Bit Security as Computational Cost for Winning Games with High Probability

Shun Watanabe[1] and Kenji Yasunaga[2]

[1] Tokyo University of Agriculture and Technology, Japan shunwata@cc.tuat.ac.jp
[2] Osaka University, Japan yasunaga@ist.osaka-u.ac.jp

Abstract. We introduce a novel framework for quantifying the bit security of security games. Our notion is defined with an operational meaning that a λ-bit secure game requires a total computational cost of 2^λ for winning the game with high probability, e.g., 0.99. We define the bit security both for search-type and decision-type games. Since we identify that these two types of games should be structurally different, we treat them differently but define the bit security using the unified framework to guarantee the same operational interpretation. The key novelty of our notion of bit security is to employ two types of adversaries: inner adversary and outer adversary. While the inner adversary plays a "usual" security game, the outer adversary invokes the inner adversary many times to amplify the winning probability for the security game. We find from our framework that the bit security for decision games can be characterized by the information measure called the *Rényi divergence* of order 1/2 of the inner adversary. The conventional "advantage," defined as the probability of winning the game, characterizes our bit security for search-type games. We present several security reductions in our framework for justifying our notion of bit security. Many of our results quantitatively match the results for the bit security notion proposed by Micciancio and Walter in 2018. In this sense, our bit security strengthens the previous notion of bit security by adding an operational meaning. A difference from their work is that, in our framework, the Goldreich-Levin theorem gives an optimal reduction only for "balanced" adversaries who output binary values in a balanced manner.

Keywords: Bit Security · Rényi Divergence · Goldreich-Levin Theorem.

1 Introduction

The security levels of cryptographic primitives are usually measured by the attacker's cost for breaking them. We say a primitive P has λ-bit security if the attacker needs to perform 2^λ operations to break it. The idea behind the notion is that an ideal scheme should be secure as if the only effective attack is the brute-force search of the λ-bit secret key. The attacker can find the key by checking each candidate roughly 2^λ times or randomly guessing a key, which is correct with probability $2^{-\lambda}$. In either way, the attacker needs a computational cost of roughly 2^λ operations to find the correct key. There is a trade-off between the computational cost T and the success probability ϵ for finding the key. Thus, a λ-bit secure primitive should satisfy the relation $T/\epsilon \geq 2^\lambda$ for any attacks. The quantity $\log_2(T/\epsilon)$ has been used to give an upper bound on bit security.

The above notion of bit security only captures *search* primitives such as one-way functions and signature schemes, where the attacker tries to find the correct answer from a wide range of the solution space. We also have another type of primitives, called *decision* primitives, such as pseudorandom generators and encryption schemes, where the attacker tries to distinguish two possible cases. Since the quantity of $\log_2(T/\epsilon)$ has an operational meaning only for search-type games, the corresponding notion for decision primitives has not been established.

Micciancio and Walter [19] introduced a unified framework for measuring bit security that captures both search and decision primitives. They discussed the validity of their definition by giving several results, including the tightness of the Goldreich-Levin hard-core predicate and a simple reduction of one-wayness of pseudorandom generators. Results obtained under their framework are compatible with what has been believed in the cryptography community. Notably, their bit security definition reflects the folklore (cf. [16]), claiming that the bit security of decision games is reciprocal of the "square" of the advantage. In the framework of [19], they consider a security game in which an attacker is allowed to output a failure symbol $\perp$; the advantage of the attacker is defined as the ratio between the mutual information and the Shannon entropy of random variables induced by the security game. However, these concepts seem to be introduced without satisfactory explanation. The security of cryptographic primitives cannot be verified by experiments, unlike physics. Thus, the compatibility of the results is not sufficient enough to justify the notion. It is desirable to build a security definition that has a firm operational meaning.

In this work, we revisit a theoretical treatment of bit security and introduce a new notion of bit security with an operational meaning. Specifically, we define *bit security* as the computational cost for winning the security game with high probability. We apply the same interpretation to both search and decision primitives but distinguish them since they should be structurally different. Below we explain the underlying idea of our framework of bit security.

In cryptography, the security of a primitive is usually defined through the security game. The game is played by an attacker and defines the success probability ϵ of the attacker. For example, in the security of one-way function f, an attacker is given $f(x)$ for random x and tries to output x' satisfying $f(x) = f(x')$. When the success probability is at most ϵ for any attackers with computational cost at most T, we say that f is (T, ϵ)-secure one-way function. Assume there is an attacker A that, given $f(x)$, can output x' with $f(x) = f(x')$ with computational cost T and success probability ϵ. What can we say about the cost of breaking the one-wayness? Suppose we run A in total N times, where A receives an independently generated challenge $f(x_i)$ for the ith time. The total cost is NT, and the success probability for finding a pair $(f(x_i), x'_i)$ satisfying $f(x'_i) = f(x_i)$ can be increased to roughly $N\epsilon$. Thus, it suffices to run A about $1/\epsilon$ times to break one-wayness with high probability. The total cost of T/ϵ corresponds with the quantity described above. Hence, if f is a λ-bit secure one-way function, it must satisfy $T/\epsilon \geq 2^\lambda$ for any attackers.

The above formulation of bit security can be adopted for other search primitives. The success probability for those primitives is designed to be sufficiently small, and it may be increased by running the base attacker repeatedly. For *decision* primitives, the success probability of an attacker is designed to be close to 1/2. In a security game of a pseudorandom generator $g : \{0,1\}^\ell \to \{0,1\}^m$, an attacker tries to distinguish whether a given bit string y is from an output $g(x)$ for random $x \in \{0,1\}^\ell$ or a random sampling from $\{0,1\}^m$. A game is such that, after choosing a bit $u \in \{0,1\}$ randomly, the attacker obtains $y = g(x)$ if $u = 0$, and random $y \in \{0,1\}^m$ if $u = 1$, and finally outputs $u' \in \{0,1\}$ as a guess. The attack succeeds if $u' = u$. We usually require that, for any attacker with cost T, the success probability ϵ is bounded by $\epsilon \leq 1/2 + \delta$ for small $\delta \geq 0$.

Although the success probability for decision primitives should be close to 1/2, it can be amplified by running the base attacker repeatedly and making the final decision from the output sequence. Thus, bit security can be defined similarly as the computational cost for winning the security game with high probability. Note that there is a structural difference between games for search and decision primitives. For search primitives, an attacker receives independently generated challenges in repeated games and wins the game if it finds any successful solution. For decision primitives, an attacker needs to determine the secret bit u, which is consistent in every repeated game.

1.1 Our Contribution

We define a notion of bit security based on the above idea. Specifically, we define a game in which two types of adversaries exist. The first adversary A, called an *inner* adversary, is an attacker for the "usual" security game. The second adversary B, called an *outer* adversary, invokes A certain times to amplify the final success probability $\epsilon_{A,B}$. The bit security is defined as (the logarithm base 2 of) the computational cost of (A, B) necessary for achieving $\epsilon_{A,B} \geq 0.99$.

The condition for success differs depending on the types of games. For decision games, the inner adversary A tries to distinguish two cases whether the secret bit u equals 0 or 1. The outer adversary also tries to distinguish the two cases by observing answers from A sufficiently many times. The success condition of (A, B) is that B outputs b with $b = u$. For search games, where a secret u is chosen from $\{0,1\}^n$ for $n > 1$, at the ith invocation of A by B, the challenge x_i is generated independently and sent to A. The pair (A, B) succeeds if at least one invocation of A could find the correct answer of the underlying security game. Thus, as long as A chooses a value from a finite solution space, the bit security takes a finite value in search games.

Suppose an adversary A runs in time T_A and achieves the success probability ϵ_A for some security game. For the search game, the advantage of A is usually defined to be $\mathsf{adv}^{\mathrm{srch}} = \epsilon_A$. Our bit security is roughly given by $\log_2 T_A + \log_2(1/\mathsf{adv}^{\mathrm{srch}}) + O(1)$. This is compatible with the well-accepted quantification of bit security in the literature.

On the other hand, for the decision game, the advantage of A is usually defined to be $\mathsf{adv}^{\mathrm{decn}} = 2\epsilon_A - 1$. Our main message of this paper is that the usual notion of advantage $\mathsf{adv}^{\mathrm{decn}}$ is useful only for a certain class of adversaries. More specifically, we introduce a class of adversaries that output in a "balanced" manner, referred to as β-balanced adversaries. For instance, the linear test of pseudorandom generators is β-balanced for $\beta = 1/2$ since it outputs 0 and 1 with equal probability when the instance is from a true random generator. For that class of adversary, we show that our bit security is roughly given by $\log_2 T_A + 2\log_2(1/\mathsf{adv}^{\mathrm{decn}}) + O(1)$. Thus, it is compatible with the folklore (cf. [16]) that the bit security of decision games is reciprocal of the square of the advantage. However, for general adversaries, we demonstrate that the bit security is characterized by the *Rényi advantage* $\mathsf{adv}_A^{\mathrm{Renyi}} = D_{1/2}(A_0 \| A_1)$, where $D_{1/2}$ is the Rényi divergence of order $1/2$ and A_u is the random variable of the output of A under the condition that u is the secret bit. This new notion of advantage is closely tied to the optimal exponential convergence of the error probability in the Bayesian hypothesis testing [5, Section 11.9]. Using the Rényi advantage, we show that our bit security is roughly given by $\log_2 T_A + \log_2(1/\mathsf{adv}_A^{\mathrm{Renyi}}) + O(1)$.

When we consider a security reduction of a decision game to the corresponding search game, it turns out that the use of the Rényi advantage instead of the advantage $\mathsf{adv}^{\mathrm{decn}}$ is crucial. As a concrete example, let us consider the case of proving that a λ-bit secure pseudorandom generator (PRG) implies a λ-bit secure one-way function (OWF). Suppose that there is an inner adversary A for the OWF with success probability ϵ_A. Then, using this adversary A, we can build an inner adversary A' for the PRG; this adversary A' outputs 0 only when A succeeds in inverting the OWF and thus is extremely biased. For such a biased adversary, it turns out that the Rényi advantage $\mathsf{adv}_A^{\mathrm{Renyi}}$ and the advantage $\mathsf{adv}^{\mathrm{decn}}$ are both $\Omega(\epsilon_A)$. Then, our estimate of the bit security using the Rényi advantage provides that the bit security of the PRG is upper bounded by $\log_2 T_A + \log_2(1/\epsilon_A) + O(1)$, which proves the desired contradiction. However, using the advantage $\mathsf{adv}^{\mathrm{decn}}$, the bit security of the PRG is only upper bounded by $\log_2 T_A + 2\log_2(1/\epsilon_A) + O(1)$, which does not prove the desired contradiction.

Using our framework, in addition to the above example of the PRG to the OWF, we present several other security reductions. For the distribution approximation problem (a.k.a. approximate samplers), we show that the approximation precision for preserving the bit security is essentially the same for search and decision primitives as long as the distributions are close enough in the *Hellinger distance*. It solves another peculiar problem raised in [19] that decision primitives may require more precise approximation than search primitives. Regarding the Goldreich-Levin hard-core predicate [10, 9], we observe that their reduction is tight as long as we consider β-balanced attackers for the hard-core predicate. Concretely, if a one-way function $f : \{0,1\}^n \to \{0,1\}^m$ is λ-bit secure, then the inner product function $\sum_i x_i \cdot r_i \bmod 2$ is a $(\lambda - O(\log_2 n))$-bit secure hard-core predicate for function $g(x,r) = (f(x), r)$ against adversaries A satisfying $\min_x \Pr[A = x] = \Omega(1)$. We observe that the well-known reduction from the Computational Diffie-Hellman (CDH) problem to the Decisional Diffie-Hellman

(DDH) problem shows that if the DDH problem has λ-bit security, then the corresponding CDH problem has $(\lambda - O(1))$-bit security. Although the DDH assumption is stronger than the CDH assumption, our result implies that the DDH problem may not necessarily have quantitatively higher bit security. In addition, we give a quantitative relationship between the IND-CPA security and the one-wayness of encryption schemes. We show that if an encryption scheme is λ-bit secure IND-CPA and the message space is of size 2^{λ}, it has $(\lambda - O(1))$-bit secure one-wayness. Finally, we show that a hybrid argument for distinguishing distributions can be generally applied in our framework.

1.2 Related Work

Our study is inspired by the bit security framework introduced by Micciancio and Walter [19]. They first defined the advantage of adversary A using the mutual information and the Shannon entropy. Then, they observed that their advantage could be approximated by $\mathsf{adv}^{\mathrm{srch}}_{\mathrm{MW}} = \alpha\beta$ for search games and $\mathsf{adv}^{\mathrm{decn}}_{\mathrm{MW}} = \alpha(2\beta - 1)^2$ for decision games, where α is the probability that A outputs values other than $\perp$ and β is the conditional probability that A succeeds in the game under the condition that A outputs values other than $\perp$. Their bit security is defined as $\min_A \log_2(T_A/\mathsf{adv}_{\mathrm{MW}})$, where T_A is the measure of resources of A. Their notion could solve peculiar problems in PRG and approximate samplers. However, it is not easy to understand the quantitative meaning of their bit security. Since the notion of bit security was introduced to offer an easy-to-understand simple metric, our new notion of bit security would be more appealing. In our framework, if a security game has λ-bit security, the game requires a total computational cost of 2^{λ} to win the game with high probability.

In [26], the closeness in Hellinger distance was used for the distribution approximation problem in the bit security framework of [19]. Although we have not found concrete relations between the frameworks of [19] and ours, the Hellinger distance plays a key role in both frameworks for the distribution approximation problem.

The Rényi divergence has been used in various problems in the information theory; see [25, 23] and references therein. Since the Rényi divergence can be regarded as a proxy of distance, it has been used as a security metric on encryption [12], an approximation metric in lattice cryptography [15, 2, 24, 4, 22], differential privacy [20], and security analysis [14, 17]. Our usage of the Rényi divergence is different from these cryptographic applications in the sense that the Rényi divergence naturally arises as a characterization of the operationally defined bit-security via the Bayesian hypothesis testing.

2 Preliminaries

We present several basic notions and their properties about probability distributions. Let P and Q be probability distributions over a finite set Ω. For a distribution P over Ω and $A \subseteq \Omega$, we denote by $P(A)$ the probability of event A, which is equal to $\sum_{x \in A} P(x)$.

The *total variation distance* between P and Q is

$$d_{\mathsf{TV}}(P,Q) = \max_{A \subseteq \Omega} |P(A) - Q(A)| = \frac{1}{2} \sum_{x \in \Omega} |P(x) - Q(x)|.$$

The *Hellinger distance* between P and Q is

$$d_{\mathsf{HD}}(P,Q) = \sqrt{\frac{1}{2} \sum_{x \in \Omega} \left(\sqrt{P(x)} - \sqrt{Q(x)} \right)^2} = \sqrt{1 - \sum_{x \in \Omega} \sqrt{P(x) \cdot Q(x)}},$$

which takes values in $[0,1]$. It holds that

$$d_{\mathsf{HD}}(P,Q)^2 \leq d_{\mathsf{TV}}(P,Q) \leq \sqrt{2} \cdot d_{\mathsf{HD}}(P,Q). \tag{1}$$

The Rényi divergence of order $1/2$ is

$$D_{1/2}(P \| Q) = -2 \ln \sum_{x \in \Omega} \sqrt{P(x)Q(x)}.$$

It holds that $1 - 1/t \leq \ln t \leq t - 1 \text{ for } t > 0$. By using this inequality, we have that

$$d_{\mathsf{HD}}(P,Q)^2 \leq \frac{1}{2} \cdot D_{1/2}(P \| Q) \leq \frac{d_{\mathsf{HD}}(P,Q)^2}{1 - d_{\mathsf{HD}}(P,Q)^2} \leq 2 \cdot d_{\mathsf{HD}}(P,Q)^2, \tag{2}$$

where the last inequality holds if $d_{\mathsf{HD}}(P,Q)^2 \leq 1/2$. Thus, if $D_{1/2}(P \| Q) \geq x$, we have

$$d_{\mathsf{HD}}(P,Q)^2 \geq \min \left\{ \frac{1}{2}, \frac{x}{2} \right\}. \tag{3}$$

3 Bit Security

Based on the idea described in Section 1, we introduce our framework of bit security. Section 3.1 provides a formal definition. Section 3.2 presents upper and lower bounds on the bit security, which will be used for security reductions.

3.1 Definition

We define an n-bit security game $G_{A,B} = (X, R, \{O_\theta\}_\theta)$ consisting of an algorithm X, a Boolean function R, and oracles $\{O_\theta\}_\theta$, played by an *inner* adversary A and an *outer* adversary B. The inner adversary A plays a usual security game. First, a secret $u \in \{0,1\}^n$ is chosen uniformly at random, and the challenge x is computed as $X(u)$. Given x, A tries to output a such that $R(u,x,a) = 1$ using oracle access to $\{O_\theta\}_\theta$. See Fig. 1. The success probability of A is

$$\epsilon_A = \Pr \left[u \xleftarrow{R} \{0,1\}^n; x \leftarrow X(u); a \leftarrow A^{\{O_\theta(\cdot)\}_\theta}(x) : R(u,x,a) = 1 \right].$$

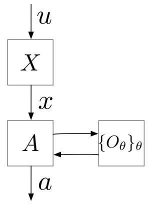

Fig. 1. A description of the inner adversary.

The outer adversary B can invoke the inner adversary A multiple times. We denote by A_i the ith invocation of A, which is the identical copy of A. The outer adversary B finally outputs b. The success condition of B depends on the type of games.

Decision Type ($n = 1$): When $n = 1$, A tries to distinguish two cases whether $u = 0$ or $u = 1$. The outer adversary B also tries to tell apart from the two cases based on the answers $a_1, a_2, \cdots$ from $A_1, A_2, \cdots$, where $a_i \in \{0, 1\}$. Thus, the success probability of B is defined as

$$\epsilon_{A,B}^{\mathrm{decn}} = \Pr\left[u \xleftarrow{R} \{0,1\}; b \leftarrow B^{O_A^{\mathrm{decn}}} : b = u\right],$$

where O_A^{decn} is the oracle that, given the ith query, computes $x_i \leftarrow X(u)$ and replies with $a_i \leftarrow A_i^{\{O_\theta(\cdot)\}_\theta}(x_i)$. See Fig. 2.

A typical example of the decision-type primitive is the pseudorandom generator. In that case, the secret describes whether the algorithm X is the pseudorandom generator ($u = 0$) or the true random generator ($u = 1$). Then, upon observing the output x from $X(u)$, the goal of the inner adversary is to estimate the value of u. Usually, the success probability is given by $\frac{1}{2}(1 + \delta)$ for some small advantage δ. The purpose of the outer adversary is to boost the success probability of estimating u by aggregating the outputs of N independent invocations of the inner adversary.

Search Type ($n > 1$): When $n > 1$, A tries to find any "correct" answer a satisfying $R(u, x, a) = 1$. Thus, B also tries to find any correct answer by invoking A_i's. At the ith invocation, a secret u_i is chosen independently and uniformly at random. Given $X(u_i)$, A_i replies with a_i. The final output of B is the list $\{(j, a_j)\}_j$ of all oracle replies. The success probability of B is defined as

$$\epsilon_{A,B}^{\mathrm{srch}} = \Pr\left[b = \{(j, a_j)\}_j \leftarrow B^{O_A^{\mathrm{srch}}} : \exists i, (i, a_i) \in b \wedge R(u_i, x_i, a_i) = 1\right],$$

where O_A^{srch} is the oracle that, given the ith query, chooses $u_i \in \{0, 1\}^n$ uniformly at random, computes $x_i \leftarrow X(u_i)$, and replies with $a_i \leftarrow A_i^{\{O_\theta(\cdot)\}_\theta}(x_i)$. See Fig. 3.

A typical example of the search-type primitive is the one-way function. In that case, the secret describes the input of the one-way function X. Then,

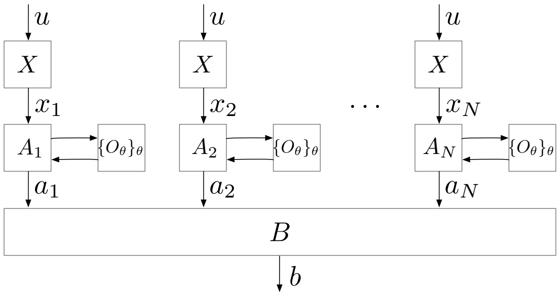

Fig. 2. A description of the outer adversary for $n = 1$.

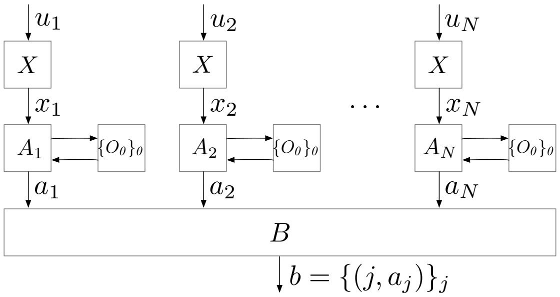

Fig. 3. A description of the outer adversary for $n > 1$.

upon observing the output of the one-way function, the goal of the inner adversary is to find an element in the inverse image of the given output. Usually, the success probability of the search-type game is tiny. Unlike the decision-type primitive, the outer adversary does not process the outputs obtained from the inner adversary; the role of the outer adversary is to invoke the inner adversary a sufficient number of times so that at least one correct estimate of the secret is included in the list.

The objective of the outer adversary B is to achieve the success probability of $1 - \mu$ for some small constant $\mu > 0$ with the least number $N = N_{A,B}$ of invocations of A. We assume that N outputs $a_1, \ldots, a_N$ are independently identically distributed according to a distribution determined by the behavior of the inner adversary A. This assumption implies that our definition captures the situation in which the outer adversary tries to amplify the success probability by observing multiple invocations of the inner adversary.

Let T_A denote the computational complexity for playing the inner game by A. Namely, it is the (worst-case) computational cost for running the experiment $\left[u \xleftarrow{R} \{0,1\}^n; x \leftarrow X(u); a \leftarrow A^{\{O_\theta(\cdot)\}_\theta}(x)\right]$. The bit security is defined as the computational cost of (A, B) necessary for achieving the success probability $\epsilon_{A,B} \geq 1 - \mu$.

Definition 1 (Bit Security). *The bit security of an n-bit game $G = (X, R, \{O_\theta\}_\theta)$ for error probability μ is defined to be*

$$\begin{aligned}\mathrm{BS}^{\mu}_{G} &\triangleq \min_{A,B} \{\log_2(N_{A,B} \cdot T_A) : \epsilon_{A,B} \geq 1-\mu\} \\ &= \min_{A} \left\{\log_2 T_A + \log_2 \min_{B}\{N_{A,B} : \epsilon_{A,B} \geq 1-\mu\}\right\},\end{aligned}$$

where $N_{A,B}$ is the number of queries to A made by the outer adversary B.

The computational complexity of B is not considered in the definition. It is for simplicity. Most of the time is consumed by the $N_{A,B}$ times running of A. Compared to it, the computational cost of B is negligibly small. Indeed, in Section 3.2, we show that simple computations of B can achieve tight upper bounds on the bit security. We note that when $n = 1$, the restriction of the output range of A to $\{0,1\}$ is necessary to ignore the computational cost of B. If A can output any values and we do not consider B's cost, B may trivially predict the value u by observing each A_i's view and performing a high-cost computation that is not counted.

By definition, the bit security of search primitives has a finite value if the output space of inner adversaries is finite. If an inner adversary A for a search-type game outputs $a \in \{0,1\}^\ell$, since a random guessing adversary has a success probability of at least $1/2^\ell$, the bit security is bounded above by $\ell + O(1)$. In contrast to this fact, decision games can have infinite bit security. For example, since the one-time pad has perfect secrecy, the bit security should be unbounded.

Measures of Computational Costs

We can adopt various measures of resources as computational complexity. The only restriction is that repeating the task with complexity T in total ℓ times takes the complexity of ℓT. This property is implicitly assumed in Definition 1.

We can assume that time complexity is employed to measure computational cost in this paper. Following the literature, one may also employ the circuit size as the computational cost. Note that there have been discussions about measuring the cost of attacks [13, 3, 6], especially in the non-uniform model.

Instantiations

Some instantiations of decision and search games in our framework are described in Table 1.

3.2 Upper and Lower Bounds

Since most cryptographic primitives are built upon unproven hardness assumptions, it is difficult to provide absolute bounds on the bit security of given primitives. In this section, we present an upper bound (Theorem 1) and a lower bound (Theorem 2) on the bit security in terms of the success probability of an inner

Table 1. Some instantiations of security games.

Game	Type*	X	R	$\{O_\theta(\cdot)\}_\theta$
OWF f	S	$f(u)$	$f(u) = f(a)$	—
PRG g	D	$\begin{cases} g(U_\ell) & u = 0 \\ U_m & u = 1 \end{cases}$	$u = a$	—
IND of (D_0, D_1)	D	D_u	$u = a$	—
IND security of $(\mathsf{Enc}, \mathsf{Dec})$	D	$(m_0, m_1, \mathsf{Enc}(m_u))$	$u = a$	—
IND-CPA of $(\mathsf{Enc}, \mathsf{Dec})$	D	pp	$u = a$	$O_e(q) = \mathsf{Enc}_{ek}(q)$ $O_c(q_0, q_1) = \mathsf{Enc}_{ek}(q_u)$
Unforgeability of $(\mathsf{Sign}, \mathsf{Vrfy})$	S	vk	$a \notin \{O_s(q_i)\}_i$ $\wedge\ \mathsf{Vrfy}_{vk}(a) = 1$	$O_s(q) = (q, \mathsf{Sign}_{sk}(q))$
2nd-preimage resistance of h	S	(u, r)	$r \neq a\ \wedge$ $h_u(r) = h_u(a)$	—
Collision resistance of h	S	u	$a_1 \neq a_2 \wedge$ $h_u(a_1) = h_u(a_2)$	—
DDH	D	$\begin{cases} (g, g^c, g^d, g^{cd}) & u = 0 \\ (g, g^c, g^d, g^e) & u = 1 \end{cases}$	$u = a$	—
CDH	S	(g, g^c, g^d)	$a = g^{cd}$	—

*S = Search, D = Decision

adversary. In Section 4, those upper bound and lower bound are used to discuss the relative loss of the bit security during reductions of cryptographic primitives.

First, we derive an upper bound. To that end, for a given inner adversary A with success probability ϵ_A, we shall derive an upper bound on the number $N_{A,B}$ of invocations necessary to attain the outer adversary's success probability $1 - \mu$. For the search-type game, the number $N_{A,B}$ can be upper bounded by a simple bound on the geometric distribution.

Lemma 1 (Upper bound for $n > 1$). *Let G be a search-type security game, and A be its inner adversary with success probability $\epsilon_A \in (0, 1]$. Then, there exists an outer adversary B such that $\epsilon_{A,B} \geq 1 - \mu$ and*

$$N_{A,B} = \left\lceil \frac{1}{\epsilon_A} \ln(1/\mu) \right\rceil.$$

Proof. We consider an adversary B that simply invokes A_i in total $N = N_{A,B}$ times. The success probability of B is $\epsilon_B = 1 - (1 - \epsilon_A)^N$. We need to guarantee that $\epsilon_B \geq 1 - \mu$, i.e., $(1 - \epsilon_A)^N \leq \mu$. Since

$$(1 - \epsilon_A)^N \leq \exp(-N\epsilon_A),$$

it suffices to choose $N = \lceil (1/\epsilon_A) \ln(1/\mu) \rceil$ for achieving $(1 - \epsilon_A)^N \leq \mu$. Hence, the statement follows. □

For the decision-type game, we need some machinery from the Bayesian hypothesis testing. Observe that the success probability of an inner adversary can be written as

$$\epsilon_A = \frac{1 + d_{\mathsf{TV}}(P_{A|U}(\cdot|0), P_{A|U}(\cdot|1))}{2},$$

where $P_{A|U}(\cdot|u)$ is the distribution of the inner adversary's output when the secret is u. When we evaluate the outer adversary's success probability, the exponential convergence is characterized by the Rényi divergence of order $1/2$. The following lemma connects the total variation distance and the Rényi divergence of order $1/2$.

Lemma 2. *For given distributions P and Q, we have*

$$d_{\mathsf{TV}}(P,Q)^2 \le 1 - \exp(-D_{1/2}(P\|Q)).$$

Proof. For example, see [8, Proposition 5]. □

By using Lemma 2, we can derive the following upper bound on $N_{A,B}$ for the decision-type game.

Lemma 3 (Upper bound for $n = 1$). *Let G be a decision-type security game, and A be its inner adversary with success probability $\epsilon_A = (1+\delta)/2$ for $\delta \in (0,1]$. Then, there exists an outer adversary B such that $\epsilon_{A,B} \ge 1 - \mu$ and*

$$N_{A,B} = \left\lceil \frac{2}{\delta^2} \ln(1/2\mu) \right\rceil. \tag{4}$$

Proof. We define the strategy of the outer adversary B as

$$b = \begin{cases} 0 & \text{if } P_{A^N|U}(a^N|0) \ge P_{A^N|U}(a^N|1) \\ 1 & \text{if } P_{A^N|U}(a^N|0) < P_{A^N|U}(a^N|1) \end{cases}$$

where $P_{A^N|U}(\cdot|u)$ is the distribution of N independent outputs $a_1, \ldots, a_N$ of the inner adversary for the secret u. Then, by using a standard technique of the Bayesian hypothesis testing (cf. [5, Section 11.9]), the error probability of the outer adversary can be bounded as

$$\begin{aligned}
\Pr[b \ne u] &= \frac{1}{2} \sum_{a^N} \min\left\{P_{A^N|U}(a^N|0), P_{A^N|U}(a^N|1)\right\} \\
&\le \frac{1}{2} \sum_{a^N} \sqrt{P_{A^N|U}(a^N|0) \cdot P_{A^N|U}(a^N|1)} \\
&= \frac{1}{2} \exp\bigg(- \frac{1}{2} D_{1/2}(P_{A^N|U}(\cdot|0) \| P_{A^N|U}(\cdot|1))\bigg) \\
&= \frac{1}{2} \exp\bigg(- \frac{N}{2} D_{1/2}(P_{A|U}(\cdot|0) \| P_{A|U}(\cdot|1))\bigg).
\end{aligned}$$

Here, by noting $e^{-t} \geq 1 - t$, Lemma 2 implies

$$\delta^2 = d_{\mathsf{TV}}(P_{A|U}(\cdot|0), P_{A|U}(\cdot|1))^2 \leq D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1)).$$

Thus, we have

$$\Pr[b \neq u] \leq \frac{1}{2} \exp\left(- \frac{\delta^2 N}{2} \right).$$

This means that, in order to satisfy $\Pr[b \neq u] \leq \mu$, it suffices to take

$$N = \left\lceil \frac{2}{\delta^2} \ln(1/2\mu) \right\rceil,$$

which implies (4). □

We estimate the computational cost for implementing the outer adversary B in the above proof. We assume that B knows the conditional probability distributions $P_{A|U}(\cdot|0)$ and $P_{A|U}(\cdot|1)$. Given $a^N \in \{0,1\}^N$, B counts the number of 0's in a^N, denoted by N_0. Let $N_1 = N - N_0$. Then, B can compute the value $P_{A^N|U}(a^N|0)$ as $P_{A|U}(0|0)^{N_0} \cdot P_{A|U}(1|0)^{N_1}$. Also, $P_{A^N|U}(a^N|1)$ can be calculated similarly. The computation of B is for counting N_0, calculating the two probabilities, and comparing them. Thus, the computational complexity of B is $O(N)$. Even if we take into account the computational complexity of B, the bit security is affected by a constant that does not depend on security games.

It follows from the proof of Lemma 3 that the *Rényi advantage*

$$\mathsf{adv}_A^{\text{Renyi}} := D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1))$$

gives an upper bound for $n = 1$.

Lemma 4 (Upper bound for $n = 1$ with Rényi advantage). *Let G be a decision-type security game, and A be its inner adversary with the Rényi advantage with $\mathsf{adv}_A^{\text{Renyi}} > 0$. Then, there exists an outer adversary B such that $\epsilon_{A,B} \geq 1 - \mu$ and*

$$N_{A,B} = \left\lceil \frac{2}{\mathsf{adv}_A^{\text{Renyi}}} \ln(1/2\mu) \right\rceil. \tag{5}$$

From the above three lemmas, we can derive the following upper bound on the bit security.

Theorem 1. *Let G be an n-bit security game, and A be its inner adversary with success probability $\epsilon_A > 0$, running time T_A, and Rényi advantage $\mathsf{adv}_A^{\text{Renyi}} > 0$. Then, we have*

$$\mathrm{BS}_G^\mu \leq \begin{cases} \log_2 T_A + \log_2\left(\frac{1}{\epsilon_A}\right) + \log_2 \ln(1/\mu) + 1 & n > 1 \\ \log_2 T_A + 2\log_2\left(\frac{1}{2(\epsilon_A - 1/2)}\right) + \log_2 \ln(1/2\mu) + 2 & n = 1 \\ \log_2 T_A + \log_2\left(\frac{1}{\mathsf{adv}_A^{\text{Renyi}}}\right) + \log_2 \ln(1/2\mu) + 2 & n = 1 \end{cases}.$$

Proof. It directly follows from the definition of the bit security and the upper and lower bounds on $N_{A,B}$ in Lemmas 1, 3, and 4. □

Next, we derive a lower bound on the bit security. To that end, for a given inner adversary with success probability ϵ_A, we need to derive a lower bound on $N_{A,B}$ for arbitrary outer adversaries B. For the search-type game, the following bound can be derived from a simple union bound.

Lemma 5 (Lower bound for $n > 1$). *Let G be an n-bit security game, and A be its inner adversary with success probability ϵ_A. Then, any outer adversary B with $\epsilon_B \geq 1 - \mu$ must satisfy*

$$N_{A,B} \geq \frac{1-\mu}{\epsilon_A}.$$

Proof. Since ϵ_B is the probability that B successfully finds u at least once, by the union bound, we have $\epsilon_B \leq N_{A,B} \cdot \epsilon_A$, which implies the claim. □

For the decision-type game, deriving a lower bound on $N_{A,B}$ is more subtle. In fact, without further assumptions on the inner adversary to be discussed at the end of this section, it is not possible to derive a desirable lower bound in terms of the success probability ϵ_A of an inner adversary. Instead, we derive a lower bound in terms of the Rényi advantage as follows.

Lemma 6 (Lower bound for $n = 1$). *Let G be a 1-bit security game, and A be its inner adversary. Then, any outer adversary B with $\epsilon_B \geq 1 - \mu$ must satisfy*

$$N_{A,B} \geq \frac{\ln(1/(4\mu))}{\mathsf{adv}_A^{\mathrm{Renyi}}},$$

Proof. For any outer adversary B, we must have

$$\Pr[b \neq u] \geq \frac{1 - d_{\mathsf{TV}}(P_{A^N|U}(\cdot|0), P_{A^N|U}(\cdot|1))}{2}. \tag{6}$$

For two distributions P and Q, Lemma 2 implies

$$\begin{aligned} d_{\mathsf{TV}}(P,Q)^2 &\leq 1 - \exp(-D_{1/2}(P\|Q)) \\ &\leq \left(1 - \frac{1}{2}\exp(-D_{1/2}(P\|Q))\right)^2, \end{aligned}$$

i.e.,

$$1 - d_{\mathsf{TV}}(P,Q) \geq \frac{1}{2}\exp(-D_{1/2}(P\|Q)).$$

Thus, by applying this inequality to (6), we have

$$\begin{aligned} \Pr[b \neq u] &\geq \frac{1}{4}\exp(-D_{1/2}(P_{A^N|U}(\cdot|0)\|P_{A^N|U}(\cdot|1))) \\ &= \frac{1}{4}\exp(-ND_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1))). \end{aligned}$$

Since $\Pr[b \neq u] \leq \mu$, it holds that

$$N \geq \frac{\ln(1/(4\mu))}{D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1))}.$$

□

From Lemma 5 and Lemma 6, we can derive the following implication on the bit security.

Theorem 2. *If an n-bit game G is not λ-bit secure, i.e., $\mathrm{BS}_G^{\mu} < \lambda$, then there exists an inner adversary A for the game such that A runs in time T_A and satisfies*

$$\epsilon_A > \frac{T_A}{2^{\lambda}}(1-\mu)$$

for the search-type game $n > 1$; and

$$\mathsf{adv}_A^{\mathrm{Renyi}} = D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1)) > \frac{T_A}{2^{\lambda}} \cdot \ln\left(1/4\mu\right)$$

and

$$d_{\mathsf{HD}}(P_{A|U}(\cdot|0), P_{A|U}(\cdot|1)) > \min\left\{\frac{1}{\sqrt{2}}, \sqrt{\frac{T_A}{2^{\lambda+1}} \cdot \ln\left(1/4\mu\right)}\right\}.$$

for the decision-type game $n = 1$.

Proof. If G is not λ-bit secure, there exist an inner adversary A and an outer adversary B such that $N_{A,B} \cdot T_A < 2^{\lambda}$. Then, the bound for the search-type game follows from Lemma 5.

For the case that $n = 1$, Lemma 6 implies that $D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1)) > (T_A/2^{\lambda}) \cdot \ln(1/4\mu)$, and thus $d_{\mathsf{HD}}(P_{A|U}(\cdot|0), P_{A|U}(\cdot|1))^2 > \min\{1/2, x/2\}$ for $x = (T_A/2^{\lambda}) \cdot \ln(1/4\mu)$ by (3). □

Discussion

Theorem 1 roughly claims that for search-type games, if there is an adversary A with success probability ϵ_A and cost T_A, then the bit security cannot be larger than $\lambda \simeq \log_2(T_A/\epsilon_A)$; on the other hand, Theorem 2 roughly claims that if the best possible inner adversary A has success probability ϵ_A and cost T_A, then the bit security of $\lambda \simeq \log_2(T_A/\epsilon_A)$ is guaranteed. Thus, the upper bound and the lower bound essentially coincide.

For the decision-type game, the situation is more subtle. Theorems 1 and 2 show that the upper bound and the lower bound coincide in terms of the Rényi advantage. With the success probability, Theorem 1 claims that, if there exists an adversary A with success probability $\epsilon_A = (1+\delta)/2$ and cost T_A, then the bit security cannot be larger than $\lambda \simeq \log_2(T_A/\delta^2)$. By using the relation (1) between the total variation and the Hellinger distances, Theorem 2 guarantees that if the best possible inner adversary A has success probability $\epsilon_A = (1+\delta)/2$ and cost T_A, the bit security is guaranteed to be at least $\lambda \simeq \log_2(T_A/\delta)$. There is a gap of $\log_2(1/\delta)$ between the bounds. As a further illustration, let us consider an inner adversary given by $P_{A|U}(0|0) = \delta$, $P_{A|U}(1|0) = 1-\delta$, $P_{A|U}(0|1) = 0$, and $P_{A|U}(1|1) = 1$; this inner adversary makes no error when $u = 1$, and it makes an error most of the time, $1-\delta$, when $u = 0$. For this adversary, the advantage is given by

$$d_{\mathsf{TV}}(P_{A|U}(\cdot|0), P_{A|U}(\cdot|1)) = \delta.$$

On the other hand, the Rényi divergence/advantage is given by

$$\begin{aligned} D_{1/2}(P_{A|U}(\cdot|0) \| P_{A|U}(\cdot|1)) &= -\ln(1-\delta) \\ &= \delta + o(\delta). \end{aligned}$$

Thus, if this kind of inner adversary exists, we can only guarantee the bit security of $\lambda \simeq \log(T_A/\delta)$ as a function of possible advantage δ.

Let us consider *linear tests* against a PRG $g : \{0,1\}^\ell \to \{0,1\}^m$ (cf. [1, 21]). It is known that they are powerful enough to give the best-known attack that yields the distinguishing advantage $\delta \geq 2^{-\ell/2}$ (See [7, 1]). These tests output $a = 0$ and $a = 1$ with the same probability for the true random generator ($u = 1$). Thus, it seems reasonable to assume that the probability of each a given u is lower bounded as $P_{A|U}(a|u) \geq \beta$ for some $\beta > 0$; in the following, a class of inner adversaries satisfying such an assumption is termed, *β-balanced* adversaries.

When probabilities are bounded below, we can connect the total variation distance and the Rényi divergence.

Lemma 7. *For given distributions P and Q, we have*

$$D_{1/2}(P\|Q) \leq D(P\|Q) \leq 2\beta_Q^{-1} d_{\mathsf{TV}}(P,Q)^2,$$

where $\beta_Q = \min_{x \in \mathcal{X}^+} Q(x)$, $\mathcal{X}^+ = \{x : Q(x) > 0\}$, and $D(P\|Q) = \sum_x P(x) \log(P(x)/Q(x))$ is the KL-divergence.

Proof. The former inequality follows from the fact that the Rényi divergence is monotonically non-decreasing with respect to α and $D(P\|Q) = \lim_{\alpha \to 1} D_\alpha(P\|Q)$. For the latter inequality, see [11, Lemma 4.1]. □

Using Lemma 7, we can derive the following lower bound on the bit security against β-balanced adversaries.

Theorem 3. *If a 1-bit game G is not λ-bit secure against β-balanced adversaries, then there exists a β-balanced inner adversary A for the game such that A runs in time T_A and the success probability $\epsilon_A = (1+\delta)/2$ satisfies*

$$\delta^2 > \frac{\beta T_A}{2^{\lambda+1}} \cdot \ln\left(\frac{1}{4\mu}\right).$$

Proof. In the same manner as Theorem 2, Lemma 6 implies that $D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1)) > (T_A/2^\lambda) \cdot \ln(1/4\mu)$, which together with Lemma 7 and the β-balanced assumption imply the desired bound. □

Theorem 3 claims that, if the best possible advantage by β-balanced adversaries is δ, the bit security of $\lambda \simeq \log(\beta T_A/\delta^2)$ is guaranteed, which coincides with the upper bound for $\beta = \Omega(1)$.

4 Security Reductions

We present several security reductions of security games.

We give the following lemma used in the proofs.

Lemma 8. *Let A_0 and A_1 be distributions over $\{0,1\}$ such that $A_0(0) = \delta, A_0(1) = 1-\delta, A_1(0) = q\delta, A_1(1) = 1-q\delta$, where $0 \le \delta \le 1/32$ and $0 \le q\delta \le 1$. Then, $D_{1/2}(A_0\|A_1) \ge \phi(q)\cdot\delta$, where*

$$\phi(q) := (1-\sqrt{q})^2 - q/16.$$

Proof. By definition,

$$\begin{aligned} D_{1/2}(A_0\|A_1) &= -2\ln\left(\sqrt{q\delta^2} + \sqrt{(1-\delta)(1-q\delta)}\right) \\ &= -\ln\left(q\delta^2 + (1-\delta)(1-q\delta) + 2\sqrt{(1-\delta)(1-q\delta)q\delta^2}\right) \\ &\ge -\ln\left(q\delta^2 + (1-\delta)(1-q\delta) + 2\sqrt{q}\delta\right) \\ &= -\ln\left(1-(1+q)\delta + 2\sqrt{q}\delta + 2q\delta^2\right) \\ &= -\ln\left(1-(1-\sqrt{q})^2\delta + 2q\delta^2\right) \\ &\ge (1-\sqrt{q})^2\delta - 2q\delta^2 \\ &\ge \left((1-\sqrt{q})^2 - q/16\right)\delta, \end{aligned}$$

where the last inequality holds for $\delta \le 1/32$. □

4.1 Goldreich-Levin Hard-Core Predicate

For functions $f : \{0,1\}^n \to \{0,1\}^m$ and $h : \{0,1\}^n \to \{0,1\}$, the hard-core predicate game for f is a decision game with $X = (f(R), h(R))$ when $u = 0$, and $X = (f(R), U_1)$ otherwise, where R is the uniform distribution over $\{0,1\}^n$ and U_1 is the uniformly random bit.

We show that the Goldreich-Levin theorem [10, 9] gives a tight reduction if adversaries for the hard-core predicate are restricted to be β-balanced for some constant $\beta > 0$. Namely, we assume that the adversary outputs each value with a not too small probability.

Theorem 4. *Let $f : \{0,1\}^n \to \{0,1\}^m$ be a λ-bit secure one-way function. Define $g : \{0,1\}^{2n} \to \{0,1\}^{n+m}$ as $g(x,r) = (f(x), r)$. Then, the function $h : \{0,1\}^{2n} \to \{0,1\}$ defined by $h(x,r) = \sum_i x_i \cdot r_i \bmod 2$ is a $(\lambda - \alpha)$-bit secure hard-core predicate for g against β-balanced adversaries, where $\alpha = 2\log_2 n + 3\log_2 \lambda + \log_2(1/\beta) + \log_2 \ln(1/\mu) + O(1)$.*

Proof. It was proved by Goldreich and Levin (cf. [10, 9]) that for any inner adversary A for the hard-core predicate game with running time T_A and

$$\delta_A = 2 \cdot \Pr[A(f(Q,R)) = h(Q,R)] - 1 > 0,$$

where Q and R are uniform distributions over $\{0,1\}^n$, there is an adversary A' that runs in time $T_{A'} = O(n^2(\log_2(1/\delta_A))^3) \cdot T_A$ such that

$$\Pr[A(f(Q,R)) = (Q,R)] = \Omega(\delta_A^2).$$

Assume for contradiction that h is not $(\lambda - \alpha)$-bit secure hard-core for g against β-balanced adversaries. Then, by Theorem 3, there exists an inner adversary A with running time T_A such that the success probability for the hard-core predicate game is $\epsilon_A = (1 + \delta_A)/2$ for $\delta_A > \sqrt{\beta T_A \cdot \ln(1/4\mu)/2^{\lambda-\alpha+1}}$. It is well-known that the distinguisher A for the hard-core predicate can be used to construct a predictor of the value $h(x,r)$. By the Goldreich-Levin theorem, there is an inner adversary A' for the OWF game that runs in time $T_{A'} = O(n^2 \cdot \lambda^3) \cdot T_A$ with success probability $\epsilon_{A'} = \Omega(\beta T_A \cdot 2^{-(\lambda-\alpha)})$. It follows from Theorem 1 that the bit security of the OWF game is bounded above by $\log_2 T_{A'} + \log_2(1/\epsilon_{A'}) + \log_2 \ln(1/\mu) + 1$, which is at most

$$\lambda - \alpha + \log_2 O(n^2\lambda^3) + \log_2(1/\beta) + \log_2 \ln(1/\mu) + 1.$$

By choosing $\alpha = 2\log_2 n + 3\log_2 \lambda + \log_2(1/\beta) + \log_2 \ln(1/\mu) + O(1)$, f is not a λ-bit secure one-way function, a contradiction. Hence, the statement follows. □

If the β-balanced assumption is removed in Theorem 4, we cannot guarantee the existence of an inner adversary A with $\delta_A \simeq 2^{-\lambda/2}$. When the hard-core predicate is λ-bit secure against general adversaries, it might be attained by a "biased" inner adversary such that $\delta_A \simeq 2^{-\lambda}$. Then, the success probability of A' guaranteed by the Goldreich-Levin theorem would be $\Omega(2^{-2\lambda})$. Consequently, we can only guarantee that a 2λ-bit secure one-way function implies a λ-bit secure hard-core predicate. In this sense, it remains an open problem to prove if λ-bit secure one-way function implies λ-secure hard-core predicate in our framework. To that end, we may need a tight reduction that directly connects the Rényi advantage of predicting the hard-core to the success probability of inverting the one-way function.

4.2 PRG Implies OWF

Consider a pseudorandom generator $g : \{0,1\}^\ell \to \{0,1\}^m$. As noted in [7], since g is also a *δ-biased* generator (cf. [21]), the seed length ℓ must be at least

$2\log(1/\delta)$ for achieving the distinguishing advantage δ even for linear tests [1]. That is, it must be that $\delta \geq 2^{-\ell/2}$. We might deduce from this fact that the bit security of PRG needs to be half of OWF. We show that this is not the case in our framework. Namely, there would be a λ-bit secure PRG that is a λ-bit secure OWF but is not a $(\lambda + \omega(1))$-bit secure OWF.

Theorem 5. *If $g : \{0,1\}^\ell \to \{0,1\}^m$ is a λ-bit secure pseudorandom generator, then g is a $(\lambda - \alpha)$-bit secure one-way function for $\alpha = \max\{\log_2(1+T_g) + \log_2(1/\phi(1/2)) + \log_2(\ln(1/2\mu)/(1-\mu)) + 2, \log_2(1+T_g) + \log_2\ln(1/2\mu) + 14\}$, where T_g is the computational complexity for evaluating g.*

Proof. Suppose for contradiction that g is not a $(\lambda - \alpha)$-bit secure one-way function. Theorem 2 implies that there exists an inner adversary A that runs in T_A and has success probability $\epsilon_A > T_A(1-\mu)/2^{\lambda-\alpha}$. Also, it must be that $N_{A,B} \cdot T_A < 2^{\lambda-\alpha}$, implying that $T_A < 2^{\lambda-\alpha}$. Consider an inner adversary A' for the PRG game G such that, on input x, A' runs $A(x)$ to get a, and outputs 0 if $g(a) = x$, and 1 otherwise. For $u, b \in \{0,1\}$, let A_u be the probability distribution on the output of A' when $u \in \{0,1\}$ was chosen in the PRG game. Then, we have

$$A_0(0) = \epsilon_A, A_0(1) = 1 - \epsilon_A, A_1(0) \leq \frac{2^\ell}{2^m}\epsilon_A, A_1(1) \geq 1 - \frac{2^\ell}{2^m}\epsilon_A.$$

We apply Lemma 8 with $A_1(0) = q\epsilon_A$ and $A_1(1) = 1 - q\epsilon_A$ for some $q \leq 1/2$. Since $\phi(q)$ is monotonically decreasing on $[0, 1/2]$, we have

$$D_{1/2}(A_0||A_1) \geq \phi(q) \cdot \epsilon_A \geq \phi(1/2) \cdot \epsilon_A$$

as long as $\epsilon_A \leq 1/32$. By using Theorem 1,

$$\begin{aligned}\mathrm{BS}^\mu_G &\leq \log_2(T_A + T_g) + \log_2(1/\phi(1/2)\epsilon_A) + \log_2\ln(1/2\mu) + 2\\ &< \lambda - \alpha + \log_2(1 + T_g/T_A) + \log_2(1/\phi(1/2)) + \log_2(\ln(1/2\mu)/(1-\mu)) + 2\\ &\leq \lambda.\end{aligned}$$

When $\epsilon_A > 1/32$, the success probability of A' is

$$\begin{aligned}\Pr[u=0] \cdot A_0(0) + \Pr[u=1] \cdot A_1(1) &\geq \frac{1}{2}\left(\epsilon_A + 1 - \frac{2^\ell}{2^m}\epsilon_A\right)\\ &\geq \frac{1}{2}\left(1 + \frac{\epsilon_A}{2}\right)\\ &> \frac{1}{2}\left(1 + \frac{1}{64}\right),\end{aligned}$$

where the second inequality follows from $m \geq \ell + 1$. By Theorem 1,

$$\begin{aligned}\mathrm{BS}^\mu_G &\leq \log_2(T_A + T_g) + 2\log_2(64) + \log_2\ln(1/2\mu) + 2\\ &< \lambda - \alpha + \log_2(1 + T_g/T_A) + \log_2\ln(1/2\mu) + 14\\ &\leq \lambda.\end{aligned}$$

In both cases, we have a contradiction. Hence, the statement follows. □

Next, we demonstrate that the bit security achieved in Theorem 5 is almost optimal. Specifically, we show that as long as considering pseudorandomness against β-balanced adversaries for constant $\beta > 0$, the PRG constructed from a λ-bit secure one-way permutation and the hard-core predicate is a $(\lambda - O(1))$-bit secure PRG. However, it is not a $(\lambda + \omega(1))$-bit secure OWF if the one-way permutation is not $(\lambda + 1)$-bit secure.

Theorem 6. *Let $f : \{0,1\}^n \to \{0,1\}^n$ be a λ-bit secure one-way permutation that is not $(\lambda + 1)$-bit secure one-way. Consider a function $g : \{0,1\}^{2n} \to \{0,1\}^{2n+1}$ defined by $g(x,r) = (f(x), r, h(x,r))$ and $h(x,r) = \sum_i x_i \cdot r_i \bmod 2$. Then, g is a $(\lambda - \alpha)$-bit secure pseudorandom generator against β-balanced adversaries, but is not a $(\lambda + \alpha')$-bit secure one-way function for $\alpha = 2\log_2 n + 3\log_2 \lambda + \log_2(1/\beta) + \log_2 \ln(1/\mu) + O(1)$ and $\alpha' = \log_2(1 + T_{f,h}) + \log_2(\ln(1/\mu)/(1-\mu)) + 2$, where $T_{f,h}$ is the computational complexity for evaluating f and h.*

Proof. First, we show that g is a PRG. Assume for contradiction that g is not a $(\lambda - \alpha)$-bit secure PRG against β-balanced adversaries. By Theorem 3, there exists a β-balanced inner adversary A for the PRG game of g that runs in T_A and has success probability $\epsilon_A = (1 + \delta_A)/2$ with $\delta_A > \sqrt{\beta T_A \ln(1/4\mu)/2^{\lambda-\alpha+1}}$. Since f is a permutation, the first $2n$ bits of g are distributed uniformly at random. Thus, the distinguisher A for the PRG g can work as a distinguisher for the hard-core predicate game of $h(x,r)$ for function $g'(x,r) = (f(x), r)$. By Theorem 4, as long as $\alpha = 2\log_2 n + 3\log_2 \lambda + \log_2(1/\beta) + \log_2 \ln(1/\mu) + O(1)$, f is not a λ-bit secure one-way function, a contradiction.

Next, we show that g is not a $(\lambda + \alpha')$-bit secure one-way function. Since f is not a $(\lambda + 1)$-bit secure one-way function, it follows from Theorem 2 that there is an inner adversary A for the OWF game of f that runs in time T_A and has success probability $\epsilon_A > T_A(1-\mu)/2^{\lambda+1}$. Consider an inner adversary A' for the OWF game of g that given (y, r, b), runs A on input y, and outputs (a, r) if A output a satisfying $y = f(a)$ and $h(a,r) = b$, and $\perp$ otherwise. Let $\epsilon_{A'}$ be the success probability of A' in the OWF game of g. Since f is a permutation, there is no $a \in \{0,1\}^n$ satisfying $f(a) = f(x)$ and $a \neq x$. Thus, A' succeeds in the OWF game of g whenever A outputs a satisfying $y = f(a)$. That is, $\epsilon_{A'} \geq \epsilon_A$. Theorem 1 implies that the bit security of g is at most

$$\begin{aligned}&\log_2(T_A + T_{f,h}) + \log_2(1/\epsilon_{A'}) + \log_2 \ln(1/\mu) + 1\\ &< \lambda + \log_2(1 + T_{f,h}) + \log_2 \frac{\ln(1/\mu)}{(1-\mu)} + 2.\end{aligned}$$

□

4.3 IND-CPA Encryption Implies OW-CPA Encryption

For an encryption scheme, the one-way chosen-plaintext-attack (OW-CPA) game $G^{\mathrm{ow}}_{A,B}$ is defined such that given a ciphertext of a randomly chosen message $m \in \mathcal{M}$, an inner adversary A tries to output the plaintext m. At any time during the game, A can query any message in $\mathcal{M}$ and receive its encrypted ciphertext.

It is well-known that IND-CPA security implies OW-CPA security if the message space is sufficiently large. We reveal the quantitative relationship between the two notions in our framework. Note that if we employ the "conventional" advantage-based argument, 2λ-bit IND-CPA security is required for achieving λ-bit OW-CPA security. The reason is that by assuming an attacker for λ-bit secure OW-CPA game with advantage $\epsilon_A \approx 2^{-\lambda}$, Theorem 1 only guarantees that the bit security of IND-CPA is at most $2\log_2(1/\epsilon_A) \approx 2\lambda$. We resolve this problem by exploiting the Rényi advantage.

Theorem 7. *If an encryption scheme with message space $\mathcal{M}$ has λ-bit secure IND-CPA security, with $|\mathcal{M}| \geq \max\{2^{\lambda-\alpha+4}/(1-\mu)+1, 65\}$, then it has $(\lambda-\alpha)$-bit secure OW-CPA security, where $\alpha = \log_2(1+2(T_{\mathrm{samp}}+T_{\mathrm{eq}})) + \max\{\log_2(\ln(1/2\mu)/(1-\mu))+3, \log_2\ln(1/2\mu)+8\}$, where T_{samp} is the computational complexity for sampling a message from $\mathcal{M}$ uniformly at random and T_{eq} is for checking the equality of given two messages in $\mathcal{M}$.*

Proof. Assume for contradiction that the scheme does not have $(\lambda-\alpha)$-bit secure OW-CPA security. Theorem 2 implies that there exists an inner adversary A with running time T_A and success probability $\epsilon_A > T_A(1-\mu)/2^{\lambda-\alpha}$. Consider an inner adversary A' for the IND-CPA game G^{IND} such that A' first chooses two different messages $m_0, m_1 \in \mathcal{M}$ uniformly at random and sends them to the challenger. Given the challenge ciphertext c for message m_u, A' runs A on input c. Oracle queries from A can be replied by querying them to the oracles of A'. If A outputs either m_0 or m_1, A' outputs the corresponding bit. Otherwise, A' outputs 1. The computational complexity of A' for running the IND-CPA game is at most $T_A + 2(T_{\mathrm{samp}} + T_{\mathrm{eq}})$. Let A_u be the probability distribution on the output of A' when $u \in \{0,1\}$ is chosen as the secret in G^{IND}. By definition, $A_0(0) = \epsilon_A$ and $A_0(1) = 1-\epsilon_A$. We note that $A_1(0)$ is not necessarily equal to 0 since A' may accidentally output m_0 even when the ciphertext of m_1 is sent to A'. Since the challenge ciphertext does not contain any information on m_0 and m_0 is randomly chosen from $\mathcal{M} \setminus \{m_1\}$ when $u=1$, the probability that A' outputs m_0 is at most $1/(|\mathcal{M}|-1)$. Hence, we have $A_1(0) = \epsilon$ and $A_1(1) = 1-\epsilon$ for some $\epsilon \leq 1/(|\mathcal{M}|-1)$. Suppose that $\epsilon_A \leq 1/32$. By Lemma 8, the Rényi advantage of A' satisfies

$$\mathsf{adv}_{A'}^{\mathrm{Renyi}} = D_{1/2}(A_0 \| A_1) \geq \phi(q) \cdot \epsilon_A$$

for $q = \epsilon/\epsilon_A$. By assumption on $|\mathcal{M}|$,

$$q = \frac{\epsilon}{\epsilon_A} \leq \frac{2^{\lambda-\alpha}}{T_A(1-\mu)(|\mathcal{M}|-1)} \leq \frac{1}{16}.$$

Since $\phi(q) > 1/2$ for $q \leq 1/16$, we have $\mathsf{adv}^{\mathrm{Renyi}}_{A'} \geq \phi(1/16) \cdot \epsilon_A > \epsilon_A/2$. Theorem 1 implies that

$$\begin{aligned}\mathrm{BS}^{\mu}_{G^{\mathrm{IND}}} &\leq \log_2(T_A + 2(T_{\mathrm{samp}} + T_{\mathrm{eq}})) + \log_2(2/\epsilon_A) + \log_2 \ln(1/2\mu) + 2 \\ &< \lambda - \alpha + \log_2(1 + 2(T_{\mathrm{samp}} + T_{\mathrm{eq}})) + \log_2(\ln(1/2\mu)/(1-\mu)) + 3 \\ &\leq \lambda.\end{aligned}$$

When $\epsilon_A > 1/32$, the success probability of A' is

$$\Pr[u = 0] \cdot A_0(0) + \Pr[u = 1] \cdot A_1(1) \geq \frac{1}{2}(\epsilon_A + 1 - \epsilon) > \frac{1}{2}\left(1 + \frac{1}{64}\right).$$

Since $T_A < 2^{\lambda-\alpha}$, it follows from Theorem 1 that

$$\begin{aligned}\mathrm{BS}^{\mu}_{G^{\mathrm{IND}}} &< \log_2(T_A + 2(T_{\mathrm{samp}} + T_{\mathrm{eq}})) + \log_2(64) + \log_2 \ln(1/2\mu) + 2 \\ &< \lambda - \alpha + \log_2(1 + 2(T_{\mathrm{samp}} + T_{\mathrm{eq}})) + \log_2 \ln(1/2\mu) + 8 \\ &\leq \lambda.\end{aligned}$$

In both cases, we have a contradiction. □

In the above reduction, the IND-CPA adversary does not make a random guess if the OW-CPA adversary fails to recover the plaintext. This reduction is different from the traditional one.

4.4 DDH and CDH Problems

Let G be a polynomial-time group-generation algorithm that outputs a description of a cyclic group $\mathbb{G}$ of prime order p and a generator $g \in \mathbb{G}$. The Computational Diffie-Hellman (CDH) problem is to compute g^{xy} from (g^x, g^y) for random $x, y \in \mathbb{Z}_p$. The success probability of an inner adversary A for the CDH game of G is formally defined by

$$\epsilon^{\mathrm{cdh}}_A = \Pr\left[(\mathbb{G}, p, g) \leftarrow G; x, y \xleftarrow{R} \mathbb{Z}_p; a \leftarrow A(\mathbb{G}, p, g, g^x, g^y) : a = g^{xy}\right]$$

The Decisional Diffie-Hellman (DDH) problem is to distinguish (g^x, g^y, g^z) from (g^x, g^y, g^{xy}) for random $x, y, z \in \mathbb{Z}_p$. The success probability of A for the DDH game of G is defined by

$$\epsilon^{\mathrm{ddh}}_A = \Pr\left[\begin{matrix} u \xleftarrow{R} \{0,1\}; (\mathbb{G}, p, g) \leftarrow G; \\ x, y, z \xleftarrow{R} \mathbb{Z}_p; (g_0, g_1) = (g^{xy}, g^z) \end{matrix} : u \leftarrow A(\mathbb{G}, p, g, g^x, g^y, g_u)\right].$$

It is well-known that the DDH problem is reducible to the corresponding CDH problem. Quantitatively, we show that the bit security of the CDH problem is at least that of the DDH problem.

Theorem 8. *Let G be a group-generation algorithm of cyclic groups of order p. If the DDH game of G has λ bit security with $p \geq \max\{2^{\lambda-\alpha+4}/(1-\mu), 64\}$, then the CDH game of G has $(\lambda - \alpha)$ bit security, where $\alpha = \log_2(1 + T_{\mathrm{eq}}) + \max\{\log_2(\ln(1/2\mu)/(1-\mu)) + 3, \log_2 \ln(1/2\mu) + 8\}$ and T_{eq} is the computational complexity for checking the equality of given two elements in G.*

Proof. Assume for contradiction that the CDH game is not $(\lambda - \alpha)$-bit secure. By Theorem 2, there exists an inner adversary A for the CDH game G^{CDH} that runs in time T_A and has success probability $\epsilon_A > T_A(1-\mu)/2^{\lambda-\alpha}$. Consider an inner adversary A' for the DDH game that, given $(\mathbb{G}, p, g, g^x, g^y, g_u)$, runs A on input $(\mathbb{G}, p, g, g^x, g^y)$ to obtain a. If $a = g_u$, A' outputs 0. Otherwise, A' outputs 1. Let A_u be the probability distribution on the output of A' when $u \in \{0, 1\}$ was chosen in the DDH game. By definition, $A_0(0) = \epsilon_A$ and $A_0(1) = 1 - \epsilon_A$. Since the probability $A_1(0)$ is bounded above by the probability that a randomly chosen z equals xy in the DDH game, we have $A_1(0) \leq 1/p$ and $A_1(1) \geq 1 - 1/p$. Suppose that $\epsilon_A \leq 1/32$. By Lemma 8, $D_{1/2}(A_0 \| A_1) \geq \phi(q) \cdot \epsilon_A$ for $q \leq 1/p\epsilon_A$. Since $p \geq 2^{\lambda-\alpha+4}/(1-\mu)$, we have

$$\frac{1}{p\epsilon_A} \leq \frac{1-\mu}{2^{\lambda-\alpha+4}} \cdot \frac{2^{\lambda-\alpha}}{T_A(1-\mu)} \leq \frac{1}{16}.$$

Hence, $\phi(q) > 1/2$. It follows from Theorem 1 that

$$\begin{aligned}\mathrm{BS}^{\mu}_{G^{\mathrm{DDH}}} &\leq \log_2(T_A + T_{\mathrm{eq}}) + \log_2(2/\epsilon_A) + \log_2 \ln(1/2\mu) + 2 \\ &< \lambda - \alpha + \log_2(1 + T_{\mathrm{eq}}) + \log_2(\ln(1/2\mu)/(1-\mu)) + 3 \\ &\leq \lambda.\end{aligned}$$

When $\epsilon_A > 1/32$, the success probability of A' is

$$\Pr[u = 0] \cdot A_0(0) + \Pr[u = 1] \cdot A_1(1) \geq \frac{1}{2}(\epsilon_A + 1 - 1/p) > \frac{1}{2}\left(1 + \frac{1}{64}\right).$$

Since $T_A < 2^{\lambda-\alpha}$, Theorem 1 implies that

$$\begin{aligned}\mathrm{BS}^{\mu}_{G^{\mathrm{DDH}}} &\leq \log_2(T_A + T_{\mathrm{eq}}) + \log_2(64) + \log_2 \ln(1/2\mu) + 2 \\ &< \lambda - \alpha + \log_2(1 + T_{\mathrm{eq}}) + \log_2 \ln(1/2\mu) + 8 \\ &\leq \lambda.\end{aligned}$$

In both cases, we have a contradiction. □

4.5 Distribution Approximation

We consider replacing probability distributions in security games. Let $G = (X, R, \{O_i\}_i)$ be a game for primitive $\mathit{\Pi}$. Suppose that a distribution ensemble $Q = (Q_\theta)_\theta$ over $(\mathit{\Omega}_\theta)_\theta$ is employed in G, where each distribution Q_θ is available in a black-box manner such that when some player queries θ, a sample from Q_θ

is replied. We denote the game by G^Q for clarity. We want to show that the bit security of Π is preserved when replacing the ensemble Q with an approximated distribution ensemble $P = (P_\theta)_\theta$ if Q_θ and P_θ are close enough each other. The question is how close P should be to Q.

Let $d(P, Q)$ be a divergence/distance on probability distributions. A divergence is said to be (β, γ)-*efficient* if it satisfies the following conditions:

1. Sub-additivity: For two distribution ensembles $(X_i)_i$ and $(Y_i)_i$ over the same finite support $\prod_i \Omega_i$,
$$d((X_i)_i, (Y_i)_i) \le \sum_i \max_{a \in \prod_{j<i} \Omega_j} d\left((X_i | X_{<i} = a), (Y_i | Y_{<i} = a)\right),$$
where $X_{<i} = (X_1, \ldots, X_{i-1})$ and $Y_{<i} = (Y_1, \ldots, Y_{i-1})$.
2. Data processing inequality: For any two distributions P and Q and function f, $d(f(P), f(Q)) \le d(P, Q)$.
3. (β, γ)-Pythagorean probability preservation: For two distribution ensembles $(X_i)_i$ and $(Y_i)_i$ over the same finite support $\prod_i \Omega_i$, if
$$d\left((X_i | X_{<i} = a_i), (Y_i | Y_{<i} = a_i)\right) \le \beta$$
for all i and $a_i \in \prod_{j<i} \Omega_j$, then
$$d_{\mathsf{TV}}((X_i)_i, (Y_i)_i) \le \gamma \cdot \left\| \left(\max_{a_i} d((X_i | X_{<i} = a_i), (Y_i | Y_{<i} = a_i)) \right)_i \right\|_2 .$$

The above is a generalization of λ-efficient divergence in [18, 19] so that it also captures the Hellinger distance as a special case.

It is known that the *max-log* distance is $(1/3, 1)$-efficient [18]. Also, the Hellinger distance is $(1, \sqrt{2})$-efficient [26]. The following lemma follows from the proof of Lemma 1 in [26].

Lemma 9. *Let $Q = (Q_1, \ldots, Q_\ell)$ and $P = (P_1, \ldots, P_\ell)$ be probability distribution ensembles over a finite support $\prod_i \Omega_i$. Then,*
$$d_{\mathsf{HD}}(P, Q) \le \sqrt{\ell} \cdot \max_{a_i \in \prod_{j<i} \Omega_j} d_{\mathsf{HD}}(P_i | a_i, Q_i | a_i).$$

We present a sufficient condition under which a distribution ensemble Q can be replaced with P without compromising bit security. Specifically, to preserve λ-bit security, two ensembles should be close enough in $(2^{-\lambda/2}, O(1))$-efficient divergences for search-type games and are close within $2^{-\lambda/2}$ in the Hellinger distance for decision-type games.

Theorem 9. *Let $Q = (Q_i)_i$ and $P = (P_i)_i$ be distribution ensembles over a finite support $\prod_i \Omega_i$.*

1. *If an n-bit security game G^Q with $n > 1$ is λ-bit secure and $d((P_i | P_{<i} = a_i), (Q_i | Q_{<i} = a_i)) \le 2^{-\lambda/2}$ for (β, γ)-efficient divergence d with $\beta \ge 2^{-\lambda/2}$, then G^P is $(\lambda - \alpha)$-bit secure for $\alpha = \max\{2 \log_2(\gamma \cdot \sqrt{\ln(1/\mu)/(1-\mu)}/(1 - 2^{-\rho} - \mu)), \rho + \log_2(\ln(1/\mu)^2/(1-\mu)) + 1\}$ and $\rho > 0$.*

2. *If a* 1*-bit security game* G^Q *is* λ*-bit secure and* $d_{\mathsf{HD}}((P_i|P_{<i} = a_i), (Q_i|Q_{<i} = a_i)) \leq 2^{-\lambda/2}$ *for any* i *and* $a_i \in \prod_{j<i} \Omega_j$*, then* G^P *is* $(\lambda - \alpha)$*-bit secure for* $\alpha = \max\{\log_2(\ln(1/2\mu)/\ln(1/4\mu)) + 3, \log_2 \ln(1/2\mu) + 6, 7\}$.

Proof. First, we show the case that $n > 1$. Let $\delta = \max_{i,a_i} d((P_i|P_{<i} = a_i), (Q_i|Q_{<i} = a_i))$, which is at most $2^{-\lambda/2}$ by assumption. Suppose for contradiction that G^P is not $(\lambda-\alpha)$-bit secure. Theorem 2 implies that there exists an inner adversary A for G^P that runs in time T_A and has success probability $\epsilon^P_A > T_A(1-\mu)/2^{\lambda-\alpha}$. Let N^P be the number of invocations of A by the outer adversary B to achieve $\epsilon^P_{A,B} \geq 1-\mu$. By Lemma 1, N^P is at most $\lceil \ln(1/\mu)/\epsilon^P_A \rceil$. Now consider the success probability $\epsilon^Q_{A,B}$, where the probability distribution P is replaced with Q. Since the number of queries to the distribution ensemble during the inner game is at most T_A, we have

$$\left|\epsilon^P_{A,B} - \epsilon^Q_{A,B}\right| \leq d_{\mathsf{TV}}(P^{N^P}, Q^{N^P}) \leq \gamma \cdot \sqrt{N^P T_A \delta^2},$$

where the last inequality follows from the (β, γ)-Pythagorean probability preservation property of d. It holds that

$$\begin{aligned}
\epsilon^Q_{A,B} &\geq \epsilon^P_{A,B} - \gamma \cdot \sqrt{N^P T_A \delta^2} \\
&> 1 - \mu - \gamma \cdot \sqrt{\frac{\ln(1/\mu)}{\epsilon^P_A} \cdot \frac{\epsilon^P_A \cdot 2^{\lambda-\alpha}}{1-\mu} \cdot \frac{1}{2^\lambda}} \\
&= 1 - \mu - \gamma \cdot \sqrt{\frac{\ln(1/\mu)}{(1-\mu)2^\alpha}} \\
&\geq 2^{-\rho},
\end{aligned}$$

where the last inequality follows by the assumption on α. We can consider the pair of adversaries (A, B) as an inner adversary A' that achieves the success probability $\epsilon_{A'} > 2^{-\rho}$ with computational complexity $T_{A'} = N^P T_A$. Thus, by Theorem 1, the bit security of G^Q is bounded above by

$$\log_2(N^P T_A) + \rho + \log_2 \ln(1/\mu) + 1 < \lambda - \alpha + \rho + \log_2(\ln(1/\mu)^2/(1-\mu)) + 1,$$

which is less than λ by assumption on α. It contradicts the assumption that G^Q is λ-bit secure.

Next, we prove the second case. Let $\delta = \max_{i,a_i} d_{\mathsf{HD}}((P_i|P_{<i} = a_i), (Q_i|Q_{<i} = a_i)) \leq 2^{-\lambda/2}$. Suppose for contradiction that G^P is not $(\lambda-\alpha)$-bit secure. Theorem 2 implies that there exists an inner adversary A for G^P that runs in time T_A and satisfies

$$d_{\mathsf{HD}}(A^P_0, A^P_1) > \min\left\{\frac{1}{\sqrt{2}}, \sqrt{\frac{T_A}{2^{\lambda-\alpha+1}} \cdot \ln(1/4\mu)}\right\} := \omega^P,$$

where A^P_u is the probability distribution of the output of A under the condition that $u \in \{0, 1\}$ is chosen in G^P. We define A^Q_0 and A^Q_1 for G^Q similarly. Since the number of queries to distribution ensembles P/Q is at most T_A, it follows from Lemma 9 and the data processing inequality that for $u \in \{0,1\}$,

$$d_{\mathsf{HD}}(A_u^P, A_u^Q) \leq \sqrt{T_A} \cdot \delta \leq \sqrt{\frac{T_A}{2^\lambda}}.$$

By the triangle inequality, we have

$$\begin{aligned} d_{\mathsf{HD}}(A_0^P, A_1^P) &\leq d_{\mathsf{HD}}(A_0^P, A_0^Q) + d_{\mathsf{HD}}(A_0^Q, A_1^Q) + d_{\mathsf{HD}}(A_1^Q, A_1^P) \\ &\leq d_{\mathsf{HD}}(A_0^Q, A_1^Q) + 2\sqrt{\frac{T_A}{2^\lambda}}. \end{aligned}$$

Thus, $d_{\mathsf{HD}}(A_0^Q, A_1^Q) \geq \omega^P - 2\sqrt{T_A/2^\lambda}$.

Suppose that $\omega^P = \sqrt{T_A \ln(1/4\mu)/2^{\lambda-\alpha+1}}$. Then,

$$\begin{aligned} d_{\mathsf{HD}}(A_0^Q, A_1^Q) &\geq \sqrt{\frac{2\ln(1/2\mu)T_A}{2^\lambda}} \left(\sqrt{\frac{2^{\alpha-2}\ln(1/4\mu)}{\ln(1/2\mu)}} - \sqrt{\frac{2}{\ln(1/2\mu)}} \right) \\ &> \sqrt{\frac{2\ln(1/2\mu)T_A}{2^\lambda}} \end{aligned}$$

by assumption on α. Let $\mathsf{adv}_{A,Q}^{\text{Renyi}}$ be the Rényi advantage of A for the game G^Q. By (2), we have $\mathsf{adv}_{A,Q}^{\text{Renyi}} \geq 2d_{\mathsf{HD}}(A_0^Q, A_1^Q)^2 > 4\ln(1/2\mu)T_A/2^\lambda$. It follows from Theorem 1 that the bit security of G^Q is at most

$$\log_2 T_A + \log_2 \left(1/\mathsf{adv}_{A,Q}^{\text{Renyi}}\right) + \log_2 \ln(1/2\mu) + 2 < \lambda.$$

Next, suppose that $\omega^P = 1/\sqrt{2}$. We have the relation that $d_{\mathsf{TV}}(A_0^P, A_1^P) \geq d_{\mathsf{HD}}(A_0^P, A_1^P)^2 \geq (\omega^P)^2 = 1/2$. Thus, adversary A has success probability $\epsilon_A^P = (1 + d_{\mathsf{TV}}(A_0^P, A_1^P))/2 \geq 3/4$ for G^P. Since we assume that G^P is not $(\lambda-\alpha)$-bit secure, it must be that $N_{A,B} \cdot T_A < 2^{\lambda-\alpha}$, implying that $T_A < 2^{\lambda-\alpha}$. Since the Hellinger distance is $(1, \sqrt{2})$-efficient, we have

$$\left|\epsilon_A^P - \epsilon_A^Q\right| \leq d_{\mathsf{TV}}(P,Q) \leq \gamma \cdot \sqrt{T_A \cdot \delta^2} \leq \sqrt{\frac{2T_A}{2^\lambda}} < \sqrt{\frac{1}{2^{\alpha-1}}} \leq \frac{1}{8},$$

where the last inequality follows from $\alpha \geq 7$. Hence, $\epsilon_A^Q \geq 5/8$. By Theorem 1, the bit security of G^Q is at most

$$\log_2 T_A + \log_2 \ln(1/2\mu) + 6 < \lambda - \alpha + \log_2 \ln(1/2\mu) + 6,$$

which is less than λ by assumption on α.

In both cases, we have shown that G^Q is not λ-bit secure, contradicting the assumption. Hence, the statement follows. □

4.6 Hybrid Arguments

We show that a hybrid argument can be generally applied to decision games in our framework.

Theorem 10. *Let $H_1, \ldots, H_{k+1}$ be distributions over the same finite alphabet. If H_i and H_{i+1} are λ-bit secure indistinguishable for all i, then H_1 and H_{k+1} are $(\lambda - \alpha)$-bit secure indistinguishable for $\alpha = 2\log_2 k + \max\{\log_2(1/2\mu) + 1, 3\}$.*

Proof. Suppose that H_1 and H_{k+1} are not $(\lambda - \alpha)$-bit secure indistinguishable. Theorem 2 implies that there exists an inner adversary A that runs in time T_A and satisfies

$$d_{\mathsf{HD}}(A_1, A_{k+1}) > x = \min\left\{\frac{1}{\sqrt{2}}, \sqrt{\frac{T_A}{2^{\lambda-\alpha+1}} \cdot \ln(1/4\mu)}\right\},$$

where A_i is the output distribution of A on input H_i. By the triangle inequality, we have

$$x < d_{\mathsf{HD}}(A_1, A_{k+1}) \leq \sum_{i=1}^{k} d_{\mathsf{HD}}(A_i, A_{i+1}).$$

There must be some i such that $d_{\mathsf{HD}}(A_i, A_{i+1}) > x/k$. Let A^u be the output distribution of A when $u \in \{0,1\}$ was chosen. By (2), the Rényi advantage of A for distinguishing A_i from A_{i+1} satisfies

$$\mathsf{adv}_A^{\mathrm{Renyi}} = D_{1/2}(A^0 \| A^1) \geq 2 d_{\mathsf{HD}}(A_i, A_{i+1})^2 > 2(x/k)^2.$$

By Theorem 1, the bit security $\mathrm{BS}^{\mu}_{i,i+1}$ for distinguish A_i from A_{i+1} satisfies

$$\mathrm{BS}^{\mu}_{i,i+1} < \log_2 T_A + 2\log_2(k/x) + \log_2(1/2\mu) + 1.$$

Suppose $x = 1/\sqrt{2}$. Since H_1 and H_{k+1} are not $(\lambda - \alpha)$-bit secure, we have $2^{\lambda-\alpha} > N_{A,B} \cdot T_A \geq T_A$. Thus, $\mathrm{BS}^{\mu}_{i,i+1} < \lambda - \alpha + 2\log_2 k + \log_2(1/2\mu) + 1 \leq \lambda$. Suppose $x = \sqrt{(T_A/2^{\lambda-\alpha+1})\ln(1/4\mu)}$. Then,

$$\begin{aligned}\mathrm{BS}^{\mu}_{i,i+1} &< \log_2 T_A + 2\log_2 k - \log_2 T_A + \lambda - \alpha + 1 - \log_2(1/4\mu) + \log_2(1/2\mu) + 1 \\ &\leq \lambda.\end{aligned}$$

In both cases, we have $\mathrm{BS}^{\mu}_{i,i+1} < \lambda$, which contradicts the assumption that H_i and H_{i+1} are λ-bit secure indistinguishable. □

Acknowledgements The work of S.W. was supported in part by JSPS KAKENHI under Grant 20H02144.

References

1. N. Alon, O. Goldreich, J. Hastad, and R. Peralta. Simple construction of almost k-wise independent random variables. *Random Structures and Algorithms*, 3(3):289–304, 1992.
2. S. Bai, A. Langlois, T. Lepoint, D. Stehlé, and R. Steinfeld. Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. In T. Iwata and J. H. Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 3–24. Springer, 2015.
3. D. J. Bernstein and T. Lange. Non-uniform cracks in the concrete: The power of free precomputation. In K. Sako and P. Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part II*, volume 8270 of *Lecture Notes in Computer Science*, pages 321–340. Springer, 2013.
4. A. Bogdanov, S. Guo, D. Masny, S. Richelson, and A. Rosen. On the hardness of learning with rounding over small modulus. In E. Kushilevitz and T. Malkin, editors, *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part I*, volume 9562 of *Lecture Notes in Computer Science*, pages 209–224. Springer, 2016.
5. T. M. Cover and J. A. Thomas. *Elements of Information Theory.* John Wiley & Sons, 2nd edition, 2006.
6. A. De, L. Trevisan, and M. Tulsiani. Time space tradeoffs for attacks against one-way functions and prgs. In T. Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*, pages 649–665. Springer, 2010.
7. Y. Dodis and J. P. Steinberger. Message authentication codes from unpredictable block ciphers. In S. Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*, pages 267–285. Springer, 2009.
8. C. A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inform. Theory*, 45(4):1216–1227, May 1999.
9. O. Goldreich. *The Foundations of Cryptography - Volume 1: Basic Techniques.* Cambridge University Press, 2001.
10. O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In D. S. Johnson, editor, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washigton, USA*, pages 25–32. ACM, 1989.
11. F. Götze, H. Sambale, and A. Sinulis. Higher order concentration for functions of weakly dependent random variables. *Electronic Journal of Probability*, 24(85):1–19, 2019.
12. M. Iwamoto and J. Shikata. Information theoretic security for encryption based on conditional Rényi entropies. In C. Padró, editor, *Information Theoretic Security - 7th International Conference, ICITS 2013, Singapore, November 28-30, 2013,*

Proceedings, volume 8317 of *Lecture Notes in Computer Science*, pages 103–121. Springer, 2013.

13. N. Koblitz and A. Menezes. Another look at non-uniformity. *Groups Complex. Cryptol.*, 5(2):117–139, 2013.
14. L. Kowalczyk, T. Malkin, J. R. Ullman, and M. Zhandry. Strong hardness of privacy from weak traitor tracing. In M. Hirt and A. D. Smith, editors, *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part I*, volume 9985 of *Lecture Notes in Computer Science*, pages 659–689, 2016.
15. A. Langlois, D. Stehlé, and R. Steinfeld. Gghlite: More efficient multilinear maps from ideal lattices. In P. Q. Nguyen and E. Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 239–256. Springer, 2014.
16. L. A. Levin. Randomness and non-determinism. *Journal of Symbolic Logic*, 58(3):1102–1103, 1993.
17. T. Matsuda, K. Takahashi, T. Murakami, and G. Hanaoka. Improved security evaluation techniques for imperfect randomness from arbitrary distributions. In D. Lin and K. Sako, editors, *Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part I*, volume 11442 of *Lecture Notes in Computer Science*, pages 549–580. Springer, 2019.
18. D. Micciancio and M. Walter. Gaussian sampling over the integers: Efficient, generic, constant-time. In J. Katz and H. Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 455–485. Springer, 2017.
19. D. Micciancio and M. Walter. On the bit security of cryptographic primitives. In J. B. Nielsen and V. Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 3–28. Springer, 2018.
20. I. Mironov. Rényi differential privacy. In *30th IEEE Computer Security Foundations Symposium, CSF 2017, Santa Barbara, CA, USA, August 21-25, 2017*, pages 263–275. IEEE Computer Society, 2017.
21. J. Naor and M. Naor. Small-bias probability spaces: Efficient constructions and applications. *SIAM Journal of Computing*, 22(4):838–856, 1993.
22. T. Prest. Sharper bounds in lattice-based cryptography using the Rényi divergence. In T. Takagi and T. Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 347–374. Springer, 2017.
23. I. Sason and S. Verdú. f-divergence inequalities. *IEEE Trans. Inform. Theory*, 62(11):5973–6006, November 2016.
24. K. Takashima and A. Takayasu. Tighter security for efficient lattice cryptography via the Rényi divergence of optimized orders. In M. H. Au and A. Miyaji, editors, *Provable Security - 9th International Conference, ProvSec 2015, Kanazawa, Japan,*

November 24-26, 2015, Proceedings, volume 9451 of *Lecture Notes in Computer Science*, pages 412–431. Springer, 2015.

25. T. van Erven and P. Harremoës. Rényi divergence and Kullback-Leibler divergence. *IEEE Trans. Inform. Theory*, 60(7):3797–3820, July 2014.
26. K. Yasunaga. Replacing probability distributions in security games via Hellinger distance. In S. Tessaro, editor, *2nd Conference on Information-Theoretic Cryptography (ITC 2021)*, volume 199 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 17:1–17:15, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.