IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 22, 2021, accepted September 30, 2021, date of publication October 13, 2021,
date of current version October 19, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3119707*

# Bit Security Estimation Using Various Information-Theoretic Measures

**DONG-HOON LEE[1], (Graduate Student Member, IEEE), YOUNG-SIK KIM[2], (Member, IEEE), AND JONG-SEON NO[1], (Fellow, IEEE)**

[1]Department of ECE, Seoul National University, Seoul 08826, South Korea
[2]Department of EE, Chosun University, Gwangju 61452, South Korea

Corresponding author: Young-Sik Kim (iamyskim@chosun.ac.kr)

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

**ABSTRACT** In this paper, we propose various quantitative information-theoretic bit security reduction measures that correlate the statistical difference between two probability distributions with the security level gap for two cryptographic schemes. We derive tighter relations between information-theoretic measures for quantifying the precision and guarantee the security level of the cryptographic scheme implemented over a precision-restricted environment. Further, the generalized versions of previous security reductions are devised by relaxing the constraints on the upper bounds of the information-theoretic measures. This makes it possible to estimate bit security more reliable and improves the security level. We also estimate the effects on the security level when the $\kappa$-bit secure original scheme is implemented on a $p$-bit precision system. In previous studies, $p$ was fixed as $\frac{\kappa}{2}$; however, the proposed schemes are generalized such that the security level $\kappa$ and precision $p$ can vary independently. This results in a significant difference. Moreover, previous results cannot provide the exact lower bound of the security level for $p \neq \frac{\kappa}{2}$. However, the proposed results can provide the exact lower bound of the estimation value of the security level as long as the precision $p$ satisfies certain conditions. We provide diverse types of security reduction formulas for the six types of information-theoretic measures. The proposed schemes can provide information-theoretic guidelines regarding the difference between the security levels of two identical cryptographic schemes when extracting randomness from two different probability distributions. In particular, the proposed schemes can be used to quantitatively estimate the effect of the statistical difference between the ideal and real distributions on the security level.

**INDEX TERMS** Bit security, Hellinger distance, information-theoretic measures, Kullback-Leibler divergence, $\lambda$-efficient measure, max-log distance, relative error, Rényi divergence, security reduction, statistical distance.

## I. INTRODUCTION

The security of almost every modern cryptographic primitive depends on randomness, which is extracted from a specific probability distribution (e.g., a lattice-based cryptographic scheme extracts its randomness from a discrete Gaussian distribution). In other words, the probability distribution of the cryptographic scheme has an important influence on its security. From this perspective, many studies have been conducted to analyze the way that the security level changes when the probability distribution for the randomness of the cryptographic scheme is replaced by another probability distribution. Traditionally, the "probability preservation property (PPP)" [4], [6], [14] has been widely used to correlate the difference between two statistical distributions based on the probability of a successful adversary attack. This type of security reduction enables us to compare the relative security levels among cryptographic schemes. However, we cannot obtain any detailed quantitative information regarding the security level using the PPP alone. In light of this, several researchers have conducted studies to enable quantitative security analyses.

Micciancio and Walter [1], [2] are considered as leaders in this field. They suggested various quantitative security reductions through information-theoretic measures, and expressed security reductions in terms of bit security. However, there is

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

a problem in that several information-theoretic measures are used for estimating the bit security of a cryptographic scheme, and the upper bounds required for each information-theoretic measure are different. In particular, when the bit security concept is applied in an actual cryptographic scheme, even if the bit security is designed at a specific level or higher, if the precision in the real system is limited to a higher degree than the security level, the security of the implemented scheme is affected. Micciancio and Walter proposed how to determine the relationship between information-theoretic measures for quantifying the precision and guaranteed the security of the cryptographic scheme implemented in a precision-restricted environment. However, note that their results provide clear information in only limited cases, for which similar types of limitations can be found in [12] and thus they can further be improved.

The contributions of this study are as follows: First, we derive tighter security reduction bounds compared with the works by Micciancio and Walter [1], [2]. Second, we propose further generalized versions of both Micciancio and Walter's [1] and Yasunaga's [12] security reductions by relaxing the constraints on the upper measurement bounds, such as $\lambda$-efficient measures and the Hellinger distance. Using these approaches, we propose methodologies for elaborately estimating the effects on the security level of the cryptographic scheme when the $\kappa$-bit secure original scheme is implemented on a $p$-bit precision system, where $p$ can be set to any value as long as certain conditions are satisfied. Third, we provide various types of security reduction formulas for the six types of information-theoretic measures: statistical distance, Rényi divergence, Kullback-Leibler divergence, max-log distance, relative error, and Hellinger distance. These measures are often used in cryptography for security reduction analyses.

The remainder of this paper is organized as follows. In Section II, we briefly introduce concepts necessary for understanding our results. In Section III, we provide three main approaches: tighter security reductions for cryptographic schemes, further generalized and more accurate security reductions, and various forms of security reductions expressed by six types of information-theoretic measures. Finally, in Section IV, we provide conclusions and directions for future research.

## II. PRELIMINARIES

### A. INFORMATION-THEORETIC MEASURES

Several widely known information-theoretic measures are used to analyze a security reduction in the cryptographic schemes.

#### 1) STATISTICAL DISTANCE ($\Delta_{SD}$)

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 the probability distribution.

#### 2) RÉNYI DIVERGENCE ($RD_\alpha$)

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

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

Here, $RD_\alpha$ satisfies many attractive features such as probability preservation, multiplicative properties, and data processing inequality [4], [5], [7].

#### 3) KULLBACK-LEIBLER DIVERGENCE ($\Delta_{KL}$)

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

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

#### 4) MAX-LOG DISTANCE ($\Delta_{ML}$)

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 $\Delta_{ML}$ only when the support sets of the two distributions are the same.

#### 5) RELATIVE ERROR ($\delta_{RE}$)

For any two discrete probability distributions $P$ and $Q$, the relative error between $P$ and $Q$ is defined as follows [3]:

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

#### 6) HELLINGER DISTANCE (HD)

For any two discrete probability distributions $P$ and $Q$ over the same support $\Omega$, the Hellinger distance between $P$ and $Q$ is defined as [12]

$$HD(P, Q) = \sqrt{\frac{1}{2} \sum_{x \in \Omega} (\sqrt{P(x)} - \sqrt{Q(x)})^2}.$$

### B. SPECIAL TYPES OF MEASURES

Micciancio and Walter defined two special types of measures [1], i.e., a "useful measure" and a "$\lambda$-efficient measure." We reuse their definitions.

#### 1) USEFUL MEASURE

Any measure $\delta$ that satisfies the following three properties is called a 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 the probability distribution $P$ (respectively, $Q$). This property makes it possible to determine the probability of an event occurring under distribution $P$ in terms of the probability of the same event occurring under distribution $Q$ and the measured value $\delta(P, Q)$. It is not difficult 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.

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 us define $X_{<i} = (X_1, \ldots, X_{i-1})$ (similarly 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 $\delta$ does not increase under an additional function application.

### 2) λ-EFFICIENT MEASURE

Consider a measure $\delta$ that satisfies the above two properties b) and c). We call this a "λ-efficient measure" if it satisfies the following property d) instead of the above property a):

d) Pythagorean probability preservation property (with parameter $\lambda$): 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 applied for all $i$ and $a_i \in \prod_{j<i} S_j$, then $\Delta_{SD}((P_i)_i, (Q_i)_i) \leq ||(\max_{a_i} \delta(P_i|a_i, Q_i|a_i))_i||_2$.

## C. NEW NOTION OF BIT SECURITY

Bit security has long played a crucial role in measuring and estimating the quantitative security level of cryptographic primitives. The traditional definition of bit security is simple and is defined as $\min_A\{\log_2 \frac{T_A}{\epsilon_A}\}$, where for an arbitrary adversary $A$, $T_A$ and $\epsilon_A$ are the resources and attack success probability of the adversary, respectively. Micciancio and Walter defined a new notion of bit security by designing a new concept of a security game [2]. Using their newly devised security game, they redefined the advantage of an adversary in terms of information-theoretic quantities. We 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 a random variable $\mathcal{C} \in \{0, 1\}^n$, from a distribution $D_{\mathcal{C}}$. At the end of the game, A outputs a value that is represented by the random variable $\mathcal{A}$. The adversary's goal is to output a value a such that $R(c, a)$, where R is a relation. In addition, 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 the corresponding random variables $\mathcal{C}$ and $\mathcal{A}(\mathcal{C})$, the advantage of the adversary 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 $\mathcal{Y}_{c,a} = \{y|\mathcal{C} = c, \mathcal{A} = a\}$, which are 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 $adv^A = \alpha^A\beta^A$, whereas for a decision game, it is $adv^A = \alpha^A(2\beta^A - 1)^2$, where $\alpha^A = Pr[\mathcal{A} \neq \perp]$ is the output probability, and $\beta^A = Pr[R(\mathcal{C}, \mathcal{A})|\mathcal{A} \neq \perp]$ is the conditional probability of success.*

## III. MAIN RESULTS

Micciancio and Walter found quantitative security reductions between two identical cryptographic schemes with all other conditions being equal and differing only in the probability distributions by which the schemes extract randomness [1], [2]. Their studies made it possible to estimate the security loss that would occur when the given probability distribution was replaced by another distribution. In other words, their approaches have provided information-theoretic guidelines of the security level of the system (i.e., how the statistical difference between two distributions affects the security level of the cryptographic scheme). However, their results might provide clear information only in a limited number of cases and can be generalized. That is, their results provide detailed information only when the information-theoretic measure values between two probability distributions are upper-bounded by a specific fixed value. Owing to these problems, it is necessary to bring about tighter and more generalized security reductions. Our first approach is a tighter version of Lemma 3 in [1], which is proved by using a similar approach to that in [1] as follows:

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

Further, we have the following:

i) For $\lambda \leq 1/3$: If $S^P$ is $\kappa$-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.

ii) For $\lambda \leq 2/9$: If $S^P$ is $\kappa$-bit secure and $\Delta_{KL}(Q_\theta||P_\theta) \leq 2^{-\frac{\kappa}{2}} (\leq 2/9)$, then $S^Q$ is $(\kappa - 2.374)$-bit secure.

iii) For $\lambda \leq 1/3$: If $S^P$ is $\kappa$-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.

*Proof:* First, we prove the main statement of this theorem. 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 us define the following notations:

a) $G_{S,A}^P$ (respectively, $G_{S,A}^Q$): Security game defining an event in which 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 $A$ will win the security game $[G_{S,A}^P]^n$ (respectively, $[G_{S,A}^Q]^n$) at least once
d) $T_{A^n}$: Required resources for $A$ to win the security game $[G_{S,A}^P]^n$ (respectively, $[G_{S,A}^Q]^n$) at least once
e) $q$: Number of queries of adversary $A$

Applying the probability preservation property and data processing inequality of $\Delta_{SD}$, we have the following:

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

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 event $E_i$, $(\theta_j, P_{\theta_j})_{j<i}$ and $(\theta_j', Q_{\theta_j'})_{j<i}$ take the same specific value, and the adversary behaves identically in the two games up to the point that it makes the $i$-th query. In particular, 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 is followed by sub-additivity for the joint distributions in which

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

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

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

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

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

From the first assumption in the proof, the following inequalities,

$$\begin{aligned}\epsilon_{A^n}^P &\geq \epsilon_{A^n}^Q - \sqrt{\frac{T_A}{2^\kappa \epsilon_A^Q}}\\ &> \epsilon_{A^n}^Q - \sqrt{2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}}\\ &= 1 - (1-\epsilon_A^Q)^n - \sqrt{2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}}\\ &> 1 - e^{-1} - \sqrt{2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}}\\ &\approx 0.1929\end{aligned}$$

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

Meanwhile, considering a union bound, we can observe that $\epsilon_{A^n}^P \leq n \times \epsilon_A^P$, and recalling the initial assumption $\epsilon_A^P \leq \frac{T_A}{2^\kappa}$, we have the following:

$$\begin{aligned}\epsilon_{A^n}^P \leq \frac{nT_A}{2^\kappa} &= \frac{T_A}{2^\kappa \epsilon_A^Q}\\ &< 2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}\\ &\approx 0.1929.\end{aligned}$$

Summarizing the above results, we obtain

$$\begin{aligned}1 - e^{-1} - \sqrt{2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}} &< \epsilon_{A^n}^P\\ &< 2^{-\log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}.\end{aligned}$$

After a simple computing verification process, we can conclude that the upper and lower bounds of $\epsilon_{A^n}^P$ are the same. This is clearly a contradiction, which must be based on the first incorrect assumption. Thus, we finally have

$$\frac{T_A}{\epsilon_A^Q} \geq 2^{\kappa - \log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}}}.$$

That is, we show that $S^Q$ preserves at least $(\kappa - \log_2 \frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}})$-bit security. Thus, we prove the main statement of this theorem.

Meanwhile, it is well known that $\Delta_{ML}$ and $\Delta_{KL}$ are $\lambda$-efficient measures for $\lambda \leq \frac{1}{3}$ and $\lambda \leq \frac{2}{9}$, respectively [1], [2]. Thus, we can easily derive i) and ii) from the main statement of the theorem. Moreover, from Lemma 6 in [1], we have the relation $\Delta_{ML}(P, Q) \leq -\ln(1 - \delta_{RE}(P, Q))$, and we can naturally derive iii) from i). □

*Remark 1: In a previous work [1], Micciancio and Walter suggested a* $(\kappa - 3)$*-bit security-preserving reduction. We propose a* $(\kappa - 2.374)$*-bit security-preserving reduction in the above theorem. Our result is almost 1-bit tighter than that of the previous reduction. Although a 1-bit improvement may seem minimal, this improvement will be enhanced in the later results, that is, for up to 2.5-bit security gains in Theorem 2 and the generalized result in Theorem 3.*

*In a previous study [9], Genise and Micciancio proposed a novel sampling algorithm for G-lattices for any modulus* $q < b^k$ *(where the positive integers* $b \geq 2$ *and* $k \geq 1$

*are implicit parameters of the algorithm). Their proposed sampler SAMPLEG outputs a sample with a distribution statistically close to* $D_{\Lambda_u^{\perp}(g^T),s}$ *(which denotes the ideal discrete Gaussian distribution defined on the lattice coset* $\Lambda_u^{\perp}(g^T)$*). In Section 3.2 in [9], a quantitative security analysis is provided regarding the extent to which security loss will occur when using SAMPLEG instead of* $D_{\Lambda_u^{\perp}(g^T),s}$*. Assuming that a cryptographic scheme using a perfect sampler for* $D_{\Lambda_u^{\perp}(g^T),s}$ *is* $\kappa$*-bit secure, they concluded that swapping* $D_{\Lambda_u^{\perp}(g^T),s}$ *with SAMPLEG yields approximately* $\kappa - 2\log(tb^2) - 3log\log q - 5$ *bits of security (where* $t$ *is a tail-cut parameter) under the given conditions. Deriving this result, they used Corollary 1, Proposition 1, and Lemma 3 in [1]. Note that they applied Lemma 3 in [1] to obtain this result. Because Theorem 1 provides an almost 1-bit tighter security reduction than that of Lemma 3 in [1], we can expect to obtain additional security gains if we apply Theorem 1 in place of this lemma.*

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 the main results. In this paper, we make both the results tighter than those in [2]. The 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 the output of* $A$*, the probability of* $E$ *is denoted by* $\gamma_P$*. The probability of* $E$ *over the output of* $A$ *when attacking* $S^Q$ *is denoted by* $\gamma_Q$*. If the efficient measure* $\delta$ *is* $\sqrt{\frac{\gamma_Q}{T}}\sqrt{(\frac{2\times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}})^{-1}}$*-efficient and*

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

*then*

$$\gamma_Q \le \frac{2\times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}} \times \gamma_P \approx 5.184 \times \gamma_P,$$

*where* $y$ *is a sufficiently small positive real number, i.e.,* $y \to 0^+$.

*Proof:* Let us consider the contraposition of Theorem 1, that is, we introduce a value $k$ 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 a sufficiently small positive real number.

For proof through a contradiction, suppose

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

We then have

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

which implies

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

Meanwhile, according to the contraposition of Theorem 1, if

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

holds, then either $2^k > \frac{T}{\gamma_P}$ or $\delta(P_\theta, Q_\theta) > 2^{-\frac{k}{2}}$ should be true. Now, let us recall the original condition of Lemma 1 such that $\delta$ satisfies

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

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 $\delta(P_\theta, Q_\theta) \le 2^{-\frac{k}{2}}$ holds for the selected $k$. Therefore, based on the contraposition of Theorem 1, $2^k > \frac{T}{\gamma_P}$ should be held; however, this contradicts (1), which implies that the initial assumption must be false. Thus, we have

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

□

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

Using Lemma 1, we can derive the following theorem that provides tighter $(\kappa - 5.54)$-bit security reduction than $(\kappa - 8)$-bit security reduction of Theorem 8 in [2]. The following theorem can be used to analyze the security of indistinguishability primitives: This proof is similar to that in [2].

*Theorem 2: Let* $S^P$ *and* $S^Q$ *be a 1-bit secrecy game with black-box access to probability ensembles* $(P_\theta)_\theta$ *and* $(Q_\theta)_\theta$*, respectively, and* $\delta$ *be a* $\lambda$*-efficient measure for any* $\lambda \le \sqrt{(\frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}})^{-1}}(\approx 0.44)$*. If* $S^P$ *is* $\kappa$*-bit secure and* $\delta(P_\theta, Q_\theta) \le 2^{-\frac{\kappa}{2}}$*, 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 a sufficiently small positive real number, that is,* $y \to 0^+$.

*Proof:* Consider an arbitrary adversary $A$ of $S^P$, whose resource is upper-bounded by $T^A$. We define the output probability of $A$ as $\alpha_P^A$, and its conditional success probability as $\beta_P^A$. From the $\kappa$-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 through contradiction, suppose the following:

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

From Lemma 1, we have

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

We can apply Lemma 1 because $\delta$ is a $\sqrt{\frac{\gamma_Q}{T^A(\frac{2\times 2^y}{3-2e^{-1}-\sqrt{5-4e^{-1}}})^{-1}}}$-efficient measure, and the following inequalities are satisfied:

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

Now, consider $\hat{S}^P$ and $\hat{S}^Q$, which are slightly modified versions of $S^P$ and $S^Q$. They are almost the same as $S^P$ and $S^Q$, with the only difference being that adversary $A$ can restart the game with completely fresh randomness whenever it wants. Consider an adversary $B$ against $\hat{S}$, which simply runs $A$ until $\mathcal{A} \neq \perp$ (restarting the game if $\mathcal{A} = \perp$) and outputs whatever $A$ returns. If we define $\alpha$ as $\alpha = \min(\alpha_P^A, \alpha_Q^A)$, the resource $T^B$ of adversary $B$ then satisfies $T^B < T^A/\alpha$. The output probability of $B$ is $\alpha_P^B = \alpha_Q^B = 1$, and the conditional success probability, i.e., the case that successfully solves the 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). Based on the properties of $\lambda$-efficient measures $\delta$ and $\Delta_{SD}$, 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 have

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

From the condition given in the theorem, we also have

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

that is,

$$\begin{aligned}
\sqrt{\frac{T^A}{\alpha \times 2^\kappa}} &\geq \sqrt{\frac{T^A}{\alpha_P^A \times 2^\kappa}} \geq 2\beta_P^A - 1 \\
&\geq 2\beta_Q^B - 1 - 2\sqrt{\frac{T^B}{2^\kappa}} > 2\beta_Q^B - 1 - 2\sqrt{\frac{T^A}{\alpha \times 2^\kappa}} \\
&\Rightarrow 3\sqrt{\frac{T^A}{\alpha \times 2^\kappa}} > 2\beta_Q^B - 1 = 2\beta_Q^A - 1.
\end{aligned}$$

If $\alpha_Q^A \leq \alpha_P^A$, then we have $\alpha = \alpha_Q^A$. Considering our proof based on a 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 computations, we can simplify the above inequality to

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

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

$$\begin{aligned}
&(\frac{2 \times 2^y}{3 - 2e^{-1} - \sqrt{5 - 4e^{-1}}})^{-1} \times \alpha_Q^A \\
&\leq \alpha_P^A < \frac{9T^A}{2^\kappa(2\beta_Q^A - 1)^2} \\
&< \frac{\alpha_Q^A(3 - 2e^{-1} - \sqrt{5 - 4e^{-1}})}{2^{y+1}}.
\end{aligned}$$

We can observe that the upper and lower bounds of $\alpha_P^A$ are the same. This fact implies that the inequalities can be reduced to $1 < 1$; thus, this case is also a contradiction. The above process indicates 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 the theorem is clearly proven. □

*Remark 3: We propose a 2.5-bit tighter security reduction than that of Theorem 8 in [2]. This can be interpreted as being six times more accurate in terms of an adversary's number of attack trials. We believe that this finding is by no means an insignificant improvement. This finding can provide a more reliable security measurement when implementing a security system in an imperfect and precision-restricted environment. We not only improve the tightness of a security reduction but also extend the possible ranges of the* $\lambda$ *value. Although Theorem 8 in [2] can be applied for* $\lambda$*, which satisfies* $\lambda \leq \frac{1}{4}$*, we extend its allowed range to* $\lambda \leq 0.44$*.*

Theorem 1 improves the approach in [1]. However, it still has significant limitations owing to its universal use because we can obtain the exact lower bound of the estimation value of the security level by applying Theorem 1 only when an efficient measure $\delta$ satisfies $\delta(P_\theta, Q_\theta) \leq 2^{-\frac{\kappa}{2}}$. In other words, we can only obtain inaccurate relative information about the security level by applying Theorem 1. There are many practical situations in which $\delta(P_\theta, Q_\theta)$ is much smaller or larger than $2^{-\frac{\kappa}{2}}$. We need more general criteria and methodologies that provide theoretical guidelines on how statistical differences affect the security level of cryptographic primitives. This motivation enables us to derive 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* $P_\theta$ *and* $Q_\theta$*, respectively. If* $S^P$ *is* $\kappa$*-bit secure and* $\delta(P_\theta, Q_\theta) \leq 2^{-\frac{f(\kappa)}{2}}$ *for some* $2^{-\frac{f(\kappa)}{2}}$*-efficient measure* $\delta$*, 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* $\kappa$ *is the security level of* $S^P$*.*

*Proof:* The overall flow of the proof is similar to that in Theorem 1. Considering an arbitrary adversary $A$, suppose that if $\frac{T_A}{\epsilon_A^P} \geq 2^\kappa$ is satisfied, then $\frac{T_A}{\epsilon_A^Q} < 2^{f(\kappa)-g(\kappa)}$ is also satisfied. Here, without a loss of generality, we assume that $g(\cdot)$ is a monotonically increasing function. We can suppose that this is because we are only interested in the value $g(\kappa)$, not the original form of the function $g(\cdot)$. Our purpose is to find $g(\kappa)$, which should be expressed by $\kappa$ and $f(\kappa)$. We then use the same notations a), b), c), d), and e) in the proof of Theorem 1.

Applying the probability preservation property and data processing inequality of $\Delta_{SD}$, 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 $E_i$ in which $(\theta_j, P_{\theta_j})_{j<i}$ and $(\theta_j', Q_{\theta_j'})_{j<i}$ take the same specific value, the adversary behaves identically in the two games up to the point at which it makes the $i$-th query. In particular, 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 is followed by sub-additivity for joint distributions such that

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

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

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

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

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

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

Meanwhile, considering the union bound, we can observe that $\epsilon_{A^n}^P \leq n \times \epsilon_A^P$. With 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 the following:

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

Note that if the inequality

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

holds, (2) becomes a contradiction. We want to find a sufficient condition to derive the contradiction in the proof to draw out the contradiction under the first assumption. Because we assume that $g(\cdot)$ is an increasing function, the left-hand side of (3) monotonically increases as $g(\kappa)$ increases. By contrast, for a fixed value $f(\kappa)$, the right-hand side of (3) monotonically decreases as $g(\kappa)$ increases. Thus, the left- and right-hand side equations meet at a single point. This inequality is reversed at that point. This implies that if we consider the equality in (3), we can have the most extreme case. By manipulating the equations, we can solve the equality equation in (3) as follows:

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

Thus we have

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

We can therefore 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. It is not difficult to show that the inequality $2\log_2(\sqrt{1+2^{f(\kappa)-\kappa+2}(1-e^{-1})}-1)-f(\kappa)+2\kappa-2 \leq \kappa$ is satisfied. This is because the following inequalities are satisfied:

$$\begin{aligned} & 2\log_2(\sqrt{1+2^{f(\kappa)-\kappa+2}(1-e^{-1})}-1)-f(\kappa)+2\kappa-2 \leq \kappa \\ & \Longleftrightarrow \log_2(\sqrt{1+2^{f(\kappa)-\kappa+2}(1-e^{-1})}-1) \leq \frac{f(\kappa)-\kappa+2}{2} \\ & \Longleftrightarrow \sqrt{1+2^{f(\kappa)-\kappa+2}(1-e^{-1})} \leq 2^{\frac{f(\kappa)-\kappa+2}{2}}+1 \\ & \Longleftrightarrow 1+2^{f(\kappa)-\kappa+2}-e^{-1}2^{f(\kappa)-\kappa+2} \\ & \leq \ \ 1+2^{f(\kappa)-\kappa+2}+2^{\frac{f(\kappa)-\kappa+4}{2}}. \end{aligned}$$

In addition, to maintain Theorem 3, the security level obtained should be non-negative. Thus, the condition $f(\kappa)-g(\kappa) \geq 0$ should be satisfied. This implies that the following inequalities are also satisfied:

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

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

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

for the theorem. Once this condition is satisfied, we can arbitrarily set $f(\kappa)$ to whatever value we want. The detailed application of Theorem 3 will be addressed in the following remark. Thus, we have completed the proof. □

*Remark 4: It is not difficult to show that Theorem 3 can be reduced to Theorem 1 when we substitute $f(\kappa)=\kappa$. It only requires some mathematical manipulations as follows:*

$$\begin{aligned} f(\kappa) \ \ = \ \ & \kappa \\ \Longrightarrow \ & \kappa-2+\log_2(\sqrt{1+4(1-e^{-1})}-1) \\ = \ \ & \kappa-\log_2\frac{2}{3-2e^{-1}-\sqrt{5-4e^{-1}}} \\ \approx \ \ & \kappa-2.374. \end{aligned}$$

*Table 1 indicates the guaranteed security level of $S^Q$ with respect to the security level parameter $\kappa$ and precision parameter $f(\kappa)$, which is obtained by applying Lemma 3 in [1] and Theorem 3. From Table 1, we can deduce the following. First, Theorem 3 provides additional (approximately) 2.5-bit security gains (particularly for $p > \frac{\kappa}{2}$, that is, $f(\kappa) > \kappa$) compared with Lemma 3 in [1]. Considering the case $f(\kappa) > \kappa$ in Table 1, we can conclude that only $(\kappa-3)$-bit security may be preserved if we apply Lemma 3 in [1]. By contrast, if we apply Theorem 3, we can conclude that almost all $\kappa$-bit securities may be preserved. Second, it should be noted that Lemma 3 in [1] cannot provide the exact lower bound of the security level of $S^Q$ for the case $f(\kappa) \neq \kappa$, and can only provide relatively inaccurate information. By contrast, Theorem 3 without exception provides the exact lower bound of the estimation value of the security level of $S^Q$ as long as $f(\kappa)$ satisfies the condition $f(\kappa) \geq -2\log_2(1-e^{-1}-2^{-\kappa})$. Theorem 3 deserves sufficient recognition for its contribution by simply removing the constraints imposed on precision in the previous study (in [1], the precision was fixed).*

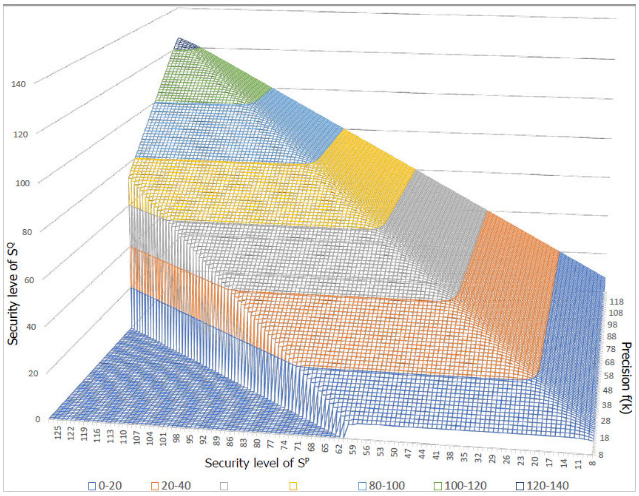

**FIGURE 1.** Security level of $S^Q$ with respect to $\kappa$ and $f(\kappa)$.

*Summarizing the discussion thus far, we can interpret Theorem 3 as follows: Through Theorem 3, we can estimate the effects on the security level when the original $\kappa$-bit secure scheme is implemented on the $\frac{f(\kappa)}{2}$-bit precision system. In a previous study [1], $f(\kappa)$ was fixed as $\kappa$, but Theorem 3 is generalized to make it possible for the security level $\kappa$ and precision $\frac{f(\kappa)}{2}$ to vary independently. Theorem 3 can provide a theoretical basis for how the security level of the 128-bit security scheme may change if it is implemented on a 32 or 64-bit precision system. Figure 1 shows a three-dimensional plot that indicates the security level of $S^Q$ determined by $\kappa$ and $f(\kappa)$.*

Until now, we have given tighter and more generalized versions of Micciancio and Walter's results, which were introduced in [1], [2]. However, Theorems 1, 2, 3, and Lemma 1 can only be applied with the $\lambda$-efficient measure $\delta$. There are several information-theoretic measures used to analyze security reduction. Among them, only the max-log distance $\Delta_{ML}$ and Kullback-Leibler divergence $\Delta_{KL}$ have been proven to be $\lambda$-efficient measures. As we already considered in Theorem 1, we can apply Theorems 1, 2, and 3 with

**TABLE 1.** **Guaranteed security level of $S^Q$ by applying Lemma 3 in [1] and Theorem 3.**

| | | $\kappa$ (Lemma 3 in [1]) | | | $\kappa$ (Theorem 3) | | |
|---|---|---|---|---|---|---|---|
| | | 104 | 116 | 128 | 104 | 116 | 128 |
| $f(\kappa)$ | 104 | 101 | ≥101 | ≥101 | 101.63 | 102.68 | 102.68 |
| | 116 | ≥101 | 113 | ≥113 | 103.31 | 113.63 | 114.68 |
| | 128 | ≥101 | ≥113 | 125 | 103.34 | 115.31 | 125.63 |

$\delta_{RE}$ from Lemma 6 in [1]. However, we cannot apply our theorems with $RD_\alpha$, $\Delta_{SD}$, and $HD$ directly. Thus, we have undertaken further research to obtain additional results for other measures. These results are given in the last three theorems. Theorem 4 deals with the infinity order of $RD$, which is well known to be closely related to $\Delta_{ML}$. Theorem 4 considers only the case in which the adversary is in a resource-restricted environment (such that the number of attack trials of an adversary is limited). Such a premise is not that impractical but is actually practically meaningful, for example, consider a situation in which an adversary should succeed within a limited time.

*Theorem (Application to an Adversary in a Resource Restricted Environment): Let $S^P$ and $S^Q$ be standard cryptographic schemes with black-box access to probability distribution ensembles $P_\theta$ and $Q_\theta$, respectively. Consider the adversary $A$, whose number of queries is upper bounded by $q$ (i.e., the attack resources of an adversary are restricted). If $S^P$ is $\kappa$-bit secure and $RD_\infty(Q_\theta||P_\theta) \le 1 + 2^{-p(\kappa)}$, then $S^Q$ is $(\kappa - \frac{q\times 2^{-p(\kappa)}}{\ln 2})$-bit secure. Here, $p(\kappa)$ should satisfy $p(\kappa) \ge -\log_2(\ln 2^\kappa) + \log_2 q$, where $\kappa$ is the security level of $S^P$.*

*Proof:* The notations are the same as the proofs of the previous theorems. From the definition and probability preservation properties of $RD_\infty$, we have

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

Subsequently, by applying the multiplicative property and data processing inequality of $RD_\infty$, we also have

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

Note that from the definition of the natural constant $e$, the following inequalities are satisfied:

$$\begin{aligned} RD_\infty(Q_\theta||P_\theta)^q &\le (1+2^{-p(\kappa)})^q \le e^{q\times 2^{-p(\kappa)}} \\ &= 2^{\log_2 e^{q\times 2^{-p(\kappa)}}}. \end{aligned}$$

From the given condition of Theorem 4, we know that $\frac{T_A}{\epsilon^P_A} \ge 2^\kappa$ is satisfied, and thus we have the following inequalities:

$$\begin{aligned} 2^{-\kappa} \ge \frac{\epsilon^P_A}{T_A} &\ge \frac{\epsilon^Q_A}{T_A}\frac{1}{RD_\infty(Q_\theta||P_\theta)^q} \ge \frac{\epsilon^Q_A}{T_A}\times 2^{-\log_2 e^{q\times 2^{-p(\kappa)}}} \\ &\iff 2^{-\kappa+\log_2 e^{q\times 2^{-p(\kappa)}}} \ge \frac{\epsilon^Q_A}{T_A} \\ &\iff \frac{T_A}{\epsilon^Q_A} \ge 2^{\kappa-\log_2 e^{q\times 2^{-p(\kappa)}}} \\ &\iff \log_2\left(\frac{T_A}{\epsilon^Q_A}\right) \ge \kappa - \log_2 e^{q\times 2^{-p(\kappa)}} \\ &= \kappa - \frac{q\times 2^{-p(\kappa)}}{\ln 2}. \end{aligned}$$

Therefore, we can conclude that $S^Q$ preserves at least $(\kappa - \frac{q\times 2^{-p(\kappa)}}{\ln 2})$-bit security. It is trivial that the inequality $\kappa - \frac{q\times 2^{-p(\kappa)}}{\ln 2} \le \kappa$ is satisfied. In addition, to ensure that Theorem 4 is meaningful, the security level obtained should be non-negative. Thus, the condition $\kappa - \log_2 e^{q\times 2^{-p(\kappa)}} \ge 0$ should be satisfied, and the following inequalities are satisfied:

$$\begin{aligned} \kappa - \log_2 e^{q\times 2^{-p(\kappa)}} &\ge 0 \\ &\iff \kappa \ge \log_2 e^{q\times 2^{-p(\kappa)}} \\ &\iff 2^\kappa \ge e^{q\times 2^{-p(\kappa)}} \\ &\iff p(\kappa) \ge -\log_2\left(\frac{\ln 2^\kappa}{q}\right) \\ &= -\log_2(\ln 2^\kappa) + \log_2 q. \end{aligned}$$

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

$$p(\kappa) \ge -\log_2(\ln 2^\kappa) + \log_2 q$$

for the theorem. Now, we complete the proof. □

*Remark 5: In Theorem 4, we derive the security reduction formula in terms of $RD_\infty$. In fact, it may be possible to derive a security reduction in terms of $RD_\infty$ as a corollary of the security reduction in terms of $\Delta_{ML}$ because $RD_\infty$ and $\Delta_{ML}$ are closely related. However, we found that eliciting an independent security reduction for $RD_\infty$ is also an interesting research topic. To the best of our knowledge, Theorem 4 is the first attempt to derive a security reduction in terms of $RD_\infty$. Some security arguments using RD were proposed in [5] but not for the case of $RD_\infty$. From the condition $p(\kappa) \ge -\log_2(\ln 2^\kappa) + \log_2 q$, which should be satisfied when applying Theorem 4, we can observe that if the number of queries of the adversary increases, $p(\kappa)$ should also increase (i.e.,* *the statistical similarity between $Q_\theta$ and $P_\theta$ should be closer) to achieve the same target security level. This fact fits well with our general intuition. Note that a Rényi divergence-based security analysis can provide significant gains when the number of queries of the adversary is restricted and the search problem is given.*

However, the most widely used information-theoretic measure to analyze the security reduction between two cryptographic schemes is the statistical distance $\Delta_{SD}$. It is important to estimate the extent to which $\Delta_{SD}$ values between two different probability distributions affects the security level. We can provide a theoretical guideline for the relationship between $\Delta_{SD}$ and security level in the following theorem.

*Theorem 4: Let $S^P$ and $S^Q$ be standard cryptographic schemes with black-box access to probability distribution ensembles $P_\theta$ and $Q_\theta$, respectively. If $S^P$ is $\kappa$-bit secure and $\Delta_{SD}(P_\theta, Q_\theta) \le 2^{-h(\kappa)}$, then $S^Q$ is $\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}}$-bit secure. Here, $h(\kappa)$ should satisfy $h(\kappa) \ge -\log_2(1-\frac{1}{2^\kappa})$, where $\kappa$ is the security level of $S^P$.*

*Proof:* The notations are the same as the proofs of the previous theorems. From the probability preservation property of $\Delta_{SD}$, we have

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

Then, by applying the additive property, data processing inequality, and $q \le T_A$, we can derive the following inequalities:

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

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

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

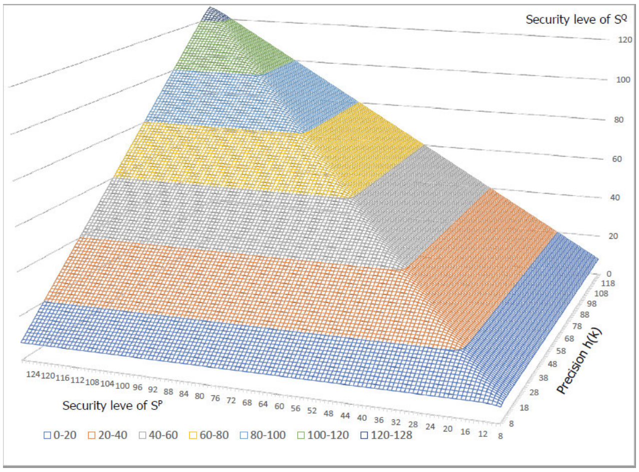

**FIGURE 2.** **Security level of $S^Q$ with respect to $\kappa$ and $h(\kappa)$.**

We can thus conclude that $S^Q$ preserves at least $\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}}$-bit security. It is trivial that the inequality $\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}} \le \kappa$ is satisfied. In addition, to maintain Theorem 5, the security level obtained should be non-negative. Thus the condition $\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}} \ge 0$ should be satisfied, and the following inequalities are satisfied:

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

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

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

for the theorem. Now, we complete the proof. □

*Remark 6: Theorem 5 proves several fundamental properties of $\Delta_{SD}$. First, Theorem 5 indicates that a $\kappa$-bit system implemented using a precision of p-bit closeness in $\Delta_{SD}$ guarantees only* $\min(\kappa, p)$ *bits of security. Second, Theorem 5 indicates that it is sufficient to select $Q_\theta$, which is close to $P_\theta$ within $2^{-\kappa}$ in $\Delta_{SD}$, to preserve the bit security. Moreover, to the best of our knowledge, Theorem 5 is the first attempt to provide a generalized security reduction with arbitrary precision in terms of $\Delta_{SD}$ in a complete form. Similar to Theorem 3, Theorem 5 can also be interpreted as follows: Theorem 5 can estimate the effects on the security level when the $\kappa$-bit secure original scheme is implemented on the $h(\kappa)$-bit precision system. Figure 2 shows a three-dimensional plot indicating the security level of $S^Q$ determined using $\kappa$ and $h(\kappa)$.*

From Theorem 5, we derive some corollaries. First, from Pinsker's inequality, for the relationship between $\Delta_{SD}$ and $\Delta_{KL}$, the following inequality is satisfied:

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

Using this formula, we can derive the following corollary:

*Corollary 1: If $S^P$ is $\kappa$-bit secure and $\Delta_{KL}(Q_\theta||P_\theta) \le 2^{1-2h(\kappa)}$, 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* $\kappa$ *is the security level of* $S^P$.

The above corollary can be easily derived from the fact that $\Delta_{KL}(Q_\theta||P_\theta) \leq 2^{1-2h(\kappa)}$ implies $\Delta_{SD}(P_\theta, Q_\theta) \leq 2^{-h(\kappa)}$ (refer to Pinsker's inequality).

In addition, in [1], the following relation was proved as

$$\Delta_{KL}(Q||P) \leq \frac{8}{9}\delta_{RE}(P, Q)^2.$$

From this formula, we can observe that $\delta_{RE}(P_\theta, Q_\theta) \leq \frac{3}{2\sqrt{2}}2^{\frac{1-2h(\kappa)}{2}}$ implies $\Delta_{KL}(Q_\theta||P_\theta) \leq 2^{1-2h(\kappa)}$. Therefore, we can derive the following corollary:

*Corollary 2: If* $S^P$ *is* $\kappa$*-bit secure and* $\delta_{RE}(P_\theta, Q_\theta) \leq \frac{3}{2\sqrt{2}}2^{\frac{1-2h(\kappa)}{2}}$, *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* $\kappa$ *is the security level of* $S^P$.

Finally, from Lemma 6 in [1], which provides the relation between $\Delta_{ML}$ and $\delta_{RE}$, note that $\Delta_{ML}(P_\theta, Q_\theta) \leq \ln(\frac{3}{2\sqrt{2}}2^{\frac{1-2h(\kappa)}{2}}+1)$ implies $\delta_{RE}(P_\theta, Q_\theta) \leq \frac{3}{2\sqrt{2}}2^{\frac{1-2h(\kappa)}{2}}$. Thus, we can derive the following corollary:

*Corollary 3: If* $S^P$ *is* $\kappa$*-bit secure and* $\Delta_{ML}(P_\theta, Q_\theta) \leq \ln(\frac{3}{2\sqrt{2}}2^{\frac{1-2h(\kappa)}{2}}+1)$, *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* $\kappa$ *is the security level of* $S^P$.

Yasunaga [12] recently revisited Micciancio and Walter's approaches [1], [2] by replacing $\lambda$-efficient measures with the Hellinger distance. They proposed a security reduction (i.e., Theorem 1 in [12]) that is mostly similar to Lemma 3 in [1]. The only difference is that the Hellinger distance was used and not the $\lambda$-efficient measures. Theorem 1 in [12] is meaningful because it derives a security reduction in terms of the Hellinger distance. However, similar to Lemma 3 in [1], Theorem 1 in [12] has significant limitations in terms of its universal use because we can obtain the exact lower bound of the estimation value of the security level by applying Theorem 1 in [12] only for precision $p = \frac{\kappa}{2}$ in terms of the Hellinger distance. We can only obtain inaccurate relative information about the security level for other cases by applying Theorem 1 in [12]. We successfully derive the generalized version of Theorem 1 in [12] based on this motivation, thereby addressing the existing limitations. The result can be found in the following theorem.

*Theorem 6 (Generalization of Theorem 1 in [12]): Let* $P = (P_i)_i$ *and* $Q = (Q_i)_i$ *be probability distribution ensembles over the same support* $\prod_i \Omega_i$. *In addition, let* $S^P$ *be a primitive for which an n-bit security game* $G^P_{S,A}$ *is defined for* $n > 1$ *(i.e., search primitives). If* $S^P$ *is* $\kappa$*-bit secure and* $HD(P_i|a_i, Q_i|a_i) \leq 2^{-\frac{w(\kappa)}{2}}$ *for any i and* $a_i \in \prod_{j<i}\Omega_j$, *then* $S^Q$ *is* $(\kappa - \log_2 B)$*-bit secure, where* $B = \frac{1}{1-e^{-1}} + \frac{2^{-w(\kappa)+\kappa}}{(1-e^{-1})^2} + \frac{\sqrt{2}\times 2^{-w(\kappa)+\kappa}}{1-e^{-1}}\sqrt{\frac{2^{w(\kappa)-\kappa}}{1-e^{-1}} + \frac{1}{2(1-e^{-1})^2}}$ *and* $w(\kappa)$ *should satisfy* $w(\kappa) \geq \max\{-\log_2(\frac{\epsilon^Q_A}{T_A}2(1-e^{-1})^2), -\log_2(\frac{(1-e^{-1})^2}{2} + 2^{-2\kappa-1} - (1-e^{-1})2^{-\kappa})\}$.

*Proof:* The overall flow of the proof is similar to that of Theorem 1 in [12], and most notations are the same as the proofs of the previous theorems. Because $S^P$ is $\kappa$-bit secure, it holds that $\frac{\epsilon^P_A}{T_A} \leq 2^{-\kappa}$ for any adversary $A$. In conclusion, it is sufficient to show that $\frac{\epsilon^Q_A}{T_A} \leq 2^{-(\kappa-\log_2 B)}$ is satisfied. We consider $l$ independent plays of $G^P_{S,A}$ and define $\epsilon^P_{A^l}$ as the probability that $A$ succeeds in at least one of $l$ plays of $G^P_{S,A}$. In other words, $\epsilon^P_{A^l} = 1-(1-\epsilon^P_A)^l$, and we define $\epsilon^Q_{A^l}$ analogously. Because the number of queries to the distribution ensemble is at most $T_A$ during each play, it holds that

$$|\epsilon^P_{A^l} - \epsilon^Q_{A^l}| \leq \Delta_{SD}(P^l, Q^l) \leq \sqrt{2lT_A}2^{-\frac{w(\kappa)}{2}},$$

where $P^l$ (respectively, $Q^l$) is the $l$-fold product of $P$ (respectively, $Q$), the first inequality is from the data processing inequality, and the second inequality follows from Lemma 1 in [12]. From the definition of $\epsilon^P_{A^l}$ and $\epsilon^Q_{A^l}$, the following inequality is satisfied:

$$(1-\epsilon^P_A)^l \leq \sqrt{2lT_A}2^{-\frac{w(\kappa)}{2}} + (1-\epsilon^Q_A)^l.$$

Based on the fact that $(1-x)^l \geq 1-lx$ for $x \in [0, 1]$ and setting $l = \frac{1}{\epsilon^Q_A}$, it holds that

$$\begin{aligned}1-\frac{\epsilon^P_A}{\epsilon^Q_A} &\leq \sqrt{\frac{2T_A2^{-w(\kappa)}}{\epsilon^Q_A}} + (1-\epsilon^Q_A)^{\frac{1}{\epsilon^Q_A}}\\ &< \sqrt{\frac{2T_A2^{-w(\kappa)}}{\epsilon^Q_A}} + e^{-1},\end{aligned}$$

where we use the relation $(1-\frac{1}{x})^x < e^{-1}$ for $x > 0$. By rewriting the inequality, we obtain

$$(\sqrt{\epsilon^Q_A} - \frac{\sqrt{T_A2^{-w(\kappa)}}}{\sqrt{2}(1-e^{-1})})^2 < \frac{\epsilon^P_A}{1-e^{-1}} + \frac{T_A2^{-w(\kappa)}}{2(1-e^{-1})^2}.$$

For sufficiently large $w(\kappa)$, (i.e., for $w(\kappa) \geq -\log_2(\frac{\epsilon^Q_A}{T_A}2(1-e^{-1})^2)$), it holds that

$$\sqrt{\epsilon^Q_A} < \sqrt{\frac{\epsilon^P_A}{1-e^{-1}} + \frac{T_A2^{-w(\kappa)}}{2(1-e^{-1})^2}} + \frac{\sqrt{T_A2^{-w(\kappa)}}}{\sqrt{2}(1-e^{-1})}.$$

Squaring both sides yields the following inequality:

$$\begin{aligned}\frac{\epsilon^Q_A}{T_A} < \; &\frac{\epsilon^P_A}{(1-e^{-1})T_A} + \frac{2^{-w(\kappa)}}{(1-e^{-1})^2}\\ &+ \frac{\sqrt{2}\times 2^{-\frac{w(\kappa)}{2}}}{1-e^{-1}}\sqrt{\frac{\epsilon^P_A}{(1-e^{-1})T_A} + \frac{2^{-w(\kappa)}}{2(1-e^{-1})^2}}.\end{aligned}$$

Because $\frac{\epsilon^P_A}{T_A} \leq 2^{-\kappa}$ is satisfied, we have

$$\begin{aligned}\frac{\epsilon^Q_A}{T_A} < \; &2^{-\kappa}(\frac{1}{1-e^{-1}} + \frac{2^{-w(\kappa)+\kappa}}{(1-e^{-1})^2}\\ &+ \frac{\sqrt{2}\times 2^{-w(\kappa)+\kappa}}{1-e^{-1}}\sqrt{\frac{2^{w(\kappa)-\kappa}}{1-e^{-1}} + \frac{1}{2(1-e^{-1})^2}})\\ &= 2^{-\kappa}B = 2^{-(\kappa-\log_2 B)}.\end{aligned}$$

**TABLE 2.** Guaranteed security level of $S^Q$ by applying Theorem 1 in [12] and Theorem 6.

| | | $\kappa$<br>(Theorem 1 in [12]) | | | $\kappa$<br>(Theorem 6) | | |
|---|---|---|---|---|---|---|---|
| | | 104 | 116 | 128 | 104 | 116 | 128 |
| $w(\kappa)$ | 104 | 101 | $\geq$101 | $\geq$101 | $\approx$101 | 101.67 | 101.67 |
| | 116 | $\geq$101 | 113 | $\geq$113 | 103.29 | $\approx$113 | 113.67 |
| | 128 | $\geq$101 | $\geq$113 | 125 | 103.33 | 115.29 | $\approx$125 |

We can thus conclude that $S^Q$ preserves at least $(\kappa - \log_2 B)$-bit security. It is trivial that the inequality $\kappa - \log_2 B \leq \kappa$ is satisfied. In addition, to maintain Theorem 6, the security level obtained should be non-negative. Thus the condition $\kappa - \log_2 B \geq 0$ should be satisfied, and the following inequalities are satisfied:

$$\begin{aligned}\kappa - \log_2 B &\geq 0\\ &\iff 2^\kappa \geq B\\ &\iff 2^{2\kappa} + \frac{1}{(1-e^{-1})^2} - \frac{2^{\kappa+1}}{1-e^{-1}}\\ &\quad - \frac{2 \times 2^{-w(\kappa)+2\kappa}}{(1-e^{-1})^2} \geq 0\\ &\iff w(\kappa) \geq -\log_2(\frac{(1-e^{-1})^2}{2} + 2^{-2\kappa-1}\\ &\quad - (1-e^{-1})2^{-\kappa}).\end{aligned}$$

Thus, for the theorem, we can conclude that $w(\kappa)$ should satisfy the condition

$$\begin{aligned}w(\kappa) \geq \max\{&-\log_2(\frac{\epsilon_A^Q}{T_A}2(1-e^{-1})^2),\\ &-\log_2(\frac{(1-e^{-1})^2}{2} + 2^{-2\kappa-1} - (1-e^{-1})2^{-\kappa})\}\end{aligned}$$

Now, we finish the proof. □

*Remark 7: Table 2 indicates the guaranteed security level of $S^Q$ with respect to the security level parameter $\kappa$ and precision parameter $w(\kappa)$, which are obtained by applying Theorem 1 in [12] and Theorem 6, respectively. From Table 2, we can deduce the following facts. First, Theorem 6 provides additional (approximately) 2.5-bit security gains (particularly for the cases $p > \frac{\kappa}{2}$, i.e., $w(\kappa) > \kappa$) in comparison with Theorem 1 in [12]. Considering the case $w(\kappa) > \kappa$ in Table 2, we can conclude that only $(\kappa - 3)$-bit security may be preserved if we apply Theorem 1 in [12]. By contrast, if we apply Theorem 6, we can conclude that almost all $\kappa$-bit security may be preserved. Second, it should be noted that Theorem 1 in [12] cannot provide the exact lower bound value of the security level of $S^Q$ for the case $w(\kappa) \neq \kappa$, and can only provide relatively inaccurate information. By contrast, Theorem 6 always provides the exact lower bound of the estimation value of the security level of $S^Q$ as long as $w(\kappa)$ satisfies the following condition*:

$$\begin{aligned}w(\kappa) \geq \max\{&-\log_2(\frac{\epsilon_A^Q}{T_A}2(1-e^{-1})^2),\\ &-\log_2(\frac{(1-e^{-1})^2}{2} + 2^{-2\kappa-1} - (1-e^{-1})2^{-\kappa})\}.\end{aligned}$$

*Theorem 6 deserves sufficient recognition for its contribution by removing the constraints imposed on the precision in the previous study [12].*

*Summarizing the discussion thus far, we can interpret Theorem 6 as follows: Through Theorem 6, we can estimate the effects on the security level when the $\kappa$-bit secure original scheme is implemented on a $\frac{w(\kappa)}{2}$-bit precision system. In a previous study [12], $w(\kappa)$ was fixed as $\kappa$, but Theorem 6 was generalized to make it possible for security level $\kappa$ and precision $\frac{w(\kappa)}{2}$ to vary independently. Through Theorem 6, we can provide a theoretical basis for how the security level of the 128-bit security scheme may change if it is implemented on a 32 or 64-bit precision system.*

## IV. CONCLUSION 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 provided diverse types of security reduction formulas for six types of information-theoretic measures: $\Delta_{SD}$, $RD_\infty$, $\delta_{KL}$, $\Delta_{ML}$, $\delta_{RE}$, and $HD$. In addition, we proposed tighter and more generalized versions of security reductions compared with previous studies [1], [2], [12]. These reduction results are expected to provide an information-theoretic methodology to estimate the security loss under such situations as a replacement with different probability distributions.

In a future study, we intend to conduct further research to prove or disprove whether the proposed quantitative security reduction results achieve information-theoretic limits (particularly for those that are given in terms of the max-log and Hellinger distances). We hope to answer the question, "Is a tighter reduction than those proposed ones (particularly in Theorems 2, 3, and 6) theoretically possible?" The second research topic will be a further generalization of Theorem 4. To date, Theorem 4 has only been able to deal with constrained adversaries and can even be applied to only *RD* of an infinity order. We want to generalize Theorem 4 to cover arbitrary (unbounded) adversaries and arbitrary orders. This task requires entirely new derivation strategies, which may be interesting topics for future research.

## REFERENCES

[1] D. Micciancio and M. Walter, "Gaussian sampling over the integers: Efficient, generic, constant-time," in *Advances in Cryptology—CRYPTO 2017* (Lecture Notes in Computer Science), vol. 10402, J. Katz and H. Shacham, Eds. Springer, Aug. 2017, pp. 455–485.

[2] D. Micciancio and M. Walter, ''On the bit security of cryptographic primitives,'' in *Advances in Cryptology—EUROCRYPT 2018* (Lecture Notes in Computer Science), vol. 10820, J. B. Nielsen and V. Rijmen, Eds. Springer, May 2018, pp. 3–28.

[3] M. Walter, ''Sampling the integers with low relative error,'' in *Progress in Cryptology—AFRICACRYPT 2019* (Lecture Notes in Computer Science), vol. 11627. Springer, 2019, pp. 157–180.

[4] S. Bai, A. Langlois, T. Lepoint, D. Stehle, and R. Steinfeld, ''Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance,'' in *Advances in Cryptology—ASIACRYPT 2015* (Lecture Notes in Computer Science), vol. 9452, T. Iwata and J. H. Cheon, Eds. Springer, Dec. 2015, pp. 3–24.

[5] T. Prest, ''Sharper bounds in lattice-based cryptography using the Rényi divergence,'' in *Advances in Cryptology—ASIACRYPT 2017* (Lecture Notes in Computer Science), vol. 10624, T. Takagi and T. Peyrin, Eds. Springer, Dec. 2017, pp. 347–374.

[6] Y. Gao and K. Wang, ''Probability preservation property in the security reduction,'' in *Proc. 8th Int. Congr. Inf. Commun. Technol.*, May 2018, vol. 131, pp. 665–675.

[7] K. Takashima and A. Takayasu, ''Tighter security for efficient lattice cryptography via Rényi divergence of optimized orders,'' in *Proc. Int. Conf. Provable Secur.*, 2015, pp. 412–431.

[8] T. Matsuda, K. Takashashi, and T. Murakami, ''Improved security evaluation techniques for imperfect randomness from arbitrary distributions,'' in *Proc. 22nd Int. Conf. Pract. Theory Public Key Cryptogr.*, 2019, pp. 549–580.

[9] N. Genise and D. Micciancio, ''Faster Gaussian sampling for trapdoor lattices with arbitrary modulus,'' in *Advances in Cryptology—EUROCRYPT 2018* (Lecture Notes in Computer Science), vol. 10820. Springer, 2018, pp. 174–203.

[10] Y. Dodis and Y. Yu, ''Overcoming weak expectations,'' in *Proc. 10th Theory Cryptogr. Conf., (TCC)*, vol. 7785. Tokyo, Japan, Mar. 2013, pp. 1–22.

[11] M. Backes, A. Kate, S. Meiser, and T. Ruffing, ''Secrecy without perfect randomness: Cryptography with (bounded) weak sources,'' in *Applied Cryptography and Network Security (ACNS)* (Lecture Notes in Computer Science), vol. 9092. Springer, 2015, pp. 675–695.

[12] K. Yasunaga, ''Replacing probability distributions in security games via Hellinger distance,'' Cryptol. ePrint Arch. Tech. Rep., 2021/110, 2021.

[13] Z. Zheng, X. Wang, G. Xu, and C. Zhao, ''Error estimation of practical convolution discrete Gaussian sampling with rejection sampling,'' *Sci. China Inf. Sci.*, vol. 64, no. 3, pp. 1–3, Mar. 2021.

[14] Y. Gao and K. Wang, ''Probability preservation property with relative error and its applications,'' in *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy*, 2018, pp. 461–468.

**DONG-HOON LEE** (Graduate Student Member, IEEE) received the B.S. degree in electronic and computer science engineering from Hanyang University, Seoul, South Korea, in 2017. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Seoul National University, Seoul. His current research interests include lattice-based cryptography and error-correcting codes.

**YOUNG-SIK KIM** (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from Seoul National University, in 2001, 2003, and 2007, respectively. He joined the Semiconductor Division, Samsung Electronics, where he performed the research and development of security hardware IPs for various embedded systems, including modular exponentiation hardware accelerator (called Tornado 2MX2) for RSA and elliptic curve cryptography in smart card products and mobile application processors of Samsung Electronics, until 2010. He is currently a Professor with Chosun University, Gwangju, South Korea. He is also a Submitter of two candidate algorithms (McNie and pqsigRM) in the first round for the NIST Post Quantum Cryptography Standardization. His research interests include post-quantum cryptography, the IoT security, physical layer security, data hiding, channel coding, and signal design. He was selected as one of the 2025's 100 Best Technology Leaders (for Crypto-Systems) by the National Academy of Engineering of Korea, in November 2017.

**JONG-SEON NO** (Fellow, IEEE) received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, South Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1988. He was a Senior MTS with Hughes Network Systems, from 1988 to 1990. He was an Associate Professor with the Department of Electronic Engineering, Konkuk University, Seoul, from 1990 to 1999. He joined the Faculty of the Department of Electrical and Computer Engineering, Seoul National University, in 1999, where he is currently a Professor. His area of research interests include error-correcting codes, cryptography, sequences, LDPC codes, interference alignment, and wireless communication systems. He became a fellow of IEEE through the IEEE Information Theory Society, in 2012. He became a member of the National Academy of Engineering of Korea (NAEK), in 2015, where he served as the Division Chair for electrical, electronic, and information engineering, from 2019 to 2020. He was a recipient of the IEEE Information Theory Society Chapter of the Year Award, in 2007. From 1996 to 2008, he has served as the Founding Chair for the Seoul Chapter of the IEEE Information Theory Society. He was the General Chair of Sequence and Their Applications 2004 (SETA2004), Seoul. He has served as the General Co-Chair for the International Symposium on Information Theory and its Applications 2006 (ISITA2006) and the International Symposium on Information Theory 2009 (ISIT2009), Seoul. He has served as the Co-Editor-in-Chief for the IEEE JOURNAL OF COMMUNICATIONS AND NETWORKS, from 2012 to 2013.