Unified View for Notions of Bit Security

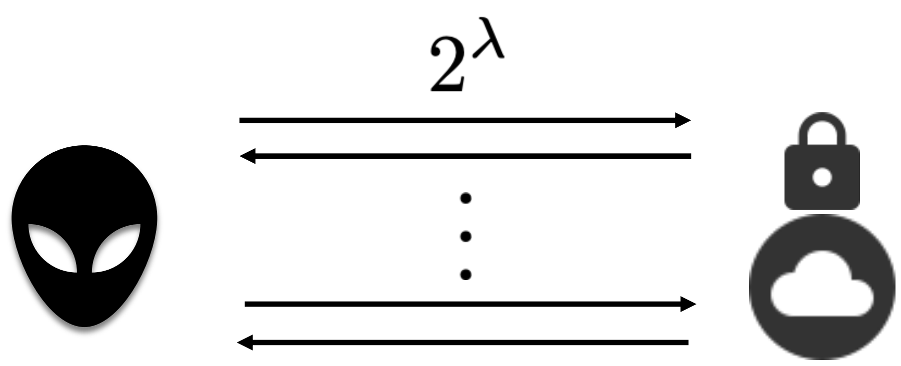
ASIACRYPT@Guangzhou, China
December, 2023

Shun Watanabe (Tokyo University of Agriculture and Technology)
Kenji Yasunaga (Tokyo Institute of Technology)

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

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?

Bit security of one-way function

Given one-way function (permutation)

a representative of search primitive

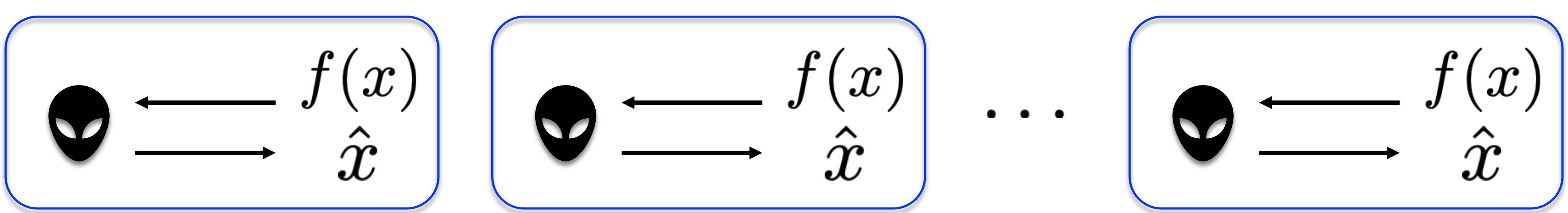
$$f : \{0,1\}^n \to \{0,1\}^n$$

and an attack with cost T such that

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

how much bit security is guaranteed?

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



N times

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

Prior work and outline of our results

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

(PRG, encryption, DDH)

Prior work and outline of our results

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

(PRG, encryption, DDH)

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

It is compatible with known facts, but did not have an operational meaning…

Prior work and outline of our results

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

(PRG, encryption, DDH)

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

It is compatible with known facts, but did not have an operational meaning…

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

It has an operational meaning; some open problems remained: connection between MW and WY.

Prior work and outline of our results

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

(PRG, encryption, DDH)

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

It is compatible with known facts, but did not have an operational meaning…

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

It has an operational meaning; some open problems remained: connection between MW and WY.

Result 1: a slight modification of WY21 is equivalent to MW18.

Result 2: Goldreich-Levin reduction is tight in WY21.

Result 3: via canonical games, it suffices to consider decision game in WY21

Result 4: application to distribution replacement theorem

Prior work and outline of our results

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

(PRG, encryption, DDH)

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

It is compatible with known facts, but did not have an operational meaning…

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

It has an operational meaning; some open problems remained: connection between MW and WY.

Result 1: a slight modification of WY21 is equivalent to MW18.

Result 2: Goldreich-Levin reduction is tight in WY21.

Result 3: via canonical games, it suffices to consider decision game in WY21

Result 4: application to distribution replacement theorem

Motivating question 1

Attack with success probability 40 %

Attack with success probability 50 %

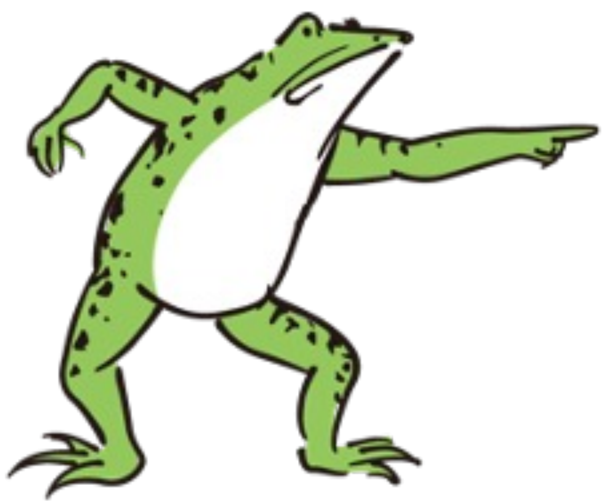
Prediction Games

Game	1	2	3	4	5	6	7	8	9	10
Prediction	1	0	0	0	1	0	0	0	1	0
Outcome	0	0	1	0	1	1	0	1	0	1

Game	1	2	3	4	5	6	7	8	9	10
Prediction	0	1	0	1	0	1	0	1	1	1
Outcome	0	0	1	0	1	1	0	1	0	1

Motivating question 2

Attack with success probability 60 %



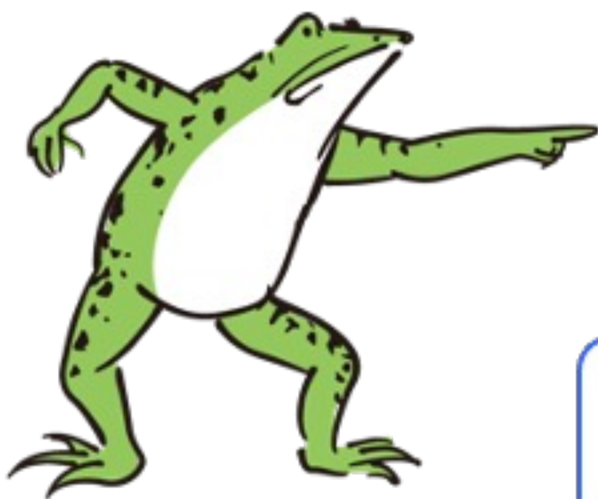
Game	1	2	3	4	5	6	7	8	9	10
Prediction	0	0	0	0	1	0	0	0	0	0
Outcome	0	0	1	0	1	1	0	1	0	1

Attack with success probability 60 %

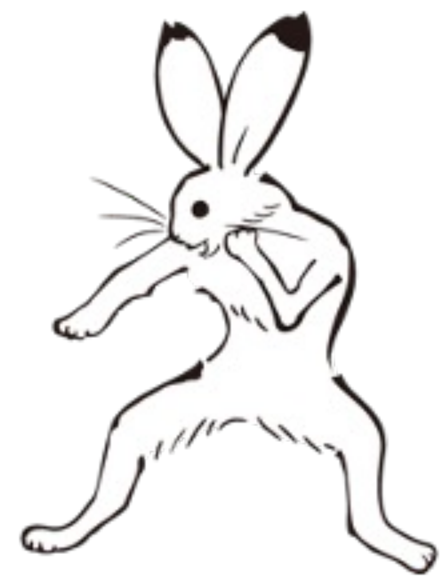
Game	1	2	3	4	5	6	7	8	9	10
Prediction	1	0	0	0	1	0	0	1	1	1
Outcome	0	0	1	0	1	1	0	1	0	1

Motivating question 2

Attack with success probability 60 %



Attack with success probability 60 %



Arranged based on the outcomes

100%

20%

Game	1 2 4 7 9	3 5 6 8 10
Prediction	0 0 0 0 0	0 1 0 0 0
Outcome	0 0 0 0 0	1 1 1 1 1

Biased adversary

60%

60%

Game	1 2 4 7 9	3 5 6 8 10
Prediction	1 0 0 0 1	0 1 0 1 1
Outcome	0 0 0 0 0	1 1 1 1 1

Unbiased adversary

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: $G(x) = (f(x), h(x))$

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

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 $2\varepsilon_2$,

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

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

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

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 $2\varepsilon_2$,

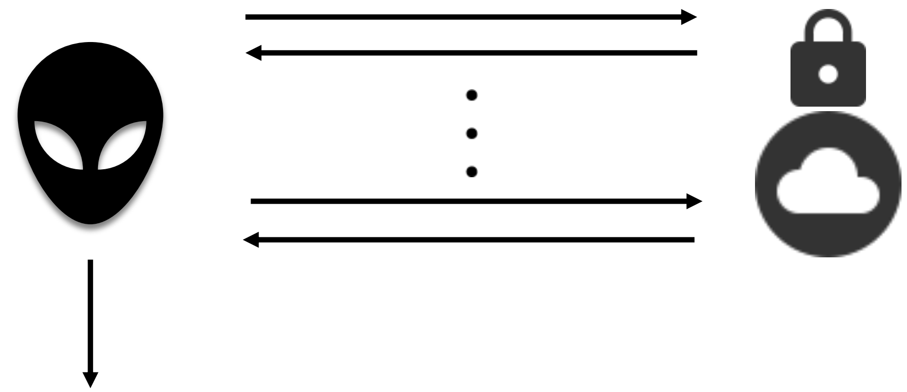
$$A_0 = \big(2\varepsilon_2, 1 - 2\varepsilon_2\big) \qquad A_1 = \big(\varepsilon_2, 1 - \varepsilon_2\big)$$

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.

Bit security framework of Micciancio-Walter



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

Bit security is defined as $$\min_A \left\{ \log \frac{T_A}{\mathrm{adv}_A^{\mathrm{MW}}} \right\}$$

mutual information

$$\mathrm{adv}_A^{\mathrm{MW}} := \frac{I(U \wedge Y)}{H(U)} = 1 - \frac{H(U|Y)}{H(U)}$$

Shannon entropy

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

Y is the adversary's output

Bit security framework of Micciancio-Walter

For decision game,

conditional square advantage

$$\mathrm{adv}_A^{\mathrm{MW}} \simeq \alpha_A \cdot (2\beta_A - 1)^2 =: \mathrm{adv}_A^{CS}$$

where

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

1) Linear test attack:

$$\alpha_A = 1, \quad \beta_A = \varepsilon_1^2 \Longrightarrow \mathrm{adv}_A^{\mathrm{CS}} = \varepsilon_1^2$$

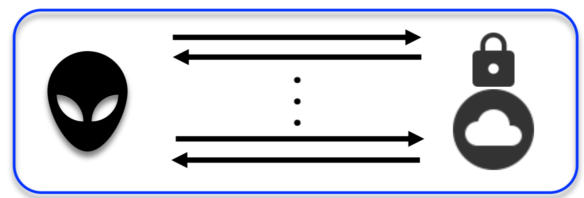
2) Inversion attack:

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

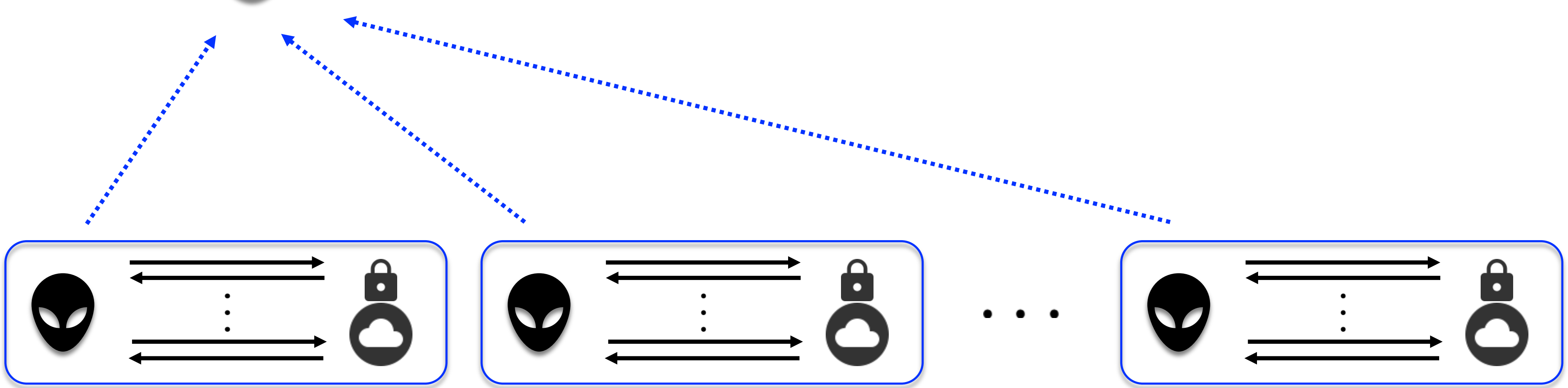
Bit security framework of WY21

Consider two types of adversaries: inner  and outer 

A B

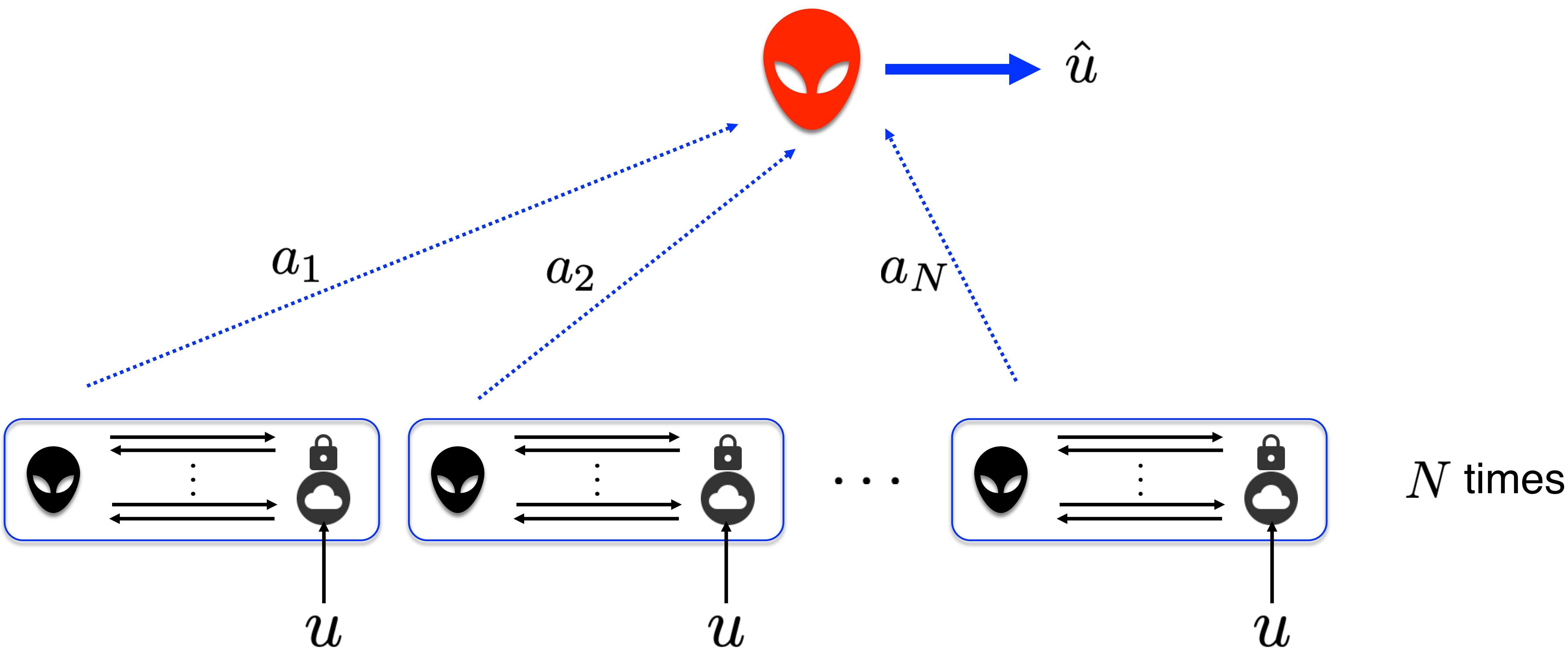
Inner  plays a usual game 

outer  invokes inner adversaries to amplify the winning probability



N times

Winning condition of outer adversary (decision)



Each inner 👽 plays an independent game with consistent u .

If $\hat{u} = u$, outer 👽 wins the game.

Bit security definition of WY21

Bit security is defined as

$$\mathrm{BS}_G^{\mu} := \min_{A,B} \left\{ \log\left(N \cdot T_A\right) : \Pr\left(B \text{ wins }\right) \geq 1-\mu \right\}$$

inner

outer

eg) $\mu = 0.01$

Characterization of Bit security of WY21

Theorem [WY21]

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

WY21 did not consider $\perp$, but the result in unchanged even if we consider $\perp$.

- Upper bound is derived using the likelihood ratio test for Bayesian hypothesis testing.
- Lower bound is derived using an inequality between Rényi divergence and TV distance.

(Fuchs-van de Graaf inequality)

Open problems in WY21

WY bit security behaves mostly the same as MW bit security.

Particularly,

1) Linear test attack: $\mathrm{adv}_A^{\mathrm{Renyi}} = \Theta(\varepsilon_1^2)$

2) Inversion attack: $\mathrm{adv}_A^{\mathrm{Renyi}} = \Theta(\varepsilon_2)$

However,

-tightness of Goldreich-Levin reduction

-connection between WY bit security and MW bit security

remained unsolved.

Relation between MW and WY (1)

Theorem 1

For any adversary A,

$$\mathrm{Adv}_A^{\mathrm{CS}} \leq 4\mathrm{Adv}_A^{\mathrm{Renyi}}$$

Implication of Theorem 1:

If a decision game G is λ bit secure in the sense of WY,

then, up to a constant bit, G is λ bit secure in the sense of MW.

The proof is via bounding the CS advantage by the Hellinger distance, and

then using a connection between Rényi divergence and Hellinger distance.

Relation between MW and WY (2)

Theorem 2

For an adversary A such that $\mathrm{Adv}_A^{\mathrm{Renyi}} \leq 1$, there exists an adversary $\tilde{A}$ such that

$$\mathrm{Adv}_A^{\mathrm{Renyi}} \leq 12\ \mathrm{Adv}_{\tilde{A}}^{\mathrm{CS}}$$

and $\tilde{A}$ has the same cost as A.

Implication of Theorem 2:

The assumption $\mathrm{Adv}_A^{\mathrm{Renyi}} \leq 1$ is not restrictive:

Even if $\mathrm{Adv}_A^{\mathrm{Renyi}} > 1$, we can consider $\theta A + (1-\theta) A_{\text{triv}}$

and apply Theorem 2 to A_θ .

If a decision game G is λ bit secure in the sense of MW,

then, up to a constant bit, G is λ bit secure in the sense of WY.

Proof outline of Theorem 2

Lemma (relabeling [MW18])

For an adversary A and $z \in \{0, 1, \perp\}$, let $\tilde{A}^z$ be an adversary such that

run A and obtain output a

output 0 if $a = z$ and $A_0(z) \geq A_1(z)$

output 1 if $a = z$ and $A_0(z) < A_1(z)$

only one of these occurs

otherwise ($a \neq z$), output $\perp$

Then,

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

Non-verifiable primitive

Computational Diffie-Hellman (CDH):

$$(g^x, g^y) \longrightarrow \boxed{A'} \longrightarrow \text{estimate } g^{xy}$$

non-verifiable search game

$\varepsilon_{A'}^{\mathrm{cdh}}$: success probability

Decision Diffie-Hellman (DDH):

$u = 0 \quad (g^x, g^y, g^{xy})$

or

$u = 1 \quad (g^x, g^y, g^z)$

$$\longrightarrow \boxed{A'} \longrightarrow \text{estimate } u$$

Attack DDH using CDH oracle: probability of $\perp$ is 0

$$A_0 = (\varepsilon_{A'}^{\mathrm{cdh}}, 1 - \varepsilon_{A'}^{\mathrm{cdh}}, 0) \qquad A_1 = (\varepsilon_{A'}^{\mathrm{cdh}}/p, 1 - \varepsilon_{A'}^{\mathrm{cdh}}/p, 0)$$

$$\mathrm{adv}_A^{\mathrm{CS}} = (\mathrm{adv}_A^{\mathrm{TV}})^2 = (1 - 1/p)^2 (\varepsilon_{A'}^{\mathrm{cdh}})^2 \quad \mathrm{adv}_A^{\mathrm{Renyi}} = \Omega(\varepsilon_{A'}^{\mathrm{cdh}})$$

The CS advantage is much smaller than the Renyi advantage

Non-verifiable primitive

Computational Diffie-Hellman (CDH):

$$(g^x, g^y) \longrightarrow \boxed{A'} \longrightarrow \text{estimate } g^{xy}$$

non-verifiable search game

Decision Diffie-Hellman (DDH):

$u=0 \quad (g^x, g^y, g^{xy})$

or

$u=1 \quad (g^x, g^y, g^z)$

$$\longrightarrow \boxed{A'} \longrightarrow \text{estimate } u$$

Apply Lemma (relabeling) with $z=0$

$$A_0 = (\varepsilon^{\mathrm{cdh}}_{A'}, 1-\varepsilon^{\mathrm{cdh}}_{A'}, 0) \qquad A_1 = (\varepsilon^{\mathrm{cdh}}_{A'}/p, 1-\varepsilon^{\mathrm{cdh}}_{A'}/p, 0)$$

$$\tilde{A}^z_0 = (\varepsilon^{\mathrm{cdh}}_{A'}, 0, 1-\varepsilon^{\mathrm{cdh}}_{A'}) \qquad \tilde{A}^z_1 = (\varepsilon^{\mathrm{cdh}}_{A'}/p, 0, 1-\varepsilon^{\mathrm{cdh}}_{A'}/p)$$

$$\mathrm{adv}^{\mathrm{CS}}_{\tilde{A}^z} = \Omega(\varepsilon^{\mathrm{cdh}}_{A'})$$

Summary of advantages for various attacks

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

The CS advantage is sensitive to “labeling”, but after relabeling,

the CS advantage and the Rényi advantage lead to essentially the same bit security.