_A} < 2^{f(\kappa)-g(\kappa)}$ is satisfied. Here, without loss of generality, we suppose that $g(\cdot)$ is a monotonically increasing function. The reason we can suppose like this is that we are only interested in the value $g(\kappa)$, not the original form of the function $g(\cdot)$. Our purpose is finding $g(\kappa)$, which should be expressed by κ and $f(\kappa)$. Then, we will use the same notations a), b), c), d), and e) in the proof of Theorem 1.

Applying probability preservation property and data processing inequality of Δ_{SD}, we have

$$\begin{aligned}\epsilon^P_{A^n} &\geq \epsilon^Q_{A^n} - \Delta_{SD}([G^P_{S,A}]^n, [G^Q_{S,A}]^n) \\ &\geq \epsilon^Q_{A^n} - \Delta_{SD}((\theta_i, P_{\theta_i})_i, (\theta'_i, Q_{\theta'_i})_i).\end{aligned}$$

Here, $(\theta_i)_i$ (respectively, $(\theta'_i)_i$) is the sequence of queries made during the game $[G^P_{S,A}]^n$ (respectively, $[G^Q_{S,A}]^n$). Note that at any point during the game, conditioned on the event E_i that $(\theta_j, P_{\theta_j})_{j<i}$ and $(\theta'_j, Q_{\theta'_j})_{j<i}$ take some specific and the same value, the adversary behaves identically in the two games up to the point that it makes the i-th query. Especially, the conditional distributions $(\theta_i|E_i)$ and $(\theta'_i|E_i)$ are the same and $\delta((\theta_i|E_i), (\theta'_i|E_i)) = 0$. This fact follows by sub-additivity for joint distributions that

$$\begin{aligned}\delta((\theta_i, P_{\theta_i}|E_i), (\theta'_i, Q_{\theta'_i}|E_i)) &\leq \delta((\theta_i|E_i), (\theta'_i|E_i)) + \delta(P_\theta, Q_\theta) \\ &\leq 0 + 2^{-\frac{f(\kappa)}{2}} = 2^{-\frac{f(\kappa)}{2}}.\end{aligned}$$

This ensures that we can apply Pythagorean probability preservation property, and thus we can guarantee that the following inequalities are also true as

$$\begin{aligned}\epsilon^P_{A^n} &\geq \epsilon^Q_{A^n} - \Delta_{SD}((\theta_i, P_{\theta_i})_i, (\theta'_i, Q_{\theta'_i})_i) \\ &\geq \epsilon^Q_{A^n} - \sqrt{q \times \delta(P_\theta, Q_\theta)^2} \\ &\geq \epsilon^Q_{A^n} - \sqrt{T_{A^n} \times \delta(P_\theta, Q_\theta)^2} \\ &\geq \epsilon^Q_{A^n} - \sqrt{T_{A^n}} \times 2^{-\frac{f(\kappa)}{2}}.\end{aligned}$$

At this point, without loss of generality, we suppose $q \leq T_{A^n}$. Now we set $\epsilon_A^Q = \frac{1}{n}$ and note that $T_{A^n} \leq n \times T_A$, and then we have

$$\begin{aligned}\epsilon_{A^n}^Q - \sqrt{T_{A^n}} \times 2^{\frac{-f(\kappa)}{2}} &\geq \epsilon_{A^n}^Q - \sqrt{\frac{nT_A}{2^{f(\kappa)}}} \\ &= \epsilon_{A^n}^Q - \sqrt{\frac{T_A}{2^{f(\kappa)}\epsilon_A^Q}}.\end{aligned}$$

Now from the first assumption $\frac{T_A}{\epsilon_A^Q} < 2^{f(\kappa)-g(\kappa)}$ in this proof, the following inequalities are satisfied as

$$\begin{aligned}\epsilon_{A^n}^P &\geq \epsilon_{A^n}^Q - \sqrt{\frac{T_A}{2^{f(\kappa)}\epsilon_A^Q}} \\ &> \epsilon_{A^n}^Q - \sqrt{2^{-g(\kappa)}} \\ &= 1 - (1-\epsilon_A^Q)^n - \sqrt{2^{-g(\kappa)}} \\ &> 1 - e^{-1} - \sqrt{2^{-g(\kappa)}}\end{aligned}$$

from $\epsilon_A^Q = \frac{1}{n}$ and $(1-\epsilon_A^Q)^n = (1-\frac{1}{n})^n < e^{-1}$.

Meanwhile, considering union bound, we can notice that $\epsilon_{A^n}^P \leq n \times \epsilon_A^P$. Reminding the initial condition $\epsilon_A^P \leq \frac{T_A}{2^\kappa}$, we have

$$\epsilon_{A^n}^P \leq \frac{nT_A}{2^\kappa} = \frac{T_A}{2^\kappa \epsilon_A^Q} < 2^{f(\kappa)-g(\kappa)-\kappa}.$$

Summarizing the above results, we have

$$1 - e^{-1} - \sqrt{2^{-g(\kappa)}} < \epsilon_{A^n}^P < 2^{f(\kappa)-g(\kappa)-\kappa}. \tag{2}$$

We notice that if the inequality

$$1 - e^{-1} - \sqrt{2^{-g(\kappa)}} \geq 2^{f(\kappa)-g(\kappa)-\kappa} \tag{3}$$

holds, (2) becomes contradiction. We want to find a sufficient condition to derive the contradiction in the proof in order to draw out the contradiction on the first assumption. Since we supposed that $g(\cdot)$ is an increasing function, the left hand side of (3) monotonically increases as $g(\kappa)$ increases. In contrary, for fixed value $f(\kappa)$, the right hand side of (3) monotonically decreases as $g(\kappa)$ increases. Thus the left hand side and the right hand side equations meet at one point. The inequality is reversed at that point. This fact implies that if we consider the equality in (3), we can have the tightest extreme case. Through some

computation, we can solve the equality equation in (3) as

$$\begin{aligned}
&1 - e^{-1} - \sqrt{2^{-g(\kappa)}} = 2^{f(\kappa)-g(\kappa)-\kappa} \\
\iff &2^{f(\kappa)-\kappa} \times 2^{-g(\kappa)} + \sqrt{2^{-g(\kappa)}} - (1 - e^{-1}) = 0 \\
\iff &\sqrt{2^{-g(\kappa)}} = \frac{\sqrt{1 + 2^{f(\kappa)-\kappa+2}(1 - e^{-1})} - 1}{2^{f(\kappa)-\kappa+1}} \\
\iff &-g(\kappa) = 2\{\log_2(\sqrt{1 + 2^{f(\kappa)-\kappa+2}(1 - e^{-1})} - 1) - (f(\kappa) - \kappa + 1)\} \\
&\qquad = 2\log_2(\sqrt{1 + 2^{f(\kappa)-\kappa+2}(1 - e^{-1})} - 1) - 2f(\kappa) + 2\kappa - 2.
\end{aligned}$$

Thus we have

$$\begin{aligned}
&f(\kappa) - g(\kappa) \\
&= 2\log_2(\sqrt{1 + 2^{f(\kappa)-\kappa+2}(1 - e^{-1})} - 1) - f(\kappa) + 2\kappa - 2.
\end{aligned}$$

Then we can conclude that S^Q preserves at least $(2\log_2(\sqrt{1 + 2^{f(\kappa)-\kappa+2}(1 - e^{-1})} - 1) - f(\kappa) + 2\kappa - 2)$-bit security. To maintain Theorem 3 meaningful, the obtained security level should be non-negative. Thus, the condition $f(\kappa) - g(\kappa) \geq 0$ should be satisfied. This fact implies that the following inequalities are satisfied as

$$\begin{aligned}
&f(\kappa) - g(\kappa) \geq 0 \\
\iff &2\log_2(\sqrt{1 + 2^{f(\kappa)-\kappa+2}(1 - e^{-1})} - 1) \geq f(\kappa) - 2\kappa + 2 \\
\iff &\sqrt{1 + 2^{f(\kappa)-\kappa+2}(1 - e^{-1})} \geq 2^{\frac{f(\kappa)-2\kappa+2}{2}} + 1 \\
\iff &2^{f(\kappa)-\kappa+2}(1 - e^{-1}) \geq 2^{f(\kappa)-2\kappa+2} + 2^{\frac{f(\kappa)-2\kappa+4}{2}} \\
\iff &2^{\frac{f(\kappa)}{2}-\kappa+2}(1 - e^{-1} - 2^{-\kappa}) \geq 2^{-\kappa+2} \\
\iff &2^{\frac{f(\kappa)}{2}} \geq \frac{1}{1 - e^{-1} - 2^{-\kappa}} \\
\iff &f(\kappa) \geq -2\log_2(1 - e^{-1} - 2^{-\kappa}).
\end{aligned}$$

Thus, we can conclude that $f(\kappa)$ should satisfy the condition

$$f(\kappa) \geq -2\log_2(1 - e^{-1} - 2^{-\kappa})$$

for applying Theorem 3. Once this condition is satisfied, we can arbitrary set $f(\kappa)$ value whatever we want. The detailed applying example of Theorem 3 will be dealt with at following remark. Thus, we finish the proof. □

Remark. Let's take a look at an application of Theorem 3. At the end of Section 5.3 in [1], Micciancio and Walter argued that for a given set of parameters, if we denote P as a perfect Gaussian distribution and Q as an output of the new sampler, $\Delta_{ML}(P, Q) \leq 2^{-52}$ is satisfied. They applied their Lemma 3 in

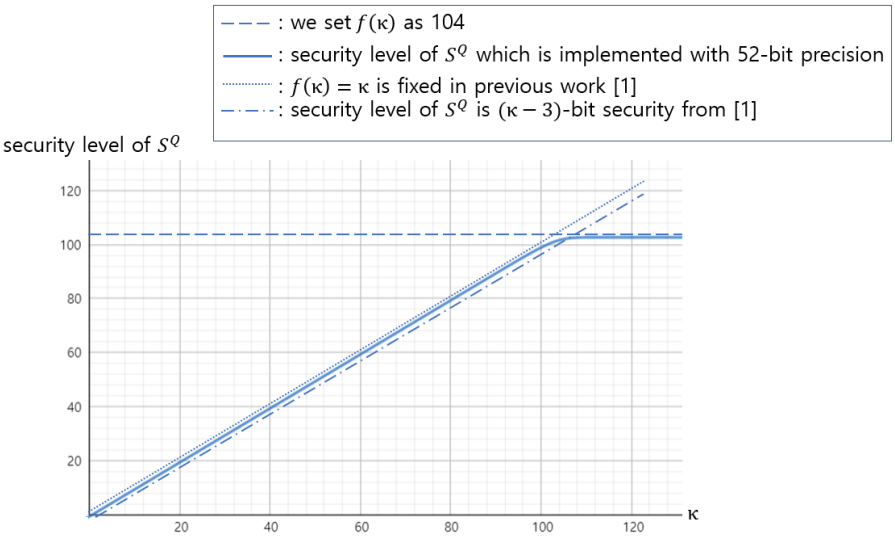

Fig. 1. Varying security level of S^Q where $f(\kappa)$ is fixed as 104.

[1] to analyze the security, but Lemma 3 in [1] has limitation that it can only be applied for S^P whose security level κ satisfies $\kappa \leq 104$. In general, 104-bit security is not enough. While in many situations, we want to be guaranteed at least 128-bit security, Lemma 3 in [1] cannot be applied for $\kappa = 128$ case. In other words, Lemma 3 in [1] cannot give any information for $\kappa > 104$. Contrary to this, we can apply Theorem 3 for these cases. Suppose S^P is 128-bit secure and $\Delta_{ML}(P, Q) \leq 2^{-52}$. We can arbitrary set as $f(128) = 104$ (i.e., $\Delta_{ML}(P, Q) \leq 2^{-52} = 2^{-\frac{f(128)}{2}}$) because the following inequality $f(128) = 104 > -2\log_2(1 - e^{-1} - 2^{-128}) \approx 1.32$ is trivially satisfied. Then, we can conclude that S^Q preserves at least $(2\log_2(\sqrt{1 + 2^{f(128)-128+2}(1 - e^{-1})} - 1) - f(128) + 2 \times 128 - 2) \approx 102.676$-bit security from Theorem 3.

Figure 1 indicates the varying security level of S^Q where $f(\kappa)$ is fixed as 104. Summarizing the discussion so far, we can interpret our Theorem 3 as follows. Through Theorem 3, we can estimate the affects on security level when κ-bit secure original scheme is implemented on $\frac{f(\kappa)}{2}$-bit precision system. In the previous work [1], $f(\kappa)$ was fixed as κ, but our Theorem 3 is generalized to make it possible to security level κ and precision $\frac{f(\kappa)}{2}$ variate independently. Through Theorem 3, we can provide the theoretic ground on how security level of 128-bit security scheme may change if it is implemented on 32-bit or 64-bit precision system. Following Figure 2 is a 3-dimensional plot which indicates the security level of S^Q determined by κ and $f(\kappa)$.

Until now, we have given tighter and more generalized versions of Micciancio and Walter's results which were introduced [1,2]. However, Theorems 1, 2, 3,

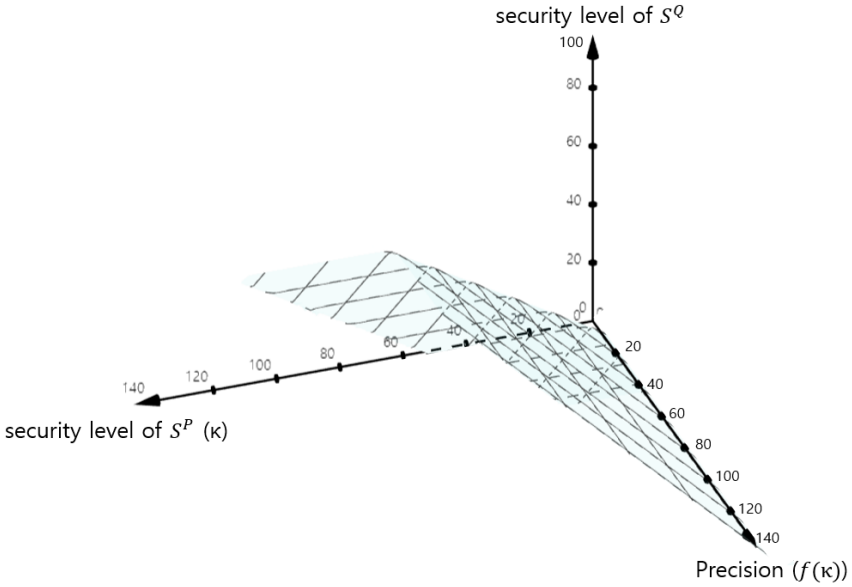

Fig. 2. Varying security level of S^Q with respect to κ and $f(\kappa)$.

and Lemma 1 can only be applied with λ-efficient measure δ. There are several information-theoretic measures which are used to analyze security reduction. Among them, only the max-log distance Δ_{ML} has been proven that it is a λ-efficient measure. As we already took a look at Corollary 2, we can apply Theorems 1 and 3 also with δ_{RE} from Lemma 6 in [1]. But, we can't apply our theorems with RD_α, Δ_{SD}, and Δ_{KL} directly. Thus, we have undertaken further research to find out additional results for other measures. Those results are given in the last two theorems and one corollary. Theorem 4 deals with infinity order of RD, which is well-known to be closely related to Δ_{ML}. Theorem 4 considers only the case that adversary is in resource restricted environment. This kind of premise is not that impractical, but actually practically meaningful, e.g., the situation that adversary should succeed the attack within short time.

Theorem 4. [Applying to adversary in resource restricted environment] Let S^P and S^Q be standard cryptographic schemes with black-box access to probability distribution ensembles P_θ and Q_θ, respectively. If S^P is κ-bit secure and $RD_\infty(Q_\theta||P_\theta) \leq 2^{\frac{1}{\kappa^n}}$, then S^Q is $(\kappa - \frac{T_A}{\kappa^n})$-bit secure, where $T_A \leq \kappa^{n+1}$ (i.e., adversary's time resources are restricted).

Proof. Notations are the same as the proofs of the previous theorems. From the definition and the probability preservation property of RD_∞, we have

$$RD_\infty(G^Q_{S,A}||G^P_{S,A}) = \max_{x\in Supp(Q)}(\frac{G^Q_{S,A}(x)}{G^P_{S,A}(x)}) \geq \frac{\epsilon^Q_A}{\epsilon^P_A}.$$

Then, by applying multiplicative property and data processing inequality of RD_∞, we also have

$$RD_\infty(G^Q_{S,A}||G^P_{S,A}) \geq \frac{\epsilon^Q_A}{\epsilon^P_A} \iff$$

$$\begin{aligned}\epsilon^P_A &\geq \frac{\epsilon^Q_A}{RD_\infty(G^Q_{S,A}||G^P_{S,A})} \\ &\geq \frac{\epsilon^Q_A}{RD_\infty(Q_\theta||P_\theta)^q} \geq \frac{\epsilon^Q_A}{RD_\infty(Q_\theta||P_\theta)^{T_A}}.\end{aligned}$$

Here, we assume that $q \leq T_A$ as usual. From the given condition of Theorem 4, we know that $\frac{T_A}{\epsilon^P_A} \geq 2^\kappa$ is satisfied, and thus we have the following inequalities as

$$2^{-\kappa} \geq \frac{\epsilon^P_A}{T_A} \geq \frac{\epsilon^Q_A}{T_A}\frac{1}{RD_\infty(Q_\theta||P_\theta)^{T_A}} \geq \frac{\epsilon^Q_A}{T_A} \times 2^{\frac{-T_A}{\kappa^n}}$$

$$\begin{aligned}&\iff 2^{-\kappa+\frac{T_A}{\kappa^n}} \geq \frac{\epsilon^Q_A}{T_A} \\ &\iff \frac{T_A}{\epsilon^Q_A} \geq 2^{\kappa-\frac{T_A}{\kappa^n}} \\ &\iff \log_2(\frac{T_A}{\epsilon^Q_A}) \geq \kappa - \frac{T_A}{\kappa^n}.\end{aligned}$$

Therefore, we can conclude that S^Q preserves at least $(\kappa - \frac{T_A}{\kappa^n})$-bit security. To maintain Theorem 4 meaningful, T_A should satisfy the condition $T_A \leq \kappa^{n+1}$ because the obtained security level should be non-negative. Now, we finish the proof. □

However, the most widely used information-theoretic measure to analyze security reduction between two cryptographic schemes is the statistical distance Δ_{SD}. It is important to estimate how much Δ_{SD} value between two different probability distributions affect on the security level. We can provide the theoretic guideline for the relationship between Δ_{SD} and the security level in the following theorem.

Theorem 5. Let S^P and S^Q be standard cryptographic schemes with black-box access to probability distribution ensembles P_θ and Q_θ, respectively. If S^P

is κ-bit secure and $\Delta_{SD}(P_\theta, Q_\theta) \leq 2^{-h(\kappa)}$, then S^Q is $\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}}$-bit secure. Here, $h(\kappa)$ should satisfy $h(\kappa) \geq -\log_2(1-\frac{1}{2^\kappa})$, where κ is the security level of S^P.

Proof. Notations are the same as the proofs of the previous theorems. From the probability preservation property of Δ_{SD}, we have

$$\Delta_{SD}(G^P_{S,A}, G^Q_{S,A}) \geq \epsilon^Q_A - \epsilon^P_A.$$

Then, applying additive property, data processing inequality, and $q \leq T_A$, we can derive the following inequalities as

$$\begin{aligned}
&\Delta_{SD}(G^P_{S,A}, G^Q_{S,A}) \geq \epsilon^Q_A - \epsilon^P_A \\
\iff \epsilon^P_A &\geq \epsilon^Q_A - \Delta_{SD}(G^P_{S,A}, G^Q_{S,A}) \\
&\geq \epsilon^Q_A - \Delta_{SD}(P_\theta, Q_\theta) \times q \\
&\geq \epsilon^Q_A - \Delta_{SD}(P_\theta, Q_\theta) \times T_A.
\end{aligned}$$

From the given condition of Theorem 5, we know that $\frac{T_A}{\epsilon^P_A} \geq 2^\kappa$ is satisfied, and thus we have the following inequalities as

$$\begin{aligned}
2^{-\kappa} \geq \frac{\epsilon^P_A}{T_A} &\geq \frac{\epsilon^Q_A}{T_A} - \Delta_{SD}(P_\theta, Q_\theta) \geq \frac{\epsilon^Q_A}{T_A} - 2^{-h(\kappa)} \\
\iff 2^{-\kappa} + 2^{-h(\kappa)} &\geq \frac{\epsilon^Q_A}{T_A} \\
\iff \frac{T_A}{\epsilon^Q_A} &\geq \frac{1}{2^{-\kappa}+2^{-h(\kappa)}} \\
\iff \log_2 \frac{T_A}{\epsilon^Q_A} &\geq \log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}}.
\end{aligned}$$

Then we can conclude that S^Q preserves at least $\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}}$-bit security. To maintain Theorem 5 meaningful, the obtained security level should be non-negative. Thus the condition $\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}} \geq 0$ should be satisfied and the following inequalities are satisfied as

$$\begin{aligned}
&\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}} \geq 0 \\
\iff &\frac{1}{2^{-\kappa}+2^{-h(\kappa)}} \geq 1 \\
\iff &2^{-\kappa}+2^{-h(\kappa)} \leq 1 \\
\iff &h(\kappa) \geq -\log_2(1-2^{-\kappa}).
\end{aligned}$$

Thus, we can conclude that $h(\kappa)$ should satisfy the condition

$$h(\kappa) \geq -\log_2(1-\frac{1}{2^\kappa})$$

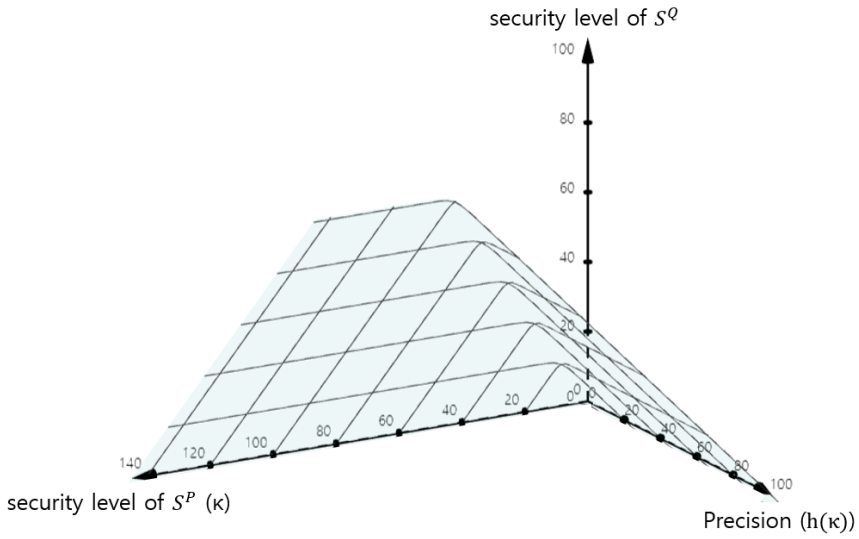

Fig. 3. Varying security level of S^Q with respect to κ and $h(\kappa)$.

for applying Theorem 5. Now, we finish the proof. □

From Pinsker's inequality, for the relationship between Δ_{SD} and Δ_{KL}, the following inequality is satisfied as

$$\Delta_{SD}(P,Q) \leq \sqrt{\frac{1}{2}\Delta_{KL}(Q||P)}.$$

Using this formula, we can derive the following corollary without proof.

Corollary 3. If S^P is κ-bit secure and $\Delta_{KL}(Q_\theta||P_\theta) \leq 2^{1-2h(\kappa)}$, then S^Q is $\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}}$-bit secure. Here, $h(\kappa)$ should satisfy $h(\kappa) \geq -\log_2(1-\frac{1}{2^\kappa})$, where κ is the security level of S^P.

Remark. Similar as Theorem 3, Theorem 5 and Corollary 3 also can be interpreted as follows. Through Theorem 5 (respectively, Corollary 3), we can estimate the affects on security level when κ-bit secure original scheme is implemented on $h(\kappa)$-bit (respectively, $(1-2h(\kappa))$-bit) precision system. Figure 3 is a 3-dimensional plot which indicates the security level of S^Q determined by κ and $h(\kappa)$.

4 Conclusions and Future Works

In this paper, information-theoretic security reductions from the statistical difference between probability distributions were derived in terms of various information-theoretic measures. We provide diverse types of security reduction formulas for the five kinds of information-theoretic measures, those measures are; Δ_{SD}, RD_{∞}, δ_{KL}, Δ_{ML}, and, δ_{RE}. We proposed tighter and more generalized version of security reductions than those of the previous works [1,2]. These reduction results are expected to provide information-theoretic methodology to estimate security loss in situation such as replacing with the different probability distributions.

For future works, we will conduct further research to prove or disprove whether the bit security reduction results are information-theoretic limit or not. We are asking the question, "Is the tighter reduction than the proposed one theoretically possible?" The second research topic is further generalization of Theorem 4. Up to now, Theorem 4 only can deal with constrained adversary and even it can be applied only for RD of infinity order. We want to generalize Theorem 4 to cover arbitrary adversary and arbitrary orders. These might be interesting future research topics.

References

1. Micciancio, D., Walter, M.: Gaussian sampling over the integers: Efficient, generic, constant-time. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10402, pp. 455-485. Springer, Cham (2017).
2. Micciancio, D., Walter, M.: On the bit security of cryptographic primitives. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10820, pp. 3-28. Springer (2018).
3. Walter, M.: Sampling the integers with low relative error. In: Buchmann, J., Nitaj, A., Rachidi, T. (eds.) AFRICACRYPT 2019. LNCS, vol. 11627, pp. 157-180. Springer (2019).
4. Bai, S., Langlois, A., Lepoint, T., Stehlé, D., Steinfeld, R.: Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 3–24. Springer, Heidelberg (2015).
5. Prest, T.: Sharper bounds in lattice-based cryptography using the Rényi divergence. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10624, pp. 347–374. Springer, Cham (2017).
6. Gao, Y., Wang, K.: Probability preservation property in the security reduction. In: ICICT 2018 (published in Procedia Computer Science), vol. 131, pp. 665-675. (2018).
7. Takashima, K., Takayasu, A.: Tighter security for efficient lattice cryptography via the Rényi divergence of optimized orders. In: Au, M.-H., Miyaji, A. (eds.) ProvSec 2015. LNCS, vol. 9451, pp. 412–431. Springer, Cham (2015).
8. Matsuda, T., Takashashi, K., Murakami, T.: Improved security evaluation techniques for imperfect randomness from arbitrary distributions. In: Lin, D., Sako, K. (eds.) PKC 2019. LNCS, vol. 11442, pp. 549-580. Springer (2019).

9. Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal gaussians. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 40–56. Springer, Heidelberg (2013).
10. Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 1–17. Springer, Heidelberg (2013).
11. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010).
12. Micciancio, D., Peikert, C.: Hardness of SIS and LWE with small parameters. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 21–39. Springer, Heidelberg (2013).
13. Ling, S., Phan, D.H., Stehle, D., Steinfeld, R.: Hardness of k-LWE and applications in traitor tracing. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 315–334. Springer, Heidelberg (2014).
14. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput. 37, 267–302 (2007).
15. Saarinen, M.-J.O.: Gaussian sampling precision in lattice cryptography. Cryptology ePrint Archive, Report 2015/953 (2015).
16. Dwarakanath, N.C., Galbraith, S.D.: Sampling from discrete gaussians for lattice-based cryptography on a constrained device. Appl. Algebra Eng. Commun. Comput. 25(3), 159–180 (2014).
17. Pöppelmann, T., Ducas, L., Güneysu, T.: Enhanced lattice-based signatures on reconfigurable hardware. In: Batina, L., Robshaw, M. (eds.) CHES 2014. LNCS, vol. 8731, pp. 353–370. Springer, Heidelberg (2014).
18. Goudarzi, D., Martinelli, A., Passelégue, A., Prest, T.: Unifying leakage models on a Rényi day. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11692, pp. 683-712. Springer (2019).