応用数学６ 2010 年 11 月 17 日

擬似ランダムネス

講師: 安永憲司

前回までは，公開鍵暗号を達成するために必要な性質を考え，その性質をもつ関数として，OWF, OWP, TDP を考えた．

公開鍵暗号において，盗聴を行なう敵は計算能力が制限された PPT アルゴリズムだと考える．それでは，PPT アルゴリズムに対して安全な暗号とはどのように定式化すればよいのか．ここでは安全性を定式化するために必要な概念である擬似ランダムネスについて考える．

1 擬似ランダムネス

秘密鍵暗号方式において完全秘匿性を達成する暗号として，使い捨て鍵暗号があった．鍵 k とメッセージ m に対して，暗号文は $\mathsf{Enc}_k(m) = m \oplus k$ である．鍵 k が一様ランダムに選ばれていることが安全性の根拠である．Shannon の定理より，鍵長はメッセージ長より短くすることができない．しかし，Shannon の定理は，敵の計算能力が十分大きいことを想定した議論であった．つまり，敵の計算能力を制限すると，Shannon の定理は当てはまらない．

そこで一つの方法として，計算能力が制限された敵にとってランダムに見える，**擬似ランダム**な系列を作ることができれば，効率的な使い捨て鍵暗号ができそうである．つまり，ランダムに見える鍵 $k' = g(k)$ を，一様ランダム系列の代わりに使うのである．

それでは，PPT アルゴリズムにとってランダムに見える擬似ランダムな系列とは，どのように定義すればよいだろうか．

- 0 と 1 が出てくる割合がほぼ等しい．
- 00 と 11 が出てくる割合がほぼ等しい．
- ある特定のビット位置において，0 と 1 が出てくる割合がほぼ等しい．
- 系列の最初の部分が与えられて，次に出てくるビットを予測するのが難しい．
- 系列の最初の部分が与えられて，次に出てくる系列を予測するのが難しい．

ここであげたものは，統計的検定のいくつかの例である．ある種のシミュレーションを行なう場合は，ある特定の検定をパスする系列であれば，一様乱数の代わりとして十分な場合がある．しかし，暗号理論においては，（効率的に実行可能な）どのような検定をもパスする系列が必要となってくる．

2 計算量的識別不能性

計算量的識別不能性 (computationally indistinguishability) という概念を導入する．

定義 1 各 $n \in \mathbb{N}$ に対して，X_n が確率分布であるとき，系列 $\{X_n\}_{n\in\mathbb{N}}$ を確率分布アンサンブルと呼ぶ．

定義 2 (計算量的識別不能性) 多項式 $\ell(\cdot)$ に対して，$\{0,1\}^{\ell(n)}$ 上の確率分布アンサンブル $\{X_n\}_n, \{Y_n\}_n$ を考える．確率分布 $\{X_n\}_n$ と $\{Y_n\}_n$ が計算量的に識別不能であるとは，任意の PPT アルゴリズム D（識別者と呼ぶ）に対して，無視できる関数 $\epsilon(\cdot)$ が存在して，すべての $n \in \mathbb{N}$ に対して，

$$|\Pr[D(t) = 1 \mid t \leftarrow X_n] - \Pr[D(t) = 1 \mid t \leftarrow Y_n]| < \epsilon(n)$$

を満たすときである．このとき，$\{X_n\}_n \approx_c \{Y_n\}_n$ と表す．

つまり，PPT アルゴリズムでは無視できる確率でしか区別をすることができないとき，計算量的に識別ができないという．また，D が確率分布 X_n と Y_n を確率 ϵ で識別できるとは，無限に多くの $n \in \mathbb{N}$ に対して，

$$|\Pr[D(t) = 1 \mid t \leftarrow X_n] - \Pr[D(t) = 1 \mid t \leftarrow Y_n]| > \epsilon$$

を満たすときである．

2.1 計算量的識別不能性に関する性質

2.1.1 効率的演算に対する閉包性

もし二つの分布が識別できないとき，それらの分布にどのような効率的な演算を加えても，識別することはできない．

補題 3 多項式 $\ell(\cdot)$ に対して，$\{0,1\}^{\ell(n)}$ 上の確率分布アンサンブル $\{X_n\}_n, \{Y_n\}_n$ を考える．このとき，任意の PPT アルゴリズム M に対して，もし $\{X_n\}_n \approx_c \{Y_n\}_n$ であれば，$\{M(X_n)\}_n \approx_c \{M(Y_n)\}_n$ である．

証明: 分布 $\{M(X_n)\}_n$ と $\{M(Y_n)\}_n$ を無視できない確率 $\mu(n)$ で識別する PPT アルゴリズム D が存在したと仮定する．つまり，

$$|\Pr[D(t) = 1 \mid t \leftarrow M(X_n)] - \Pr[D(t) = 1 \mid t \leftarrow M(Y_n)]| > \mu(n)$$

である．このとき，

$$|\Pr[D(M(t)) = 1 \mid t \leftarrow X_n] - \Pr[D(M(t)) = 1 \mid t \leftarrow Y_n]| > \mu(n)$$

であることがわかる．つまり，PPT アルゴリズム $D'(\cdot) = D(M(\cdot))$ は，$\{X_n\}_n$ と $\{Y_n\}_n$ を確率 $\mu(n)$ で識別している．これは，$\{X_n\}_n \approx_c \{Y_n\}_n$ という仮定に反する． □

2.1.2 推移律

次に，推移律が成り立つことを示す．つまり，$\{A_n\}_n \approx_c \{B_n\}_n$ かつ $\{B_n\}_n \approx_c \{C_n\}_n$ であれば，$\{A_n\}_n \approx_c \{C_n\}_n$ である．ここでは，一般化した補題を示す．

補題 4 (ハイブリッド補題) 確率分布の系列 $X^1, X^2, \ldots, X^m$ を考える．ただし，m は n の多項式サイズである．PPT アルゴリズム D が X^1 と X^m を確率 ϵ で識別できたとする．このとき，ある $i \in \{1, 2, \ldots, m-1\}$ が存在して，D は X^i と X^{i+1} を確率 $\frac{\epsilon}{m}$ で識別できる．

証明: D が X^1 と X^m を確率 ϵ で識別できると仮定する．つまり，

$$|\Pr[D(t) = 1 \mid t \leftarrow X^1] - \Pr[D(t) = 1 \mid t \leftarrow X^m]| > \epsilon$$

そして，$g_i = \Pr[D(t) = 1 \mid t \leftarrow X^i]$ とおく．つまり，$|g_1 - g_m| > \epsilon$ である．このとき，

$$\begin{aligned} &|g_1 - g_2| + |g_2 - g_3| + \cdots + |g_{m-1} - g_m| \\ &\quad \geq |g_1 - g_2 + g_2 - g_3 + \cdots + g_{m-1} - g_m| \\ &\quad = |g_1 - g_m| > \epsilon \end{aligned}$$

である．したがって，ある i が存在して，$|g_i - g_{i+1}| > \frac{\epsilon}{m}$. □

上記の補題より，すべての $i \in \{1, 2, \ldots, m-1\}$ について $X^i \approx_c X^{i+1}$ であれば，$X^1 \approx_c X^m$ であることがわかる．

2.1.3 識別者と予測者

計算量的識別不能性は，効率的な識別者では，無視できる確率でしか二つの分布を識別することができないことを保証している．このことから，分布からのサンプルが与えられたとき，それがどちらの分布からのサンプルであるかを予測することは，無視できる関数 $\epsilon(\cdot)$ に対して，$1/2+\epsilon(n)$ の確率でしかできない．以下の補題では，その逆も成り立つことを示している．つまり，サンプルがどちらの分布のものであるかを予測できないならば，その二つの分布は識別できないのである．

補題 5 (予測補題) 多項式 $\ell(\cdot)$ に対して，$\{0,1\}^{\ell(n)}$ 上の確率分布アンサンブル $\{X_n^0\}_n, \{X_n^1\}_n$ を考える．PPT アルゴリズム D を，無限に多くの $n\in\mathbb{N}$ に対して，$\{X_n^0\}_n$ と $\{X_n^1\}_n$ とを確率 $\mu(\cdot)$ で識別する識別者だとする．このとき，PPT アルゴリズム A が存在して，無限に多くの $n\in\mathbb{N}$ に対して，

$$\Pr[A(t)=b \mid b \xleftarrow{R} \{0,1\}, t \leftarrow X_n^b] \geq \frac{1}{2}+\frac{\mu(n)}{2}.$$

証明: 無限に多くの $n\in\mathbb{N}$ に対して，PPT アルゴリズム D が $\{X_n^0\}_n$ と $\{X_n^1\}_n$ とを確率 $\mu(\cdot)$ で識別できると仮定する．一般性を失うことなく，D は $\{X_n^0\}_n$ からのサンプルよりも $\{X_n^1\}_n$ からのサンプルのときに，1 を出力する確率が高いと仮定する．つまり，

$$\Pr[D(t)=1 \mid t \leftarrow X_n^1] - \Pr[D(t)=1 \mid t \leftarrow X_n^0] > \mu(n).$$

この議論が一般性を失わない理由は，$D'(\cdot)=1-D(\cdot)$ という PPT アルゴリズム D' を考えると，D と D' の少なくとも一方は，無限に多くの n に対して識別できているからである．

このとき，識別者 D は，どちらの分布であるかを予測することもできる．

$$\begin{aligned}
&\Pr[D(t)=b \mid b \xleftarrow{R} \{0,1\}, t \leftarrow X_n^b] \\
&= \frac{1}{2}\Pr[D(t)=1 \mid t \leftarrow X_n^1] + \frac{1}{2}\Pr[D(t)\neq 1 \mid t \leftarrow X_n^0] \\
&= \frac{1}{2}\Pr[D(t)=1 \mid t \leftarrow X_n^1] + \frac{1}{2}\left(1-\Pr[D(t)=1 \mid t \leftarrow X_n^0]\right) \\
&= \frac{1}{2}+\frac{1}{2}\left(\Pr[D(t)=1 \mid t \leftarrow X_n^1] - \Pr[D(t)=1 \mid t \leftarrow X_n^0]\right) \\
&\geq \frac{1}{2}+\frac{\mu(n)}{2}.
\end{aligned}$$

□

3 擬似ランダム分布

$\{0,1\}^n$ 上の一様分布を U_n と表す．一様分布と識別ができない分布のことを擬似ランダム分布と呼ぶ．

定義 6 (擬似ランダム分布アンサンブル) ある多項式 $\ell(\cdot)$ に対して，$\{0,1\}^{\ell(n)}$ 上の確率分布アンサンブル $\{X_n\}_n$ を考える．$\{X_n\}_n \approx_c \{U_{\ell(n)}\}_n$ であるとき，$\{X_n\}_n$ は擬似ランダムであるという．

擬似ランダム分布は，一様分布と比べたときに，すべての効率的な統計的検定をパスしなければならない．すべての効率的な検定をパスするという性質を満たすことやそれを証明することは難しいように見える．しかし，完全性をもつ統計的検定が知られている．つまり，その検定さえパスすれば，すべての統計的検定をパスすることができるのである．

完全性をもつ統計的検定: 次ビット予測検定

次ビット予測検定 (next-bit predictability test) とは，分布からサンプルした系列の任意の接頭辞が与えられたとき，その次のビットを予測できるかどうかを調べる検定である．予測できる確率が 1/2 程度で抑えられるとき，次ビット予測検定をパスしたという．

定義 7 多項式 $\ell(\cdot)$ に対して，$\{0,1\}^{\ell(n)}$ 上の確率分布アンサンブル $\{X_n\}_n$ を考える．この確率分布が**次ビット予測検定**をパスするとは，すべての PPT アルゴリズム A に対して，無視できる関数 $\epsilon(\cdot)$ が存在し，すべての $n \in \mathbb{N}, i \in \{0,1,\ldots,\ell(n)\}$ に対して，

$$\Pr[A(1^n, t_1 t_2 \cdots t_i) = t_{i+1} \mid t \leftarrow X_n] < \frac{1}{2} + \epsilon(n)$$

が成り立つときである．ただし，t_i は t の i ビット目を表している．

定理 8 (次ビット予測検定の完全性) 確率分布アンサンブル $\{X_n\}_n$ が次ビット予測検定をパスするとき，$\{X_n\}_n$ は擬似ランダムである．

証明: 証明の方針としては，$\{X_n\}_n$ と一様分布を区別することができる PPT アルゴリズムが存在したと仮定すると，$\{X_n\}_n$ は次ビット予測検定をパスすることができないことを示す．

PPT 識別者 D と多項式 $p(\cdot)$ が存在して，D は，無限に多くの $n \in \mathbb{N}$ について，X_n と $U_{\ell(n)}$ を確率 $\frac{1}{p(n)}$ で識別できると仮定する．以下で定義される**ハイブリッド分布**を考える．

$$H_n^i = \{x_0 x_1 \cdots x_i u_{i+1} \cdots u_{\ell(n)} \mid x \leftarrow X_n, u \leftarrow U_{\ell(n)}\}.$$

つまり，H_n^i は，最初の i ビットが X_n のサンプルの最初の i ビットであり，残りの $\ell(n) - i$ ビットが $U_{\ell(n)}$ からのサンプルの最後の $\ell(n) - i$ ビットである．したがって，$H_n^0 = U_{\ell(n)}$ であり，$H_n^{\ell(n)} = X_n$ である．仮定より，D は H_n^0 と $H_n^{\ell(n)}$ を確率 $\frac{1}{p(n)}$ で識別できる．ハイブリッド補題より，ある $i \in [0, \ell(n)]$ が存在して，D は H_n^i と H_n^{i+1} を確率 $\frac{1}{p(n)\ell(n)}$ で識別できる．ここで注目するのは，H_n^i と H_n^{i+1} の違いは，$(i+1)$ ビット目の値だけという点である．H_n^i のときは u_{i+1} であり，H_n^{i+1} のときは x_{i+1} である．つまり，直感的には，D は，$x_1 \cdots x_i$ が与えられたときに，x_{i+1} と一様ランダムビットを識別している．このとき，D は，x_{i+1} と $\bar{x}_{i+1}$ をも識別しているのである．ただし，$b \in \{0,1\}$ に対して，$\bar{b}$ は b の反転であり，$\bar{b} = 1 - b$ である．より正確に議論をするため，次の分布を考える．

$$\widetilde{H}_n^i = \{x_0 \cdots x_{i-1} \bar{x}_i u_{i+1} \cdots u_{\ell(n)} \mid x \leftarrow X_n, u \leftarrow U_{\ell(n)}\}.$$

つまり，$\widetilde{H}_n^i$ は H_n^i の i ビット目を反転した分布である．すると，分布 H_n^i は，分布 $\frac{1}{2}H_n^{i+1} + \frac{1}{2}\widetilde{H}_n^{i+1}$ だとみなすことができる．このとき，

$$\begin{aligned}
&\left|\Pr[D(t) = 1 \mid t \leftarrow H_n^{i+1}] - \Pr[D(t) = 1 \mid t \leftarrow H_n^i]\right| \\
&= \left|\Pr[D(t) = 1 \mid t \leftarrow H_n^{i+1}] - \left(\frac{1}{2}\Pr[D(t) = 1 \mid t \leftarrow H_n^{i+1}] + \frac{1}{2}\Pr[D(t) = 1 \mid t \leftarrow \widetilde{H}_n^{i+1}]\right)\right| \\
&= \frac{1}{2}\left|\Pr[D(t) = 1 \mid t \leftarrow H_n^{i+1}] + \Pr[D(t) = 1 \mid t \leftarrow \widetilde{H}_n^{i+1}]\right|
\end{aligned}$$

が成り立つ．D は H_n^i と H_n^{i+1} を確率 $\frac{1}{p(n)\ell(n)}$ で識別できることから，H_n^{i+1} と $\widetilde{H}_n^{i+1}$ を確率 $\frac{2}{p(n)\ell(n)}$ で識別できる．予測補題を用いると，ある PPT アルゴリズム A が存在して，

$$\Pr[A(t) = b \mid b \xleftarrow{R} \{0,1\}, t \leftarrow H_n^{i+1,b}] \geq \frac{1}{2} + \frac{1}{p(n)\ell(n)}$$

を満たす．ただし，$H_n^{i+1,0} = H_n^{i+1}, H_n^{i+1,1} = \widetilde{H}_n^{i+1}$ である．アルゴリズム A を利用して，次ビット予測を行なうアルゴリズム A' を構成する．

1. A' は，入力 $(1^n, t_1 t_2 \cdots t_i)$ に対して，$\ell(n) - i$ ビットのランダム系列 $u_{i+1} \cdots u_{\ell(n)} \leftarrow U_{\ell(n)-i}$ をサンプルし，$g \leftarrow A(t_1 \cdots t_i u_{i+1} \cdots u_{\ell(n)})$ とする．
2. もし $g = 1$ であれば，u_{i+1} を出力し，そうでなければ，$\bar{u}_{i+1} = 1 - u_{i+1}$ を出力する．

このとき，

$$\begin{aligned}\Pr[A'(1^n, t_1 \cdots t_i) = t_{i+1} \mid t \leftarrow X_n] &= \Pr[A(t) = 1 \mid b \xleftarrow{R} \{0,1\}, t \leftarrow H_n^{i+1,b}] \\ &\geq \frac{1}{2} + \frac{1}{p(n)\ell(n)}.\end{aligned}$$

つまり，A' は次ビット予測ができている． □

4 擬似乱数生成器

擬似乱数生成器 (pseudorandom generator; PRG) とは，入力として一様乱数を受け取り，擬似ランダム分布を出力する関数のことである．ただし，出力長は入力長よりも大きい必要がある．

定義 9 (擬似乱数生成器) 関数 $G : \{0,1\}^* \to \{0,1\}^*$ が擬似乱数生成器であるとは，以下の三つを満たすときである．

1. 効率性．G は PPT アルゴリズムで計算できる．
2. 拡大性．$|G(x)| > |x|$.
3. 擬似ランダム性．分布 $\{G(x) \mid x \leftarrow U_n\}_n$ が擬似ランダムである．

4.1 ハードコアビット

一方向性関数とは，ランダムな入力 x に対して $f(x)$ の逆像を計算するのが困難な関数であった．しかし，$f(x)$ から x に関する部分情報を得ることができる可能性はある．例えば，f が一方向性関数であるとき，$g(x_1, x_2) = (x_1, f(x_2)), |x_1| = |x_2|$ という関数も一方向性関数である．関数 g は，入力 (x_1, x_2) のうち，x_1 の部分については完全にわかってしまうが，$f(x_2)$ の部分の逆計算が困難であるため，g 全体としても逆計算は困難である．

一方向性という性質だけでは，$f(x)$ から x に関する部分情報が漏れている可能性がある．それでは，x に関して全く漏れることのない部分情報は存在するだろうか．逆計算が困難であることから，x に関する何らかの情報は計算できないはずである．このような，x に関して全く漏れることのない部分情報を定義する．

定義 10 (ハードコアビット) 関数 $h : \{0,1\}^* \to \{0,1\}$ が $f(x)$ のハードコアビットであるとは，h は PPT アルゴリズムで計算可能であり，任意の PPT アルゴリズム A に対して，無視できる関数 $\epsilon(\cdot)$ が存在し，すべての $n \in \mathbb{N}$ に対して，

$$\Pr[A(1^n, f(x)) = h(x) \mid x \xleftarrow{R} \{0,1\}^n] \leq \frac{1}{2} + \epsilon(n)$$

を満たすときである．

ハードコアビット $h(x)$ は，$f(x)$ が与えられたとしてもその値を予測することができない．つまり，$f(x)$ が与えられたとしても，ランダムに見えるビットである．ここでは，1 ビットの値として $h(x)$ を定義してい

るが，より一般的に，系列として定義することもできる．しかし，その場合は議論が複雑になることが多く，また，今後の議論では 1 ビットで十分である．

ハードコアビットは，OWF, OWP, TDP 等から，PRG や公開鍵暗号を構成する際に便利である．

ハードコアビットを考えるときは，具体的な OWF に対してそのハードコアビットを考えるという方向と，一般的に，任意の OWF に対してそのハードコアビットを考えるという方向の，二つの方向が考えられる．例えば，ハードコアビットとして，

$$MSB_n(x) = \begin{cases} 0 & x < \frac{n}{2} \\ 1 & x \geq \frac{n}{2} \end{cases}$$

という関数を考える．すると，離散対数仮定のもとで，一方向性関数 $f_{p,g}(x) = g^x \bmod p$ に対して，$MSB_{p-1}(x)$ はハードコアビットであることが知られている．また，RSA 関数 $f_{N,e}(x) = e^x \bmod N$ は，$MSB_N(x)$ がハードコアビットであるだけでなく，x のすべてのビットがハードコアビットであることが知られている．

4.2 PRG の構成

定理 11 一方向性置換 f とそのハードコアビット h を考える．このとき，$G(x) = (f(x), h(x))$ は擬似乱数生成器である．

証明: 矛盾を導くため，ある PPT アルゴリズム A と多項式 $p(n)$ が存在して，無限に多くの n に対して，ある $i \in \{1, \ldots, n+1\}$ が存在し，A は i ビット目を確率 $\frac{1}{p(n)}$ で予測できると仮定する．G の出力の最初の n ビットは，一様乱数を f で置換しているだけであり，一様乱数のままである．したがって，A は $n+1$ ビット目を，確率 $\frac{1}{p(n)}$ で予測する必要がある．つまり，

$$\Pr[A(1^n, f(x)) = h(x) \mid x \leftarrow U_n] \geq \frac{1}{2} + \frac{1}{p(n)}$$

が成り立つ．しかし，これは h がハードコアビットであることに矛盾している． □

4.3 PRG の伸長

補題 12 擬似乱数生成器 $G : \{0,1\}^n \to \{0,1\}^{n+1}$ が存在するとき，任意の多項式 $\ell(\cdot)$ に対して，関数 $G' : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ を以下のように定義する．

$$\begin{aligned} &G'(x) = b_1 \cdots b_{\ell(n)} \\ &\text{ただし } x_0 \leftarrow x \\ &\qquad (x_1, b_1) \leftarrow G(x_0) \\ &\qquad (x_2, b_2) \leftarrow G(x_1) \\ &\qquad\quad \vdots \\ &\qquad (x_{\ell(n)}, b_{\ell(n)}) \leftarrow G(x_{\ell(n)-1}) \end{aligned}$$

このとき，G' は擬似乱数生成器である．

定理 11 と補題 12 から，次のような PRG の構成法が得られる．

系 13 一方向性置換 f とそのハードコアビット h，任意の多項式 $\ell(\cdot)$ に対して，

$$G(x) = (h(x), h(f(x)), h(f^{(2)}(x)), \ldots, h(f^{(\ell(n))}(x)))$$

は擬似乱数生成器である．

4.4 任意の OWF からのハードコアビットの構成法

系列 $x, r \in \{0,1\}^n$ に対して，内積を $\langle x, r\rangle = \sum_i x_i r_i \bmod 2$ と定義する．

定理 14 (Goldreich-Levin) 一方向性関数 f に対して，$f'(x,r) = (f(x), r), |x| = |r|$ と定義する．このとき，関数 f' は一方向性関数であり，$h(x,r) = \langle x, r\rangle$ は f' のハードコアビットである．

ここでは，議論を簡単にするため，一方向性関数 f が置換（つまり OWP）である場合の証明を与える．したがって，$(f(x), r)$ から $\langle x, r\rangle$ は一意に定まる．

証明の方針は，ハードコアビットでないことを仮定すると，一方向性が破れることを示す．より詳しく述べると，$f'(x,r)$ が与えられたときに $h(x,r)$ を計算することが，$\frac{1}{2}$ よりも無視できないほど大きな確率でできる PPT アルゴリズム A が存在したと仮定すると，f の逆計算が出来る PPT アルゴリズム B が存在することを示す．つまり，B は $y = f(x)$ が与えられて，A を利用することで x を無視できない確率で計算できることを示す．まずは単純化した場合の議論をみていく．

4.4.1 最も単純な場合

A が確率 1 で $h(x,r)$ を正しく計算する場合を考える．この場合，次のような方法で B は $f(x)$ の逆計算ができる．まず，B は，入力 y に対して，$x_i = A(y, e_i)$ とする．ただし，$e_i \in \{0,1\}^n$ は i ビット目が 1 で，その他はすべて 0 であるようなベクトルである．そして，B は $x_1 x_2 \cdots x_n$ を出力する．定義より $\langle x, e_i\rangle = x_i$ であり，仮定より $A(f(x), r) = \langle x, r\rangle$ であるため，B は逆計算が出来ている．

4.4.2 比較的単純な場合

次に，A が確率 $\frac{3}{4} + \epsilon$ で $h(x,r)$ を正しく計算する場合を考える．ただし，ある多項式 $p(\cdot)$ に対して，$\epsilon = \frac{1}{p(n)}$ である．以下に述べる理由のため先ほどの方法はうまくいかない．

1. A はすべての y に対して正しい出力を返すとは限らない．
2. A が $h(x,r)$ を高い確率で予測できたとしても，特定の $r = e_i$ に対して，予測を間違えるかもしれない．

一つ目の問題点について，入力 x のある程度の割合については，A は正しい出力を返すことを示す．

$$S = \left\{ x \;\middle|\; \Pr[A(f(x), r) = h(x,r) \mid r \xleftarrow{R} \{0,1\}^n] > \frac{3}{4} + \frac{\epsilon}{2} \right\}$$

と定義する．このとき，

$$\Pr[x \in S] \geq \frac{\epsilon}{2}$$

であることがわかる．なぜならば，もし満たさないとすると，

$$\begin{aligned}
&\Pr[A(f(x), r) = h(x,r) \mid x, r \xleftarrow{R} \{0,1\}^n] \\
&\quad \leq \Pr[x \in S] + \Pr[x \notin S] \cdot \Pr[A(f(x), r) = h(x,r) \mid x \notin S] \\
&\quad < \frac{\epsilon}{2} + \frac{3}{4} + \frac{\epsilon}{2} = \frac{3}{4} + \epsilon
\end{aligned}$$

となり，矛盾する．

二つ目の問題点を対処するため，内積関数 $\langle \cdot, \cdot \rangle$ の線形性を利用する．

事実 15 $\langle a, b \oplus c\rangle = \langle a, b\rangle \oplus \langle a, c\rangle$.

証明: $\langle a, b\oplus c\rangle = (\sum_i a_i(b_i + c_i)) \bmod 2 = (\sum_i a_i b_i + \sum_i a_i c_i) \bmod 2 = (\sum_i a_i b_i \bmod 2) + (\sum_i a_i c_i \bmod 2) \bmod 2 = \langle a, b\rangle \oplus \langle a, c\rangle$ □

A は，$\langle x, e_i\rangle$ を計算するために，ランダムに r を選び，$\langle x, r\rangle$ と $\langle x, r + e_i\rangle$ を計算し，それらの排他的論理和を計算する．もし，二つとも正しく計算できていれば，$\langle x, e_i\rangle$ の正しい値を得ることができる．そして，この計算を $m = \mathrm{poly}(\log n/\epsilon^2)$ 回繰り返し，得られた m 回の結果の多数決をとって，$\langle x, e_i\rangle$ の最終的な予測結果とする．

上記の方法がうまくいく理由を説明する．もし $x \in S$ である場合，$A(y, r) \neq h(x, r)$ である確率は $\frac{1}{4} - \frac{\epsilon}{2}$ 以下であり，$A(y, r + e_i) \neq h(x, r)$ である確率も $\frac{1}{4} - \frac{\epsilon}{2}$ 以下である．したがって，A の答えがともに正しい確率は $\frac{1}{2} + \epsilon$ 以上である．つまり，A は $\langle x, e_i\rangle$ を確率 $\frac{1}{2} + \epsilon$ 以上で正しく計算できる．この試行を m 回繰り返し，多数決をとれば，Chernoff 限界から，A は $\langle x, e_i\rangle$ を確率 $1 - \frac{1}{n^2}$ 以上で正しく計算できる．

上記の方法で，$x_i = \langle x, e_i\rangle$ を確率 $1 - \frac{1}{n^2}$ 以上で正しく求めることができる．これをすべての $i \in \{1, \ldots, n\}$ に対して行なったとき，そのうち少なくとも一つの x_i で間違ってしまう確率は $\frac{n}{n^2} = \frac{1}{n}$ 以下であり，したがって，B は，確率 $1 - \frac{1}{n}$ 以上で x を求めることができる．これは，無視できない確率で f の逆計算に成功しており，f の一方向性に矛盾する．

補足 16 Chernoff 限界は，独立に t 回サンプルして平均を取った値が，平均値より ϵ 以上離れてしまう確率は，$e^{-\Omega(\epsilon^2 t)}$ で抑えられることを示している．

形式的には，$X_1, X_2, \ldots, X_t$ が，$\Pr[X_i = 1] = p$ であるような，$\{0, 1\}$ 上の値をとる独立同分布確率変数とする．このとき，任意の $0 < \epsilon < 1$ に対し，t が十分大きいとき，

$$\Pr\left[\sum_{i=1}^{t} X_i \geq (p + \epsilon)t\right] \leq 2^{-\epsilon^2 t/3}, \qquad \Pr\left[\sum_{i=1}^{t} X_i \leq (p - \epsilon)t\right] \leq 2^{-\epsilon^2 t/3}.$$

先ほどの議論では，ある i について，m 回繰り返して x_i の計算を行っている．j 回目の繰り返しで正しく計算できたときに $X_j = 1$ だとすると，$\Pr[X_j = 1] = p = \frac{1}{2} + \epsilon$ であった．m 回の結果の多数決を取ったときに，結果が間違ってしまう確率は，$\Pr[\sum_i^m X_i \leq \frac{m}{2}]$ 以下であり，$m = \mathrm{poly}(\log n/\epsilon^2)$ とすれば，$\frac{1}{n^2}$ 以下に抑えることができる．

4.4.3 一般的な場合

最も一般的な場合，つまり，A が確率 $\frac{1}{2} + \epsilon$ で $h(x, r)$ を正しく計算する場合を考える．先ほどと同様に，

$$S = \left\{x \;\middle|\; \Pr[A(f(x), r) = h(x, r) \mid r \xleftarrow{R} \{0, 1\}^n] > \frac{1}{2} + \frac{\epsilon}{2}\right\}$$

と定義する．そして，同様に，

$$\Pr[x \in S] \geq \frac{\epsilon}{2}$$

が成り立つ．

B を構成するため，$f(x)$ が与えられたときに，以下のサンプルを出力してくれるオラクル C が存在すると仮定する．

$$(\langle x, r_1\rangle, r_1), \ldots, (\langle x, r_m\rangle, r_m)$$

ただし，$r_1, \ldots, r_n$ は独立に選んだランダムな値である．まず，このような C が存在したときに，f の逆計算を行う B を構成できることを示す．B は，$y = f(x)$ を受け取ったとき，x_i を計算するために以下を

行なう．$C(y)$ の出力を $(b_1, r_1), \ldots, (b_m, r_m)$ とする．そして，$j = 1, \ldots, m$ に対して，$r'_j = e_j \oplus r_j$ として，$g_j = b_j \oplus A(y, r'_j)$ とする．そして，$g_1, \ldots, g_m$ の値で多数決をとった値を x_i の予測結果とする．もし，$x \in S$ である場合，g_j が正しい結果である確率は，S の定義より，$\frac{1}{2} + \frac{\epsilon}{2} = \frac{1}{2} + \epsilon'$ 以上である．先ほどと同様に，$m = \mathrm{poly}(\log n/\epsilon'^2)$ とすれば，x_i を確率 $1 - \frac{1}{n^2}$ 以上の確率で計算できる．結果として，B は $f(x)$ を無視できない確率で逆計算できる．

問題は，C をどのように実現するかである．まず，C の出力 $(\langle x, r_1\rangle, r_1), \ldots, (\langle x, r_m\rangle, r_m)$ は，（一様ランダムではなく）対独立（pair-wise independent）であったとしても，議論はうまくいくことを示す．以下に示す，対独立サンプリング不等式を用いると，x_i が間違っている確率は，$\frac{1}{\epsilon'^2 m}$ 以下である．少なくとも一つの x_i で間違ってしまう確率は，$\frac{n}{\epsilon'^2 m}$ 以下であり，$m \geq \frac{2n}{\epsilon'^2}$ であれば，$\frac{1}{2}$ 以下に抑えることができる．以上より，C の出力として $\frac{2n}{\epsilon'^2}$ 個の対独立サンプルを計算できれば，B は無視できない確率で逆計算ができる．

単純に，ランダムサンプル $r_1, \ldots, r_m$ に対して，$b_1, \ldots, b_m$ をランダムに推測すると，すべての b_i が正しい確率は 2^{-m} となってしまう．そこで，$\log m$ 個のランダムサンプル $s_1, \ldots, s_{\log m}$ に対して，$b'_1, \ldots, b'_{\log m}$ を推測することにする．すると，すべての推測が正しい確率は $\frac{1}{m}$ になる．そして，サンプル $r_1, \ldots, r_m$ は，$s_1, \ldots, s_{\log m}$ の組合せによって代用することにする．$b_1, \ldots, b_m$ も同様に $b'_1, \ldots, b_{\log m}$ を利用する．つまり，

$$r_i = \sum_{j \in I_i} s_j \quad \text{ただし } j \in I_j \Leftrightarrow i_j = 1$$
$$b_i = \sum_{j \in I_i} b'_j$$

このとき，各 r_i は対独立であり，$b_1, \ldots, b_m$ がすべて正しい確率は $\frac{1}{m}$ である．

これまでの議論から，$x \in S$ であるとき，C の出力として m 個の対独立なサンプルがあれば，確率 $\frac{1}{2}$ 以上で $f(x)$ から x を計算することができた．そして，m 個の対独立サンプルは，確率 $\frac{1}{m}$ で計算することができるため，最終的に B が f の逆計算ができる確率は，$m = \frac{2n}{\epsilon'^2}$ とすると，

$$\epsilon' \cdot \frac{1}{2} \cdot \frac{1}{m} = \frac{\epsilon'^3}{4n}$$

以上であり，これは無視できない確率である．したがって f の一方向性に矛盾する．

命題 17 (対独立サンプリング不等式) $X_1, \ldots, X_t$ は，$E[X_i] = \mu$，$|X_i| \leq 1$ である対独立な確率変数だとする．このとき，

$$\Pr\left[\left|\frac{\sum_i X_i}{t} - \mu\right| \geq \epsilon\right] \leq \frac{1 - \mu^2}{\epsilon^2 t}.$$

この不等式は，以下に示す Chebyshev の不等式から導かれる．平均 $E[X]$，分散 σ^2 の確率変数 X に対し，任意の $k > 0$ に対して，

$$\Pr[|X - E[X]| \geq k] \leq \frac{\sigma^2}{k^2}.$$