Bit Security as Computational Cost for Winning Games with High Probability

Shun Watanabe Tokyo University of Agriculture and Technology

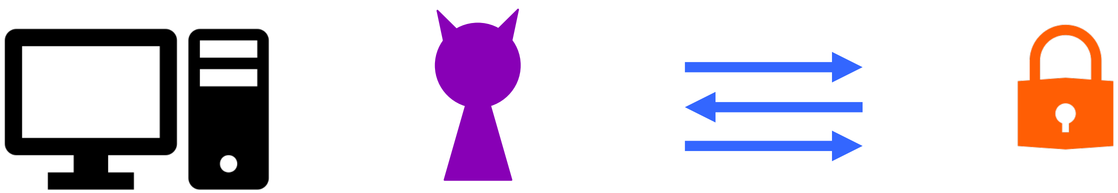
Kenji Yasunaga Tokyo Institute of Technology

Asiacrypt 2021, Virtual

What is Bit Security?

A "well-established" measure of quantifying the security level

Primitive P has k-bit security $\Leftrightarrow$ 2^k operations are needed to break P



How can we define bit security?

Bit Security of One-Way Function

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

Adversary A breaks one-wayness of f $\Leftrightarrow$ $A(f(x))$ outputs y s.t. $f(x) = f(y)$

What is the computational cost needed to break OW?

Solution 1 (Brute-force search):

For $y = 00\cdots0$ to $11\cdots1$ {
  If $f(x) = f(y)$, then output y;
}

Solution 2 (Random guess):

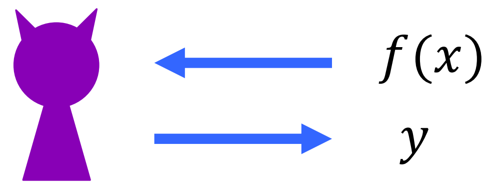
While {
  Choose $y \in \{0,1\}^n$ at random;
  If $f(x) = f(y)$, then output y;
}

⇒ The total cost is $O(t_f \cdot 2^n)$

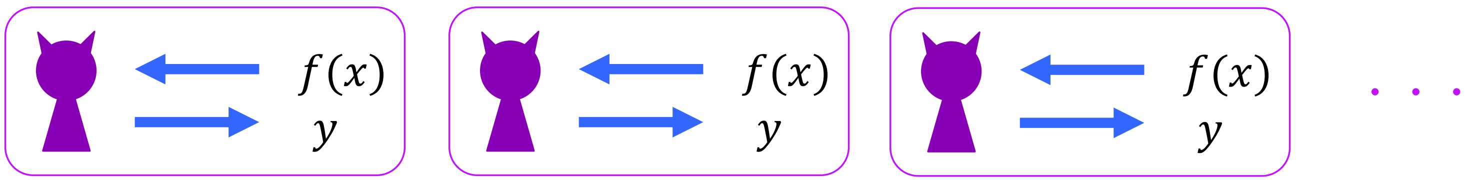
Bit Security of One-Way Function

Solution 3 (Good algorithm):

$\exists A$ with comp. cost T s.t. $\Pr[A \text{ breaks OW}] = \varepsilon$



What if invoking A in total N times?



Roughly, $\Pr[\text{ some } A \text{ breaks OW }]$ will be amplified to εN

The total cost is $O(N \cdot T) = O\left(\frac{T}{\varepsilon}\right)$

Bit Security of One-Way Function

The total cost of $O\left(\frac{T}{\varepsilon}\right)$ is consistent in all solutions

Solution 1 (Brute force): Cost = $t_f \cdot 2^n$ & $\Pr[A \text{ breaks OW}] = 1$

Solution 2 (Random guess): Cost = t_f & $\Pr[A \text{ breaks OW}] = 2^{-n}$

Solution 3 (Good algorithm): Cost = T & $\Pr[A \text{ breaks OW}] = \varepsilon$

⇒ Bit security should be $\min_A \left\{\log_2\left(\frac{T}{\varepsilon}\right) + O(1)\right\}$

Can be extended to other search primitives (signatures, MAC) and assumptions (factoring, discrete logarithm problem, CDH)

Questions

How to define bit security of decision primitives/assumptions (PRG, encryption, DDH) ?

Is the conventional advantage of $2 \cdot \left|\Pr[A \text{ wins game } G] - \frac{1}{2}\right|$ the right measure for bit security?

Our Contributions

Introduce a new framework for defining bit security

- Defined for security games G
- Same operational meaning for search/decision games:

G has k-bit security $\Leftrightarrow$ Every adversary needs cost of 2^k for winning G with high probability (say 0.99)

- Defining the winning condition of search/decision games differently

Rényi advantage is the right measure for decision games

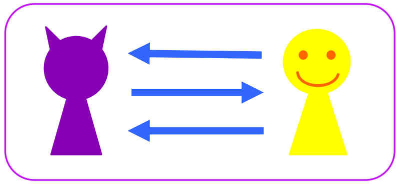
Reductions of bit security between security games

Compare with the framework of Micciancio and Walter (Eurocrypt 2018)

Our Framework

Two adversaries: inner and outer

Inner plays a "usual" game G



For random secret $u \in \{0,1\}^n$

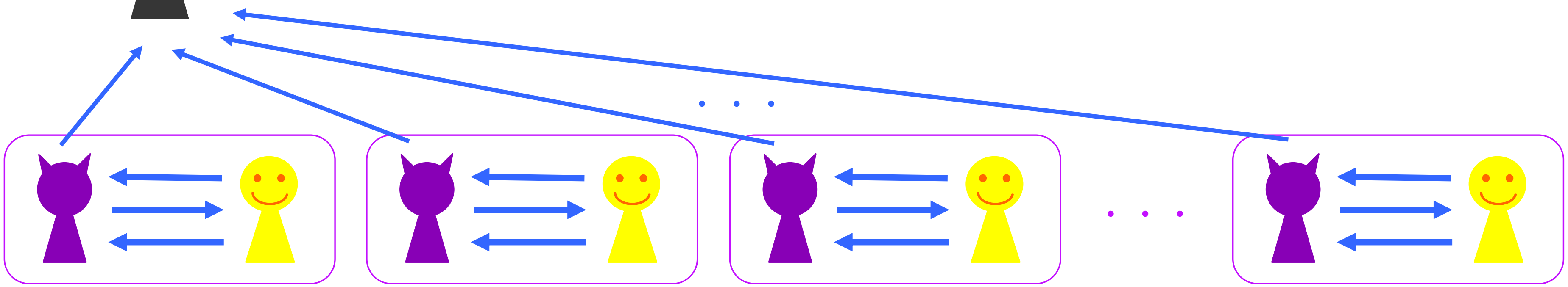
Search game ($n \gg 1$) :

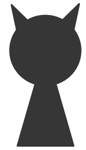
$\Pr[\quad \text{wins } G] \approx 0$

Decision game ($n = 1$) :

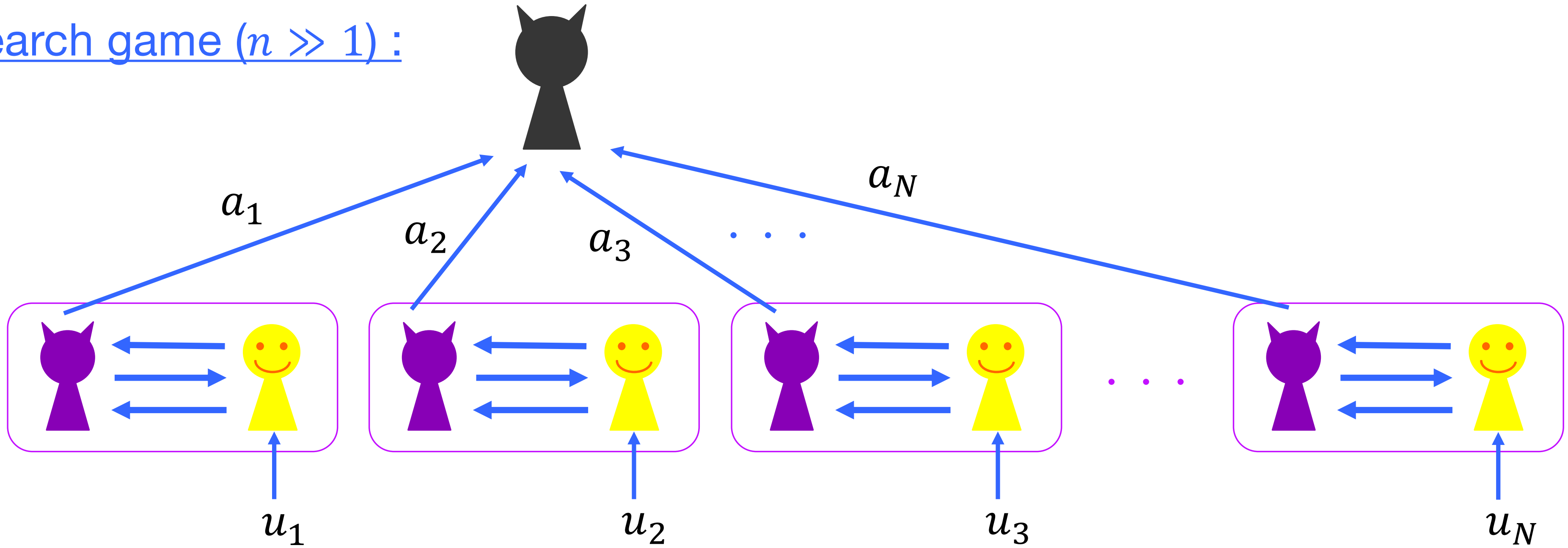
$\Pr[\quad \text{wins } G]$
$:= \Pr[\quad \text{predicts } u] \approx \frac{1}{2}$

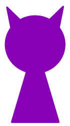
Outer invokes game G to amplify the "winning probability"

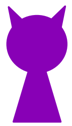
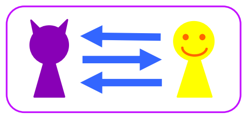


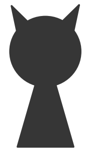
The Winning Condition of 

Search game ($n \gg 1$) :

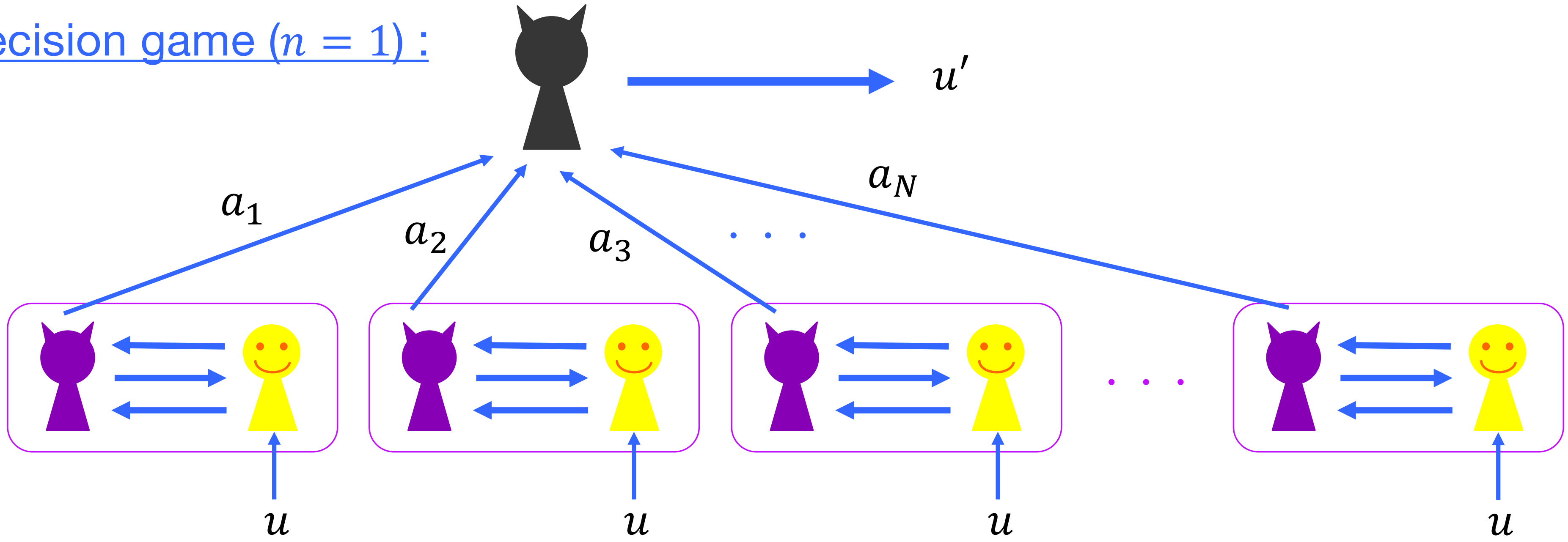


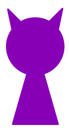
Each  plays an independent game with fresh u_i

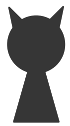
Pr[ wins] $:=$ Pr [some  wins ]

The Winning Condition of 

Decision game ($n = 1$) :



Each  plays an independent game with consistent u

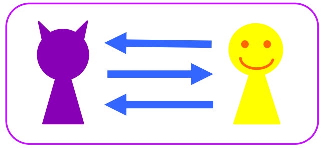
$\Pr[$  wins $] := \Pr[\, u' = u \,]$

Bit Security in Our Framework

Error probability, say $\mu = 0.01$

Bit security of game G $:= \min\left\{ \log_2(N \cdot T) \,:\, \Pr\left[\right.\right.$  $\left.\left.\text{wins}\right] \geq 1 - \mu \right\}$

\# invocations by 

Complexity of 

Implications:

- Every search game has finite bit security ($\leq m + O(1)$ if $a_i \in \{0,1\}^m$)
- A decision game may have infinite bit security
- For decision games,  plays binary hypothesis testing

Characterizing Bit Security

Theorem: For any security game G,

Complexity of

$$\text{Bit security of } G = \min \left\{ \log_2 \left(\frac{T}{\mathrm{adv}(\ )} \right) \right\} + O(1)$$

where

$\mathrm{adv}(\ ) = \Pr[\ \text{wins}\ \ ]$ for search game G;

$\mathrm{adv}(\ ) = \mathrm{adv}^{\mathrm{Renyi}}(\ ) := D_{1/2}(A_0 \| A_1)$ for decision game G;

Rényi divergence of order 1/2

A_u : Output distribution of when $u \in \{0,1\}$ is chosen

Conventional Advantage vs Rényi Advantage

Decision game (n = 1) :

$$\mathrm{adv}^{\mathrm{conv}}\left(\ \right) = \varepsilon \quad \text{if} \quad \Pr\left[\ \text{wins in } \boxed{\ \leftrightarrows\ }\ \right] = \frac{1}{2}(1+\varepsilon)$$

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

Proposition: For any decision game,

$$\varepsilon^2 \lesssim \mathrm{adv}^{\mathrm{Renyi}}\left(\ \right) \lesssim \varepsilon \qquad \text{for any}$$

$$\mathrm{adv}^{\mathrm{Renyi}}\left(\ \right) \approx \varepsilon^2 \qquad \text{for balanced}$$

$$\Pr\left[\ \text{outputs } 0\ \right] > \beta$$

$$\Pr\left[\ \text{outputs } 1\ \right] > \beta$$

for constant $\beta > 0$

"Peculiar" problem of linear tests for PRG can be resolved

PRG against Linear Tests

Pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^m$

For any G, ∃linear test T s.t.

$$\Pr[T(G(x)) = 1] \approx \frac{1}{2}\left(1 + 2^{-\frac{n}{2}}\right)$$ [Alon, Goldreich, Hastad, Perlata (1992)]

Since any linear test is balanced, we have

$$\mathrm{adv}^{\mathrm{conv}}(T) \approx 2^{-\frac{n}{2}}, \qquad \mathrm{adv}^{\mathrm{Renyi}}(T) \approx 2^{-n}$$

If $\mathrm{BS} = \min\left\{\log_2\left(\frac{T}{\mathrm{adv}^{\mathrm{conv}}}\right)\right\}$, it must be $\leq \frac{n}{2}$

Counterintuitive!

In our framework, possible to achieve $\mathrm{BS} = \min\left\{\log_2\left(\frac{T}{\mathrm{adv}^{\mathrm{Renyi}}}\right)\right\} \approx n$

Micciancio & Walter (2018) resolved the problem by their framework

Bit Security Reductions

k-bit secure PRG ➡ k-bit secure OWF

k-bit secure IND-CPA Enc ➡ k-bit secure OW-CPA Enc

k-bit secure DDH assumption ➡ k-bit secure CDH assumption

Goldreich-Levin theorem:

- k-bit secure OWF ➡ k-bit secure HC for balanced adversaries

General case remains open

Distribution approximation:

- Game G^Q employing distribution Q is k-bit secure
- Distri. P and Q are k-bit secure indistinguishable

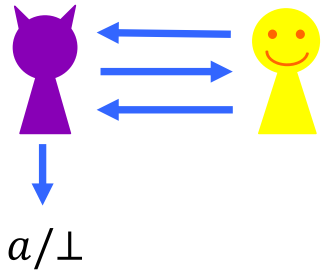
➡ G^P is k-bit secure

Bit Security framework of Micciancio & Walter (2018)

Bit security is defined as $\min_A \left\{ \log_2 \left(\frac{T}{\mathrm{adv}^{\mathrm{MW}}(A)} \right) \right\}$

$$\mathrm{adv}^{\mathrm{MW}}(A) := \frac{I(X,Y)}{H(X)} = 1 - \frac{H(X|Y)}{H(X)}$$

$I(\cdot,\cdot)$: mutual information
$H(\cdot)$: Shannon entropy



where

$X \in \{0,1\}^n$ is a random secret of game G,
$Y \in \{0,1\}^n$ is defined as

$$Y = \begin{cases} \perp & \text{if } A \text{ outputs } \perp \\ X & \text{if } A \text{ wins game } G \\ \text{uniform over } \{0,1\}^n \setminus \{X\} & \text{o.w.} \end{cases}$$

Bit Security framework of Micciancio & Walter (2018)

The advantage can be approximated by

$$\mathrm{adv}^{\mathrm{MW}}(A) \approx \Pr[\, A \text{ wins } G\,] \qquad \text{for search games}$$

$$\mathrm{adv}^{\mathrm{MW}}(A) \approx \alpha_A \cdot (2\beta_A - 1)^2 \qquad \text{for decision games}$$

where

$$\alpha_A = \Pr[A \text{ outputs } a \neq \perp], \quad \beta_A = \Pr[A \text{ wins } G \,|\, A \text{ outputs } a \neq \perp]$$

- If $\Pr[A \text{ wins game } G] \leq \frac{1}{2}\left(1 + 2^{-k/2}\right)$ for any A, G has k-bit security
- GL theorem is tight (k-BS OWF → k-BS HC)

Our Framework:

- BS has operational meaning
- If $\Pr[A \text{ wins game } G] \leq \frac{1}{2}\left(1 + 2^{-k/2}\right)$ for any A, G has bit security $\frac{k}{2}$ to k
- Tightness of GL theorem requires improved reductions

Conclusions

Bit security framework with operational meaning

G has k-bit security $\Leftrightarrow$ Every adversary needs cost of 2^k for winning G with probability 0.99

Rényi advantage is the right measure for decision games

Future Work

Tight reduction for GL theorem in our framework

Which notion should we employ for bit security?
Axiomatic approach?

Thank you