# Unified View for Notions of Bit Security

Shun Watanabe* Kenji Yasunaga†

February 9, 2023

**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 the notion of bit security by Watanabe and Yasunaga is equivalent to that of Micciancio and Walter (Eurocrypt 2018) up to constant bits. Also, we demonstrate that several existing notions of advantages can be captured in a unified way. Based on this equivalence, we show that the reduction algorithm of Hast (J. Cryptology, 2004) gives a tight reduction of the Goldreich-Levin hard-core predicate to the hardness of one-way functions. These two results resolved open problems that remained.

We show that all games we need to care about in their framework are decision games. Namely, for every search game $G$, there is the corresponding decision game $G'$ such that $G$ has $\lambda$-bit security if and only if $G'$ has $\lambda$-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 replacement theorem. Suppose a game using distribution $Q$ in a black-box manner is $\lambda$-bit secure, and two distributions $P$ and $Q$ are computationally $\lambda$-bit secure indistinguishable. In that case, the game where $Q$ is replaced by $P$ is also $\lambda$-bit secure.

## 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 $\lambda$-bit security (or security level $\lambda$) if we need $2^\lambda$ operations to break $P$. Although the statement is simple, we encounter difficulties formalizing such security levels exactly. In particular, the difficulty is defining bit security for *decision games*, such as pseudorandom generators and encryption schemes. For search games, such as the security games of one-way functions and signature schemes, the well-known expression of $\log_2(T/\varepsilon)$ can be justified for attacker $A$ with computational cost $T$ and winning probability $\varepsilon$; If we run $A$ in total $N$ times, the probability that some adversary wins the game is amplified to $\varepsilon N$. Thus it is sufficient to choose $N = 1/\varepsilon$ for winning the game with a probability of almost one. Hence, the total cost is $TN = 2^{\log_2(T/\varepsilon)}$.

In decision games, the attacker tries to distinguish two possible cases ($u = 0$ and $u = 1$). Even the random-guessing attacker can correctly predict the secret value $u$ with probability $1/2$. Thus, we usually define the advantage of the attacker $A$ to be $\mathsf{Adv}_A = 2|p - 1/2|$, where

*Tokyo University of Agriculture and Technology shunwata@cc.tuat.ac.jp
†Tokyo Institute of Technology yasunaga@c.titech.ac.jp

$p$ is the winning probability of $A$. We need to evaluate the security level of the primitive by assuming the existence of attacker $A$ with advantage $\mathsf{Adv}_A$.

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 $\varepsilon_1$, where $A_u = (p_0, p_1)$ means that $\Pr[A = 0 \mid u] = p_0$ and $\Pr[A = 1 \mid u] = p_1$. The (standard) advantage of this attack is $\mathsf{Adv}_A = \varepsilon_1$.

2. *Inversion attack:* First, the adversary tries to invert the one-way permutation, which will succeed with probability $\varepsilon_2$. If the inversion is successful and $h(x)$ coincides with $z$, the adversary outputs 0 (PRG); otherwise (if 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 $u \in \{0,1\}$ consists of $A_0 = (\varepsilon_2, 1 - \varepsilon_2)$ and $A_1 = (\varepsilon_2/2, 1 - \varepsilon_2/2)$. The (standard) advantage of this attack is $\mathsf{Adv}_A = \varepsilon_2/2$.

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]). When we use a random-guessing inversion attack, where $A$ chooses a random value $x'$, the inversion succeeds with probability $\varepsilon_2 = 2^{-n}$. Does this imply that the linear test attack is exponentially more sophisticated than the inversion attack? Or is this inner-product attack a basic one, as is the inversion attack?

In order to circumvent the subtlety mentioned above in defining bit security for decision games, Micciancio and Walter [14] introduced an alternative definition of advantage; when the random secret is $U$ and the adversary's output is $A$, their advantage is defined as the ratio $\mathsf{Adv}^{\mathrm{MW}} = \frac{I(U \wedge A)}{H(U)}$ between the mutual information and the Shannon entropy. They showed that, under a certain assumption, their advantage can be approximated by the *conditional squared (CS) advantage* $\mathsf{Adv}^{\mathrm{CS}}$ to be explained later (see (8)). In fact, $\mathsf{Adv}^{\mathrm{MW}}$ was only used as a justification of the CS advantage, and the bit security of specific results in [14] are evaluated with respect to the CS advantage. They used $\min_A\{\log_2(T_A/\mathsf{Adv}^{\mathrm{CS}}_A)\}$ as the definition of bit security, where $T_A$ is the computational cost of $A$. Even though the results obtained by their definition match our intuition, the definition lacks an *operational meaning*. The quantity of $\log_2(T_A/\mathsf{Adv}^{\mathrm{CS}}_A)$ is just a combination of the two values $T_A$ and $\mathsf{Adv}^{\mathrm{CS}}_A$. We cannot explain the meaning of this quantity from its definition. A good example of the quantity with operational meaning is the Shannon entropy $H(X)$ of the information source $X$. When we define the minimum average length of lossless compression functions $f$ for $X$ as $\mathrm{MinLen}(X) := \min_f\{\mathbb{E}[|f(X)|]\}$, we can show that the Shannon entropy approximates it as $H(X) \leq \mathrm{MinLen}(X) < H(X) + 1$. Hence, we say that $H(X)$ is the length limit of lossless compression of $X$.

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 $2^\lambda$, game $G$ is said to be $\lambda$-bit secure. Notably, they *characterized* their notion by advantages. They showed that the bit security of game $G$ is approximated by $\min_A\{\log_2(T_A/\mathsf{Adv}_A)\}$,[1] where $\mathsf{Adv}_A$ 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 [8, 7], they proved that a $\lambda$-bit secure one-way function gives a $\lambda$-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 [14], where they showed that the Goldreich-Levin reduction [8, 7] was indeed optimal.

Another open problem was the relationship between the two frameworks [14, 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 [14]. We show that the CS advantage of [14] for decision games is bounded above by the Rényi advantage. In other words, the Rényi advantage evaluates adversaries more pessimistically than the CS advantage. As an extreme case, there is an attack that achieves $\Theta(\delta)$ in the Rényi advantage but has 0 in the CS advantage (see Table 1). The above relation implies that if decision primitive $P$ has $\lambda$-bit security in [18], $P$ also has $\lambda$-bit security in [14]. Even though the converse is not necessarily true (see Section 1.3), we show that the CS advantage can be increased to the same level as the Rényi advantage if we appropriately modify the attack; essentially, the modified adversary relabels the output of the original adversary. Thus, we can transform an adversary so that the CS advantage is almost the same as the Rényi advantage. These two directions of bounds imply that the two notions of bit security in [14] and [18] are equivalent within constant bits. We compare the three advantages (standard (TV), CS, and Rényi) for several attacks in Section 1.3. We can see that the CS advantage is *sensitive* to labeling the adversary's output. Namely, the failure symbol $\perp$ has a unique role in the CS advantage but does not in the Rényi advantage.

Furthermore, we demonstrate that several existing notions of advantages [13, 11, 14] can be captured in a unified way. Specifically, the three quantities in [13, 11, 14] are the same except for a constant factor. Based on this equivalence, we show that the reduction algorithm of Hast [11]

[1] More precisely, it should be expressed by $\min_A\{\log_2 T_A + \log_2\lceil 1/\mathsf{Adv}_A\rceil)\}$ as $\mathsf{Adv}_A$ may take values greater than 1 for decision games.

gives a tight[2] reduction of the Goldreich-Levin hard-core predicate [8] to the hardness of one-way functions. Namely, we resolved another open problem that remained in [18]. Although we can derive a similar result from our general transformation described above together with the tightness result of the Goldreich-Levin theorem in [14], we give proof through the reduction of Hast [11]. An advantage of this route is that we can obtain an explainable algorithm (namely, Hast's algorithm) for improving the Goldreich-Levin algorithm. Although the transformation enables the adversary to have the Rényi advantage at the same level as the CS advantage, it may not be easy to understand the factor for improvement. We believe Hast's improved algorithm can be a hint for designing algorithms/reductions that attain high Rényi advantages.

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 $\lambda$-bit security if and only if the corresponding canonical game has $\lambda$-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 [16, 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 replacement theorem. Suppose that game $G^Q$ using black-box access to distribution $Q$ is $\lambda$-bit secure and two distributions $P$ and $Q$ are $\lambda$-bit secure indistinguishable. The theorem asserts that game $G^P$, where distribution $Q$ is replaced by $P$, is also $\lambda$-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 $\lambda$-bit secure indistinguishability is sufficient for preserving the $\lambda$-bit security of games. As an instance, we apply the theorem to the leftover hash lemma (LHL) [5, 12] and show that the seed of a $\lambda$-bit secure randomness extractor using universal hash functions can be safely replaced by the output of a $\lambda$-bit secure PRG. As a side result (and maybe implicit from [18]), we show that the entropy loss in the LHL to preserve $\lambda$-bit security in the framework of [18] is $\lambda$.

### 1.2 Related Work

Micciancio and Walter [14] 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 [13]. Levin's notion appeared in evaluating the security of the hard-core predicate of Goldreich and Levin [8]. Hast [11] 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 its operational interpretation. The standard advantage of $2|p - 1/2|$ 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 [13, 11, 14], reveal the relation to the framework of [14], and give an optimal reduction algorithm for the Goldreich-Levin theorem.

[2]We say a reduction is tight if it can be used to show that $\lambda$-bit security implies $(\lambda - o(\lambda))$-bit security.

Table 1: Comparison of advantages for four types of attacks

| Attacks | $\mathsf{Adv}^{\mathrm{TV}}$ | $\mathsf{Adv}^{\mathrm{CS}}$ | $\mathsf{Adv}^{\mathrm{Renyi}}$ |
|---|---|---|---|
| Balanced attack without $\perp$<br>$A_0 = (1/2+\delta, 1/2-\delta)$<br>$A_1 = (1/2, 1/2)$<br>e.g.) Linear test attack for PRG | $\delta$ | $\delta^2$ | $\Theta(\delta^2)$ |
| Unbalanced attack with $\perp$<br>$A_0 = (\delta, 0, 1-\delta)$<br>$A_1 = (\delta/2, \delta/2, 1-\delta)$<br>e.g.) Inversion attack for PRG | $\delta/2$ | $\delta/2$ | $\Theta(\delta)$ |
| Unbalanced attack without $\perp$<br>$A_0 = (\delta, 1-\delta)$<br>$A_1 = (\delta/p, 1-\delta/p)$<br>e.g.) CDH oracle attack for DDH | $(1-1/p)\delta$ | $(1-1/p)^2\delta^2$ | $\Theta(\delta)$ |
| Balanced 0/1-unbalanced $\perp$ attack<br>$A_0 = (1/2-\delta/2, 1/2-\delta/2, \delta)$<br>$A_1 = (1/2-\delta/4, 1/2-\delta/4, \delta/2)$<br>e.g.) Inversion attack using $\perp$ | $\delta/2$ | 0 | $\Theta(\delta)$ |

The entropy loss of randomness extractors is inevitable [15]. The LHL-based extractors achieve an optimal entropy loss of $2\log(1/\varepsilon)$ for closeness $\varepsilon$ 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 [14]. In other words, a $\lambda$-bit entropy loss in LHL is sufficient to preserve $\lambda$-bit security in bit security of [14]. In this work, we explicitly state that the same thing also holds in the framework of [18].

### 1.3 Comparing Two Frameworks of Bit Security

**Sensitivity of Advantages** We show the equivalence of the two notions of bit security in [14] and [18] up to a constant. The first one is given by $\min_A\{\log_2(T_A/\mathsf{Adv}_A^{\mathrm{CS}})\}$, and the second one is characterized by $\min_A\{\log_2 T_A + \log_2\lceil 1/\mathsf{Adv}_A^{\mathrm{Renyi}}\rceil\}$, where $\mathsf{Adv}_A^{\mathrm{CS}}$ and $\mathsf{Adv}_A^{\mathrm{Renyi}}$ are the CS advantages and the Rényi of adversary $A$, respectively. We stress that the two quantities coincide only when we optimize over adversaries. In fact, $\mathsf{Adv}_A^{\mathrm{Renyi}}$ is always bounded below by $\mathsf{Adv}_A^{\mathrm{CS}}$ for any adversary $A$, but $\mathsf{Adv}_A^{\mathrm{CS}}$ can be significantly smaller than $\mathsf{Adv}_A^{\mathrm{Renyi}}$. In this sense, there may be a risk of underestimating the potential impact of attacks when evaluating the bit security with $\mathsf{Adv}_A^{\mathrm{CS}}$. This is caused by the fact that $\mathsf{Adv}_A^{\mathrm{CS}}$ is *sensitive* to the labeling of the output of the adversary, while $\mathsf{Adv}_A^{\mathrm{Renyi}}$ is not; the failure symbol has a unique role in $\mathsf{Adv}_A^{\mathrm{CS}}$, while the failure symbol is just one of the symbols in $\mathsf{Adv}_A^{\mathrm{Renyi}}$.

The concern mentioned above can be illustrated by comparing the advantages of the following four types of attacks, summarized in Table 1. The first one, a balanced attack without $\perp$, is a type of attack such as the linear test attack mentioned above. The second one, an unbalanced attack with $\perp$, is an attack such as the inversion attack for PRG mentioned above. The third one, an unbalanced attack without $\perp$, is a type of attack that may occur in an attack against a decisional Diffie-Hellman (DDH) problem using an oracle for a computational Diffie-Hellman (CDH) problem. The CDH is a typical example of the so-called *privately-verifiable* search problem [9]. This type of attack naturally occurs when the privately-verifiable search oracle is available. The final attack, a balanced 0/1-unbalanced $\perp$ attack, is introduced for

comparison. This attack can be realized as a modification of the second attack for PRG; the adversary outputs $\perp$ when the inversion attack succeeded; otherwise, it outputs a random bit.

For the first two attacks, the advantages of $\mathsf{Adv}^{\mathrm{CS}}$ and $\mathsf{Adv}^{\mathrm{Renyi}}$ do not make a difference. However, while $\mathsf{Adv}^{\mathrm{Renyi}} = \Theta(\delta)$ for the third and the fourth attacks, $\mathsf{Adv}^{\mathrm{CS}}$ varies much for these cases. Namely, the CS advantage is inherently sensitive to attacks. For more detail on the comparison, see Section 4.2.

By comparing the two notions of bit security in [14] and [18], although these two quantities almost match when optimizing attacks, the framework of [18] seems to have several advantages. First, it has an operational meaning by definition. Second, its characterization, i.e., Rényi advantage, is preferable to the CS advantage employed in [14] because of the lack of sensitivity. A possible disadvantage of the Rényi advantage may be its complicated calculus. Several inequalities ((2), Lemma 1, Lemma 2, and Theorem 1) in this paper may help it.

### 1.4 Paper Organization

We review the framework of [18] in Section 3. In Section 4, we compare the two notions of advantages, the CS advantage of [14] and the Rényi advantage of [18], where the former can be seen as a unified notion as it is equivalent to other notions in the literature [13, 11]. As a result, we show that two notions of bit security in [14] and [18] are equivalent within constant bits. We show a tight reduction of the Goldreich-Levin theorem in Section 5. In Section 6, we show a canonical decision game such that every search game preserves its bit security in the corresponding canonical game. We prove the distribution replacement theorem in Section 7. We conclude the paper in Section 8.

## 2 Preliminaries

In this section, we present several basic notions and their properties to be used in proofs of the main results.

Let $P$ and $Q$ be probability distributions over a finite set $\Omega$. For a distribution $P$ over $\Omega$ 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 $[0,1]$. The *Rényi divergence of order* $1/2$ is defined by [3]

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

The Hellinger distance and the total variation distance can be related as follows:

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

[3] When $P$ and $Q$ have disjoint support, we set $D_{1/2}(P\|Q) = \infty$.

On the other hand, by noting $1 - 1/t \le \ln t \le t - 1$ for $t > 0$, the Hellinger distance and the Rényi divergence of order 1/2 can be related as follows:[4]

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

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

We present a few technical lemmas used in the paper.

**Lemma 1.** *For given distributions $P$ and $Q$ with $P \ll Q$,[5] we have*

$$D_{1/2}(P\|Q) \le D(P\|Q) \le \sum_{x \in \mathcal{X}^+} \frac{(P(x) - Q(x))^2}{Q(x)} \le 2\beta_Q^{-1} d_{\mathsf{TV}}(P,Q)^2,$$

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

*Proof.* The first inequality follows from the fact that the Rényi divergence is monotonically non-decreasing with respect to $\alpha$ and $D(P\|Q) = \lim_{\alpha \to 1} D_\alpha(P\|Q)$. For the last inequality, see [10, Lemma 4.1]; the second inequality appears in the middle of the proof of [10, Lemma 4.1]. □

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

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

*for $\phi(q) = (1 - \sqrt{q})^2 - q/16$. The same conclusion holds when $A_0 = (1/2 - \delta/2, 1/2 - \delta/2, \delta)$ and $A_1 = (1/2 - q\delta/2, 1/2 - q\delta/2, q\delta)$. In particular, $\phi(q) > 1/2$ for $q \le 1/16$.*

*Proof.* The first claim is the same as [18, Lemma 8]. The second one follows from the fact that the value $\sum_{x \in \{0,1,\perp\}} \sqrt{A_0(x)A_1(x)}$ is the same as the first case. □

## 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

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

where $O_A^{\mathrm{decn}}$ is the oracle that, given the $i$th 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

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

[4] The second inequality holds as long as $D_{1/2}(P\|Q) < \infty$.

[5] Here, $P \ll Q$ indicates that $\{x : P(x) > 0\} \subseteq \{x : Q(x) > 0\}$.

where $O_A^{\mathrm{srch}}$ is the oracle that, given the $i$th 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 $A$. We can employ various computational complexity measures, such as time complexity and circuit complexity, as $T_A$. The only restriction is that an $N$-times use of the same algorithm of cost $T$ can be done with cost $NT$. The bit security of an $n$-bit game $G = (X, R, \{O_\theta\}_\theta)$ for error probability $\mu$ is defined to be

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

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

Roughly speaking, the bit security of the game is at least $\lambda$ if the computational complexity of the adversary for achieving the success probability $1-\mu$ is at least $2^\lambda$. 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 as[6]

$$\mathrm{BS}_G^\mu = \min_A \left\{ \log_2 T_A + \log_2 \left\lceil \frac{1}{\mathsf{Adv}_{G,A}^{\mathrm{Renyi}}} \right\rceil \right\} + \mathcal{O}(1). \tag{5}$$

where the *Rényi advantage* is defined as

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

where $A_u$ is the output distribution of $A$ in the 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. See Appendix A for the detailed statements. 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. For simplicity, we may write $\mathsf{Adv}_A^{\mathrm{Renyi}}$ for $\mathsf{Adv}_{G,A}^{\mathrm{Renyi}}$.

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], where (5) and the theorems in Appendix A were derived, 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 [14], we allow an inner adversary to output the failure symbol $\perp$.

For an adversary $A$ for a decision game, we write $A_u = (A_u(0), A_u(1), A_u(\perp))$ for $u \in \{0,1\}$. We may simply write $A_u = (A_u(0), A_u(1))$ if $A$ never outputs $\perp$.

[6]The ceiling function appears since the inner adversary must be invoked at least once even if the Rényi advantage is larger than 1.

# 4 Rényi Advantage and Conditional Squared Advantage

This section discusses the connection between the Rényi advantage and the advantage used in [14], 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 [14] 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 B)

$$\mathsf{Adv}_A^{\mathrm{CS}} := \mathbb{E}\left[\frac{\psi(A)}{\sqrt{\mathbb{E}[\psi(A)^2]}}\psi(U)\right]^2 \tag{6}$$

$$= \frac{4\Big(\Pr(A = U) - \frac{1}{2}\Pr(A \neq \perp)\Big)^2}{\Pr(A \neq \perp)} \tag{7}$$

$$= \Pr(A \neq \perp)\big(2\Pr(A = U | A \neq \perp) - 1\big)^2. \tag{8}$$

It can be verified that $0 \leq \mathsf{Adv}_A^{\mathrm{CS}} \leq 1$. Historically speaking, the expression (6) was introduced by Levin in [13]; the expression (7) was introduced (up to the constant factor of 4) by Hast in [11, Theorem 3] to characterize the success probability of the modified Goldreich-Levin algorithm; Micciancio and Walter introduced the expression (8) in [14, Theorem 1, Definition 10], and they initiated the use of this quantity as an advantage to characterize their notion of bit security.

Although the two notions of advantages $\mathsf{Adv}_A^{\mathrm{Renyi}}$ and $\mathsf{Adv}_A^{\mathrm{CS}}$ appear to be different quantities, in fact, they are closely related quantitatively. We first show that $\mathsf{Adv}_A^{\mathrm{CS}}$ can be upper bounded by $\mathsf{Adv}_A^{\mathrm{Renyi}}$ up to a constant.

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

$$\mathsf{Adv}_A^{\mathrm{CS}} \leq 8\mathsf{Adv}_A^{\mathrm{Renyi}}. \tag{9}$$

*Proof.* First, by noting that

$$\Pr(A \neq \perp) = A_0(0) + A_1(0) + A_0(1) + A_1(1)$$

and

$$2\Pr(A = U) - \Pr(A \neq \perp) = A_0(0) - A_1(0) + A_1(1) - A_0(1),$$

we can bound $\mathsf{Adv}_A^{\mathrm{CS}}$ as

$$\begin{aligned}
\mathsf{Adv}_A^{\mathrm{CS}} &= \frac{(A_0(0) - A_1(0) + A_1(1) - A_0(1))^2}{(A_0(0) + A_1(0) + A_0(1) + A_1(1))} \\
&\leq \frac{(|A_0(0) - A_1(0)| + |A_1(1) - A_0(1)|)^2}{(A_0(0) + A_1(0) + A_0(1) + A_1(1))} \\
&\leq \max_{a \in \{0,1\}} \frac{4(A_0(a) - A_1(a))^2}{(A_0(0) + A_1(0) + A_0(1) + A_1(1))} \\
&\leq \max_{a \in \{0,1\}} \frac{4(A_0(a) - A_1(a))^2}{(A_0(a) + A_1(a))}.
\end{aligned} \tag{10}$$

Next, by noting that the inequality

$$(s - t)^2 = ((\sqrt{s} - \sqrt{t})(\sqrt{s} + \sqrt{t}))^2 \leq 2(\sqrt{s} - \sqrt{t})^2$$

holds for any $0 \le s, t \le 1$ satisfying $s + t = 1$, we have

$$\begin{aligned}
&\frac{4(A_0(a) - A_1(a))^2}{(A_0(a) + A_1(a))} \\
&= 4(A_0(a) + A_1(a))\left(\frac{A_0(a)}{A_0(a) + A_1(a)} - \frac{A_1(a)}{A_0(a) + A_1(a)}\right)^2 \\
&\le 8(A_0(a) + A_1(a))\left(\sqrt{\frac{A_0(a)}{A_0(a) + A_1(a)}} - \sqrt{\frac{A_1(a)}{A_0(a) + A_1(a)}}\right)^2 \\
&= 8(\sqrt{A_0(a)} - \sqrt{A_1(a)})^2 \\
&\le 8 \sum_{a' \in \{0,1,\perp\}} (\sqrt{A_0(a')} - \sqrt{A_1(a')})^2 \\
&= 16 d_{\mathsf{HD}}(A_0, A_1)^2 \qquad (11)
\end{aligned}$$

for every $a \in \{0, 1\}$. Thus, by combining (10) and (11), and by using the left inequality of (2), we have (9). □

Theorem 1 implies that, up to constant bits, if a decision game is $\lambda$ bit secure in [18], then it is also $\lambda$ bit secure in the sense of [14].

In general, it is not possible to derive an upper bound on $\mathsf{Adv}^{\mathrm{Renyi}}_A$ in terms of $\mathsf{Adv}^{\mathrm{CS}}_A$. For instance, for the inversion attack mentioned in Section 1, $\mathsf{Adv}^{\mathrm{Renyi}}_A = \Theta(\varepsilon)$ while $\mathsf{Adv}^{\mathrm{CS}}_A = \varepsilon^2$. However, for a given adversary $A$, we can always construct an adversary $\tilde{A}$ having the same cost and $\mathsf{Adv}^{\mathrm{CS}}_{\tilde{A}}$ is as large as $\mathsf{Adv}^{\mathrm{Renyi}}_A$.

**Theorem 2.** *For an adversary $A$ of a decision game satisfying $\mathsf{Adv}^{\mathrm{Renyi}}_A \le 1$, there exists an adversary $\tilde{A}$ having the same cost as $A$, and it satisfies*

$$\mathsf{Adv}^{\mathrm{Renyi}}_A \le 12 \mathsf{Adv}^{\mathrm{CS}}_{\tilde{A}}.$$

*Proof.* To prove Theorem 2, we use the following lemma from [14, Lemma 1]. Since the proof was absent in [14], we also give a proof for completeness.

**Lemma 3** ([14])**.** *For a given adversary $A$ of a decision game and for each symbol $z \in \{0, 1, \perp\}$, let $\tilde{A}^z$ be an adversary defined as follows: first $\tilde{A}^z$ run $A$; if the output $a$ of $A$ satisfies $a = z$ and $A_0(z) \ge A_1(z)$, then $\tilde{A}^z$ outputs 0; if the output $a$ of $A$ satisfies $a = z$ and $A_0(z) < A_1(z)$, then $\tilde{A}^z$ outputs 1; otherwise (i.e., $a \ne z$), $\tilde{A}^z$ outputs $\perp$.*[7] *Then, $\tilde{A}^z$ has the same cost as $A$ and satisfies*

$$\mathsf{Adv}^{\mathrm{CS}}_{\tilde{A}^z} = \frac{1}{2}\frac{(A_0(z) - A_1(z))^2}{(A_0(z) + A_1(z))}. \qquad (12)$$

*Proof.* The probability that $\tilde{A}^z$ does not output $\perp$ is $\Pr(\tilde{A}^z \ne \perp) = \frac{A_0(z)+A_1(z)}{2}$, and the probability that $\tilde{A}^z$ outputs the correct value is $\Pr(\tilde{A}_z = U) = \frac{A_0(z)}{2}$ if $A_0(z) \ge A_1(z)$ and $\Pr(\tilde{A}_z = U) = \frac{A_1(z)}{2}$ if $A_0(z) < A_1(z)$. Thus, by substituting these probabilities into (7), we have (12). □

[7] Note that $\tilde{A}^z$ outputs only one of 0 or 1 and $\perp$ with positive probability.

Now, we are ready to prove Theorem 2. Under the assumption $\mathsf{Adv}_A^{\mathrm{Renyi}} \leq 1$, (2) implies

$$\begin{aligned}
\mathsf{Adv}_A^{\mathrm{Renyi}} &= D_{1/2}(A_0 \| A_1) \\
&\leq 4 d_{\mathsf{HD}}(A_0, A_1)^2 \\
&= 2 \sum_{a \in \{0,1,\perp\}} (\sqrt{A_0(a)} - \sqrt{A_1(a)})^2 \\
&\leq 6 \max_{a \in \{0,1,\perp\}} (\sqrt{A_0(a)} - \sqrt{A_1(a)})^2 \\
&= 6 \max_{a \in \{0,1,\perp\}} \frac{(A_0(a) - A_1(a))^2}{(\sqrt{A_0(a)} + \sqrt{A_1(a)})^2} \\
&\leq 6 \max_{a \in \{0,1,\perp\}} \frac{(A_0(a) - A_1(a))^2}{(A_0(a) + A_1(a))}.
\end{aligned}$$

Thus, by Lemma 3, we can construct an adversary $\tilde{A}$ satisfying the claim of the theorem. □

Since $\mathsf{Adv}_A^{\mathrm{Renyi}}$ can be unbounded while $\mathsf{Adv}_{\tilde{A}}^{\mathrm{CS}} \leq 1$, the assumption $\mathsf{Adv}_A^{\mathrm{Renyi}} \leq 1$ in Theorem 2 is crucial. Even though $\mathsf{Adv}_A^{\mathrm{Renyi}}$ can be larger than 1 in general, by using Theorem 2 together with an additional argument, we can show that $\lambda$ bit security in the sense of [14] implies $\lambda$ bit security in the sense of [18] up to constant bits as follows. To prove the contraposition, suppose that there exists an adversary $A$ such that $\log T_A + \log\lceil 1/\mathsf{Adv}_A^{\mathrm{Renyi}} \rceil$ is smaller than $\lambda$ (i.e., not $\lambda$ bit secure in the sense of [18]). If $\mathsf{Adv}_A^{\mathrm{Renyi}} \leq 1$, we can directly apply Theorem 2 and conclude that the game is not $\lambda$ bit secure in the sense of [14] as well. When $\mathsf{Adv}_A^{\mathrm{Renyi}} > 1$, for a parameter $0 \leq \theta \leq 1$, let consider the following adversary $A^\theta$. First, $A^\theta$ flip a coin $C$ that takes 1 with probability $\theta$ and 0 with probability $1-\theta$; when $C = 1$, $A^\theta$ runs $A$ and outputs $A$'s outcome; when $C = 0$, $A^\theta$ always outputs $\perp$. Then, the cost of this adversary is $T_{A^\theta} = \theta T_A$, and the distributions of outcomes can be written as $A_u^\theta = \theta A_u + (1-\theta) A_{\mathtt{triv}}$, where $A_{\mathtt{triv}}(\perp) = 1$. By the joint convexity of the Rényi divergence of order 1/2 [17, Theorem 11], we can verify that the Rényi advantage of $A^\theta$ given by

$$\mathsf{Adv}_{A^\theta}^{\mathrm{Renyi}} = D_{1/2}(\theta A_0 + (1-\theta) A_{\mathtt{triv}} \| \theta A_1 + (1-\theta) A_{\mathtt{triv}})$$

is a convex (and thus continuous) function of $0 \leq \theta \leq 1$, and $\mathsf{Adv}_{A^0}^{\mathrm{Renyi}} = 0$ and $\mathsf{Adv}_{A^1}^{\mathrm{Renyi}} = \mathsf{Adv}_A^{\mathrm{Renyi}}$. Thus, there exists $\theta'$ such that $\mathsf{Adv}_{A^{\theta'}}^{\mathrm{Renyi}} = 1$. Since $\log T_{A^{\theta'}}$ is smaller than $\lambda$, by applying Theorem 2, we can show the existence of an adversary $\tilde{A}^{\theta'}$ such that $\log T_{\tilde{A}^{\theta'}} + \log(1/\mathsf{Adv}_{\tilde{A}^{\theta'}}^{\mathrm{CS}})$ is smaller than $\lambda$ up to a constant, which implies that the game is not $\lambda$ bit secure in the sense of [14].

### 4.1 The Case that $\mathsf{Adv}_A^{\mathrm{Renyi}} \leq 1$

We observe that the Rényi advantage must be at most 1 for some class of decision games, although it is generally unbounded by definition. Intuitively, the class consists of games such that the game for $u = 0$ is identical to the game for $u = 1$ with some probability.

Let $G$ be a decision game. We write $G = (G_0, G_1)$, where $G_u$ is the game when the secret is $u \in \{0,1\}$. We say game $G$ is *identical to game $G'$ with probability $p$* if $G$ is equal to $G'$ with probability $p$ and is equal to some game $G''$ with probability $1-p$.

**Proposition 1.** *Let $G = (G_0, G_1)$ be a decision game. If $G_u$ is identical to $G_{1-u}$ with probability at least $1/e$ for some $u \in \{0,1\}$, then $\mathsf{Adv}_A^{\mathrm{Renyi}} \leq 1$ for any adversary $A$.*

*Proof.* Without loss of generality, we assume that $G_0$ is identical to $G_1$ with probability $\gamma \geq 1/e$. For an adversary $A$ for game $G$, suppose that the output distribution when $u = 0$ is $A_0 = (p_0, p_1, p_\perp)$, where $p_0 + p_1 + p_\perp = 1$. Let $A_1 = (p'_0, p'_1, p'_\perp)$ be the output distribution when $u = 1$. By assumption, we have $p'_a \geq \gamma \cdot p_a$ for every $a \in \{0, 1, \perp\}$. Thus,

$$\sum_{a\in\{0,1,\perp\}} \sqrt{A_0(a)A_1(a)} = \sum_{a\in\{0,1,\perp\}} \sqrt{p_a \cdot p'_a} \geq \sqrt{\gamma} \geq \sqrt{1/e}.$$

Hence, we have

$$\mathsf{Adv}_A^{\mathrm{Renyi}} = -2\ln \sum_{a\in\{0,1,\perp\}} \sqrt{A_0(a)A_1(a)} \leq -2\ln(\sqrt{1/e}) = 1.$$

□

The hard-core predicate *distinguishing* game described in Section 5.1 satisfies the condition in the proposition. In this game, the adversary receives $(f(x), h(x))$ for random input $x$ when $u = 0$, and $(f(x), \sigma)$ for random bit $\sigma$ when $u = 1$, where $f$ is a one-way function and $h$ is its hard-core predicate. Since the probability distribution of $(f(x), \sigma)$ is equal to the distribution $\frac{1}{2}(f(x), h(x)) + \frac{1}{2}(f(x), 1 - h(x))$, the game for $u = 1$ is identical to the game for $u = 0$ with probability $1/2$, which is at least $1/e$.

Note also that the Rényi advantage of an adversary cannot be larger than the Rényi advantage achieved by computationally unbounded adversaries. In the case of the above-mentioned hard-core predicate, we can verify that the Rényi divergence between the distributions of $(f(x), h(x))$ and $(f(x), \sigma)$ is bounded by 1.

## 4.2 Comparison

Even though Theorem 1 and Theorem 2 imply that the two notions of bit security in [14] and [18] are equivalent within a constant, we stress that two quantities coincide only when we optimize over adversaries. In this section, we illustrate the difference between the two notions of bit security for a typical attack that may occur in the privately-verifiable primitives.

### 4.2.1 Difference in Privately-Verifiable Primitives

Let us consider an attack against a decision Diffie-Hellman (DDH) problem using an oracle for a computational Diffie-Hellman (CDH) 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

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

The 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

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

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 $A_0 = (\varepsilon^{\mathrm{cdh}}_{A'}, 1 - \varepsilon^{\mathrm{cdh}}_{A'})$ and $A_1 = (\varepsilon^{\mathrm{cdh}}_{A'}/p, 1 - \varepsilon^{\mathrm{cdh}}_{A'}/p)$. Note that, for adversary $A$ that does not output $\perp$, the CS advantage coincides with the square of the standard advantage (total variation distance). Thus, we have $\mathsf{Adv}^{\mathrm{CS}}_A = (1 - 1/p)^2(\varepsilon^{\mathrm{cdh}}_{A'})^2$. On the other hand, using Lemma 2, we can verify that the Rényi advantage is $\mathsf{Adv}^{\mathrm{Renyi}}_A = \Omega(\varepsilon^{\mathrm{cdh}}_{A'})$. When $\varepsilon^{\mathrm{cdh}}_{A'} \simeq 2^{-\lambda}$, this attack implies that the bit security of [14] must be at most $2\lambda$, while that of [18] is reduced to $\lambda$.

### 4.2.2 Comparing Three Advantages

In Table 1 of Section 1.3, 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 four types of attacks: (1) balanced attack without $\perp$; (2) unbalanced attack with $\perp$; (3) unbalanced attack without $\perp$; and (4) balanced 0/1-unbalanced $\perp$ attack.

The first two attacks already appeared in Section 1 as the linear test attack and the inversion attack for PRG. The third attack appeared just in the above as the DDH attack using the CDH oracle. For comparison, we introduce another *unusual* attack for PRG as the fourth attack. Recall the situation in Section 1 where the adversary $A$, given $(f(x), z)$, tries to distinguish whether $z = h(x)$ or $z$ is a random bit, where $f$ is a one-way permutation, $x$ is a random input, and $h$ is a hard-core predicate. We consider adversary $A$ such that $A$ tries to invert $f(x)$ and outputs $\perp$ if the inversion succeeded and $h(x) = z$. Otherwise, $A$ outputs a random bit. The output distribution of $A$ consists of $A_0 = (1/2 - \delta/2, 1/2 - \delta/2, \delta)$ and $A_1 = (1/2 - \delta/4, 1/2 - \delta/4, \delta/2)$, where $\delta$ is the success probability of the inversion attack. Note that the CS advantage of this adversary is 0 since it outputs 0 and 1 with the same probabilities in either case of $u \in \{0, 1\}$.

For all types of attacks, the standard advantage is roughly $\delta$. The values of $\mathsf{Adv}^{\mathrm{TV}}$ and $\mathsf{Adv}^{\mathrm{CS}}$ are computed by a straightforward calculation; the values of $\mathsf{Adv}^{\mathrm{Renyi}}$ can be derived by Lemma 1, Lemma 2, and Theorem 1. Note that the bit security of [14] 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 first two attacks; however, there are discrepancies for the last two attacks. As discussed above, the CS advantage can be a square of the Rényi advantage for the privately-verifiable problems. Furthermore, the fourth attack demonstrates the case that the CS advantage may take 0 even if the other advantages take $\Theta(\delta)$. Although $\mathsf{Adv}^{\mathrm{CS}}$ can be increased to the same level as $\mathsf{Adv}^{\mathrm{Renyi}}$ by using the transformation of Theorem 2, it is possible to underestimate the adversary's ability when using $\mathsf{Adv}^{\mathrm{CS}}$ as evaluation. In this sense, it seems that $\mathsf{Adv}^{\mathrm{Renyi}}$ is preferable to $\mathsf{Adv}^{\mathrm{CS}}$ when evaluating the impact of attacks.

# 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 the formulation of bit security in [18], 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 $\sigma$ 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 [11], a predictor $\mathcal{P}$ is said to be an $(\varepsilon, \delta)$-*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, $(\varepsilon, \delta)$-predictor $\mathcal{P}$ has CS advantage $\mathsf{Adv}^{\mathrm{CS}}_{\mathcal{P}} = \frac{4\varepsilon^2}{\delta}$.

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

**Theorem 3.** *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*[8]

$$\mathsf{Adv}^{\mathrm{CS}}_{\mathcal{P}} \geq \frac{1}{3}\mathsf{Adv}^{\mathrm{Renyi}}_{A}. \tag{13}$$

*Proof.* Using adversary $A$, similarly to [11, 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.,

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

Note the support of $(f(x), h(x))$ is included in the support of $(f(x), \sigma)$.[9] Thus, if the adversary $A$ outputs a symbol $a$ with positive probability under $u = 0$, then $A$ must output $a$ with positive probability under $u = 1$ as well, i.e., $P_{A|U}(\cdot|0) \ll P_{A|U}(\cdot|1)$.

Let $a^\star \in \{0, 1, \perp\}$ be such that $P_{A|U}(a^\star|1) > 0$ and

$$\max_{\substack{a \in \{0,1,\perp\}: \\ P_{A|U}(a|1) > 0}} \frac{(P_{A|U}(a|0) - P_{A|U}(a|1))^2}{P_{A|U}(a|1)} = \frac{(P_{A|U}(a^\star|0) - P_{A|U}(a^\star|1))^2}{P_{A|U}(a^\star|1)}.$$

Then, by Lemma 1, we have

$$D_{1/2}(P_{A|U}(\cdot|0) \| P_{A|U}(\cdot|1)) \leq 3\frac{(P_{A|U}(a^\star|0) - P_{A|U}(a^\star|1))^2}{P_{A|U}(a^\star|1)}. \tag{14}$$

We consider two cases separately.

[8] As we can find from the proof, the output alphabet of $A$ being $\{0, 1, \perp\}$ is not crucial; the same argument goes through for any output alphabet $\mathcal{A}$ if replace the factor of $\frac{1}{3}$ by $\frac{1}{|\mathcal{A}|}$ in (13).

[9] Here, the support is the set of realizations that occur with positive probability.

**When** $P_{A|U}(a^\star|0) \geq P_{A|U}(a^\star|1)$ : In this case, we consider the following predictor $\mathcal{P}$. First, we sample the uniform random bit $\sigma$. Second,

- If $A(f(x), \sigma) = a^\star$, then $\mathcal{P}$ outputs $\sigma$;
- If $A(f(x), \sigma) \neq a^\star$, then $\mathcal{P}$ outputs $\perp$.

The rate of this predictor is

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

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

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

Thus, the advantage of this predictor is

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

Then, by using (14), we have

$$\begin{aligned}\frac{\varepsilon^2}{\delta} &= \frac{(P_{A|U}(a^\star|0) - P_{A|U}(a^\star|1))^2}{4P_{A|U}(a^\star|1)} \\ &\geq \frac{1}{12} D_{1/2}(P_{A|U}(\cdot|0) \| P_{A|U}(\cdot|1)),\end{aligned}$$

which implies (13).

**When** $P_{A|U}(a^\star|0) < P_{A|U}(a^\star|1)$ : In this case, we consider the following predictor. First, we sample the uniform random bit $\sigma$. Second,

- If $A(f(x), \sigma) = a^\star$, then $\mathcal{P}$ outputs $\sigma \oplus 1$;
- If $A(f(x), \sigma) \neq a^\star$, then $\mathcal{P}$ outputs $\perp$.

The rate of this predictor is

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

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

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

Thus, the advantage of this predictor is

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

Then, by using (14), we have

$$\begin{aligned}\frac{\varepsilon^2}{\delta} &= \frac{(P_{A|U}(a^\star|1) - P_{A|U}(a^\star|0))^2}{4P_{A|U}(a^\star|1)} \\ &\geq \frac{1}{12} D_{1/2}(P_{A|U}(\cdot|0) \| P_{A|U}(\cdot|1)),\end{aligned}$$

which implies (13). □

As a corollary of Theorem 3, 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 twelve).

**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*

$$\mathsf{Adv}^{\mathrm{CS}}_{A'} \geq \frac{1}{12}\mathsf{Adv}^{\mathrm{Renyi}}_{A}.$$

*Proof.* By Theorem 3, there exists an $(\varepsilon, \delta)$-predictor $\mathcal{P}$ that invokes $A$ once and $\frac{\varepsilon^2}{\delta} \geq \frac{1}{12}\mathsf{Adv}^{\mathrm{Renyi}}_{A}$. 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 $\mathsf{Adv}^{\mathrm{CS}}_{A'} = \frac{\varepsilon^2}{\delta} \geq \frac{1}{12}\mathsf{Adv}^{\mathrm{Renyi}}_{A}$. □

### 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 by Hast [11].

**Theorem 4** ([11])**.** *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 $\mathsf{Inv}$ that runs in cost (expected time) $(T_{\mathcal{P}} + t \log n) \cdot t \cdot \mathcal{O}(n^2)$ and satisfies*

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

By combining Theorem 4 and Theorem 3, 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 adversaries without $\beta$-balanced assumption.

**Theorem 5.** *Let $f : \{0,1\}^n \to \{0,1\}^m$ be a $\lambda$-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 Theorem 9, 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

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

By Theorem 3, there exists a predictor $\mathcal{P}$ of the hard-core predicate $h$ with cost $T_A$ such that

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

Then, by Theorem 4, 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 $t = \log(4/\mathsf{Adv}^{\mathrm{CS}}_{\mathcal{P}}) \le \lambda + 2$. It follows from Theorem 8 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[10]

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

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 $\lambda$ bit secure one-way function, a contradiction. Hence, the statement follows. □

## 6 Search Games as Decision Games

We show that every $\lambda$-bit secure search game can be formalized as a decision game with (almost) $\lambda$-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

[10] We assume $T_A \ge 1$.

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 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 $O_{\mathrm{aprv}}$ 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 $O_{\mathrm{aprv}}$ 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 6.** *If a search game $G$ satisfies*

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

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

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

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

*Proof.* Suppose that $\mathrm{BS}^{\mu}_{G'} < \lambda$. It follows from Theorem 9 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 $O_{\mathrm{aprv}}$, the above inequality implies that $A$ queries a value $a$ to $O_{\mathrm{aprv}}$ 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 $O_{\mathrm{aprv}}$, the adversary outputs $a$. It follows from Theorem 8 that

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

a contradiction.

For the other direction, suppose that $\mathrm{BS}^{\mu}_{G} < \lambda$. 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 $O_{\mathrm{aprv}}$. Finally, $A'$ outputs 0 if the answer from $O_{\mathrm{aprv}}$ 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

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

a contradiction. □

Theorem 6 implies that all the security games we need to consider are decision games if a constant difference of bit security can be ignored.

# 7 Distribution Replacement 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 $\lambda$-bit secure, to what extent does $Q$ need to be indistinguishable from $P$ to preserve that $G^P$ is $\lambda$-bit secure? We prove a natural reduction showing that $\lambda$-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 $G^{\mathrm{ind}}_{P,Q} = (X, R, O)$ 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 $\lambda - \mathcal{O}(1)$.

Due to Theorem 6, it is sufficient to prove the theorem for decision games.

**Theorem 7.** *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 $G^{\mathrm{ind}}_{P,Q}$ has $\lambda$-bit security. If game $G^Q$ has $\lambda$-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 Theorem 9, there is an inner adversary $A$ for game $G^P$ with computational complexity $T_A$ such that

$$d_{\mathsf{HD}}(A^P_0, A^P_1) > \sqrt{\frac{T_A \cdot \ln(1/4\mu)}{2^{\lambda-\alpha+1}}} \tag{15}$$

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

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

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 $G^{\mathrm{ind}}_{P,Q}$. We construct an inner adversary $\tilde{A}$ for the game $G^{\mathrm{ind}}_{P,Q}$ 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 $G^{\mathrm{ind}}_{P,Q}$, each answer from $O$ is an independent sample according to $P$ if the secret bit $\tilde{u}$ of $G^{\mathrm{ind}}_{P,Q}$ 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 $G^{\mathrm{ind}}_{P,Q}$ and its computational complexity is $T_A$. Since $G^{\mathrm{ind}}_{P,Q}$ has $\lambda$-bit security, it follows from Theorem 8 that

$$\lambda \leq \mathrm{BS}^{\mu}_{G^{\mathrm{ind}}_{P,Q}} \leq \log_2 \left( \frac{T_A \cdot \ln(1/2\mu)}{\mathsf{Adv}^{\mathrm{Renyi}}_{G^{\mathrm{ind}}_{P,Q},\tilde{A}}} \right), \tag{16}$$

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

$$\mathsf{Adv}^{\mathrm{Renyi}}_{G^{\mathrm{ind}}_{P,Q},\tilde{A}} = \mathsf{Adv}^{\mathrm{Renyi}}_{G^{P,Q}_u,A} = D_{1/2}(A^P_u \| A^Q_u). \tag{17}$$

Thus, by (2), (16), and (17),

$$d_{\mathsf{HD}}(A^P_u, A^Q_u) \leq \sqrt{\frac{1}{2} \cdot D_{1/2}(A^P_u \| A^Q_u)} \leq \sqrt{\frac{T_A \cdot \ln(1/2\mu)}{2^{\lambda+1}}} \tag{18}$$

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

The triangle inequality of $d_{\mathsf{HD}}$ and (18) implies that

$$\begin{aligned} d_{\mathsf{HD}}(A_0^P, A_1^P) &\le d_{\mathsf{HD}}(A_0^P, A_0^Q) + d_{\mathsf{HD}}(A_0^Q, A_1^Q) + d_{\mathsf{HD}}(A_1^Q, A_1^P) \\ &\le d_{\mathsf{HD}}(A_0^Q, A_1^Q) + \sqrt{\frac{T_A \cdot \ln(1/2\mu)}{2^{\lambda-1}}}. \end{aligned} \tag{19}$$

It follows from (15) and (19) that

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

by assumption on $\alpha$. Then, we have

$$\mathsf{Adv}^{\mathrm{Renyi}}_{A,G^Q} = D_{1/2}(A_0^Q \| A_1^Q) \ge 2d_{\mathsf{HD}}(A_0^Q, A_1^Q)^2 > \frac{4T_A \cdot \ln(1/2\mu)}{2^{\lambda}}.$$

By Theorem 8, 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 7 is a generalization of [18, Theorem 9], where the condition is that $d_{\mathsf{HD}}(P, Q) \le 2^{-\lambda/2}$. The above theorem only requires a computational condition that $G^{\mathrm{ind}}_{P,Q}$ has $\lambda$-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* $(k, \lambda)$-extractor *if for every distribution* $X$ *over* $\{0,1\}^n$ *with* $H_{\mathsf{min}}(X) \ge k$*, a 1-bit security game* $G^{\mathrm{ext}}_{\mathsf{Ext},X} := G^{\mathrm{ind}}_{P,Q}$ *has* $\lambda$*-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 $\mathsf{Ext}$ is a $(k, \varepsilon)$-*it-extractor* if for every distribution $X$ with $H_{\mathsf{min}}(X) \ge k$,

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

We can see that if $\mathsf{Ext}$ is a $(k, 2^{-\lambda})$-it-extractor, then $\mathsf{Ext}$ is a $(k, \lambda)$-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, 12]. 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 4** (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 $x, x' \in \{0,1\}^n$, $\Pr_{H\sim\mathcal{H}}(H(x) = H(x')) \le 2^{-m}$. 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 $\mathsf{Ext}$ gives an extractor for the Hellinger distance[11]. Namely, for the defined parameters, we have that

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

By (2), it holds that

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

Hence, the statement follows. □

We apply Theorem 7 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 $\lambda$-bit secure PRG. In other words, the game $G^{\mathrm{ind}}_{g(U_{d'}),U_d}$ has $\lambda$-bit security. Since the extractor of Lemma 4 is a $(k,\lambda)$-extractor, Theorem 7 guarantees that the seed of the LHL can be replaced by the output of $g$. Namely, the distribution $(H(X), g(S'))$ is $\lambda$-bit secure indistinguishable from the uniform distribution $U_{m+d}$, where $X$ is a source with $H_{\mathsf{min}}(X) \ge k$, $S' = U_{d'}$, and $H$ is randomly chosen from a family of universal hash functions using the seed $g(S')$.[12]

### 7.1.1 Entropy Loss in LHL

The *entropy loss* of $(k,\varepsilon)$-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 [15] that the entropy loss of $2\log(1/\varepsilon)$ is necessary for constructing a $(k,\varepsilon)$-it-extractor where the closeness $\varepsilon$ 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 [14]. The entropy loss for preserving $\lambda$-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 Future Perspective

This paper has shown that the two notions of bit security in [14] and [18] are equivalent by proving that the CS advantage and the Rényi advantage can be related. Thus, in future research on bit security, we can flexibly use these two advantages depending on the situations. For instance, as seen in Section 5, the CS advantage might be useful in the context of reduction via decoding with erasure (cf. [11]). On the other hand, we might use nice properties of the Rényi divergence, such as the convexity, to evaluate the Rényi advantage for certain types of randomized adversaries.

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

[12] 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 $S'$.

# A Characterization of Bit Security of [18]

The following theorems are the characterization proved in [18].

**Theorem 8.** *[18, Theorem 1] Let $G$ be an $n$-bit security game, and $A$ be its inner adversary with success probability $\varepsilon_A > 0$, computational complexity $T_A$, and Rényi advantage $\mathsf{Adv}_A^{\mathrm{Renyi}} > 0$. Then, we have*

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

**Theorem 9.** *[18, Theorem 2] If an $n$-bit game $G$ is not $\lambda$-bit secure, i.e., $\mathrm{BS}_G^{\mu} < \lambda$, then there exists an inner adversary $A$ for the game such that $A$ has computational complexity $T_A$ and satisfies*

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

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

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

*and*

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

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

# B Equivalence of (6)-(8)

Note that

$$\mathbb{E}[\psi(A)^2] = \Pr(A \neq \perp) \tag{20}$$

and

$$\begin{aligned} \mathbb{E}[\psi(A)\psi(U)] &= \Pr(A = U) - \Pr(A \neq \perp, A \neq U) \\ &= \Pr(A = U) - \big(\Pr(A \neq \perp) - \Pr(A \neq \perp, A = U)\big) \\ &= 2\Pr(A = U) - \Pr(A \neq \perp), \end{aligned} \tag{21}$$

where we used

$$\Pr(A = U) = \Pr(A \neq \perp, A = U) \tag{22}$$

in the third equality. By substituting (20) and (21) into (6), we have (7). By noting (22), (8) follows from (7).

## 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] Boaz Barak, Yevgeniy Dodis, Hugo Krawczyk, Olivier Pereira, Krzysztof Pietrzak, François-Xavier Standaert, and Yu Yu. Leftover hash lemma, revisited. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2011. doi:10.1007/978-3-642-22792-9_1.

[3] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Serge Vaudenay, editor, *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*, volume 4004 of *Lecture Notes in Computer Science*, pages 409–426. Springer, 2006. doi:10.1007/11761679_25.

[4] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41(6):1915–1923, 1995. doi:10.1109/18.476316.

[5] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. How to reduce your enemy's information (extended abstract). In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 468–476. Springer, 1985. doi:10.1007/3-540-39799-X_37.

[6] Yevgeniy Dodis and John P. Steinberger. Message authentication codes from unpredictable block ciphers. In Shai 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. doi:10.1007/978-3-642-03356-8_16.

[7] Oded Goldreich. *The Foundations of Cryptography - Volume 1: Basic Techniques*. Cambridge University Press, 2001. URL: http://www.wisdom.weizmann.ac.il/%7Eoded/foc-vol1.html, doi:10.1017/CBO9780511546891.

[8] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In David 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. doi:10.1145/73007.73010.

[9] Shafi Goldwasser and Yael Tauman Kalai. Cryptographic assumptions: A position paper. In Eyal Kushilevitz and Tal 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 505–522. Springer, 2016. doi:10.1007/978-3-662-49096-9_21.

[10] 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.

[11] G. Hast. Nearly one-sided tests and the Goldreich-Levin predicate. *Journal of Cryptology*, 17:209–229, 2004.

[12] Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Pseudo-random generation from one-way functions (extended abstracts). In David S. Johnson, editor, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washigton, USA*, pages 12–24. ACM, 1989. doi:10.1145/73007.73009.

[13] Leonid A. Levin. Randomness and non-determinism. *Journal of Symbolic Logic*, 58(3):1102–1103, 1993. doi:10.1137/S0895480197329508.

[14] Daniele Micciancio and Michael Walter. On the bit security of cryptographic primitives. In Jesper Buus Nielsen and Vincent 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. doi:10.1007/978-3-319-78381-9_1.

[15] Jaikumar Radhakrishnan and Amnon Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM J. Discrete Math.*, 13(1):2–24, 2000. doi:10.1137/S0895480197329508.

[16] Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *IACR Cryptol. ePrint Arch.*, page 332, 2004. URL: http://eprint.iacr.org/2004/332.

[17] T. van Erven and P. Harremoës. Rényi divergence and Kullback-Leibler divergence. *IEEE Trans. Inform. Theory*, 60(7):3797–3820, July 2014.

[18] Shun Watanabe and Kenji Yasunaga. Bit security as computational cost for winning games with high probability. In Mehdi Tibouchi and Huaxiong Wang, editors, *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*, volume 13092 of *Lecture Notes in Computer Science*, pages 161–188. Springer, 2021. doi:10.1007/978-3-030-92078-4_6.

[19] Kenji Yasunaga. Replacing probability distributions in security games via Hellinger distance. In Stefano 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. URL: https://drops.dagstuhl.de/opus/volltexte/2021/14336, doi:10.4230/LIPIcs.ITC.2021.17.