Bit-Security Preserving Hardness Amplification

TCC2024@Milan, December 2024

Shun Watanabe (Tokyo Univ. of Agri. and Tech.)

Kenji Yasunaga (Institute of Science Tokyo)

Outline

1. Background on bit-security

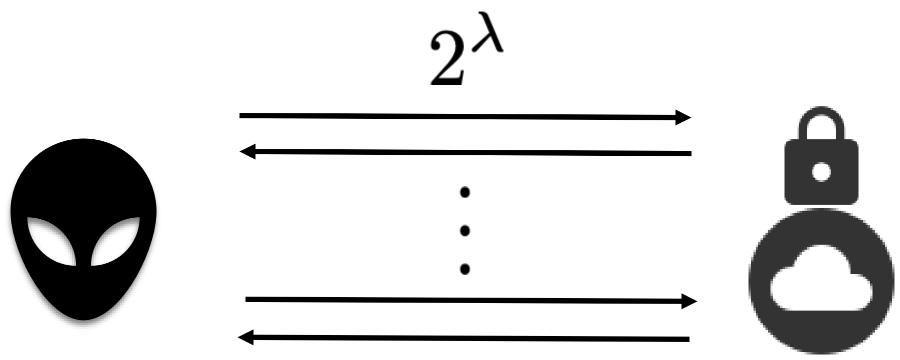
2. Motivation: what is bit-security preserving hardness amplification

3. Technical results

What is bit security?

We shall quantify how much security a certain system provide…

Roughly, a system is λ bit secure if 2^λ operations are needed to break the system.



Bit security of one-way function

Given one-way function (permutation)

a representative of search primitive

$$f : \{0,1\}^n \to \{0,1\}^n$$

and an attack with cost T such that

$$\Pr\left(A(f(x)) = x\right) = \varepsilon_A$$

how much bit security is guaranteed?

Bit security of one-way function

a representative of search primitive

Given one-way function (permutation)

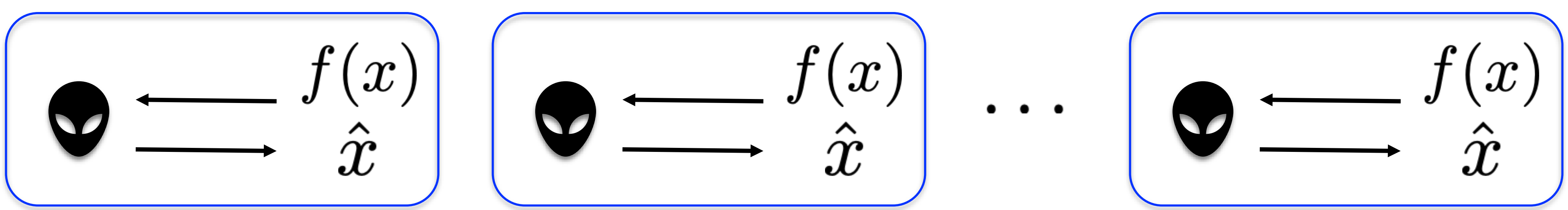
$$f : \{0,1\}^n \to \{0,1\}^n$$

and an attack with cost T such that

$$\Pr\big(A(f(x)) = x\big) = \varepsilon_A$$

how much bit security is guaranteed?

The success probability can be amplified to $\simeq N\varepsilon_A$



N times

Total cost is $\mathcal{O}(N \cdot T_A) = \mathcal{O}\left(\frac{T_A}{\varepsilon_A}\right) \implies \mathrm{BS} = \min_A \left\{ \log_2 \left(\frac{T_A}{\varepsilon_A} \right) \right\}$

Bit security of decision primitive

How should we define bit security of decision primitives/assumptions.

(PRG, encryption, DDH)

Bit security of decision primitive

How should we define bit security of decision primitives/assumptions.

(PRG, encryption, DDH)

Micciancio-Walter (EUROCRYPT 2018) introduced a notion of bit security.

Search/decision primitives are treated in a unified manner.
It is compatible with known facts.

Bit security of decision primitive

How should we define bit security of decision primitives/assumptions.

(PRG, encryption, DDH)

Micciancio-Walter (EUROCRYPT 2018) introduced a notion of bit security.

Search/decision primitives are treated in a unified manner.

It is compatible with known facts.

Watanabe-Yasunaga (ASIACRYPT 2021) introduced an alternative notion of bit security.

Operational meaning is clearer.

Bit security of decision primitive

How should we define bit security of decision primitives/assumptions.

(PRG, encryption, DDH)

Micciancio-Walter (EUROCRYPT 2018) introduced a notion of bit security.

Search/decision primitives are treated in a unified manner.
It is compatible with known facts.

Watanabe-Yasunaga (ASIACRYPT 2021) introduced an alternative notion of bit security.

Operational meaning is clearer.

It turned out that MW18 and WY21 are essentially equivalent (ASIACRYPT 2023).

Motivation: Two kinds of adversaries of PRG

Consider a construction of PRG using one-way permutation.

Given one-way permutation

$$f : \{0,1\}^n \to \{0,1\}^n$$

and its hard-core predicate

$$h : \{0,1\}^n \to \{0,1\}$$

Seed: $x \in_R \{0,1\}^n$ Output: $G(x) = (f(x), h(x))$

Motivation: Two kinds of adversaries of PRG

Consider a construction of PRG using one-way permutation.

Given one-way permutation

$$f : \{0,1\}^n \to \{0,1\}^n$$

and its hard-core predicate

$$h : \{0,1\}^n \to \{0,1\}$$

Seed: $x \in_R \{0,1\}^n$ Output: $G(x) = (f(x), h(x))$

Indistinguishability game:

PRG: $u = 0$ $(y,z) = (f(x), h(x))$

TRG: $u = 1$ $(y,z) = (f(x), \sigma)$ $\sigma \in_R \{0,1\}$

Motivation: Two kinds of adversaries of PRG

There are a few possible attacks:

1) Linear test attack:

For a fixed vector $v \in \{0,1\}^{n+1}$, output $\hat{u} = 0$ if $\langle v, (y,z) \rangle = 0$

$$A_0 = \left(1/2 + \varepsilon_1, 1/2 - \varepsilon_1\right) \qquad A_1 = \left(1/2, 1/2\right)$$

There exists v such that $\varepsilon_1 \geq 2^{-n/2}$ [Alon-Goldreich-Hastad-Peralta 92].

2) Inversion attack:

Invert $f(x)$, and output $\hat{u} = 0$ if it succeed and $h(x) = z$.

If the success probability of inversion is $2\varepsilon_2$,

$$A_0 = \left(2\varepsilon_2, 1 - 2\varepsilon_2\right) \qquad A_1 = \left(\varepsilon_2, 1 - \varepsilon_2\right)$$

Motivation: Two kinds of adversaries of PRG

There are a few possible attacks:

1) Linear test attack:

For a fixed vector $v \in \{0,1\}^{n+1}$, output $\hat{u} = 0$ if $\langle v, (y, z) \rangle = 0$

$$A_0 = \big(1/2 + \varepsilon_1, 1/2 - \varepsilon_1\big) \qquad A_1 = \big(1/2, 1/2\big)$$

There exists v such that $\varepsilon_1 \geq 2^{-n/2}$ [Alon-Goldreich-Hastad-Peralta 92].

2) Inversion attack:

Invert $f(x)$, and output $\hat{u} = 0$ if it succeed and $h(x) = z$.

If the success probability of inversion is $2\varepsilon_2$,

$$A_0 = \big(2\varepsilon_2, 1 - 2\varepsilon_2\big) \qquad A_1 = \big(\varepsilon_2, 1 - \varepsilon_2\big)$$

Note that the advantage is

$$2\big(\Pr(\hat{u} = u) - 1/2\big) = \varepsilon_i, \quad i = 1, 2$$

Motivation: Two kinds of adversaries of PRG

There are a few possible attacks:

1) Linear test attack:

For a fixed vector $v \in \{0,1\}^{n+1}$, output $\hat{u} = 0$ if $\langle v, (y,z) \rangle = 0$

$$A_0 = \big(1/2 + \varepsilon_1, 1/2 - \varepsilon_1\big) \qquad A_1 = \big(1/2, 1/2\big)$$

There exists v such that $\varepsilon_1 \geq 2^{-n/2}$ [Alon-Goldreich-Hastad-Peralta 92].

2) Inversion attack:

Invert $f(x)$, and output $\hat{u} = 0$ if it succeed and $h(x) = z$.

If the success probability of inversion is $2\varepsilon_2$,

$$A_0 = \big(2\varepsilon_2, 1 - 2\varepsilon_2\big) \qquad A_1 = \big(\varepsilon_2, 1 - \varepsilon_2\big)$$

Note that the advantage is

$$2\big(\Pr(\hat{u} = u) - 1/2\big) = \varepsilon_i, \quad i = 1,2$$

The standard advantage cannot capture the difference of biased and unbiased adversaries.

Motivation: Two kinds of adversaries of PRG

There are a few possible attacks:

1) Linear test attack:

For a fixed vector $v \in \{0,1\}^{n+1}$, output $\hat{u} = 0$ if $\langle v, (y,z) \rangle = 0$

$$A_0 = \big(1/2 + \varepsilon_1, 1/2 - \varepsilon_1\big) \qquad A_1 = \big(1/2, 1/2\big)$$

There exists v such that $\varepsilon_1 \geq 2^{-n/2}$ [Alon-Goldreich-Hastad-Peralta 92].

2) Inversion attack:

Invert $f(x)$, and output $\hat{u} = 0$ if it succeed and $h(x) = z$.

If the success probability of inversion is $2\varepsilon_2$,

$$A_0 = \big(2\varepsilon_2, 1 - 2\varepsilon_2\big) \qquad A_1 = \big(\varepsilon_2, 1 - \varepsilon_2\big)$$

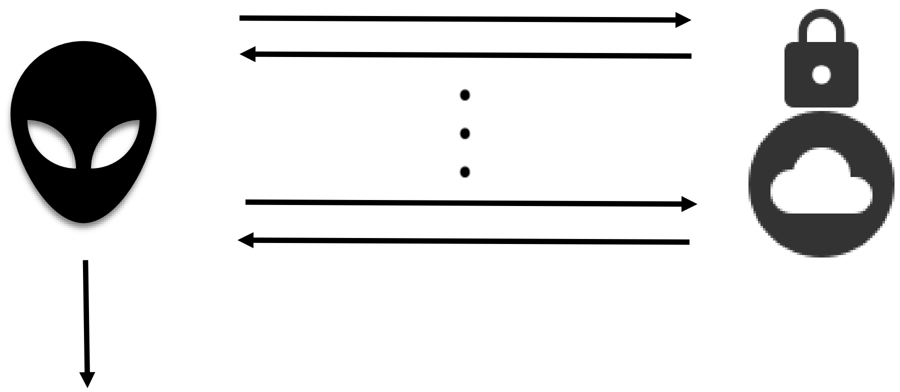
Note that the advantage is

$$2\big(\Pr(\hat{u} = u) - 1/2\big) = \varepsilon_i, \quad i = 1, 2$$

The standard advantage cannot capture the difference of biased and unbiased adversaries.

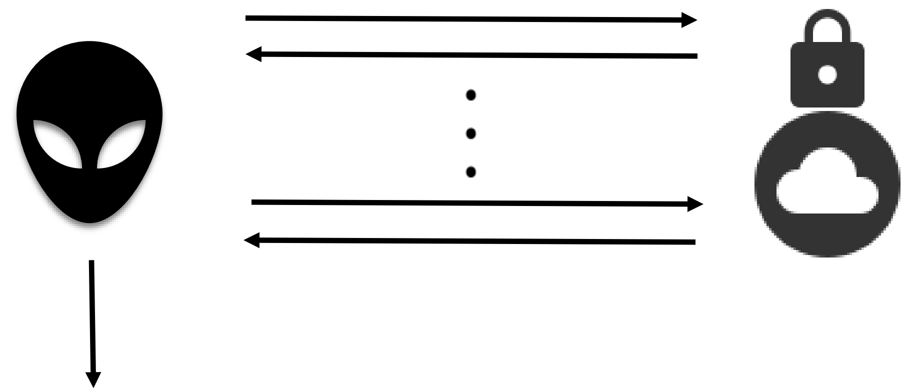
For advantage ε, should we define $\log \dfrac{T}{\varepsilon^2}$ or $\log \dfrac{T}{\varepsilon}$?

Bit security framework of Micciancio-Walter



$$y \in \{0,1\} \cup \{\perp\}$$

Bit security framework of Micciancio-Walter



$$y \in \{0,1\} \cup \{\perp\}$$

Bit security is defined as $\min_A \left\{ \log \frac{T_A}{\mathrm{adv}_A^{\mathrm{CS}}} \right\}$ for $\mathrm{adv}_A^{CS} := \alpha_A \cdot (2\beta_A - 1)^2$

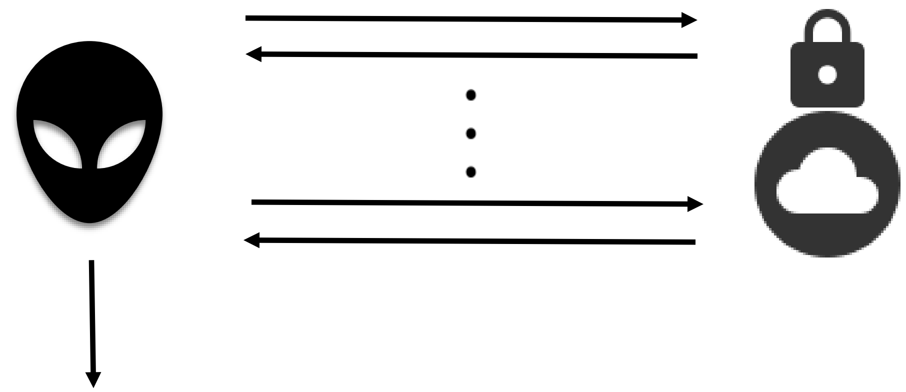
where

$$\alpha_A := \Pr\left(A \text{ outputs } Y \neq \perp\right) \quad \beta_A := \Pr\left(Y = U | A \text{ outputs } Y \neq \perp\right)$$

$U \in \{0,1\}$ is a random secret of game

Y is the adversary's output

Bit security framework of Micciancio-Walter



$$y \in \{0,1\} \cup \{\perp\}$$

Bit security is defined as $\min_A \left\{ \log \frac{T_A}{\mathrm{adv}_A^{\mathrm{CS}}} \right\}$ for $\mathrm{adv}_A^{CS} := \alpha_A \cdot (2\beta_A - 1)^2$

where

$$\alpha_A := \Pr\left(A \text{ outputs } Y \neq \perp\right) \quad \beta_A := \Pr\left(Y = U \middle| A \text{ outputs } Y \neq \perp\right)$$

$U \in \{0,1\}$ is a random secret of game

Y is the adversary's output

1) Linear test attack: $\alpha_A = 1, \quad \beta_A = \varepsilon_1^2 \Longrightarrow \mathrm{adv}_A^{\mathrm{CS}} = \varepsilon_1^2$

2) Inversion attack: $\alpha_A = 2\varepsilon_2, \quad \beta_A = 1/4 \Longrightarrow \mathrm{adv}_A^{\mathrm{CS}} = \varepsilon_2/2$

Characterization of Bit security of WY21

Bit security was operationally defined as a cost for winning with high probability.

Bit security can be characterized as

$$\mathrm{BS}_G^{\mu} := \min_A \left\{ \log\left(\frac{T_A}{\mathrm{adv}_A}\right) \right\} + \mathcal{O}(1)$$

where $\mathrm{adv}_A = \mathrm{adv}_A^{\mathrm{Renyi}} := D_{1/2}(A_0 \| A_1)$

A_u : probability distribution of output a by A when secret is u

$$D_{1/2}(A_0 \| A_1) = -2 \ln \sum_a \sqrt{A_0(a) A_1(a)}$$

Rényi divergence of order 1/2

Characterization of Bit security of WY21

Bit security was operationally defined as a cost for winning with high probability.

Bit security can be characterized as

$$\mathrm{BS}^{\mu}_{G} := \min_{A} \left\{ \log \left(\frac{T_A}{\mathrm{adv}_A} \right) \right\} + \mathcal{O}(1)$$

where $\mathrm{adv}_A = \mathrm{adv}_A^{\mathrm{Renyi}} := D_{1/2}(A_0 \| A_1)$

A_u : probability distribution of output a by A when secret is u

$$D_{1/2}(A_0 \| A_1) = -2 \ln \sum_{a} \sqrt{A_0(a) A_1(a)}$$

Rényi divergence of order 1/2

Theorem [WY23]

The bit security notions of MW18 and WY21 are essentially equivalent, i.e.,

$$\mathrm{adv}_A^{\mathrm{CS}} \simeq \mathrm{adv}_A^{\mathrm{Renyi}}$$

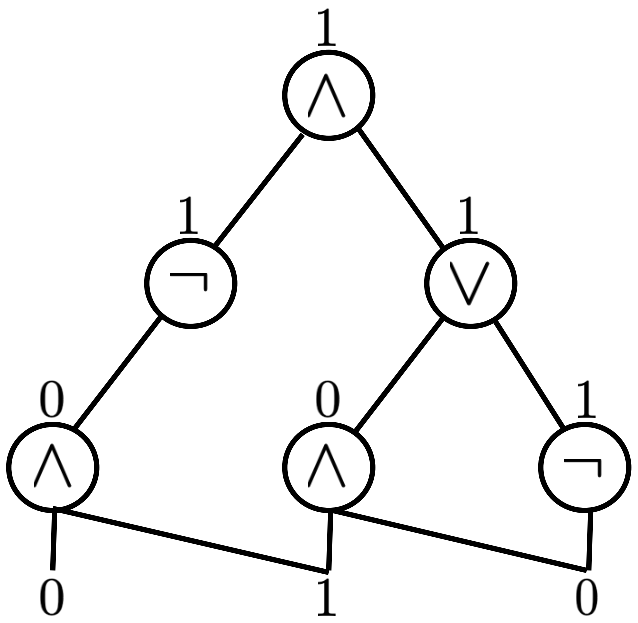
up to a constant (with some modification of adversary).

Hardness amplification (Yao's Xor lemma)

We shall discuss hardness of computing a function

$$f : \{0,1\}^n \to \{0,1\}$$

by a Boolean circuits.

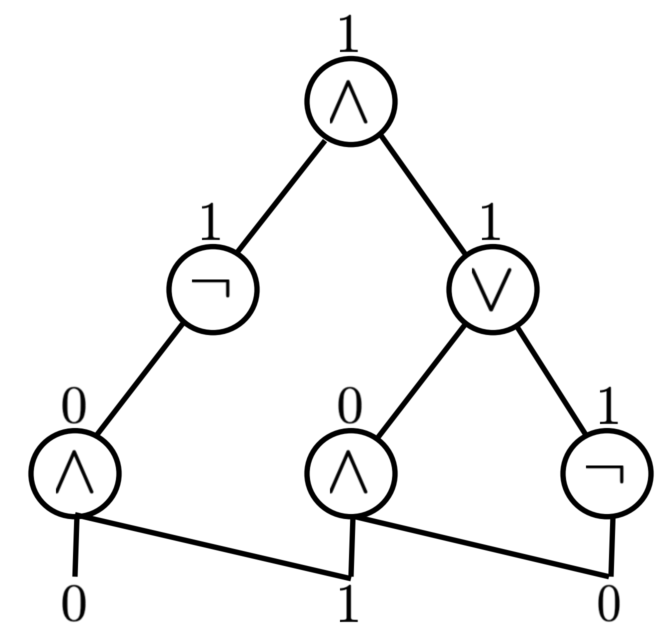


Hardness amplification (Yao's Xor lemma)

We shall discuss hardness of computing a function

$$f : \{0,1\}^n \to \{0,1\}$$

by a Boolean circuits.



$(s, 1-\delta)$ -mildly hard

For a given $f : \{0,1\}^n \to \{0,1\}$, suppose that

$$\Pr_{x \sim U_n} \big(C(x) = f(x)\big) \le 1 - \delta$$

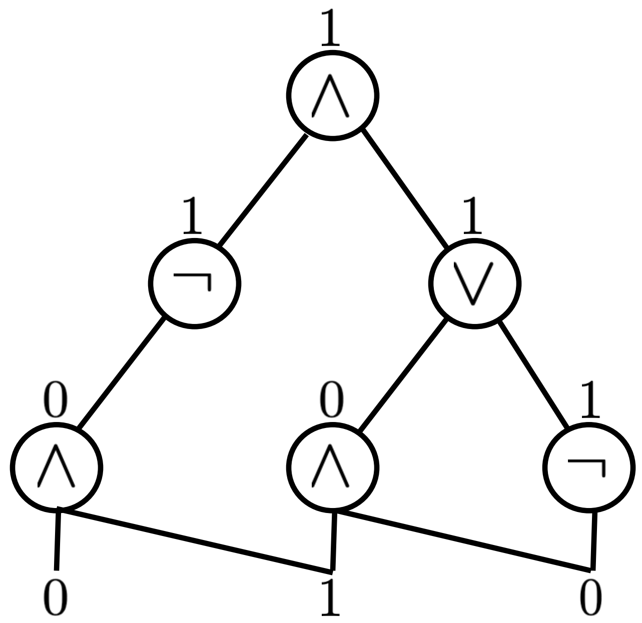
for any circuit C of size s.

Hardness amplification (Yao's Xor lemma)

We shall discuss hardness of computing a function

$$f : \{0,1\}^n \to \{0,1\}$$

by a Boolean circuits.



$(s, 1-\delta)$ -mildly hard

For a given $f : \{0,1\}^n \to \{0,1\}$, suppose that

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

for any circuit C of size s.

We shall prove that

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

is very hard.

Hardness amplification (Yao's Xor lemma)

<u>Proposition (Xor lemma)</u>

If $f : \{0,1\}^n \to \{0,1\}$ is $(s, 1-\delta)$-mildly hard and $\varepsilon \geq 2(1-\delta)^k$, then

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

for any circuit C of size $s' = \Omega\left(\frac{\varepsilon^2}{\ln(1/\delta)}\right)s$.

The circuit size of adversary is reduced by the factor of $\frac{\varepsilon^2}{\ln(1/\delta)}$

Hardness amplification (Yao's Xor lemma)

<u>Proposition (Xor lemma)</u>

If $f : \{0,1\}^n \to \{0,1\}$ is $(s, 1-\delta)$-mildly hard and $\varepsilon \geq 2(1-\delta)^k$, then

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

for any circuit C of size $s' = \Omega\left(\frac{\varepsilon^2}{\ln(1/\delta)}\right) s$.

The circuit size of adversary is reduced by the factor of $\frac{\varepsilon^2}{\ln(1/\delta)}$

It only guarantees

$$\mathrm{BS}_{s'}(G_{f^{\oplus k}}) \geq \log \frac{s'}{\varepsilon} = \underbrace{\log s}_{\text{initial bit security}} - \underbrace{\mathcal{O}\left(\log \frac{\ln(1/\delta)}{\varepsilon}\right)}_{\text{loss of bit security}}$$

Outline of our results

Bit security is preserved in the hardness amplification?

Not guaranteed by the standard hardness amplification …

We derive a hardness amplification result for the Renyi advantage.

It guarantees that the bit security is preserved.

The proof is based on the hardcore lemma for CS advantage.

It uses a boosting algorithm with $\perp$.

Bit security preserving hardness amplification

Theorem 1 (Xor lemma for Renyi advantage)

If $f : \{0,1\}^n \to \{0,1\}$ is $(s, 1-\delta)$-mildly hard and $\varepsilon \geq 2(1-\delta)^k$, then

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

for any circuit A of size $s' = \Omega\left(\frac{\varepsilon}{\ln(1/\delta)}\right) s$.

Caveat: Theorem 1 is only valid for $s = \omega\left(\frac{\ln(1/\delta)}{\varepsilon^2}\right)$

This is due to that we use the weighted majority in the proof…

Bit security preserving hardness amplification

Theorem 1 (Xor lemma for Renyi advantage)

If $f:\{0,1\}^n \to \{0,1\}$ is $(s, 1-\delta)$-mildly hard and $\varepsilon \geq 2(1-\delta)^k$, then

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

for any circuit A of size $s' = \Omega\left(\frac{\varepsilon}{\ln(1/\delta)}\right)s$.

Caveat: Theorem 1 is only valid for $s = \omega\left(\frac{\ln(1/\delta)}{\varepsilon^2}\right)$

This is due to that we use the weighted majority in the proof…

Theorem 1 guarantees that

$$\begin{aligned}\mathrm{BS}_{s'}(G_{f^{\oplus k}}) &\geq \log \frac{s'}{\varepsilon} \\ &= \log s - \mathcal{O}(\log \ln(1/\delta))\end{aligned}$$

bit security loss does not depend on ε

Standard Hardcore lemma

<u>Proposition (hardcore lemma [Impagliazzo])</u>

If $f : \{0,1\}^n \to \{0,1\}$ is $(s, 1-\delta)$-mildly hard, then there exists H with density δ

such that

$$\Pr_{x \sim H}\left(C(x) = f(x)\right) \leq \frac{1}{2} + \varepsilon$$

for any circuit C of size $s' = \Omega\left(\frac{\varepsilon^2}{\ln(1/\delta)}\right)s$.

Hardcore lemma implies Xor lemma (rough idea):

To compute $f^{\oplus k}(x_1, \ldots, x_k) := f(x_1) \oplus \cdots \oplus f(x_k)$ strictly better than random guess,

x_i's must avoid hard instances for every coordinates, which occurs with $(1-\delta)^k$

Advantage cannot be much larger than $(1-\delta)^k$.

A novel hardcore lemma

Since the standard hardcore lemma is insufficient, we prove a novel hardcore lemma.

For $C : \{0,1\}^n \to \{0,1,\perp\}$ and $x \sim P$

$$\mathrm{Adv}^{\mathrm{CS}}_{C,f|P} := \frac{\left(\Pr(C(x) = f(x)) - \Pr(C(x) = \overline{f(x)})\right)^2}{\Pr(C(x) \neq \perp)} \qquad \overline{f(x)} = f(x) \oplus 1$$

Lemma (hardcore lemma for CS advantage)

If $f : \{0,1\}^n \to \{0,1\}$ is $(s, 1-\delta)$-mildly hard, then there exists H with density δ

such that

$$\mathrm{Adv}^{\mathrm{CS}}_{C,f|H} \leq \varepsilon$$

for any circuit C of size $s' = \Omega\left(\frac{\varepsilon}{\ln(1/\delta)}\right)s$.

Proof of hardcore lemma

Impagliazzo presented two proofs of hardcore lemma:

(1) minimax theorem (attributed to Nisan)

$\mathrm{Adv}^{\mathrm{CS}}_{C,f|H}$ is not linear (may not be convex in H nor concave in P_C).

We cannot apply the minimax approach to the CS advantage…

(2) Boosting (connection pointed out in [Klivans-Servedio '03])

We prove the hardcore lemma for CS advantage using a modified boosting algorithm.

Alternative motivation

Goldreich-Levin theorem guarantees existence of hardcore predicate

for every (modified) one-way function.

A proof of GL theorem is related to list-decoding of the Hadamard code.

Hast '04 proposed a modified GL algorithm by taking into account an adversary with $\perp$

(erasure list-decoding of the Hadamard code)

The performance of Hast's algorithm is evaluated by the CS advantage.

It is natural to consider the hardcore lemma for CS advantage.

A difficulty is that the role of $\perp$ is not clear in boosting algorithm…

Modified boosting algorithm

(contrapositive) assumption

For each P with density δ , there exists C_P of size s' such that

$$\mathrm{Adv}^{\mathrm{CS}}_{C_P,f|P} > \varepsilon \quad (*)$$

existence of weak learners

Alrorithm

Initialize $P^{(1)} = \mathsf{unif}(\{0,1\}^n)$

For $1 \le t \le T$

(1) For $C_{P^{(t)}}$ satisfying (*) against $P^{(t)}$, set

specified in the next page

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

normalizer

(2) For the set $\mathcal{P}_\delta$ of all distributions with density δ , set

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

Modified boosting algorithm

The update weight is $\gamma_t = \dfrac{\Delta_t}{4\alpha_t}$ for

$$\alpha_t := \Pr_{x \sim P^{(t)}} (C_{P^{(t)}}(x) \neq \perp)$$

$$\Delta_t := \Pr_{x \sim P^{(t)}} (C_{P^{(t)}}(x) = f(x)) - \Pr_{x \sim P^{(t)}} (C_{P^{(t)}}(x) = \overline{f(x)})$$

Our algorithm is similar to the standard boosting, and it does not use $\perp$ explicitly.

But, $\perp$ is incorporated in the update weight γ_t.

Modified boosting algorithm

The update weight is $\gamma_t = \dfrac{\Delta_t}{4\alpha_t}$ for

$$\alpha_t := \Pr_{x \sim P^{(t)}}(C_{P^{(t)}}(x) \neq \perp)$$

$$\Delta_t := \Pr_{x \sim P^{(t)}}(C_{P^{(t)}}(x) = f(x)) - \Pr_{x \sim P^{(t)}}(C_{P^{(t)}}(x) = \overline{f(x)})$$

Our algorithm is similar to the standard boosting, and it does not use $\perp$ explicitly.

But, $\perp$ is incorporated in the update weight γ_t .

Roughly, our algorithm put more weight on

$$\boxed{\begin{array}{c}\alpha_t \simeq \varepsilon \\ \Delta_t \simeq \varepsilon\end{array}} \quad \text{than} \quad \boxed{\begin{array}{c}\alpha_t \simeq 1 \\ \Delta_t \simeq \varepsilon\end{array}}$$

Untalkative weak learner is more reliable!

Conclusion

Adversary	$\mathtt{Adv}^{\mathrm{TV}}$	$\mathtt{Adv}^{\mathrm{CS}} / \mathtt{Adv}^{\mathrm{Renyi}}$	bit-security of standard Xor lemma	bit-security of our Xor lemma
Balanced eg) Linear test attack	ε	$\Theta(\varepsilon^2)$	$\log\left(\frac{\varepsilon^2 s}{\varepsilon^2}\right)$	$\log\left(\frac{\varepsilon^2 s}{\varepsilon^2}\right)$
Unbalanced eg) Inversion attack	ε	$\Theta(\varepsilon)$	$\log\left(\frac{\varepsilon^2 s}{\varepsilon}\right)$	$\log\left(\frac{\varepsilon s}{\varepsilon}\right)$

For balanced adversary, the bit-security is unchanged;

For unbalanced adversary, the bit-security is improved.

Open problems:

- Can we prove a uniform hardcore lemma for CS advantage?
- The circuit size loss ε of the hardcore lemma for CS advantage is unavoidable?