判定問題が 128 ビット安全であるとは？

渡辺 峻 （東京農工大学）　安永 憲司 （東京工業大学）

SCIS 2023 @ リーガロイヤルホテル小倉

暗号で登場する計算問題・安全性

- 素因数分解問題
- 離散対数問題
- 計算型 Diffie-Hellman (CDH) 問題
- Learning with Errors (LWE) 問題
- 判定型 Diffie-Hellman (DDH) 問題
- 判定型 LWE 問題

- 関数の一方向性
- 署名の偽造不可能性
- 確率分布の識別不可能性
- 擬似ランダム関数の安全性
- 暗号方式の IND-CPA 安全性
- プロトコルのゼロ知識性
- 汎用的結合可能 (UC) 安全性

暗号で登場する計算問題・安全性

探索問題

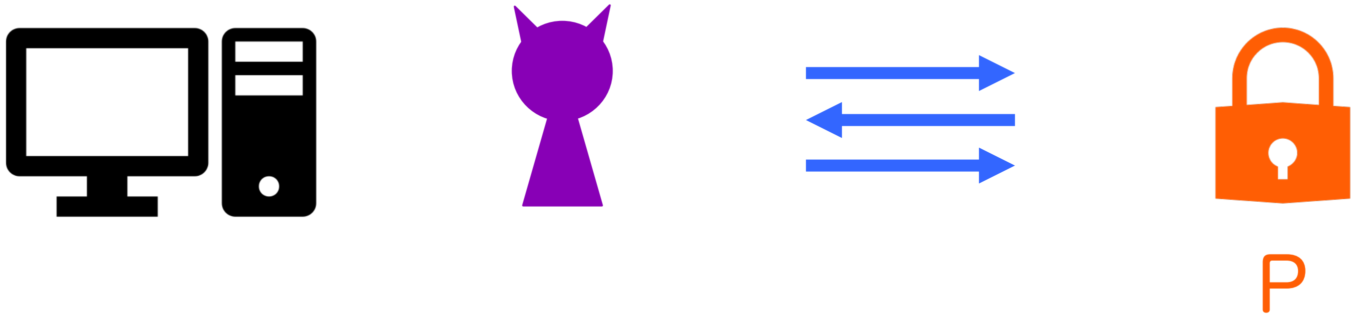
- 素因数分解問題
- 離散対数問題
- 計算型 Diffie-Hellman (CDH) 問題
- Learning with Errors (LWE) 問題
- 判定型 Diffie-Hellman (DDH) 問題
- 判定型 LWE 問題

判定問題

- 関数の一方向性
- 署名の偽造不可能性
- 確率分布の識別不可能性
- 擬似ランダム関数の安全性
- 暗号方式の IND-CPA 安全性
- プロトコルのゼロ知識性
- 汎用的結合可能 (UC) 安全性

128 ビット安全性

暗号技術 P が 128 ビット安全 ⇔ P への攻撃に 2^{128} 回の演算が必要



判定問題への攻撃の脅威をどのように見積もるべきか？

Q1. どちらがより脅威か？

攻撃成功確率 40 %

攻撃成功確率 50 %

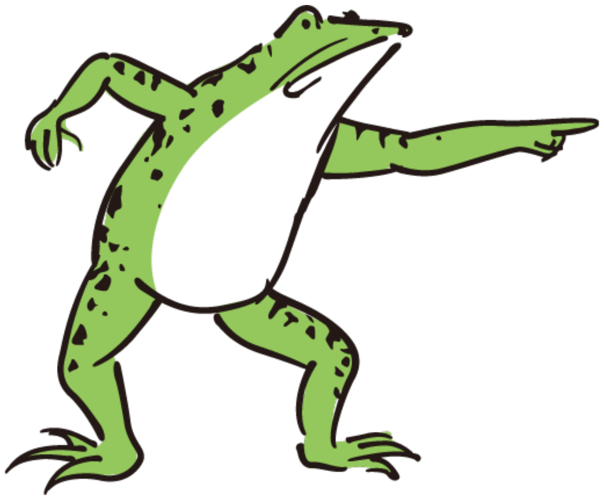
予測ゲーム

ゲーム	1	2	3	4	5	6	7	8	9	10
予測	1	0	0	0	1	0	0	0	1	0
結果	0	0	1	0	1	1	0	1	0	1

ゲーム	1	2	3	4	5	6	7	8	9	10
予測	0	1	0	1	0	1	0	1	1	1
結果	0	0	1	0	1	1	0	1	0	1

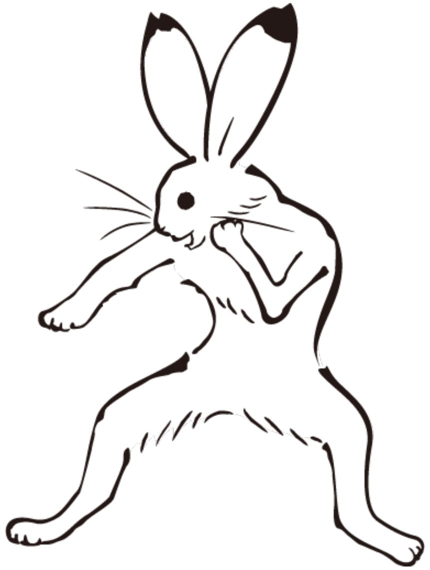
Q2. どちらがより脅威か？

攻撃成功確率 60 %



ゲーム	1	2	3	4	5	6	7	8	9	10
予測	0	0	0	0	1	0	0	0	0	0
結果	0	0	1	0	1	1	0	1	0	1

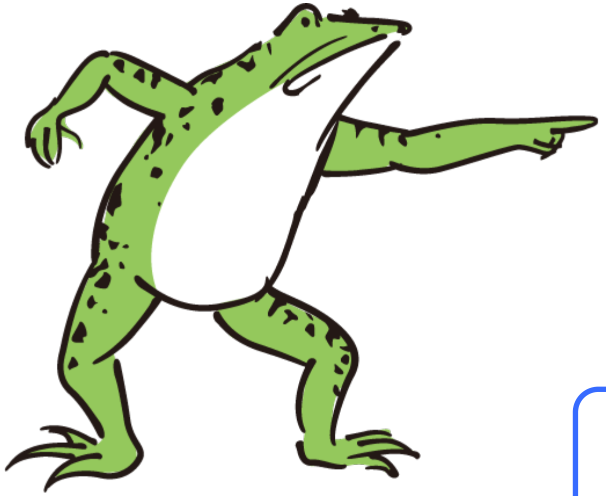
攻撃成功確率 60 %



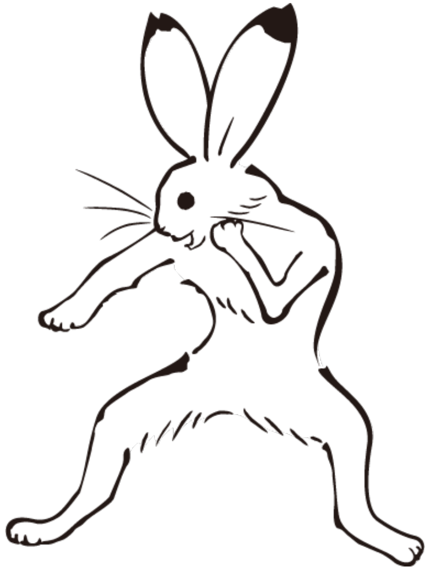
ゲーム	1	2	3	4	5	6	7	8	9	10
予測	1	0	0	0	1	0	0	1	1	1
結果	0	0	1	0	1	1	0	1	0	1

Q2. どちらがより脅威か？

攻撃成功確率 60 %



攻撃成功確率 60 %



結果毎に並べ替え

100%　　20%

ゲーム	1 2 4 7 9	3 5 6 8 10
予測	0 0 0 0 0	0 1 0 0 0
結果	0 0 0 0 0	1 1 1 1 1

60%　　60%

ゲーム	1 2 4 7 9	3 5 6 8 10
予測	1 0 0 0 1	0 1 0 1 1
結果	0 0 0 0 0	1 1 1 1 1

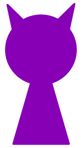
本研究の成果

判定問題のビット安全性に関する２つの枠組み

- Micciancio-Walter (Eurocrypt 2018)
- Watanabe-Yasunaga (Asiacrypt 2021)

で評価される量は「ほぼ」等しい

よく使われている



$$\mathrm{adv}^{\mathrm{TV}} = 2 \cdot \left| \Pr\left[\text{が安全性ゲームに勝つ} \right] - \frac{1}{2} \right|$$

という優位性 (advantage) では不十分

判定問題のビット安全性の枠組み

[Micciancio, Walter (Eurocrypt 2018)]

- 判定問題のビット安全性を導入
- 攻撃者の出力として $\perp$ (失敗) を許す
- 相互情報量やシャノンエントロピーを使った定義

[Watanabe, Yasunaga (Asiacrypt 2021)]

- 操作的な定義

[Watanabe, Yasunaga (ePrint 2022)]

- 上記 [WY21] において出力に $\perp$ を許す

操作的な定義

何らかの量を操作 (operation) によって定めること

例．損失なしデータ圧縮におけるシャノンエントロピー

情報源 X の損失なし圧縮関数 $f:\ \mathcal{X} \to \{0,1\}^*$ に対し,

操作的な定義

最小平均符号長を $\mathrm{minLen}(X) := \min_f \left\{ \mathbb{E}\left[\mathrm{Len}\left(f(X) \right) \right] \right\}$ と定めると

$$H(X) - \log_2(e(H(X)+1)) \le \mathrm{minLen}(X) \le H(X)$$

のようにシャノンエントロピー $H(X)$ で特徴づけられる

[Micciancio, Walter (Eurocrypt 2018)]

$I(\cdot,\cdot)$: 相互情報量
$H(\cdot)$: シャノンエントロピー

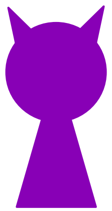
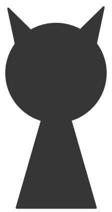
- 新しい優位性 $\mathrm{adv}^{\mathrm{MW}}(A) := \dfrac{I(U,Y)}{H(U)}$ を導入し，
  ビット安全性を $\min_A \left\{\log_2\left(\dfrac{T_A}{\mathrm{adv}^{\mathrm{MW}}(A)}\right)\right\}$ と定義（探索・判定問題で共通）
  - $U \in \{0,1\}$: 秘密，　$Y \in \{0,1,\perp\}$: 攻撃者 A の出力，　T_A ： A の計算コスト

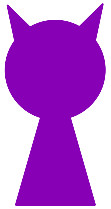
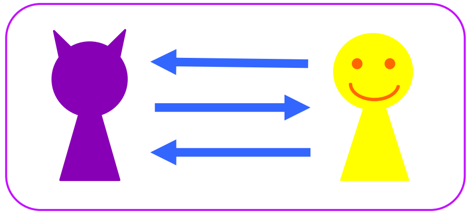
- 判定問題に対し，$\mathrm{adv}^{\mathrm{MW}}(A) \approx \dfrac{1}{2\ln 2} \cdot \alpha_A(2\beta_A - 1)^2$ を証明
  - $\alpha_A = \Pr[Y \neq \perp]$，$\beta_A = \Pr[Y = U \mid Y \neq \perp]$

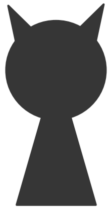
- 条件付き二乗 (Conditional Squared) 優位性 $\mathrm{adv}^{\mathrm{CS}}(A) := \alpha_A \cdot (2\beta_A - 1)^2$ により
  判定問題のビット安全性を $\min_A \left\{\log_2\left(\dfrac{T_A}{\mathrm{adv}^{\mathrm{CS}}(A)}\right)\right\}$ と再定義

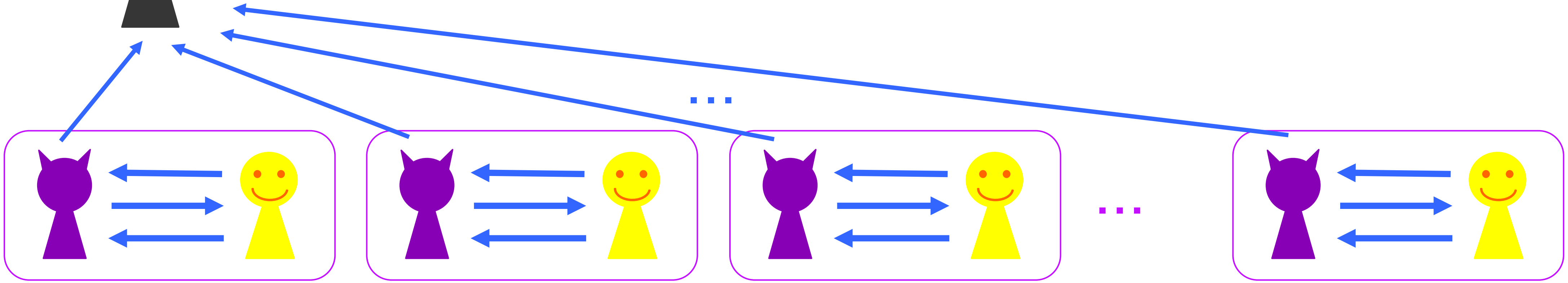
操作的な意味は不明確

Watanabe-Yasunaga の枠組み

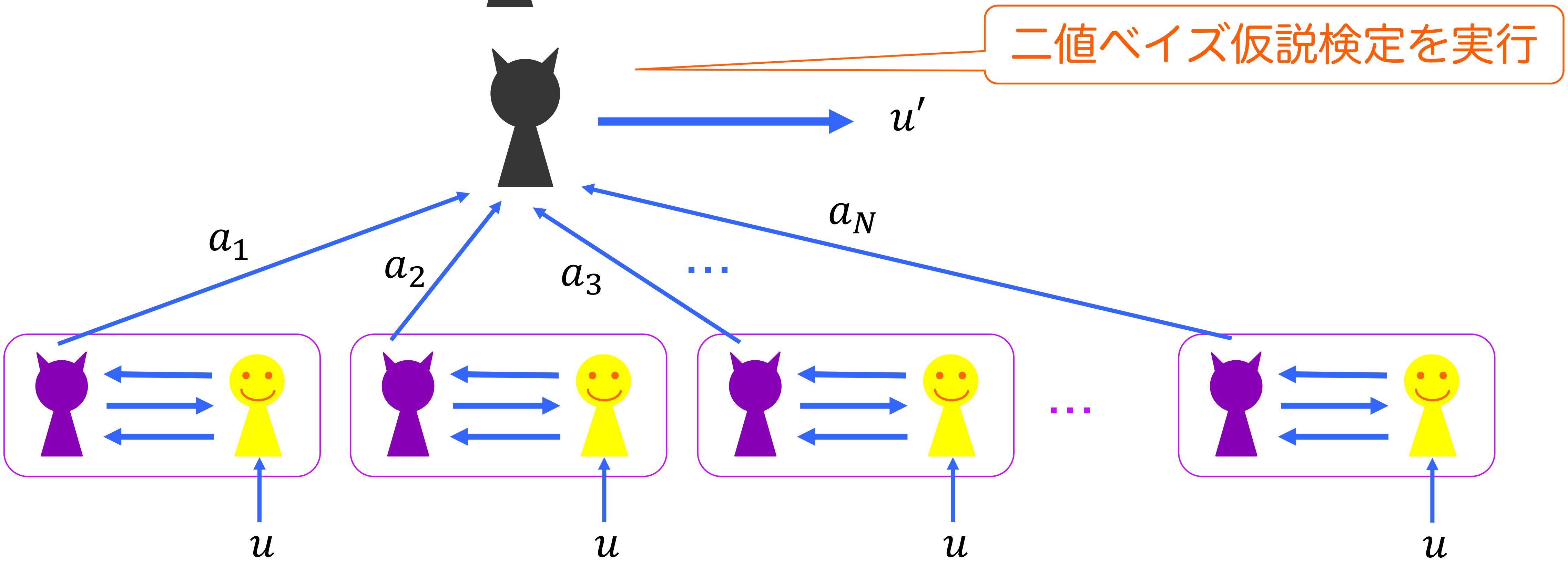
二種類の攻撃者：内側  と外側 

内側  は安全性ゲーム G を実行 

外側  はゲーム G を繰り返し実行して「勝率」を上げる



外側 の勝率（判定問題のとき）



内側 の各ゲームは同じ秘密 $u \in \{0,1\}$ で独立に実行

の勝率 $:= \Pr[\, u' = u \,]$

Watanabe-Yasunaga の枠組み

誤り確率 μ $(= 0.01)$

ゲーム G のビット安全性 $\mathrm{BS}_G := \min\left\{ \log_2(N \cdot T) : \right.$ の勝率 $\left. \geq 1 - \mu \right\}$

による繰り返し回数

ゲーム の実行コスト

特徴づけとして

$$\mathrm{BS}_G = \min \left\{ \log_2 \left(\frac{T_A}{\mathrm{adv}^{\mathrm{Renyi}}(\ )} \right) \right\} + O(1)$$ を証明

A_u : 秘密が $u \in \{0,1\}$ の ときの の出力分布

- Rényi 優位性 $\mathrm{adv}^{\mathrm{Renyi}}(\ ) := D_{1/2}(A_0 \| A_1) := -2 \log_2 \sum_x \sqrt{A_0(x) A_1(x)}$

次数 1/2 の Rényi divergence

$\mathrm{adv}^{\mathrm{CS}}(A)$ と $\mathrm{adv}^{\mathrm{Renyi}}(A)$ の関係

定理：任意の A に対し,

- $\mathrm{adv}^{\mathrm{CS}}(A) \lesssim \mathrm{adv}^{\mathrm{Renyi}}(A)$
- コスト同等の A' が存在し，$\mathrm{adv}^{\mathrm{CS}}(A') \gtrsim \mathrm{adv}^{\mathrm{Renyi}}(A)$

各 A については　$\mathrm{adv}^{\mathrm{CS}}(A) \lesssim \mathrm{adv}^{\mathrm{Renyi}}(A)$ であるが,

$$\min_A \left\{ \log_2 \left(\frac{T_A}{\mathrm{adv}^{\mathrm{CS}}(A)} \right) \right\} \approx \min_A \left\{ \log_2 \left(\frac{T_A}{\mathrm{adv}^{\mathrm{Renyi}}(A)} \right) \right\}$$

$\mathrm{adv}^{\mathrm{TV}}(A)$, $\mathrm{adv}^{\mathrm{CS}}(A)$, $\mathrm{adv}^{\mathrm{Renyi}}(A)$ の比較

$$A_u = (p_0, p_1, p_\perp) \Leftrightarrow \Pr[Y = 0|u] = p_0, \Pr[Y = 1|u] = p_1, \Pr[Y = \perp] = p_\perp$$

攻撃分布	$\mathrm{adv}^{\mathrm{TV}}(A)$	$\mathrm{adv}^{\mathrm{CS}}(A)$	$\mathrm{adv}^{\mathrm{Renyi}}(A)$
$A_0 = \left(\frac{1}{2}+\varepsilon,\ \frac{1}{2}-\varepsilon,\ 0\right)$ $A_1 = \left(\frac{1}{2},\ \frac{1}{2},\ 0\right)$ 例．PRG への線形検査攻撃	ε	ε^2	$\Theta(\varepsilon^2)$
$A_0 = (\varepsilon,\ 0,\ 1-\varepsilon)$ $A_1 = \left(\frac{\varepsilon}{2},\ \frac{\varepsilon}{2},\ 1-\varepsilon\right)$ 例．PRG への逆像攻撃	$\varepsilon/2$	$\varepsilon/2$	$\Theta(\varepsilon)$
$A_0 = (\varepsilon,\ 1-\varepsilon,\ 0)$ $A_1 = \left(\frac{\varepsilon}{p},\ 1-\frac{\varepsilon}{p},\ 0\right)$ 例．CDH攻撃者を使ったDDH攻撃	$\left(1-\frac{1}{p}\right)\varepsilon$	$\left(1-\frac{1}{p}\right)^2\varepsilon^2$	$\Theta(\varepsilon)$
$A_0 = \left(\frac{1}{2}-\frac{\varepsilon}{2},\ \frac{1}{2}-\frac{\varepsilon}{2},\ \varepsilon\right)$ $A_1 = \left(\frac{1}{2}-\frac{\varepsilon}{4},\ \frac{1}{2}-\frac{\varepsilon}{4},\ \frac{\varepsilon}{2}\right)$ 例．PRG への ⊥ を使った逆像攻撃	$\varepsilon/2$	0	$\Theta(\varepsilon)$

A1. どちらが脅威か？

攻撃成功確率 40 %

ゲーム	1 2 3 4 5 6 7 8 9 10
予測	1 0 0 0 1 0 0 0 1 0
結果	0 0 1 0 1 1 0 1 0 1

$\Pr[A\text{ が勝つ}] = 0.4$

ゲーム	1 2 4 7 9	3 5 6 8 10
予測	1 0 0 0 1	0 1 0 0 0
結果	0 0 0 0 0	1 1 1 1 1

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

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

攻撃成功確率 50 %

ゲーム	1 2 3 4 5 6 7 8 9 10
予測	0 1 0 1 0 1 0 1 1 1
結果	0 0 1 0 1 1 0 1 0 1

$\Pr[A\text{ が勝つ}] = 0.5$

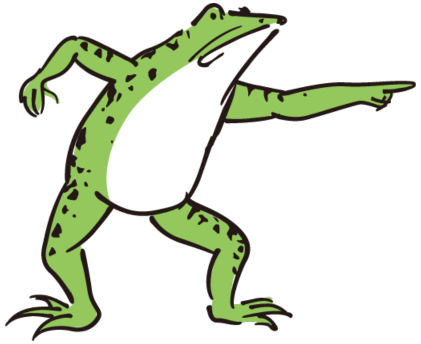
ゲーム	1 2 4 7 9	3 5 6 8 10
予測	0 1 1 0 1	0 0 1 1 1
結果	0 0 0 0 0	1 1 1 1 1

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

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

A2. どちらが脅威か？

攻撃成功確率 60 %



ゲーム	1	2	3	4	5	6	7	8	9	10
予測	0	0	0	0	1	0	0	0	0	0
結果	0	0	1	0	1	1	0	1	0	1

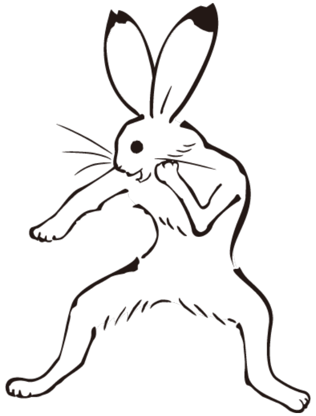
$\Pr[A \text{が勝つ}] = 0.6$

ゲーム	1	2	4	7	9	3	5	6	8	10
予測	0	0	0	0	0	0	1	0	0	0
結果	0	0	0	0	0	1	1	1	1	1

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

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

攻撃成功確率 60 %



ゲーム	1	2	3	4	5	6	7	8	9	10
予測	1	0	0	0	1	0	0	1	1	1
結果	0	0	1	0	1	1	0	1	0	1

$\Pr[A \text{が勝つ}] = 0.6$

ゲーム	1	2	4	7	9	3	5	6	8	10
予測	1	0	0	0	1	0	1	0	1	1
結果	0	0	0	0	0	1	1	1	1	1

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

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

まとめ

判定問題のビット安全性を評価する２つの枠組

Micciancio-Walter (Eurocrypt 2018)

- 相互情報量やエントロピーを利用
- $\mathrm{adv}^{\mathrm{MW}}(A) = \frac{I(U,Y)}{H(U)} \approx \mathrm{adv}^{\mathrm{CS}}(A)$ を踏まえ，
  $\min_{A}\left\{\log_2\left(\frac{T_A}{\mathrm{adv}^{\mathrm{CS}}(A)}\right)\right\}$ として定義

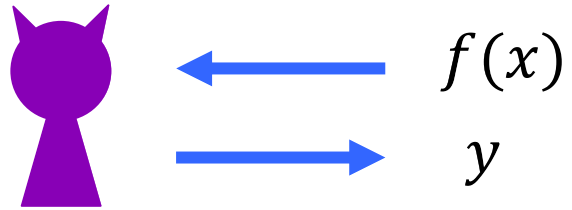
Watanabe-Yasunaga (Asiacrypt 2021)

- 操作的な定義
- $\min_{A}\left\{\log_2\left(\frac{T_A}{\mathrm{adv}^{\mathrm{Renyi}}(A)}\right)\right\}$ として特徴づけ

- よく使われる優位性 $\mathrm{adv}^{\mathrm{TV}}(A)$ は不十分
- ２つの枠組みで評価される量は「ほぼ」同じ
  - 一般には $\mathrm{adv}^{\mathrm{CS}}(A) \lesssim \mathrm{adv}^{\mathrm{Renyi}}(A)$
  - $\mathrm{adv}^{\mathrm{CS}}(A)$ は $\{0,1,\perp\}$ の出力確率の割当に依存するが，$\mathrm{adv}^{\mathrm{Renyi}}(A)$ は割当に依存しない

一方向性関数（探索問題）のビット安全性

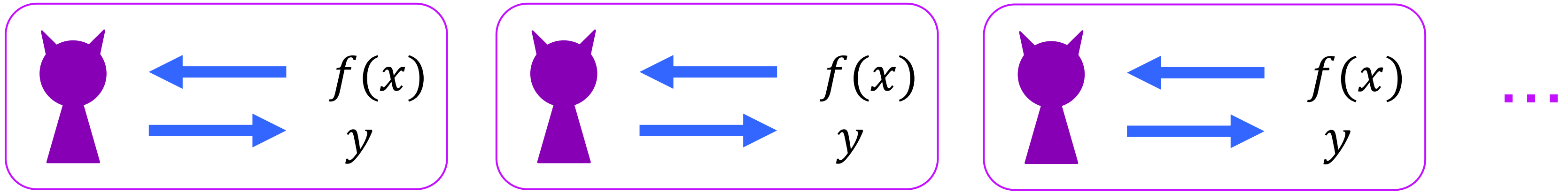
$f:\{0,1\}^n \to \{0,1\}^n$



計算コスト T ・確率 ε で一方向性を破る A が存在

⇒ f のビット安全性 $\leq \log_2\left(\frac{T}{\varepsilon}\right)$

A を N 回実行すると



A が一度でも攻撃に成功する確率は εN 以上

⇒ 総計算コストは $O(N \cdot T) = O\left(\frac{T}{\varepsilon}\right)$ ⇒ ビット安全性 $= \min_A \left\{\log_2\left(\frac{T}{\varepsilon}\right)\right\}$

$\mathrm{adv}^{\mathrm{CS}}(A)$ と $\mathrm{adv}^{\mathrm{Renyi}}(A)$ の関係

定理１： $\mathrm{adv}^{\mathrm{CS}}(A) \leq 8 \cdot \mathrm{adv}^{\mathrm{Renyi}}(A)$

定理２： $\mathrm{adv}^{\mathrm{Renyi}}(A) \leq 1$ のとき，A とコスト同等の A' が存在し，

$$\mathrm{adv}^{\mathrm{CS}}(A') \geq \left(\frac{1}{12}\right) \cdot \mathrm{adv}^{\mathrm{Renyi}}(A)$$

各 A については $\mathrm{adv}^{\mathrm{CS}}(A) \lesssim \mathrm{adv}^{\mathrm{Renyi}}(A)$ であるが，

$$\min_A \left\{\log_2\left(\frac{T}{\mathrm{adv}^{\mathrm{CS}}(A)}\right)\right\} \approx \min_A \left\{\log_2\left(\frac{T}{\mathrm{adv}^{\mathrm{Renyi}}(A)}\right)\right\}$$

[Micciancio, Walter (Eurocrypt 2018)]

- 新しい優位性 $\mathrm{adv}^{\mathrm{MW}}(A) := \dfrac{I(U,Y)}{H(U)}$ を導入し，

  $I(\cdot,\cdot)$: 相互情報量
  $H(\cdot)$: シャノンエントロピー

  ビット安全性を $\min_A \left\{\log_2\left(\frac{T}{\mathrm{adv}^{\mathrm{MW}}(A)}\right)\right\}$ と定義（探索・判定問題で共通）
  - （判定問題のとき）$U \in \{0,1\}$: 秘密，　$Y \in \{0,1,\perp\}$: 攻撃者 A の出力

- 判定問題に対し，　$\mathrm{adv}^{\mathrm{MW}}(A) = \frac{\alpha_A \cdot (2\beta_A - 1)^2}{2\ln 2} + O(\alpha_A \cdot (2\beta_A - 1)^4)$ を証明
  - $\alpha_A = \Pr[Y \neq \perp]$，$\beta_A = \Pr[Y = U \mid Y \neq \perp]$

操作的な意味は不明確

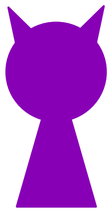
- 条件付き二乗優位性 $\mathrm{adv}^{\mathrm{CS}}(A) := \alpha_A \cdot (2\beta_A - 1)^2$ を用いて

  （判定問題の）ビット安全性を $\min_A \left\{\log_2\left(\frac{T}{\mathrm{adv}^{\mathrm{CS}}(A)}\right)\right\}$ と再定義

線形検査攻撃は脅威なのか？

擬似乱数生成器 (PRG) $g\colon \{0,1\}^n \to \{0,1\}^m$

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

$y \longrightarrow$  $\longrightarrow u'$

任意の関数 g に対し，コスト $O(n)$ の線形検査 L が存在し，

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

ビット安全性を $\min\left\{\log_2\left(\frac{T}{\mathrm{adv}^{\mathrm{TV}}}\right)\right\}$ で定めると，必ず $\frac{n}{2}$ 以下