不完全な乱数と暗号

安永憲司

金沢大学

暗号理論秋学校@河口湖セントビレッヂ 2015.9.14-17

暗号理論と乱数

- 鍵生成には乱数が必要
- CPA 安全な PKE では暗号化に乱数が必要
- 素数性判定は乱数を使うと高速に実行可能
- 対話証明系（零知識証明等）も乱数が必要
- 差分プライバシーは雑音（乱数）が必要

→ 暗号では乱数が本質的に必要
理論では、アルゴリズムは「完全な乱数」が利用できると仮定
→ 乱数が完全でない場合にどうなるか不透明

今回の講義内容

- Yevgeniy Dodis (New York University) の講義 “Randomness in Cryptography, Spring 2013” の講義資料をベース

- 内容
  - 不完全な乱数とは
  - 不完全な乱数による MAC
  - 不完全な乱数による秘匿性技術

不完全な乱数

- 完全な乱数
  = 各ビットが独立かつ一様に選ばれる系列
  - U_n : $\{0,1\}^n$ 上の一様分布

- 不完全さをどう表現するか？ → エントロピー
  - シャノンエントロピー (Shannon entropy)
  - 最小エントロピー (min-entropy)

エントロピー

- 分布 R のシャノンエントロピー H(R)

$$H(R) = \mathop{\mathrm{E}}_{r}\left[\log \frac{1}{p_R(r)}\right] = \sum_{r \in \mathrm{supp}(R)} p_R(r) \log \frac{1}{p_R(r)}$$

  - $p_R(r) := \Pr[\, R = r \,]$
- 分布 R の最小エントロピー $H_\infty(R)$

$$H_\infty(R) = \min_{r \in \mathrm{supp}(R)} \left[\log \frac{1}{p_R(r)}\right] = \log\left(\frac{1}{guess(R)}\right)$$

  - $guess(R) := \max_r(\Pr[\, R = r \,])$
  - $H_\infty(R) \geq k$ のとき R を k-source と呼ぶ

エントロピーの例

- $H(U_n) = H_\infty(U_n) = n$
- 分布 R_1 : $Pr[\ R_1 = r^*\ ] = 1$
  - $H(R_1) = H_\infty(R_1) = 0$
- 分布 R_2 : $S \subseteq \{0,1\}^n$ 上の一様分布
  - $H(R_2) = H_\infty(R_2) = \log |S|$
- 分布 R_3 : r^* だけ 1/2, その他は S 上の一様分布
  $Pr[\ R_3 = r^*\ ] = 1/2,\ \ Pr[\ R_3 = r\ ] = 1/(2|S|)$
  - $H(R_3) = (1/2)\cdot 1 + \sum_{r\in S} 1/(2|S|)\cdot(\log 2|S|)$
    $= 1/2(\ 1 + \log 2|S|\ )$
  - $H_\infty(R_3) = 1$

One-Time Message Authentication Code (MAC)

- Tag : $\{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}^\lambda$ が (R, δ)-secure MAC
  ⇔
  $\forall$ E, $E_{r \leftarrow R}[\ Adv_E(r)\ ] \leq \delta$
  - $Adv_E(G_r) = Pr[$ E wins $G_r\ ]$
  - ゲーム G_r:
    1. x ← E(・)
    2. t = Tag(r, x)
    3. (x', t') ← E(t)
    E wins if x'≠ x ∧ Tag(r, x') = t'
  - $R = U_m$ のときは単に δ-secure

almost XOR-universal (AXU) functions

- $H = \{ h_a: \{0,1\}^n \rightarrow \{0,1\}^\lambda \mid a \in \{0,1\}^p \}$ が
  δ-almost XOR-universal (δ-AXU)
  ⇔
  $\forall x \neq x' \in \{0,1\}^n, y \in \{0,1\}^\lambda$
  $\Pr[h_a(x) \oplus h_a(x') = y] \leq \delta$ （ただし $a \leftarrow U_p$）

  - $\delta = 2^{-\lambda}$ のとき、XOR universal (XU)
  - $y = 0^n$ のとき、δ-almost universal (δ-AU)
  - $\delta = 2^{-\lambda}$ かつ $y = 0^n$ のとき、universal

δ-AXU の構成法

- 構成法 1: $a \in \{0,1\}^{\lambda \times n}$, $h_a(x) = a \cdot x$
  - 鍵長 $p = n\lambda$ の XU
- 構成法 2: $a \in GF(2^n)$, $h_a(x) =$ ($a \cdot x$ の下位 λ bit)
  - 鍵長 $p = n$ の XU
- 構成法 3: $n = \lambda b$, $b \in N$ とする.
  $a = (a_1, \ldots, a_b) \in GF(2^\lambda)^b$, $x = (x_1, \ldots, x_b) \in GF(2^\lambda)^b$,
  $h_a(x) = < a, x > = \Sigma_i a_i x_i$
  - 鍵長 $p = n$ の XU
- 構成法 4: $n = \lambda b$, $b \in N$. $h_a(x) = \Sigma_i a^i \cdot x_i$
  - 鍵長 $p = \lambda$ の ($2^{-\lambda} \cdot n/\lambda$)-AXU

系 $\forall$ n, δ, $\exists$ δ-AXU with $p = \lambda = \log (n/\delta)$

δ-AXU の構成法

定理

構成法 3 ($n = \lambda b$, $b \in N$. $h_a(x) = \langle a,x \rangle = \sum_i a_i x_i$, $a = (a_1, \ldots, a_b) \in GF(2^\lambda)^b$, $x \in GF(2^\lambda)^b$) は鍵長 $p = n$ の XU

証明:

$x \neq x' \in GF(2^\lambda)^b$ と $y \in GF(2^\lambda)$ を固定.

$z = x - x' \neq 0^b$ とする. このとき

$$Pr_a[\, h_a(x) \oplus h_a(x') = y \,] = Pr_a[\, \langle a,x \rangle \oplus \langle a,x' \rangle = y \,]$$
$$= Pr_a[\, \langle a, z \rangle = y \,]$$

この確率が $2^{-\lambda}$であることを示す

$z_1 \neq 0$ だとすると、任意の $a_2, \ldots, a_b$ に対して

$$Pr_{a1}[\, \langle a,z \rangle = y \,] = Pr_{a1}[\, a_1 = c \,] = 2^{-\lambda}$$

ここで $c = (y - \sum_{i \geq 2} a_i z_i) \cdot z_1^{-1} \in GF(2^\lambda)$ □

δ-AXU の構成法

定理

構成法 4 ($n = \lambda b, b \in N. h_a(x) = \sum_i a^i \cdot x_i$) は
鍵長 $p = \lambda$ の ($2^{-\lambda} \cdot n/\lambda$)-AXU

証明:

$x \neq x'$ と y を固定し、$z = x - x' \neq 0^b$ とする
$z_0 = y$ とすると、

$$Pr_a[\, h_a(x) \oplus h_a(x') = y \,] = Pr_a[\, \sum_{i=0}^{b} a^i \cdot z_i = 0 \,]$$

$h_a(x) \oplus h_a(x') = y$ となるのは
多項式 $\phi(s) = \sum z_i \cdot s^i$ が根をもつときだけであり、
$\phi(s)$ は次数 b 以下なので根は $b = n/\lambda$ 個以下 □

AXU による OT-MAC

定理

H : δ-AXU
$r = (a, b) \in \{0,1\}^p \times \{0,1\}^\lambda$ のとき
$Tag(r, x) = h_a(x) \oplus b$ は δ-secure one-time MAC

証明:

G_R: 1. $X \leftarrow E(\cdot)$
2. $(A, B) \leftarrow U_p \times U_\lambda$
$T = Tag_{(A,B)}(X) = h_A(X) \oplus B$
3. $(X', T') \leftarrow E(T)$
4. E wins if $X \neq X' \wedge Tag_{(A,B)}(X') = T'$

証明の続き:

G_R': 1. $X \leftarrow E(\cdot)$

2. $(A, B) \leftarrow U_p \times U_\lambda$

   $T = h_A(X) \oplus B$

3. $(X', T \oplus T') \leftarrow E(T)$

4. E wins if $X \neq X' \wedge h_A(X) \oplus h_A(X') = T \oplus T'$

G_R'': 1. $X \leftarrow E(\cdot)$

2. $T \leftarrow U_\lambda$

3. $(X', T \oplus T') \leftarrow E(T)$

4. $A \leftarrow U_p$

5. E wins if $X \neq X' \wedge h_A(X) \oplus h_A(X') = T \oplus T'$

$\max_E(\mathrm{Adv}_E(G_R)) = \max_E(\mathrm{Adv}_E(G_R') = \max_E(\mathrm{Adv}_E(G_R''))$

であり、δ-AXU より、$\max_E(\mathrm{Adv}_E(G_R'')) \leq \delta$ □

不完全乱数による MAC

- Tag が (k, δ)-secure MAC
  ⇔ ∀ k-source R, Tag が (R, δ)-secure

定理

Tag が鍵長 m の δ-secure MAC のとき、
すべての $k \leq m$ に対し、Tag は $(k, 2^{m-k} \cdot \delta)$-secure MAC

証明: 以下の補題から示せる □

補題

すべての関数 $f : \{0,1\}^m \to \mathbf{R}_{\geq 0}$ と $\{0,1\}^m$ 上の k-source R に対して、$E[f(R)] \leq 2^{m-k} \cdot E[f(U_m)]$

不完全乱数による MAC の証明

補題

すべての関数 $f : \{0,1\}^m \to \mathbf{R}_{\geq 0}$ と $\{0,1\}^m$ 上の k-source R に対して、$E[\, f(R) \,] \leq 2^{m-k} \cdot E[\, f(U_m) \,]$

証明: $\Pr[\, R = r \,] \leq \mathrm{guess}(R)$ であることから

$$
\begin{aligned}
E[\, f(R) \,] &= \sum_r \Pr[R = r] \cdot f(R) \\
&\leq \mathrm{guess}(R) \cdot 2^m \cdot \sum_r 2^{-m} \cdot f(r) \\
&= 2^{m - H_\infty(R)} \cdot E[\, f(U_m) \,]
\end{aligned}
$$

□

MAC の可能性・不可能性結果

定理（不完全乱数による MAC の可能性）

$\forall$ k s.t. m/2 + log n < k ≤ m に対し、
効率的な Tag : $\{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}^\lambda$ が存在し、
Tag は $(k, n \cdot 2^{m/2-k})$-secure MAC with $\lambda = m/2$
別の言い方をすると、
$\forall$ n, δ, m ≥ 2log(n/δ), k s.t. m/2+log(n/δ) < k ≤ m に対し、
効率的な (k,δ)-secure MAC with $\lambda = m/2$ が存在

定理（不完全乱数による MAC の不可能性）

Tag : $\{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}^\lambda$ とする.
$\forall$ k ≤ m に対し、以下の R with $H_\infty(R) \geq k$ と E が存在
(a) k ≤ m/2 ならば $Adv_E(R) = 1$
(b) k > m/2 ならば $Adv_E(R) \geq 2^{m/2-k}$

暗号化方式と統計的距離

- (Enc, Dec) で与えられる
  - Enc : $\{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}^\lambda$
  - Dec : $\{0,1\}^m \times \{0,1\}^\lambda \rightarrow \{0,1\}^n$
    - Enc(r,・) と Dec(r,・) は、$\mathrm{Enc}_r(\cdot)$ と $\mathrm{Dec}_r(\cdot)$ で表す
  - 正当性 : $\forall$ r, x, $\mathrm{Dec}_r(\mathrm{Enc}_r(x)) = x$
- 統計的距離 (statistical distance)
  - $\mathrm{SD}(A, B) = \max_E | \Pr[E(A) = 1] - \Pr[E(B) = 1] |$
    $= 1/2 \sum_r |\Pr[A = r] - \Pr[B = r] |$
- 統計的独立性 (statistical independence)
  - SI(A, B) = SD((A,B), A×B)

暗号化方式の安全性

- (Enc, Dec) が (R, ε)-secure
  ⇔ $SI(X; C) \leq \varepsilon$, $C = Enc_R(X)$
- (Enc, Dec) が (k, ε)-secure
  ⇔ ∀ k-source R, (Enc, Dec) が (R, ε)-secure

定理

One-Time Pad は (m,0)-secure

→ 一様分布が手に入れば十分

乱数抽出

- 不完全乱数から一様乱数を求める手続き
- Ext : $\{0,1\}^m \to \{0,1\}$ が (k, ε)-bit-extractor
  $\Leftrightarrow \forall$ k-source R on $\{0,1\}^m$, $SD(Ext(R), U_1) \leq \varepsilon$

定理

$(m - 1, 0.99)$-bit-extractor は存在しない

証明:

bit-extractor Ext に対し、
$S_0 = Ext^{-1}(0)$, $S_1 = Ext^{-1}(1)$ とする. $|S_0| \geq |S_1|$ と仮定.
このとき、$H_\infty(S_0) \geq m - 1$ だが、$Ext(S_0) = 0$ である □

不完全乱数による秘匿性

補題

2つの関数 $f, g : \{0,1\}^m \to C$ および $0 \le t \le m$ に対し

$\Pr_{r \leftarrow U}[\, f(r) \neq g(r) \,] \ge 2^{-t}$

であるとき、以下の R_1 と R_2 が存在する

(a) $H_\infty(R_1) \ge m-t-1$ かつ $SD(\, f(R_1), g(R_1) \,) \ge 1/2$

(b) $H_\infty(R_2) \ge m-t-2$ かつ $SD(\, f(R_2), g(R_2) \,) \ge 1$ (??)

証明: アイディア: 値が異なる部分からサンプルした分布

まず $C = \{0,1\}$ の場合を証明する.

$D = \{\, z : f(z) \neq g(z) \,\}$ とすると $|D| \ge 2^{m-t}$

$S_{01} = \{\, z : f(z)=0, g(z)=1 \,\}$, $S_{10} = \{\, z : f(z)=1, g(z)=0 \,\}$

$|S_{01}| \ge |S_{10}|$ と仮定すると $|S_{01}| \ge |D|/2 \ge 2^{m-t-1}$

$R_1 = U_{S01}$ とすれば $H_\infty(R_1) \ge m-t-1$ であり

$SD(\, f(R_1), g(R_1) \,) = 1$ となり (a), (b) が示せた

アイディア: ハッシュで潰して
C = {0,1} の場合に帰着

証明の続き（その１）：

universal hash H = { h : C → {0,1} }

(∀ z ≠ z', $\Pr_{h \leftarrow H}$[h(z) ≠ h(z')] = 1/2)

$S_{\alpha,\beta}$ (h) = { r ∈ D | h(f(r)) = α ∧ h(g(r)) = β }

今計算したい値は、

$$E_{h\in H}\left[\left|S_{01}(h)\right|+\left|S_{10}(h)\right|\right]=E_{h\in H}\left[\sum_{r\in D}X_{S_{01}(h)\cup S_{10}(h)}(r)\right]$$

$$=\sum_{r\in D}\Pr_{h\in H}\left[r\in S_{01}(h)\cup S_{10}(h)\right]=\sum_{r\in D}\Pr\left[h(f(r))\neq h(g(r))\right]\geq\frac{D}{2}$$

ただし、$X_A(r)$:= 1 if r ∈ A, 0 o.w.

このとき、ある h* : C → {0,1} が存在して、

$|S_{01}(h^*) \cup S_{10}(h^*)| \geq |D|/2 \geq 2^{m-t-1}$

$|S_{01}(h^*)| \geq |S_{10}(h^*)|$ と仮定すると、$|S_{01}(h^*)| \geq 2^{m-t-2}$

証明の続き（その２）：

$R_2 : S_{01}(h^*)$ 上の一様分布. $H_\infty(R_2) \geq m\text{-}t\text{-}2$ であり、

$h^*(f(R_2)) = 0$, $h^*(f(R_2)) = 1$ から $SD(f(R_2), g(R_2)) = 1$

→ (b) が示された

$R_1 : S_{01}(h^*) \cup S_{10}(h^*)$ 上の一様分布

$H_\infty(R_1) \geq m\text{-}t\text{-}1$ であり、

$Eve(C) = 1 \Leftrightarrow h^*(C) = 0$ である Eve を考えると、

$$
\begin{aligned}
& SD(f(R_1), g(R_1)) \\
& \geq \Pr[Eve(f(R_1)) = 1] - \Pr[Eve(g(R_1)) = 1] \\
& = \Pr[h^*(f(R_1)) = 0] - \Pr[h^*(g(R_1)) = 0] \\
& \geq \Pr[R_1 \in S_{01}] - \Pr[R_1 \in S_{10}] \\
& = \Pr[R_1 \in S_{01}] - (1 - \Pr[R_1 \in S_{01}]) \\
& \geq 2\Pr[R_1 \in S_{01}] - 1 \geq 1/2 \quad (??)
\end{aligned}
$$

不完全乱数による暗号化方式

定理

n = 1 のとき、(m-1, 1/2)-secure または (m-2,0)-secure 暗号化方式は存在しない

証明:

$f(r) = Enc_r(0)$, $g(r) = Enc_r(1)$ とする.

暗号化方式の正当性より、 $\forall r, Enc_r(0) \neq Enc_r(1)$

t=0 で補題を適用すると、R_1, R_2 が存在して、

$SD(Enc_{R1}(0), Enc_{R1}(1)) \geq 1/2$

$SD(Enc_{R2}(0), Enc_{R2}(1)) = 1$

$H_\infty(R_1) \geq m-1$, $H_\infty(R_2) \geq m-2$ □

不完全乱数によるコミットメント

- Com : $\{0,1\} \times \{0,1\}^m \rightarrow \{0,1\}^\lambda$ が
  (k,ε)-secure コミットメント
  ⇔
  - Hiding:
    ∀k-source R, SD(Com(0,R), Com(1,R)) ≤ ε
  - (weak) Binding:
    $\Pr_{r \leftarrow U}[\ \mathrm{Com}(0,R) \neq \mathrm{Com}(1,R)\ ] \geq 1/2$

- 不可能性:
  f(r) = Com(0,r), g(r) = Com(1,r) とすると、
  (m-1, 0.99)-secure コミットメントは存在しない

不完全乱数による秘密分散

- (Share, Rec) が (k, ε)-secure (2,T)-秘密分散
  ⇔
  $S_1 = \mathrm{Share}_1(b;r), \ldots, S_T = \mathrm{Share}_T(b,r)$ のとき
  - $\mathrm{Rec}(S_1, \ldots, S_T) = b$
  - $\forall$ k-source R, $i \in [T]$,
    $\mathrm{SD}(\mathrm{Share}_i(0,R), \mathrm{Share}_i(1,R)) \leq \varepsilon$

不完全乱数による秘密分散

定理

(m – log(T) – 1, 0.99)-secure または (m – log(T) – 2, 1/2)-secure (2,T)-秘密分散は存在しない

証明:

すべての r について

$(\mathrm{Share}_1(0,r), \ldots, \mathrm{Share}_T(0,r)) \neq (\mathrm{Share}_1(1,r), \ldots, \mathrm{Share}_T(1,r))$

→ ある $j \in [T]$ が存在して $\mathrm{Share}_j(0,r) \neq \mathrm{Share}_j(1,r)$

→ ある $j^* \in [T]$ が存在して

$|\{ r : \mathrm{Share}_{j^*}(0,r) \neq \mathrm{Share}_{j^*}(1,r) \}| \geq 2^m/T$

$f(r) = \mathrm{Share}_{j^*}(0,r)$, $g(r) = \mathrm{Share}_{j^*}(1,r)$ とすると

$\Pr[f(r) \neq g(r)] \geq 1/T$ であり、あとは補題より　□

不可能性の回避策

- 不完全乱数による秘匿性を回避するには？
  - k-source よりも構造をもつ情報源
  - 正当性を緩和
  - 完全乱数 (乱数の抽出可能性) が本質的に必要
  - 公開乱数を利用

ブロック情報源 (block sources)

- 系列 $R_1, R_2, \ldots$ が (k,m)-block source
  $\Leftrightarrow \forall i, |R_i| = m$ であり、
  $\forall i, \forall r_1, \ldots, r_{i-1} \in \{0,1\}^m$,
  $H_\infty(R_i \mid R_1 = r_1, \ldots, R_{i-1} = r_{i-1}) \geq k$
  - m : ブロック長, k/m : エントロピーレート

- 系列 $R_1, R_2, \ldots$ が (k,m)-enhanced block source
  $\Leftrightarrow \forall i, |R_i| = m$ であり、
  $\forall i, \forall I \subseteq [r]$ s.t. $i \notin I$, $\forall r_I = (r_i)_{i \in I} \in \{0,1\}^{m \times |I|}$,
  $H_\infty(R_i \mid R_I = r_I) \geq k$

Santha-Vazirani 情報源

- m = 1 のブロック情報源
- SV(γ)

  $= \{ B_1B_2\ldots \mid \forall\, i\ \forall\, b_1, \ldots, b_{i-1} \in \{0,1\}^{i-1} :$
  $\Pr[\, B_i=0 \mid B_1=b_1, \ldots, B_{i-1}=b_{i-1} \,] \in ((1-\gamma)/2, (1+\gamma)/2) \}$

  $= \{ B_1B_2\ldots \mid \forall\, i\ \forall\, b_1, \ldots, b_{i-1} \in \{0,1\}^{i-1} :$
  $\mathrm{Bias}(B_i \mid B_{\{1,\ldots,i-1\}} = b_{\{1,\ldots,i-1\}}) \le \gamma \}$

  - エントロピーレートは $\log(2/(1+\gamma))$

- eSV(γ, N)

  $= \{ B_1\ldots B_N \mid \forall i\ \forall b_{[N]\setminus\{i\}} : \mathrm{Bias}(B_i \mid B_{[N]\setminus\{i\}} = b_{[N]\setminus\{i\}}) \le \gamma \}$

semi-flat 情報源

- γ-semi-flat source $H_S(\gamma, N)$ ($S \subseteq \{0,1\}^N$, $|S| = 2^{N-1}$)
  - $H_S(\gamma, N) = \begin{cases} \Pr[R = r] = (1+\gamma)\, 2^{-N} & \text{if } r \in S \\ \Pr[R = r] = (1-\gamma)\, 2^{-N} & \text{if } r \notin S \end{cases}$
  - γ-biased コインで S or $\bar{S}$ を選択し、その後、選んだ集合で一様に選択
  - $H(\gamma, N) = \{ H_S(\gamma, N) \mid S \subseteq \{0,1\}^N, |S| = 2^{N-1} \}$

補題 $H(\gamma, N) \subset eSV(\gamma, N)$

証明: $\forall\, b_i \in \{0,1\}, b_{-i} \in \{0,1\}^{N-1}$, $H_S(\gamma, N) = (B_i, B_{-i})$

$$\frac{\alpha}{\beta} = \frac{\Pr[B_i = 0 \mid B_{-i} = b_{-i}]}{\Pr[B_i = 1 \mid B_{-i} = b_{-i}]} = \frac{\Pr[(B_i, B_{-i}) = (0, b_{-i})]}{\Pr[(B_i, B_{-i}) = (1, b_{-i})]} \in \left[\frac{1-\gamma}{1+\gamma}, \frac{1+\gamma}{1-\gamma} \right]$$

α + β = 1 であり α, β ∈ [(1-γ)/2, (1+γ)/2] □

SV 情報源による乱数抽出の不可能性

定理

$\forall N \forall Ext : \{0,1\}^N \rightarrow \{0,1\}, \exists \gamma\text{-semi-flat 情報源}$
$R \in H(\gamma, N) \subset eSV(\gamma, N)$ s.t. $Bias(Ext(R)) \geq \gamma$

証明:

一般性を失うことなく、$|Ext^{-1}(0)| \geq |Ext^{-1}(1)|$ と仮定.
$\forall S \subseteq Ext^{-1}(0), |S| = 2^{N-1}$ に対して $R = H_S(\gamma, N)$ とすると

$$Pr[Ext(R) = 1] \geq Pr[R \in S] = (1+\gamma)/2 \quad \square$$

SV 情報源による秘匿性の不可能性

補題

関数 $f, g : \{0,1\}^N \to C$ が、ある $T \geq 1$ に対して
$\Pr_{r \leftarrow U}[f(r) \neq g(r)] \geq 1/T$ であるとき、
ある $S \subseteq \{0,1\}^N$, $|S| = 2^{N-1}$ が存在し、
$R = H_S(\gamma, N)$ とすると、$SD(f(R), g(R)) \geq \gamma/2T$

証明:

$D = \{ z : f(z) \neq g(z) \}$ とすると $|D| \geq 2^N/T$
universal hash $H = \{ h : C \to \{0,1\} \}$ を考えると、
$(\forall z \neq z', \Pr_{h \leftarrow H}[h(z) \neq h(z')] = 1/2)$
以前の補題と同様に、ある $h^* : C \to \{0,1\}$ が存在して、
$|S_{01}(h^*) \cup S_{10}(h^*)| \geq |D|/2 \geq 2^N/2T$
$|S_{01}(h^*)| \geq |S_{10}(h^*)|$ と仮定すると、$|S_{01}(h^*)| \geq 2^N/4T$

証明の続き:

集合 $S \subseteq \{0,1\}^N$: $S_{01}(h^*)$ を含み、$S_{10}(h^*)$ を含まない
$|S| = 2^{N-1}$ である任意の集合

分布 $R = H_S(\gamma, N)$ とする

Eve(C) = 1 $\Leftrightarrow$ $h^*(C) = 0$ である Eve を考えると

SD(f(R), g(R))

$\geq | \Pr[h^*(f(R)) = 0] - \Pr[h^*(g(R)) = 1] |$

$= \Pr[h^*(f(R)) = 0] - \Pr[h^*(g(R)) = 0]$

$\geq \Pr[R \in S_{01}] - \Pr[R \in S_{10}]$

$= (1+\gamma)2^{-N} |S_{01}| - (1-\gamma)2^{-N} |S_{10}|$

$= 2^{-N} (|S_{01}| - |S_{10}| + \gamma (|S_{01}| + |S_{10}|))$

$\geq 2^{-N} \cdot \gamma|D|/2 \geq \gamma / 2T$ □

まとめ

- MAC は k-source を使って安全性を保証できる
- 秘匿性に関する技術（暗号方式、秘密分散等）は k-source では安全の保証が難しい
  - 方式に対して安全性を破る分布が存在
  - Santha-Varizani 情報源に制限してもダメ
  - 乱数抽出可能なことが本質的