セキュリティ定量化のための理論的枠組み

安永憲司　東京工業大学

2022.3.18 @ 研究集会「量子暗号理論と耐量子暗号」早稲田大学（オンライン）

目次

- セキュリティの定量化とは？
- WY21 の枠組み
- WY21 からの考察
- まとめ・今後の展望

[WY21] Shun Watanabe, Kenji Yasunaga. Bit Security as Computational Cost for Winning Games with High Probability. Asiacrypt 2021

セキュリティの定量化とは？

セキュリティの定量化とは？

セキュリティ

セキュリティ（英: security）

- 危険や脅威から解放された状態[1]。この抽象的な概念から下のようなさまざまな、より具体的な概念が派生している。

情報セキュリティ

情報セキュリティ（じょうほうセキュリティ、英: information security）とは、情報の機密性、完全性、可用性を維持すること。

ていりょうか —りやうくわ 0 【定量化】

(名)スル

一般には質的にしか表せないと考えられている事物を, 数量で表そうとすること。「香りの—」

Q.セキュリティの定量化は今までしてないの？

A. もちろんしています.

(c) EdDSA で利用される曲線の安全性評価

EdDSA に対する最良の攻撃法である ρ 法は誕生日の逆理に基づく確率的アルゴリズムであるため、付録 3 ではこの攻撃法に基づいて、Curve25519 及び Curve448 における ECDLP を解くにはそれぞれ $2^{125.8257}$ 回と $2^{222.8257}$ 回の楕円加算が必要であると見積もっている。そのためそれぞれの ECDLP はほぼ 128 ビットのセキュリティレベルとほぼ 224 ビットセキュリティレベルを持つとしている。

また、付録 5 では量子アルゴリズムによる脅威に関しても言及されている。これまでの見積もりでは、256 ビット ECDLP を解くためには 2000-3000 量子ビットが必要だと思われ、誤り訂正などを考慮に入れると 600 万量子ビットが必要だと考えられる。近年の量子コンピュータの実装の進展を考えると、今後の発展を注視する必要はあるものの、これから 10 年間 EdDSA を使い続けて問題はないと考える。

「CRYPTREC Report 2020 暗号技術評価委員会報告」17ページ

Q. じゃあ何がしたいの？

A. 情報セキュリティのすべてを定量化したい

素因数分解・離散対数問題・偽造不可能性などの探索問題だけでなく，
判定 Diffie-Hellman (DDH) 仮定や
暗号の秘匿性（選択平文安全性）などの判定問題も定量化したい

複雑に組み合わせた技術・プロトコルのセキュリティも定量化したい

基本的な資源（乱数情報源・（量子）通信路など）の定量化も必要？

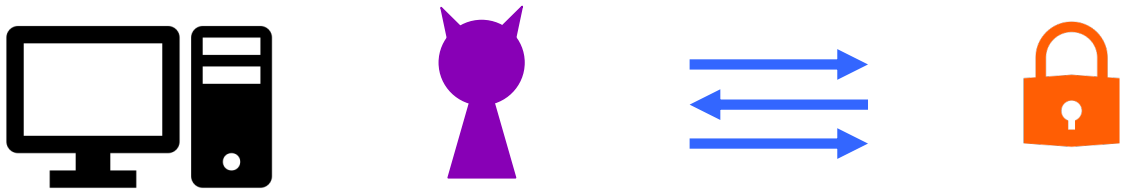
WY21 の枠組み

[WY21] Shun Watanabe, Kenji Yasunaga. Bit Security as Computational Cost for Winning Games with High Probability (Asiacrypt 2021)

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

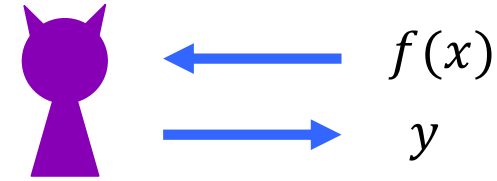


How can we define bit security?

Bit Security of One-Way Function

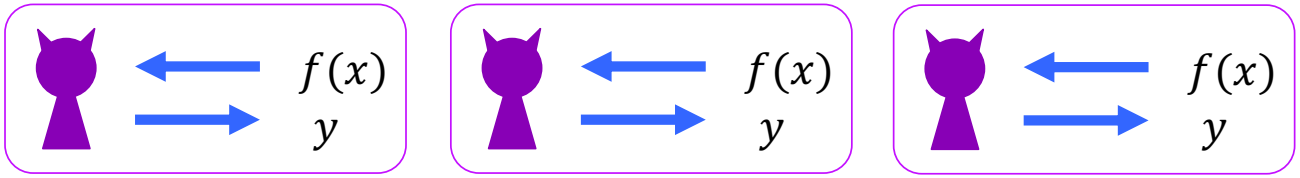
$f : \{0,1\}^n \to \{0,1\}^n$

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



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

What if invoking A in total N times?



Can be extended to other search primitives and assumptions (Signature, Factoring, CDH)

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

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

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)

Characterizing bit security

- Rényi advantage is the right measure for decision games
  - Adversary plays binary hypothesis testing

Bit-security reductions between security games

Implications by Our Work

Bit security is formalized with operational meaning

- Cf. [Micciancio, Walter (Eurocrypt 2018)]

Quantity is defined by the task

Security levels of different primitives can be compared quantitatively

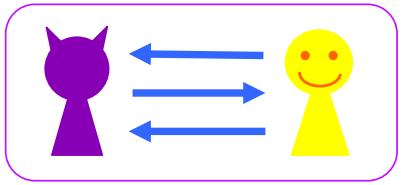
Reduction *tightness* may be reconsidered

- Tight reduction ⇔ No bit-security loss

Our Framework

Two adversaries: inner  and outer 

Inner  plays a "usual" game G



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

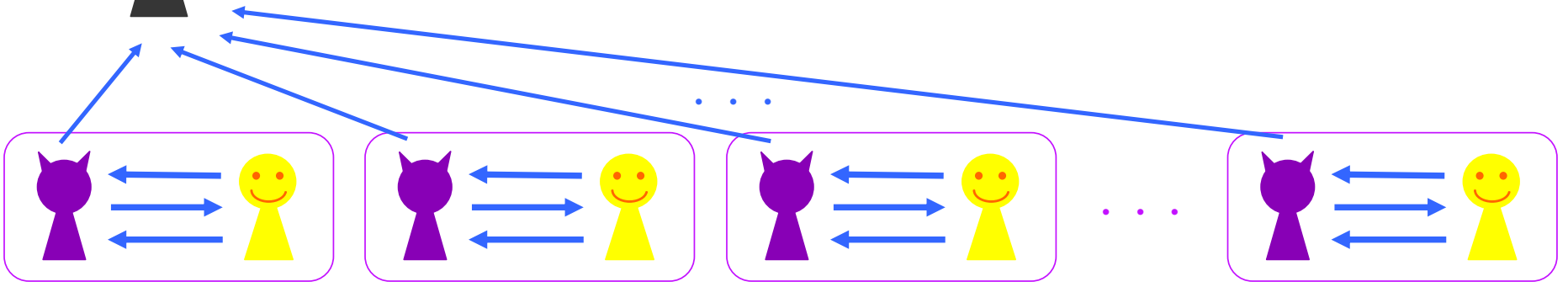
Search game ($n \gg 1$) :

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

Decision game ($n = 1$) :

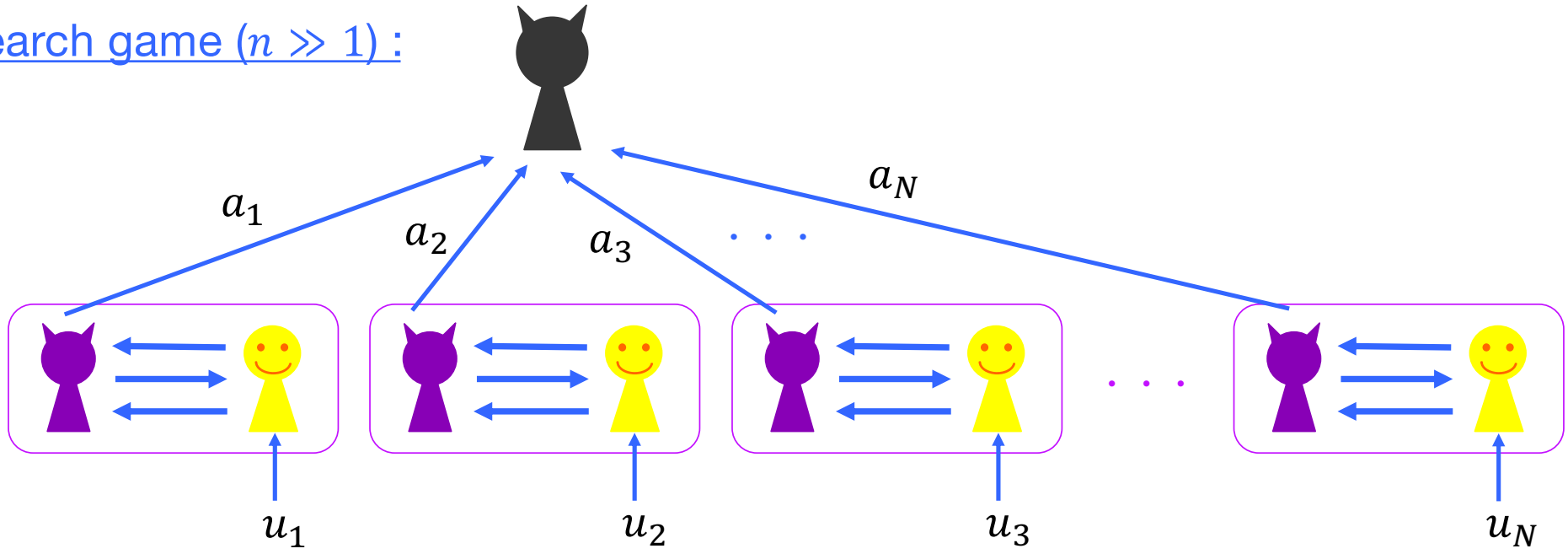
$\Pr[$  wins $G]$
$:= \Pr[$  predicts $u] \approx \frac{1}{2}$

Outer  invokes game G to amplify the "winning probability"

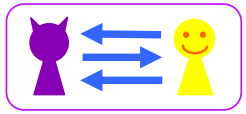


The Winning Condition of 

Search game ($n \gg 1$) :

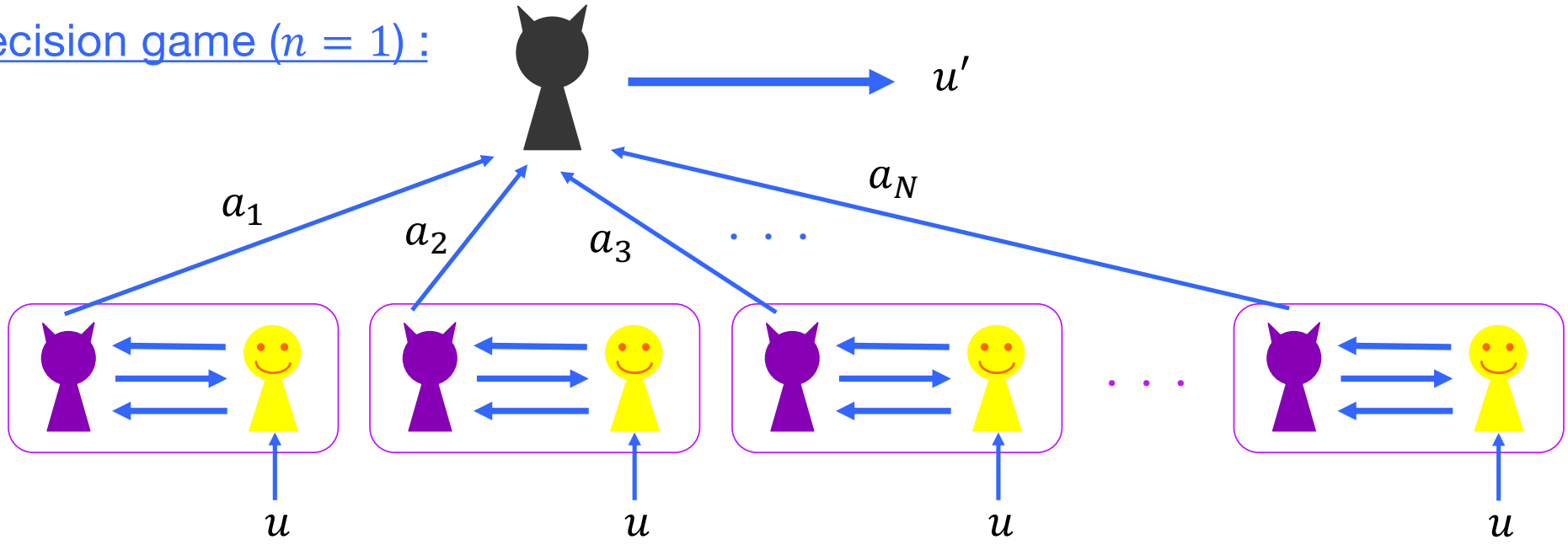


Each  plays an independent game with fresh u_i

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

The Winning Condition of 

Decision game ($n = 1$) :



Each  plays an independent game with consistent u

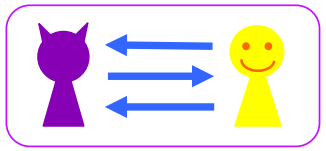
$$\Pr\left[\ \text{wins}\ \right] := \Pr[\ u' = u\ ]$$

Bit Security in Our Framework

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

Error probability, say $\mu = 0.01$

invocations by ⚔

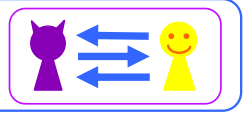
Cost for running 

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 (e.g. OTP encryption)
- For decision games, ⚔ plays binary hypothesis testing

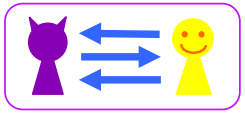
Characterizing Bit Security

Theorem 1: For any security game G,

Cost for running 

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

where

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

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

Rényi divergence of order 1/2

$$D_{1/2}(P\|Q) := -2 \ln \sum_x \sqrt{P(x)Q(x)}$$

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

Proof Overview of Theorem 1 (for Decision Game)

Upper Bound

- Need to show $N \approx \frac{1}{D_{1/2}(A_0 \| A_1)}$ is sufficient to achieve $\Pr\left[\text{  } \text{ predicts } u \right] \geq 0.99$
- By standard technique of Bayesian hypothesis testing, the error probability is bounded by $\mu \leq \frac{1}{2} \exp\left(-\frac{N}{2} D_{1/2}(A_0 \| A_1)\right)$


plays each game independently

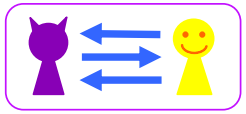
Lower Bound

- It holds that $1 - \Pr\left[\text{  } \text{ predicts } u \right] \geq \frac{1}{2}\left(1 - \mathrm{TV}(A_0, A_1)\right)$
- Also we have $1 - \mathrm{TV}(A_0, A_1) \geq \frac{1}{2} \exp\left(-N D_{1/2}(A_0 \| A_1)\right)$
- Thus it must be $N \gtrsim \frac{1}{D_{1/2}(A_0 \| A_1)}$


plays each game independently

Conventional Advantage vs Rényi Advantage

Decision game (n = 1) :

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

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

Proposition 1: For any decision game,

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

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

$\Pr\left[\right.$ outputs 0 $\left.\right] > \beta$

$\Pr\left[\right.$ outputs 1 $\left.\right] > \beta$

for constant $\beta > 0$

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

PRG against Linear Tests

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

For any g, ∃linear test T s.t.

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

Hybrid arguments:

H_i and H_{i+1} is k-BS IND ➡ H_1 and H_m is $(k - 2\log_2 m)$-BS IND

A Technical Lemma

Lemma 1: Suppose A is an attacker for 1-bit game s.t.

$A_0 = (\delta, 1 - \delta)$, $A_1 = (q\delta, 1 - q\delta)$ for $0 \leq \delta \leq \frac{1}{32}, 0 \leq q \leq \frac{1}{16}$.

Then, $\mathrm{adv}^{\mathrm{Renyi}}(A) := D_{1/2}(A_0 \| A_1) \geq \delta/2$

PRG implies OWF

Theorem 2: k-bit secure PRG g is $(k-\alpha)$-bit secure OWF for $\alpha = \log_2 T_g + O(1)$, where T_g is the cost for evaluating g

Proof:

- Suppose g is NOT $(k-\alpha)$-bit secure OWF
- By Theorem 1, ∃OWF attacker A with cost T and $\mathrm{adv}^{\mathrm{OWF}}(A) \gtrsim T/2^{k-\alpha}$
- PRG attacker A': Given x, runs A(x) = a. Outputs 0 if g(a) = x, and 1 o.w.
  - Complexity of A' is $T' = T + T_g$
- By Lemma 1, $\mathrm{adv}^{\mathrm{PRG}}(A') \gtrsim \Omega\left(T/2^{k-\alpha}\right)$

IND-CPA Encryption implies OW-CPA Encryption

Theorem 3: Let P be an encryption scheme for message space M.
If P is k-bit secure IND-CPA and $|M| \geq 2^{k-\alpha+O(1)}$,
then P is $(k-\alpha)$-bit secure OW-CPA for $\alpha = \log_2(T_{\text{samp}} + T_{\text{eq}}) + O(1)$,
where T_{samp} and T_{eq} are the costs for sampling from M and checking the equality of two messages

Proof:

- Suppose P is NOT $(k-\alpha)$-bit secure OW-CPA
- By Theorem 1, ∃OW-CPA attacker A with cost T and $\text{adv}^{\text{OW-CPA}}(A) \gtrsim T/2^{k-\alpha}$
- IND-CPA attacker A':
  - Choose two challenge messages $m_0, m_1 \in M$ uniformly at random
  - Given challenge ciphertext c, run A(c)
  - If A outputs either m_0 or m_1, output the corresponding bit b'. Otherwise output 1.
  - Complexity of A' is $T' = T + T_{\text{samp}} + T_{\text{eq}}$
- By Lemma 1, $\text{adv}^{\text{IND-CPA}}(A') \gtrsim \Omega\left(T/2^{k-\alpha}\right)$

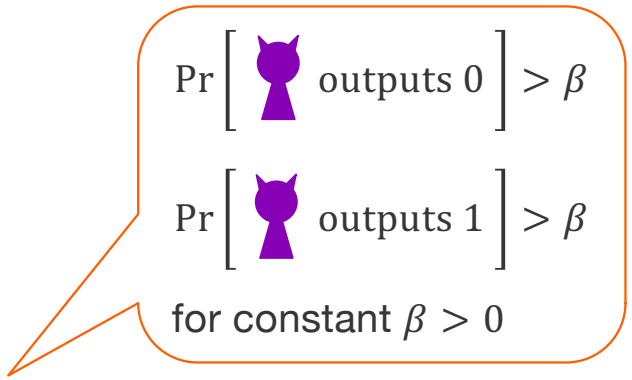
DDH implies CDH

Theorem 4: Let G be a cyclic group of order p.
If the DDH game of G is k-bit secure with $p \geq \max\{2^{k-O(1)}, 64\}$,
then the CDH game of G is $(k-\alpha)$-bit secure for $\alpha = \log_2 T_{\text{eq}} + O(1)$,
where T_{eq} is the cost for checking the equality of two elements in G

Proof:

- Suppose the CDH game of G is NOT $(k-\alpha)$-bit secure
- By Theorem 1, ∃CDH attacker A with cost T and $\text{adv}^{\text{CDH}}(A) \gtrsim T/2^{k-\alpha}$
- DDH attacker A':
  - Given (g^x, g^y, g_u), run $a \leftarrow A(g^x, g^y, g_u)$. Output 0 if $a = g_u$, and 1 o.w.
  - Complexity of A' is $T' = T + T_g$
- By Lemma 1, $\text{adv}^{\text{PRG}}(A') \gtrsim \Omega\left(T/2^{k-\alpha}\right)$

Balanced-Adversary Lemma



Lemma: If a 1-bit game G is not s.t. k-bit secure for balanced adversaries, then ∃balanced adversary A with running time T s.t.

$\Pr[A \text{ wins } G] = \frac{1+\delta}{2}$ for $\delta \gtrsim \sqrt{T/2^k}$

Goldreich-Levin Theorem

Theorem 5: Let $f:\{0,1\}^n \to \{0,1\}^m$ be a k-bit secure OWF.
Define $g:\{0,1\}^{2n} \to \{0,1\}^{n+m}$ as $g(x,r) = (f(x),r)$
Then, $h(x,r) = \sum_i x_i \cdot r_i \bmod 2$ is $(k-\alpha)$-bit secure hard-core predicate for g against balanced adversaries for $\alpha = 2\log_2 n + 3\log_2 k + O(1)$.

Proof:

- Goldreich-Levin theorem:
  For ∀hard-core pred. attacker A with $\Pr[A(g(x,r)) = h(x,r)] > \frac{1+\delta}{2}$ and running time T_A,
  ∃OWF inverter A' s.t. $\Pr[A(g(x,r)) = (x,r)] = \Omega(\delta^2)$ and running time $T_{A'} = O\left(n^2 \left(\log_2\left(\frac{1}{\delta}\right)\right)^3 T_A\right)$
- Suppose that $h(x,r)$ is not $(k-\alpha)$-bit secure HC for balanced adversaries
- By Balanced-Adversary Lemma, ∃balanced HC attacker A with running time T_A
  $\Pr[A(g(x,r)) = h(x,r)] > \frac{1+\delta}{2}$ for $\delta \gtrsim \sqrt{T_A/2^{k-\alpha}}$
- By GL theorem, ∃OWF inverter A' s.t. $\Pr[A(g(x,r)) = (x,r)] = \Omega\left(T_{A'}/2^{k-\alpha}\right)$ → f is not k-BS

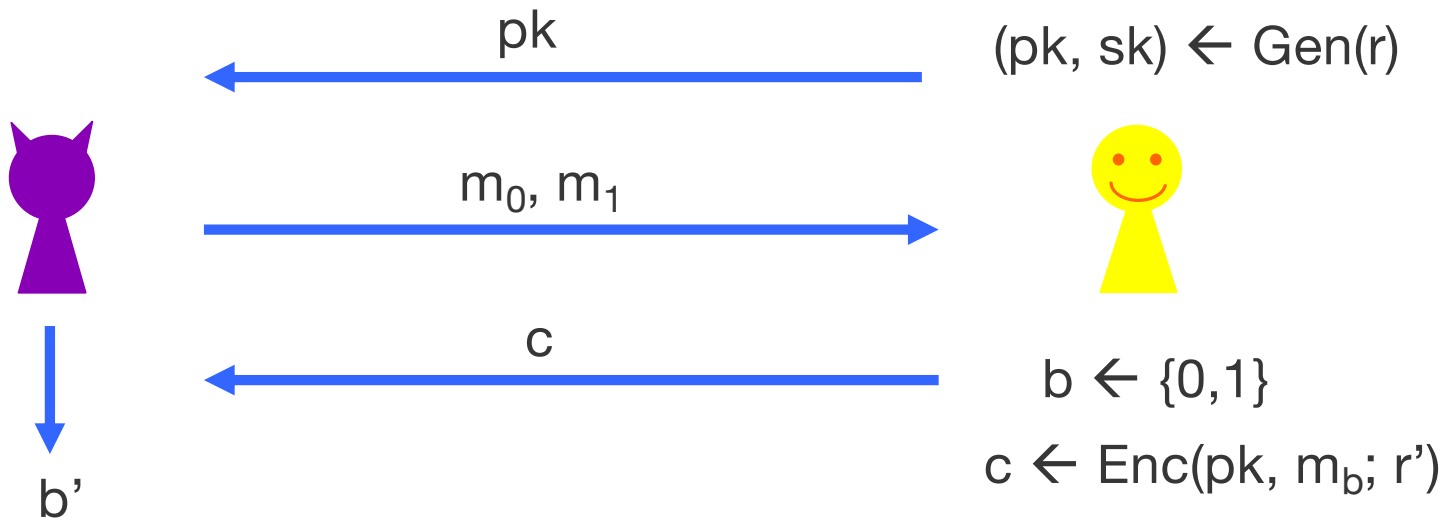
WY21 からの考察

確率分布の近さを測るなら全変動距離よりも Hellinger 距離

（[WY21] の Distribution approximation の結果）

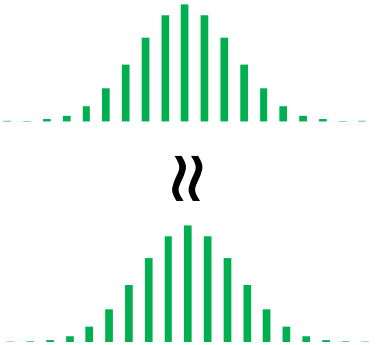
[Y21] Kenji Yasunaga. Replacing Probability Distributions in Security Games via Hellinger Distance. Information-Theoretic Cryptography (ITC) 2021

Security game for PKE



Pr[b' = b] ≈ 1/2

Security game for PKE



pk

(pk, sk) ← Gen(r)

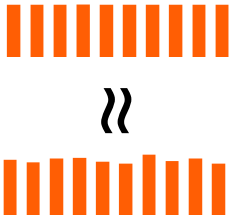
m_0, m_1

c

b ← {0,1}

c ← Enc(pk, m_b; r')

b'

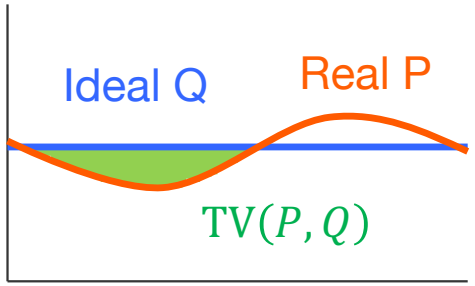


Pr[b' = b] ≈ 1/2

What closeness do we need to preserve the security level?

Total Variation Distance (a.k.a. Statistical Distance)

$$\mathrm{TV}(P,Q) = \frac{1}{2}\sum_x |P(x) - Q(x)|$$



Security Analysis:

(1) Pr[A wins the ideal game G_Q] = ε_Q

(2) TV(P, Q) ≤ δ

➔ Pr[A wins the real game G_P] = $\varepsilon_P \le \varepsilon_Q + \delta$

δ = 2^{-80} is sufficient for 80 bit security ($\varepsilon_P \approx 2^{-80}$)

Results of [WY21] & [Y21]

In Hellinger distance, $\delta = 2^{-40}$ is sufficient for 80 bit security

- Both for search and decision games
- Bit Security framework of [WY21] (as well as [MW18])

Leftover Hash Lemma for Hellinger distance

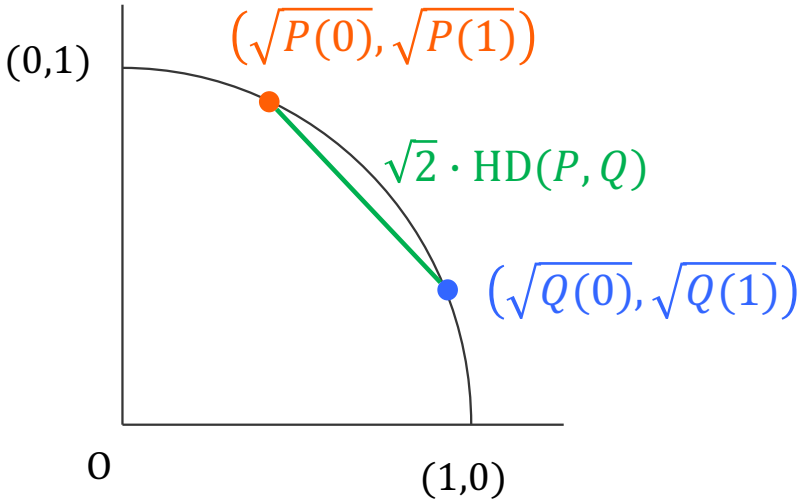
- The same parameters as for TV [Y21]
- Can be shown by LHL for KL divergence [BBCM94] and relation b/w KL & HD

➔ Entropy loss of LHL can be reduced by half with HD-based analysis

[BBCM94] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Ueli M. Maurer: Generalized privacy amplification. IEEE Trans. Inf. Theory 41(6), 1994

Hellinger Distance

$$\mathrm{HD}(P,Q) = \sqrt{\frac{1}{2}\sum_x \left(\sqrt{P(x)} - \sqrt{Q(x)}\right)^2} = \sqrt{1 - \sum_x \sqrt{P(x)\cdot Q(x)}}$$



- $0 \le \mathrm{HD}(P,Q) \le 1$
- $\mathrm{HD}(P,Q)^2 \le \mathrm{TV}(P,Q) \le \sqrt{2}\cdot \mathrm{HD}(P,Q)$
- $D_{1/2}(P\|Q) \approx \mathrm{HD}(P,Q)^2$ for $D_{1/2}(P\|Q) \le \frac{1}{2}$
- $\mathrm{HD}(P,Q)^2 \le \frac{1}{2}\mathrm{KL}(P,Q)$
- Tensorization Property:

  For product dist. $P^\ell = (P,\cdots,P), Q^\ell = (Q,\cdots,Q)$,

  $$\mathrm{HD}\left(P^\ell, Q^\ell\right) \le \sqrt{\ell}\cdot \mathrm{HD}(P,Q)$$

  ➔ $\mathrm{TV}\left(P^\ell, Q^\ell\right) \le \sqrt{2\ell}\cdot \mathrm{HD}(P,Q)$
  - Cf. $\mathrm{TV}\left(P^\ell, Q^\ell\right) \le \ell\cdot \mathrm{TV}(P,Q)$

Theorem 6 (Security for search/decision game):

If G_Q has k-bit security and $\mathrm{HD}(P, Q) \leq 2^{-k/2}$, then G_P has $(k - O(1))$-bit security.

Theorem holds for both search/decision games in the frameworks [MW18] [WY21]

Proofs crucially use Tensorization Property of HD

Proof Overview of Theorem 6 (for Decision Game)

- Suppose G_P is not $(k-\alpha)$-bit secure
- By Theorem 1, ∃A s.t. $\frac{T}{\mathrm{adv}(A)} \lesssim 2^{k-\alpha}$ where $\mathrm{adv}(A) \approx \mathrm{HD}(A_0^P, A_1^P)^2$
- By Tensorization Property, $\mathrm{HD}\left(A_u^P, A_u^Q\right) \leq \sqrt{T} \cdot 2^{-k/2}$
- By Triangle Inequality,

$$\begin{aligned}\mathrm{HD}(A_0^P, A_1^P) &\leq \mathrm{HD}\left(A_0^P, A_0^Q\right) + \mathrm{HD}\left(A_0^Q, A_1^Q\right) + \mathrm{HD}\left(A_1^Q, A_1^P\right) \\ &\leq \mathrm{HD}\left(A_0^Q, A_1^Q\right) + 2\sqrt{T \cdot 2^{-k}}\end{aligned}$$

- Thus, $\mathrm{HD}\left(A_0^Q, A_1^Q\right) \geq \sqrt{T \cdot 2^{-(k-\alpha)}} - 2\sqrt{T \cdot 2^{-k}} \approx \sqrt{T \cdot 2^{-k}}$
- A satisfies $\frac{T}{\mathrm{adv}(A)} = \frac{T}{\mathrm{HD}\left(A_0^Q, A_1^Q\right)^2} \lesssim 2^k$, a contradiction (Q.E.D.)

Leftover Hash Lemma for Hellinger distance

Leftover Hash Lemma [BB85, ILL89] :

Universal hash family $\boldsymbol{H} = \{H: \{0,1\}^n \to \{0,1\}^m\}$ with $|\boldsymbol{H}| = 2^d$ gives a (k, ε)-strong extractor

Ext: $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ for $k - m = 2\log\left(\frac{1}{\varepsilon}\right) - 1$

$\mathrm{TV}\big((Ext(X, U_d), U_d), U_{m+d}\big) \leq \varepsilon$

Entropy Loss

Theorem 7:

Universal hash family gives a (k, ε)-strong Hellinger extractor for $k - m = 2\log\left(\frac{1}{\varepsilon}\right) - 1$

$\mathrm{HD}\big((Ext(X, U_d), U_d), U_{m+d}\big) \leq \varepsilon$

まとめ・今後の展望

まとめ

操作的な意味をもつセキュリティ定量化の枠組み [WY21]

G が k-ビットセキュリティ　⇔　どの攻撃者も G に 99% の確率で勝つには計算コスト 2^k が必要

判定ゲームでは Rényi advantage を使うべき

確率分布の近さを測るには全変動距離ではなく Hellinger 距離

今後の展望

様々な安全性（情報理論的安全性，量子情報）への適用可能

内側・外側攻撃者を使った新しい帰着？（既存は内側だけ）

タイトな帰着 ➔ ビットセキュリティ損失なし帰着

資源（情報源・通信路）のビットセキュリティ？