# I240 暗号理論 2019
## 公開鍵暗号と署名（1）

2019/11/20 講師 藤崎

# 1 安全性の根拠となる問題

## 1.1 RSA 問題

### 1.1.1 RSA 関数

$n$ を $n = pq$ なる相異なる素数 $p, q$ の積とする。このとき、環 $\mathbb{Z}/n\mathbb{Z}$ の乗法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ の位数はオイラー関数より $\phi(n) = (p-1)(q-1)$ である。全ての $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ は、Lagrange の定理より、$\#\langle a\rangle | \phi(n)$ である。$\langle a\rangle$ の位数と $a$ の位数（$a^\lambda = 1$ となる最小の正の整数 $\lambda$）は、準同型定理より $\mathbb{Z}/\lambda\mathbb{Z} \cong \langle a\rangle$ であり等しい。さらに

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$$

であるから、$a = (a_p, a_q) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ と同一視すると、$a$ の位数 $\lambda$ は、$\lambda(n) := \mathsf{lcm}(p-1, q-1)$ の約数であるから、全ての $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対して、$a^{\lambda(n)} \equiv 1 \pmod{n}$ が成り立つ。

**問題 1** 位数がちょうど $\lambda(n)$ となる $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ はどんな値か。

**定義 2** 整数 $e$ を $\gcd(e, \lambda(n)) = 1$ とし、

$$f_{(n,e)}(x) := x^e \bmod n$$

と定義された関数 $f_{n,e} : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ を RSA 関数と呼ぶことにする。

**補題 3** $f_{n,e}$ は $(\mathbb{Z}/n\mathbb{Z})^\times$ 上の置換（全単射写像）になる。

**(証明)**

- (単射) $f_{n,e}(x) = f_{n,e}(y)$、すなわち $x^e \equiv y^e \pmod{n}$ ならば、$x \equiv y \pmod{n}$ を示せば良い。$d := e^{-1} \bmod \lambda(pq)$ とおくと、

$$(x^e)^d \equiv x^{ed} \equiv x^{1+k\lambda(n)} \equiv x \pmod{n}.$$

  $(x^e)^d \equiv (y^e)^d \pmod{n}$ であるので、$x \equiv y \pmod{n}$ となる。
- (全射) 任意の $y \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対して、$x := y^d \bmod n$ とすると、$y = x^e \bmod n$ である。よって全射。

### 1.1.2 RSA 仮定

**定義 4（RSA 問題）** 相異なる素数 $p, q$ の積 $n = pq$、$\gcd(e, \lambda(pq)) = 1$ である奇素数 $e(\geq 3)$、$y \in (\mathbb{Z}/n\mathbb{Z})^\times$ が与えられたとき、$x^e \equiv y \pmod{n}$ なる $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ を求める問題を RSA 問題という。

$\mathsf{KGen}_{\mathrm{RSA}}$ を次のような確率的アルゴリズムとする。

1. $\mathsf{KGen}_{\mathrm{RSA}}$ はセキュリティパラメータ $1^\kappa$ を入力として受け取る。

2. $|pq| = \kappa$ となる相異なる素数 $p, q$ を、$|p| = |q|$ かつ、$\lambda(pq)$ が大きな素数の倍数となるように（ある分布から）選ぶ。ここで、正の整数 $x$ に対して、$|x| := \lfloor \log_2(x) \rfloor$（$x$ をビット列としてみたときの長さ）を表し、$\lambda(pq) := \gcd(p-1, q-1)$ とする。
3. $\gcd(e, \lambda(pq)) = 1$ なる素数 $e \geq 3$ を選ぶ。
4. $d := e^{-1} \bmod \lambda(pq)$ を計算する。
5. $n := pq$ として、$pk := (n, e)$ と $sk := (pk, d)$ を出力する。

$\mathsf{KGen}_{\mathrm{RSA}}$ を RSA 鍵生成アルゴリズムと呼び、このアルゴリズムの試行を

$$(pk, sk) \leftarrow \mathsf{KGen}_{\mathrm{RSA}}(1^\kappa).$$

と書く [*1]。

RSA 仮定とは次のように定義される。

**定義 5（RSA 仮定）** $\mathsf{KGen}_{\mathrm{RSA}}$ を上記のようなアルゴリズムとする。RSA 問題を解くアルゴリズム $A$ の成功確率を

$$\mathsf{Adv}^{\mathsf{ow}}_{A,\mathsf{KGen}_{\mathrm{RSA}}}(\kappa) := \Pr[(pk, sk) \leftarrow \mathsf{KGen}_{\mathrm{RSA}}(1^k);\, y \leftarrow (\mathbb{Z}/n\mathbb{Z})^\times :\, A(pk, y) = y^d \in (\mathbb{Z}/n\mathbb{Z})^\times.]$$

と定義する。ある鍵生成アルゴリズム $\mathsf{KGen}_{\mathrm{RSA}}$ が存在して、いかなる多項式時間アルゴリズムの敵 $A$ に対しても $\mathsf{Adv}^{\mathsf{ow}}_{A,\mathsf{KGen}_{\mathrm{RSA}}}(\kappa) = \mathsf{negl}(\kappa)$ となるとする。このような鍵生成アルゴリズム $\mathsf{KGen}_{\mathrm{RSA}}$ の存在を仮定することを RSA 仮定と言う。

RSA 仮定とは、ある鍵生成アルゴリズム $\mathsf{KGen}_{\mathrm{RSA}}$ が存在して、それにより作られる関数族 $f_{n,e}$ が、一方向性関数であると仮定することと同義である。

特に、任意の $t$-時間アルゴリズム（の族）$A$ に対して、$\mathsf{Adv}^{\mathsf{ow}}_{A,\mathsf{KGen}_{\mathrm{RSA}}}(\kappa) \leq \epsilon$ であるならば、（$\mathsf{KGen}_{\mathrm{RSA}}$ により導出される）RSA 関数（族）$f_{n,e}$ は $(t, \epsilon)$-OW であるという。

$$f^{-1}_{n,e}(x) = x^d \pmod{n}$$

は効率よく計算できる（バイナリー法）。$f^{-1}_{n,e}$ を関数 $f_{n,e}$ の落し戸 (trapdoor) とよぶ。

**定義 6（落し戸付き一方向性関数（One-Way Trapdoor Function））** 落し戸をもつ一方向性関数（族）を、落し戸付き一方向性関数（族）とよぶ。

## 1.2 離散対数問題、DH 問題、DDH 問題

### 1.2.1 巡回群

$G$ を有限群とする（演算は乗法で表す）このとき、$\langle g \rangle$（$g \in G$）は、$G$ の有限可換部分群であり、準同型定理により、$\langle g \rangle$ の位数と $g$ の位数は一致し（それを $q$ とおく）、

$$f : x \in \mathbb{Z}/q\mathbb{Z} \to g^x \in \langle g \rangle$$

は同型写像である（$\mathbb{Z}/q\mathbb{Z}$ は加法で定義された群）。今後、$G_q := \langle g \rangle$ と書くことにする。我々は、$q$ が素数となるようなものに特に興味がある。Lagrange の定理により、群 $G_q$ の部分群を $H$ とすると、$\#H | q$. $q$ は素数

[*1] 実際は、$e, p, q$ の選び方にさらなる制限がついているが細かいことは今回は気にしない。

であるから、$H$ は、$\{1\}$ または $G_q$ のどちらかである。よって、任意の $g' \in G_q \backslash \{1\}$ は $G_q$ の生成元であり、$\langle g' \rangle = G_q$.

**具体例 1:** 有限体 $\mathbb{F}_p (= \mathbb{Z}/p\mathbb{Z})$（$p$ は素数）を考える。有限体の乗法群は巡回群であるので、乗法群 $\mathbb{F}_p^\times$ はある生成元 $\tilde{g} \in \mathbb{F}_p^\times$ が存在し、$\langle \tilde{g} \rangle = \mathbb{F}_p^\times$ となる。体では、$\mathbb{F}_p^\times = \mathbb{F}_p \backslash \{0\}$ であるから、$\#\mathbb{F}_p^\times = p-1$ である。$q$ を $q|p-1$ なる奇素数とする。すると、$g := \tilde{g}^k$（$p-1 = qk$）と置くと、$f(x) = g^x \bmod p$ は、

$$f : x \in \mathbb{Z}/q\mathbb{Z} \to g^x \in G_q (= \langle g \rangle)$$

の同型写像である。

**具体例２:** $E(\mathbb{F}_p)$ を、有限体 $\mathbb{F}_p$ 上の楕円曲線 $E$ の $\mathbb{F}_p$-有理点から作られる群とする。Hasse の定理により、$E(\mathbb{F}_p)$ の位数は $p+1-2\sqrt{p} \le \#E(\mathbb{F}_p) \le p+1+2\sqrt{p}$ である。$q|\#E(\mathbb{F}_p)$ なる素数を位数とする $P \in E(\mathbb{F}_p)$ の作る巡回群を $\langle P \rangle = G_q$ と置くと、

$$f : x \in \mathbb{Z}/q\mathbb{Z} \ \to \ xP \in G_q \subset E(\mathbb{F}_p)$$

は $\mathbb{Z}/q\mathbb{Z}$ から $G_q$ への同型写像である。

### 1.2.2 離散対数問題、DH 問題、DDH 問題

**定義 7（離散対数 (Discrete-log (DL)) 問題）** $G_q$ を素数位数 $q$ の巡回群（演算を乗法で書くことにする）とする。元 $g, h \in G_q$ が与えられたとき、$h = g^x$ なる $x \in \mathbb{Z}/q\mathbb{Z}$ を求める問題を $G_q$ 上の離散対数問題という。

$h = g^x$ なる $x$ を、$x = \log_g(h)$ と書く。

**定義 8（Diffie-Hellman (DH) 問題）** $G_q$ を素数位数 $q$ の巡回群（演算を乗法で書くことにする）とする。元 $g, h_1, h_2 \in G_q$ が与えられたとき、$k = g^{xy} = h_2^x = h_1^y$ なる $k \in G_q$ を求める問題を $G_q$ 上の DH 問題という。ここで、$x := \log_g(h_1)$, $y := \log_g(h_2)$ とする。

別の言い方をすると、$g$, $h_1 = g^x$, $h_2 = g^y$ から、$x, y$ は教えられずに $g^{xy}$ を計算する問題を DH 問題という。

**定義 9（Decisional Diffie-Hellman (DDH) 問題）** $G_q$ を素数位数 $q$ の巡回群（演算を乗法で書くことにする）とする。$G_q$ の元 $g_1, g_2, h_1, h_2 \in G_q$ に対して、$\log_{g_1}(h_1) = \log_{g_2}(h_2)$ であるとき、DDH 関係を満たしているという。

$$\mathrm{DDH}(G_q^4) := \{(g_1, g_2, h_1, h_2) \in G_q^4 \mid \log_{g_1}(h_1) = \log_{g_2}(h_2)\}.$$

DDH 関係か、否かを判定する問題を $G_q$ 上の DDH 問題という。

$G_q$ の元の 4 つ組の集合 $G_q^4 = \{(g_1, g_2, h_1, h_2) \mid g_1, g_2, h_1, h_2 \in G_q\}$ とすると、$\mathrm{DDH}(G_q^4) \subset G_q^4$.

**注釈 10** DDH 関係とは、図 1 のように 4 元のうち 3 元を選んだとき、最後の 1 元が DH 問題の解になっている関係と言い直すことができる。

$\mathsf{KGen}_{\mathsf{group}}$ を次のような確率的アルゴリズムとする。

1. $\mathsf{KGen}_{\mathsf{group}}$ はセキュリティパラメータ $1^\kappa$ を入力として受け取る。
2. $|q| = \kappa$ となる素数と、$q$ を位数とする巡回群 $G_q$ を選ぶ。
3. $(G_q, , q)$ を出力する。

このアルゴリズムの試行を

$$(G_q, q) \leftarrow \mathsf{KGen}_{\mathsf{group}}(1^\kappa)$$

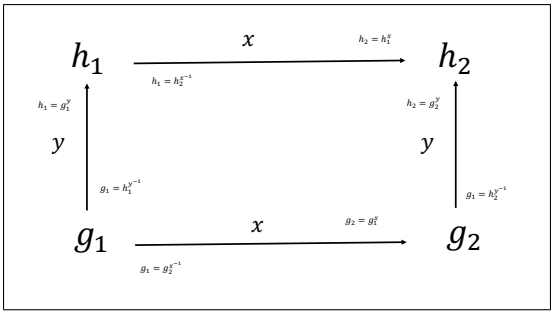


図 1　DDH 関係の図

と書く。

**定義 11（DL 仮定）** DL 問題を解くアルゴリズム $A$ の成功確率を

$$\mathsf{Adv}^{\mathrm{DL}}_{A,\mathsf{KGen}_{\mathsf{group}}}(\kappa) := \Pr[(G_q, q) \leftarrow \mathsf{KGen}_{\mathsf{group}}(1^\kappa); (g, h) \leftarrow G_q^2; x \leftarrow A(g, h) : y = g^x]$$

と定義する。ある巡回群生成アルゴリズム $\mathsf{KGen}_{\mathsf{group}}$ が存在して、いかなる多項式時間アルゴリズムの敵 $A$ に対しても $\mathsf{Adv}^{\mathrm{DL}}_{A,\mathsf{KGen}_{\mathsf{group}}}(\kappa) = \mathsf{negl}(\kappa)$ となるとする。このような $\mathsf{KGen}_{\mathsf{group}}$ の存在を仮定することを DL 仮定と言う。

**定義 12（DH 仮定）** DH 問題を解くアルゴリズム $A$ の成功確率を

$$\mathsf{Adv}^{\mathrm{DH}}_{A,\mathsf{KGen}_{\mathsf{group}}}(\kappa) := \Pr[(G_q, q) \leftarrow \mathsf{KGen}_{\mathsf{group}}(1^\kappa); (g, h_1, h_2) \leftarrow G_q^3 : A(g, h_1, h_2) = g^{xy}]$$

と定義する（ただし $x = \log_g(h_1)$, $y = \log_g(h_2)$）。ある巡回群生成アルゴリズム $\mathsf{KGen}_{\mathsf{group}}$ が存在して、いかなる多項式時間アルゴリズムの敵 $A$ に対しても $\mathsf{Adv}^{\mathrm{DH}}_{A,\mathsf{KGen}_{\mathsf{group}}}(\kappa) = \mathsf{negl}(\kappa)$ となるとする。このような $\mathsf{KGen}_{\mathsf{group}}$ の存在を仮定することを DH 仮定と言う。

**定義 13（DDH 仮定）** DDH 関係を判定するアルゴリズム $D$ の成功確率を

$$\mathsf{Adv}^{\mathrm{DH}}_{D,\mathsf{KGen}_{\mathsf{group}}}(\kappa) := |\Pr_{G_q, U_{\mathrm{DDH}}(G_q^4)}[D(U_{\mathrm{DDH}}(G_q^4)) = 1] - \Pr_{G_q, U(G_q^4)}[D(U(G_q^4)) = 1]|$$

と定義する。ただし、$G_q$ は、$\mathsf{KGen}_{\mathsf{group}}(1^\kappa)$ の分布に従った確率変数、$U_{\mathrm{DDH}}(G_q^4)$ は、$\mathrm{DDH}(G_q^4)$ 上の一様分布に従う確率変数、$U(G_q^4)$ は、$G_q^4$ 上の一様分布に従う確率変数である。ある巡回群生成アルゴリズム $\mathsf{KGen}_{\mathsf{group}}$ が存在して、いかなる多項式時間アルゴリズムの敵 $D$ に対しても $\mathsf{Adv}^{\mathrm{DDH}}_{D,\mathsf{KGen}_{\mathsf{group}}}(\kappa) = \mathsf{negl}(\kappa)$ となるとする。このような $\mathsf{KGen}_{\mathsf{group}}$ の存在を仮定することを DDH 仮定と言う。

# 2　公開鍵暗号

## 2.1　公開鍵暗号の定義

$\Pi = (\mathbf{K}, \mathbf{E}, \mathbf{D})$ はセキュリティパラメータ $\kappa \in \mathbb{N}$ に依存する三つのアルゴリズムの組みであり次のように定義される：

- 鍵生成アルゴリズム $\mathbf{K}$: $1^\kappa$ を入力としてとり、$(pk, sk)$ を出力する確率的多項式時間アルゴリズム。この試行を $(pk, sk) \leftarrow \mathbf{K}(1^\kappa)$ と書く。$(pk, sk)$ をそれぞれ公開鍵、秘密鍵と呼ぶ。

- 暗号化アルゴリズム $\mathbf{E}$: 公開鍵 $pk$ と $m \in \mathcal{M}$ を入力としてとり、$\mathsf{ct}$ を出力する確率的多項式時間アルゴリズム。この試行を $\mathsf{ct} \leftarrow \mathbf{E}_{pk}(m)$ と書く。$m$ を平文、$\mathsf{ct}$ を暗号文と呼ぶ。
- 復号化アルゴリズム $\mathbf{D}$: 秘密鍵 $sk$ と暗号文 $\mathsf{ct} \in \mathcal{C}$ を入力としてとり $m$ を出力する確定的多項式時間アルゴリズム。この試行を $m \leftarrow \mathbf{D}_{sk}(\mathsf{ct})$ と書く。

平文空間 $\mathcal{M}$ と暗号文空間 $\mathcal{C}$ は $pk$ に依存して $\{0,1\}^*$ の部分集合として一意に定まるものとする。

**定義 14** $\Pi = (\mathbf{K}, \mathbf{E}, \mathbf{D})$ が、十分大きな全てのセキュリティパラメータ $\kappa \in \mathbb{N}$ に対して、$(pk, sk) \in \mathbf{K}(1^\kappa)$, $m \in \mathcal{M}$, $\mathsf{ct} \in \mathbf{E}_{pk}(m)$ なら $\mathbf{D}_{sk}(\mathsf{ct}) = m$ を常に満足する **(Correctness)** とき、$\Pi$ を**公開鍵暗号**とよぶ。

## 2.2 教科書的 RSA 暗号と El Gamal 暗号

### 2.2.1 RSA 暗号

一方向性落とし戸置換族は, 公開鍵暗号の定義を満たすので、RSA 関数から公開鍵暗号を容易に作れる。鍵生成アルゴリズムを $\mathbf{K} = \mathsf{KGen}_{\mathrm{RSA}}$ とする。暗号化アルゴリズム $\mathbf{E}_{pk}(m) := f_{n,e}(m) = m^e \bmod n$（ここで、$pk = \{n, e\}$）。復号アルゴリズム $\mathbf{D}_{sk}(c) := f_{n,e}^{-1}(c) = c^d \bmod n$（ここで、$sk = \{pk, d\}$）。

### 2.2.2 El Gamal 暗号

El Gamal 暗号 $\Pi = (\mathbf{K}, \mathbf{E}, \mathbf{D})$ は次のようなアルゴリズムの組である。それぞれのアルゴリズムの試行は図 2 になる。ここで、$\mathcal{M} = G_q$、$\mathcal{C} = G_q \times G_q$ であり、$\mathbf{E}_{pk}(m; r) = (g^r, m \cdot h^r)$、$\mathbf{D}_{sk}(\mathsf{ct}) = c_2 / c_1^x$ となる。

| | | |
|---|---|---|
| $(pk, sk) \leftarrow \mathbf{K}(1^\kappa)$. | $\mathsf{ct} \leftarrow \mathbf{E}_{pk}(m)$. | $m \leftarrow \mathbf{D}_{sk}(\mathsf{ct})$. |
| Input $1^\kappa$. | | |
| $(G_q, q) \leftarrow \mathsf{KGen}_{\mathsf{group}}(1^\kappa)$; | Input $(pk, m)$. | Input $(sk, \mathsf{ct})$. |
| $g \leftarrow G_q \backslash \{1\}$; $x \leftarrow \mathbb{Z}/q\mathbb{Z}$; | $r \leftarrow \mathbb{Z}/q\mathbb{Z}$; | Parse $\mathsf{ct} = (c_1, c_2)$; |
| $h := g^x$; | $c_1 := g^r$; | $k := c_1^x$; |
| $pk := (G_q, q, g, h)$; | $k := h^r$; | $m := c_2/k$; |
| $sk := (pk, x)$; | $c_2 := m \cdot k$; | Return $m$. |
| Return $(pk, sk)$. | Return $\mathsf{ct} := (c_1, c_2)$. | |

図 2 El Gamal

## 2.3 公開鍵暗号の安全性のクラス

公開鍵暗号の安全性は, 攻撃者 (adversary) の解読目標（「部分解読」か「完全解読」等）と, 攻撃者の利用可能な環境（選択平文攻撃, 選択暗号文攻撃）の 2 つの独立な要素の組み合わせによって定義される。「解読目標」には,「一方向性（ one-wayness, 完全解読不可)」,「識別不可能性（ indistinguishability, いかなる部分解読も不可)」,「頑強性（ non-malleability )」などが存在する。一方, 攻撃者の環境には,「受動的攻撃（選択平文攻撃 (chosen-plaintext attack) 」,「非適応的選択暗号文攻撃 (non-adaptive chosen-ciphertext attack or lunch-time attack) 」,「適応的選択暗号文攻撃 (adaptive chosen-ciphertext attack) 」などがある。

**■識別不可能性** (indistinguishability) 公開鍵暗号が暗号が通信情報を秘匿するものであることを鑑みると, 一方向性は暗号の安全性を定義するのに十分な概念とは言えない。公開鍵暗号のいかなる部分情報解読も不可で

あることを示すのに, 次のようなゲームが利用される。

**[公開鍵暗号 $\Pi$ の識別ゲーム]**　ゲームは, 攻撃者 $A$ と攻撃者に問題を与える挑戦者 $S$ からなる。

1. 挑戦者 $S$ は, $\mathbf{K}$ を起動して $(pk, sk) \leftarrow \mathbf{K}(1^k)$ を得た後, 攻撃者 $A$ に $pk$ を与える。
2. 攻撃者 $A$ は, 二つの平文 $m_0, m_1 \in \mathcal{M}$ を出力する。
3. 挑戦者 $S$ は, コイン $b \in \{0,1\}$ をふり, $m_0, m_1$ のどちらを暗号化するか決める。
4. 攻撃者 $A$ に $\mathbf{E}_{pk}(m_b)$ を入力する。
5. 攻撃者 $A$ は, ビット $b' \in \{0,1\}$ を出力する。
6. $b = b'$ の時, $A$ の勝利, それ以外のときは $S$ の勝利とする。

仮に, $\Pi$ がいかなる部分情報も漏らさないのであれば, $A$ が勝利できる確率は, 高々 $1/2$ である。$A$ の $1/2$ を超えて勝利できる確率を, $A$ の成功確率として（以下に詳しく）定義する。しかしまず, このゲームにバリエーションを与えてやることを考える。

**■選択平文攻撃・（適応的）選択暗号文攻撃**　$A$ が, 暗号化オラクル $\mathbf{E}_{pk}$, 復号化オラクル $\mathbf{D}_{sk}$ を利用できるかで, 上記のゲームは二つのバリエーションができる。暗号化オラクル $\mathbf{E}_{pk}$ を利用できる環境を, 選択平文攻撃という。一方, 復号化オラクル $\mathbf{D}_{sk}$ を利用できる環境を, 選択暗号文攻撃という。

公開鍵暗号では, $A$ は $pk$ を知っているので, 自分で $\mathbf{E}_{pk}$ を利用して任意の平文 $m$ を暗号化できる。よって選択平文攻撃はもっとも弱い $A$ の攻撃法である。

選択暗号文攻撃では, $A$ は上記のゲームにおいていかなる時でも, 復号化オラクル $\mathbf{D}_{sk}$ を利用できる。唯一の制限は, ステップ (4) で入力された暗号文 $\mathbf{E}_{pk}(m_b)$ を復号化オラクルに質問してはいけないということである。通常このような攻撃法を適応的選択暗号文攻撃 (adaptive chosen-ciphertext attack) と呼ぶが, ここでは単に選択暗号文攻撃 (chosen-ciphertext attack) と呼ぶことにする。

**■IND-CPA-安全, IND-CCA-安全**　以下は, 環境が $b$ を選んだとき, 選択平文（および暗号文）攻撃で攻撃者 $A$ がビット $b'$ を出力する事象をあらわしている。

$A^{\mathsf{cpa}}(\mathbf{E}_{pk}(m_b)) = b' \Leftrightarrow$

$$(pk, sk) \leftarrow \mathbf{K}(1^k);\ (m_0, m_1) \leftarrow A(pk):\ A(pk, \mathbf{E}_{pk}(m_b)) = b'.$$

$A^{\mathsf{cca}}(\mathbf{E}_{pk}(m_b)) = b' \Leftrightarrow$

$$(pk, sk) \leftarrow \mathbf{K}(1^k);\ (m_0, m_1) \leftarrow A^{\mathbf{D}_{sk}}(pk):\ A^{\mathbf{D}_{sk}}(pk, \mathbf{E}_{pk}(m_b)) = b'.$$

$P_b^{\mathsf{cpa}} := \Pr[A^{\mathsf{cpa}}(\mathbf{E}_{pk}(m_b)) = 1]$, $P_b^{\mathsf{cca}} := \Pr[A^{\mathsf{cca}}(\mathbf{E}_{pk}(m_b)) = 1]$ と定義し, 攻撃者 $A$ の $\Pi$ に対する選択平文（および選択暗号文）攻撃成功確率を

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{A,\Pi}(k) := |P_1^{\mathsf{cpa}} - P_0^{\mathsf{cpa}}|$$
$$\mathsf{Adv}^{\mathsf{ind\text{-}cca}}_{A,\Pi}(k) := |P_1^{\mathsf{cca}} - P_0^{\mathsf{cca}}|$$

と定義する。上記確率は $\mathbf{K}, \mathbf{E}_{pk}, A$（の内部コインに）依存する。

**定義 15**　任意の $t(k)$-時間アルゴリズム(族)の攻撃者 $A$ に対して, 十分大きな全ての $k \in \mathbb{N}$ で, $\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{A,\Pi}(k) \leq \epsilon(k)$ が成立するとき, 公開鍵暗号 $\Pi$ は, $(t(k), \epsilon(k))$-IND-CPA-安全であるという。

特に $t : \mathbb{N} \to \mathbb{R}^+$ が多項式制限, $\epsilon : \mathbb{N} \to \mathbb{R}^+$ が無視できる関数のとき, $\Pi$ は IND-CPA-安全であるという。

同様に, IND-CCA-安全を定義する。

**定義 16**　攻撃者 $A$ は $t(k)$-時間アルゴリズムで, 作動時間内に $q(k)$ 回まで復号オラクルにアクセスできるとする。任意の $t(k)$-時間アルゴリズム (族) の攻撃者 $A$ に対して, 十分大きな全ての $k \in \mathbb{N}$ で, $\mathsf{Adv}^{\mathsf{ind\text{-}cca}}_{A,\Pi}(k) \leq \epsilon(k)$ が成立するとき, 公開鍵暗号 $\Pi$ は, $(t(k), q(k), \epsilon(k))$-IND-CCA-安全であるという。ただし, $q(k)$ はセキュリティパラメータが $k$ のときの $A$ の復号オラクル $\mathbf{D}_{sk}$ への質問回数を示す。

特に $t : \mathbb{N} \to \mathbb{R}^+$ が多項式制限, $\epsilon : \mathbb{N} \to \mathbb{R}^+$ が無視できる関数, さらに $q : \mathbb{N} \to \mathbb{N}$ が多項式制限であるとき, $\Pi$ は IND-CCA-安全であるという。

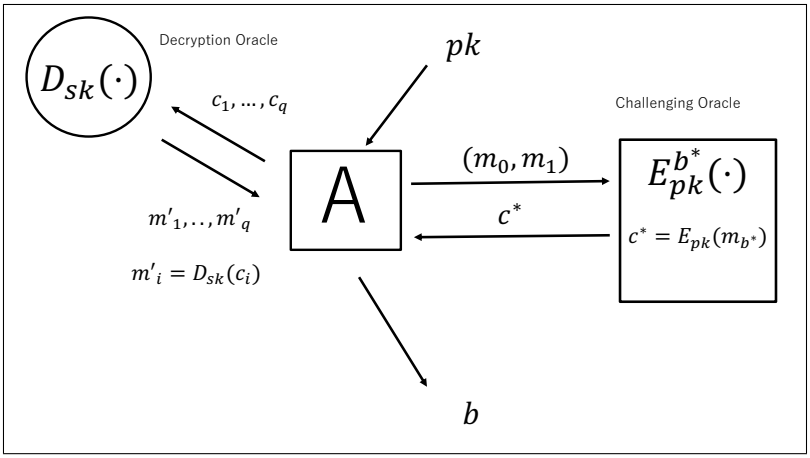


図 3　IND-CCA 安全性モデル

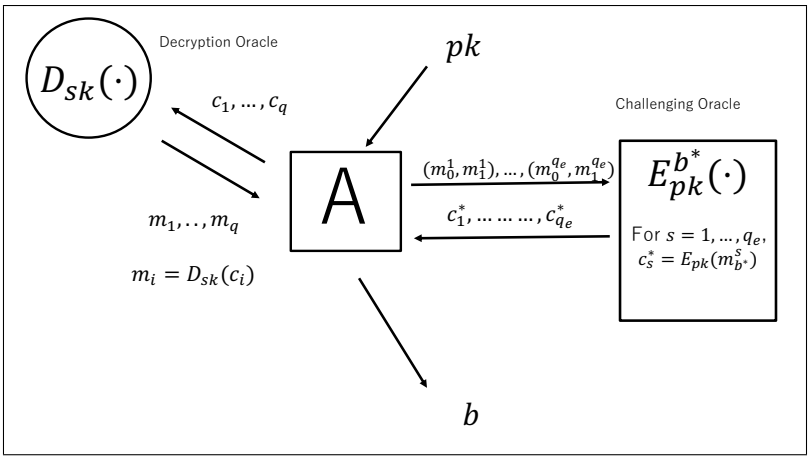


図 4　複数チャレンジ IND-CCA 安全性モデル

## 2.4　Blum-Goldwasser 暗号

$f : \{0,1\}^* \to \{0,1\}^*$ を一方向性落とし戸付き置換とする（本当は置換の族であるが省略)。$b : \{0,1\}^* \to \{0,1\}$ を $f$ のハードコア述語とする。関数 $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ を

$$G(x) := \quad \Big(b(x),\, b(f^1(x)),\, \ldots,\, b(f^{\ell-1}(x))\Big) \in \{0,1\}^{\ell}$$

と定義する。すると, $pk = \{f\}$, $sk = \{f^{-1}\}$, $\mathcal{M} = \{0,1\}^{\ell}$, $\mathsf{CT} = \{0,1\}^{n+\ell}$, $\mathbf{E}_{pk}(x;r) := (f^{\ell}(x), m \oplus G(x))$ (ただし $f^i(x) := \overbrace{f(\ldots(f}^{i}(x)\ldots))$ で公開鍵暗号が定義できる。復号アルゴリズム $\mathbf{D}_{sk}$ は, $y := f^{\ell}(x)$, $c = m \oplus G(x)$ とすると, $D_{sk}(y,c) := c \oplus \Big(b(f^{-\ell}(y)),\ \ldots,\ b(f^{-1}(y))\Big)$ となる。

**定理 17**　$f$ が，一方向性落とし戸付き置換で, $b$ が $f$ のハードコア述語であれば, BG 暗号は，CPA 安全な公開鍵暗号である。

この定理は下記の補題から容易に導ける。

**補題 18**　一方向性置換 $f$ のハードコア述語 $b$ を $(t,\epsilon)$-HC と仮定する。すると, 確率変数 $(f(U_n), G(U_n))$ と $(f(U_n), U_\ell)$　は, $(t',\epsilon')$-計算量的識別不可で,

$$t'(n) = t(n) - (\ell(n)-1)\tau_f(n) - \tau_R(n),$$
$$\epsilon'(n) \leq \epsilon(n)\ell(n).$$

である。ここで, $U_n$, $U_\ell$ は, それぞれ $\{0,1\}^n$, $\{0,1\}^{\ell}$ 上の一様分布に従って選ばれた独立な確率変数であり, $\tau_f(n)$ は $f$ を一回実行する計算時間, $T_R(n)$ は, $n$ ビットの乱数列の生成時間をあらわす。

# 3　ディジタル署名

## 3.1　ディジタル署名の定義

$\mathsf{SIG} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$ をセキュリティパラメータ $\kappa \in \mathbb{N}$ に依存する三つのアルゴリズムの組とし次のように定義する：

- 鍵生成アルゴリズム KGen: $1^{\kappa}$ を入力としてとり、検証鍵と署名鍵 $(vk, sk)$ を出力する確率的多項式時間アルゴリズム。この試行を $(vk, sk) \leftarrow \mathsf{KGen}(1^k)$ と書く。
- 署名生成アルゴリズム Sign: 署名鍵 $sk$ と 平文 $m \in \{0,1\}^*$ を入力としてとり，署名 $\sigma$ を出力する確率的多項式時間アルゴリズム。この試行を $\sigma \leftarrow \mathsf{Sign}(sk, m)$ と書く。
- 署名検証アルゴリズム Vrfy: 検証鍵 $vk$, 平文と署名の組 $(m, \sigma)$ を入力としてとり，承認か拒絶を意味する 1 ビットを出力する確定的多項式時間アルゴリズム。この試行を $b \leftarrow \mathsf{Vrfy}(vk, m, \sigma)$ と書く。

**定義 19**　$\mathsf{SIG} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$ が、十分大きな全ての $\kappa \in \mathbb{N}$ に対して、$(vk, sk) \in \mathsf{KGen}(1^k)$、$m \in \{0,1\}^*$、$\sigma \in \mathsf{Sign}(sk, m)$ なら、常に $\mathsf{Vrfy}(vk, m, \sigma) = 1$ を満足するとき、SIG を**ディジタル署名**とよぶ。

## 3.2　ディジタル署名の安全性のクラス

■EUF-CMA **安全性**　ディジタル署名 SIG に対する次のような攻撃者 $A$ を考える。$A$ は検証鍵 $vk$ を受け取り, 署名オラクル $\mathsf{Sign}_{sk}$ に $q$ 回まで平文を送ることができる。署名オラクル $\mathsf{Sign}_{sk}$ は各質問された平文に正しい署名をそのつど返す。$A$ の署名オラクル $\mathsf{Sign}_{sk}$ へ質問した平文と対応する署名の集合を $L = \{(m_1, \sigma_1), \ldots, (m_q, \sigma_q)\}$ とし、平文の集合を特に $L(m) = \{m_1, \ldots, m_q\}$ と書くことにする。$A$ が最終的に $L(m)$ に含まれない平文 $m^*$ への正しい署名 $\sigma^*$ （正しい署名とは, $\mathsf{Vrfy}(vk, m^*, \sigma^*) = 1$ なる署名のこと）を出力して来た場合、$A$ の勝ちと定義する。

$A$ が、ディジタル署名 SIG に対する EUF-CMA ゲームに勝つ確率を、$A$ の SIG に対するアドバンテージ

と呼び、$\mathsf{Adv}^{\mathsf{euf\text{-}cma}}_{A,\mathsf{SIG}}(\lambda) :=$

$$\Pr[(vk, sk) \leftarrow \mathsf{KGen}(1^\kappa); (m^*, \sigma^*) \leftarrow A^{\mathsf{Sign}_{sk}}(vk) : \mathsf{Vrfy}(vk, m^*, \sigma^*) = 1 \wedge m^* \notin L(m)]$$

によって表す。上記確率は, $\mathsf{KGen}, \mathsf{Sign}, A$（の内部コイン）に依存する。

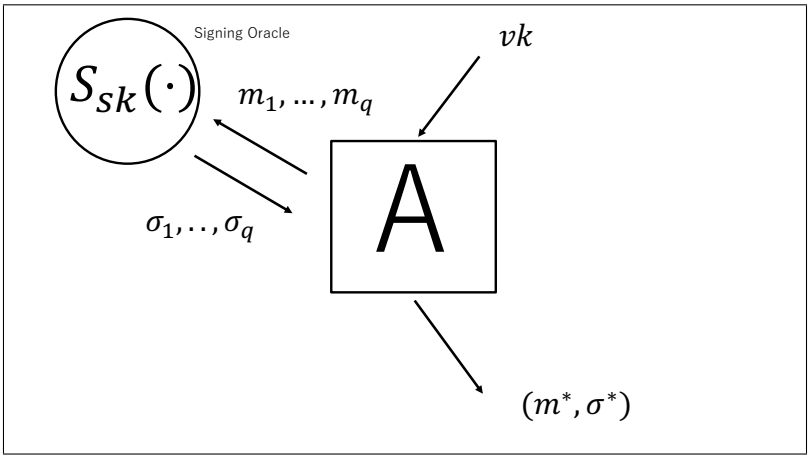


図 5　EUF-CMA 安全性モデル

**定義 20（EUF-CMA 安全性）** 署名オラクルに $q$ 回までアクセスできる任意の $t$-時間アルゴリズム（族）の攻撃者 $A$ に対して, 十分大きな全ての $\kappa$ で, $\mathsf{Adv}^{\mathsf{euf\text{-}cma}}_{A,\mathsf{SIG}}(\kappa) \leq \epsilon$ が成立するとき、ディジタル署名 SIG は $(t, q, \epsilon)$-**EUF-CMA 安全**という。特に, $t, q = O(\mathrm{poly}(\kappa))$ で、$\epsilon(\kappa) = \mathsf{negl}(\kappa)$ であるとき、SIG は EUF-CMA **安全**、または**選択平文攻撃 (chosen-message attack) に対して存在的偽造不可 (existentially-unforgeable)** という。

**■sEUF-CMA 安全性**　sEUF-CMA ゲームは、EUF-CMA ゲームとほぼ同じだが、$A$ の勝利条件が、$L$ に含まれない平文と正しい署名の組 $(m^*, \sigma^*)$（すなわち、$(m^*, \sigma^*) \in L$）を出力して来た場合, $A$ の勝ちと定義する。 これは EUF-CMA ゲームの勝利条件より厳しくなっている。$A$ が、ディジタル署名 SIG に対する sEUF-CMA ゲームに勝つ確率を、$A$ の SIG に対するアドバンテージと呼び、

$\mathsf{Adv}^{\mathsf{seuf\text{-}cma}}_{A,\mathsf{SIG}}(\kappa) :=$

$$\Pr[(vk, sk) \leftarrow \mathsf{KGen}(1^n); (m^*, \sigma^*) \leftarrow A^{\mathsf{Sign}_{sk}}(vk) : \mathsf{Vrfy}(vk, m^*, \sigma^*) = 1 \wedge (m^*, \sigma^*) \notin L]$$

によって評価される。上記確率は, $\mathsf{KGen}, \mathsf{Sign}, A$（の内部コイン）に依存する。

**定義 21（sEUF-CMA 安全性）** 署名オラクルに $q$ 回までアクセスできる任意の $t$-時間アルゴリズム（族）の攻撃者 $A$ に対して, 十分大きな全ての $\kappa$ で, $\mathsf{Adv}^{\mathsf{seuf\text{-}cma}}_{A,\mathsf{SIG}}(\kappa) \leq \epsilon$ が成立するとき、ディジタル署名 SIG は, $(t, q, \epsilon)$-**sEUF-CMA 安全**という。特に, $t, q = O(\mathrm{poly}(\kappa))$ で、$\epsilon(\kappa) = \mathsf{negl}(\kappa)$ であるとき、SIG は **sEUF-CMA 安全**、または**選択平文攻撃 (chosen-message attack) に対して強存在的偽造不可 (strongly existentially-unforgeable)** という。

# 4　ランダムオラクルモデル (Random Oracle Model)

ランダムオラクルモデルとは、攻撃者を含む全てのアルゴリズムがランダム関数にオラクルアクセスできる環境のことを言う。例えばハッシュ関数 $H : X \to Y$ をランダム関数とみなすとは、$H$ が全ての関数の集合

$\mathsf{Func}(X,Y) = \{f : X \to Y\}$ からランダムに選ばれたものと考えるということである。ハッシュ関数をランダム関数とみなし、そのハッシュ関数へは誰もがオラクルアクセスできるモデルで暗号方式の安全性を証明したとき、その暗号方式は**ランダムオラクルモデルで安全**という。

### 4.1 署名の場合

現実の署名方式では、署名すべき平文をハッシュ関数という短いデータに圧縮してから署名生成アルゴリズムに入力する場合がほとんどである (hash-then-sign)。署名 SIG のランダムオラクルモデルでの sEUF-CMA 安全性を示すにはそのハッシュ関数 $H$ をランダム関数と扱いつぎのことを証明する。$A$ の SIG に対するランダムオラクルモデルでの sEUF-CMA 偽造成功確率は, $\mathsf{Adv}^{\mathsf{seuf\text{-}cma}}_{A,\Sigma}(\kappa) :=$

$$\Pr[H \leftarrow \mathsf{Func};\ (vk, sk) \leftarrow \mathsf{KGen}(1^n);\ (m^*, \sigma^*) \leftarrow A^{\mathsf{Sign}^H_{sk}, H}(vk) :\ \mathsf{Vrfy}^H(vk, m^*, \sigma^*) = 1 \wedge (m^*, \sigma^*) \notin L]$$

によって評価される。上記確率は, $H, \mathsf{KGen}, \mathsf{Sign}, A$ に依存する。$A$ はランダム関数 $H$ をオラクルとして利用できる。

$t$-時間確率的アルゴリズム $A$ の $H$ オラクルへの質問回数が $q_h(n)$ 回, 署名オラクル $\mathsf{Sign}^H_{sk}$ への質問回数が $q_s(n)$ 回とすると、上と同様に署名 $\mathsf{SIG}^H$ に対する $(t, q_h, q_s, \epsilon)$-sEUF-CMA 安全性が定義出来る。同様に, $t, q_h, q_s$ が多項式制限で、$\epsilon$ が無視できる関数であるとき, SIG はランダムオラクルモデルで sEUF-CMA 安全という。

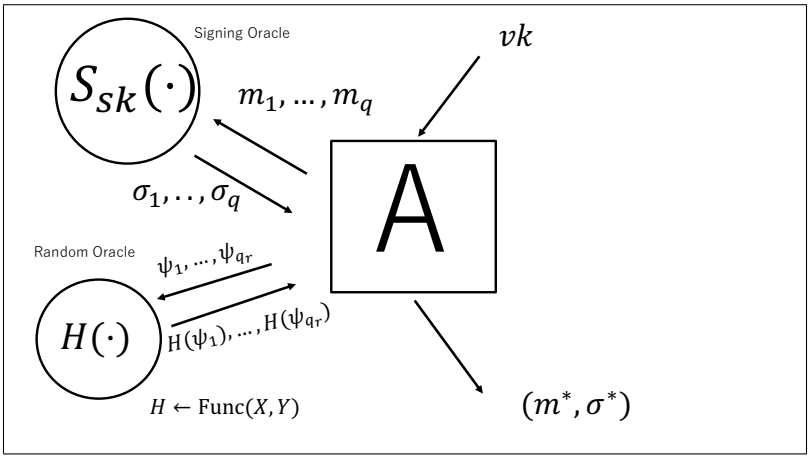


図 6　EUF-CMA in ROM

### 4.2 公開鍵暗号の場合

公開鍵暗号の安全性も同様に定義できる。

## 5 Full-Domain Hash 署名

$F = \{f\}$ を落とし戸つき一方向置換族とする。$F$-FDH 署名 $\mathsf{SIG} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$ を次のように定義する。鍵生成アルゴリズム KGen はセキュリティパラメタ $\kappa$ をとり、落とし戸つき一方向性置換 $f : \{0,1\}^\kappa \to \{0,1\}^\kappa$ を選び、$vk := f$, $sk := f^{-1}$ を出力する。$(f, f^{-1}) \leftarrow \mathsf{KGen}(1^\kappa)$. 署名生成アルゴリズム Sign は、秘密鍵 $sk(= f^{-1})$ と平文 $m$ をとり、$f_i^{-1}(H(m))$ を出力する。$\sigma \leftarrow \mathsf{Sign}^H_{sk}(m)$. 署名検証アルゴ

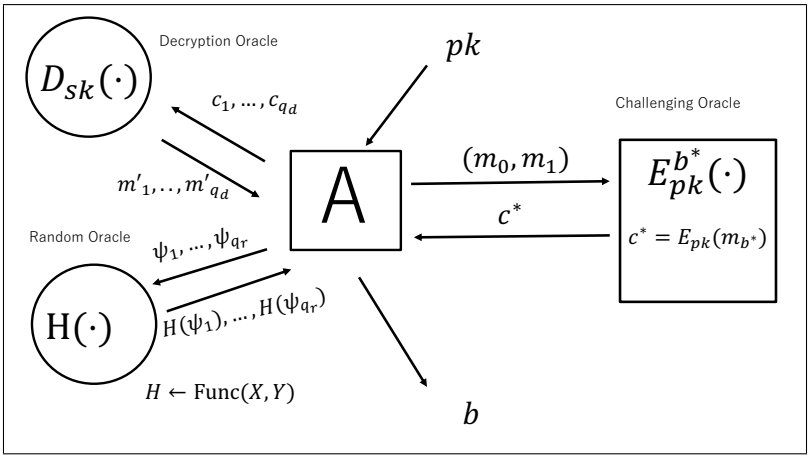


図 7　IND-CCA in ROM

リズム Vrfy は、検証鍵 $vk(=f)$ と $(m,\sigma)$ をとり、$H(m)=f(\sigma)$ の時、1 を出力し、それ以外の時は 0 を出力する。$b \leftarrow \mathsf{Vrfy}(vk,m,\sigma)$.

特に RSA 関数を使った場合、RSA-FDH 署名と呼ばれる。

**定理** 22　落とし戸付き置換族 $F$ が, $(t,\epsilon)$-OW であるならば, $F$-FDH 署名はランダムオラクルモデルで $(t',q_h,q_s,\epsilon')$-sEUF-CMA 安全であり,

$$t' \leq t - (q_h + q_s - 1)\cdot(T_R(\kappa) + T_F(\kappa))$$
$$\epsilon' \leq \Big(q_h + g_s\Big)\cdot\epsilon(n) + 2^{-\kappa}.$$

ただし, $\kappa$ ビットの乱数列の生成時間を $T_R(\kappa)$, $f:\{0,1\}^\kappa \to \{0,1\}^\kappa$ の計算時間を $T_F(\kappa)$ とする。

**(証明)**

**■証明の概要**　$F$-FDH 署名を sEUF-CMA ゲームで、ランダムオラクルと署名オラクルへの質問回数がそれぞれ $q_h(k), q_s(k)$ 回で $t'$-時間で走る確率的アルゴリズム $A_{\mathsf{SIG}}$ を考える。この $A_{\mathsf{SIG}}$ のアドバンテージを上から抑えるために、一方向性置換族 $F$ を攻撃するアルゴリズム $A_F$ を $A_{\mathsf{SIG}}$ を用いて作ることを考える。$A_F$ は、$A_{\mathsf{SIG}}$ を内部で使っているため、$A_F$ の成功確率は $A_{\mathsf{SIG}}$ のアドバンテージに依存する。一方、$A_F$ の走行時間が $t$ 以内であれば、その成功確率は、仮定により $\epsilon$ で抑えられなければいけない。よって、$A_{\mathsf{SIG}}$ の走行時間を $A_F$ の走行時間が $t$ 以内となるように調整してやれば、$A_{\mathsf{SIG}}$ のアドバンテージは、$A_F$ の限界 $\epsilon$ によって抑えられる。

**■$A_F$ の構成**　$A_F$ は, $(f,y^*)$ を入力として, $A_{\mathsf{SIG}}$ を使いながら $f^{-1}(y^*)$ を出力するアルゴリズム。

**[アルゴリズム $A_F$]**

1. $I \leftarrow \{1,\ldots,q_h+q_s\}$.
2. $q_h+q_s-1$ 個の独立な乱数 $x_1,\ldots,x_{I-1}, x_{I+1},\ldots,x_{q_h+q_s} \leftarrow \{0,1\}^\kappa$ を計算する。
3. リスト $L$ を用意する。初めは $L=\emptyset$ である。
4. $pk := f$ とし, $A_{\mathsf{SIG}}$ に入力。
5. $A_{\mathsf{SIG}}$ がランダムオラクル $H$ に質問してきたとき、
   (a) リスト $L$ に登録されている平文（質問）であれば、登録されている対応する $y$ を返す。
   (b) もし $i$ 回目の新しい質問 $m_i$ $(1 \leq i \leq q_h+q_s)$ である場合、

i. $i \neq I$ であれば、$y_i := f(x_i)$ を計算し、$y_i$ を答えとして返し、$L$ に $(m_i, x_i, y_i)$ を登録する。

ii. $i = I$ のときは、$y_I := y^*$ とし、$y_I$ を答えとして返し、$L$ に $(\star, y_I)$ を登録する。

6. $A_{\mathsf{SIG}}$ が署名オラクル $\mathsf{Sign}_{sk}^{H}$ に質問してきたとき、

(a) $H$ にまだ質問されていない $i$ 回目の新しい質問 $m_i$ $(1 \leq i \leq q_h + q_s)$ である場合、

i. $i \neq I$ であれば、$y_i := f(x_i)$ を計算し、$x_i$ を答えとして返し、$L$ に $(m_i, x_i, y_i)$ を登録する。

ii. $i = I$ のときは、アルゴリズムを停止する。

(b) 過去にランダムオラクル $H$ に質問した平文である場合、

i. その平文が $m_I$ と異なる場合は、$L$ に登録されている $x$ を署名として返してやる。

ii. $m_I$ であるときは、アルゴリズムを停止する。

7. $A_{\mathsf{SIG}}$ が 平文と署名の組 $(m^*, \sigma^*)$ を出力したとき、$m^* = m_I$ なら、$\sigma^*$ を出力し、それ以外のときは停止する。

**■$A_F$ の成功確率の解析**　$A_{\mathsf{SIG}}$ が $m^*$ をオラクル $H$ に質問する事象を $\mathsf{Ask}H$ と書くことにする。また、$A_{\mathsf{SIG}}$ が勝つ事象を $\mathsf{Succ}(A_{\mathsf{SIG}})$ と書くことにする。$A_F$ が成功する事象は、$(m^* = m_I) \wedge \mathsf{Succ}(A_{\mathsf{SIG}})$ が起きる事象である。$m^* = m_I$ が起きるということは、$\mathsf{Ask}H$ が起きていないといけないので、この確率は

$$\begin{aligned}\Pr[(m^* = m_I) \wedge \mathsf{Succ}(A_{\mathsf{SIG}}) \wedge \mathsf{Ask}H] &= \Pr[(m^* = m_I) \wedge \mathsf{Succ}(A_{\mathsf{SIG}}) \,|\, \mathsf{Ask}H] \Pr[\mathsf{Ask}H] \\ &= \Pr[m^* = m_I | \mathsf{Ask}H] \cdot \Pr[\mathsf{Succ}(A_{\mathsf{SIG}}) | \mathsf{Ask}H] \cdot \Pr[\mathsf{Ask}H] \\ &= \frac{1}{q_h + q_s} \Pr[\mathsf{Succ}(A_{\mathsf{SIG}}) | \mathsf{Ask}H] \cdot \Pr[\mathsf{Ask}H]\end{aligned}$$

と展開できる。ここで、$A_F$ がコインを振って選んだ $I$ と $A_{\mathsf{SIG}}$ が $I$ 番目の質問に署名をし偽造に成功する確率は独立であるので、

$$\Pr[(m^* = m_I) \wedge \mathsf{Succ}(A_{\mathsf{SIG}}) \,|\, \mathsf{Ask}H] = \Pr[m^* = m_I \,|\, \mathsf{Ask}H] \cdot \Pr[\mathsf{Succ}(A_{\mathsf{SIG}}) \,|\, \mathsf{Ask}H]$$

と、$\Pr[m^* = m_I \,|\, \mathsf{Ask}H] = \frac{1}{q_h + q_s}$ を使った。これより、$A_F$ の走行時間が $t$ 以内であれば、仮定から $A_F$ の成功確率は $\epsilon$ で抑えられるので、

$$\Pr[\mathsf{Succ}(A_{\mathsf{SIG}}) | \mathsf{Ask}H] Pr[\mathsf{Ask}H] \leq (q_h + q_s)\epsilon$$

である。

事象 $\mathsf{Succ}(A_{\mathsf{SIG}})$ の確率（アドバンテージ）は、

$$\begin{aligned}\mathsf{Adv}^{\mathsf{seuf\text{-}cma}}_{A_{\mathsf{SIG}},\mathsf{SIG}}(\kappa) &= \Pr[\mathsf{Succ}(A_{\mathsf{SIG}}) | \mathsf{Ask}H] \cdot \Pr[\mathsf{Ask}H] + \Pr[\mathsf{Succ}(A_{\mathsf{SIG}}) | \neg\mathsf{Ask}H] \cdot \Pr[\neg\mathsf{Ask}H] \\ &\leq \Pr[\mathsf{Succ}(A_{\mathsf{SIG}}) | \mathsf{Ask}H] \cdot \Pr[\mathsf{Ask}H] + 2^{-\kappa}\end{aligned}$$

と評価できる。ここで 2 行目は、$H$ に質問せずに $H(m^*)$ を正しく出力できる確率は高々 $2^{-\kappa}$ を使った。$t' \leq t - (q_h + q_s - 1) \cdot (T_R(\kappa) + T_F(\kappa))$ とすると、$\Pr[\mathsf{Succ}(A_{\mathsf{SIG}}) | \mathsf{Ask}H] \Pr[\mathsf{Ask}H] \leq (q_h + q_s)\epsilon$ を代入できるので、

$$\mathsf{Adv}^{\mathsf{seuf\text{-}cma}}_{A_{\mathsf{SIG}},\mathsf{SIG}}(\kappa) \leq (q_h + q_s) \cdot \epsilon(\kappa) + 2^{-\kappa}.$$

である。よって定理の式を得る。　■

## 付録 A　有限体上の楕円曲線

$K$ を標数 $\mathsf{chr}(K) \neq 2, 3$ なる体とする（標数が 5 以上の有限体、または無限位数の体）。このとき、$K$ 係数の曲線

$$y^2 = x^3 + ax + b \qquad (a, b \in K)$$

を考える。$4a^3+27b^2 \neq 0$ (*) のとき、この曲線を $K$ 上の楕円曲線という（$\mathrm{chr}(K)=2,3$ のときは別の式で楕円曲線は与えられる）。(*) の条件は、$f(x)=x^3+ax+b$ が重根を持たないのと同じである。

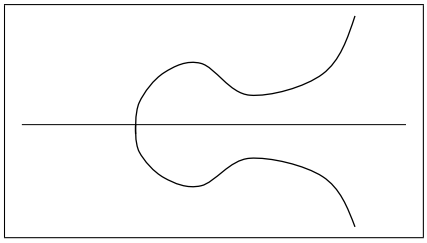

図 8　$f(x)=0$ の根が一つ

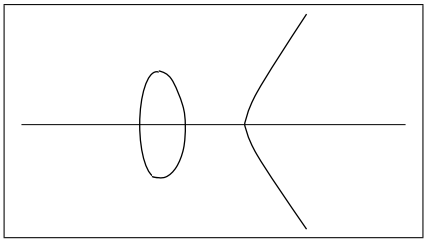

図 9　$f(x)=0$ の根が 3 つ

楕円曲線の点 $(x,y) \in K^2$（$K$-有理点）を $(x,y) \in E(K)$ と書くことにする。$K$ 上の楕円曲線には $K$-有理点が必ず存在し、（楕円曲線上にはない）特別な点 $O$ を加えた集合を $E(K)$ と書く。$E(K)$ は、下記の演算により $O$ を零元とする加法群になる。$P=(x_1,y_1)$, $Q=(x_2,y_2)$ とし $P+Q=(x_3,y_3)$ を、

$$x_3 := \lambda^2 - x_1 - x_2, \qquad y_3 := \lambda(x_1-x_3)-y_1$$

と定義する。ただし、

$$\lambda := \begin{cases} \frac{y_2-y_1}{x_2-x_1} & (P \neq Q) \\ \frac{3x_1^2+a}{2y_1} & (P=Q) \end{cases}$$

とする。$K=\mathbb{F}_q$ なる有限体とすると、Hasse の定理により、群 $E(\mathbb{F}_q)$ の位数は

$$q+1-2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q+1+2\sqrt{q}$$

であることが知られている。

楕円曲線上の演算は、次のように幾何学的に定義できる。

- $y \neq 0$ である $K$-有理点 $P \in E(K)$ を通り、$y$-軸と平行な直線は、$K$-有理点 $P'$ とのみ交わる。$P+P'=O$ と演算を定義し、$P'=-P$ と定義する。ここで、$y^2=x^3+ax+b$ は、$x$ 軸に対して対象なので、$P=(x,y)$ とすれば、$-P=(x,-y)$ であることがわかる。また、$O$ に対しては $O=-O$ と定義する。
- $P,Q \in E(K)$ を通る直線が第 3 点 $R'$ で楕円曲線と交わった場合、これも $K$-有理点 $R'$ となり、$P+Q+R'=O$ と定義することで、$R:=-R'=P+Q$ と定義できる。
- $2P(=P+P)$ は、楕円曲線の $P$ での接線を考え、第 3 点 $R'$ で交わった場合、$2P+R'=O$ と定義することで $R:=-R'=2P$ と定義できる。交わる点がない場合、$2P=O$ と定義する。そのとき $R:=O=-O=2P$ と定義する。

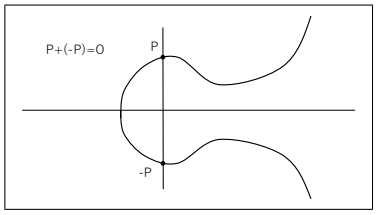


図 10　$P+(-P)=O$

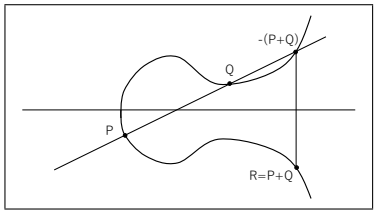


図 11　$R=P+Q$

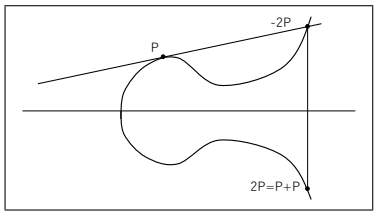


図 12　$R=2P$