Unified View for Notions of Bit Security

Shun Watanabe[1] and Kenji Yasunaga[2]

[1] Tokyo University of Agriculture and Technology, Japan
shunwata@cc.tuat.ac.jp
[2] Tokyo Institute of Technology, Japan
yasunaga@c.titech.ac.jp

Abstract. We study the framework of Watanabe and Yasunaga (Asiacrypt 2021) that enables us to evaluate the bit security of cryptographic primitives/games with an operational meaning. First, we observe that their quantitative results preserve even if adversaries are allowed to output the failure symbol in games. With this slight modification, we show that their framework evaluates the advantage of adversaries more pessimistically than that of Micciancio and Walter (Eurocrypt 2018). Also, we prove the optimality of the Goldreich-Levin hard-core predicate by employing the reduction algorithm of Hast (J. Cryptology, 2004). These two results resolve open problems that remained.
We demonstrate that all games we need to care about in their framework are decision games. Namely, we show that for every search game G, there is the corresponding decision game G' such that G has λ-bit security if and only if G' has λ-bit security. The game G' consists of the real and the ideal games, where attacks in the ideal game are never approved. Such games often appear in game-hopping security proofs. The result justifies such security proofs because they lose no security. Finally, we provide a distribution replacing theorem. Suppose that a game using distribution Q in a black-box manner is λ-bit secure, and two distributions P and Q are computationally λ-bit secure indistinguishable. In that case, the game where Q is replaced by P is also λ-bit secure.

Keywords: Bit Security · Operational Approach · Goldreich-Levin Theorem.

1 Introduction

Quantifying the security levels of cryptographic primitives is a significant task both for theoreticians and practitioners around information security and cryptography. The evaluations directly affect using cryptographic primitives in our daily lives. We usually say that primitive P has λ-bit security (or security level λ) if we need 2^λ operations to break P. Although the statement is simple, we encounter difficulties formalizing such security levels exactly.

For example, suppose that an encryption scheme Π is proven to be secure, assuming some computational assumption X and a secure signature scheme S. We expect that if both X and S have λ-bit security, then Π also has λ-bit security.

In the cryptographic literature, we instead discuss the *advantages* of the primitives, say $\mathsf{adv}_{\varPi} \leq \mathsf{adv}_X + \mathsf{adv}_S$, where $\mathsf{adv}_{\varPi}, \mathsf{adv}_X, \mathsf{adv}_S$ are the advantages of the adversary for scheme $\varPi$, assumption X, and scheme S, respectively. However, we have not paid much attention to the precise interpretation of these advantages. While adv_S for signature scheme S is usually defined as the winning probability in the forgery game, $\mathsf{adv}_{\varPi}$ for encryption scheme $\varPi$ is different from the winning probability p in the IND-CPA game and is defined as $\mathsf{adv}_{\varPi} = |2p-1|$. Hence, even if we can suppose that $\mathsf{adv}_S \leq 2^{-\lambda}$ and $\mathsf{adv}_X \leq 2^{-\lambda}$ (thus $\mathsf{adv}_{\varPi} \leq 2^{-\lambda+1}$), we cannot say that $\varPi$ has λ-bit security because of λ-bit security of S and X.

The difficulty mentioned above stems from the unclarity of the interpretation of advantage for decision games. In order to clarify the subtlety, let us consider the following decision game to distinguish between the pseudorandom number generator (PRG) and the true random number generator (TRG): the outcome (y, z) of PRG consists of the image $y = f(x)$ of a one-way permutation f over $\{0,1\}^n$ and its hard-core predicate $z = h(x)$; the outcome (y, z) of TRG consists of $y = f(x)$ and a random bit $z = \sigma$ that is independent of the seed x. For this game, we can consider the following two possible attacks:

1. *Linear test attack*: For a prescribed binary vector v of length $n+1$, the adversary computes the inner product of v and (y, z); if the outcome is 0, the adversary outputs 0 (PRG); and outputs 1 (TRG) otherwise. For such an attack, the output distribution A_u of the adversary A given $u \in \{0,1\}$ ($u = 0$ for PRG and $u = 1$ for TRG) are $A_0 = (1/2 + \varepsilon_1, 1/2 - \varepsilon_1)$ and $A_1 = (1/2, 1/2)$ for some bias ε_1. How much bit security does the PRG have against this attack? Note that the (standard) advantage of this attack is ε_1.
2. *Inversion attack*: First, the adversary tries to invert the one-way permutation, which will succeed with probability ε_2. If the inversion is successful and $h(x)$ coincides with z, the adversary outputs 0 (PRG); otherwise (the inversion is unsuccessful or $h(x) \neq z$), the adversary outputs 1 (TRG). For such an attack, the output distribution of the adversary A given $u \in \{0,1\}$ are $A_0 = (\varepsilon_2, 1 - \varepsilon_2)$ and $A_1 = (\varepsilon_2/2, 1 - \varepsilon_2/2)$. How much bit security does the PRG have against this attack? Note that the (standard) advantage of this attack is $\varepsilon_2/2$.

It is known that, for an appropriately chosen vector v, the advantage of the linear test can be $\varepsilon_1 \geq 2^{-n/2}$ (cf. [1, 6]). Since we expect that the bit security of PRG for seed length n is close to n, should we define the bit security for a given level of advantage ε as $\log(1/\varepsilon^2)$? However, if we define the bit security as such, then the bit security against the inversion attack would be $2n$ if $\varepsilon_2 \simeq 1/2^n$, i.e., random guess is the best possible strategy of the adversary; this is unnatural since the seed length is n. Thus, these attacks suggest that the commonly used notion of advantage may not be appropriate to evaluate bit security.

In order to circumvent the subtlety mentioned above in defining the bit security for decision games, Micciancio and Walter [15] introduced an alternative definition of advantage (see (7)). Their notion of bit security was defined based on this advantage. Even though the results obtained by their definition of bit security match our intuition, the definition lacks an operational meaning.

In [18], Watanabe and Yasunaga introduced a framework for evaluating the security level of primitives with operational meanings. In their framework, there are two types of adversaries attacking a security game G. The *inner* adversary A plays a usual security game G. The *outer* adversary B invokes A sufficiently many times to achieve the winning probability close to one. If the total computational cost needed to achieve this task is 2^λ, game G is said to be λ-bit secure. Notably, they characterized their notion by advantages. They showed that the bit security of game G is approximated by $\min_A\{\log_2(T_A/\mathsf{adv}_A)\}$, where T_A is the computational cost of adversary A and adv_A is equal to the winning probability of A in G for *search* games and is the *Rényi advantage* of A for *decision* games. The Rényi advantage was introduced in [18] and is defined as the Rényi divergence of order $1/2$ between the output distributions of two cases in the decision game. Their framework gives an operational interpretation of these advantages in security games.

Several problems remained open in [18]. Regarding the Goldreich-Levin theorem [9, 8], they proved that a λ-bit secure one-way function gives a λ-bit secure hard-core predicate against *balanced* adversaries. The balanced adversaries are restricted such that the probability of outputting each value (0 or 1) must be at least constant. An example is a linear test attack described above; when $u = 1$ (TRG), the test (adversary) outputs 0 and 1 with probability $1/2$, a constant. Such adversaries, however, may not be typical in security proofs. The inversion attack described above is typical in many security proofs. Since the success probability of inversion is usually small and close to zero, the attack is not balanced. Removing the balanced-adversary condition in the Goldreich-Levin theorem has been an open problem. The result was in contrast to the framework of Micciancio and Walter [15], where they showed that the Goldreich-Levin reduction [9, 8] was indeed optimal.

Another open problem was the relationship between the two frameworks [15, 18]. Although finding similar features in the two definitions seems complicated, they mostly share the same quantitative results. The exception was the Goldreich-Levin theorem as described above. Clarifying the relation is helpful for researchers analyzing and evaluating concrete cryptographic primitives.

1.1 Our Results

In this work, we further study the framework of [18] and resolve open problems. First, we observe that the results of [18] preserve even if inner adversaries for decision games are allowed to output the failure symbol $\perp$ as well as $\{0, 1\}$. See Section 3 for the details. This slight modification reveals a relation between the bit security notions of [18] and [15]. We show that the advantage of [15], which we term conditional squared advantage (CS advantage), for decision games is bounded above by that of [18] (Rényi advantage). In other words, the Rényi advantage evaluates adversaries in a more "pessimistic" way than the CS advantage. If decision primitive P has λ-bit security in [18], P also has λ-bit security in [15]. The converse is not necessarily true (see Section 8). We also demonstrate that several existing notions of advantages [14, 12, 15] can be captured in a unified way. Specifically, the three quantities in [14, 12, 15] are the same except for a constant factor. Based on this equivalence, we show that the reduction algorithm of Hast [12] gives a tight reduction of the Goldreich-Levin hard-core predicate [9] to the hardness of one-way functions. Namely, we resolved another open problem that remained in [18].

In addition to the above, we give several results regarding the framework of [18]. We show that every search game can be replaced by a specific decision game, named a *canonical* game. Specifically, we show that a search game has λ-bit security if and only if the corresponding canonical game has λ-bit security. In canonical games, while the adversary plays as usual in the real game, attacks by the adversary will never be approved in the ideal game. This treatment of adversaries often appears in game-hopping security proofs [17, 3]; e.g., the adversary may play a game where every forgery of the signature cannot be approved. Our result may justify such a treatment in security proofs because such game-hopping loses no security. We also provide a distribution replacing theorem. Suppose that game G^Q using black-box access to distribution Q is λ-bit secure and two distributions P and Q are λ-bit secure indistinguishable. The theorem asserts that game G^P, where distribution Q is replaced by P, is also λ-bit secure. This result is a generalization of [18, Theorem 9], where the sufficient condition is that distributions P and Q are information-theoretically close enough in the Hellinger distance. Our result relaxed the requirement into the computational one. It guarantees that λ-bit secure indistinguishability is sufficient for preserving the λ-bit security of games. As an instance, we apply the theorem to the leftover hash lemma (LHL) [5, 13] and show that the seed of a λ-bit secure randomness extractor using universal hash functions can be safely replaced by the output of a λ-bit secure PRG. As a side result (and maybe implicit from [18]), we show that the entropy loss in the LHL to preserve λ-bit security in the framework of [18] is just λ.

1.2 Related Work

Micciancio and Walter [15] initiated the theoretical study of quantifying the security level of cryptographic primitives. They proposed a framework for evaluating the bit security based on the Shannon entropy and the mutual information. A key novelty of their framework was allowing the adversary to output the failure symbol $\perp$ in security games. They showed that their notion of bit security could be characterized by the advantage introduced by Levin [14]. Levin's notion appeared in evaluating the security of the hard-core predicate of Goldreich and Levin [9]. Hast [12] studied efficient reduction algorithms for improving the Goldreich-Levin theorem against nearly one-sided adversaries.

Watanabe and Yasunaga [18] introduced another framework for quantifying the bit security of games with an operational meaning. One of their contributions was characterizing the bit security using the Rényi advantage and giving an operational interpretation of it. The usual advantage of $|2p - 1|$ for the winning probability p in decision games may behave differently from the Rényi advantage, according to the discussion in [18]. Our study mainly relies on their framework to evaluate bit security. A small but crucial difference is that we allow the adversary to output the failure symbol in the game. The modification enables us to unify several existing notions of advantages [14, 12, 15], reveal the relation to the framework of [15], and give an optimal reduction algorithm for the Goldreich-Levin theorem.

The entropy loss of randomness extractors is inevitable [16]. The LHL-based extractors achieve an optimal entropy loss of $2\log(1/\varepsilon)$ for closeness ε to the uniform distribution in the total variation distance. Barak et al. [2] studied the possibilities of reducing the loss to $\log(1/\varepsilon)$ for several primitives. It is shown in [19] that the same reduction of the entropy loss can be achieved for all primitives when using the bit security framework of [15]. In other words, a λ-bit entropy loss in LHL is sufficient to preserve λ-bit security in bit security of [15]. In this work, we explicitly state that the same thing also holds in the framework of [18].

2 Preliminaries

In this section, 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

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

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

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

where the last inequality holds if $d_{\mathsf{HD}}(P,Q)^2 \le 1/2$. We have the following lemma.

Lemma 1. *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]. □

3 Bit Security Framework of [18]

An n-bit game $G = (X, R, \{O_\theta\}_\theta)$, played by an inner adversary A and an outer adversary B, consists of an algorithm X, a Boolean function R, and oracles $\{O_\theta\}_\theta$. The success probability of A is

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

We consider two types of games: decision games ($n = 1$) and search games ($n \gg 1$). The success probability of the pair (A, B) is defined depending on the game type. For decision games, the success probability of (A, B) is

$$\varepsilon^{\mathrm{decn}}_{A,B} = \Pr\left[u \xleftarrow{R} \{0,1\}; b \leftarrow B^{O^{\mathrm{decn}}_A} : b = u\right], \tag{3}$$

where O^{decn}_A is the oracle that, given the ith query, computes $x_i \leftarrow X(u)$ and replies with $a_i \leftarrow A_i^{\{O_\theta(\cdot)\}_\theta}(x_i)$. For search games, the success probability of (A, B) is

$$\varepsilon^{\mathrm{srch}}_{A,B} = \Pr\left[\{(j, a_j)\}_j \leftarrow B^{O^{\mathrm{srch}}_A} : \exists i, (i, a_i) \in b \wedge R(u_i, x_i, a_i) = 1\right], \tag{4}$$

where O^{srch}_A 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 $a_i \leftarrow A_i^{\{O_\theta(\cdot)\}_\theta}(x_i)$.

Let T_A denote the computational complexity for running the experiment $\left[u \xleftarrow{R} \{0,1\}^n; x \leftarrow X(u); a \leftarrow A^{\{O_\theta(\cdot)\}_\theta}(x)\right]$. For simplicity, we call T_A the computational complexity (or cost) of A. The bit security of an n-bit game $G = (X, R, \{O_\theta\}_\theta)$ for error probability μ is defined to be

$$\begin{aligned}\mathrm{BS}^\mu_G &:= \min_{A,B} \{\log_2(N_{A,B} \cdot T_A) : \varepsilon_{A,B} \geq 1 - \mu\} \\ &= \min_A \left\{\log_2 T_A + \log_2 \min_B \{N_{A,B} : \varepsilon_{A,B} \geq 1 - \mu\}\right\},\end{aligned}$$

where $N_{A,B}$ is the number of invocations to A made by the outer adversary B and $\varepsilon_{A,B}$ is $\varepsilon^{\mathrm{decn}}_{A,B}$ for $n = 1$, and is $\varepsilon^{\mathrm{srch}}_{A,B}$ for $n \gg 1$. We say G has λ-bit security if $\mathrm{BS}^\mu_G \geq \lambda$.

Roughly speaking, the bit security of the game is at least λ if the computational complexity of the adversary for achieving the success probability $1-\mu$ is at least 2^{λ}. The bit security is defined without taking into account the computational complexity of B. The reason is that the complexity of B can be relatively small compared to the total computational complexity; See [18] for details.

In [18], the authors showed that the bit security of decision games could be characterized by the *Rényi advantage*, which is defined as

$$\mathsf{Adv}^{\mathrm{Renyi}}_{G,A} := D_{1/2}(A_0 \| A_1),$$

where A_u is the output distribution of A in game G under the condition that $u \in \{0,1\}$ is chosen in the game. For the case of search games, the bit security is characterized by the winning probability of A as usual. When we want to emphasize that A_u is the conditional distribution of the output of A given secret value $U=u$, we denote $P_{A|U}(\cdot|u)$. We use A_u and $P_{A|U}(\cdot|u)$ interchangeably in the rest of the paper.

In [18], the bit security was defined based on a game in which an inner adversary outputs $a \in \{0,1\}^n$. However, the general results in [18, Section 3] do not depend on the fact that $a \in \{0,1\}^n$. Thus, for the convenience of relating the bit security defined in [18] with another one in [15], we allow an inner adversary to output the abort symbol $\perp$. However, we restrict our attention to an inner adversary that aborts obliviously to the value of secret $u \in \{0,1\}^n$, i.e., $P_{A|U}(\perp|u)$ does not depend on u. This assumption of oblivious abortion is consistent with [15, Theorem 1]. To fix ideas, for a given one-way permutation $f(x)$, let us consider an adversary distinguishing whether the next bit is a hard-core predicate $z=h(x)$ of $f(x)$, which corresponds to $u=0$, or a random bit $z=\sigma$ that is independent of $f(x)$, which corresponds to $u=1$; see Section 5.1 for a more detailed description of the hard-core predicate game. Suppose that the adversary first tries to invert $f(x)$ to obtain x with success probability ν. If the inversion is succeeded and $h(x)=z$, then the adversary outputs $a=0$ as an estimate of u; if the inversion is succeeded but $h(x)\neq z$, then the adversary outputs $a=1$ as an estimate of u; if the inversion is failed, then the adversary outputs $\perp$. In this case, the adversary abort with probability $1-\nu$ obliviously to the value of u.

4 Rényi Advantage and Conditional Squared Advantage

This section discusses the connection between the Rényi advantage and the advantage used in [15], which we term the conditional squared (CS) advantage. The former was used in [18] to characterize their notion of bit security for decision games; on the other hand, the latter was used in [15] to characterize their notion of bit security for decision games.

Let $\psi : \{0, 1, \perp\} \to \{1, 0, -1\}$ be the function given by $\psi(0) = 1$, $\psi(1) = -1$, and $\psi(\perp) = 0$. Then, we define (see also Appendix A)

$$\begin{aligned}\mathsf{Adv}_A^{\mathrm{CS}} &:= \mathbb{E}\left[\frac{\psi(A)}{\sqrt{\mathbb{E}[\psi(A)^2]}}\psi(U)\right]^2 && (5)\\ &= \frac{4\left(\Pr(A = U) - \frac{1}{2}\Pr(A \neq \perp)\right)^2}{\Pr(A \neq \perp)} && (6)\\ &= \Pr(A \neq \perp)\big(2\Pr(A = U|A \neq \perp) - 1\big)^2. && (7)\end{aligned}$$

It can be verified that $0 \leq \mathsf{Adv}_A^{\mathrm{CS}} \leq 1$. Historically speaking, the expression (5) was introduced by Levin in [14]; the expression (6) was introduced (up to the constant factor of 4) by Hast in [12, Theorem 3] to characterize the success probability of the modified Goldreich-Levin algorithm; Micciancio and Walter introduced the expression (7) in [15, Theorem 1, Definition 10], and they initiated the use of this quantity as an advantage to characterize their notion of bit security.

By the oblivious abortion assumption, we have

$$\delta := \Pr(A \neq \perp) = \Pr(A \neq \perp \mid U = 0) = \Pr(A \neq \perp \mid U = 1).$$

Thus, denoting the conditional distribution of A given U and the event $\mathcal{E} = \{A \neq \perp\}$ as $P_{A|U\mathcal{E}}(a|u) = P_{A|U}(a|u)/\delta$, we have

$$d_{\mathsf{TV}}(P_{A|U}(\cdot|0), P_{A|U}(\cdot|1)) = \delta d_{\mathsf{TV}}(P_{A|U\mathcal{E}}(\cdot|0), P_{A|U\mathcal{E}}(\cdot|1)). \tag{8}$$

We also note that

$$\big(2\Pr(A = U|A \neq \perp) - 1\big)^2 = d_{\mathsf{TV}}(P_{A|U\mathcal{E}}(\cdot|0), P_{A|U\mathcal{E}}(\cdot|1))^2 \tag{9}$$

For later use in Section 5.1, we provide a variant of (8) for the Rényi divergence of order 1/2.

Lemma 2. *It holds that*

$$D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1)) \leq \delta D_{1/2}(P_{A|U\mathcal{E}}(\cdot|0)\|P_{A|U\mathcal{E}}(\cdot|1)).$$

Proof. Note that

$$P_{A|U}(a|u) = \delta P_{A|U\mathcal{E}}(\cdot|0)\mathbf{1}[a \neq \perp] + (1 - \delta)\mathbf{1}[a = \perp].$$

Thus, the claim follows from the joint convexity of the Rényi divergence of order 1/2; e.g., see [7, Theorem 11]. □

We close this section by presenting a connection between the Rényi advantage and the CS advantage.

Theorem 1. *For an arbitrary adversary A for decision games, it holds that*

$$\mathsf{Adv}_A^{\mathrm{CS}} \le \mathsf{Adv}_A^{\mathrm{Renyi}}.$$

Proof. From the leftmost inequality of (2), we have

$$\mathsf{Adv}_A^{\mathrm{Renyi}} = D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1)) \ge 2d_{\mathsf{HD}}(P_{A|U}(\cdot|0), P_{A|U}(\cdot|1))^2.$$

Here, note that

$$\begin{aligned} d_{\mathsf{HD}}(P_{A|U}(\cdot|0), P_{A|U}(\cdot|1))^2 &= 1 - \sum_{a \in \{0,1,\perp\}} \sqrt{P_{A|U}(a|0)P_{A|U}(a|1)} \\ &= 1 - (1-\delta) - \delta \sum_{a \in \{0,1\}} \sqrt{P_{A|U\mathcal{E}}(a|0)P_{A|U\mathcal{E}}(a|1)} \\ &= \delta d_{\mathsf{HD}}(P_{A|U\mathcal{E}}(\cdot|0), P_{A|U\mathcal{E}}(\cdot|1))^2. \end{aligned}$$

Furthermore, by using the right inequality of (1) and by noting (9), we have

$$\begin{aligned} 2\delta d_{\mathsf{HD}}(P_{A|U\mathcal{E}}(\cdot|0), P_{A|U\mathcal{E}}(\cdot|1))^2 &\ge \delta d_{\mathsf{TV}}(P_{A|U\mathcal{E}}(\cdot|0), P_{A|U\mathcal{E}}(\cdot|1))^2 \\ &= \mathsf{Adv}_A^{\mathrm{CS}}, \end{aligned}$$

which completes the proof. □

Theorem 1 implies that, up to a constant bit, if a decision game is λ bit secure in [18], then it is also λ bit secure in the sense of [15]. It is not clear if the opposite implication holds; however, in Section 5.1, we show the opposite implication for a specific game of the hard-core predicate.

5 Hard-Core Predicate Game

5.1 Distinguisher and Predictor

For a one-way function $f : \{0,1\}^n \to \{0,1\}^m$, a function $h : \{0,1\}^n \to \{0,1\}$ is termed a hard-core predicate if the value of $h(x)$ cannot be predicted from the function output $f(x)$. When we discuss the security of the hard-core predicate, there are two types of formulations: the prediction game and the distinguishing game. Even though it is more common to define the security of the hard-core predicate in terms of the prediction game, since the distinguishing game is more suitable for our formulation of the bit security, we first introduce the distinguishing game and later discuss the connection between the two formulations.

In the distinguishing game of hard-core predicate, when $u = 0$, an inner adversary A observes $(f(x), h(x))$ for random $x \in \{0,1\}^n$; when $u = 1$, the inner adversary A observes $(f(x), \sigma)$, where σ is a random bit that is independent of x. Based on the observation, the inner adversary A outputs an estimate a of u or $\perp$. Then, the outer adversary B invokes the inner adversary $N_{A,B}$ times so that the success probability $\varepsilon_{A,B}$ of estimating u is at least $1 - \mu$. The bit security of the hard-core predicate is defined as the minimum of $\log_2(N_{A,B} \cdot T_A)$ under the constraint $\varepsilon_{A,B} \geq 1 - \mu$, where T_A is the cost of the inner adversary.

On the other hand, in the prediction game of hard-core predicate, a predictor $\mathcal{P}$ observes $f(x)$, and outputs an estimate of $h(x)$ or $\perp$. Following the terminology in [12], a predictor $\mathcal{P}$ is said to be an (ε, δ)-predictor if the *rate* is

$$\delta = \Pr(\mathcal{P}(f(x)) \neq \perp)$$

and the *advantage* is

$$\varepsilon = \Pr(\mathcal{P}(f(x)) = h(x)) - \frac{1}{2} \Pr(\mathcal{P}(f(x)) \neq \perp).$$

In other words, (ε, δ)-predictor $\mathcal{P}$ has CS advantage $\mathsf{Adv}_{\mathcal{P}}^{\mathrm{CS}} = \frac{4\varepsilon^2}{\delta}$.

The following theorem connects the Rényi advantage of the distinguishing game and the CS advantage of the prediction game.

Theorem 2. *For a given one-way function f with hard-core predicate h, let A be an inner adversary for the hard-core predicate distinguishing game. Then, there exists a predictor $\mathcal{P}$ of the hard-core predicate that invokes A once and*

$$\mathsf{Adv}_{\mathcal{P}}^{\mathrm{CS}} \geq \frac{1}{2} \mathsf{Adv}_{A}^{\mathrm{Renyi}}. \tag{10}$$

Proof. Using adversary A, similarly to [12, Section 6], we construct a predictor as follows. Let $P_{A|U}(\cdot|u)$ be the distribution of the output of A given u, i.e.,

$$P_{A|U}(a|0) = \Pr(A(f(x), h(x)) = a),$$
$$P_{A|U}(a|1) = \Pr(A(f(x), \sigma) = a).$$

Since the inner adversary A aborts obliviously to the value of u, the probability of no abortion satisfies

$$\delta_0 := P_{A|U}(0|0) + P_{A|U}(1|0) = P_{A|U}(0|1) + P_{A|U}(1|1)$$

For $a, u \in \{0, 1\}$, let

$$P_{A|U\mathcal{E}}(a|u) := \frac{P_{A|U}(a|u)}{\delta_0}$$

be the conditional distribution of the inner adversary provided that it does not abort. Without loss of generality, we can assume $P_{A|U\mathcal{E}}(0|0) \geq P_{A|U\mathcal{E}}(0|1)$.[3] We consider two cases separately.

When $P_{A|U\mathcal{E}}(0|1) \leq \frac{1}{2}$: In this case, we consider the following predictor $\mathcal{P}$. First, we sample the uniform random bit σ. Second,

- If $A(f(x), \sigma) = 0$, then $\mathcal{P}$ outputs σ;

[3] If not, we can flip the outputs 0 and 1 of A.

– If $A(f(x),\sigma) \in \{1,\perp\}$, then $\mathcal{P}$ outputs $\perp$.

The rate of this predictor is

$$\begin{aligned}\delta &= \Pr(\mathcal{P}(f(x)) \neq \perp)\\ &= \Pr(A(f(x),\sigma)=0)\\ &= P_{A|U}(0|1).\end{aligned}$$

On the other hand, the success probability of the predictor is

$$\begin{aligned}\Pr(\mathcal{P}(f(x))=h(x)) &= \Pr(\sigma=h(x))\Pr(A(f(x),\sigma)=0|\sigma=h(x))\\ &= \Pr(\sigma=h(x))\Pr(A(f(x),h(x))=0)\\ &= \frac{P_{A|U}(0|0)}{2}.\end{aligned}$$

Thus, the advantage of this predictor is

$$\begin{aligned}\varepsilon &= \Pr(\mathcal{P}(f(x))=h(x)) - \frac{1}{2}\Pr(\mathcal{P}(f(x))\neq\perp)\\ &= \frac{P_{A|U}(0|0)-P_{A|U}(0|1)}{2}.\end{aligned}$$

From Lemmas 2 and 1, we have

$$\begin{aligned}D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1)) &\leq \delta_0 D_{1/2}(P_{A|U\mathcal{E}}(\cdot|0)\|P_{A|U\mathcal{E}}(\cdot|1))\\ &\leq 2\delta_0\beta^{-1}d_{\mathsf{TV}}(P_{A|U\mathcal{E}}(\cdot|0),P_{A|U\mathcal{E}}(\cdot|1))^2 \qquad (11)\end{aligned}$$

for $\beta = \min[P_{A|U\mathcal{E}}(0|1), P_{A|U\mathcal{E}}(1|1)] = P_{A|U\mathcal{E}}(0|1)$. By using (11) and by noting

$$d_{\mathsf{TV}}(P_{A|U\mathcal{E}}(\cdot|0),P_{A|U\mathcal{E}}(\cdot|1)) = P_{A|U\mathcal{E}}(0|0) - P_{A|U\mathcal{E}}(0|1),$$

we have

$$\begin{aligned}\frac{\varepsilon^2}{\delta} &= \frac{(P_{A|U}(0|0)-P_{A|U}(0|1))^2}{4P_{A|U}(0|1)}\\ &= \frac{\delta_0(P_{A|U\mathcal{E}}(0|0)-P_{A|U\mathcal{E}}(0|1))^2}{4P_{A|U\mathcal{E}}(0|1)}\\ &= \frac{\delta_0 d_{\mathsf{TV}}(P_{A|U\mathcal{E}}(\cdot|0),P_{A|U\mathcal{E}}(\cdot|1))^2}{4\beta}\\ &\geq \frac{1}{8}D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1)),\end{aligned}$$

which implies (10).

When $P_{A|U\mathcal{E}}(0|1) > \frac{1}{2}$: In this case, we consider the following predictor. First, we sample the uniform random bit σ. Second,

– If $A(f(x),\sigma) \in \{0,\perp\}$, then $\mathcal{P}$ outputs $\perp$;

– If $A(f(x),\sigma)=1$, then $\mathcal{P}$ outputs $\sigma\oplus 1$.

The rate of this predictor is

$$\begin{aligned}\delta &= \Pr(\mathcal{P}(f(x))\neq\bot)\\ &= \Pr(A(f(x),\sigma)=1)\\ &= P_{A|U}(1|1).\end{aligned}$$

On the other hand, the success probability of this predictor is

$$\begin{aligned}\Pr(\mathcal{P}(f(x))=h(x)) &= \Pr(\sigma=h(x)\oplus 1, A(f(x),\sigma)=1)\\ &= \Pr(A(f(x),\sigma)=1)-\Pr(\sigma=h(x),A(f(x),\sigma)=1)\\ &= P_{A|U}(1|1)-\Pr(\sigma=h(x))\Pr(A(f(x),\sigma)=1|\sigma=h(x))\\ &= P_{A|U}(1|1)-\Pr(\sigma=h(x))\Pr(A(f(x),h(x))=1)\\ &= P_{A|U}(1|1)-\frac{P_{A|U}(1|0)}{2}.\end{aligned}$$

Thus, the advantage of this predictor is

$$\begin{aligned}\varepsilon &= \Pr(\mathcal{P}(f(x))=h(x))-\frac{1}{2}\Pr(\mathcal{P}(f(x))\neq\bot)\\ &= \frac{P_{A|U}(1|1)-P_{A|U}(1|0)}{2}.\end{aligned}$$

By using (11) for $\beta=\min[P_{A|U\mathcal{E}}(0|1),P_{A|U\mathcal{E}}(1|1)]=P_{A|U\mathcal{E}}(1|1)$ and by noting

$$d_{\mathsf{TV}}(P_{A|U\mathcal{E}}(\cdot|0),P_{A|U\mathcal{E}}(\cdot|1))=P_{A|U\mathcal{E}}(1|1)-P_{A|U\mathcal{E}}(1|0),$$

we have

$$\begin{aligned}\frac{\varepsilon^2}{\delta} &= \frac{(P_{A|U}(1|1)-P_{A|U}(1|0))^2}{4P_{A|U}(1|1)}\\ &= \frac{\delta_0(P_{A|U\mathcal{E}}(1|1)-P_{A|U\mathcal{E}}(1|0))^2}{4P_{A|U\mathcal{E}}(1|1)}\\ &= \frac{\delta_0 d_{\mathsf{TV}}(P_{A|U\mathcal{E}}(\cdot|0),P_{A|U\mathcal{E}}(\cdot|1))^2}{4\beta}\\ &\geq \frac{1}{8}D_{1/2}(P_{A|U}(\cdot|0)\|P_{A|U}(\cdot|1)),\end{aligned}$$

which implies (10). □

As a corollary of Theorem 2, we show that the CS advantage of the adversary for the hard-core predicate (distinguishing) game can be bounded below by the Rényi advantage (divided by eight). Namely, the converse of Theorem 1 holds for the hard-core predicate games.

Corollary 1. *For a given one-way function f with hard-core predicate h, let A be an inner adversary for the distinguishing game. Then, there exists an adversary A' of the hard-core predicate distinguishing game that invokes A once and*

$$\mathsf{Adv}^{\mathrm{CS}}_{A'} \geq \frac{1}{8}\mathsf{Adv}^{\mathrm{Renyi}}_{A}.$$

Proof. By Theorem 2, there exists an (ε, δ)-predictor $\mathcal{P}$ that invokes A once and $\frac{\varepsilon^2}{\delta} \geq \frac{1}{8}\mathsf{Adv}^{\mathrm{Renyi}}_{A}$. Let A' be an adversary defined as follows for given input $(f(x), z)$:

- If $\mathcal{P}(f(x)) = z$, then A' outputs 0;
- If $\mathcal{P}(f(x)) = z \oplus 1$, then A' outputs 1;
- If $\mathcal{P}(f(x)) = \perp$, then A' outputs $\perp$.

Obviously, the rate of this adversary is

$$\Pr(A'(f(x), z)) \neq \perp) = \Pr(\mathcal{P}(f(x)) \neq \perp) = \delta.$$

Furthermore, the advantage of this adversary is

$$\begin{aligned}
&\Pr(A'(f(x), z) = U) - \frac{1}{2}\Pr(A'(f(x), z) \neq \perp) \\
&= \frac{1}{2}\Pr(\mathcal{P}(f(x)) = h(x)) + \frac{1}{2}\Pr(\mathcal{P}(f(x)) = \sigma \oplus 1) - \frac{1}{2}\Pr(A'(f(x), z) \neq \perp) \\
&= \frac{1}{2}\Pr(\mathcal{P}(f(x)) = h(x)) + \frac{1}{2}\Pr(\mathcal{P}(f(x)) \neq \perp) \cdot \frac{1}{2} - \frac{1}{2}\Pr(A'(f(x), z) \neq \perp) \\
&= \frac{1}{2}\varepsilon.
\end{aligned}$$

Thus, the CS advantage of this adversary is $\mathsf{Adv}^{\mathrm{CS}}_{A'} = \frac{\varepsilon^2}{\delta} \geq \frac{1}{8}\mathsf{Adv}^{\mathrm{Renyi}}_{A}$. □

5.2 Reduction by Goldreich-Levin Algorithm

For a given one-way function $f(x)$, let $g(x, r) = (f(x), r)$ be a function from $\{0, 1\}^n \times \{0, 1\}^n$ to $\{0, 1\}^m \times \{0, 1\}^n$. Then, it is known that $h(x, r) = x \cdot r$ plays a role in the hard-core predicate. This section aims to connect the bit security of $g(x, r)$ and the bit security of the hard-core predicate $h(x, r)$. To that end, we consider the reduction algorithm, the so-called Goldreich-Levin algorithm. In order to evaluate the efficiency of the Goldreich-Levin algorithm, we use the following result from [12].

Theorem 3 ([12]). *Let $\mathcal{P}$ be a predictor of the hard-core $h(x, r) = x \cdot r$ with cost $T_{\mathcal{P}}$. Define $t = \log(4/\mathsf{Adv}^{\mathrm{CS}}_{\mathcal{P}})$. Then, there exists an algorithm Inv that runs in cost (expected time) $(T_{\mathcal{P}} + t \log n) \cdot t \cdot \mathcal{O}(n^2)$ and satisfies*

$$\Pr_{x \in_R \{0,1\}^n}\big(f(\mathsf{Inv}(f(x)) = f(x)\big) = \Omega\Big(\mathsf{Adv}^{\mathrm{CS}}_{\mathcal{P}}\Big).$$

By combining Theorem 3 and Theorem 2, we have the following estimate of the efficiency of the Goldreich-Levin algorithm in terms of the bit security, which is a generalization of [18, Theorem 4] for adversary without β-balanced assumption.

Theorem 4. *Let $f : \{0,1\}^n \to \{0,1\}^m$ be a λ-bit secure one-way function. Then, for a function $g(x,r) = (f(x), r)$, the function $h(x,r) = x \cdot r$ is a $(\lambda - \alpha)$-bit secure hard-core predicate for g, where $\alpha = \log\big(((\lambda+2)\log n) \cdot (\lambda+2) \cdot \mathcal{O}(n^2)\big) + \log\ln(1/\mu) + \mathcal{O}(1)$.*

Proof. Assume for contradiction that h is not $(\lambda - \alpha)$-bit secure hard-core for g. Then, by [18, Theorem 2], there exists an inner adversary A (for the distinguishing game of the hard-core predicate) such that the cost is T_A and the Rényi advantage is

$$\mathsf{Adv}_A^{\mathrm{Renyi}} > \frac{T_A}{2^{(\lambda-\alpha)}} \cdot \ln(1/4\mu).$$

By Theorem 2, there exists a predictor $\mathcal{P}$ of the hard-core predicate h with cost T_A such that

$$\mathsf{Adv}_{\mathcal{P}}^{\mathrm{CS}} > \frac{T_A}{2^{(\lambda-\alpha)+1}} \ln(1/4\mu).$$

Then, by Theorem 3, there exists an inner adversary A' of the OWF game that run in cost $T_{A'} = (T_A + t\log n) \cdot t \cdot \mathcal{O}(n^2)$ with success probability $\varepsilon_{A'} = \Omega(T_A \cdot 2^{-(\lambda-\alpha)})$, where $t = \log(4/\mathsf{Adv}_{\mathcal{P}}^{\mathrm{CS}}) \leq \lambda + 2$. It follows from [18, Theorem 1] that the bit security of OWF game is bounded above by $\log T_{A'} + \log(1/\varepsilon_{A'}) + \log\ln(1/\mu) + 1$, which is at most[4]

$$\lambda - \alpha + \log\big(((\lambda+2)\log n) \cdot (\lambda+2) \cdot \mathcal{O}(n^2)\big) + \log\ln(1/\mu) + \mathcal{O}(1).$$

By choosing $\alpha = \log\big(((\lambda+2)\log n) \cdot (\lambda+2) \cdot \mathcal{O}(n^2)\big) + \log\ln(1/\mu) + \mathcal{O}(1)$, f is not a λ bit secure one-way function, a contradiction. Hence, the statement follows. □

6 Search Games as Decision Games

We show that every λ-bit secure search game can be formalized as a decision game with (almost) λ-bit security. The search game is usually defined such that the adversary's success probability is small enough. Hence, it seems natural to define the decision game where the adversary tries to distinguish the following two cases of *real* and *ideal* games. While the real game is almost the same as the original search game, the ideal game is an idealized one where the adversary's solution will never be approved. For example, the unforgeability game of the signature scheme is usually defined as a search game. We may define the

[4] We assume $T_A \geq 1$.

corresponding ideal game such that the adversary cannot forge the signature. Such games often appear in game-hopping security proofs. When a party generates a secure signature of a message in a security game, we usually consider another game in which the forgery of the message is never approved. We realize the approval of the solution of the search game by adding an oracle in a decision game.

For an n-bit search game $G = (X, R, \{O_\theta\}_\theta)$, we define the *canonical decision game* G' of G such that $G' = (X, R', O')$ is a 1-bit game where the success probability of an inner adversary A is

$$\varepsilon_A = \Pr\left[\begin{matrix} u' \xleftarrow{R} \{0,1\}; u \xleftarrow{R} \{0,1\}^n; \\ x \leftarrow X(u); a' \leftarrow A^{O'}(x) \end{matrix} : a' = u'\right],$$

where $O' = \{O_\theta\}_\theta \cup O_{\mathrm{aprv}}$ and O_{aprv} is an oracle that can be accessed only once and is defined as

$$O_{\mathrm{aprv}}(a) = \begin{cases} 1 & (R(u,x,a) = 1) \wedge (u' = 0) \\ 0 & \text{otherwise} \end{cases}.$$

The additional oracle O_{aprv} answers whether the given value a satisfies the relation R only when $u' = 0$. In the ideal game, where $u = 1$, the oracle always answers 0, meaning that every valid solution a is never approved.

We show that the canonical game preserves the bit security of the underlying search game. The result implies no bit-security loss in transforming original games into such idealized games. It also justifies that every search game can be defined as a decision game.

Theorem 5. *If a search game G satisfies*

$$\mathrm{BS}_G^\mu \geq \lambda + \log_2 \frac{\ln(1/\mu)}{\ln(1/4\mu)} + 2,$$

then the corresponding canonical decision game G' satisfies $\mathrm{BS}_{G'}^\mu \geq \lambda$. Conversely, if G' satisfies

$$\mathrm{BS}_{G'}^\mu \geq \lambda + \log_2 \frac{\ln(1/2\mu)}{1-\mu} + 2,$$

then G satisfies $\mathrm{BS}_G^\mu \geq \lambda$.

Proof. Suppose that $\mathrm{BS}_{G'}^\mu < \lambda$. It follows from [18, Theorem 2] that there is an inner adversary A with computational complexity T_A for game G' that satisfies

$$d_{\mathsf{HD}}(A_0, A_1)^2 > \frac{T_A \cdot \ln(1/4\mu)}{2^{\lambda+1}}$$

for $\lambda \geq \log_2 \ln(1/4\mu)$. By (1), we have

$$d_{\mathsf{TV}}(A_0, A_1) > \frac{T_A \cdot \ln(1/4\mu)}{2^{\lambda+1}}.$$

Since the only way that A obtains the information on u' is to make queries to O_{aprv}, the above inequality implies that A queries a value a to O_{aprv} satisfying $R(u, x, a) = 1$ with probability more than $T_A \cdot \ln(1/4\mu)/2^{\lambda+1}$. Hence, A can be used as an inner adversary of the search game G. Namely, the inner adversary simulates A and monitors the oracle queries of A. If A queries a to the oracle O_{aprv}, the adversary outputs a. It follows from [18, Theorem 1] that

$$\begin{aligned}\mathrm{BS}_G^{\mu} &< \log_2 T_A + \lambda + 1 - \log_2(T_A \cdot \ln(1/4\mu)) + \log_2 \ln(1/\mu) + 1\\ &= \lambda + \log_2 \frac{\ln(1/\mu)}{\ln(1/4\mu)} + 2,\end{aligned}$$

a contradiction.

For the other direction, suppose that $\mathrm{BS}_G^{\mu} < \lambda$. Theorem 2 of [18] implies that there is an inner adversary A with computational complexity T_A for game G that satisfies the success probability

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

Consider an inner adversary A' of game G' that simulates $a \leftarrow A$ and queries a to O_{aprv}. Finally, A' outputs 0 if the answer from O_{aprv} is 1, and 1 otherwise. The computational complexity of A' is T_A. Let $A'_{u'}$ be the output distribution of A' when $u' \in \{0, 1\}$ is chosen as a secret. Then, $\Pr[A'_0 = 0] > T_A(1-\mu)/2^{\lambda}$ and $\Pr[A'_1 = 0] = 0$. By using [18, Lemma 8] with $q = 0$, we have

$$D_{1/2}(A'_0 \| A'_1) > \frac{T_A(1-\mu)}{2^{\lambda}}.$$

Theorem 1 of [18] implies that

$$\begin{aligned}\mathrm{BS}_{G'}^{\mu} &< \log_2 T_A + \lambda - \log_2(T_A(1-\mu)) + \log_2 \ln(1/2\mu) + 2\\ &= \lambda + \log_2 \frac{\ln(1/2\mu)}{1-\mu} + 2,\end{aligned}$$

a contradiction. □

Theorem 5 implies that all the security games we need to discuss are decision games if a constant difference of bit security can be ignored.

7 Distribution Replacing Theorem

Let $G = (X, R, \{O_i\}_i)$ be an n-bit security game. Suppose that G uses a probability distribution Q in a black-box manner. Namely, whenever some player makes a query to Q, the player will receive a sample according to Q. We denote the game by G^Q for clarity. Let P be another distribution that is supposed to be (computationally) close to Q. The question is, when G^Q is λ-bit secure, to what extent does Q need to be indistinguishable from P to preserve that G^P is

λ-bit secure. We prove a natural reduction showing that λ-bit secure indistinguishability is sufficient to replace the ideal distribution Q.

Before proving the theorem, we formally define the distribution indistinguishability game. For two distributions P and Q, let $G^{\text{ind}}_{P,Q} = (X, R, O)$ be a 1-bit security game such that X is empty, the oracle O outputs a sample from P when $u = 0$, and Q otherwise, and $R(u, x, a) = 1 \Leftrightarrow u = a$. Namely, the game is to discriminate between P and Q by oracle queries. For example, if $D_{1/2}(P\|Q) \leq 2^{-\lambda}$, the number of samples needed to distinguish P from Q must be $\Omega(2^{\lambda})$, which is a standard result of the Bayesian hypothesis testing. Since the number of samples is a lower bound of the computational complexity for the discrimination with high probability, the bit security must be at least $\lambda - O(1)$.

Due to Theorem 5, it is sufficient to prove the theorem for decision games.

Theorem 6. *Let G^Q be a 1-bit security game with black-box access to distribution Q. Let P be a probability distribution such that game $G^{\text{ind}}_{P,Q}$ has λ-bit security. If game G^Q has λ-bit security, then game G^P has $(\lambda - \alpha)$-bit security for $\alpha = 3 + \log_2(\ln(1/2\mu)/\ln(1/4\mu))$.*

Proof. Suppose that G^P is not $(\lambda - \alpha)$-bit secure. By [18, Theorem 2], there is an inner adversary A for game G^P with computational complexity T_A such that

$$d_{\mathsf{HD}}(A^P_0, A^P_1) > \sqrt{\frac{T_A \cdot \ln(1/4\mu)}{2^{\lambda-\alpha+1}}} \tag{12}$$

for $\lambda \geq \log_2 \ln(1/4\mu)$, where A^P_u is the output distribution of A when $u \in \{0, 1\}$ is chosen in G^P. We define A^Q_0 and A^Q_1 for the game G^Q similarly.

For a 1-bit game G, we write $G := (G_0, G_1)$, where G_u is the game G in which the secret bit $u \in \{0, 1\}$ is chosen. In other words, G is the game where a secret bit $u \in \{0, 1\}$ is randomly chosen and plays game G_u.

By following the above notation, we write $G^D = (G^D_0, G^D_1)$ for $D \in \{P, Q\}$. Also, we define a new game $G^{P,Q}_u := (G^P_u, G^Q_u)$. Consider an inner adversary A for the game G^D. For $u \in \{0, 1\}$ and $D \in \{P, Q\}$, let A^D_u be the output distribution of A in G^D when u is chosen as the secret bit. Then, by definition, we have

$$\mathsf{Adv}^{\text{Renyi}}_{G^D,A} = D_{1/2}(A^D_0 \| A^D_1) \quad \text{and} \quad \mathsf{Adv}^{\text{Renyi}}_{G^{P,Q}_u,A} = D_{1/2}(A^P_u \| A^Q_u)$$

for $u \in \{0, 1\}$ and $D \in \{P, Q\}$.

We show that the Rényi advantage of A in game $G^{P,Q}_u$ is bounded by that in $G^{\text{ind}}_{P,Q}$. We construct an inner adversary $\tilde{A}$ for the game $G^{\text{ind}}_{P,Q}$ by using A. The adversary $\tilde{A}$ runs the game $G^{P,Q}_u$ in which A plays. Whenever the game makes an oracle query, $\tilde{A}$ replies with an answer obtained by querying to the oracle O. By definition of $G^{\text{ind}}_{P,Q}$, each answer from O is an independent sample according to P if the secret bit $\tilde{u}$ of $G^{\text{ind}}_{P,Q}$ is 0, and Q otherwise. Thus, $\tilde{A}$ correctly simulates A in the game G^P_u when $\tilde{u} = 0$, and G^Q_u otherwise. Finally, $\tilde{A}$ outputs the same value as those of A in $G^{P,Q}_u$. Note that $\tilde{A}$ is an inner adversary of $G^{\text{ind}}_{P,Q}$ and its computational complexity is T_A. Since $G^{\mathrm{ind}}_{P,Q}$ has λ-bit security, it follows from [18, Theorem 1] that

$$\lambda \leq \mathrm{BS}^{\mu}_{G^{\mathrm{ind}}_{P,Q}} \leq \log_2 \left(\frac{T_A \cdot \ln(1/2\mu)}{\mathsf{Adv}^{\mathrm{Renyi}}_{G^{\mathrm{ind}}_{P,Q},\tilde{A}}} \right), \tag{13}$$

where $\mathsf{Adv}^{\mathrm{Renyi}}_{G^{\mathrm{ind}}_{P,Q},\tilde{A}} = D_{1/2}(\tilde{A}^P \| \tilde{A}^Q)$, and $\tilde{A}^D$ is the output distribution of $\tilde{A}$ in game $G^{\mathrm{ind}}_{P,Q}$ when the oracle outputs a sample according to D. Since $\tilde{A}$ correctly simulates A in the game $G^{P,Q}_u$, we have

$$\mathsf{Adv}^{\mathrm{Renyi}}_{G^{\mathrm{ind}}_{P,Q},\tilde{A}} = \mathsf{Adv}^{\mathrm{Renyi}}_{G^{P,Q}_u,A} = D_{1/2}(A^P_u \| A^Q_u). \tag{14}$$

Thus, by (2), (13), and (14),

$$d_{\mathsf{HD}}(A^P_u, A^Q_u) \leq \sqrt{\frac{1}{2} \cdot D_{1/2}(A^P_u \| A^Q_u)} \leq \sqrt{\frac{T_A \cdot \ln(1/2\mu)}{2^{\lambda+1}}} \tag{15}$$

for $u \in \{0, 1\}$.

The triangle inequality of d_{HD} and (15) implies that

$$\begin{aligned} d_{\mathsf{HD}}(A^P_0, A^P_1) &\leq d_{\mathsf{HD}}(A^P_0, A^Q_0) + d_{\mathsf{HD}}(A^Q_0, A^Q_1) + d_{\mathsf{HD}}(A^Q_1, A^P_1) \\ &\leq d_{\mathsf{HD}}(A^Q_0, A^Q_1) + \sqrt{\frac{T_A \cdot \ln(1/2\mu)}{2^{\lambda-1}}}. \end{aligned} \tag{16}$$

It follows from (12) and (16) that

$$\begin{aligned} d_{\mathsf{HD}}(A^Q_0, A^Q_1) &> \sqrt{\frac{T_A \cdot \ln(1/4\mu)}{2^{\lambda-\alpha+1}}} - \sqrt{\frac{T_A \cdot \ln(1/2\mu)}{2^{\lambda-1}}} \\ &\geq \sqrt{\frac{2T_A \cdot \ln(1/2\mu)}{2^{\lambda}}} \end{aligned}$$

by assumption on α. Then, we have

$$\mathsf{adv}^{\mathrm{Renyi}}_{A,G^Q} = D_{1/2}(A^Q_0 \| A^Q_1) \geq 2 d_{\mathsf{HD}}(A^Q_0, A^Q_1)^2 > \frac{4T_A \cdot \ln(1/2\mu)}{2^{\lambda}}.$$

By [18, Theorem 1], the bit security of G^Q is at most

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

a contradiction. Therefore, we have shown that G^P is $(\lambda - \alpha)$-bit secure. □

Theorem 6 is a generalization of [18, Theorem 9], where the condition is that $d_{\mathsf{HD}}(P, Q) \leq 2^{-\lambda/2}$. The above theorem only requires a computational condition that $G^{\mathrm{ind}}_{P,Q}$ has λ-bit security.

7.1 Application to Randomness Extraction

A randomness extractor is a procedure that converts a min-entropy source to an almost uniform distribution. The *min-entropy* of distribution X over $\{0,1\}^n$ is defined as $H_{\mathsf{min}}(X) = -\log_2 \max_{x\in\{0,1\}^n} P_X(x)$. Here, we define a seeded extractor through a 1-bit security game.

Definition 1. *A function* $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is said to be a* (k,λ)-extractor *if for every distribution* X *over* $\{0,1\}^n$ *with* $H_{\mathsf{min}}(X) \geq k$*, a* 1*-bit security game* $G^{\mathrm{ext}}_{\mathsf{Ext},X} := G^{\mathrm{ind}}_{P,Q}$ *has* λ*-bit security for* $P = (\mathsf{Ext}(X,S),S)$ *and* $Q = U_{m+d}$*, where* $S = U_d$*.*

The above is a definition of a *computational* extractor. We can define an *information-theoretic* extractor as usual. Although the total variation distance is usually used for the definition, the Rényi divergence of order 1/2 is a natural choice for cryptographic purposes, as we have seen so far. We say Ext is a (k,ε)-*it-extractor* if for every distribution X with $H_{\mathsf{min}}(X) \geq k$,

$$D_{1/2}((\mathsf{Ext}(X,S),S)\|U_{m+d}) \leq \varepsilon.$$

We can see that if Ext is a $(k,2^{-\lambda})$-it-extractor, then Ext is a (k,λ)-extractor.

It is well-known that a family of universal hash functions gives an information-theoretic extractor. The claim is also known as *the leftover hash lemma (LHL)* [5,13]. Although the lemma usually says that the extractor's output is close to the uniform distribution in the total variation distance, we need the closeness in the Rényi divergence of order 1/2. We have the following strengthened version of the leftover hash lemma.

Lemma 3 (LHL for Rényi Divergence). *Let* $\mathcal{H} = \{H : \{0,1\}^n \to \{0,1\}^m\}$ *be a* universal *family of hash functions; Namely, for any distinct* $x,x' \in \{0,1\}^n$*,* $\Pr_{H\sim\mathcal{H}}(H(x) = H(x')) \leq 2^{-m}$*. Suppose that* $|\mathcal{H}| = 2^d$ *and* $m = k - \lambda - 1$*. Then, function* $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *defined by* $\mathsf{Ext}(x,H) = H(x)$ *is a* $(k,2^{-\lambda})$*-it-extractor.*

Proof. It is shown in [19, Theorem 3] that the construction of Ext gives an extractor for the Hellinger distance[5]. Namely, for the defined parameters, we have that

$$d_{\mathsf{HD}}((\mathsf{Ext}(X,S),S),U_{m+d}) \leq 2^{-(\lambda+2)/2}.$$

By (2), it holds that

$$D_{1/2}((\mathsf{Ext}(X,S),S)\|U_{m+d}) \leq 4 \cdot d_{\mathsf{HD}}((\mathsf{Ext}(X,S),S),U_{m+d})^2 \leq 2^{-\lambda}.$$

Hence, the statement follows. □

[5] The claim can also be recovered by combining the leftover hash lemma of [4] for the KL divergence D and the relation that $d_{\mathsf{HD}}(P,Q)^2 \leq D_{1/2}(P\|Q) \leq D(P\|Q)$.

We apply Theorem 6 to the LHL. We consider replacing the seed of the extractor with the output of a pseudorandom generator (PRG). Suppose that $g : \{0,1\}^{d'} \to \{0,1\}^d$ is a λ-bit secure PRG. In other words, the game $G^{\mathrm{ind}}_{g(U_{d'}),U_d}$ has λ-bit security. Since the extractor of Lemma 3 is a (k, λ)-extractor, Theorem 6 guarantees that the seed of the LHL can be replaced by the output of g. Namely, the distribution $(H(X), g(S'))$ is λ-bit secure indistinguishable from the uniform distribution U_{m+d}, where X is a source with $H_{\mathsf{min}}(X) \geq k$, $S' = U_{d'}$, and H is randomly chosen from a family of universal hash functions using the seed $g(S')$.[6]

Entropy Loss in LHL The *entropy loss* of (k, ε)-it-extractors $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is defined as $k - m$, which is the amount of entropy lost for extracting randomness from entropy sources. It is proved in [16] that the entropy loss of $2\log(1/\varepsilon)$ is necessary for constructing a (k, ε)-it-extractor where the closeness ε is measured in the total variation distance. Large entropy loss is critical for applications where the amount of entropy is limited, such as biometric information. Barak et al. [2] showed that the loss could be reduced to $\log(1/\varepsilon)$ for some applications, including several decision primitives and all search primitives. It is shown in [19] that the same entropy loss can be achieved in the framework of [15]. The entropy loss for preserving λ-bit security in the above lemma is $\lambda+1$. Thus, the framework of [18] could reduce the entropy loss in LHL by half, as similarly shown in [2, 19].

8 Discussion

In this paper, by investigating the relationship between the CS advantage and the Rényi advantage, we clarified the relation between the notions of bit security introduced in [15] and [18]. As demonstrated in Theorem 1, λ bit security in the sense of [18] implies the same bit security (up to constant) in the sense of [15]. For some games, such as the hard-core predicate distinguishing game, the converse also holds (Corollary 1). However, the bit security of [15] may be overestimated than that of [18].

Difference in Privately-Verifiable Primitives. As evidence, let us consider an attack against a DDH (decision Diffie-Hellman) problem using an oracle for a CDH (computational Diffie-Hellman) problem. 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 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 adversary A' for the CDH game of G is defined by

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

[6] Barak et al. [2] studied a similar but different problem. In [2, Section 4], they considered the problem trying to achieve that $(\mathsf{Ext}(X, g(S')), S')$ is close to the uniform distribution. Namely, the seed S' of the PRG g is revealed. In our case, $g(S')$ is revealed but not S'.

Table 1. Comparison of advantages for various types of attacks.

Attacks	$\mathsf{Adv}^{\mathrm{TV}}$	$\mathsf{Adv}^{\mathrm{CS}}$	$\mathsf{Adv}^{\mathrm{Renyi}}$
Balanced attack $A_0 = (1/2 + \delta, 1/2 - \delta)$ $A_1 = (1/2, 1/2)$ e.g.) Linear test attack for PRG	δ	δ^2	$\Theta(\delta^2)$
Unbalanced attack with $\perp$ $A_0 = (\delta, 0, 1 - \delta)$ $A_1 = (\delta/2, \delta/2, 1 - \delta)$ e.g.) Inversion attack for PRG	$\delta/2$	$\delta/2$	$\Theta(\delta)$
Unbalanced attack without $\perp$ $A_0 = (\delta, 1 - \delta)$ $A_1 = (\delta/p, 1 - \delta/p)$ e.g.) CDH oracle attack for DDH	$(1 - 1/p)\delta$	$(1 - 1/p)^2\delta^2$	$\Theta(\delta)$

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

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

Let us consider the following adversary A for DDH invoking A' as an oracle for CDH. Given (g^x, g^y, g_u), the adversary A invokes A' with input (g^x, g^y) to obtain a candidate w of g^{xy}. Then, if $w = g_u$, A outputs $a = 0$; otherwise, A outputs $a = 1$. For this adversary, the output distribution A_u of A given u is $A_0 = (\varepsilon_{A'}^{\mathrm{cdh}}, 1 - \varepsilon_{A'}^{\mathrm{cdh}})$ and $A_1 = (\varepsilon_{A'}^{\mathrm{cdh}}/p, 1 - \varepsilon_{A'}^{\mathrm{cdh}}/p)$. Note that, for an adversary A that does not output $\perp$, the CS advantage coincides with the square of the standard advantage (total variation distance). Thus, we have $\mathsf{Adv}_A^{\mathrm{CS}} = (1 - 1/p)^2(\varepsilon_{A'}^{\mathrm{cdh}})^2$. On the other hand, using [18, Lemma 8], we can verify that the Rényi advantage is $\mathsf{Adv}_A^{\mathrm{Renyi}} = \Omega(\varepsilon_{A'}^{\mathrm{cdh}})$. If $\varepsilon_{A'}^{\mathrm{cdh}} \simeq 2^{-\lambda}$, then the bit security of [15] against this attack is roughly 2λ while the bit security of [18] against the same attack is roughly λ. Note that, for the CDH, it is difficult for the adversary to verify $w = g^{xy}$ and to outputs $\perp$ in a manner oblivious to the value of u. Perhaps, the security level evaluated using the framework of [15] may be higher than that of [18] when the so-called privately-verifiable search problems [10], such as the CDH, are involved.

Comparing Three Advantages. In Table 1, the standard advantage using the total variation distance $\mathsf{Adv}^{\mathrm{TV}}$, the CS advantage $\mathsf{Adv}^{\mathrm{CS}}$, and the Rényi advantage $\mathsf{Adv}^{\mathrm{Renyi}}$ are compared for three types of typical attacks: the balanced attack, the unbalanced attack with $\perp$, and the unbalanced attack without $\perp$. For the attack with $\perp$, the distribution of adversary is $A_u = (A_u(0), A_u(1), A_u(\perp))$. For all types of attacks, the standard advantage is roughly δ. The values of $\mathsf{Adv}^{\mathrm{TV}}$ and $\mathsf{Adv}^{\mathrm{CS}}$ are computed by a straightforward calculation; the value of $\mathsf{Adv}^{\mathrm{Renyi}}$

can be derived by Lemma 1, [18, Lemma 8], and Theorem 1. Note that the bit security of [15] is roughly $\log \frac{1}{\mathsf{Adv}^{\mathrm{CS}}}$ and that of [18] is roughly $\log \frac{1}{\mathsf{Adv}^{\mathrm{Renyi}}}$. From the table, we can find that the two notions of bit security coincide for the balanced attack and the unbalanced attack with $\perp$; however, as we discussed in the previous paragraph, there is a discrepancy between the two notions for the unbalanced attack without $\perp$; perhaps, $\mathsf{Adv}^{\mathrm{CS}}$ may overestimate the bit security. Even though it is not easy to reach a consensus on a good definition of bit security, it seems that the definition of [18] does not have any defects so far.

A Equivalence of (5)-(7)

Note that

$$\mathbb{E}[\psi(A)^2] = \Pr(A \neq \perp) \tag{17}$$

and

$$\begin{aligned}\mathbb{E}[\psi(A)\psi(U)] &= \Pr(A = U) - \Pr(A \neq \perp, A \neq U) \\ &= \Pr(A = U) - \bigl(\Pr(A \neq \perp) - \Pr(A \neq \perp, A = U)\bigr) \\ &= 2\Pr(A = U) - \Pr(A \neq \perp), \end{aligned} \tag{18}$$

where we used

$$\Pr(A = U) = \Pr(A \neq \perp, A = U) \tag{19}$$

in the third equality. By substituting (17) and (18) into (5), we have (6). By noting (19), (7) follows from (6).

References

1. Alon, N., Goldreich, O., Hastad, J., Peralta, R.: Simple construction of almost k-wise independent random variables. Random Structures and Algorithms **3**(3), 289–304 (1992)
2. Barak, B., Dodis, Y., Krawczyk, H., Pereira, O., Pietrzak, K., Standaert, F., Yu, Y.: Leftover hash lemma, revisited. In: Rogaway, P. (ed.) Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6841, pp. 1–20. Springer (2011). https://doi.org/10.1007/978-3-642-22792-9“˙1, https://doi.org/10.1007/978-3-642-22792-9_1
3. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4004, pp. 409–426. Springer (2006). https://doi.org/10.1007/11761679“˙25, https://doi.org/10.1007/11761679_25

4. Bennett, C.H., Brassard, G., Crépeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inf. Theory **41**(6), 1915–1923 (1995). https://doi.org/10.1109/18.476316, https://doi.org/10.1109/18.476316
5. Bennett, C.H., Brassard, G., Robert, J.: How to reduce your enemy's information (extended abstract). In: Williams, H.C. (ed.) Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings. Lecture Notes in Computer Science, vol. 218, pp. 468–476. Springer (1985). https://doi.org/10.1007/3-540-39799-X“˙37, https://doi.org/10.1007/3-540-39799-X_37
6. Dodis, Y., Steinberger, J.P.: Message authentication codes from unpredictable block ciphers. In: Halevi, S. (ed.) Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5677, pp. 267–285. Springer (2009). https://doi.org/10.1007/978-3-642-03356-8“˙16, https://doi.org/10.1007/978-3-642-03356-8_16
7. van Erven, T., Harremoës, P.: Rényi divergence and Kullback-Leibler divergence. IEEE Trans. Inform. Theory **60**(7), 3797–3820 (July 2014)
8. Goldreich, O.: The Foundations of Cryptography - Volume 1: Basic Techniques. Cambridge University Press (2001). https://doi.org/10.1017/CBO9780511546891, http://www.wisdom.weizmann.ac.il/%7Eoded/foc-vol1.html
9. Goldreich, O., Levin, L.A.: A hard-core predicate for all one-way functions. In: Johnson, D.S. (ed.) Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washigton, USA. pp. 25–32. ACM (1989). https://doi.org/10.1145/73007.73010, https://doi.org/10.1145/73007.73010
10. Goldwasser, S., Kalai, Y.T.: Cryptographic assumptions: A position paper. In: Kushilevitz, E., Malkin, T. (eds.) Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part I. Lecture Notes in Computer Science, vol. 9562, pp. 505–522. Springer (2016). https://doi.org/10.1007/978-3-662-49096-9“˙21, https://doi.org/10.1007/978-3-662-49096-9_21
11. Götze, F., Sambale, H., Sinulis, A.: Higher order concentration for functions of weakly dependent random variables. Electronic Journal of Probability **24**(85), 1–19 (2019)
12. Hast, G.: Nearly one-sided tests and the Goldreich-Levin predicate. Journal of Cryptology **17**, 209–229 (2004)
13. Impagliazzo, R., Levin, L.A., Luby, M.: Pseudo-random generation from one-way functions (extended abstracts). In: Johnson, D.S. (ed.) Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washigton, USA. pp. 12–24. ACM (1989). https://doi.org/10.1145/73007.73009, https://doi.org/10.1145/73007.73009
14. Levin, L.A.: Randomness and non-determinism. Journal of Symbolic Logic **58**(3), 1102–1103 (1993). https://doi.org/10.1137/S0895480197329508
15. Micciancio, D., Walter, M.: On the bit security of cryptographic primitives. In: Nielsen, J.B., Rijmen, V. (eds.) 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. Lecture Notes in Computer Science, vol. 10820, pp. 3–28. Springer (2018). https://doi.org/10.1007/978-3-319-78381-9“˙1, https://doi.org/10.1007/978-3-319-78381-9_1

16. Radhakrishnan, J., Ta-Shma, A.: Bounds for dispersers, extractors, and depth-two superconcentrators. SIAM J. Discrete Math. **13**(1), 2–24 (2000). https://doi.org/10.1137/S0895480197329508, https://doi.org/10.1137/S0895480197329508
17. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. IACR Cryptol. ePrint Arch. p. 332 (2004), http://eprint.iacr.org/2004/332
18. Watanabe, S., Yasunaga, K.: Bit security as computational cost for winning games with high probability. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13092, pp. 161–188. Springer (2021). https://doi.org/10.1007/978-3-030-92078-4“˙6, https://doi.org/10.1007/978-3-030-92078-4_6
19. Yasunaga, K.: Replacing probability distributions in security games via Hellinger distance. In: Tessaro, S. (ed.) 2nd Conference on Information-Theoretic Cryptography (ITC 2021). Leibniz International Proceedings in Informatics (LIPIcs), vol. 199, pp. 17:1–17:15. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany (2021). https://doi.org/10.4230/LIPIcs.ITC.2021.17, https://drops.dagstuhl.de/opus/volltexte/2021/14336