# Quantifying the Security Levels of Cryptographic Primitives


Kenji Yasunaga

Tokyo Institute of Technology, Japan

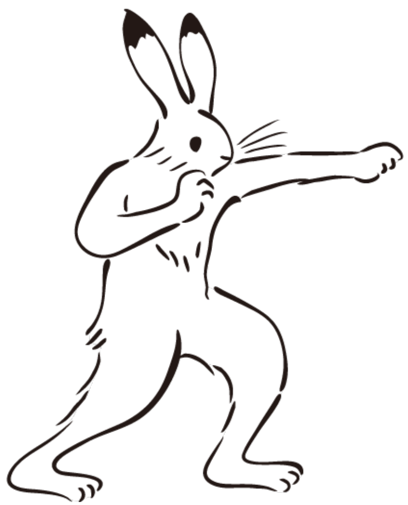


T3: Information Sciences, TENCON 2022

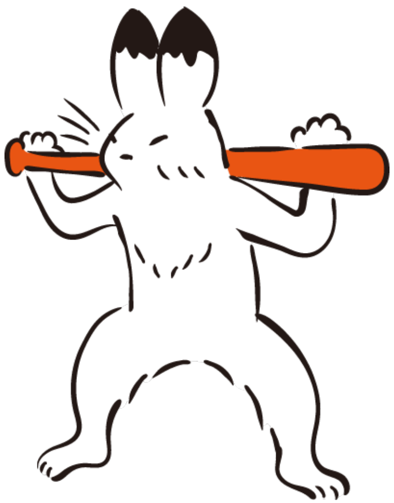
Nov. 1-4 2022 @ Hybrid (Hong Kong | Online)

# Q1. Which is more serious?

Attack with success probability 1 %



Attack with success probability 50 %



# Q2. Which is more serious?

$10 attack with success prob. 1 %

$1000 attack with success prob. 50 %

# Q3. Which is more serious?

Attack with success probability 40 %

Attack with success probability 50 %

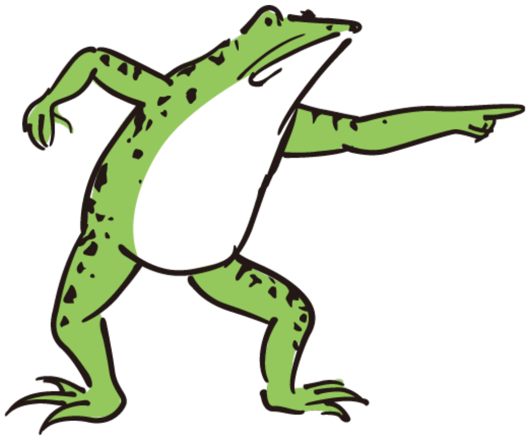
Prediction Games

| 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 |

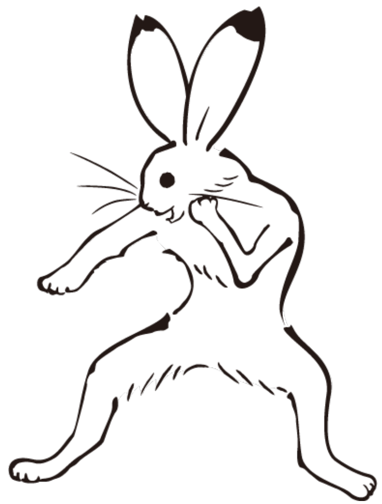
# Q4. Which is more serious?

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 |

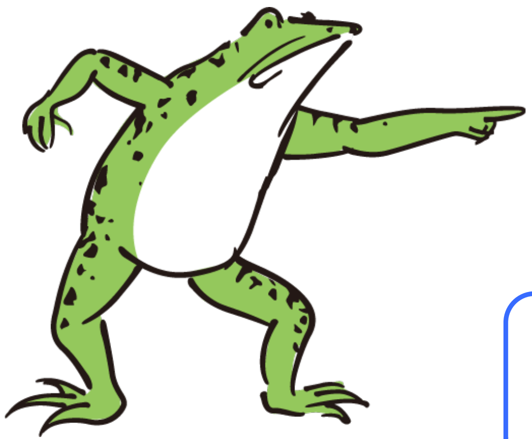
Attack with success probability 60 %



| 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 |

# Q4. Which is more serious?

Attack with success probability 60 %

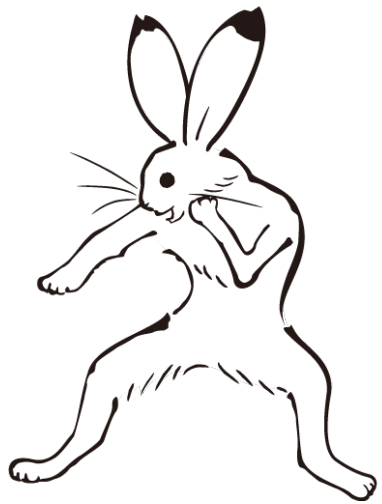


Arranged based on the outcomes

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 |

Attack with success probability 60 %



60% | 60%

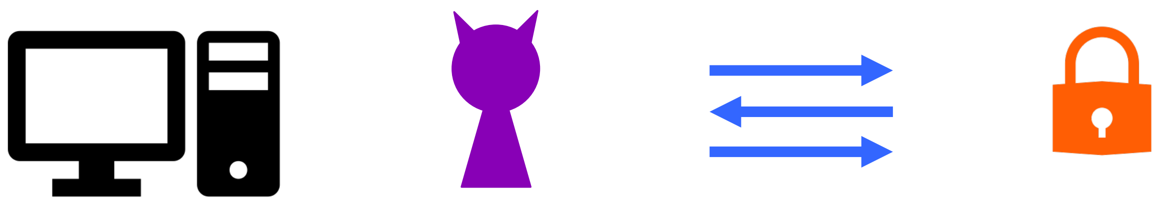
| Game | 1 2 4 7 9 | 3 5 6 8 10 |
|---|---|---|
| Prediction | 1 0 0 0 1 | 0 1 0 1 1 |
| Outcome | 0 0 0 0 0 | 1 1 1 1 1 |

# Bit Security

# What is Bit Security?

A "well-established" measure of quantifying the security levels of cryptographic primitives

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

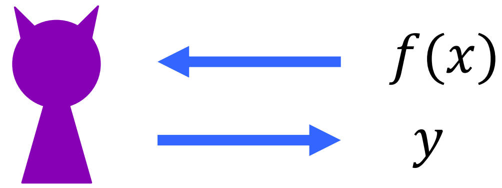


Formally defined?

# Bit Security of One-Way Function

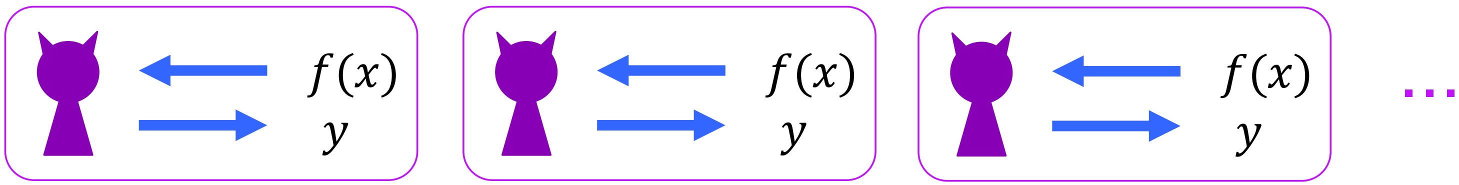
$f: \{0,1\}^n \to \{0,1\}^n$ $\qquad x \underset{\text{hard}}{\overset{\text{easy}}{\rightleftarrows}} f(x)$

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




⇒ Bit security is $\le \log_2\left(\frac{T}{\varepsilon}\right)$ Why?

What if invoking $A$ in total $N$ times?




$\Pr[\text{ some } A \text{ breaks OW }]$ will be amplified to $\varepsilon N$

⇒ The total cost is $O(N \cdot T) = O\left(\frac{T}{\varepsilon}\right)$ ⇒ $\mathrm{BS} = \min_A \left\{\log_2\left(\frac{T}{\varepsilon}\right)\right\}$

# Types of Security Games

## Search Games

finds a solution from $\{0,1\}^n$ for $n >> 1$

- One-way function (OWF)
- Signature scheme

Bit security can be defined similarly to OWF

- Factoring / Computational Diffie-Hellman (CDH) assumptions

## Decision Games

distinguishes the two cases (0/1)

- Pseudorandom generator (PRG)
- Encryption scheme
- Decisional Diffie-Hellman (DDH) assumption

# Questions

How to define bit security of decision games ?

Is the “conventional” advantage of

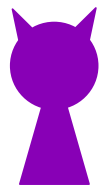
$$\mathrm{adv}^{\mathrm{conv}} = 2 \cdot \left| \Pr\left[ \quad \text{wins the game} \right] - \frac{1}{2} \right|$$

the right measure for bit security?

# A Peculiar Problem: PRG against Linear Tests

Pseudorandom generator (PRG) $g\colon \{0,1\}^n \to \{0,1\}^m$

$$y = \begin{cases} g(U_n) & (u = 0) \\ U_m & (u = 1) \end{cases}$$

$y \longrightarrow$  $\longrightarrow u'$

For any $g$, ∃linear test $L$ of cost $O(n)$ s.t.

$$\Pr\left[L\left(g(U_n)\right) = 1\right] \approx \frac{1}{2}\left(1 + 2^{-\frac{n}{2}}\right) \ \& \ \Pr[L(U_m) = 1] = \frac{1}{2}$$ [Alon et al. (1992)]

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

Counterintuitive!

# Bit Security Frameworks

[Micciancio, Walter (Eurocrypt 2018)]

- First theoretical framework of BS
- Allowing $\perp$ (failure symbol) as output
- Based on Mutual Information and Shannon Entropy

[Watanabe, Yasunaga (Asiacrypt 2021)]

- Operational approach

[Watanabe, Yasunaga (ePrint 2022)]

- Allowing $\perp$ in the framework of [WY21]

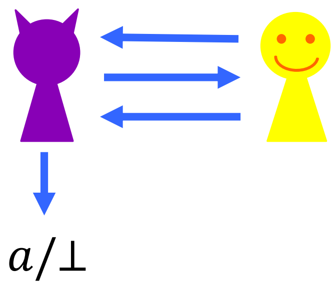
# Framework of Micciancio & Walter (2018)

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

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

where

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




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

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

# Framework of Micciancio & Walter (2018)

The CS advantage can be approximated as

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

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

where

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

Notes:

- Resolved the linear test problem of PRG:

  $\Pr\left[L\left(g(U_n)\right) = 1\right] \approx \frac{1}{2}\left(1 + 2^{-\frac{n}{2}}\right)$ & $\Pr[L(U_m) = 1] = \frac{1}{2}$ ➔ $\mathrm{adv}^{\mathrm{CS}}(L) \approx 2^{-n}$

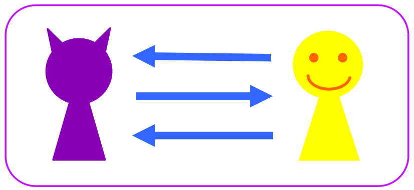
- Difficult to understand the operational meaning

# Bit Security Framework of [WY21]

# [WY21] Framework

Two adversaries: inner and outer

Inner plays a "usual" game $G$



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

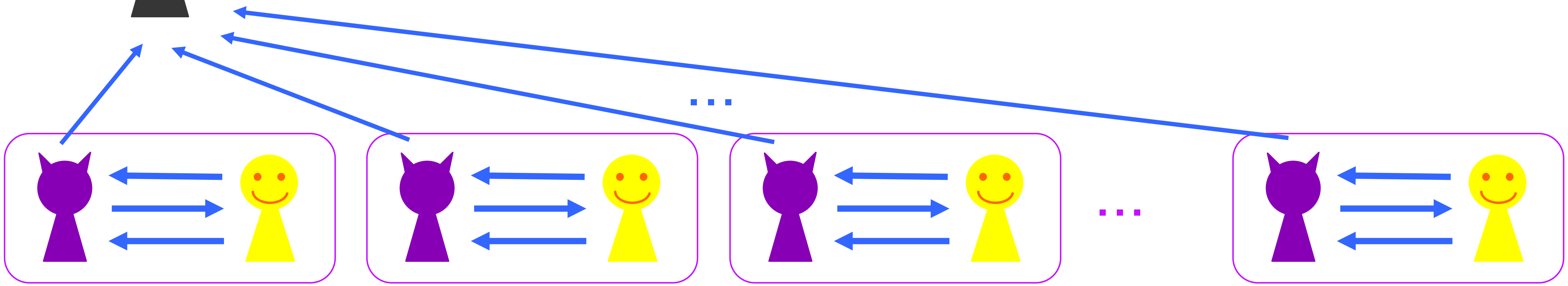
Search game ($n \gg 1$) :

$\Pr[$ wins $G] \approx 0$

Decision game ($n = 1$) :

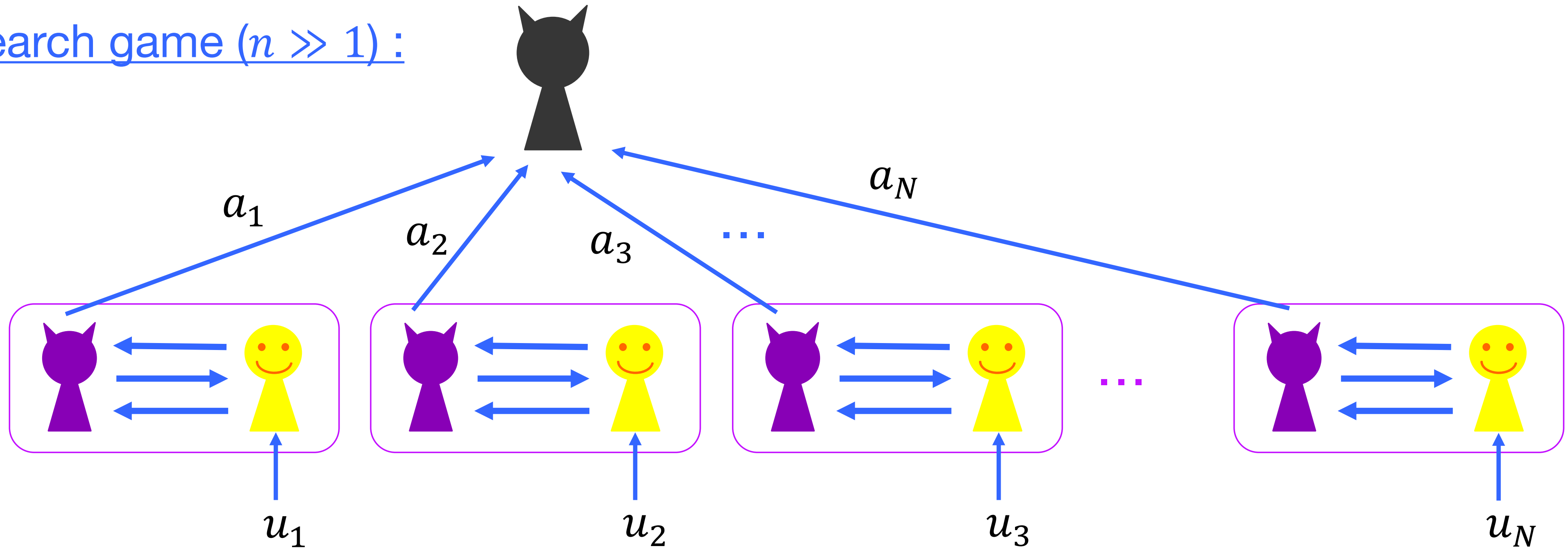
$\Pr[$ wins $G]$
$:= \Pr[$ predicts $u] \approx \frac{1}{2}$

Outer invokes game $G$ to amplify the "winning probability"



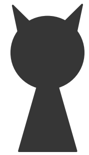
# The Winning Condition of

Search game ($n \gg 1$) :

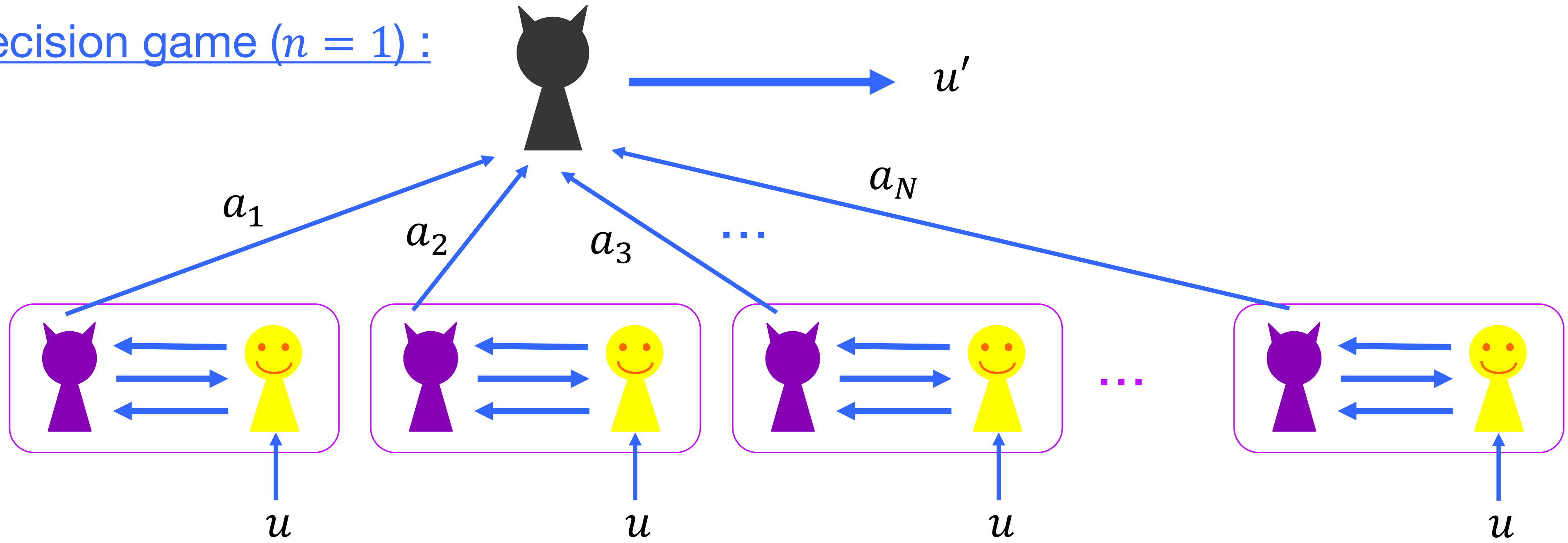


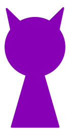

Each plays an independent game with fresh $u_i$

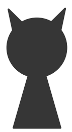
$$\Pr\big[\ \text{wins}\ \big] := \Pr\big[\text{some}\ \ \text{wins}\ \ \big]$$

## The Winning Condition of 

Decision game ($n = 1$) :




Each  plays an independent game with consistent $u$

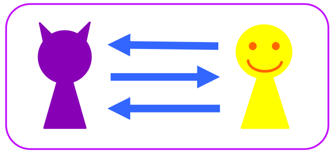
Pr[  wins ] $:= \Pr[\, u' = u \,]$

# [WY21] Framework

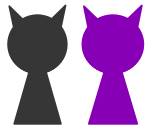


Bit security of game $G$ $:= \min$  $\left\{ \log_2(N \cdot T) : \Pr\left[\right.\right.$  $\left.\left.\text{wins}\right] \geq 1 - \mu \right\}$

Notes:

- Bit security is defined *operationally*
  - (Logarithm of) the total cost of  to win game with high probability
- For decision games,  plays Bayesian hypothesis testing

# Characterizing Bit Security of [WY21]

**Theorem** : For any security game $G$,

Cost of running

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

where

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

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

Rényi divergence of order 1/2

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

# Implications of [WY21] Framework

Resolved the linear test problem of PRG:

$$\Pr\left[L\left(g(U_n)\right) = 1\right] \approx \frac{1}{2}\left(1 + 2^{-\frac{n}{2}}\right) \ \& \ \Pr[L(U_m) = 1] = \frac{1}{2}$$

$$\Rightarrow \ \mathrm{adv}^{\mathrm{Renyi}}(L) \in \left[2^{-n}, 2^{-\frac{n}{2}}\right]$$

- Cf. $\mathrm{adv}^{\mathrm{CS}}(L) \approx 2^{-n}$

Two frameworks ([MW18], [WY21]) are “essentially” equivalent [WY22]:

- $\mathrm{adv}_A^{\mathrm{CS}} \leq O\left(\mathrm{adv}_A^{\mathrm{Renyi}}\right)$ for any adversary $A$
- Any adversary $A$ ( with $\mathrm{adv}_A^{\mathrm{CS}} \ll \mathrm{adv}_A^{\mathrm{Renyi}}$ ) can be converted to $A'$ s.t.

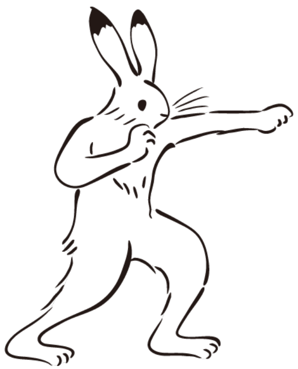
$$\mathrm{adv}_{A'}^{\mathrm{CS}} \geq \Omega\left(\mathrm{adv}_A^{\mathrm{Renyi}}\right)$$

# Evaluations in Two Frameworks [MW18], [WY21]

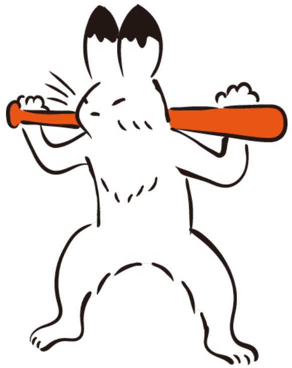
(Answers to Q1 ~ Q4)

# A1. (Search Games)

Attack with success probability 1 %



Attack with success probability 50 %



$$\mathrm{adv}^{\mathrm{CS}} = \mathrm{adv}^{\mathrm{Renyi}} = \Pr[A \text{ wins}]$$

$\Pr[A \text{ wins}] = 0.01$

$\Pr[A \text{ wins}] = 0.5$

# A2. (Search Games)

$10 attack with success prob. 1 %

$$\text{TotalCost}_{[\text{MW18}]} = \text{TotalCost}_{[\text{WY21}]}$$
$$= \frac{\text{Cost}}{\Pr[A \text{ wins}]} = \frac{10}{0.01} = 1000 \ \ (\text{dollars})$$

$1000 attack with success prob. 50 %

$$\text{TotalCost}_{[\text{MW18}]} = \text{TotalCost}_{[\text{WY21}]}$$
$$= \frac{\text{Cost}}{\Pr[A \text{ wins}]} = \frac{1000}{0.5} = 2000 \ \ (\text{dollars})$$

# A3. (Decision Games)

## Attack with success probability 40 %

| 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 |

$\Pr[A \text{ wins}] = 0.4$

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

$A_0 = (0.6, 0.4)$
$A_1 = (0.8, 0.2)$

$$\mathrm{adv}^{\mathrm{CS}} = (2 \cdot 0.4 - 1)^2 = 0.04$$
$$\mathrm{adv}^{\mathrm{Renyi}} = D_{1/2}\left(A_0 \| A_1\right) \approx 0.049$$

## Attack with success probability 50 %

| 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 |

$\Pr[A \text{ wins}] = 0.5$

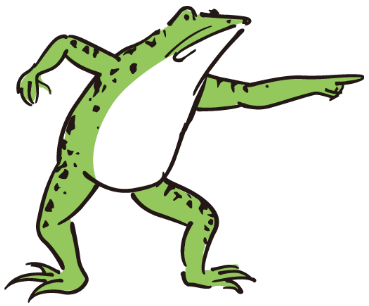
| Game | 1 | 2 | 4 | 7 | 9 | 3 | 5 | 6 | 8 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Prediction | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| Outcome | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |

$A_0 = (0.4, 0.6)$
$A_1 = (0.4, 0.6)$

$$\mathrm{adv}^{\mathrm{CS}} (2 \cdot 0.5 - 1)^2 = 0$$
$$\mathrm{adv}^{\mathrm{Renyi}} = D_{1/2}\left(A_0 \| A_1\right) = 0$$

# A4. (Decision Games)

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 |

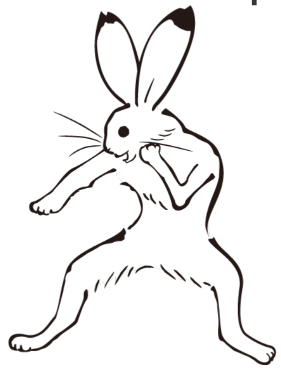
$\Pr[A \text{ wins}] = 0.6$

| 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 |

$A_0 = (1, 0)$
$A_1 = (0.6\ 0.4)$

$$\mathrm{adv}^{\mathrm{CS}} = (2 \cdot 0.6 - 1)^2 = 0.04$$
$$\mathrm{adv}^{\mathrm{Renyi}} = D_{1/2}\left(A_0 \| A_1\right) \approx 0.51$$

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 |

$\Pr[A \text{ wins}] = 0.6$

| 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 |

$A_0 = (0.6, 0.4)$
$A_1 = (0.4, 0.6)$

$$\mathrm{adv}^{\mathrm{CS}} (2 \cdot 0.6 - 1)^2 = 0.04$$
$$\mathrm{adv}^{\mathrm{Renyi}} = D_{1/2}\left(A_0 \| A_1\right) = 0.041$$

# Conclusions

Two frameworks for evaluating bit security

**Micciancio and Walter (Eurocrypt 2018)**
- Mutual information and Shannon entropy
- Defined by $\min_A \left\{ \log_2 \left( \frac{T}{\mathrm{adv}^{\mathrm{CS}}(A)} \right) \right\}$

**Watanabe and Yasunaga (Asiacrypt 2021)**
- Operational definition
- Characterized by $\min_A \left\{ \log_2 \left( \frac{T}{\mathrm{adv}^{\mathrm{Renyi}}(A)} \right) \right\}$


- Both resolved the linear test problem of PRG
- They are essentially equivalent
  - $\mathrm{adv}_A^{\mathrm{CS}} \leq O\left(\mathrm{adv}_A^{\mathrm{Renyi}}\right)$ for any adversary $A$
  - Any adversary $A$ can be converted to $A'$ s.t. $\mathrm{adv}_{A'}^{\mathrm{CS}} \geq \Omega\left(\mathrm{adv}_A^{\mathrm{Renyi}}\right)$