数理解析研究所講究録
1148巻 2000年 118-123

弱いランダム仮定の元での公開鍵暗号の強秘匿性について

通信・放送機構/横浜リサーチセンター　小柴 健史 (Takeshi Koshiba)*
東京工業大学/数理・計算科学専攻　渡辺 治 (Osamu Watanabe)

1 はじめに

公開鍵暗号に対する複数の安全性の概念の間がどうなっているのかを明確にすることは重要なことである．一般に安全性の概念は，敵対者の能力，敵対者の成功基準，暗号化 (および復号) の際に利用できる資源によって測られている．敵対者の能力とは，選択平文攻撃ができるとか，適応的選択暗号文攻撃ができるとかいった能力である．敵対者の成功基準とは，暗号文から平文が完全解読できたときに成功と言うとか，暗号文から平文の情報の1ビットでも解読できたときに成功と言うとかである．

公開鍵暗号系の安全性については Goldwasser らが [7] において semantic security という安全性の概念を定めている．直観的に言えば，暗号文から平文の1ビットの情報も得られないという概念の定式化になっている．同時に暗号文の indistinguishability という概念を任意の異なる2つ平文に対する暗号文を有意差をもって区別できないことと定めている．[7] において indistinguishability を持つ公開鍵暗号は semantically secure であることが証明されている．また [11] で逆方向の証明が与えられている．semantic security や indistinguishability の性質を持つ暗号は暗号化に本質的に乱数を利用している．ここでは，その乱数の部分をよりランダム性の弱い擬似乱数に置換した場合について semantic security や indistinguishability の定義を与え，その概念間の関係を明確にする．

2 準備

定義 1 暗号系 (G, E, D) とは以下を満足する確率的多項式時間アルゴリズムの3つ組である．

1. 入力 1^n に対してアルゴリズム G (鍵生成アルゴリズムと呼ぶ) は2進列の組を出力する．
2. $G(1^n)$ が出力するような任意の組 (e, d) と任意の $\alpha \in \{0,1\}^*$ に対して，アルゴリズム E (暗号化アルゴリズム) と D (復号アルゴリズム) は $\Pr[D(d, E(e, \alpha)) = \alpha] = 1$ を満足する．ただし，確率はアルゴリズム E と D のコイン投げ上で考える．

* e-mail: koshiba@acm.org

正整数 n はセキュリティパラメータとして系に与えられるものである．$G(1^n)$ が出力する (e, d) は暗号化鍵と復号鍵に対応する．文字列 $E(e, \alpha)$ は平文 $\alpha \in \{0,1\}^*$ を暗号化鍵 e を利用して作った暗号文であり，$D(d, \beta)$ は暗号文 β を復号鍵 d を用いて復号した平文である．

以下では，$E(e, \alpha)$ の替りに単に $E_e(\alpha)$ と表記する場合もある．$D_d(\beta)$ についても同様．また，$G_1(1^n)$ を $G(1^n)$ の出力の1つ目の構成要素とする．

定義 2 暗号系 (G, E, D) が semantically secure であるとは，ある確率的多項式時間アルゴリズム T が存在して，すべての多項式サイズ回路族 $\{C_n\}$ とすべての確率分布族 $\{X_n\}_{n \in N}$ (ただし $|X_n| = \mathrm{poly}(n)$)，すべての多項式時間計算可能関数 $f, h : \{0,1\}^* \to \{0,1\}^*$，すべての多項式 $p(\cdot)$ に対して，十分大きな n で以下が成立するときを言う．

$$\Pr[C_n(G_1(1^n), E_{G_1(1^n)}(X_n), 1^{|X_n|}, h(X_n)) = f(X_n)] < \Pr[C'_n(G_1(1^n), 1^{|X_n|}, h(X_n)) = f(X_n)] + \frac{1}{p(n)}$$

ただし $C'_n = T(C_n)$．また，上式の確率はアルゴリズム G_1 と E のコイン投げおよび確率分布 X_n 上で考える．

定義 3 暗号系 (G, E, D) が indistinguishability の性質を持つとは，すべての多項式サイズ回路族 $\{C_n\}$，すべての多項式 $p(\cdot)$，十分大きな n，すべての $x, y \in \{0,1\}^{\mathrm{poly}(n)}$ (即ち $|x| = |y|$) に対して以下が成立するときを言う．

$$\left|\Pr[C_n(G_1(1^n), E_{G_1(1^n)}(x)) = 1] - \Pr[C_n(G_1(1^n), E_{G_1(1^n)}(y)) = 1]\right| < \frac{1}{p(n)}.$$

ただし，確率はアルゴリズム G_1 と E のコイン投げ上で考える．

上の2つの定義は単一の平文を暗号化したときの系の安全性に関するものである．現実的は同一の鍵で複数の平文を暗号化することが一般的であり，その場合の安全性も考えることがより現実的な安全性の定義となっている．

定義 4 暗号系 (G, E, D) が複数平文に対して semantically secure であるとは，ある確率的多項式時間アルゴリズム T が存在して，すべての多項式 $t(\cdot)$，すべての多

項式サイズ回路族 $\{C_n\}$, すべての確率分布族 $\{\bar{X}_n\}_{n\in N}$ (ただし $|\bar{X}_n| = t(n)\cdot \mathrm{poly}(n)$), すべての多項式時間計算可能 $f, h : \{0,1\}^* \to \{0,1\}^*$, すべての多項式 $p(\cdot)$ に対して, 十分大きな n で以下が成立するときを言う.

$$\Pr[C_n(G_1(1^n), \bar{E}_{G_1(1^n)}(\bar{X}_n), 1^{|\bar{X}_n|}, h(\bar{X}_n)) = f(\bar{X}_n)] < \Pr[C'_n(G_1(1^n), 1^{|\bar{X}_n|}, h(\bar{X}_n)) = f(\bar{X}_n)] + \frac{1}{p(n)}$$

ただし $C'_n = T(C_n)$, $\bar{X}_n = (X_n^{(1)}, \ldots, X_n^{(t(n))})$, $\bar{E}_e(\bar{X}_n) = E_e(X_n^{(1)}), \ldots, E_e(X_n^{(t(n))})$.

定義 5 暗号系 (G,E,D) が複数平文に対して *indistinguishability* の性質を持つとは, すべての多項式 $t(\cdot)$, すべての多項式サイズ回路族 $\{C_n\}$, すべての多項式 $p(\cdot)$ に対して, 十分大きな n で, そしてすべての $x_1, \ldots, x_{t(n)}$, $y_1, \ldots, y_{t(n)} \in \{0,1\}^{\mathrm{poly}(n)}$ に対して以下が成立するときを言う.

$$\left|\Pr[C_n(G_1(1^n), \bar{E}_{G_1(1^n)}(\bar{x})) = 1] - \Pr[C_n(G_1(1^n), \bar{E}_{G_1(1^n)}(\bar{y})) = 1]\right| < \frac{1}{p(n)}$$

ただし $\bar{x} = (x_1, \ldots, x_{t(n)})$, $\bar{y} = (y_1, \ldots, y_{t(n)})$.

定理 6 暗号系 (G,E,D) において以下は同値である.

1. (G,E,D) が *semantically secure* である.
2. (G,E,D) が *indistinguishability* の性質を持つ.
3. (G,E,D) が複数平文に対して *semantically secure* である.
4. (G,E,D) が複数平文に対して *indistinguishability* の性質を持つ.

この定理から, より強い安全性の概念である複数平文に対する semantic security を示すのに単一平文の semantic security あるいは indistinguishability を持つことを証明しさえすればよいというありがたい性質があるということが言える. しかしこの性質は理想乱数の元での性質であり次で扱う擬似乱数版での安全性では一般にこのようなことは言えないのである.

3 擬似乱数生成器によるランダム仮定の緩和

擬似乱数生成器 g とは $\{0,1\}^n$ の要素を入力とし $\{0,1\}^{\ell(n)}$ $(n < \ell(n))$ の要素を出力する関数で, 入力を一様ランダムに動かしたとき, その出力と $\{0,1\}^{\ell(n)}$ 上の一様ランダムな要素を識別する効率的なアルゴリズムが存在しないようなものである [1, 13]. この擬似乱数生成器を利用する, つまり, 利用する乱数列のサイズが小さくてすむ状況で, 公開鍵暗号系 (G,E,D) が semantically secure であることと複数平文に対して semantically secure であることは依然として等価である.

しかしながら, 擬似乱数生成器を利用したランダムモデルにおいては, 以下のような実際的な問題がある. 2 つの連続する平文に対して semantically secure であることを保証する場合, 疑似乱数生成器は入力サイズの 2 倍の出力が要求される. 平文 2 つをこの擬似乱数列を利用して暗号化することで, 2 つの連続する平文に対して semantically secure であることを保証される. さらに連続的に暗号化をしなければならない要求が発生し, 3 つの連続する平文に対して semantically secure であることが要求された場合はいままでの暗号化の結果はすべて破棄し, 3 倍にする擬似乱数生成器を利用して初めから暗号化をしなければならない. つまり, 疑似乱数生成器を利用する限りその安全性を保証するためには, 擬似乱数列生成をバッチ処理しなければならない. 十分長い連続する平文に対して semantically secure であることを保証するには予め十分長い乱数列を計算し記憶しておく必要がある.

擬似乱数生成器によるランダム仮定の緩和はバッチ的な運用が要求されるのに対して, オンライン的な暗号化処理の方が望ましい場合があろう. 特に, 記憶領域が十分でない場合がそうである. 以下では, オンライン的な暗号化処理に適したランダム仮定の緩和を考えることにする.

4 オンライン的擬似乱数モデルでの安全性

ここでは, 暗号化において乱数の替りにある決定的な方法で生成される数列を利用した場合の暗号の安全性の定義を与える.

定義 7 数列生成オラクル V とは以下を満足する計算メカニズムである. ただし, V は暗号系 (G,E,D) と共に利用されることを前提とする. $G(1^n)$ が (e,d) を出力した場合を考える. 暗号化アルゴリズム E_e が利用する乱数の空間を R_e とする (即ち $R_e = \{0,1\}^{\mathrm{poly}(n)}$). ある $S_e = \{0,1\}^{\mathrm{poly}(n)}$ が存在して, V は入力 (init, e) に対しては $r \in R_e, s \in S_e$ をランダムに生成し r を返す. (r,s) の値は内部状態として保持するものとする. V は入力 (next, e) に対しては内部状態 (r,s) から決定性多項式時間で計算できる (r',s') (ただし $r' \in R_e, s' \in S_e$) を出力する. 更に (r',s') を新しい内部状態として更新する. 暗号系 (G,E,D) において暗号化の乱数をオラクル V で置換した系を数列生成オラクル上の暗号系と呼び, (G,E,D,V) で表す.

今 $e, r_0 \in R_e, s_0 \in S_e$ を固定する. このとき $(r_i, s_i) = V(e, r_{i-1}, s_{i-1})$ と定める. $\{r_i\}$ を暗号系 (G,E,D) において (e, r_0, s_0) が定める V-数列と呼ぶ. とくに初期値 r_0, s_0 の選択が問題にならないような場合は, 単に e が定める V-数列と呼び, V_e-数列と表記する.

特に断らない限りは r の R_e からのランダムチョイスは $V(\mathsf{init}, e)$ の返り値のことを指し，$v_e^i(r)$ は最近の $V(\mathsf{init}, e)$ の呼び出しから数えて i 回目の $V(\mathsf{next}, e)$ の呼び出しの返り値とする．

定義 8 数列生成オラクル上の暗号系 (G, E, D, V) が，m 個の平文に対して *semantically secure* であるとは，ある確率的多項式時間アルゴリズム T が存在して，すべての多項式サイズ回路族 $\{C_n\}$，すべての確率分布族 $\{\bar{X}_n\}$ (ただし $|\bar{X}_n| = m \cdot \mathrm{poly}(n)$)，すべての多項式時間計算可能 f, $h : \{0,1\}^* \to \{0,1\}^*$，すべての多項式 $p(\cdot)$ に対して，十分大きな n で以下が成立するときを言う．

$$\Pr[C_n(G_1(1^n), \bar{E}_{G_1(1^n)}(\bar{X}_n, \bar{r}), 1^{|\bar{X}_n|}, h(\bar{X}_n)) = f(\bar{X}_n)] < \Pr[C'_n(G_1(1^n), 1^{|\bar{X}_n|}, h(\bar{X}_n)) = f(\bar{X}_n)] + \frac{1}{p(n)}$$

ただし $C'_n = T(C_n)$, $\bar{X}_n = (X_n^{(1)}, \ldots, X_n^{(m)})$, $\bar{E}_e(\bar{X}_n, \bar{r}) = E_e(X_n^{(1)}, r), E_e(X_n^{(2)}, v_e(r)), \ldots, E_e(X_n^{(m)}, v_e^{m-1}(r))$. また，上式の確率はアルゴリズム G_1 のコイン投げ，r の一様ランダムな選択および確率分布 $\bar{X}_n$ 上で考える．

定義 9 数列生成オラクル上の暗号系 (G, E, D, V) が，m 個の平文に対して indistinguishability の性質を持つとは，すべての多項式サイズ回路族 $\{C_n\}$，すべての多項式 $p(\cdot)$ に対して，十分大きな n で，そしてすべての $x_1, \ldots, x_m, y_1, \ldots, y_m \in \{0,1\}^{\mathrm{poly}(n)}$ に対して以下が成立するときを言う．

$$\left|\Pr[C_n(G_1(1^n), \bar{E}_{G_1(1^n)}(\bar{x}, \bar{r})) = 1] - \Pr[C_n(G_1(1^n), \bar{E}_{G_1(1^n)}(\bar{y}, \bar{r})) = 1]\right| < \frac{1}{p(n)}$$

ただし $\bar{x} = (x_1, \ldots, x_m)$, $\bar{y} = (y_1, \ldots, y_m)$, $\bar{E}_e(\bar{x}, \bar{r}) = E_e(x_1, r), E_e(x_2, v_e(r)), \ldots, E_e(x_m, v_e^{m-1}(r))$, $\bar{E}_e(\bar{y}, \bar{r}) = E_e(y_1, r), E_e(y_2, v_e(r)), \ldots, E_e(y_m, v_e^{m-1}(r))$. また，上式の確率はアルゴリズム G_1 のコイン投げと r の一様ランダムな選択上で考える．

定義 10 数列生成オラクル上の暗号系 (G, E, D, V) が，m 個の平文に対して super-indistinguishability の性質を持つとは，すべての多項式サイズ回路族 $\{C_n\}$，すべての多項式 $p(\cdot)$ に対して，十分大きな n で，そしてすべての $x_1, \ldots, x_m, y_1, \ldots, y_m \in \{0,1\}^{\mathrm{poly}(n)}$ に対して以下が成立するときを言う．

$$\left|\Pr[C_n(G_1(1^n), \bar{E}_{G_1(1^n)}(\bar{x}, \bar{r})) = 1] - \Pr[C_n(G_1(1^n), \bar{E}_{G_1(1^n)}(\bar{y}, \bar{r})) = 1]\right| < \frac{1}{p(n)}$$

ただし $\bar{x} = (x_1, \ldots, x_m)$, $\bar{y} = (y_1, \ldots, y_m)$, $\bar{E}_e(\bar{x}, \bar{r}) = E_e(x_1, r), E_e(x_2, v_e(r)), \ldots, E_e(x_m, v_e^{m-1}(r))$, $\bar{E}_e(\bar{y}, \bar{r}) = E_e(y_1, r_1), E_e(y_2, r_2)), \ldots, E_e(y_m, r_m))$. また，上式の前者の確率はアルゴリズム G_1 のコイン投げと r の一様ランダムな選択上で考え，後者の確率はアルゴリズム G_1 のコイン投げと $r_1, \ldots, r_m$ の R_e からの独立かつ一様ランダムな選択上で考える．

定義 11 暗号系 (G, E, D) で利用する数列生成オラクル V が m-semi-random であるとは，すべての多項式サイズ回路族 $\{C_n\}$，すべての多項式 $p(\cdot)$ に対して，十分大きな n で以下が成立するときを言う．

$$\left|\Pr[C_n(G_1(1^n), r, v_e(r), \ldots, v_e^{m-1}(r)) = 1] - \Pr[C_n(G_1(1^n), r_1, \ldots, r_m) = 1]\right| < \frac{1}{p(n)}$$

ただし，上式の前者の確率はアルゴリズム G_1 のコイン投げと r の一様ランダムな選択上で考え，後者の確率はアルゴリズム G_1 のコイン投げと $r_1, \ldots, r_m$ の R_e からの独立かつ一様ランダムな選択上で考える．

定義 12 数列生成オラクル V が m-simulatable であるとはある多項式時間アルゴリズム A が存在して，すべての多項式 $p(\cdot)$ に対して，十分大きな n で以下が成立するときを言う．

$$\max_Z\{|\Pr[A(r) \in Z] - \Pr[(r, v(r), \ldots, v^{m-1}(r)) \in Z]|\} < \frac{1}{p(n)}.$$

ただし，r の一様ランダムな選択上で考える．

定理 13 数列生成オラクル上での暗号系 (G, E, D, V) が $m = O(\log(n))$ 個の平文に対して *semantically secure* であるならば (G, E, D, V) も m 個の平文に対して *indistinguishability* の性質を持つ．

Proof: $m = 2$ の場合の対偶を示す．ある多項式サイズ回路族 $\{D_n\}$，ある多項式 $p(\cdot)$ が存在して無限に多くの n で以下が成立すると仮定する．

$$\left|\Pr[D_n(E_e(x_n, r), E_e(y_n, v_e(r))) = 1] - \Pr[D_n(E_e(\tilde{x}_n, r), E_e(\tilde{y}_n, v_e(r))) = 1]\right| > \frac{1}{p(n)}. \tag{1}$$

また，無限に多くの n で以下も成立する．

$$\Pr[D_n(E_e(x_n, r), E_e(y_n, v_e(r))) = 1] - \Pr[D_n(E_e(\tilde{x}_n, r), E_e(\tilde{y}_n, v_e(r))) = 1] > \frac{1}{p(n)}. \tag{2}$$

ただし，式 (2) を満たす無限列 $\{x_n, y_n, \tilde{x_n}, \tilde{y_n}\}$ は式 (1) を満たす無限列の部分列である．

X_n, Y_n を $\Pr[X_n = x_n] = \Pr[X_n = \tilde{x}_n] = 1/2$, $\Pr[Y_n = y_n] = \Pr[Y_n = \tilde{y}_n] = 1/2$ を満たす確率変数とする．また f を $f(x_n, y_n) = 3$, $f(x_n, \tilde{y}_n) = 2$, $f(\tilde{x}_n, y_n) = 1$, $f(\tilde{x}_n, \tilde{y}_n) = 0$ を満たす関数とす

る．今，次のような回路 C_n を考える．C_n への入力 $E_e(x,r), E_e(y,v_e(r))$ に対して，回路 D_n を同じ入力で利用する．D_n の出力が 1 のときは C_n の出力として 3 を返し，それ以外の場合は 0 を返す回路とする．このとき，次の確率を見積る．

$$\begin{aligned}
&\Pr[C_n(E_e(X_n,r),E_e(Y_n,v_e(r))) = f(X_n,Y_n)] \\
&= \frac{1}{4}\Pr[C_n(E_e(X_n,r),E_e(Y_n,v_e(r))) \\
&\qquad = f(X_n,Y_n) | X_n = x_n, Y_n = y_n] \\
&\quad + \frac{1}{4}\Pr[C_n(E_e(X_n,r),E_e(Y_n,v_e(r))) \\
&\qquad = f(X_n,Y_n) | X_n = \tilde{x}_n, Y_n = y_n] \\
&\quad + \frac{1}{4}\Pr[C_n(E_e(X_n,r),E_e(Y_n,v_e(r))) \\
&\qquad = f(X_n,Y_n) | X_n = x_n, Y_n = \tilde{y}_n] \\
&\quad + \frac{1}{4}\Pr[C_n(E_e(X_n,r),E_e(Y_n,v_e(r))) \\
&\qquad = f(X_n,Y_n) | X_n = \tilde{x}_n, Y_n = \tilde{y}_n] \\
&\geq \frac{1}{4}\Pr[C_n(E_e(x_n,r),E_e(y_n,v_e(r))) = 3] \\
&\quad + \frac{1}{4}\Pr[C_n(E_e(\tilde{x}_n,r),E_e(\tilde{y}_n,v_e(r))) = 0] \\
&= \frac{1}{4}(\Pr[D_n(E_e(x_n,r),E_e(y_n,v_e(r))) = 1] + 1 \\
&\quad - \Pr[D_n(E_e(\tilde{x}_n,r),E_e(\tilde{y}_n,v_e(r))) = 1]) \\
&\geq \frac{1}{4} + \frac{1}{4p(n)}.
\end{aligned}$$

一方で $\Pr[C'_n(1^{|X_n|}) = f(X_n,Y_n)] \leq 1/4$ である．よって $\{C_n\}$ は (G,E,D,V) が 2 個の平文に対して semantically secure を破る多項式サイズ回路族となる．一般の m についても $O(\log n)$ であれば同様．□

定理 14 数列生成オラクル上の暗号系 (G,E,D,V) が m 個の平文に対して *indistinguishability* の性質を持つとする．V が *m-simulatable* ならば (G,E,D,V) は m 個の平文に対して *semantically secure* である．

Proof: $m=2$ の場合の対偶を示す．ある多項式サイズ回路族 $\{C_n\}$ が存在し，ある多項式 $p(\cdot)$ と多項式時間計算可能関数 h が存在して無限に多くの n で以下が成立するとする．

$$\begin{aligned}
&\Pr[C_n(h(X_n,Y_n),E_e(X_n,r),E_e(Y_n,v_e(r))) = f(X_n,Y_n)] \\
&\quad - \Pr[C'_n(h(X_n,Y_n),1^{|X_n|}) = f(X_n,Y_n)] > \frac{1}{p(n)}.
\end{aligned}$$

今，次のような回路 C'_n を考える．まず r をランダムに選択し r を利用して $1^{|X_n|}$ を暗号化する．(正確には r を利用する回路 $C'_{n,r}$ があり r によって回路が一様に選択される．) 次に $v_e(r)$ の計算をし $v_e(r)$ を乱数と見なして $1^{|X_n|}$ を暗号化する．これらの 2 つの暗号文を入力として回路 C_n に与える．この C'_n は v_e が多項式時間計算可能なので C_n から計算が可能となる．このとき，

$$\begin{aligned}
&\Pr[C_n(h(X_n,Y_n),E_e(X_n,r),E_e(Y_n,v_e(r))) = f(X_n,Y_n)] \\
&\quad - \Pr[C_n(h(X_n,Y_n),E_e(1^{|X_n|},r),E_e(1^{|X_n|},v_e(r))) \\
&\qquad = f(X_n,Y_n)] > \frac{1}{p(n)}
\end{aligned}$$

が成立する．今，上の式の差を最大にする X_n および Y_n の値を x_n, y_n とする．この x_n, y_n を用いて回路 D_n を次のように構成する．D_n への入力 $E_e(\alpha,r), E_e(\beta,v_e(r))$ に対して回路 C_n への入力として $(h(x_n,y_n), E_e(\alpha,r), E_e(\beta,v_e(r)))$ を与える．C_n の出力が $g(x_n,y_n)$ と一致するときは D_n の出力として 1 を返し，そうでない場合は 0 を返す．このようにすると，

$$\begin{aligned}
&\Pr[D_n(E_e(x_n,r),E_e(y_n,v_e(r))) = 1] \\
&\quad - \Pr[D_n(E_e(1^{|X_n|},r),E_e(1^{|X_n|},f_e(r))) = 1] > \frac{1}{p(n)}
\end{aligned}$$

が成立する．よって $\{D_n\}$ は，2 個の平文に対して indistinguishability の性質を破るような多項式サイズ回路族である．一般の m についても同様．□

定理 15 数列生成オラクル上の暗号系 (G,E,D,V) が m 個の平文に対して *super-indistinguishability* の性質を持つとする．このとき (G,E,D,V) は m 個の平文に対して *semantically secure* である．

Proof: 定理 14 の証明とほぼ同じ．$v_e(r)$ の計算する替りに別の乱数 r' を利用して 2 番目の暗号化を行うことだけが異なる．□

定理 16 V が *m-semi-random* な数列生成オラクル上の暗号系 (G,E,D,V) を考える．このとき m 個の平文に対して *indistinguishability* の性質を持つことと m 個の平文に対して *super-indistinguishability* の性質を持つことは同値である．

Proof: (G,E,D,V) が m 個の平文に対して indistinguishability の性質を持つならば m 個の平文に対して super-indistinguishability の性質を持つことの対偶を $m=2$ の場合について示す．ある多項式 $p(\cdot)$ が存在し，ある多項式サイズ回路族 $\{D_n\}$ が存在し無限の多くの n で以下が成立するとする．

$$\begin{aligned}
&|\Pr[D_n(E_e(x,r),E_e(y,r')) = 1] \\
&\quad - \Pr[D_n(E_e(\tilde{x},r),E_e(\tilde{y},v_e(r))) = 1]| > \frac{1}{p(n)}.
\end{aligned}$$

今 $x=\tilde{x}$ かつ $y=\tilde{y}$ とすると，D_n と E_e を利用して (r,r') と $(r,v_e(r))$ を区別する多項式サイズ回路が構成できてしまい，F が 2-semi-random であることに矛盾してしまう．よって少くとも $x \neq \tilde{x}$ または $y \neq \tilde{y}$ となる．F が 2-semi-random なので，$p(n) < q(n)$ なる多

項式 $q(n)$ においても

$$|\Pr[D_n(E_e(x,r),E_e(y,r'))=1] - \Pr[D_n(E_e(x,r),E_e(y,v_e(r)))=1]| < \frac{1}{q(n)}$$

が成立する．よってある多項式 $p'(n)$ が存在して

$$|\Pr[D_n(E_e(x,r),E_e(y,v_e(r)))=1] - \Pr[D_n(E_e(\tilde{x},r),E_e(\tilde{y},v_e(r)))=1]| > \frac{1}{p(n)} - \frac{1}{q(n)} > \frac{1}{p'(n)}$$

となり，2 個の平文に対して indistinguishability の性質を破る多項式サイズ回路族が存在することになる．

逆方向も同様に示すことができる．また，一般の m についても同様．□

5 応用

ElGamal 暗号 [4] は Diffie-Hellman 判定問題 ([2] などを参照) が難しいという仮定の元で semantically secure であることが証明されている [12] [1]．Diffie-Hellman 判定問題とは，直観的に言うと，(g,g^a,g^b,g^{ab}) と (g,g^a,g^b,g^c) を識別する問題のことである．乱数を擬似乱数 (数列生成オラクル) へ置換した場合の ElGamal 暗号の一方向的安全性については [9] において既に議論されている．ここでは ElGamal 暗号の際に利用する乱数を数列生成オラクルに置換した場合の semantic security について考察する．

まずはオリジナルの ElGamal 暗号の記述を以下に与える．

鍵生成：素数 p，生成元 $g \in Z_p^*$，$x \in Z_{p-1}$ を選択し，$y = g^x \bmod p$ とする．公開鍵は $\langle p,g,y\rangle$ で秘密鍵は x である．

暗号化：まず，$r \in Z_{p-1}$ を一様ランダムに選択する．メッセージ m に対して暗号化関数

$$E(\langle p,g,y\rangle,m,r) = (g^r \bmod p,\ y^r m \bmod p)$$

で暗号化する．

復号：受け取った暗号文 (c_m,c_r) に対して復号関数

$$D(\langle p,g,y\rangle,x,c_m,c_r) = c_m/(c_r)^x \bmod p$$

で復号する．このままでは semantically secure でないが，Z_p^* の奇数位数部分群を利用すれば semantically secure にすることができる．(が，ここでは本質の関係ないので割愛する．)

最も単純な数列生成オラクルの例として線形合同法を考える．線形合同法は $r_i = ar_{i-1}+b \bmod m$ の形の数列 $\{r_i\}$ を生成する．ただし，m は正整数で $a,b,s_0 \in Z_m$ とする．ここでは，線形合同法の様々な性質については言及しない．線形合同法の詳細については [8] などの教科書を参照のこと．この場合，$V_{lc}(\mathsf{init},e)$ は (r,λ) を内部状態とし r を返すものとする．ただし，r は Z_{p-1} から一様に選択される．また，内部状態 (r,λ) のとき $V_{lc}(\mathsf{next},e)$ は $r' = ar+b \bmod (p-1)$ を返し，内部状態を (r',λ) とする．ただし，a,b は e (と p) から一意的に決めるものとする．このとき，数列生成オラクル V_{lc} 上の ElGamal 暗号は 2 個の平文に対して semantically secure でないことが容易に確かめられる．定義において $h(X_1,X_2) = X_1$，$f(X_1,X_2) = X_2$ とすればよい．よって，2 個の平文に対して indistinguishability の性質も持っていないことも示せる．

もう一つ数列生成オラクルを考えよう．$V_{ddh}(\mathsf{init},e)$ は (r,a) を内部状態とし r を返すものとする．r は Z_p^* から，a は Z_{p-1} から一様ランダムに選択する．内部状態 (r,a) から $V_{ddh}(\mathsf{next},e)$ は $r' = r^a \bmod p$ を返し，内部状態を (r',a) に更新する．このようにすると，$(r,v_e(r))$ と (r,r') を識別する問題はまさに Diffie-Hellman 判定問題であり，ElGamal 暗号においては Diffie-Hellman 判定の困難性を前提にしているので V_{ddh} は 2-semi-random である．数列生成オラクル V_{lc} 上の ElGamal 暗号は 2 個の平文に対して indistinguishability あるいは super-indistinguishability を持つことは容易に示すことができ，結局，2 個の平文に対して semantically secure であるがことが保証される．

ここで，擬似乱数の強度が導入できる．

定義 17 数列生成オラクル上の暗号系 (G,E,D,V) の on-line degree $od(G,E,D,V)$ とは (G,E,D,V) が m 個の平文に対して semantically secure であるような最大の m の値とする．

このようにすると $od(\mathrm{ElGamal},V_{lc}) = 1$ であり，$od(\mathrm{ElGamal},V_{ddh}) \geq 2$ と言える．

6 単一平文での安全性への帰着

通常の乱数モデルでは hybrid argument により m 個の平文に対して indistinguishabile であることと 1 つの平文に対して indistinguishabile が等価であることが証明することができる．数列生成オラクルモデルの元では一般に hybrid argument によってこの等価性は証明されないが，特殊な状況においては hybrid argument が適用できる．

定義 18 数列生成オラクル上の暗号系 (G,E,D,V) が m-generable であるとはある多項式時間アルゴリズム A が存在して，すべての多項式 $p(\cdot)$ に対して，十分大きな n で以下が成立するときを言う．任意の $x_1,x_2,\ldots,x_m$

[1] オリジナルの ElGamal 暗号についてではなく修正が施されている

と $1 \leq i \leq m$ に対して

$$\max_Z\{|\Pr[A(E(x_i, v^{i-1}(r)), x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m) \in Z] - \Pr[(E(x_1, r), E(x_2, v(r)), \ldots, E(x_m, v^{m-1}(r))) \in Z]|\} < \frac{1}{p(n)}.$$

ただし，確率は r の一様ランダムな選択上で考える．

定理 19 数列生成オラクル上の暗号系 (G, E, D, V) が *m-generable* であるならば，m 個の平文に対して *indistinguishabile* であることと 1 個の平文に対して *indistinguishabile* であることは等価である．

Proof: $m = 2$ の場合の対偶を示す．ある多項式サイズ回路族 $\{D_n\}$，ある多項式 $p(\cdot)$ が存在して無限に多くの n で以下が成立するとする．

$$|\Pr[D_n(E_e(x, r), E_e(y, v_e(r))) = 1] - \Pr[D_n(E_e(\tilde{x}, r), E_e(\tilde{y}, v_e(r))) = 1]| > \frac{1}{p(n)}.$$

このとき，以下の不等式の少くとも一方が成立する．

$$|\Pr[D_n(E_e(x, r), E_e(y, v_e(r))) = 1] - \Pr[D_n(E_e(x, r), E_e(\tilde{y}, v_e(r))) = 1]| > \frac{1}{2p(n)}$$

または

$$|\Pr[D_n(E_e(x, r), E_e(\tilde{y}, v_e(r))) = 1] - \Pr[D_n(E_e(\tilde{x}, r), E_e(\tilde{y}, v_e(r))) = 1]| > \frac{1}{2p(n)}.$$

一般性を失わずに後者が成立するとする．今，次のような回路 C_n を考える．入力 $E_e(x', r)$ に対して平文 $\tilde{y}$ の暗号文 $E_e(\tilde{y}, v(r))$ を構成する．これは 2-generable であるので可能である．このとき回路 D_n に入力 $E_e(x', r)$, $E_e(\tilde{y}, v(r))$ を与え，D_n の出力をそのまま C_n の出力とする．このとき，

$$|\Pr[C_n(E_e(x, r))) = 1] - \Pr[C_n(E_e(\tilde{x}, r)) = 1]| = |\Pr[D_n(E_e(x, r), E_e(\tilde{y}, v_e(r))) = 1] - \Pr[D_n(E_e(\tilde{x}, r), E_e(\tilde{y}, v_e(r))) = 1]| > \frac{1}{2p(n)}.$$

よって 1 個の平文に対して indistinguishabile の性質を破る多項式サイズ回路族が存在することになる．一般の m についても同様． □

7 おわりに

擬似乱数生成器を使ったランダムネスの削減は，バッチ的な利用法での安全性を保証するのに対して，ここではオンライン的な利用法に適したランダムネス削減モデルを新たに導入した．擬似乱数生成器を利用したモデルにおいては多項式個の平文に対する semantic security が 1 つの平文に対する semantic security に帰着できるのに対して，数列生成オラクルモデルにおいては，(擬似ランダム関数を除き) 多項式個の平文に対する semantic security を保証する技術がいまのところなく，その手法を開発するのが課題である．

参考文献

[1] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM J. Computing*, 13(4):850–864, 1984.

[2] D. Boneh. The decision Diffie-Hellman problem. In *Lecture Notes in Computer Science 1423*, pages 48–63, 1998.

[3] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Trans. Info. Theory*, IT-22(6):644–654, 1976.

[4] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Info. Theory*, IT-31(4):469–472, 1985.

[5] O. Goldreich. Foundation of Cryptography (fragment of a book – version 2.03), 1998.

[6] O. Goldreich and M. Sudan. Computational indistinguishability: A sample hierarchy. *J. Comp. Sys. Sci.*, 59(2):253–269, 1999.

[7] S. Goldwasser and S. Micali. Probabilistic encryption. *J. Comp. Sys. Sci.*, 28(2):270–299, 1984.

[8] D. E. Knuth. *The Art of Computer Programming*, volume 2. Seminumerical Algorithms. Addison-Wesley, 3rd edition, 1998.

[9] T. Koshiba. A theory of randomness for public key cryptosystems: The ElGamal cryptosystem case. To appear in IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences.

[10] M. Luby. *Pseudorandomness and Cryptographic Applications*. Princeton Univ. Press, 1996.

[11] S. Micali, C. Rackoff, and B. Sloan. The notion of security for probabilistic cryptosystems. *SIAM J. Computing*, 17(2):412–426, 1988.

[12] Y. Tsiounis and M. Yung. On the security of ElGamal based encryption. In *Lecture Notes in Computer Science 1431*, pages 117–134, 1998.

[13] A. C. Yao. Theory and applications of trapdoor functions. In *Proc. 23rd FOCS*, pages 80–91, 1982.