Bit-Security Preserving Hardness Amplification

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. Hardness amplification is one of the important reduction techniques in cryptography, and it has been extensively studied in the literature. The standard XOR lemma known in the literature evaluates the hardness in terms of the probability of correct prediction; the hardness is amplified from mildly hard (close to 1) to very hard $1/2+\varepsilon$ by inducing ε^2 multiplicative decrease of the circuit size. Translating such a statement in terms of the bit-security framework introduced by Micciancio-Walter (EUROCRYPT 2018) and Watanabe-Yasunaga (ASIACRYPT 2021), it may cause the bit-security loss by the factor of $\log(1/\varepsilon)$. To resolve this issue, we derive a new variant of the XOR lemma in terms of the Rényi advantage, which directly characterizes the bit security. In the course of proving this result, we prove a new variant of the hardcore lemma in terms of the conditional squared advantage; our proof uses a boosting algorithm that may output the $\perp$ symbol in addition to 0 and 1, which may be of independent interest.

1 Introduction

In modern cryptography, cryptographic primitives are usually proposed with security proofs. When proving the security of a primitive under some hardness assumption, we show a *reduction* that solves a hard problem by assuming the existence of an adversary attacking the primitive. If the reduction requires much more computational cost than the assumed adversary, we need a stronger hardness assumption to achieve a target level of security. Thus, *tight* reductions of security proofs are desirable for the efficient use of cryptographic primitives.

A recent approach of *concrete security* reveals quantities related to security reductions. Suppose we want to prove the security of primitive Q assuming the security of primitive P (or hardness of some problem). Typically, we show that for any adversary B of primitive Q with running time $t_B(n)$ and advantage $\varepsilon_B(n)$, there is an adversary A of primitive P such that the running time $t_A(n)$ and the advantage $\varepsilon_A(n)$ satisfy $t_A(n) \leq \phi(t_B(n))$ and $\varepsilon_A(n) \geq \psi(\varepsilon_B(n))$ for some functions ϕ and ψ. Here, n is a security parameter, and a reduction is a construction of A out of B. We may understand the tightness of the reduction by specifying two functions, ϕ and ψ. We prefer smaller $t_A(n)$ and larger $\varepsilon_A(n)$ for tight reductions. Thus, it is tempted to combine the two quantities as $t_A(n)/\varepsilon_A(n)$ and achieve the value as small as $t_B(n)/\varepsilon_B(n)$ of adversary B.

Namely, we want the loss function

$$L(n) = \frac{t_A(n)}{\varepsilon_A(n)} \cdot \frac{\varepsilon_B(n)}{t_B(n)}$$

to be as small as possible.

The above way of quantifying the security loss has been used in the cryptographic literature. In [24], the quantity of $t_A(n)/\varepsilon_A(n)$ was used to define the security of primitives. The same treatment has been employed in the literature [4, 2, 27, 6]. For *search* primitives such as one-way functions and signature schemes, the advantage $\varepsilon_A(n)$ is simply defined as the adversary's success probability. For *decision* primitives such as pseudorandom generators and encryption schemes, it is usually defined as the gap between two probabilities, which we want to be as small as possible. This treatment of defining advantages has been standard in the cryptography community. In the literature listed above, the advantage $\varepsilon_A(n)$ was defined in this way for analyzing the quantity $t_A(n)/\varepsilon_A(n)$.

In [11], Goldreich noted that Levin suggested using another quantity $t_A(n)/\varepsilon_A^2(n)$, called *work*, for decision primitives. The reason is that if the gap of two probabilities is $\varepsilon_A(n)$, we need to repeat the experiment (security game) for $\mathcal{O}(1/\varepsilon_A(n)^2)$ times to amplify it to a constant, say $2/3$. The use of this quantity was not justified well at that time.

Micciancio and Walter [26] initiated a theoretical study for quantifying the security level of primitives, referring to it as *bit security*. They proposed using another notion of advantage, which we call *conditional squared (CS) advantage*, for evaluating the decision primitives. Their notion elegantly resolved paradoxical situations in pseudorandom generators and approximate samplers. In [23], the notion of [26] was extended for capturing both computational and statistical parameters. The authors [30] defined bit security with an *operational meaning* to justify the formalization of the security level of primitives and characterized the quantity by another notion called *Rényi advantage*. The follow-up work [31] demonstrated that the two advantages of [26, 30] are essentially equivalent[3].

In this work, based on the recent advances in the notion of bit security (or the quantity $t_A(n)/\varepsilon_A(n)$), we focus on a basic problem of *hardness amplification* [13] of Boolean functions. A Boolean function $f : \{0,1\}^n \to \{0,1\}$ is said to be *mildly hard (unpredictable)* if every polynomial-time algorithm fails to compute f on a δ-fraction of input $x \in \{0,1\}^n$ for a noticeable δ. The task of hardness amplification is to convert f into another function f' so that f' is *strongly hard* in the sense that every polynomial-time algorithm fails to compute f' on a $(1/2-\varepsilon)$-fraction of input. The most well-known technique is Yao's XOR lemma; $f'(x_1, \ldots, x_k) = f(x_1) \oplus \cdots \oplus f(x_k)$ for $x_i \in \{0,1\}^n$. In the framework of bit security, hardness amplification is to reduce the advantage $\mathsf{Adv}_{A,f}(n)(= 1/2-\delta)$ to $\mathsf{Adv}_{B,f'}(n)(= \varepsilon)$, where $\mathsf{Adv}_{A,f}(n)$ is the advantage of adversary A predicting f over random guessing.

[3] Generally, the CS advantage is bounded above by the Rényi advantage. While the CS advantage may take a much smaller value in some cases, the CS advantage can be increased to the level of the Rényi advantage by modifying adversaries appropriately.

In the two bit-security frameworks of [26, 30], a decision game is formalized such that an adversary tries to guess the secret bit $u \in \{0,1\}$ by playing the game. Thus, we can write a decision game as $G = (G_0, G_1)$, where a secret bit u is initially chosen uniformly at random, and the adversary plays G_u for guessing u. The hardness of predicting a Boolean function $f : \{0,1\}^n \to \{0,1\}$ can be captured by the game G_f as follows; first $x \in \{0,1\}^n$ and $\sigma \in \{0,1\}$ are chosen uniformly at random. Then, the adversary receives $(x, f(x))$ when $u = 0$, and (x, σ) when $u = 1$, and outputs a symbol in $\{0, 1, \perp\}$.[4]

When employing the framework of [30, 31], the bit security of game $G_f = (G_0, G_1)$ against adversaries with computational cost s can be approximated as

$$\mathrm{BS}_s(G_f) = \log \min_{A \text{ with cost } s} \frac{s}{\mathsf{Adv}^{\mathrm{Renyi}}_{A,G_f}}, \tag{1}$$

where $\mathsf{Adv}^{\mathrm{Renyi}}_{A,G_f} = D_{1/2}(A_0 \| A_1)$ is the Rényi advantage of A in game G_f, $D_{1/2}(\cdot\|\cdot)$ is the Rényi divergence of order $1/2$, and A_u is the output distribution of A when playing G_u.

With the notions of bit security, hardness amplification is the task of converting f into f' such that $\max_B \mathsf{Adv}^{\mathrm{Renyi}}_{B,G_{f'}}$ is much smaller than $\max_A \mathsf{Adv}^{\mathrm{Renyi}}_{A,G_f}$, where A and B are taken over adversaries with costs s and s', respectively. We want the following loss function

$$L^{\mathrm{amp}}(n) = \frac{s \cdot \max_B \mathsf{Adv}^{\mathrm{Renyi}}_{B,G_{f'}}}{s' \cdot \max_A \mathsf{Adv}^{\mathrm{Renyi}}_{A,G_f}}$$

to be as small as possible. Ideally, we want to achieve $L^{\mathrm{amp}}(n) = \mathcal{O}(1)$.

The most efficient reductions of the XOR lemma until now were given in [21, 3] using boosting versions of *hardcore lemmas* [19]. They guarantee $s' = \Omega(\varepsilon^2/\log(1/\delta)) \cdot s$, where $\max_A \Pr(A(x) = f(x)) = 1 - \delta$ and $\max_B \Pr(B(x) = f'(x)) = 1/2 + \varepsilon$, where the maxima are taken over algorithms with cost s and s', respectively. Such a *predictor* A with $\Pr(A(x) = f(x)) = 1 - \delta$ can be easily converted to a *distinguisher* A' with the same cost such that $\mathsf{Adv}^{\mathrm{TV}}_{A',G_f} = d_{\mathsf{TV}}(A'_0, A'_1) = (1-\delta) - 1/2 = 1/2 - \delta$, where $d_{\mathsf{TV}}(\cdot,\cdot)$ is the total variation distance. For any adversary A of game $G_f = (G_0, G_1)$, it holds that

$$\left(\mathsf{Adv}^{\mathrm{TV}}_{A,G_f}\right)^2 \le \mathsf{Adv}^{\mathrm{Renyi}}_{A,G_f} \le \mathcal{O}\left(\mathsf{Adv}^{\mathrm{TV}}_{A,G_f}\right).$$

Thus, if $\mathsf{Adv}^{\mathrm{Renyi}}_{A,G_f} \approx \left(\mathsf{Adv}^{\mathrm{TV}}_{A,G_f}\right)^2$ holds for every adversary A, the XOR lemma in [21, 3] gives

$$L^{\mathrm{amp}}(n) = \mathcal{O}\left(\frac{\log(1/\delta)}{\varepsilon^2} \cdot \frac{\varepsilon^2}{(1/2-\delta)^2}\right) = \mathcal{O}(\log(1/\delta)),$$

meaning that the reduction seems to be optimal. Indeed, as observed in [30], $\mathsf{Adv}^{\mathrm{Renyi}}_{A,G_f} \approx \left(\mathsf{Adv}^{\mathrm{TV}}_{A,G_f}\right)^2$ holds for *balanced* adversaries, who output every value

[4] The symbol $\perp$ indicates that the adversary gives up the prediction.

with probability $\Omega(1)$. However, generally, we have $\mathsf{Adv}^{\mathrm{Renyi}}_{A,G_f} = \mathcal{O}\left(\mathsf{Adv}^{\mathrm{TV}}_{A,G_f}\right)$. Thus, the reductions in [21, 3] imply that

$$L^{\mathrm{amp}}(n) = \mathcal{O}\left(\frac{\log(1/\delta)}{\varepsilon^2} \cdot \frac{\varepsilon}{1/2-\delta}\right) = \mathcal{O}\left(\frac{\log(1/\delta)}{\varepsilon}\right), \tag{2}$$

which does not seem to be optimal.

1.1 Our results

In this work, in order to evaluate the bit security of hardness amplification directly, we derive a new variant of the XOR lemma in terms of the Rényi advantage. Roughly, our XOR lemma claims that if a function is mildly hard in the sense that $\Pr(A(x) = f(x)) \leq 1-\delta$ for any adversary A of size s, then the Rényi advantage of the XOR function f' satisfies $\mathsf{Adv}^{\mathrm{Renyi}}_{B,G_{f'}} \leq \varepsilon$ for any adversary B of size $s' = \Omega(\varepsilon/\ln(1/\delta)) \cdot s$.[5] This implies that the loss of the reduction is

$$L^{\mathrm{amp}}(n) = \mathcal{O}\left(\frac{\log(1/\delta)}{\varepsilon} \cdot \frac{\varepsilon}{1/2-\delta}\right) = \mathcal{O}\left(\log(1/\delta)\right),$$

which improves upon the loss in (2) by the factor of $1/\varepsilon$ for general adversaries.

To derive our XOR lemma for the Rényi advantage, we prove a new variant of the hardcore lemma, originally proved by Impagliazzo [19]. Our hardcore lemma is stated in terms of the CS advantage. Then, by using the connection between the CS advantage and the Rényi advantage in [31], we prove the XOR lemma via the hardcore lemma.

To prove our hardcore lemma, we analyze the performance of the boosting algorithm such that weak learners may output the $\perp$ symbol in addition to 0 and 1. Our main technical contribution in this paper is characterizing the performance of the boosting algorithm with $\perp$ in terms of the CS advantage.

1.2 Related work

The study of hardness amplification has a long history, and there are several proofs of the XOR lemma; see [9] for a thorough review. As mentioned in Section 1.1, in this paper, we prove our XOR lemma along the line of the proof by Impagliazzo using the hardcore lemma [19].

Another line of studies on hardness amplification is the direct-product constructions; it aims to construct strongly hard (search type) functions from weak ones [12, 10, 22]. See [22] and the literature therein for recent related work. In this work, we focus on amplifying the hardness of Boolean (decision type) functions.

In the original paper [19], Impagliazzo provided two proofs of the hardcore lemma, a constructive one and one based on the min-max theorem.[6] Later, it

[5] More precisely, this statement assumes that a weighted majority can be implemented for free. If $s = \omega(\log(1/\delta)/\varepsilon^2)$, the cost of the weighted majority is negligible; See Remark 1 for discussion.

[6] The latter was attributed to Nisan.

was pointed out that the constructive proof can be interpreted as the boosting algorithm in learning theory [21]. Based on such identification, there have been several improvements and applications of the hardcore lemma [18, 20, 3, 25, 29].

In contrast to the standard hardcore lemma stated in terms of the probability of correct prediction, our hardcore lemma is stated in terms of the CS advantage. The main difficulty of handling the CS advantage is that it may not be linear with respect to either the input distribution or (stochastic) circuit. Thus, it is unclear if the min-max theorem is applicable to prove the hardcore lemma for the CS advantage. To overcome this difficulty, we devise a modified version of boosting algorithm in [20, 3] by considering that the adversary (weak learner in the context of learning) may output $\perp$ in addition to 0 and 1. In the context of learning theory, by considering the asymmetry of weak learners' confidence for each output, we can improve the standard AdaBoost, which is known as the confidence-rated AdaBoost or the infoBoosting [28, 1, 16, 17]. Our boosting algorithm is closely related in spirit to those algorithms in the sense that the symbol $\perp$ signifies that weak learners' confidence is zero. Since the CS advantage is a criterion initiated in cryptography, we believe it is an interesting contribution to characterize the boosting algorithm with $\perp$ in terms of the CS advantages of weak learners; perhaps, it may have certain applications in learning theory.

A utility of the CS advantage in the context of the Goldreich-Levin (GL) algorithm has been reported by Hast in [15]; he proposed a modified version of the GL algorithm by taking into account adversaries that may output $\perp$ when predicting the hardcore bit and characterized the performance of such a GL algorithm in terms of the CS advantage. His algorithm was used in [31] to prove the tightness of the GL theorem. In this work, we use the utility of outputting $\perp$ in a hardcore lemma to provide a tight reduction of hardness amplification.

1.3 Paper organization

We present the formulation of the hardness amplification and the XOR lemma for the Rényi advantage in Section 2. In Section 3, we present the hardcore lemma for the CS advantage and its proof using the boosting algorithm with $\perp$. Section 4 presents the proof of the XOR lemma by using the hardcore lemma. Other than the fact of approximation as in (1), we do not use the knowledge of bit security frameworks [26, 30]. For readers' convenience, we review the bit-security frameworks in Appendix A.

2 Hardness amplification for Rényi advantage

For $0 \leq \rho \leq 1$ and a function $f : \{0,1\}^n \to \{0,1\}$, ρ-hardness $\mathrm{H}^{\rho}_{\mathsf{avg}}(f)$ of function f is the largest integer s such that any circuit $C : \{0,1\}^n \to \{0,1,\perp\}$ of size at most s satisfies

$$\Pr_{x \sim U_n}\big(C(x) = f(x)\big) \leq \rho,$$

where U_n is the uniform distribution on $\{0,1\}^n$. For a prescribed (typically small) margin $\delta > 0$, a function f is regarded as *mildly hard* if the value of $\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$ is sufficiently large. By using the function f as a building block, we are interested in constructing another function that is much harder than f itself. A typically used construction is the so-called XOR construction: for a given integer $k \geq 2$, let $f^{\oplus k} : \{0,1\}^{nk} \to \{0,1\}$ be the function defined by

$$f^{\oplus k}(x_1, \ldots, x_k) := f(x_1) \oplus \cdots \oplus f(x_k),$$

where $x_1, \ldots, x_k \in \{0,1\}^n$. The standard XOR lemma of Yao claims that $f^{\oplus k}$ is hard in the sense that $\mathrm{H}^{1/2+\varepsilon}_{\mathsf{avg}}(f^{\oplus k})$ is as large as $\frac{\varepsilon^2}{\ln(1/\delta)}\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$ for $\varepsilon \geq 2(1-\delta)^k$; this means that even though the circuit size is decreased by the factor of $\frac{\varepsilon^2}{\ln(1/\delta)}$, we can guarantee that the adversary's success probability of predicting the value of function $f^{\oplus k}$ is at most $\frac{1}{2} + \varepsilon$. More precisely, the following holds:

Proposition 1 (XOR lemma). *For $\varepsilon \geq 2(1-\delta)^k$, it holds that*

$$\Pr_{x_1,\ldots,x_k \sim U_n}\left(C(x_1, \ldots, x_k) = f^{\oplus k}(x_1, \ldots, x_k)\right) \leq \frac{1}{2} + \varepsilon$$

for every circuit C of size at most s for $s = \Omega\left(\frac{\varepsilon^2}{\ln(1/\delta)}\right) \cdot \mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$.

In order to discuss the bit security of the XOR function, let us consider the distinguishing game between $u = 0$ instance $(x_1, \ldots, x_k, f^{\oplus k}(x_1, \ldots, x_k))$ and $u = 1$ instance $(x_1, \ldots, x_k, \sigma)$, where σ is a random bit that is independent of $(x_1, \ldots, x_k)$. Proposition 1 implies that (by the standard argument of converting a distinguisher to a predictor), for every circuit of size at most s, the standard distinguishing advantage (in terms of the total variation distance) is less than ε. However, as discussed in [26, 30] (see also [31] for more detail), the standard advantage is not suitable for evaluating bit security. Thus, the above-mentioned XOR lemma does not guarantee that the bit security is preserved during the process of constructing $f^{\oplus k}$ from f. To resolve this issue, we derive an alternative version of the XOR lemma in terms of Rényi advantage

$$\mathsf{Adv}^{\mathrm{Renyi}}_{A, f^{\oplus k}} = D_{1/2}(A_0 \| A_1) = -2 \ln \sum_a \sqrt{A_0(a) A_1(a)},$$

where A_u is the distribution of the output by adversary when the instance is u. As we mentioned in Section 1 (see also Appendix A), the bit security can be approximated by the Rényi advantage up to a constant. To that end, it is desirable to derive a trade-off between the adversary's Rényi advantage and the circuit size. We use the weighted majority gate once in the reduction proof of the following theorem. To avoid the effect of how the weighted majority gate is implemented, we first assume that the weighted majority gate is available for free in the evaluation of the initial hardness $\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$; in Remark 1, we will provide an estimate for the effect of implementing the weighted majority gate.

Theorem 1 (XOR lemma for Rényi advantage). *For $\varepsilon \geq 2(1-\delta)^k$, it holds that*

$$\mathsf{Adv}^{\mathrm{Renyi}}_{A,f^{\oplus k}} \leq \varepsilon$$

for every circuit A of size $s' \leq \frac{\varepsilon}{48\ln(1/\delta)}\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$, where the initial hardness $\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$ is evaluated under the assumption that the weighted majority gate is available for free.

Remark 1. The assumption of the availability of the weighted majority gate comes from the fact that it is used in the proof of the hardcore lemma of Lemma 1. As we discuss in Remark 2, the effect of implementing the weighted majority gate can be estimated. More specifically, the statement of Theorem 1 holds for circuit size $s' \leq \frac{\varepsilon}{64\ln(1/\delta)}\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f) - \frac{c}{\varepsilon}$ for some constant c. Thus, when the initial hardness is $\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f) = \omega(\log(1/\delta)/\varepsilon^2)$, then the effect of the weighted majority is negligible.

We shall discuss an implication of Theorem 1. For a given integer s, the bit security against adversaries with cost s is evaluated as (1). In fact, in the setting of this section, the initial hardness $s = \mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$ means $\mathrm{BS}_s(G_f) = \log s + \mathcal{O}(1)$. For the function f itself, since circuits of much smaller size s' may have the same success probability $1-\delta$, we cannot guarantee $\mathrm{BS}_{s'}(G_f) \geq \mathrm{BS}_s(G_f)$. However, Theorem 1 implies that the XOR function $f^{\oplus k}$ satisfies

$$\mathrm{BS}_{s'}(G_{f^{\oplus k}}) \geq \mathrm{BS}_s(G_f) - \mathcal{O}(\log\ln(1/\delta))$$

for $s' = \frac{\varepsilon}{48\ln(1/\delta)}\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$. In this sense, the bit security is preserved in the hardness amplification.

3 Hardcore lemma for CS advantage

We shall prove Theorem 1 along the line of the proof by Impagliazzo using the hardcore lemma [19]. To that end, we develop a new variant of the hardcore lemma in this section.

By the definition of hardness, any circuit C of size $s \leq \mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$ must satisfy

$$\Pr_{x\sim U_n}\big(C(x) = f(x)\big) \leq 1-\delta. \tag{3}$$

This means that there exists a set $\mathcal{H}_C \subset \{0,1\}^n$ of hard inputs such that $|\mathcal{H}_C| \geq \delta 2^n$ and the circuit C fails to compute $f(x)$ for every $x \in \mathcal{H}_C$; however, the hard sets may differ for different circuits. Impagliazzo's hardcore lemma claims that there exists a set of inputs that are universally hard for every circuit having a smaller size. It is more convenient to consider probability distributions, rather than sets, having density δ; a distribution P on $\{0,1\}^n$ is said to have density δ if $P(x) \leq \frac{1}{\delta 2^n}$ for every $x \in \{0,1\}^n$, or equivalently, the min-entropy satisfies $H_{\min}(P) \geq n - \log(1/\delta)$. The standard hardcore lemma is a statement as follows:

Proposition 2 (Hardcore lemma). *There exists a hardcore distribution H having density δ such that*

$$\Pr_{x\sim H}\big(C(x)=f(x)\big)\le\frac{1}{2}+\varepsilon \tag{4}$$

for every circuit C of size at most s for $s=\Omega\left(\frac{\varepsilon^2}{\ln(1/\delta)}\right)\cdot \mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$.

Since the standard hardcore lemma, Lemma 2, is insufficient to prove Theorem 1, we derive the following variant of the hardcore lemma in terms of the conditional squared (CS) advantage. For a given distribution P on $\{0,1\}^n$ and a circuit $C:\{0,1\}^n\to\{0,1,\bot\}$, the CS advantage of predicting f is defined as[7]

$$\mathsf{Adv}^{\mathrm{CS}}_{C,f|P}:=\frac{4\Big(\Pr(C(x)=f(x))-\frac{1}{2}\Pr(C(x)\neq\bot)\Big)^2}{\Pr(C(x)\neq\bot)} \tag{5}$$

$$=\frac{\Big(\Pr(C(x)=f(x))-\Pr(C(x)\neq\overline{f(x)})\Big)^2}{\Pr(C(x)\neq\bot)} \tag{6}$$

where the probability is with respect to $x\sim P$ and $\overline{f(x)}=f(x)\oplus 1$.

Lemma 1 (Hardcore lemma for CS advantage). *There exists a hardcore distribution H having density δ such that*

$$\mathsf{Adv}^{\mathrm{CS}}_{C,f|H}\le\varepsilon \tag{7}$$

for every circuit C of size at most $s':=\frac{\varepsilon}{8\ln(1/\delta)}\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$.

For a circuit that does not output $\bot$, i.e., $\Pr(C(x)\neq\bot)=1$, we can rewrite (5) as

$$\Pr(C(x)=f(x))=\frac{1}{2}+\frac{\sqrt{\mathsf{Adv}^{\mathrm{CS}}_{C,f|P}}}{2}.$$

For such a circuit, the bounds (4) and (7) are the same up to a constant (ε^2 in Lemma 2 corresponds to ε in Lemma 1). A main new feature of Lemma 1 is that it can be applied to circuits that may output $\bot$ with significant probability.

In contrast to the standard correct probability (the left-hand side of (4)), the CS advantage is not linear with respect to either the input distribution or (stochastic) circuit. Thus, it is unclear if the min-max theorem is applicable to prove Lemma 1. Instead, we consider a modified version of boosting algorithm by taking into account the fact that the adversary (weak learner in the context of learning) may output $\bot$ in addition to 0 and 1.

[7] More precisely, the CS advantage in (5) is for a predictor; on the other hand, when we define the bit security, we consider the CS advantage for a distinguisher (cf. (24)). The CS advantage for a predictor was first introduced in the context of the Goldreich-Levin algorithm [15].

Algorithm 1: Boosting

Input: The number $T \in \mathbb{N}$ of iteration and a circuit C_P satisfying (8) for each P with density δ

Output: A sequence of circuits $C_{P^{(1)}}, \dots, C_{P^{(T)}}$

1: Initialize $P^{(1)}$ as the uniform distribution on $\{0,1\}^n$;

2: Repeat Step 3 and Step 4 for $1 \le t \le T$;

3: For a circuit $C_{P^{(t)}}$ that satisfies (8) for $P^{(t)}$, set $\gamma_t = \frac{\Delta_t}{4\alpha_t}$ for

$$\alpha_t := \Pr_{x \sim P^{(t)}} \big(C_{P^{(t)}}(x) \neq \perp\big),$$
$$\Delta_t := \Pr_{x \sim P^{(t)}} \big(C_{P^{(t)}}(x) = f(x)\big) - \Pr_{x \sim P^{(t)}} \big(C_{P^{(t)}}(x) = \overline{f(x)}\big),$$

and set

$$\hat{P}^{(t+1)}(x) = \frac{P^{(t)}(x) \exp\big(-\gamma_t \big\{\mathbf{1}[C_{P^{(t)}}(x) = f(x)] - \mathbf{1}[C_{P^{(t)}}(x) = \overline{f(x)}]\big\}\big)}{Z_{P^{(t)}}},$$

where $\overline{f(x)} = f(x) \oplus 1$ and

$$Z_{P^{(t)}} = \sum_x P^{(t)}(x) \exp\big(-\gamma_t \big\{\mathbf{1}[C_{P^{(t)}}(x) = f(x)] - \mathbf{1}[C_{P^{(t)}}(x) = \overline{f(x)}]\big\}\big)$$

is the normalizer;

4: For the set $\mathcal{P}_\delta$ of all distributions with density δ, set

$$P^{(t+1)} = \operatorname*{argmin}_{P \in \mathcal{P}_\delta} D(P \| \hat{P}^{(t+1)}),$$

where D is the KL-divergence.

To prove Lemma 1 via a contradiction, suppose that for each distribution P having density δ, there exists a circuit C_P of size at most s' such that

$$\mathsf{Adv}^{\mathrm{CS}}_{C_P, f|P} > \varepsilon. \tag{8}$$

Starting from the uniform distribution $P^{(1)}$ and a circuit that satisfies (8) for $P^{(1)}$, we are going to sequentially update distributions and corresponding circuits that satisfy (8); then, by combining those circuits, we eventually construct a circuit that violates the assumption (3) on the hardness of f. As we mentioned above, this procedure is essentially the same as the boosting algorithm in learning theory, in which we construct a strong learner from weak learners. Our algorithm for boosting is described in Algorithm 1. The sequence of distributions generated by the algorithm satisfies the following.

Lemma 2. *The distributions $P^{(1)}, \dots, P^{(T)}$ generated by Algorithm 1 satisfy*

$$\sum_{t=1}^{T} \frac{1}{T} \frac{\mathsf{Adv}^{\mathrm{CS}}_{C_P^{(t)}, f|P^{(t)}}}{8}$$

$$\leq \mathbb{E}_{x\sim P}\left[\sum_{t=1}^{T}\frac{1}{T}\gamma_t\big\{\mathbf{1}[C_{P^{(t)}}(x)=f(x)]-\mathbf{1}[C_{P^{(t)}}(x)=\overline{f(x)}]\big\}\right]+\frac{D(P\|P^{(1)})}{T} \tag{9}$$

for every $P\in\mathcal{P}_\delta$, where $\mathcal{P}_\delta$ is the set of all distributions with density δ.

Proof. The proof proceeds along the line of [20, 3]; however, we need more careful analysis to take into account the probability of $\perp$. First, for an arbitrary $P\in\mathcal{P}_\delta$, from the definition of the KL-divergence and the update rule of $\hat{P}^{(t+1)}$, we have

$$\begin{aligned}
&D(P\|P^{(t)})-D(P\|\hat{P}^{(t+1)})\\
&=\sum_x P(x)\ln\frac{\hat{P}^{(t+1)}(x)}{P^{(t)}(x)}\\
&=-\gamma_t\sum_x P(x)\big\{\mathbf{1}[C_{P^{(t)}}(x)=f(x)]-\mathbf{1}[C_{P^{(t)}}(x)=\overline{f(x)}]\big\}-\ln Z_{P^{(t)}}\\
&=-\gamma_t\mathbb{E}_{x\sim P}\left[\big\{\mathbf{1}[C_{P^{(t)}}(x)=f(x)]-\mathbf{1}[C_{P^{(t)}}(x)=\overline{f(x)}]\big\}\right]-\ln Z_{P^{(t)}}.
\end{aligned}$$

Here, we can evaluate $\ln Z_{P^{(t)}}$ as

$$\begin{aligned}
\ln Z_{P^{(t)}}&=\ln\sum_x P^{(t)}(x)\exp\big(-\gamma_t\big\{\mathbf{1}[C_{P^{(t)}}(x)=f(x)]-\mathbf{1}[C_{P^{(t)}}(x)=\overline{f(x)}]\big\}\big)\\
&\leq\ln\sum_x P^{(t)}(x)\big(1-\gamma_t\big\{\mathbf{1}[C_{P^{(t)}}(x)=f(x)]-\mathbf{1}[C_{P^{(t)}}(x)=\overline{f(x)}]\big\}\\
&\qquad\qquad+2\gamma_t^2\mathbf{1}[C_{P^{(t)}}(x)\neq\perp]\big)\\
&=\ln\Bigg(1-\gamma_t\big\{\Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x)=f(x)\big)-\Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x)=\overline{f(x)}\big)\big\}\\
&\qquad\qquad+2\gamma_t^2\Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x)\neq\perp\big)\Bigg)\\
&\leq-\gamma_t\big\{\Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x)=f(x)\big)-\Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x)=\overline{f(x)}\big)\big\}\\
&\qquad\qquad+2\gamma_t^2\Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x)\neq\perp\big),
\end{aligned}$$

where the first inequality follows from[8] $e^{-\theta}\leq 1-\theta+2\theta^2$ for $\theta\in[-1,1]$ and that

$$\exp\big(-\gamma_t\big\{\mathbf{1}[C_{P^{(t)}}(x)=f(x)]-\mathbf{1}[C_{P^{(t)}}(x)=\overline{f(x)}]\big\}\big)=1$$

[8] By the Taylor approximation, we have

$$e^{-\theta}\leq 1-\theta+\sup_{-1\leq\tau\leq 1}\frac{e^{-\tau}}{2}\theta^2\leq 1-\theta+\frac{e}{2}\theta^2\leq 1-\theta+2\theta^2.$$

when $C_{P^{(t)}}(x) = \perp$; and the second inequality follows from $\ln(1-\theta) \le -\theta$ for $\theta < 1$. Thus, we have

$$\begin{aligned}
&D(P\|P^{(t)}) - D(P\|\hat{P}^{(t+1)}) \\
&\ge -\gamma_t \mathbb{E}_{x\sim P}\left[\left\{\mathbf{1}[C_{P^{(t)}}(x) = f(x)] - \mathbf{1}[C_{P^{(t)}}(x) = \overline{f(x)}]\right\}\right] \\
&\quad + \gamma_t\Big\{\Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x) = f(x)\big) - \Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x) = \overline{f(x)}\big)\Big\} \\
&\quad - 2\gamma_t^2 \Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x) \ne \perp\big). \qquad (10)
\end{aligned}$$

Here, we apply the Pythagorean inequality by noting that $\mathcal{P}_\delta$ is a closed convex set: it holds that (e.g., see [5, Theorem 3.1])

$$D(P\|P^{(t+1)}) + D(P^{(t+1)}\|\hat{P}^{(t+1)}) \le D(P\|\hat{P}^{(t+1)})$$

for any $P \in \mathcal{P}_\delta$, which implies

$$D(P\|P^{(t+1)}) \le D(P\|\hat{P}^{(t+1)}). \qquad (11)$$

Thus, (10) and (11) imply

$$\begin{aligned}
&D(P\|P^{(t)}) - D(P\|P^{(t+1)}) \\
&\ge -\gamma_t \mathbb{E}_{x\sim P}\left[\left\{\mathbf{1}[C_{P^{(t)}}(x) = f(x)] - \mathbf{1}[C_{P^{(t)}}(x) = \overline{f(x)}]\right\}\right] \\
&\quad + \gamma_t\Big\{\Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x) = f(x)\big) - \Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x) = \overline{f(x)}\big)\Big\} \\
&\quad - 2\gamma_t^2 \Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x) \ne \perp\big).
\end{aligned}$$

By taking the summation of the both sides for $t = 1$ through T, we have

$$\begin{aligned}
&D(P\|P^{(1)}) - D(P\|P^{(T+1)}) \\
&\ge -\mathbb{E}_{x\sim P}\left[\sum_{t=1}^{T}\gamma_t\left\{\mathbf{1}[C_{P^{(t)}}(x) = f(x)] - \mathbf{1}[C_{P^{(t)}}(x) = \overline{f(x)}]\right\}\right] \\
&\quad + \sum_{t=1}^{T}\gamma_t\Big\{\Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x) = f(x)\big) - \Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x) = \overline{f(x)}\big)\Big\} \\
&\quad - \sum_{t=1}^{T} 2\gamma_t^2 \Pr_{x\sim P^{(t)}}\big(C_{P^{(t)}}(x) \ne \perp\big). \qquad (12)
\end{aligned}$$

Since $D(P\|P^{(T+1)}) \ge 0$, by substituting α_t, Δ_t and $\gamma_t = \frac{\Delta_t}{4\alpha_t}$ defined in Algorithm 1, and by rearranging terms, we have

$$\begin{aligned}
&\sum_{t=1}^{T}\frac{\Delta_t^2}{8\alpha_t} \\
&\le \mathbb{E}_{x\sim P}\left[\sum_{t=1}^{T}\gamma_t\left\{\mathbf{1}[C_{P^{(t)}}(x) = f(x)] - \mathbf{1}[C_{P^{(t)}}(x) = \overline{f(x)}]\right\}\right] + D(P\|P^{(1)}).
\end{aligned}$$

Finally, by noting that $\mathsf{Adv}^{\mathrm{CS}}_{C_P^{(t)},f|P^{(t)}} = \frac{\Delta_t^2}{\alpha_t}$ and by dividing by T, we have (9). □

Proof of Lemma 1 To prove via a contradiction, suppose that for each distribution P having density δ, there exists a circuit C_P of size at most s' satisfying (8). We shall prove that there exists a circuit $C^\star$ of size at most $s := \mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$ such that

$$\Pr_{x\sim U_n}\big(C^\star(x) = f(x)\big) > 1-\delta. \tag{13}$$

We construct $C^\star$ as follows. For $T = \frac{8\ln(1/\delta)}{\varepsilon}$, let $C_{P^{(1)}}, \ldots, C_{P^{(T)}}$ be the circuits obtained by Algorithm 1. For a given input $x \in \{0,1\}^n$, by invoking the weighted majority oracle, $C^\star$ outputs $a \in \{0,1\}$ if (the tie can be decided arbitrarily)

$$\sum_{t=1}^{T} \frac{1}{T}\gamma_t\big\{\mathbf{1}[C_{P^{(t)}}(x) = a] - \mathbf{1}[C_{P^{(t)}}(x) = \overline{a}]\big\} > 0, \tag{14}$$

where $\overline{a} = a \oplus 1$. Note that the size of $C^\star$ is Ts'. Note also that $C^\star$ makes an error for input x, i.e., $C^\star(x) = \overline{f(x)}$ only if

$$\sum_{t=1}^{T} \frac{1}{T}\gamma_t\big\{\mathbf{1}[C_{P^{(t)}}(x) = f(x)] - \mathbf{1}[C_{P^{(t)}}(x) = \overline{f(x)}]\big\} \le 0. \tag{15}$$

Let

$$\mathcal{E} = \left\{x \in \{0,1\}^n : \sum_{t=1}^{T} \frac{1}{T}\gamma_t\big\{\mathbf{1}[C_{P^{(t)}}(x) = f(x)] - \mathbf{1}[C_{P^{(t)}}(x) = \overline{f(x)}]\big\} \le 0\right\}.$$

be the set of all inputs such that $C^\star$ may make an error. If we prove $\frac{|\mathcal{E}|}{2^n} < \delta$, we are done, i.e., (13) holds. To prove via a contradiction, assume that $\frac{|\mathcal{E}|}{2^n} \ge \delta$, which implies that the uniform distribution $P_{\mathcal{E}}$ on $\mathcal{E}$ has density δ. Since $P^{(1)}$ is the uniform distribution, we have

$$D(P_{\mathcal{E}}\|P^{(1)}) = \sum_x P_{\mathcal{E}}(x)\ln 2^n P_{\mathcal{E}}(x) \le \sum_x P_{\mathcal{E}}(x)\ln(1/\delta) = \ln(1/\delta).$$

By applying Lemma 2 for $P_{\mathcal{E}}$, by noting (8) for each $C_{P^{(t)}}$, and by noting that (15) with probability 1 for $x \sim P_{\mathcal{E}}$, we have

$$\begin{aligned}\frac{\varepsilon}{8} &< \mathbb{E}_{x\sim P_{\mathcal{E}}}\left[\sum_{t=1}^{T}\frac{1}{T}\gamma_t\big\{\mathbf{1}[C_{P^{(t)}}(x) = f(x)] - \mathbf{1}[C_{P^{(t)}}(x) = \overline{f(x)}]\big\}\right] + \frac{D(P_{\mathcal{E}}\|P^{(1)})}{T}\\ &\le \frac{D(P_{\mathcal{E}}\|P^{(1)})}{T}\\ &\le \frac{\varepsilon}{8},\end{aligned}$$

which is a contradiction. □

Remark 2. Even though we did not take into account the precision of the weight γ_t in the proof of Lemma 1, it can be evaluated as follows. Note that α_t and Δ_t in Algorithm 1 satisfy

$$\varepsilon < \frac{\Delta_t^2}{\alpha_t} \le \frac{\Delta_t}{\alpha_t} \le 1.$$

By setting $\tau = \lceil \log(1/\varepsilon) \rceil$ so that $\frac{1}{2^\tau} \le \varepsilon$, we divide the interval $(1/2^\tau, 1]$ into τ parts

$$\left(\frac{1}{2^\tau}, \frac{1}{2^{\tau-1}}\right], \left(\frac{1}{2^{\tau-1}}, \frac{1}{2^{\tau-2}}\right], \ldots, \left(\frac{1}{2}, 1\right].$$

Then, each $\frac{\Delta_t}{\alpha_t}$ satisfies

$$\frac{\Delta_t}{\alpha_t} \in \left(\frac{1}{2^{\ell_t}}, \frac{1}{2^{\ell_t - 1}}\right]$$

for some ℓ_t; if we set $\gamma_t = \frac{1}{2^{\ell_t+2}}$, then we have

$$\frac{\Delta_t}{8\alpha_t} \le \gamma_t < \frac{\Delta_t}{4\alpha_t}. \tag{16}$$

If we use $\gamma_t = \frac{1}{2^{\ell_t+2}}$ instead of $\gamma_t = \frac{\Delta_t}{4\alpha_t}$ in Algorithm 1, the last two terms of (12) is lower bounded as

$$\begin{aligned}
&\sum_{t=1}^{T} \gamma_t \Big\{ \Pr_{x\sim P^{(t)}} \left(C_{P^{(t)}}(x) = f(x)\right) - \Pr_{x\sim P^{(t)}} \left(C_{P^{(t)}}(x) = \overline{f(x)}\right) \Big\} \\
&\quad - \sum_{t=1}^{T} 2\gamma_t^2 \Pr_{x\sim P^{(t)}} \left(C_{P^{(t)}}(x) \neq \perp\right) \\
&= \sum_{t=1}^{T} \frac{\Delta_t^2}{\alpha_t} \gamma_t \frac{\alpha_t}{\Delta_t} \left(1 - 2\gamma_t \frac{\alpha_t}{\Delta_t}\right) \\
&\ge \sum_{t=1}^{T} \frac{\Delta_t^2}{\alpha_t} \frac{1}{8} \left(1 - \frac{2}{8}\right) = \sum_{t=1}^{T} \frac{3\Delta_t^2}{32\alpha_t},
\end{aligned}$$

where the inequality follows from that the function $g(\theta) = \theta(1-2\theta)$ is lower bounded by $g(1/8)$ for $1/8 \le \theta \le 1/4$ and (16). Thus, even if we take into account the precision of the weight γ_t, we have the same claim as Lemma 1 except that the factor $\frac{1}{8}$ in s' is replaced by $\frac{3}{32}$.

Furthermore, since each weight γ_t takes a value between $1/2^{\tau+2}$ and $1/8$, we can implement the weighted majority by creating $2^{\tau+2}\gamma_t \le 1/\varepsilon$ copies of each input and by using the majority.[9] If we take into account the cost of the weighted

[9] Such a naive implementation of the weighted majority has been studied in the circuit complexity [8].

majority, the proof goes through as long as

$$Ts' + \frac{cT}{\varepsilon} = T\left(s' + \frac{c}{\varepsilon}\right) \le s$$

for some constant c.[10] Thus, the claim of Lemma 1 still holds for every circuit of size at most $s' = \frac{3\varepsilon}{32\ln(1/\delta)}\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f) - \frac{c}{\varepsilon}$; when the initial hardness is $\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f) = \omega(\log(1/\delta)/\varepsilon^2)$, then the cost of the weighted majority is negligible.

4 Proof of Theorem 1

For notational simplicity, we prove the case of $k = 2$; general $k \ge 2$ can be proved similarly. Toward deriving a contradiction, suppose that there exists A with size $s' \le \frac{\varepsilon}{48\ln(1/\delta)}\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$ such that $\mathsf{Adv}^{\mathrm{Renyi}}_{A,f^{\oplus k}} > \varepsilon$. By Lemma 1, there exists a hardcore distribution H with density δ such that

$$\mathsf{Adv}^{\mathrm{CS}}_{C,f|H} \le \frac{\varepsilon}{6} \tag{17}$$

for every circuit C of size $s' \le \frac{\varepsilon}{48\ln(1/\delta)}\mathrm{H}^{1-\delta}_{\mathsf{avg}}(f)$. Let G be the distribution on $\{0,1\}^n$ given by $G(x) = \frac{1/2^n - \delta H(x)}{1-\delta}$. Then, the uniform distribution U_n on $\{0,1\}^n$ can be decomposed as

$$U_n(x) = (1-\delta)G(x) + \delta H(x). \tag{18}$$

When (x_1, x_2) are distributed according to distribution Q, we denote the output distribution of adversary A by A^Q_u for $u = 0, 1$ (note that, when $u = 1$, σ is generated independently of $(x_1, x_2) \sim Q$). Then, the output distribution A_u of adversary A under the uniform distribution can be decomposed as

$$A_u = (1-\delta)^2 A^{GG}_u + (1-\delta)\delta A^{GH}_u + \delta(1-\delta)A^{HG}_u + \delta^2 A^{HH}_u. \tag{19}$$

By the joint convexity of the Rényi divergence of order $1/2$ (e.g., see [7, Theorem 11]), we have

$$\begin{aligned}
\varepsilon &< \mathsf{Adv}^{\mathrm{Renyi}}_{A,f^{\oplus k}} \\
&= D_{1/2}(A_0 \| A_1) \\
&\le (1-\delta)^2 D_{1/2}(A^{GG}_0 \| A^{GG}_1) + (1-\delta)\delta D_{1/2}(A^{GH}_0 \| A^{GH}_1) \\
&\quad + \delta(1-\delta) D_{1/2}(A^{HG}_0 \| A^{HG}_1) + \delta^2 D_{1/2}(A^{HH}_0 \| A^{HH}_1).
\end{aligned}$$

Since $(1-\delta)^2 < \frac{\varepsilon}{2}$ by the assumption and $D_{1/2}(A^{GG}_0 \| A^{GG}_1) \le 1$ (cf. [31, Proposition 1]), we have

$$\begin{aligned}
\frac{\varepsilon}{2} &< (1-\delta)\delta D_{1/2}(A^{GH}_0 \| A^{GH}_1) \\
&\quad + \delta(1-\delta) D_{1/2}(A^{HG}_0 \| A^{HG}_1) + \delta^2 D_{1/2}(A^{HH}_0 \| A^{HH}_1).
\end{aligned}$$

[10] It comes from the fact that the majority can be realized by a circuit of linear size of inputs [32].

Since the summation of $(1-\delta)\delta$, $\delta(1-\delta)$, and δ^2 is less than 1, by the averaging argument, at least one of $D_{1/2}(A_0^{GH}\|A_1^{GH})$, $D_{1/2}(A_0^{HG}\|A_1^{HG})$, or $D_{1/2}(A_0^{HH}\|A_1^{HH})$ is larger than $\frac{\varepsilon}{2}$. For instance, suppose that $D_{1/2}(A_0^{GH}\|A_1^{GH}) > \frac{\varepsilon}{2}$ (other cases are similar). We can write

$$\begin{aligned} A_0^{GH}(a) &= \Pr_{\substack{x\sim G\\ y\sim H}}\big(A(x,y,f(x)\oplus f(y))=a\big) \\ &= \mathbb{E}_{x\sim G}\left[\Pr_{y\sim H}\big(A(x,y,f(x)\oplus f(y))=a\big)\right] \end{aligned}$$

and

$$\begin{aligned} A_1^{GH}(a) &= \Pr_{\substack{x\sim G\\ y\sim H}}\big(A(x,y,\sigma)=a\big) \\ &= \Pr_{\substack{x\sim G\\ y\sim H}}\big(A(x,y,f(x)\oplus\sigma)=a\big) \qquad (20)\\ &= \mathbb{E}_{x\sim G}\left[\Pr_{y\sim H}\big(A(x,y,f(x)\oplus\sigma)=a\big)\right], \end{aligned}$$

where the identity (20) holds since σ being a random bit independent of (x,y) implies that $f(x)\oplus\sigma$ is a random bit independent of (x,y). For each $x\in\{0,1\}^n$, let us consider an adversary A^x for distinguishing between $(y,f(y))$ and (y,σ) for $y\sim H$; given input (y,z), A^x runs $A(x,y,f(x)\oplus z)$ (since we consider non-uniform complexity, $f(x)$ can be precomputed and provided to the circuit, and the size of A^x is s'). By applying the joint convexity of the Rényi divergence of order $1/2$ once more, we have

$$\begin{aligned} \frac{\varepsilon}{2} &< D_{1/2}(A_0^{GH}\|A_1^{GH}) \qquad (21)\\ &\le \mathbb{E}_{x\sim G}\Big[D_{1/2}(A_0^x\|A_1^x)\Big]. \qquad (22) \end{aligned}$$

Thus, there exists $x\in\{0,1\}^n$ such that

$$\frac{\varepsilon}{2} < D_{1/2}(A_0^x\|A_1^x).$$

By the same argument as [31, Theorem 3] (for completeness, we provide a proof in Appendix B), there exists a predictor $C:\{0,1\}^n\to\{0,1,\perp\}$ that invokes A^x once and satisfies

$$\mathsf{Adv}^{\mathrm{CS}}_{C,f|H} \ge \frac{1}{3}D_{1/2}(A_0^x\|A_1^x) > \frac{\varepsilon}{6}, \qquad (23)$$

which contradicts (17). □

A Bit-security frameworks

As we mentioned in Section 1, the bit security for decision game G was first introduced in [26], and an operational framework was later introduced in [30]. For readers' convenience, in this appendix, we review the bit-security frameworks of [26] and [30] and discuss their equivalence shown in [31]. Since the main focus of this paper is decision games, we only present the formulation of the decision game in the following; see [26, 30] for the formulation of the search game.

Let U be the random variable describing the choice of a decision game; for instance, in the indistinguishability game of pseudorandom number generator (PRG) from the true random number generator (TRG), $U = 0$ corresponds to the game played with PRG and $U = 1$ corresponds to the game played with TRG. In the framework of [26], we consider an adversary A that outputs $\perp$ in addition to 0 and 1; the symbol $\perp$ signifies that the adversary has difficulty predicting the value of U and gives up the prediction. For the random variable Y describing the adversary's output, let

$$\alpha_A := \Pr(Y \neq \perp),$$
$$\beta_A := \Pr(Y = U | Y \neq \perp),$$

and define the conditional squared (CS) advantage

$$\mathsf{Adv}^{\mathrm{CS}}_{A,G} := \alpha_A (2\beta_A - 1)^2. \tag{24}$$

Then, the bit security of [26] is defined as[11]

$$\min_A \left\{ \log_2 \left(\frac{s_A}{AdvL_{A,G}} \right) \right\}, \tag{25}$$

where s_A is the cost of the adversary.[12]

In the bit-security framework of [30], in order to define the bit security operationally, we consider an outer adversary B in addition to the inner adversary A that plays the given security game. In the framework, the outer adversary B seeks to increase the success probability of predicting U by invoking the inner adversary A for $N_{A,B}$ times. Then, by integrating the outputs from the invocations of the inner adversary, the outer adversary outputs the predicted value Z. Then, for a prescribed success probability $1 - \mu$ (say 0.99), the bit security of decision game G is defined as

$$\mathrm{BS}^{\mu}_{G} := \min_{A,B} \left\{ \log_2(N_{A,B} \cdot s_A) : \Pr(Z = U) \geq 1 - \mu \right\}. \tag{26}$$

[11] In [26], the authors first introduced an advantage using the Shannon entropy and the mutual information; then, in order to justify the definition (25), they discussed that that advantage is approximated by the CS advantage.

[12] In this paper, we focus on the circuit size.

Furthermore, it was shown in [30] that the bit security is characterized by the Rényi advantage up to a constant, i.e.,

$$\mathrm{BS}_G^{\mu} = \min_A \left\{ \log_2 s_A + \log_2 \left\lceil \frac{1}{\mathsf{Adv}_{A,G}^{\mathrm{Renyi}}} \right\rceil \right\} + \mathcal{O}(1), \tag{27}$$

where the Rényi advantage is given by the Rényi divergence

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

for the distributions A_0 and A_1 of adversary for $U = 0$ and $U = 1$, respectively.

At first glance, the bit security defined in (25) and that in (27) (defined via operational formula (26)) are different quantities. However, it was shown in [31] that the two notions of bit security are equivalent in the following sense.

Proposition 3. *For an arbitrary adversary A for a decision game G, it holds that $\mathsf{Adv}_{A,G}^{\mathrm{CS}} \le 8\mathsf{Adv}_{A,G}^{\mathrm{Renyi}}$. On the other hand, for an arbitrary adversary A satisfying $\mathsf{Adv}_{A,G}^{\mathrm{Renyi}} \le 1$, there exists an adversary $\tilde{A}$ having the same cost as A such that $\mathsf{Adv}_{A,G}^{\mathrm{Renyi}} \le 12\mathsf{Adv}_{\tilde{A},G}^{\mathrm{CS}}$.*

By using the conversion of two advantages in Proposition 3, we can argue that the two notions of bit security coincide up to a constant; for more detail, see [31, Section 4]. Since the two notions are equivalent, in the main body of the paper, we focus on the bit security characterized by the Rényi advantage, (27). However, the CS advantage adapted for predictors also plays an important role when we prove the hardcore lemma in Section 3. From a technical perspective, it seems that the CS advantage is more suitable for analyzing the performance of algorithms; on the other hand, the Rényi advantage is more convenient for analysis in a certain situation since it satisfies (joint) convexity with respect to the distributions, which is used in the proof of Theorem 1.

Here, we should note that the standard advantage defined by the total variation distance between A_0 and A_1 is unsuitable for evaluating bit security. Notably, as was pointed out in [26] (see also [31, Section 1.3] further discussion), the standard advantage cannot resolve the paradoxical nature of the linear test for the PRG.

B Proof of (23)

In this appendix, we prove that there exists a predictor $C : \{0,1\}^n \to \{0,1,\perp\}$ that invokes A^x once and satisfies (23). We use the following technical lemma.

Lemma 3. *For given distributions P and Q with $P \ll Q$, we have*

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

where $\mathcal{X}^+ = \{x : Q(x) > 0\}$, 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 $D(P\|Q) = \lim_{\alpha\to 1} D_\alpha(P\|Q)$. The latter inequality appears in the middle of the proof of [14, Lemma 4.1]. □

Note that, for $y \sim H$, the distribution of the adversary A^x for $u = 0$ instance $(y, f(y))$ and $u = 1$ instance (y, σ) are given by

$$\begin{aligned} A_0^x(a) &= \Pr_{y\sim H}\big(A^x(y, f(y)) = a\big), \\ A_1^x(a) &= \Pr_{y\sim H}\big(A^x(y, \sigma) = a\big) \end{aligned}$$

for $a \in \{0, 1, \perp\}$. Note that the support of $(y, f(y))$ is included in the support of (y, σ).[13] Thus, if the adversary A^x outputs a symbol a with positive probability under $u = 0$, then A^x must output a with positive probability under $u = 1$ as well, i.e., $A_0^x \ll A_1^x$.

Let $a^\star \in \{0, 1, \perp\}$ be such that $A_1^x(a^\star) > 0$ and

$$\max_{\substack{a\in\{0,1,\perp\}:\\ A_1^x(a)>0}} \frac{(A_0^x(a) - A_1^x(a))^2}{A_1^x(a)} = \frac{(A_0^x(a^\star) - A_1^x(a^\star))^2}{A_1^x(a^\star)}.$$

Then, by Lemma 3, we have

$$D_{1/2}(A_0^x\|A_1^x) \le 3\frac{(A_0^x(a^\star) - A_1^x(a^\star))^2}{A_1^x(a^\star)}. \tag{28}$$

We consider two cases separately.

When $A_0^x(a^\star) \ge A_1^x(a^\star)$ In this case, we consider the following predictor C. First, we sample the uniform random bit σ. Second,

- If $A^x(y, \sigma) = a^\star$, then C outputs σ;
- If $A^x(y, \sigma) \ne a^\star$, then C outputs $\perp$.

For this predictor, we have

$$\begin{aligned} \Pr_{y\sim H}\big(C(y) \ne \perp\big) &= \Pr_{y\sim H}\big(A^x(y, \sigma) = a^\star\big) \\ &= A_1^x(a^\star) \end{aligned}$$

and

$$\begin{aligned} \Pr_{y\sim H}\big(C(y) = f(y)\big) &= \frac{1}{2}\Pr_{y\sim H}\big(A^x(y, \sigma) = a^\star|\sigma = f(y)\big) \\ &= \frac{1}{2}\Pr_{y\sim H}\big(A^x(y, f(y)) = a^\star\big) \\ &= \frac{A_0^x(a^\star)}{2}, \end{aligned}$$

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

which implies

$$\Pr_{y\sim H}\big(C(y)=f(y)\big)-\frac{1}{2}\Pr_{y\sim H}\big(C(y)\neq\perp\big)=\frac{A_0^x(a^\star)-A_1^x(a^\star)}{2}.$$

Thus, the CS advantage of C satisfies (cf. (5))

$$\begin{aligned}\mathsf{Adv}^{\mathrm{CS}}_{C,f|H}&=\frac{(A_0^x(a^\star)-A_1^x(a^\star))^2}{A_1^x(a^\star)}\\&\geq\frac{1}{3}D_{1/2}(A_0^x\|A_1^x),\end{aligned}$$

where the last inequality follows from (28).

When $A_0^x(a^\star)<A_1^x(a^\star)$ In this case, we consider the following predictor. First, we sample the uniform random bit σ. Second,

- If $A^x(y,\sigma)=a^\star$, then C outputs $\sigma\oplus 1$;
- If $A^x(y,\sigma)\neq a^\star$, then C outputs $\perp$.

For this predictor, we have

$$\begin{aligned}\Pr_{y\sim H}\big(C(y)\neq\perp\big)&=\Pr_{y\sim H}\big(A^x(y,\sigma)=a^\star\big)\\&=A_1^x(a^\star)\end{aligned}$$

and

$$\begin{aligned}\Pr_{y\sim H}\big(C(y)=f(y)\big)&=\Pr_{y\sim H}\big(\sigma=f(y)\oplus 1,A^x(y,\sigma)=a^\star\big)\\&=\Pr_{y\sim H}\big(A^x(y,\sigma)=a^\star\big)-\Pr_{y\sim H}\big(\sigma=f(y),A^x(y,\sigma)=a^\star\big)\\&=A_1^x(a^\star)-\frac{1}{2}\Pr_{y\sim H}\big(A^x(y,\sigma)=a^\star|\sigma=f(y)\big)\\&=A_1^x(a^\star)-\frac{1}{2}\Pr_{y\sim H}\big(A^x(y,f(y))=a^\star\big)\\&=A_1^x(a^\star)-\frac{A_0^x(a^\star)}{2},\end{aligned}$$

which implies

$$\Pr_{y\sim H}\big(C(y)=f(y)\big)-\frac{1}{2}\Pr_{y\sim H}\big(C(y)\neq\perp\big)=\frac{A_1^x(a^\star)-A_0^x(a^\star)}{2}.$$

Thus, the CS advantage of C again satisfies

$$\begin{aligned}\mathsf{Adv}^{\mathrm{CS}}_{C,f|H}&=\frac{(A_0^x(a^\star)-A_1^x(a^\star))^2}{A_1^x(a^\star)}\\&\geq\frac{1}{3}D_{1/2}(A_0^x\|A_1^x).\end{aligned}$$

□

References

1. Aslam, J.A.: Improving algorithms for boosting. In: Proceedings of the 13th Annual Conference on Computational Learning Theory. pp. 200–207 (2000)
2. Bader, C., Jager, T., Li, Y., Schäge, S.: On the impossibility of tight cryptographic reductions. In: Fischlin, M., Coron, J. (eds.) Advances in Cryptology - EUROCRYPT 2016. Lecture Notes in Computer Science, vol. 9666, pp. 273–304. Springer (2016). https://doi.org/10.1007/978-3-662-49896-5“˙10, https://doi.org/10.1007/978-3-662-49896-5_10
3. Barak, B., Hardt, M., Kale, S.: The uniform hardcore lemma via approximate Bregman projections. In: Proceedings of the 2009 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA). pp. 1193–1200 (2009)
4. Bellare, M., Ristenpart, T.: Simulation without the artificial abort: Simplified proof and improved concrete security for waters' ibe scheme. In: Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Lecture Notes in Computer Science, vol. 5479, pp. 407–424. Springer (2009). https://doi.org/10.1007/978-3-642-01001-9˙24
5. Csiszár, I., Shields, P.C.: Information theory and statistics: A tutorial. Found. Trends Commun. Inf. Theory **1**(4) (2004). https://doi.org/10.1561/0100000004, https://doi.org/10.1561/0100000004
6. Diemert, D., Jager, T.: On the tight security of TLS 1.3: Theoretically sound cryptographic parameters for real-world deployments. J. Cryptol. **34**(3), 30 (2021). https://doi.org/10.1007/s00145-021-09388-x, https://doi.org/10.1007/s00145-021-09388-x
7. van Erven, T., Harremoës, P.: Rényi divergence and Kullback-Leibler divergence. IEEE Trans. Inform. Theory **60**(7), 3797–3820 (July 2014)
8. Goldmann, M., Håstad, J., Razborov, A.: Majority gates vs. general weighted threshold gates. Computational Complexity **2**, 277–300 (1992)
9. Goldreich, O., Nisan, N., Wigderson, A.: On Yao's XOR lemma. Electronic Colloquium on Computational Complexity (March 1995)
10. 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
11. Goldreich, O.: On security preserving reductions - revised terminology. In: Goldreich, O. (ed.) Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation, Lecture Notes in Computer Science, vol. 6650, pp. 540–546. Springer (2011)
12. Goldreich, O., Impagliazzo, R., Levin, L.A., Venkatesan, R., Zuckerman, D.: Security preserving amplification of hardness. In: 31st Annual Symposium on Foundations of Computer Science, St. Louis, Missouri, USA, October 22-24, 1990, Volume I. pp. 318–326. IEEE Computer Society (1990). https://doi.org/10.1109/FSCS.1990.89550, https://doi.org/10.1109/FSCS.1990.89550
13. Goldreich, O., Nisan, N., Wigderson, A.: On yao's xor-lemma. In: Goldreich, O. (ed.) Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation, Lecture Notes in Computer Science, vol. 6650, pp. 273–301. Springer (2011). https://doi.org/10.1007/978-3-642-22670-0“˙23, https://doi.org/10.1007/978-3-642-22670-0_23

14. 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)
15. Hast, G.: Nearly one-sided tests and the Goldreich-Levin predicate. Journal of Cryptology **17**, 209–229 (2004)
16. Hatano, K., Warmuth, M.K.: Boosting versus covering. In: Advances in Neural Information Processing Systems. vol. 16 (2003)
17. Hatano, K., Watanabe, O.: Learning r-of-k functions by boosting. In: Proceedings of the 15th International Conference on Algorithmic Learning Theory. pp. 114–126 (2004)
18. Holenstein, T.: Key agreement from weak bit agreement. In: Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC '05). pp. 664–673. ACM Press (2005)
19. Impagliazzo, R.: Hard-core distribution for somewhat hard problems. In: Proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science (FOCS '95). pp. 538–545 (1995)
20. Kale, S.: Boosting and hard-core set constructions: a simplified approach (2007), electronic Colloquium on Computational Complexity (ECCC), Report No. 131
21. Klivans, A.R., Servedio, R.A.: Boosting and hard-core set construction. Machine Learning **51**, 217–238 (2003)
22. Lanzenberger, D., Maurer, U.: Direct product hardness amplification. In: Nissim, K., Waters, B. (eds.) Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part II. Lecture Notes in Computer Science, vol. 13043, pp. 605–625. Springer (2021). https://doi.org/10.1007/978-3-030-90453-1“˙21, https://doi.org/10.1007/978-3-030-90453-1_21
23. Li, B., Micciancio, D., Schultz, M., Sorrell, J.: Securing approximate homomorphic encryption using differential privacy. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022. Lecture Notes in Computer Science, vol. 13507, pp. 560–589. Springer (2022). https://doi.org/10.1007/978-3-031-15802-5“˙20, https://doi.org/10.1007/978-3-031-15802-5_20
24. Luby, M.: Pseudorandomness and cryptographic applications. Princeton computer science notes, Princeton University Press (1996)
25. Maurer, U., Tessaro, S.: A hardcore lemma for computational indistinguishability: Security amplification for arbitrary weak PRGs with optimal stretch. In: TCC 2010. Lecture Notes in Computer Science, vol. 5078, pp. 237–254. Springer (2010)
26. Micciancio, D., Walter, M.: On the bit security of cryptographic primitives. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology - EUROCRYPT 2018. Lecture Notes in Computer Science, vol. 10820, pp. 3–28. Springer (2018). https://doi.org/10.1007/978-3-319-78381-9“˙1
27. Morgan, A., Pass, R.: On the security loss of unique signatures. In: Theory of Cryptography. Theory of Cryptography, vol. 11239, pp. 507–536. Springer (2018). https://doi.org/10.1007/978-3-030-03807-6˙19
28. Schapire, R.E., Singer, Y.: Improved boosting algorithm using confidence-rated predictions. Machine Learning **37**(3), 297–336 (1999)
29. Vadhan, S., Zheng, C.J.: A uniform min-max theorem with applications in cryptography. In: Advances in Cryptography–CRYPTO '13. Lecture Notes in Computer Science, vol. 8042, pp. 93–110. Springer (2013)
30. 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. Lecture Notes in Computer Science, vol. 13092, pp. 161–188. Springer (2021)
31. Watanabe, S., Yasunaga, K.: Unified view for notions of bit security. Cryptology ePrint Archive, Paper 2022/693 (2022), https://eprint.iacr.org/2022/693, https://eprint.iacr.org/2022/693
32. Wegener, I.: The Complexity of Boolean Functions. Wiley (1991)