中央大学数学教室講究録　No.4

# 公開鍵暗号の数理

岡本 龍明
原稿作成：森山 大輔

中央大学理工学部数学教室
2010 年 3 月

中央大学数学教室講究録　4

# 公開鍵暗号の数理

岡本 龍明
(NTT 研究所)
原稿作成：森山 大輔
(情報セキュリティ大学院大学情報セキュリティ研究科博士課程後期
課程)

中央大学理工学部数学教室
2010 年 3 月

# まえがき

本書は，2010 年 1 月 27 日から 2 月 4 日にかけて中央大学大学院 理工学研究科 数学専攻 情報数学特別講義第四 において行われた講義の講義ノートである．

この講義は，代数学の応用の一例として情報セキュリティの基盤技術の 1 つである公開鍵暗号に焦点を当てたものであり，NTT 研究所に所属しておられる岡本龍明 氏を講師としてお招きし，現代の公開鍵暗号の構成要素や安全性の厳密な定義等，様々な解説を行っていただいた．講義は 7 日間に渡って行われ，暗号の最も基本的な構成要素である一方向性関数や落とし戸一方向性関数の定義や公開鍵暗号の安全性の定義に関する等価性や相互関係についての説明，具体的な方式についての安全性証明等暗号の分野に関しての深い研究についての説明が行なわれた．

岡本龍明氏は忙しい中を，日々発展している暗号の安全性に関する生々しい概念を丁寧に講義をして下さり，その内容をこの様な形で記録し学生・研究者への便宜を図って下さったことに，本講座の取り纏め役として心より感謝を申し上げる次第である．

また，本原稿は情報セキュリティ大学院大学情報セキュリティ研究科博士後期課程 森山大輔氏により取り纏められたものである．この原稿を作成して戴いたことに，ここに深く謝意を表したい．

2010 年 3 月 7 日

中央大学数学教室　關口　力

# 目 次

# 1　イントロダクション

本講義では，現代暗号の最も基本的な概念である公開鍵暗号とディジタル署名を中心としてその安全性の定義および代表的な方式の安全性証明を最新のスタイルでできるだけ厳密に紹介することを目的とする．まず，暗号の安全性を証明するための基盤となるモデル (標準モデル，ランダムオラクルモデルなど) を紹介する．つぎに，暗号において最も基本的な構成要素である一方向性関数とトラップドア一方向性置換の紹介を行い，それらを用いて擬似乱数生成器や擬似ランダム関数が構成できることを示す．公開鍵暗号の安全性の定義（とくに，強秘匿性，頑健性）のいくつかの定式化を紹介し，それら定式化間の同等性や相互関係を示す．効率的で安全な公開鍵暗号として Cramer-Shoup 暗号を紹介し，その安全性を証明する．

## 1.1　用語及び基本概念

$\mathbb{N}$: 自然数の集合

$\mathbb{Z}_q$: 0 以上 $q$ 未満の整数の集合，$\mathbb{Z}/q\mathbb{Z}$

$\mathbb{Z}_q^\times$: $(\mathbb{Z}/q\mathbb{Z})^\times$

$\mathbb{R}$: 実数

$\mathbb{R}^+$: 正の実数

$\mathbb{G}$: 群

$\mathbb{F}_q$: 位数 $q$ の有限体

$\mathbb{F}_q^\times$: 位数 $q$ の有限体における乗法群

$a \mid b$: $a$ は $b$ を割り切る

$1^k$: 1 の $k$ ビット列

$\{0,1\}^k$: $k$ ビット長のバイナリ系列

$\{0,1\}^{\ell(k)}$: 多項式 $\ell(k)$ ビットの長さのバイナリ系列

$\{0,1\}^* := \bigcup_{k\in\mathbb{N}} \{0,1\}^k$: 任意長のバイナリ系列

確率変数 $X_k$: ある確率分布に従って生起する変数 $\{(x, P_x) | x \in \{0,1\}^{\ell(k)};\ P_x : \text{生起確率}\ \}$

確率変数族 $\{X_k\}_{k\in\mathbb{N}}$: 確率変数 $X_k$ の集合

$a \xleftarrow{\mathsf{U}} A$: 集合 $A$ から一様ランダムに要素を選び $a$ に代入

$a \xleftarrow{\mathsf{R}} A$: 確率変数 $A$ から分布に従って選び $a$ に代入

$a := A(x)$: アルゴリズム $A$ に $x$ を入力した際の出力 $a$

$a \in X$: $a$ は $X$ に含まれる値

$a \oplus b$: $a$ と $b$ のビット毎の排他的論理和

$a \| b$: $a$ と $b$ のビット列の結合

$a \wedge b$: $a$ かつ $b$

$a := b \bmod n$: $b \bmod n$ となる値を $a$ に代入

$a \equiv b \pmod{n}$: $a$ と $b$ は $n$ を法として合同

$x \oplus y$: $x = (x_1, \ldots, x_k) \in \{0,1\}^k$, $y = (x_1, \ldots, x_k) \in \{0,1\}^k$ としたとき，$x \oplus y := (x_1 \oplus y_1, \ldots, x_k \oplus y_k) \in \{0,1\}^k$

$x \odot y$: $x = (x_1, \ldots, x_k) \in \{0,1\}^k$, $y = (x_1, \ldots, x_k) \in \{0,1\}^k$ としたとき，$x \odot y := (x_1 \cdot y_1) \oplus \cdots \oplus (x_k \cdot y_k) \in \{0,1\}$

$\Pr[A(x) \to a]$: アルゴリズム $A$ が $x$ を入力としたとき $a$ を出力する確率

$T(k) = \mathcal{O}(f(k))$: $\exists c \in \mathbb{R}^+ \ \exists K \in \mathbb{N} \ \forall k > K, |T(k)/f(k)| < c \ (f(k) > 0)$

$T(k) = o(f(k))$: $\lim_{k \to \infty} T(k)/f(k) = 0$

$T(k) = \Omega(f(k))$: $\exists c \in \mathbb{R}^+ \ \exists K \in \mathbb{N} \ \forall k > K, |T(k)/f(k)| > c \ (f(k) > 0)$

$T(k) = \Theta(f(k))$: $T(k) = \mathcal{O}(f(k)) \wedge T(k) = \Omega(f(k))$

$f(k) < \epsilon(k)$: いかなる $c > 0$ に対しても，ある $K \in \mathbb{N}$ が存在し，いかなる整数 $k > K$ に対しても $f(k) < k^{-c}$ が成り立つ関数．ある関数 $f$ に対して $f(k) < \epsilon(k)$ であるとき，$f(k)$ は $k$ に関して negligible という．

# 2 準備

## 2.1 暗号理論におけるモデル

暗号理論においては，暗号方式 (プロトコル) を動作させる各パーティや安全性を考えるときの攻撃者などはすべてチューリングマシン (TM: Turing Machine) としてモデル化を行う．チューリングマシンとは与えられた特定の計算を行う機械のモデル

であり，我々が日常で利用しているコンピュータはすべてチューリングマシンである．なお，暗号において攻撃者をチューリングマシンとしてモデル化する場合は，

- 一様チューリングマシン: 無限長のテープを入力とした有限サイズのマシン (有限オートマトン)．入力サイズに関わらず与えられたプログラムを実行するものとして定式化される．
- 非一様チューリングマシン: 入力サイズ (セキュリティパラメータ) ごとに決まる回路．

の 2 通りに分けられる．

一様チューリングマシンは入力サイズに関わらず与えられたプログラムを実行するものとして定式化されるが，非一様チューリングマシンでは入力サイズごとに新しい情報を追加して別の回路を定めることが出来るため，一様チューリングマシンよりも強力なモデルとなっている．そのため，一様チューリングマシンとして考えた攻撃者に対しての安全性と非一様チューリングマシンとして考えた攻撃者に対しての安全性は異なることに注意したい．ただし，一般的な暗号の場合には攻撃者は一様チューリングマシンとして定式化したものを考える．

### 2.1.1 標準モデル

暗号の標準モデルとは，以下の条件を満たすモデルを指す．

1. 計算モデル – まず各パーティや攻撃者は確率的多項式時間チューリングマシン (PPT TM: Polynomial-Probabilistic-Time Turing Machine) としてモデル化する (多項式時間とはあるセキュリティパラメータ $k$ を決めたとき，処理時間がある $c > 0$ が存在し $O(k^c)$ で抑えられるものを指す)．また，暗号の安全性は漸近的安全性として捉え，ある 1 つの固定されたセキュリティパラメータ $k$ のみにおいて議論するのではなく，任意の $k$ に対して攻撃者が暗号を破る確率が $\epsilon(k)$ となるように安全性を考える．
2. 通信モデル – 各パーティ間での通信が行われるときには，通信は必ず攻撃者を経由して行われるものとして定式化する．つまり，攻撃者は通信路の中身を盗聴することができ，それらをどのパーティに入力するのかを自由に決定することができる．
3. セットアップモデル – モデルとしては，事前に特定のセットアップを想定しない．

### 2.1.2 ランダムオラクルモデル

通常の暗号学的ハッシュ関数の場合は，入力値に対して確定的かつ効率的な計算により出力が決まるが，ランダムオラクルモデルではハッシュ関数を理想的なランダム関数と想定したモデルとする．ランダムオラクルモデルにおいては，理想的ランダム関数は入力ビット列に関しての出力ビット列のテーブルとし，その出力ビット列は一様なコイン投げによって決まる．つまり，関数 $H : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ ($\ell(n)$ は $n$ の多項式) をランダムオラクルモデルの下で考えた場合，すべての $x \in \{0,1\}^n$ に対し，$H(x) \xleftarrow{\cup} \{0,1\}^{\ell(n)}$ となっている．また，ランダムオラクルモデルにおいては，この理想的ランダム関数は全てのパーティに共有される．従って同じ入力値に対しての出力値は全パーティにおいて同じである．

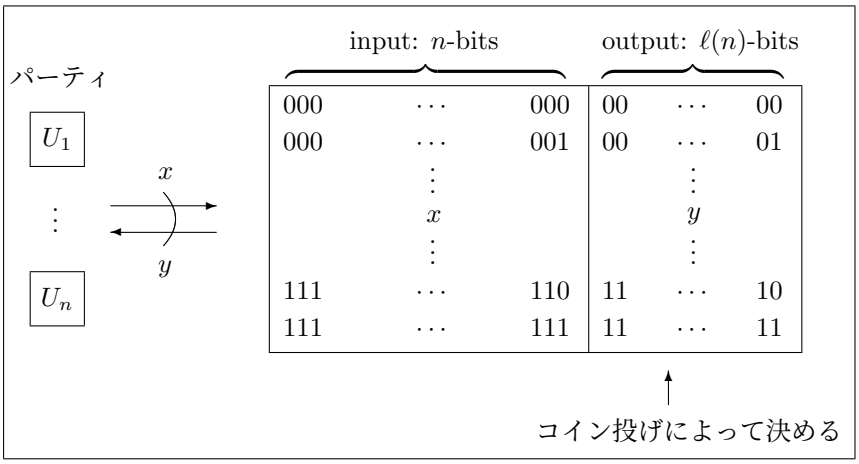


図 1: ランダムオラクルモデル

### 2.1.3 ジェネリック群モデル

2.1.2 節で述べたランダムオラクルモデルがハッシュ関数を理想化させたものであるのに対し，ジェネリック群モデルは群 $\mathbb{G}$ 上の演算を理想化したモデルである．ジェネリック群モデルでは，群 $\mathbb{G}$ のすべての要素は (無意味な) シンボルとして与えられ，群の演算法則に関する関係がオラクルによって保持されている．その群上で演算を行う場合，各パーティは群 $\mathbb{G}$ のオラクルにアクセスし，その返答 (シンボル) を演算結果として受け取る．

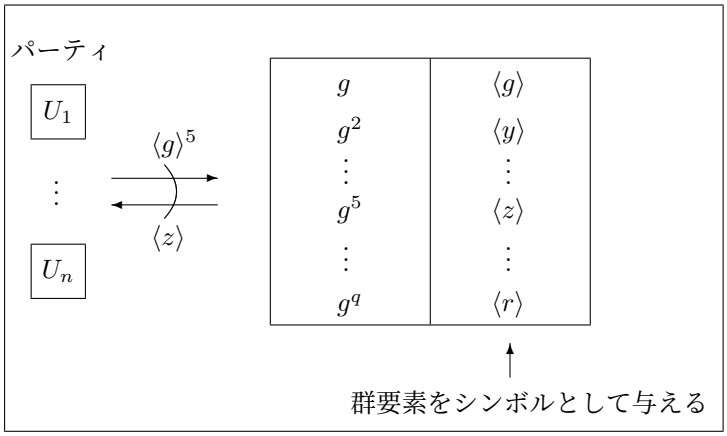

図 2: ジェネリック群モデル

## 2.2 証明可能安全性

ある暗号が安全であるということを証明したいとき,『何を』証明すべきであろうか. 一番理想的なものとしては，ある入力サイズに関しては対象とした暗号方式はこれだけの時間がかかったとしても安全である，ということが言えることである．暗号理論において，このような安全性は情報理論的安全性と呼ばれており，典型的な例としてはワンタイムパッドが挙げられる．ワンタイムパッドは，送信者と受信者が $k$ ビットの同じ鍵 $sk$ を持っているという前提で，送信者は $k$ ビットの平文 $m$ を $sk$ で排他的論理和をとり暗号文

$$c := m \oplus sk$$

を生成して $c$ を送り，復号する側は

$$m' := c \oplus sk$$

として平文を復号する方式である．また，物理的安全性という量子暗号等で用いられている物理的装置を用いた量子原理に基づいたものに関しても高い安全性を考えることができる．

しかしながら，現代の多くの公開鍵暗号においては計算量的安全性というものを考える．計算量的安全性では少なくとも前提条件を置き,「この問題を解くためには最低限これ程の計算時間がかかる」という事に仮定として定めることで暗号方式の安全性を議論する．そして，ある暗号方式を破る攻撃者が存在すると仮定するならば，その攻撃者を利用することでその前提としている仮定を破ることが出来るアルゴリズムが構成出来る，という帰着 (reduction) を考えて証明を行う．正しく帰着を行うことが出来たならば，仮定に矛盾するためその暗号方式はその仮定の下で安全である (つま

りその暗号方式を破るためには仮定を破るための計算時間が必要である)，と言える．特に，攻撃者がどのようなメカニズムかに関しては触れず入出力のみで帰着を行う場合，その帰着はブラックボックス帰着と呼ばれる．

**計算量的仮定**　上記で述べたように暗号の安全性を考える上では計算量的仮定をおいて証明を行うが，どのような仮定かによっても安全性は異なる．現在では，この計算量的仮定は

- 標準的仮定: 一方向性関数の存在，落とし戸一方向性関数の存在，素因数分解 (IF) 仮定，RSA 仮定，離散対数 (DL) 仮定，CDH 仮定，DDH 仮定，GDH 仮定
- Falsifiable 仮定: $\ell$-SDH 仮定，Strong RSA 仮定 等
- Unfalsifiable 仮定: KEA1 仮定 等

と大きく 3 つに分類される (GDH 仮定，$\ell$-SDH 仮定および KEA1 仮定の詳細な定義については付録 A 参照)．標準的仮定は，暗号理論の研究において基礎的な仮定として広く知られているものを指し，falsifiable 仮定はそうでない様々な仮定を指す．また，falsifiable 仮定と unfalsifiable 仮定の違いは，falsifiable 仮定ではその仮定が誤った仮定であったとき,「その仮定は誤っている仮定である」というアルゴリズムを記述することが出来る仮定であり，そのような記述を行うことができない unfalsifiable 仮定とは区別して考える．様々な公開鍵暗号の基礎となる素因数分解仮定，RSA 仮定，離散対数仮定および CDH 仮定は以下のようなものである．

素因数分解 (IF: Integer Factoring) 仮定

$1^k$ ($k$ : セキュリティパラメータ) を入力し，$k$ ビットの素数 $p, q$ を選び，$n := pq$ として $(n, p, q)$ を出力する多項式時間アルゴリズムを $\mathsf{GenMod}$ と呼ぶことにする．このとき，合成数 $n$ が与えられたときに $n = p'q'$ を満たす $(p', q')$ を出力する問題を素因数分解問題と呼ぶ．あるアルゴリズム $\mathcal{A}$ の素因数分解問題に対しての優位性は

$$\mathsf{Adv}^{\mathsf{IF}}_{\mathcal{A}}(k) := \Pr\left[ n = p'q' \;\middle|\; \begin{array}{l} (n,p,q) \xleftarrow{\mathsf{R}} \mathsf{GenMod}(1^k); \\ (p',q') \xleftarrow{\mathsf{R}} \mathcal{A}(k,n) \end{array} \right]$$

として定義される．

**定義 2.1.** いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても，素因数分解問題に対しての優位性が $\mathsf{Adv}^{\mathsf{IF}}_{\mathcal{A}}(k) < \epsilon(k)$ である場合，*IF* 仮定が保たれているという．

RSA 仮定

$1^k$ ($k$ : セキュリティパラメータ) を入力し，$(n, p, q) := \mathsf{GenMod}(1^k)$ を求め，$\phi(n) := (p-1)(q-1)$ とし $e \xleftarrow{\mathsf{U}} \mathbb{Z}_{\phi(n)}$，$d := e^{-1} \bmod \phi(n)$ として $(n, e, d)$ を出力する多項式

時間アルゴリズムを $\mathsf{GenRSA}$ と呼ぶことにする．このとき，$y \xleftarrow{\mathsf{U}} \mathbb{Z}_n$ として $(e, n, y)$ が入力された場合に，$x^e \equiv y \pmod{n}$ を満たす $x$ を求める問題を RSA 問題と呼ぶ．あるアルゴリズム $\mathcal{A}$ の RSA 問題に対しての優位性は

$$\mathsf{Adv}^{\mathsf{RSA}}_{\mathcal{A}}(k) := \Pr\left[\begin{array}{l|l} x^e \equiv y \pmod{n} & \begin{array}{l}(n,p,q) \xleftarrow{\mathsf{R}} \mathsf{GenMod}(1^k);\\ \phi(n) := (p-1)(q-1);\\ e \xleftarrow{\mathsf{U}} \mathbb{Z}_{\phi(n)};\ y \xleftarrow{\mathsf{U}} \mathbb{Z}_n;\\ x \xleftarrow{\mathsf{R}} \mathcal{A}(e,n,y)\end{array}\end{array}\right]$$

として定義される．

**定義 2.2.** いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても，*RSA* 問題に対しての優位性が $\mathsf{Adv}^{\mathsf{RSA}}_{\mathcal{A}}(k) < \epsilon(k)$ である場合，*RSA* 仮定が保たれているという．

離散対数 (DL: Discrete Logarithm) 仮定

$1^k$ ($k$ : セキュリティパラメータ) を入力し，$k$ ビットの素数 $p$ から有限体 $\mathbb{F}_p$ の乗法群 $\mathbb{F}_p^\times$ の部分群として素位数 $q$ の群 $\mathbb{G}$ と $\mathbb{G}$ の生成元 $g$ を選び，$(p, q, g)$ を出力する多項式時間アルゴリズムを $\mathsf{GenG}$ と呼ぶことにする．このとき，$x \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ から $X := g^x \bmod p$ として $(p, q, g, X)$ を入力したとき，$g^{x'} \equiv X \pmod{p}$ を満たす $x' \in \mathbb{Z}_q$ を出力する問題を $\mathsf{GenG}$ における離散対数問題と呼ぶ．あるアルゴリズム $\mathcal{A}$ の離散対数問題に対しての優位性は

$$\mathsf{Adv}^{\mathsf{DL}}_{\mathcal{A}}(k) := \Pr\left[\begin{array}{l|l} g^{x'} \equiv X \pmod{p} & \begin{array}{l}(p,q,g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k);\\ x \xleftarrow{\mathsf{U}} \mathbb{Z}_q;\\ X := g^x \bmod p;\\ x' \xleftarrow{\mathsf{R}} \mathcal{A}(p,q,g,X)\end{array}\end{array}\right]$$

として定義される．

**定義 2.3.** いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても，離散対数問題に対しての優位性が $\mathsf{Adv}^{\mathsf{DL}}_{\mathcal{A}}(k) < \epsilon(k)$ である場合，*DL* 仮定が保たれているという．

CDH (Computational Diffie-Hellman) 仮定

$1^k$ ($k$ : セキュリティパラメータ) を入力し，$(p, q, g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k)$ を求める．$x, y \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ から $g_1 := g^x \bmod p, g_2 := g^y \bmod p$ を求める．このとき，$(p, q, g, g_1, g_2)$ が入力されたときに，$g_3 \equiv g^{xy} \bmod p$ を求める問題を CDH 問題と呼ぶ．あるアルゴリズム $\mathcal{A}$ の CDH 問題に対しての優位性は

$$\mathsf{Adv}^{\mathsf{CDH}}_{\mathcal{A}}(k) := \Pr\left[\begin{array}{l|l} g_3 \equiv g^{xy} \pmod{p} & \begin{array}{l}(p,q,g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k);\ x,y \xleftarrow{\mathsf{U}} \mathbb{Z}_q;\\ g_1 := g^x \bmod p;\ g_2 := g^y \bmod p;\\ g_3 \xleftarrow{\mathsf{R}} \mathcal{A}(p,q,g,g_1,g_2)\end{array}\end{array}\right]$$

として定義される．

**定義 2.4.** いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても，*CDH* 問題に対しての優位性が $\mathsf{Adv}^{\mathsf{CDH}}_{\mathcal{A}}(k) < \epsilon(k)$ である場合，*CDH* 仮定が保たれているという．

## 2.3 確率論の手法

ある一つの確率空間における確率事象を $A, B, C$ とする．このとき，

- $\Pr[A \wedge B] = \Pr[A \mid B] \cdot \Pr[B]$
- $\Pr[A \vee B] \leq \Pr[A] + \Pr[B]$
- $\Pr[A_1 \vee \cdots \vee A_n] \leq \sum_{i=1}^{n} \Pr[A_i]$ (union bound)
- $\Pr[A] = \Pr[A \wedge B] + \Pr[A \wedge \neg B]$
- $\Pr[A \wedge \neg C] = \Pr[B \wedge \neg C] \Rightarrow |\Pr[A] - \Pr[B]| \leq \Pr[C]$ (difference lemma)

が成り立つ．なお，difference lemma に関しては

$$\Pr[A] = \Pr[A \wedge C] + \Pr[A \wedge \neg C] = \Pr[A \mid C]\Pr[C] + \Pr[A \mid \neg C]\Pr[\neg C]$$
$$\Pr[B] = \Pr[B \wedge C] + \Pr[B \wedge \neg C] = \Pr[B \mid C]\Pr[C] + \Pr[B \mid \neg C]\Pr[\neg C]$$

から

$$\begin{aligned}
&|\Pr[A] - \Pr[B]| \\
&= |\Pr[A \mid C]\Pr[C] + \Pr[A \mid \neg C]\Pr[\neg C] - \Pr[B \mid C]\Pr[C] - \Pr[B \mid \neg C]\Pr[\neg C]| \\
&= |\Pr[C] \cdot (\Pr[A \mid C] - \Pr[B \mid C]) + \Pr[\neg C] \cdot (\Pr[A \mid \neg C] - \Pr[B \mid \neg C])| \\
&= |\Pr[\Pr[A \mid C] - \Pr[B \mid C]| \cdot \Pr[C] \\
&\leq \Pr[C]
\end{aligned}$$

として導くことが出来る．

また，これらの関係から以下のような不等式が満たされることが知られている．

**定理 2.1** (マルコフの不等式)**.** 変数 $X$ を $\mathbb{R}^+$ *(*非負の実数*)* 上の確率変数とし，$v \in \mathbb{R}^+$ とする．また，$X$ の期待値を $\mathbf{E}(X)$ で表すものとする．このとき，

$$\Pr[X \geq v] \leq \frac{\mathbf{E}(X)}{v}$$

が成り立つ．

証明. 期待値の定義から,

$$\mathbf{E}(X) = \sum_x \Pr[X = x] \cdot x$$

である．よって

$$\mathbf{E}(X) \geq \sum_{x<v} \Pr[X = x] \cdot 0 + \sum_{x \geq v} \Pr[X = x] \cdot v = \sum_{x \geq v} \Pr[X = x] \cdot v$$

となる． □

**定理 2.2.** *2* つの変数 $\varepsilon, \delta$ を $0 < \varepsilon, \delta < 1$ とし，$Y$ は区間 $[0, 1]$ 上の確率変数とする．このとき

$$\mathbf{E}(Y) = \delta + \varepsilon \Rightarrow \Pr\left[Y \geq \delta + \frac{\varepsilon}{2}\right] > \frac{\varepsilon}{2}$$

が成り立つ.

証明. 背理法によって証明を行う．そのため，$\Pr[Y \geq \delta + \varepsilon/2] \leq \varepsilon/2$ であると仮定しよう．すると

$$\sum_{y \geq \delta + \varepsilon/2} \Pr[Y = y] \cdot y \leq \sum_{y \geq \delta + \varepsilon/2} \Pr[Y = y] \cdot 1 = \frac{\varepsilon}{2}$$
$$\sum_{y < \delta + \varepsilon/2} \Pr[Y = y] \cdot y \leq \sum_{y \geq \delta + \varepsilon/2} 1 \cdot y = \delta + \frac{\varepsilon}{2}$$

となる．よって $\mathbf{E}(Y) < \varepsilon/2 + \delta + \varepsilon/2 = \delta + \varepsilon$ となり最初に仮定していた $\mathbf{E}(Y) = \delta + \varepsilon$ と矛盾する．よって $\Pr[Y \geq \delta + \varepsilon/2] > \varepsilon/2$ である． □

**定理 2.3** (チェビシェフの不等式)**.** 変数 $X$ を $\mathbb{R}^+$ 上の確率変数とし，$\delta \in \mathbb{R}^+$ とする．また，$X$ の分散を $\mathbf{Ver}(X)$ で表すものとする．このとき

$$\Pr[|X - \mathbf{E}(x)| \geq \delta] \leq \frac{\mathbf{Ver}(X)}{\delta^2}$$

が成り立つ.

証明. 確率変数 $Y$ を $Y := (X - \mathbf{E}(X))^2$ とおき，$Y$ に対してマルコフの不等式を適応すると

$$\Pr[|X - \mathbf{E}(x)| \geq \delta] = \Pr[(X - \mathbf{E}(X))^2 \geq \delta^2] \leq \frac{\mathbf{E}(Y)}{\delta^2} = \frac{\mathbf{Ver}(X)}{\delta^2}$$

となるためチェビシェフの不等式が得られる． □

**補題 2.1** (対独立サンプリング Lemma)．確率変数 $X_1, \ldots, X_n$ を対独立な確率変数とする．確率変数が対独立とは，すべての $i \neq j$ に対して，$\Pr[X_i = a \wedge X_j = b] = \Pr[X_i = a] \cdot \Pr[X_j = b]$ である事を意味する．また，それぞれの確率変数における期待値と分散は同じであるとし $\mu := \mathbf{E}(X_1) = \cdots = \mathbf{E}(X_n)$, $\sigma^2 := \mathbf{Ver}(X_1) = \cdots \mathbf{Ver}(X_n)$ とおく．このとき

$$\Pr\left[\left|\frac{\sum_{i=1}^n X_i}{n} - \mu\right| \geq \delta\right] \leq \frac{\sigma^2}{\delta^2 n}$$

が成り立つ．[1]

証明. 確率変数 $\bar{X}_i$ を $\bar{X}_i := X_i - \mathbf{E}(X_i)$ とおく．$X_1, \ldots, X_n$ が対独立であるので $\bar{X}_1, \ldots, \bar{X}_n$ も対独立であり，すべての $i$ に対して $\mathbf{E}(\bar{X}_i) = 0$ となる．このとき確率変数 $\sum_{i=1}^n (X_i/n)$ をチェビシェフの不等式に適応させると ($\mathbf{E}(\sum_{i=1}^n (X_i/n)) = \mu$),

$$\begin{aligned}
\Pr\left[\left|\frac{\sum_{i=1}^n X_i}{n} - \mu\right| \geq \delta\right] &\leq \frac{\mathbf{Ver}\left(\sum_{i=1}^n \frac{X_i}{n}\right)}{\delta^2} \\
&= \frac{\mathbf{E}\left(\left(\sum_{i=1}^n \frac{X_i}{n} - \mu\right)^2\right)}{\delta^2} \\
&= \frac{\mathbf{E}\left(\left(\sum_{i=1}^n \frac{X_i - \mu}{n}\right)^2\right)}{\delta^2} \\
&= \frac{1}{\delta^2 n^2} \cdot \mathbf{E}\left(\left(\sum_{i=1}^n \bar{X}_i\right)^2\right) \\
&= \frac{1}{\delta^2 n^2} \cdot \left(\sum_{i=1}^n \mathbf{E}(\bar{X}_i^2) + \sum_{i \leq i \neq j \leq n} \mathbf{E}(\bar{X}_i \bar{X}_j)\right) \\
&= \frac{1}{\delta^2 n^2} \cdot n\sigma^2 = \frac{\sigma^2}{\delta^2 n}
\end{aligned}$$

となる．よって対独立サンプリング Lemma が証明された． □

**定理 2.4** (チェルノフ限界式)．確率変数 $X_1, \ldots, X_n$ を独立な確率変数とし，各々の確率変数は $X_i \in \{0, 1\}$ であるとする．変数 $p$ を $p \leq 1/2$ とし，すべての $i$ に対して $\Pr[X_i = 1] = p$ とする．このとき，$0 \leq \delta \leq p(1-p)$ を満たす任意の $\delta$ に対し，

$$\Pr\left[\left|\frac{\sum_{i=1}^n X_i}{n} - p\right| \geq \delta\right] < 2 \cdot e^{-\frac{\delta^2}{2p(1-p)} \cdot n}$$

が成り立つ．

また，チェルノフ限界式の確率変数 $X_i$ を ($X_i \in \{0, 1\}$ ではなく) より一般的に拡張したものは Hoefding 不等式と呼ばれている．

[1] 対独立サンプリング Lemma において，$n = 1$ の場合チェビシェフの不等式と等価となる．

# 3 基礎理論

## 3.1 一方向性関数

一方向性関数には強一方向性関数と弱一方向性関数の 2 つの定式化がある。

**定義 3.1** (強一方向性関数 [9])**.** 関数 $f : \{0,1\}^* \to \{0,1\}^*$ が強一方向性関数であるとは，以下の *2* つを満たすことである．

1. ある確率的多項式時間アルゴリズム $\mathcal{A}$ が存在し，任意の入力 $x \in \{0,1\}^k$ に対して $f(x)$ を出力する ($\exists$PPT Algorithm $\mathcal{A}$ $\forall x \in \{0,1\}^k,\ A(x) \to f(x)$).
2. いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\Pr[f(z) = y \mid x \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(x);\ z \xleftarrow{\mathsf{R}} \mathcal{A}(1^k, y)] < \epsilon(k)$$

が成り立つ．

なお，2 つ目の条件において，アルゴリズム $\mathcal{A}$ は $y := f(x)$ となっている $x$ を出力しなければいけないわけではない．$x \neq z$ であったとしても $f(z) = y$ を満たすものであればよく，そのような $z$ を出力する確率が無視出来るほど小さいような関数を強一方向性関数と呼ぶ．

**定義 3.2** (弱一方向性関数 [47])**.** 関数 $f : \{0,1\}^* \to \{0,1\}^*$ が弱一方向性関数であるとは，以下の *2* つを満たすことである．

1. ある確率的多項式時間アルゴリズム $\mathcal{A}$ が存在し，任意の入力 $x \in \{0,1\}^k$ に対して $f(x)$ を出力する ($\exists$PPT Algorithm $\mathcal{A}$ $\forall x \in \{0,1\}^k,\ \mathcal{A}(x) \to f(x)$).
2. ある定数 $c > 0$ が存在し，いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対してもある $K$ が存在し，任意の $k > K$ に対して

$$\Pr[f(z) = y \mid x \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(x);\ z \xleftarrow{\mathsf{R}} \mathcal{A}(1^k, y)] \leq 1 - 1/k^c$$

が成り立つ．

弱一方向性関数は強一方向性関数とは違い，$f(z) = y$ を満たす $z$ を出力する確率が 1 ではなく，失敗する確率が必ず存在することを考えた定式化となっている．そのため，強一方向性関数が存在するならば弱一方向性関数が存在することは明らかである．しかしながら，弱一方向性関数が存在するならば強一方向性関数を構成することが出来ることが知られている [47, 12].

**定理 3.1.** 関数 $f$ を弱一方向性関数とする．このとき，関数 $g$ を

$$g(x_1, \ldots, x_t) := (f(x_1), \ldots, f(x_t))$$

としたとき，$g$ は強一方向性関数である．

一般的に一方向性関数と呼ぶ場合は強一方向性関数を指す.

**関数族.** 上記で定義した一方向性関数の場合，一つの定義によって定義域と値域が定まった一意の関数 $f$ が定義されるが，一般的な関数の場合あるパラメータに依存して定義域と値域が定まる場合が多い．そのため，関数ではなく関数族としてひとまとめに関数を考えることが良い．つまり，$\mathcal{F} := \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_i$ という $i$ でインデックス付けされた関数 $f_i$ の集合として関数族を考える.

**定義 3.3.** 関数族 $\mathcal{F} := \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_i$ が多項式時間関数族であるとは，以下の $3$ つの条件を満たす多項式時間アルゴリズム $(\mathsf{Gen}, \mathsf{Samp}, f)$ が存在することである.

1. $\mathsf{Gen}$ : パラメータ生成アルゴリズム – $1^k$ *(*$k$ : セキュリティパラメータ*)* を入力し，インデックスの集合 $\mathcal{I}$ からランダムに一つのインデックス $i \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ $(i \in \mathcal{I})$ を出力するアルゴリズム．$|i| \geq k$ とし，それぞれのインデックスによってドメイン $\mathcal{D}_i$ とレンジ $\mathcal{R}_i$ が定まる.

2. $\mathsf{Samp}$ : サンプリングアルゴリズム – $i \in \mathcal{I}$ を入力とし，$i$ が定めるドメイン $\mathcal{D}_i$ から *(*分布に従って*)* ランダムに $x \xleftarrow{\mathsf{R}} \mathsf{Samp}(i)$ $(x \in \mathcal{D}_i)$ を出力するアルゴリズム．$(i, x)$ は $k$ に関する多項式で表される.

3. $f$ : 評価アルゴリズム – $(i, x)$ を入力とし，$y := f_i(x) \in \mathcal{R}_i$ を出力するアルゴリズム.

**定義 3.4.** 関数族 $\mathcal{F} := \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_i$ が一方向性関数族であるとは，いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\Pr[f_i(z) = y \mid i \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k);\ x \xleftarrow{\mathsf{R}} \mathsf{Samp}(i);\ y := f_i(x); z \xleftarrow{\mathsf{R}} \mathcal{A}(1^k, y, i)] < \epsilon(k)$$

が満たされる関数族のことをいう.

具体例 (冪乗関数)

まず，$1^k$ ($k$ : セキュリティパラメータ) を入力し，$(p, q, g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k)$ を動作させる．このとき，関数族 $\mathbf{Exp} := \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ を

$$\begin{aligned} \mathcal{I} &:= \{(p, q, g) \mid (p, q, g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k)\} \\ \mathcal{D}_i &:= \{x \mid x \in \mathbb{Z}_q\} \\ \mathcal{R}_i &:= \mathbb{Z}_p^\times \\ f_{p,q,g}(x) &:= g^x \bmod p \end{aligned}$$

として考えたとき，離散対数仮定の下ではいかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\Pr\left[g^z \equiv y \pmod{p} \;\middle|\; \begin{array}{l}(p,q,g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k);\ x \xleftarrow{\mathsf{U}} \mathbb{Z}_q; \\ y := g^x \bmod p;\ z \xleftarrow{\mathsf{R}} \mathcal{A}(1^k,p,q,g,y)\end{array}\right] < \epsilon(k)$$

が満たされるため，関数族 $\mathbf{Exp}$ は離散対数仮定の下で一方向性関数族となる．

**定義 3.5** (一方向性置換族)**.** 関数族 $\mathcal{F} := \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_i$ が一方向性置換族であるとは，$\mathcal{F}$ が一方向性関数族であることに加えて，$\mathcal{D}_i = \mathcal{R}_i$ かつ $f_i$ が全単射であるものを指す．

## 3.2 落とし戸付き一方向性関数

落とし戸付き一方向性関数は 3.1 節の一方向性関数を拡張したもので，ある落とし戸を知っているとその関数の逆像を計算することが容易であり，落とし戸を与えられなければ従来同様逆像の計算が困難な一方向性関数のことを指す．

**定義 3.6.** 関数族 $\mathcal{F} := \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i\in\mathcal{I}}$ が落とし戸付き一方向性関数とは，以下の 5 つの条件を満たす確率的多項式時間アルゴリズム $(\mathsf{Gen}, \mathsf{Samp}, f, g)$ が存在することである．

1. $\mathsf{Gen}$ : パラメータ生成アルゴリズム – $1^k$ *(*$k$ : セキュリティパラメータ*)* を入力し，インデックスの集合 $\mathcal{I}$ の中のインデックスの *1* つ $i$ とその関数における落とし戸 $t$ を $(i,t) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ $(i \in \mathcal{I})$ として出力するアルゴリズム．$|i| \geq k$ とし，それぞれのインデックスによってドメイン $\mathcal{D}_i$ とレンジ $\mathcal{R}_i$ が定まる．

2. $\mathsf{Samp}$ : サンプリングアルゴリズム – $i \in \mathcal{I}$ を入力とし，$i$ が定めるドメイン $\mathcal{D}_i$ から *(*分布に従って*)* ランダムに $x \xleftarrow{\mathsf{R}} \mathsf{Samp}(i)$ $(x \in \mathcal{D}_i)$ を出力するアルゴリズム．$(i,x)$ は $k$ に関する多項式で表される．

3. $f$ : 評価アルゴリズム – $(i,x)$ を入力とし，$y := f_i(x) \in \mathcal{R}_i$ を出力するアルゴリズム．

4. 一方向性 – いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

   $$\Pr\left[f_i(z) = y \mid i \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k);\ x \xleftarrow{\mathsf{R}} \mathsf{Samp}(i);\ y := f_i(x); z \xleftarrow{\mathsf{R}} \mathcal{A}(1^k,y,i)\right] < \epsilon(k)$$

   が満たされる．

5. $g$ : 落とし戸アルゴリズム – $(y,i,t)$ を入力とし，$f_i(z) = y$ を満たす $z$ を $z \xleftarrow{\mathsf{R}} g(y,i,t)$ として出力するアルゴリズム．

具体例 (RSA [43])
関数族 $\mathbf{RSA} := \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ を

$$\begin{aligned}
\mathcal{I} &:= \{(n,e) \mid (n,e,d) \xleftarrow{\mathsf{R}} \mathsf{GenRSA}(1^k)\},\ d : \text{落とし戸} \\
\mathcal{D}_i &:= \mathbb{Z}_n^\times \\
\mathcal{R}_i &:= \mathbb{Z}_n^\times \\
f_{n,e}(x) &:= x^e \bmod n \\
g_{n,e,d}(y) &:= y^d \bmod n
\end{aligned}$$

として考えたとき，関数族 $\mathbf{Exp}$ は離散対数仮定の下で落とし戸一方向性関数族となる．なぜならば，RSA 仮定の下ではいかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\Pr\left[z^e \equiv y \pmod n \;\middle|\; \begin{array}{l}(n,e,d) \xleftarrow{\mathsf{R}} \mathsf{GenRSA}(1^k);\ x \xleftarrow{\mathsf{U}} \mathbb{Z}_n^\times; \\ y := x^e \bmod p;\ z \xleftarrow{\mathsf{R}} \mathcal{A}(1^k,n,e,y)\end{array}\right] < \epsilon(k)$$

であるため一方向性が満たされ，かつ

$$\Pr\left[z^e \equiv y \pmod n \;\middle|\; \begin{array}{l}(n,e,d) \xleftarrow{\mathsf{R}} \mathsf{GenRSA}(1^k);\ x \xleftarrow{\mathsf{U}} \mathbb{Z}_n^\times; \\ y := x^e \bmod p;\ z := g(y,n,e,d)\end{array}\right] = 1$$

であるため $(z^e \equiv y^{ed} \equiv y \pmod n)$，$g$ は落とし戸アルゴリズムとなっている．

## 3.3 ハードコア述語

一方向性関数 $f$ は「$x$ から $f(x)$ を求めることは容易であるが，その逆像を求めることは困難である」という性質を捉えたものであり，これは $f(x)$ から $x$ の部分情報が得られていない，ということを示しているものではない．しかしながら，$f(x)$ からその逆像を求めることが困難であるならば，少なくとも $x$ から求められたある 1 ビットは求めることが困難である，と考えることは自然である．この性質を考えたものがハードコア述語である．

**定義 3.7** (ハードコア述語 [6])**.** 関数 $\mathsf{hc} : \{0,1\}^* \to \{0,1\}$ が関数 $f$ のハードコア述語 *(hardcore predicate)* であるとは，いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\left|2 \cdot \Pr[b' = \mathsf{hc}(x) \mid x \xleftarrow{\mathsf{U}} \{0,1\}^*;\ y := f(x);\ b' \xleftarrow{\mathsf{R}} \mathcal{A}(1^k,y)] - 1\right| < \epsilon(k)$$

が満たされていることをいう．

もし任意の一方向性関数からハードコア述語を構成出来るならば，$f(x)$ に対し $\mathsf{hc}(x)$ が一様な値かを識別できないので，それは計算量的にエントロピーが増大していることを意味する．また，このようなビットを積み重ねていくことで多項式サイズのランダムな値を得ることが出来る (擬似乱数生成器の構成)．

それでは，どのような値であれば求めることが困難な 1 ビットになるであろうか？非常に直感的な構成としては，$n$ ビットの値 $x$ を $x := (x_1, \ldots, x_n)$ $(\forall i,\ x_i \in \{0,1\})$ としたとき $b := x_1 \oplus \cdots \oplus x_n$ とした値 $b$ はたとえ $x$ が 99 ビット漏れていたとしても残りの 1 ビットによってランダムな値となるため求めることは困難である．そのため，これはハードコア述語の候補として当てはまるように見える．しかしながら，これに対してブラックボックス帰着を考え，ハードコア述語を破ることが出来ると仮定した場合に $y := f(x)$ から $f^{-1}(y)$ を求めることができるアルゴリズムを構成することは非常に難しい．

結論からいうと，Goldreich と Levin は以下のような構成によって任意の一方向性関数からハードコア述語が構成出来ることを示した [16]．

**定理 3.2.** 関数 $f : \{0,1\}^* \to \{0,1\}^*$ を任意の一方向性関数とし，関数 $g$ を $g(x,r) := (f(x), r)$ と定義する $(x, r \in \{0,1\}^k)$．そして，$\mathsf{hc}(x,r) := x \odot r := (x_1 \odot r_1) \oplus \cdots \oplus (x_k \odot r_k)$ $(x_i \odot r_i := x_i \cdot r_i \bmod 2)$ としたとき，$\mathsf{hc}$ は $g$ のハードコア述語となる．

Goldreich-Levin のこの構成は，$f$ に関してハードコア述語が存在すると言っているのではなく，$f$ を用いることでハードコア述語付きの一方向性関数 $g$ が構成出来るという事を示している．

この定理は以下の 3 つの補題を証明することで示すことが出来る．

**補題 3.1.** ある確率的多項式時間攻撃者 $\mathcal{A}$ がハードコア述語を

$$\Pr[b' = \mathsf{hc}(x) \mid x \xleftarrow{\mathsf{U}} \{0,1\}^*;\ y := f(x);\ b' \xleftarrow{\mathsf{R}} \mathcal{A}(1^k, y)] = 1$$

の確率で破ると仮定すると，関数 $f$ の一方向性を破る確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. 補題 3.1 は非常に特殊なケースであるため，図 3 のように簡単にアルゴリズム $\mathcal{B}$ を構成することが出来る．アルゴリズム $\mathcal{B}$ は $y := f(x)$ を受け取ると，$e_i$ を $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$ という $i$ 番目のビットのみが 1 であるような値を選ぶ．そして関数 $g$ の出力として $(y, e_i)$ を $\mathcal{A}$ に入力する．$\mathcal{A}$ が $x'_i$ を出力してきたならば，$\mathcal{B}$ は $i = 1, \ldots, k$ まで攻撃者 $\mathcal{A}$ を繰り返し動作させ，最終的に $\mathcal{A}$ の $k$ 回分の出力を用いて $z := (x'_1, \ldots, x'_k)$ を出力する．

上記のように $\mathcal{B}$ を構成した場合，$\mathsf{hc}(x) = x \odot e_i = x_i$ となるため，確率 1 で正しいハードコア述語を出力する攻撃者 $\mathcal{A}$ の出力は $x'_i = x_i$ である．よって繰り返し動作させることで $\mathcal{B}$ は $y$ を入力として $f(z) = y$ なる $z$ を求めることが出来る． □

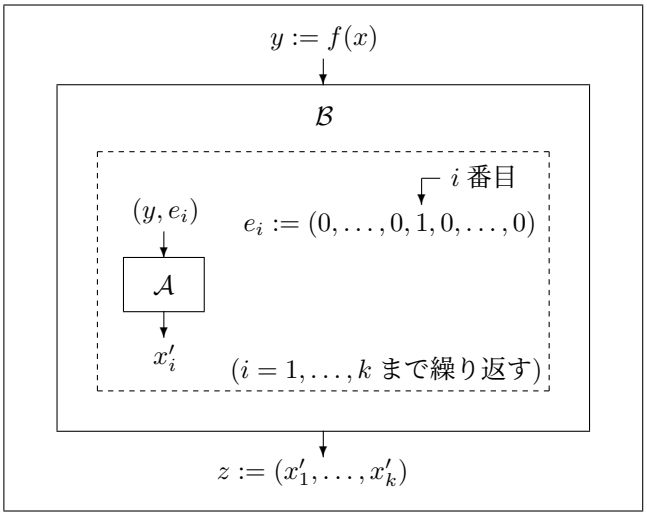

図 3: 補題 3.1 の証明

ただし，この構成は攻撃者 $\mathcal{A}$ が確率 1 よりも小さい確率 $p < 1$ の場合にのみハードコア述語を破ることに成功する場合，一方向性関数を破るアルゴリズムの成功確率は $p^k$ となるため，別の戦略が必要になる．そこで，次に攻撃者 $\mathcal{A}$ のハードコア述語を破る確率が $3/4 + \varepsilon(k)$ である場合を考える．

**補題 3.2.** ある確率的多項式時間攻撃者 $\mathcal{A}$ がハードコア述語を無視できない確率

$$\Pr[b' = \mathsf{hc}(x) \mid x \xleftarrow{\mathsf{U}} \{0,1\}^*;\ y := f(x);\ b' \xleftarrow{\mathsf{R}} \mathcal{A}(1^k, y)] = 3/4 + \varepsilon(k)$$

で破ると仮定すると，関数 $f$ の一方向性を破る確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. 補題 3.1 と異なり，各々の $i = 1, \ldots, k$ において攻撃者 $\mathcal{A}$ を 2 回動作させる場合を考える．すると，内積の線形性から任意の $r \xleftarrow{\mathsf{U}} \{0,1\}^k$ に対して

$$\begin{aligned}
\mathsf{hc}(x, r) \oplus \mathsf{hc}(x, r \oplus e_i) &= (x \odot r) \oplus (s \odot (r \oplus e_i)) \\
&= (x \odot r) \oplus (x \odot r) \oplus (x \odot e_i) \\
&= (x \odot e_i) \\
&= x_i
\end{aligned}$$

である．よって，$\mathcal{A}$ に対して $(f(x), r)$ を与えた場合に $x'_i = \mathsf{hc}(x, r)$ なる $x'_i$ が出力され，かつ $(f(x), r \oplus e_i)$ を与えた場合に $x''_i = \mathsf{hc}(x, r \oplus e_i)$ なる $x''_i$ が出力されるならば，$\mathcal{B}$ は $x'_i \oplus x''_i = x_i$ を得ることが出来る．このとき，1 つのハードコア述語を当てる確率が $3/4 + \varepsilon(k)$ であるならば，2 つのハードコア述語の両方を当てることができ

る確率は少なくとも

$$1 - 2 \cdot \left(1 - \left(\frac{3}{4} + \varepsilon(k)\right)\right) = \frac{1}{2} + 2\varepsilon(k)$$

である．また，$2\varepsilon(k)$ の偏りを利用し各々の $i$ に対して攻撃者を多項式回動作させることで，多項式個の $x'_i \oplus x''_i \in \{0,1\}$ のうち過半数を占めたほうを $z_i$ と定めることで高い確率で $f(z) = y$ となる $z := (z_1, \ldots, z_k)$ を求めることが出来る． □

補題 3.2 を証明手法をさらに応用し，攻撃者 $\mathcal{A}$ がハードコア述語を $1/2 + \varepsilon(k)$ の確率で破る場合を考える．

**補題 3.3.** ある確率的多項式時間攻撃者 $\mathcal{A}$ がハードコア述語を無視できない確率 $\Pr[b' = \mathsf{hc}(x) \mid x \xleftarrow{\mathsf{U}} \{0,1\}^*;\ y := f(x);\ b' \xleftarrow{\mathsf{R}} \mathcal{A}(1^k, y)] = 1/2 + \varepsilon(k)$ で破ると仮定すると，関数 $f$ の一方向性を破る確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. まず，$x$ を確率空間とする確率変数 $Y_x$ を

$$Y_x := \Pr[b' = \mathsf{hc}(x) \mid x \xleftarrow{\mathsf{U}} \{0,1\}^*;\ y := f(x);\ b' \xleftarrow{\mathsf{R}} \mathcal{A}(1^k, y)]$$

と定める．$Y_x$ の期待値は $\mathbf{E}(Y_x) = 1/2 + \varepsilon(k)$ であり，定理 2.2 から

$$\Pr_x\left[Y_x \leq \frac{1}{2} + \frac{\varepsilon(k)}{2}\right] > \frac{\varepsilon(k)}{2}$$

である．これは，$2^k$ 通りある $x$ に関して，$\varepsilon(k)/2$ の確率で $Y_x \leq 1/2 + \varepsilon(k)/2$ が満たされるものが存在することを意味する．そこで，全体のうちこのような性質の良い $x$ のみを考え (このような $x$ を $\mathsf{Good}$ と呼ぶことにする)，$x \in \mathsf{Good}$ を固定させて $r$ のみに関して考えることにする．

まず，$k$ ビットの $\ell$ 個の乱数 $s_1, \ldots, s_\ell \xleftarrow{\mathsf{U}} \{0,1\}^k$ (ただし $\ell = \log(t+1)$，$t = 2k/\varepsilon(k)^2$ とする)，1 ビットの $\ell$ 個の値 $\sigma_1, \ldots, \sigma_\ell \xleftarrow{\mathsf{U}} \{0,1\}$ および $2^\ell - 1$ 個の冪集合 $\mathcal{I} \in 2^{\{1,\ldots,\ell\}} \backslash \{\phi\}$ を考える．そして，$r^{\mathcal{I}} := \bigoplus_{j \in \mathcal{I}} s_j$，$\rho^{\mathcal{I}} := \bigoplus_{j \in \mathcal{I}} \sigma_j$ という値を考える (例: $r^{\{1,3\}} = s_1 \oplus s_3 \in \{0,1\}^k$)．すると，$\sigma_i$ は一様ランダムに選んでいることから

$$\Pr[\sigma_i = x \odot s_i] = \frac{1}{2}$$

であり，

$$\Pr[\forall i,\ \sigma_i = x \odot s_i] = \Pr[\rho^{\mathcal{I}} = x \odot r^{\mathcal{I}}] = \frac{1}{2^\ell}$$

が成り立つ．このとき $1/2^\ell$ は

$$\frac{1}{2^\ell} = \frac{1}{\frac{2k}{\varepsilon(k)^2} + 1} = \frac{\varepsilon(k)^2}{2k + \varepsilon(k)^2}$$

であるのでこれは $k$ に関して多項式である．そのため，補題 3.2 では固定された $(r, e_i)$ に対して攻撃者を 2 回動作させていたが，補題 3.3 では片側を $\rho^{\mathcal{I}}$ として推測し，もう片側に関してのみ攻撃者を利用する．つまり，具体的に一方向性関数を破るアルゴリズム $\mathcal{B}$ を構成する場合，$\mathcal{B}$ は固定された $i$ に関して $(y, r^{\mathcal{I}} \oplus e_i)$ を $\mathcal{A}$ に入力し出力を得るという動作を $\mathcal{I}$ の値を変化させて $2^\ell - 1$ 回繰り返す ($\mathcal{I}$ は $2^\ell - 1$ 通り存在する)．そして，その出力と $\rho^{\mathcal{I}}$ との排他的論理和をとり $(z_i^{\mathcal{I}} := \rho^{\mathcal{I}} \oplus \mathcal{A}(y, r^{\mathcal{I}} \oplus e_i))$，$2^\ell - 1$ 個分の値に関して過半数を占めたほうを $z_i$ と定める $(z_i := \mathsf{majority}^{\mathcal{I}}(z_i^{\mathcal{I}}))$．

ここで，$(s_1, \ldots, s_\ell)$ は独立に選んでいるが，$r^{\mathcal{I}}$ は $(s_1, \ldots, s_\ell)$ から選んでいるため $2^\ell - 1$ 個の値 $r^{\mathcal{I}}$ はすべて独立というわけではない．しかし，2 つの値を比べた場合必ずどちらかには $(s_1, \ldots, s_\ell)$ のうち用いられていない変数が存在するため，$r^{\mathcal{I}}$ は対独立な変数であるということができる．

最終的に $\mathcal{B}$ がどの程度の確率で一方向性関数を破るかについて考えよう．まず，確率変数 $\zeta_i^{\mathcal{I}}$ を $\zeta_i^{\mathcal{I}} = 1 \Leftrightarrow z_i^{\mathcal{I}} = x_i$ と定める．すると $\sum_i \zeta_i^{\mathcal{I}} > t/2$ $(t := 2^\ell - 1)$ は過半数を占めた値が正しい値であるという事を意味する．このとき，

$$\begin{aligned}\Pr\left[\sum_i \zeta_i^{\mathcal{I}} - \left(\frac{1}{2} + \frac{\varepsilon(k)}{2}\right) t \le -\frac{\varepsilon(k)}{2} t\right] &\le \Pr\left[\left|\sum_i \zeta_i^{\mathcal{I}} - \left(\frac{1}{2} + \frac{\varepsilon(k)}{2}\right) t\right| \ge \frac{\varepsilon(k)}{2} t\right] \\ &= \Pr\left[\left|\frac{\sum_i \zeta_i^{\mathcal{I}}}{t} - \left(\frac{1}{2} + \frac{\varepsilon(k)}{2}\right)\right| \ge \frac{\varepsilon(k)}{2}\right]\end{aligned}$$

となる．そして，チェビシェフの不等式から

$$\Pr\left[\left|\frac{\sum_i \zeta_i^{\mathcal{I}}}{t} - \left(\frac{1}{2} + \frac{\varepsilon(k)}{2}\right)\right| \ge \frac{\varepsilon(k)}{2}\right] \le \frac{\mathsf{Ver}[\zeta_i^{\mathcal{I}}]}{(\varepsilon(k)/2)^2 t} \le \frac{1}{\varepsilon(k)^2 t} = \frac{1}{2k}$$

が得られる．よって，$i = 1, \ldots, k$ と $k$ 回動作させたとしても，失敗する確率は高々 $1/2$ である．そのため，最終的に $\mathcal{B}$ が正しい答えを出力する成功確率は

$$\begin{aligned}&\Pr[x \in \mathsf{Good}] \cdot \Pr[\rho^{\mathcal{I}}\text{の } \mathit{Guess} \text{ が正しい}] \cdot \Pr[\forall i,\ z_i^{\mathcal{I}} = x_i] \\ &\ge \frac{\varepsilon(k)}{2} \cdot \frac{\varepsilon(k)^2}{5k} \cdot \frac{1}{2} = \frac{\varepsilon(k)^3}{20k}\end{aligned}$$

となり，無視できない確率で $\mathcal{B}$ が $f$ の一方向性関数を破ることを意味しているので補題 3.3 が証明された． □

## 3.4 擬似乱数生成器

一般に，モンテカルロ法のようなシミュレーションを行うための擬似乱数を生成する場合，その擬似乱数は分布がランダムであればよいと言う性質があれば十分である．しかしながら，暗号学的な観点で見た時の擬似乱数生成とは、いかなる確率的多項式

時間アルゴリズムに対しても真の乱数と擬似乱数とが識別できないと言うことが要求される。そのため，まずは計算量的識別不可能性 [17] を定式化しよう．

ある 2 つの確率変数 $X := \{X_k\}_{k\in\mathbb{N}}$, $Y := \{Y_k\}_{k\in\mathbb{N}}$ に対し，識別不可能性は以下のように 3 つに分けることができる．

1. 完全識別不可 – いかなる $k$ に関しても $X_k = Y_k$ であること．
2. 統計的識別不可 – 2 つの確率変数の統計距離を
$$\Delta(X,Y) := \frac{1}{2}\sum_{\alpha\in\{0,1\}^*} |\Pr[X_k = \alpha] - \Pr[Y_k = \alpha]|$$
と定義したとき，$\Delta(X,Y) < \epsilon(k)$ となること．
3. 計算量的識別不可 – いかなる確率的多項式時間アルゴリズム $\mathcal{D}$ に対しても
$$|\Pr[\mathcal{D}(X_k) \to 1] - \Pr[\mathcal{D}(Y_k) \to 1]| < \epsilon(k)$$
であること．特に $X_k$ と $Y_k$ が計算量的識別不可であるとき，$X_k \approx_{\mathsf{c}} Y_k$ と書く．

**定義 3.8** (擬似乱数生成器 [6])**.** 確定的多項式時間アルゴリズム $G$ が擬似乱数生成器であるとは，以下の *2* つが成立することである．

*1.* $k$ ビットの入力 $s \in \{0,1\}^k$ から $k$ ビットよりも長いビット列 $G(s)$ ($|G(S)| = \ell(k) > k$) を出力する．

*2.* いかなる確率的多項式時間攻撃者 $\mathcal{D}$ に対しても
$$\left|\Pr[\mathcal{D}(G(s)) \to 1 \mid s \xleftarrow{\cup} \{0,1\}^k] - \Pr[\mathcal{D}(R) \to 1 \mid R \xleftarrow{\cup} \{0,1\}^{\ell(k)}]\right| < \epsilon(k)$$
が満たされること．

擬似乱数生成器は 一方向性置換関数と 14 ページで述べたハードコア述語が存在すれば構成出来ることが知られている [47].

**定理 3.3.** 関数 $f$ を一方向性置換とし，$\mathsf{hc}$ を $f$ のハードコア述語とする．このとき 関数 $G(s) := (f(s), \mathsf{hc}(s))$ は $k$ ビットを $k+1$ ビットに伸長する擬似乱数生成器である．

なお，1 ビット伸ばすことが出来るならば何度も適応させることで任意の長さに伸長することが出来るため，理論的には 1 ビット伸長する擬似乱数生成器が構成できればよい．

証明. もし擬似乱数生成器 $G$ の安全性を無視できない確率 $\varepsilon(k)$ で破る確率的多項式時間アルゴリズム $\mathcal{A}$ が存在するならば，ハードコア述語 $\mathsf{hc}$ の安全性を破る確率的多項式時間アルゴリズム $\mathcal{B}$ が構成出来ることを示す．

まず，$\varepsilon(k)$ は $\mathcal{A}$ の擬似乱数生成器に対する優位性であるので

$$\begin{aligned}\varepsilon(k) &:= \left|\Pr[\mathcal{A}(G(s)) \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k] - \Pr[\mathcal{A}(R) \to 1 \mid R \xleftarrow{\mathsf{U}} \{0,1\}^{k+1}]\right| \\ &= \left|\Pr[\mathcal{A}(f(s), \mathsf{hc}(s)) \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k] - \Pr[\mathcal{A}(R) \to 1 \mid R \xleftarrow{\mathsf{U}} \{0,1\}^{k+1}]\right| \quad (1)\end{aligned}$$

と表すことができ，特に式 (1) における後者の確率は

$$\begin{aligned}& \Pr[\mathcal{D}(R) \to 1 \mid R \xleftarrow{\mathsf{U}} \{0,1\}^{k+1}] \\ = \;& \Pr[\mathcal{A}(y, r') \to 1 \mid y \xleftarrow{\mathsf{U}} \{0,1\}^k;\ r' \xleftarrow{\mathsf{U}} \{0,1\}] \\ = \;& \Pr[\mathcal{A}(f(s), r') \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ r' \xleftarrow{\mathsf{U}} \{0,1\}] \\ = \;& \Pr[\mathcal{A}(f(s), r') \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ \mathsf{hc}(s) = r'] \cdot \Pr[\mathsf{hc}(s) = r'] \\ & + \Pr[\mathcal{A}(f(s), r') \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ \mathsf{hc}(s) \neq r'] \cdot \Pr[\mathsf{hc}(s) \neq r']\end{aligned}$$

となるため

$$\varepsilon(k) = \frac{1}{2}\left|\begin{array}{l}\Pr[\mathcal{A}(f(s), \mathsf{hc}(s)) \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k] \\ -\Pr[\mathcal{A}(f(s), \overline{\mathsf{hc}(s)}) \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k]\end{array}\right|$$

である ($\overline{\mathsf{hc}(s)}$ は $\mathsf{hc}(s)$ のビットを反転させたものを表す)．このことを利用して，以下のような動作を行うアルゴリズム $\mathcal{B}$ を考える．

1. $y := f(s)$ を受け取ると，$r' \xleftarrow{\mathsf{U}} \{0,1\}$ を選ぶ．
2. $(y, r')$ を $\mathcal{A}$ に入力し，$\mathcal{A}$ から出力 $b$ を受け取る．
3. $b = 1$ であれば $b' := r'$ を，$b = 0$ であれば $b' := 1 - r'$ を出力する．

上記のように $\mathcal{B}$ を構成すると，

$$\begin{aligned}& \Pr[b' = \mathsf{hc}(s) \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(s);\ b' \xleftarrow{\mathsf{R}} \mathcal{B}(y)] \\ &= \frac{1}{2}\left(\begin{array}{l}\Pr[b' = \mathsf{hc}(s) \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(s);\ b' \xleftarrow{\mathsf{R}} \mathcal{B}(y);\ r' = \mathsf{hc}(s)] \\ + \Pr[b' = \mathsf{hc}(s) \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(s);\ b' \xleftarrow{\mathsf{R}} \mathcal{B}(y);\ r' \neq \mathsf{hc}(s)]\end{array}\right) \\ &= \frac{1}{2}\left(\begin{array}{l}\Pr[\mathcal{D}(f(s), \mathsf{hc}(s)) \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(s)] \\ + \Pr[\mathcal{D}(f(s), \overline{\mathsf{hc}(s)}) \to 0 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(s)]\end{array}\right) \\ &= \frac{1}{2}\left(\begin{array}{l}\Pr[\mathcal{D}(f(s), \mathsf{hc}(s)) \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(s)] \\ + (1 - \Pr[\mathcal{D}(f(s), \overline{\mathsf{hc}(s)}) \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(s)])\end{array}\right) \\ &= \frac{1}{2} + \frac{1}{2}\left(\begin{array}{l}\Pr[\mathcal{D}(f(s), \mathsf{hc}(s)) \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(s)] \\ - \Pr[\mathcal{D}(f(s), \overline{\mathsf{hc}(s)}) \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k;\ y := f(s)]\end{array}\right) \\ &= \frac{1}{2} + \varepsilon(k)\end{aligned}$$

が得られる．これは $\mathcal{B}$ がハードコア述語の安全性 (14 ページ参照) を破っていることを意味するので，矛盾が生じる．つまり背理法により $G$ は擬似乱数生成器であることが示された． □

## 3.5 擬似ランダム関数

乱数に対しての擬似乱数があるように，ランダム関数に対して擬似ランダム関数という概念が存在する．擬似ランダム関数 $f$ にはある $k$ ビットのシードと呼ばれる真の乱数 $s \xleftarrow{\mathsf{U}} \{0,1\}^k$ が与えられており，その下で入力 $x \in \mathcal{D}$ に対して出力 $f_s(x) \in \mathcal{R}$ を行う関数である．擬似ランダム関数に対しての計算量的識別不可能性では，ランダム関数か擬似ランダム関数のどちらかにアクセスしているときに，どちらの関数とアクセスしているのかを計算量的に識別不可能であることをいう [14, 15].

**定義 3.9.** 関数族 $\mathcal{F} : \{F_s : \{0,1\}^k \to \{0,1\}^{\ell(k)} \mid s \in \{0,1\}^k\}_{k\in\mathbb{N}}$ が擬似ランダム関数であるとは，いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\left|\Pr[\mathcal{A}^{F_s(\cdot)}(1^k) \to 1 \mid s \xleftarrow{\mathsf{U}} \{0,1\}^k] - \Pr[\mathcal{A}^{\mathsf{RF}(\cdot)}(1^k) \to 1 \mid \mathsf{RF} \xleftarrow{\mathsf{U}} \{0,1\}^{2^k\cdot\ell(k)}]\right| < \epsilon(k)$$

である場合をいう *(*RF はランダム関数*).*

**定理 3.4** (擬似ランダム関数の存在 [14, 15])**.** 擬似乱数生成器が存在するならば，擬似ランダム関数が存在する．

証明. 具体的に，擬似乱数生成器 $G$ を用いて以下のような関数 $F$ を考える．まず，擬似乱数生成器 $G$ は $k$ ビットの乱数から $2k$ ビットの擬似乱数を生成するものとする．このとき，擬似乱数生成器によって生成された $2k$ ビットの乱数を 2 つの $k$ ビットの値に分け，そしてその $k$ ビットに対して擬似乱数生成器 $G$ を用いて $2k$ ビットの擬似乱数を生成し，また $k$ ビットに分けてそれぞれに擬似乱数生成器を適応し，という操作を繰り返し行う．つまり，図 4 のように関数の入力値をビット列で表したとき，そのビットが 1 ならば右側，0 ならば左側，というように辿っていき最終的な出力として生成された値を返す，という方法である．

この構成においては，ランダム関数と擬似ランダム関数が識別できる場合，ハイブリッド論法 (hybrid argumen) により乱数と擬似乱数の識別に帰着することができる (この手法は [14] で初めて使われた)．例えば，図 4 のように構成した関数において，1 段目の出力をランダムな値に置き換えたとき，擬似乱数生成器が安全なのであれば識別は不可能である．もし擬似ランダム関数に対してある確率的多項式時間攻撃者 $\mathcal{A}$ がどちらかの関数にアクセスしたとき，これらを識別することができるのであれば，擬似乱数生成器の安全性を破るアルゴリズム $\mathcal{B}$ を構成することが出来る ($\mathcal{B}$ は通常通りに構成した関数 $F_s$ と，1 段目までをランダムな値に変更した関数 $F^1$ を用意し，ど

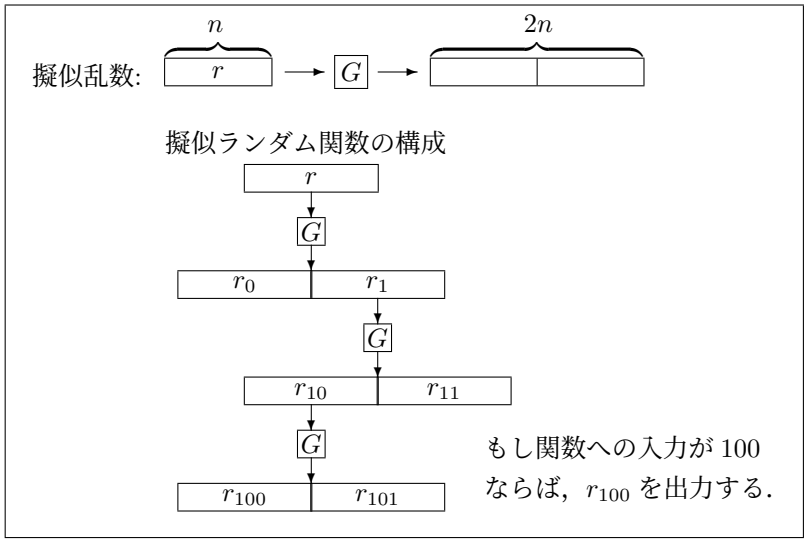


図 4: 擬似ランダム関数の構成例

ちらかを $\mathcal{A}$ にアクセスさせればよい)．これらを帰納的に用いることで，$i$ 段までをランダムな値に変更した関数と $i+1$ 段までランダムな値に変更した関数は計算量的に識別不可能であるので，最終的に $k$ 段までランダムな値に変更することが出来る．$k$ 段までランダムな値に変更した関数はランダム関数と等価であるので，擬似乱数生成器が安全なのであれば

$$\Pr[\mathcal{A}^{F_s(\cdot)} \to 1] \approx_{\mathsf{c}} \Pr[\mathcal{A}^{F^1(\cdot)} \to 1] \approx_{\mathsf{c}} \cdots \approx_{\mathsf{c}} \Pr[\mathcal{A}^{F^k(\cdot)} \to 1] = \Pr[\mathcal{A}^{\mathsf{RF}(\cdot)} \to 1]$$

となり，関数 $F$ は擬似ランダム関数の安全性を満たす． □

## 3.6 ハッシュ関数

ハッシュ関数とは，任意長の文字列をより短い一定の長さに圧縮する関数のことである．暗号学的なハッシュ関数にはいくつかの安全性要件が存在する．

**定義 3.10.** 関数族 $\mathcal{H} : \{\mathcal{H}_{hk} : \mathcal{D}_{hk} \to \mathcal{R}_{hk}\}_{hk \in \mathsf{KH}_k}$ がハッシュ関数族であるとは，セキュリティパラメータ $k$ に関する確率的多項式時間アルゴリズム $(\mathsf{Gen}, \mathsf{HF})$ が存在し以下の 2 つを満たすことである．

- $\mathsf{Gen}$ : 鍵生成アルゴリズム – $1^k$ $(k$ : セキュリティパラメータ$)$ を入力し，鍵空間 $\mathsf{KH}_k$ から鍵 $hk \in \mathsf{KH}_k$ を出力するアルゴリズム．
- $\mathsf{HF}$ : 評価アルゴリズム – $(hk, x)$ $(hk \in \mathsf{KH}_k, x \in \mathcal{D}_{hk})$ を入力とし，$y := \mathsf{HF}_{hk}(x) \in \mathcal{R}_{hk}$ を出力するアルゴリズム．

**定義 3.11** (衝突困難性)**.** ハッシュ関数族 $\Pi := (\mathsf{Gen}, \mathsf{HF})$ が衝突困難ハッシュ関数族であるとは，いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\mathsf{Adv}^{\mathsf{CR}}_{\mathcal{A}}(k) := \Pr\left[ x \neq x' \wedge \mathsf{HF}_{hk}(x) = \mathsf{HF}_{hk}(x') \;\middle|\; \begin{array}{l} hk \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k); \\ (x, x') \xleftarrow{\mathsf{R}} \mathcal{A}(1^k, hk) \end{array} \right] < \epsilon(k)$$

が満たされることである．

**定義 3.12** (標的衝突困難性)**.** ハッシュ関数族 $\Pi := (\mathsf{Gen}, \mathsf{HF})$ が標的衝突困難ハッシュ関数族であるとは，いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\mathsf{Adv}^{\mathsf{TCR}}_{\mathcal{A}}(k) := \Pr\left[ x \neq x' \wedge \mathsf{HF}_{hk}(x) = \mathsf{HF}_{hk}(x') \;\middle|\; \begin{array}{l} hk \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k);\ x \xleftarrow{\mathsf{U}} \mathcal{D}_{hk}; \\ x' \xleftarrow{\mathsf{R}} \mathcal{A}(1^k, hk, x) \end{array} \right] < \epsilon(k)$$

が満たされることである．

# 4 公開鍵暗号

公開鍵暗号は近年になってから発展した暗号で，共通鍵暗号とは異なり暗号化するための鍵と復号するための鍵は違うものを用いる暗号である．

## 4.1 定義と構成

公開鍵暗号は 3 つの多項式時間アルゴリズム $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ からなっており，

Gen : 鍵生成 – $1^k$ ($k$ : セキュリティパラメータ) を入力し，公開鍵と秘密鍵のペア $(pk, sk)$ を出力するアルゴリズム．このとき，システム上の平文空間 $\mathcal{M}_{pk}$ が定まる．つまり $\mathcal{M}_{pk}$ は $pk$ に含まれるとする．

$$1^k \rightarrow \boxed{\mathsf{Gen}} \rightarrow (pk, sk)$$

Enc : 暗号化 – 公開鍵 $pk$ と平文 $m \in \mathcal{M}_{pk}$ を入力とし，暗号文 $c$ を出力するアルゴリズム．

$$(pk, m) \rightarrow \boxed{\mathsf{Enc}} \rightarrow c$$

Dec : 復号 – 公開鍵 $pk$ と秘密鍵 $sk$ と暗号文 $c$ を入力とし，平文 $m$ あるいは復号不可を表す特別な記号 $\perp$ を出力するアルゴリズム．

$$(pk, sk, c) \rightarrow \boxed{\mathsf{Dec}} \rightarrow m \text{ or } \perp$$

で表される．セキュリティパラメータは公開鍵や秘密鍵のサイズを決定し，例えば $k = 1024$ のとき鍵生成アルゴリズム Gen は 1024 bit の公開鍵を生成する．このとき，Gen は確率的なアルゴリズムであり，同じセキュリティパラメータが入力されてもそのアルゴリズム内の乱数が作用することで毎回異なる値を出力するアルゴリズムである．また，復号に関してはほとんどの場合において確定的なアルゴリズムである．なお，以降簡単のため $\mathsf{Dec}(pk, sk, c)$ を $\mathsf{Dec}(sk, c)$ と表記する．

公開鍵暗号では，正しく平文 $m$ を Enc アルゴリズムによって暗号化した場合，その復号結果が正しく元の平文 $m$ に戻ること，つまり

$$\Pr\left[m' = m \;\middle|\; \begin{array}{l}(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k);\ m \xleftarrow{\mathsf{U}} \mathcal{M}_{pk};\\ c \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m);\ m' := \mathsf{Dec}(sk, c)\end{array}\right] = 1$$

が満たされることが前提として挙げられる (公開鍵暗号の正当性).

## 4.2 安全性

公開鍵暗号の安全性は達成度と攻撃法の 2 つの強度を考えることで捉えることができる．

### 4.2.1 安全性の達成度

公開鍵暗号における安全性の達成度は以下のように整理できる．

- 秘匿性: 平文の情報の秘匿の度合いを捉えたもの．以下の典型的な 2 つの秘匿の度合いがある．
  - **一方向性 (OW: One Wayness)** – 暗号文 $c$ から平文 $m$ 全体が得られないこと．
  - **強秘匿性 (IND: Indistinguishability, SS: Semantic Security)** – 暗号文 $c$ から平文 $m$ のいかなる部分情報も得られないこと．
- **頑強性 (NM: Non Malleability)** – 平文 $m$ に対する暗号文 $c = \mathsf{Enc}(pk, m)$ が与えられていることが、何らかの有益な暗号文を出力することに繋がらないこと．

**頑強性に関しての具体例: 電子入札**

例えば，A 社と B 社が電子入札を利用して 1 つのある物を競り落とす場合を考える．その入札金額は公開鍵暗号方式 Π によって暗号化の処理が施されているとする．A 社は 1000 万で入札するため平文 $m :=$ 1000 万 から暗号文 $c := \mathsf{Enc}(pk, m)$ として入札したとする．このとき，B 社は A 社の暗号文 $c$ を傍受しても，その暗号方式 Π が強秘匿性を満たしていれば 1000 万円で入札したという情報はまったく分からない．

しかし，もし $\Pi$ が頑強性を満たしていない場合，暗号文 $c$ から $m' := 1001$ 万 となる暗号文 $c' := \mathsf{Enc}(pk, m')$ を作ることで，A 社の入札金額に 1 万足した値の暗号文を作ることができる．このような暗号文を作ることができないという安全性を捉えたものが頑強性である．

#### 4.2.2 攻撃法

公開鍵暗号における攻撃の種類は以下のように分けることができる．

- **選択平文攻撃 (CPA: Chosen Plaintext Attack)** - ターゲットとする暗号文 $c$ を受け取る前後において，攻撃者は自分で選んだ平文に対する暗号文を得ることができる．

- **選択暗号文攻撃 (CCA1: Non-adaptive Chosen Ciphertext Attack)** - 選択平文攻撃で行うことができる攻撃に加え，ターゲットとする暗号文 $c$ を受け取る前において，攻撃者は自分で選んだ暗号文を送ることでその復号結果を返してくれる復号オラクルを利用することができる．

- **適応的選択暗号文攻撃 (CCA2: Adaptive Chosen Ciphertext Attack)** - 選択暗号文攻撃で行うことができる攻撃に加え，ターゲットとする暗号文 $c$ を受け取った後においても，攻撃者は自分で選んだ暗号文を送ることでその復号結果を返してくれる復号オラクルを利用することができる．

注意: 選択暗号文攻撃や適応的選択暗号文攻撃は仮想的 (理論的) な攻撃と考えるかも知れないが，現実に等価な攻撃が起こり得ることに注意．例えば初期の SSL 等においては，システムは復号結果が正しくないフォーマットになっている場合などに，その旨の返答を返すプロトコルになっており，これを用いて復号結果を得ることができる場合がある (Bleichenbach の攻撃法 [5])．

### 4.3 安全性の定式化

公開鍵暗号の安全性を評価するため，4.2 節で述べた公開鍵暗号の安全性を，よりフォーマルな形で定式化を行う．

#### 4.3.1 一方向性

ある公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ に対する一方向性は，攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ と挑戦者のゲーム (OW-ATK ゲーム) で捉える．OW-ATK ゲームは以下の 5 つの段階を時系列順に行うものである．

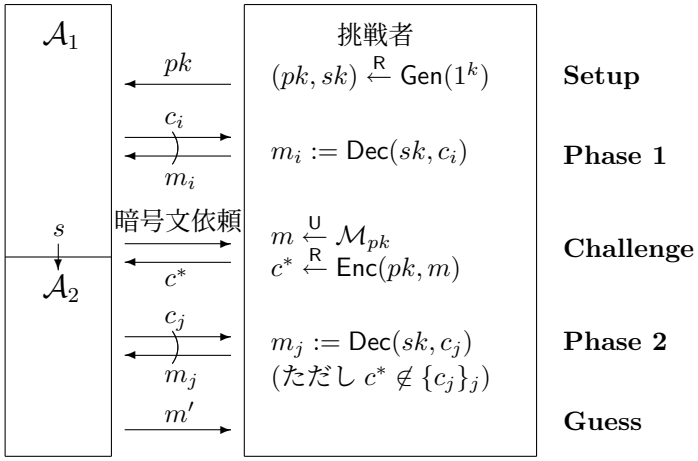


図 5: OW-CCA2 ゲーム

**OW-ATK ゲーム:**

**Setup**: $1^k$ ($k$ : セキュリティパラメータ) を入力とし，挑戦者は Gen アルゴリズムから公開鍵 $pk$ および秘密鍵 $sk$ の生成を行い，攻撃者 $\mathcal{A}_1$ に公開鍵 $pk$ を入力する．また，このときシステム上の平文空間 $\mathcal{M}_{pk}$ が定まる．

**Phase 1**: 選択暗号文攻撃および適応的選択暗号文攻撃の場合，攻撃者 $\mathcal{A}_1$ は自分で選んだ暗号文の復号結果を返してくれる復号オラクルを利用することができる．

**Challenge**: $\mathcal{A}_1$ は状態情報 $s$ を出力し，挑戦者に対してチャレンジ暗号文の作成を依頼する．挑戦者は平文空間から平文 $m \xleftarrow{\mathsf{U}} \mathcal{M}_{pk}$ を選び，その平文を暗号化したもの $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m)$ を作成し $\mathcal{A}_2$ に返答する．

**Phase 2**: 攻撃者 $\mathcal{A}_2$ は $(c^*, s)$ を入力とし，適応的選択暗号文攻撃の場合は $c^*$ 以外の暗号文に対して復号オラクルを利用することができる．

**Guess**: $\mathcal{A}_2$ はチャレンジ暗号文に対する平文 $m'$ を出力する．このとき，$m' = m$ であれば攻撃者の勝ちとする．

例えば，OW-CCA2 ゲームは図 5 のように表される．また，OW-CCA1 ゲームは図 5 の Phase 2 が省かれたゲームであり，OW-CPA ゲームは Phase 1 および Phase 2 の両方が省かれたゲームである．このゲームに関する攻撃者の優位性を定義するため，以下のような実験を考える．

$\underline{\mathsf{Exp}^{\mathsf{OW\text{-}ATK}}_{\Pi,\mathcal{A}}(k)}$
$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$;
$s \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$m \xleftarrow{\mathsf{U}} \mathcal{M}_{pk}$;
$c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m)$;
$m' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$:
$m' = m$ ならば 1 を出力
そうでなければ 0 を出力

この実験は，攻撃者が OW-ATK ゲームに勝った場合は 1 を，そうでない場合は 0 を出力するものである．このとき，攻撃者の優位性は

$$\mathsf{Adv}^{\mathsf{OW\text{-}ATK}}_{\Pi,\mathcal{A}}(k) := \left| \Pr\left[\mathsf{Exp}^{\mathsf{OW\text{-}ATK}}_{\Pi,\mathcal{A}}(k) \to 1\right] - \frac{1}{|\mathcal{M}_{pk}|} \right|$$

で定義される．また，攻撃の種類によって，攻撃者は

- ATK=CPA: $\mathcal{O}_1 = \emptyset$, $\mathcal{O}_2 = \emptyset$
- ATK=CCA1: $\mathcal{O}_1 = \mathsf{Dec}(sk, \cdot)$, $\mathcal{O}_2 = \emptyset$
- ATK=CCA2: $\mathcal{O}_1 = \mathsf{Dec}(sk, \cdot)$, $\mathcal{O}_2 = \mathsf{Dec}(sk, \cdot)$

のように暗号文を入力するとその平文の返答を行う復号オラクルを利用することができる ($\emptyset$ の場合は復号オラクルを利用することが出来ない)．ただし，Phase 2 においてチャレンジ暗号文そのものを復号オラクルに聞くことは禁止する．そして，いかなる確率的多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}^{\mathsf{OW\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ で抑えられるならば，その公開鍵暗号は OW-ATK 安全であるという．

**定義 4.1.** ある公開鍵暗号 $\Pi$ に対して，いかなる確率的多項式時間攻撃者 $\mathcal{A}$ が最大 $q_d$ 回の復号オラクルを利用したとしても $q_d$ が $k$ に関する多項式で表されるときに $\Pi$ に対して $\mathsf{Adv}^{\mathsf{OW\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ である場合，$\Pi$ は *OW-ATK* 安全であるという．

攻撃の種類が選択平文攻撃である場合は $q_d = 0$ であり，この場合は OW-CPA 安全となる．なお，安全性証明の際にランダムオラクルモデルが用いられる場合には，Phase 1 および Phase 2 において復号オラクルだけでなくランダムオラクルが付け加わるため，安全性のパラメータにランダムオラクルに対しての上限回数 $q_h$ が付け加わる．

### 4.3.2 強秘匿性の定義

公開鍵暗号の秘匿性を考える場合，一方向性よりも強力な安全性としては暗号文から平文のいかなる部分情報も得られない強秘匿性であることが求められる．なお，強

秘匿性には **Indistinguishability (IND)** と **Semantic Security (SS)** という代表的な 2 つの定義があり，その等価性が示されている [17]．IND は安全性の証明をする際に利用しやすい定義であり，SS は強秘匿性という意味を考慮した定義である．

IND は，攻撃者が平文 2 つを選び，その一方を暗号化して受け取ったときにどちらが暗号化されたのかを識別できないならば，暗号文から平文の情報は一切得られていないということを定式化したものであり，攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ と挑戦者の以下のようなゲームとして定式化される．公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ に対する IND-ATK ゲームは以下の 5 つの段階を時系列順に行うものである．

**IND-ATK ゲーム:**

**Setup**: $1^k$ ($k$ : セキュリティパラメータ) を入力とし，挑戦者は $\mathsf{Gen}$ アルゴリズムから公開鍵 $pk$ および秘密鍵 $sk$ の生成を行い，攻撃者 $\mathcal{A}_1$ に公開鍵 $pk$ を入力する．また，このときシステム上の平文空間 $\mathcal{M}_{pk}$ が定まる．

**Phase 1**: 選択暗号文攻撃および適応的選択暗号文攻撃の場合，攻撃者 $\mathcal{A}_1$ は自分で選んだ暗号文の復号結果を返してくれる復号オラクルを利用することができる．

**Challenge**: $\mathcal{A}_1$ は 2 つの平文 $m_0, m_1 \in \mathcal{M}_{pk}$ と自身の状態情報 $s$ を出力する．挑戦者は $(m_0, m_1)$ を受け取ると，$b \xleftarrow{\mathsf{U}} \{0,1\}$ としてどちらか一方の平文 $m_b$ を選び，その平文を $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_b)$ として暗号化する (この暗号文をチャレンジ暗号文と呼ぶ)．挑戦者は $c^*$ を攻撃者 $\mathcal{A}_2$ に入力する．

**Phase 2**: 攻撃者 $\mathcal{A}_2$ は $(c^*, s)$ を入力とし，適応的選択暗号文攻撃の場合は $c^*$ 以外の暗号文に対して復号オラクルを利用することができる．

**Guess**: $\mathcal{A}_2$ はチャレンジ暗号文のどちらが暗号化されたかに対しての推測 $b'$ を出力する．このとき，$b' = b$ であれば攻撃者の勝ちとする．

例えば，IND-CCA2 ゲームは図 6 のように表される．また，IND-CCA1 ゲームは図 6 の Phase 2 が省略されたゲームであり，IND-CPA ゲームは Phase 1 および Phase 2 が省略されたゲームである．

IND-ATK では，攻撃者がランダムにビット $b'$ を選び返答したとしても 1/2 の確率でゲームに勝つため，攻撃者の優位性は

$$\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(k) := |2 \cdot \Pr[b' = b] - 1|$$

で表される．

また，上記のゲームとは別の形で攻撃者の優位性を表現することもできる．これは，Challenge において $m_1$ が暗号化される場合と $m_0$ が暗号化される場合に分けてその差を考えることで攻撃者の優位性を定式化したもので，2 つの実験

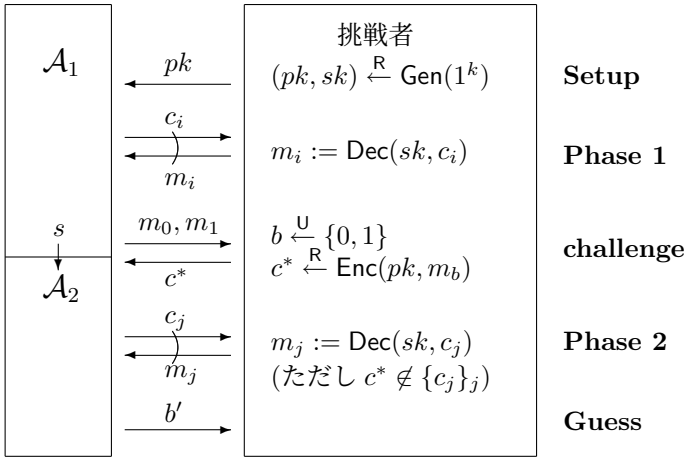


図 6: IND-CCA2

$\underline{\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k)}$
$(pk, sk) \xleftarrow{R} \mathsf{Gen}(1^k)$;
$(m_0, m_1, s) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \xleftarrow{R} \mathsf{Enc}(pk, m_0)$;
$b' \xleftarrow{R} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$:
$b'$ を出力

$\underline{\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k)}$
$(pk, sk) \xleftarrow{R} \mathsf{Gen}(1^k)$;
$(m_0, m_1, s) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \xleftarrow{R} \mathsf{Enc}(pk, m_1)$;
$b' \xleftarrow{R} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$:
$b'$ を出力

を考えた場合に，攻撃者の優位性を

$$\left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1\right] \end{array} \right|$$

として捉えたものである．なお，攻撃の種類によって

- IND-CPA: $\mathcal{O}_1 = \emptyset$, $\mathcal{O}_2 = \emptyset$
- IND-CCA1: $\mathcal{O}_1 = \mathsf{Dec}(sk, \cdot)$, $\mathcal{O}_2 = \emptyset$
- IND-CCA2: $\mathcal{O}_1 = \mathsf{Dec}(sk, \cdot)$, $\mathcal{O}_2 = \mathsf{Dec}(sk, \cdot)$

のように暗号文を入力するとその平文の返答を行う復号オラクルを利用することができる．ただし，Phase 2 においてチャレンジ暗号文 $c^*$ を復号オラクルに聞くことは禁止する．

このとき，

$$
\begin{aligned}
&\Pr[b' = b] \\
&= \Pr[b = 1] \cdot \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1 \mid b = 1\right] \\
&\quad + \Pr[b = 0] \cdot \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 0 \mid b = 0\right] \\
&= \frac{1}{2} \cdot \left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1\right] + \frac{1}{2} \cdot \left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 0\right] \\
&= \frac{1}{2} \cdot \left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1\right] + \frac{1}{2}\left(1 - \left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1\right]\right) \\
&= \frac{1}{2} + \frac{1}{2}\left(\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1\right] - \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1\right]\right)
\end{aligned}
$$

という関係が成り立つため，

$$
\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(k) = \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1\right] \end{array} \right|
$$

であり等価な関係であることが分かる．そして，いかなる確率的多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ が満たされているならば，その公開鍵暗号は IND-ATK に対して安全であるという．

**定義 4.2.** ある公開鍵暗号 $\Pi$ に対していかなる確率的多項式時間攻撃者 $\mathcal{A}$ が最大 $q_d$ 回の復号オラクルを利用したとしても，$q_d$ が $k$ に関する多項式で表されるときに *IND-ATK* に対する優位性が $\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ である場合，その公開鍵暗号は *IND-ATK* 安全であるという．

なお，安全性証明の際にランダムオラクルモデルが用いられる場合には，Phase 1 および Phase 2 において復号オラクルだけでなくランダムオラクルが付け加わるため，安全性のパラメータにランダムオラクルに問い合わすことができる上限回数 $q_h$ が付け加わる．

なお，ある公開鍵暗号方式の暗号化アルゴリズムが確定的である場合，挑戦者に送る 2 つの平文 $(m_0, m_1)$ を両方とも暗号化すると必ずどちらかがチャレンジ暗号文と一致するため，攻撃者は必ず IND-CPA を破ることができる．つまり，暗号化アルゴリズムが確定的な公開鍵暗号方式は IND-CPA 安全を満たさない．

**命題 4.1.** いかなる公開鍵暗号方式も，暗号化アルゴリズムが確定的である場合 *IND-CPA* 安全を満たさない．

例えば，RSA 暗号や Rabin 暗号の暗号化アルゴリズムは確定的であるので，これらは IND-CPA 安全を満たさない．

SS は強秘匿性の意味を考慮した定義で，暗号文を受け取っている状態で平文の情報を推測する確率と，暗号文を受け取っていない状態で平文の情報を推測する確率の差が $\epsilon(k)$ で抑えられるならば，暗号文から平文の情報は一切得られていないということを定式化したものである．それぞれの違いを定式化するため，SS-ATK-0 を暗号文を受け取っている状態で平文の情報を推測する実験，SS-ATK-1 を暗号文を受け取っていない状態で平文の情報を推測する実験とし，それぞれ攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ とアルゴリズム $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ を用いた以下の実験を考える．

| $\underline{\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A},h}(k)}$ | $\underline{\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},h}(k)}$ |
|---|---|
| $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ |
| $(\mathcal{M}, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $(\mathcal{M}, s) \xleftarrow{\mathsf{R}} \mathcal{S}_1(pk)$; |
| $m \xleftarrow{\mathsf{U}} \mathcal{M}$; | $m \xleftarrow{\mathsf{U}} \mathcal{M}$; |
| $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m)$; | |
| $(v, f) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m), s)$: | $(v, f) \xleftarrow{\mathsf{R}} \mathcal{S}_2(h(m), s)$: |
| $v = f(m)$ ならば 1 を出力 | $v = f(m)$ ならば 1 を出力 |
| $v \neq f(m)$ ならば 0 を出力 | $v \neq f(m)$ ならば 0 を出力 |

なお，$\mathcal{M}$ は平文空間を表すものであり，$h$ は多項式時間で計算可能な関数とする．このとき，攻撃の種類によって，攻撃者 $\mathcal{A}$ は

- ATK=CPA: $\mathcal{O}_1 = \emptyset$, $\mathcal{O}_2 = \emptyset$
- ATK=CCA1: $\mathcal{O}_1 = \mathsf{Dec}(sk, \cdot)$, $\mathcal{O}_2 = \emptyset$
- ATK=CCA2: $\mathcal{O}_1 = \mathsf{Dec}(sk, \cdot)$, $\mathcal{O}_2 = \mathsf{Dec}(sk, \cdot)$

のように暗号文を入力するとその平文の返答を行う復号オラクルを利用することができる．ただし，ATK=CCA2 の場合 $\mathcal{A}_2$ が $c^*$ を復号オラクルに聞くことは禁止されているものとする．また，SS-ATK-0 では $\mathcal{S}$ には攻撃の種類に関わらず復号オラクルは与えられないものとする．

SS-ATK-0 において 1 が出力される確率と SS-ATK-1 において 1 が出力される確率の差を

$$\mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},h}(k) := \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A},h}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},h}(k) \to 1\right] \end{array} \right|$$

と定義したとき，いかなる関数 $h$ およびいかなる確率的多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},h}(k) < \epsilon(k)$ となる $\mathcal{S}$ が存在する場合，その公開鍵暗号方式 $\Pi$ は強秘匿性が保たれているという．

**定義 4.3.** ある公開鍵暗号 $\Pi$ に対して，いかなる関数 $h$ および最大 $q_d$ 回の復号オラクルを利用するいかなる確率的多項式時間攻撃者 $\mathcal{A}$ に対してもあるアルゴリズム $\mathcal{S}$

が存在し，$q_d$ が $k$ に関する多項式で表されるときに *SS-ATK-b* の実験に関する優位性が $\mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},h}(k) < \epsilon(k)$ であるならばその公開鍵暗号は *SS-ATK* 安全であるという．

**定理 4.1.** いかなる攻撃の種類 $ATK \in \{CPA, CCA1, CCA2\}$ に対しても，公開鍵暗号が *SS-ATK* 安全であることと，*IND-ATK* 安全であることは等価である．

### 4.3.3 頑強性

頑強性 (NM: Non Malleability) は 1991 年に Dolev, Dwork, Naor によって定義されたもので [10]，Bellare, Sahai や Pass, Shelat, Vaukuntanathan によってより一般的な定式化および強秘匿性との等価性や差が示された [4, 38]．ここでは，Pass, Shelat, Vaukuntanathan によって定式化されたものを取り上げる．

Pass, Shelat, Vaukuntanathan は頑強性に関して**シミュレーションベース頑強性 (SNM: Simulation Based Non-Malleability)** と**識別不可能性ベース頑強性 (INM: Indistinguishability Based Non-Malleability)** に分け，一般的な場合にこれらが等価であることを示した．まずは，SNM に関して説明しよう．

シミュレーションベース頑強性は，ある平文 $m$ の暗号文 $c^*$ を受け取っている状態で暗号文の集合 $\mathbf{c}$ を出力した場合と，暗号文を受け取っていない状態で暗号文の集合 $\mathbf{c}$ を出力した場合で，それぞれの出力分布が計算量的識別不可能であるならば暗号文 $c^*$ から平文 $m$ の情報は一切得られていないということを定式化したものである．ある公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ に対するシミュレーションベース頑強性は攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ とアルゴリズム $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$，そして関係 $\mathcal{R}$ を用いた次のような 2 つの実験を用いて定式化される．

$\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A},\mathcal{R},h}(k)$

$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$;
$(\mathcal{M}, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$m \xleftarrow{\mathsf{U}} \mathcal{M}$;
$c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m)$;
$(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m), s_1)$;
$(c_1, \ldots, c_n) := \mathbf{c}$
　もし $c_i = c^*$ ならば $d_i := \perp'$;
　そうでなければ
　$d_i := \mathsf{Dec}(pk, c_i)$;
$b' \xleftarrow{\mathsf{R}} \mathcal{R}(\mathcal{M}, m, \{d_i\}, s_2)$;
$b'$ を出力

$\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{R},h}(k)$

$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$;
$(\mathcal{M}, s_1) \xleftarrow{\mathsf{R}} \mathcal{S}_1(pk)$;
$m \xleftarrow{\mathsf{U}} \mathcal{M}$;

$(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{S}_2(h(m), s_1)$;
$(c_1, \ldots, c_n) := \mathbf{c}$
　もし $c_i = \perp'$ ならば $d_i := \perp'$;
　そうでなければ
　$d_i := \mathsf{Dec}(pk, c_i)$;
$b' \xleftarrow{\mathsf{R}} \mathcal{R}(\mathcal{M}, m, \{d_i\}, s_2)$;
$b'$ を出力

$h$ は多項式時間で計算可能な関数とし，もし攻撃者 $\mathcal{A}_2$ が出力した暗号文が $c^*$ と一致している場合は復号せずに特別な記号 $\perp'$ を出力するものとする．攻撃の種類によって攻撃者は

- ATK=CPA: $\mathcal{O}_1 = \emptyset, \qquad \mathcal{O}_2 = \emptyset$
- ATK=CCA1: $\mathcal{O}_1 = \mathsf{Dec}(sk, \cdot)$, $\mathcal{O}_2 = \emptyset$
- ATK=CCA2: $\mathcal{O}_1 = \mathsf{Dec}(sk, \cdot)$, $\mathcal{O}_2 = \mathsf{Dec}(sk, \cdot)$

のように復号オラクルを利用することが出来る．ただし，SNM-CCA2 の場合 $\mathcal{A}_2$ は $c^*$ を復号オラクルに聞くことは禁止するものとする．また，SNM-ATK-0 の実験では攻撃の種類に関わらず復号オラクルは与えられないものとする．また，SNM の定義では $\mathcal{A}, \mathcal{S}$ には

**非重複性:** $c_i = c^*$ となる暗号文を出力しないこと

**正当性** 最終的に出力する暗号文 $(c_1, \ldots, c_n)$ はすべて暗号化関数の出力値からなる空間に含まれていること $(\forall c_i \ \exists m_i, c_i = \mathsf{Enc}(pk, m_i))$.

という制約が設けられているものとする．そして，いかなる確率的多項式時間攻撃者 $\mathcal{A}$ に対してもあるアルゴリズム $\mathcal{S}$ が存在し，いかなる関係 $\mathcal{R}$ に対しても

$$\mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{R},h}(k) := \left| \begin{array}{l} \Pr[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A},\mathcal{R},h}(k) \to 1] \\ -\Pr[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{R},h}(k) \to 1] \end{array} \right|$$

が $\mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{R},h}(k) < \epsilon(k)$ で抑えられるならば公開鍵暗号方式 $\Pi$ は SNM-ATK 安全であるという．

**定義 4.4.** ある公開鍵暗号 $\Pi$ に対して，いかなる関数 $h$，いかなる関係 $\mathcal{R}$ および最大 $q_d$ 回の復号オラクルを利用し $n$ 個の暗号文を出力するいかなる確率的多項式時間攻撃者 $\mathcal{A}$ に対してもあるアルゴリズム $\mathcal{S}$ が存在し，$q_d, n$ が $k$ に関する多項式であるときに *SNM-ATK-b* の実験に対する優位性が $\mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{R},h}(k) < \epsilon(k)$ であるならば，その公開鍵暗号は *SNM-ATK* 安全であるという．ただし $\mathcal{A}, \mathcal{S}$ はともに非重複性および正当性を満たしている出力を行うものとする．

安全性証明の際にランダムオラクルモデルが用いられる場合には，安全性のパラメータにハッシュオラクルに対しての上限回数 $q_h$ が付け加わる．

また，定義 4.4 をよりも強い定義として，攻撃者 $\mathcal{A}$ が上記の実験において非重複性および正当性の 2 つの条件を除いた場合においても安全性が失われない場合，$\Pi$ は SNM′-ATK 安全であるという．

**定義 4.5.** ある公開鍵暗号 $\Pi$ に対して，いかなる関数 $h$ および最大 $q_d$ 回の復号オラクルを利用し $n$ 個の暗号文を出力するいかなる確率的多項式時間攻撃者 $\mathcal{A}$ に対してもあるアルゴリズム $\mathcal{S}$ が存在し，$q_d, n$ が $k$ に関する多項式であるときにいかなる関係 $\mathcal{R}$ に対しても *SNM′-ATK-b* の実験に対する優位性が $\mathsf{Adv}^{\mathsf{SNM'\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{R},h}(k) < \epsilon(k)$ であるならば，その公開鍵暗号は *SNM-ATK* 安全であるという．

次に，識別不可能性ベース頑強性に関する定義を示そう．

識別不可能性ベース頑強性は IND-ATK 安全性を拡張したもので，攻撃者が最終的に出力するものがチャレンジ暗号文に対するビットではなく，暗号文の集合で表される．そして，$m_1$ に対する暗号文を受け取っている場合と $m_0$ に対する暗号文を受け取っている場合で，最終的に出力した暗号文の集合が計算量的識別不可能であれば INM′-ATK 安全性が保たれているという．ある公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ に対する識別不可能性ベース頑強性は攻撃者 $\mathcal{B} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ と挑戦者の以下のような 2 つの実験を用いて定式化される．

$\underline{\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k)}$
$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$;
$(m_0, m_1, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$;
$(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s_1)$;
$(c_1, \ldots, c_n) := \mathbf{c}$
　$c_i = c^*$ ならば $d_i := \perp'$;
　そうでなければ
　$d_i := \mathsf{Dec}(pk, c_i)$;
$b' \xleftarrow{\mathsf{R}} \mathcal{A}_3(d_1, \ldots, d_n, s_2)$:
$b'$ を出力

$\underline{\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k)}$
$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$;
$(m_0, m_1, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$;
$(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s_1)$;
$(c_1, \ldots, c_n) := \mathbf{c}$
　$c_i = c^*$ ならば $d_i := \perp'$;
　そうでなければ
　$d_i \xleftarrow{\mathsf{R}} \mathsf{Dec}(pk, c_i)$:
$b' \xleftarrow{\mathsf{R}} \mathcal{A}_3(d_1, \ldots, d_n, s_2)$:
$b'$ を出力

攻撃の種類によって，攻撃者は

- ATK=CPA: $\mathcal{O}_1 = \emptyset$, $\mathcal{O}_2 = \emptyset$
- ATK=CCA1: $\mathcal{O}_1 = \mathsf{Dec}(sk, \cdot)$, $\mathcal{O}_2 = \emptyset$
- ATK=CCA2: $\mathcal{O}_1 = \mathsf{Dec}(sk, \cdot)$, $\mathcal{O}_2 = \mathsf{Dec}(sk, \cdot)$

のように適応的に暗号文を復号して返答する復号オラクルを利用することが出来る．ただし，ATK=CCA2 の場合 $\mathcal{A}_2$ が $c^*$ を復号オラクルに聞くことは禁止されているものとする．SNM-ATK の場合と同様に，INM-ATK では $\mathcal{A}$ は非重複性および正当性という性質を満たしているものとする．そして，いかなる確率的多項式時間攻撃者 $\mathcal{A}$ に対しても，INM-ATK-$b$ の実験に関する優位性

$$\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{A}}(k) := \left| \begin{array}{l} \Pr[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1] \\ -\Pr[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1] \end{array} \right|$$

が $\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ で抑えられるならば公開鍵暗号方式 $\Pi$ は INM-ATK 安全であるという．

**定義 4.6.** ある公開鍵暗号方式 $\Pi$ に対して，いかなる確率的多項式時間攻撃者 $\mathcal{A}$ が最大 $q_d$ 回の復号オラクルを利用し $n$ 個の暗号文の集合と出力したとしても $q_d, n$ が $k$ に関する多項式であるときに *INM-ATK-b* の実験に関する優位性が $\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ であるならば，その公開鍵暗号は *INM-ATK* 安全であるという．ただし $\mathcal{A}$ はともに非重複性および正当性を満たしている出力を行うものとする．

また，定義 4.6 をよりも強い定義として，攻撃者 $\mathcal{B}$ が上記の実験において非重複性および正当性の 2 つの条件を除いた場合においても安全性が失われない場合，$\Pi$ は INM′-ATK 安全であるという．

**定義 4.7.** ある公開鍵暗号方式 $\Pi$ に対して，いかなる確率的多項式時間攻撃者 $\mathcal{A}$ が最大 $q_d$ 回の復号オラクルを利用し $n$ 個の暗号文の集合と出力したとしても $q_d, n$ が $k$ に関する多項式であるときに *INM′-ATK-b* の実験に関する優位性が $\mathsf{Adv}^{\mathsf{INM'\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ であるならば，その公開鍵暗号は *INM′-ATK* 安全であるという．

## 4.4 公開鍵暗号の具体例

### 4.4.1 Rabin 暗号

Rabin 暗号は 1979 年に Rabin によって提案されたもので [41]，素因数分解問題の難しさを仮定して安全性が証明された初めての公開鍵暗号である．ここでは，2 章で述べた blum 数を用いた場合の一意復号可能な方式について紹介しよう．

**Gen:** $1^k$ ($k$ : セキュリティパラメータ) を入力し，素数 $p, q$ を $p \equiv 3 \pmod 4, q \equiv 3 \pmod 4$ となる値として選び，$n := pq$ とする．ここで，$|n| = k$ とする．公開鍵を $pk := n$，秘密鍵を $sk := (p, q)$ と定める．平文空間は $\mathcal{M}_{pk} := \mathbb{Z}_n^\times$ とする．

$$pk = n,\ sk = (p, q)$$

**Enc:** 公開鍵 $pk$ とメッセージ $m \in \mathbb{Z}_n^\times$ を入力とし，$c := m^2 \bmod n$ を求める．また，ルジャンドル記号を用いて $a := \left(\frac{m}{n}\right)$ を求める．さらに $m < n/2$ ならば $b := 0$，$m \geq n/2$ ならば $b := 1$ として，$C := (c, a, b)$ を暗号文として出力する．

**Dec:** 公開鍵 $pk$ と秘密鍵 $sk$ と暗号文 $C = (c, a, b)$ を入力とし，

$$m'_p := c^{1/2} \bmod p$$
$$m'_q := c^{1/2} \bmod q$$

を求める．$(m_p, m_q), (m_p, -m_q), (-m_p, m_q), (-m_p, -m_q)$ をそれぞれ中国人剰余定理によって合成することで，$c = (m')^2 \bmod n$ を満たすそれぞれ平文の候補 4 つ $(m_1, m_2, m_3, m_4)$ が求められる．blum 数の性質を用いることで，$m_1 <$

$m_4, m_2 < m_3$ としたとき $(a, b) = (1, 0), (-1, 0), (-1, 1), (1, 1)$ に応じて $m_1, m_2$, $m_3, m_4$ が定まるため該当する平文を出力する．

Rabin 暗号の安全性の根拠となる数論仮定は，IF (Integer Factoring) 仮定であり，特に blum 数を用いている場合の IF 仮定を以下のように定義しよう．

Blum 数における IF 仮定

$1^k$ ($k$ : セキュリティパラメータ) を入力し，$p, q$ を素数の集合の中から $p \equiv q \equiv 3 \bmod 4$ を満たす値を選び，$n := pq$ を求める．$|n| = k$ であるとし，このような $(n, p, q)$ を出力するアルゴリズムを $\mathsf{GenBlum}$ と呼ぶ．このとき，$n$ が入力された場合に $n = p'q'$ を満たす $p', q'$ を求める問題を Blum 数における IF 問題と呼ぶ．このとき，あるアルゴリズム $\mathcal{A}$ の Blum 数における IF 問題に対しての優位性は

$$\mathsf{Adv}^{\mathsf{BIF}}_{\mathcal{A}}(k) := \Pr\left[n = p'q' \mid (n, p, q) \xleftarrow{\mathsf{R}} \mathsf{GenBlum}(1^k);\ (p', q') \xleftarrow{\mathsf{R}} \mathcal{A}(n)\right]$$

として定義される．

**定義 4.8.** いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても，*Blum* 数を用いた *IF* 問題に対しての優位性が $\mathsf{Adv}^{\mathsf{BIF}}_{\mathcal{A}}(k) < \epsilon(k)$ である場合，*Blum* 数を用いた *IF* 仮定が満たされているという．

**定理 4.2.** *Blum* 数における *IF* 仮定が保たれているならば，*Rabin* 暗号 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ は *OW-CPA* 安全な公開鍵暗号である．特に，いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対してもある確率的多項式時間アルゴリズム $\mathcal{B}$ が存在し

$$\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\Pi,\mathcal{A}}(k) \leq \mathsf{Adv}^{\mathsf{BIF}}_{\mathcal{B}}(k) - \frac{1}{n}$$

が成り立つ．

証明. ゲーム列を用いて，いかなる確率的多項式時間アルゴリズム $\mathcal{B}$ に対しても $\mathsf{Adv}^{\mathsf{BIF}}_{\mathcal{B}}(k) < \epsilon(k)$ であるならば，いかなる確率的多項式時間攻撃者 $\mathcal{A}$ に対しても Rabin 暗号の OW-CPA に対する優位性が $\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ であることを示そう．それぞれのゲーム Game $i$ において 1 が出力される事象を $S_i$ と置くことにする．

**Game 0:** Game 0 は通常の Rabin 暗号に対しての OW-CPA ゲームとする．
Rabin 暗号に対する OW-CPA の実験 (つまり Game 0) は以下のように表わされる．

Game 0 (OW-CPA)
$(n, p, q) \xleftarrow{\mathsf{R}} \mathsf{GenBlum}(1^k)$;
$pk := n$;
$m \xleftarrow{\mathsf{U}} \mathbb{Z}_n^\times$;
$(c, a, b) \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m)$;
$m' \xleftarrow{\mathsf{R}} \mathcal{A}(pk, (c, a, b))$:
$m' = m$ ならば 1 を出力
そうでなければ 0 を出力

Game 0 は通常の OW-CPA の実験と等価であるので $\Pr[S_0] = \mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\Pi,\mathcal{A}}(k)$ である．

**命題 4.2.** $\Pr[S_0] \leq \mathsf{Adv}^{\mathsf{IF}}_{\mathcal{B}}(k)$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. もし $S_1$ が起こる確率が無視出来ないのならば，IF 仮定を破ることができる確率的多項式時間アルゴリズム $\mathcal{B}$ が構成できることを示す．$\mathcal{B}$ が $\mathcal{A}$ を内部で利用し以下のような動作を行った場合を考える．

$\mathcal{B}(n)$
$pk := n$;
$m \xleftarrow{\mathsf{U}} \mathbb{Z}_n^\times$;
$(c, a, b) \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m)$;
$m' \xleftarrow{\mathsf{R}} \mathcal{A}(pk, (c, -a, b))$;
$p' := \mathrm{GCD}(m' - m, n)$, $q' := n/p'$;
$(p', q')$ を出力

上記の動作において，$\mathcal{B}$ は $\mathcal{A}$ に対して $m$ の正しい暗号文 $(c, a, b)$ から $a$ の符号を反転させたもの $(c, -a, b)$ を入力している．そのため，$S_0$ が起こる場合 $\mathcal{A}$ が出力した $m'$ は $m$ とは一致せず，$m$ を $m \equiv (m_p \pmod p, m_q \pmod q)$ としたとき $m'$ は $m' \equiv (m_p \pmod p, -m_q \pmod q)$ あるいは $m' \equiv (-m_p \pmod p, m_q \pmod q)$ のうちいずれかを満たす．従って $m - m' \equiv (0 \pmod p, 2m_q \pmod q)$ あるいは $m - m' \equiv (2m_p \pmod p, 0 \pmod q)$ であり，$p' := \mathrm{GCD}(m - m', n)$ は $p$ あるいは $q$ となるため，$p', q' := n/p'$ は $n = p'q'$ を満たす．よって

$$\Pr[S_0] \leq \mathsf{Adv}^{\mathsf{BIF}}_{\mathcal{B}}(k)$$

が得られる． ■

命題 4.2 より Rabin 暗号に関しては Game 0 から直接 IF 仮定に帰着させることができ，

$$\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\Pi,\mathcal{A}}(k) = \Pr[S_0] - \frac{1}{|\mathcal{M}_{pk}|} \leq \mathsf{Adv}^{\mathsf{BIF}}_{\mathcal{B}}(k) - \frac{1}{n}$$

となる．□

Rabin 暗号は OW-CPA 安全であるが，暗号化アルゴリズムは確定的であるため命題 4.1 から IND-CPA 安全ではない．また，Rabin 暗号は OW-CCA1 安全ではないことを示すことができる．

**定理 4.3.** *Rabin* 暗号は *OW-CCA1* 安全ではない．

ある攻撃者 $\mathcal{A}$ が $m \xleftarrow{\mathsf{U}} \mathbb{Z}_n^\times$ から正しい暗号化の手順から $C := (c, a, b)$ を求め，$a$ のビットを反転させたもの $C' := (c, \bar{a}, b)$ を復号オラクルに聞いたとき，命題 4.2 同様に計算を行うことで $p, q$ を求めることができる．そのため，チャレンジ暗号文 $c^*$ を受け取った場合に正しく復号を行い元の平文を求めることができる．よって $\mathsf{Adv}^{\mathsf{OW\text{-}CCA1}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ とはならないので Rabin 暗号は OW-CCA1 安全ではない．

### 4.4.2 ElGamal 暗号

ElGamal 暗号は 1984 年 ElGamal によって提案された公開鍵暗号である [11].

**Gen:** $1^k$ ($k$ : セキュリティパラメータ) を入力し，$(p, q, g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k)$ を求める．そして，$x \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ から $y := g^x \bmod p$ を求め，$pk := (p, q, g, y)$，$sk := x$ と定める．平文空間は $\mathcal{M}_{pk} := \mathbb{G}$ とする．

$$pk = (p, q, g, y),\ sk = x$$

**Enc:** 公開鍵 $pk$ および平文 $m \in \mathbb{G}$ を入力とし

1. $t \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ を選ぶ.
2. $c_1 := g^t \bmod p, c_2 := y^t \cdot m \bmod p$ を計算する.
3. $c := (c_1, c_2)$ を暗号文として出力する.

**Dec:** 公開鍵 $pk$ と秘密鍵 $sk$ と暗号文 $c$ を入力とし，$m' := c_2 \cdot c_1^{-x} \bmod p$ を平文として出力する．

ElGamal 暗号において平文が正しく暗号化されていれば，

$$m' \equiv c_2 \cdot c_1^{-x} \equiv y^t \cdot m \cdot (g^t)^{-x} \equiv m \cdot g^{xt} \cdot g^{-xt} \equiv m \pmod p$$

となり，暗号化した平文が正しく復号される．

ElGamal 暗号の安全性の根拠となる数論仮定は，DDH (Decision Diffie-Hellman) 仮定と呼ばれるものである．

DDH 仮定

$1^k$ ($k$ : セキュリティパラメータ) を入力し，$(p,q,g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k)$ を求める．$x,y,z \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ から $g_1 := g^x \bmod p, g_2 := g^y \bmod p, g_3 := g^{xy} \bmod p$ あるいは $g_3 := g^z \bmod p$ を求める．このとき，$(p,q,g,g_1,g_2,g_3)$ が入力されたときに，$g_3 \equiv g^{xy} \bmod p$ であるかを判定する問題を DDH 問題と呼ぶ．あるアルゴリズム $\mathcal{A}$ の DDH 問題に対しての優位性は

$$\mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{A}}(k) := \left| \begin{array}{l} \Pr\left[\mathcal{A}(p,q,g,g_1,g_2,g_3) \to 1 \;\middle|\; \begin{array}{l} x,y \xleftarrow{\mathsf{U}} \mathbb{Z}_q;\ g_1 := g^x \bmod p; \\ g_2 := g^y \bmod p;\ g_3 := g^{xy} \bmod p \end{array}\right] \\ -\Pr\left[\mathcal{A}(p,q,g,g_1,g_2,g_3) \to 1 \;\middle|\; \begin{array}{l} x,y,z \xleftarrow{\mathsf{U}} \mathbb{Z}_q;\ g_1 := g^x \bmod p; \\ g_2 := g^y \bmod p;\ g_3 := g^z \bmod p \end{array}\right] \end{array} \right|$$

として定義される．

**定義 4.9.** いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても，*DDH* 問題に対しての優位性が $\mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{A}}(k) < \epsilon(k)$ である場合，*DDH* 仮定が保たれているという．

**定理 4.4.** *DDH* 仮定が保たれているならば，*ElGamal* 暗号 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ は *IND-CPA* 安全な公開鍵暗号である．特に，いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対してもある確率的多項式時間アルゴリズム $\mathcal{B}$ が存在し

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi,\mathcal{A}}(k) \leq \mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{B}}(k)$$

が成り立つ．

証明. ゲーム列を用いて，いかなる確率的多項式時間アルゴリズム $\mathcal{B}$ に対しても $\mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{B}}(k) < \epsilon(k)$ であるならば，いかなる確率的多項式時間攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対しても ElGamal 暗号に対しての IND-CPA の優位性が $\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ で抑えられることを示そう．Game $i$ において攻撃者がゲームに勝つ (つまり $b' = b$) 事象を $S_i$ と置くことにする．

**Game 0:** Game 0 は通常の ElGamal 暗号に対しての IND-CPA ゲームとする．
**Game 1:** Game 1 では，Game 0 におけるゲームにおいてチャレンジ暗号文を $c_1 := X^y \cdot m_b$ と計算していた箇所を $z \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ から $c_1 := g^z \cdot m_b$ とした値へと変更する．

なお，ElGamal 暗号に対する IND-CPA の実験 (つまり Game 0) は以下のように表わされる．

$\underline{\text{Game 0 (IND-CPA)}}$
$((p,q,g,y),x) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$;
$pk := (p,q,g,X)$;
$(m_0,m_1,s) \xleftarrow{\mathsf{R}} \mathcal{A}_1(pk)$;
$b \xleftarrow{\mathsf{U}} \{0,1\}$; $t \xleftarrow{\mathsf{U}} \mathbb{Z}_q$;
$c_0 := g^t$; $g_3 := y^t$; $c_1 := g_3 \cdot m_b$;
$c^* := (c_0, c_1)$;
$b' \xleftarrow{\mathsf{R}} \mathcal{A}_2(c^*, s)$

まず，Game 0 は通常の ElGamal 暗号に対しての IND-CPA ゲームであるので

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi,\mathcal{A}}(k) = \left|\Pr[S_0] - \frac{1}{2}\right|$$

である．次に，以下の命題を証明し Game 0 と Game 1 において攻撃者がゲームに勝つ確率の差は無視できるほど小さいことを示そう．

**命題 4.3.** $|\Pr[S_0] - \Pr[S_1]| \leq \mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{B}}(k)$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. もし攻撃者 $\mathcal{A}$ が Game 0 と Game 1 においてゲームに勝つ確率の差が無視出来ない値であるならば，DDH 仮定を破ることができる確率的多項式時間アルゴリズム $\mathcal{B}$ が構成できることを示す．$\mathcal{B}$ が $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ を内部で利用し以下のような動作を行った場合を考える．

$\underline{\mathcal{B}(p,q,g,g_1,g_2,g_3)}$
$pk := (p,q,g,g_1)$;
$(m_0,m_1,s) \xleftarrow{\mathsf{R}} \mathcal{A}_1(pk)$;
$b \xleftarrow{\mathsf{U}} \{0,1\}$; $c_0 := g_2$; $c_1 := g_3 \cdot m_b$;
$c^* := (c_0, c_1)$;
$b' \xleftarrow{\mathsf{R}} \mathcal{A}_2(c^*, s)$;
もし $b' = b$ ならば 1 を出力
もし $b' \neq b$ ならば 1 を出力

このアルゴリズムの動作は Game 0 と Game 1 の中間に位置するもので，もし $\mathcal{B}$ への入力が $(g, g_1 := g^x \bmod p, g_2 := g^t \bmod p, g_3 := g^{xt} \bmod p)$ ならば $\mathcal{A}$ から見たときこのときの入出力は Game 0 の場合と等価な分布である．よって $\mathcal{B}$ が 1 を出力するのは事象 $S_0$ が起きた時であるため

$$\Pr\left[\mathcal{B}(g,g_1,g_2,g_3) \to 1 \;\middle|\; \begin{array}{l} x,t \xleftarrow{\mathsf{U}} \mathbb{Z}_q;\ g_1 := g^x \bmod p; \\ g_2 := g^t \bmod p;\ g_3 := g^{xt} \bmod p \end{array}\right] = \Pr[S_0]$$

である．一方，$\mathcal{B}$ への入力が $(g, g_1 := g^x \bmod p, g_2 := g^y \bmod p, g_3 := g^z \bmod p)$ ならば $\mathcal{A}$ から見たときこのときの入出力は Game 1 の場合と等価な分布であり，$\mathcal{B}$ が 1 を出力するのは事象 $S_1$ が起きた時である．つまり

$$\Pr\left[\mathcal{B}(g, g_1, g_2, g_3) \to 1 \,\middle|\, \begin{array}{l} x, t, u \xleftarrow{\mathsf{U}} \mathbb{Z}_q;\ g_1 := g^x \bmod p; \\ g_2 := g^t \bmod p;\ g_3 := g^u \bmod p \end{array}\right] = \Pr[S_1]$$

となる．よって

$$\mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{B}}(k) \geq |\Pr[S_1] - \Pr[S_0]|$$

が得られる． □

Game 1 において，$z \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ は $b, g_1, c_0$ とは独立に選ばれている値であるため，$g_3 := g^z$ は $\mathbb{G}$ 上で一様ランダムな値である．よって $c_1 = g_3 \cdot m_b$ も $\mathbb{G}$ 上で一様分布となるため攻撃者が $c_1$ から $m_b$ の値を得ることは (情報理論的に) 不可能である．よって攻撃者がチャレンジ暗号文 $m_b$ に対しての推測 $b'$ を $1/2$ 以上の確率で当てることは不可能であり，

$$\Pr[S_1] = \frac{1}{2}$$

である．

最終的に，

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi,\mathcal{A}}(k) \leq \mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{B}}(k)$$

が得られる．DDH 仮定が成り立っているならばいかなる確率的多項式時間アルゴリズム $\mathcal{B}$ に対しても $\mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{B}}(k) < \epsilon$ であるため，$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ が成り立つ．従って ElGamal 暗号は IND-CPA 安全である． □

ElGamal 暗号の安全性としては，IND-CPA 安全であることは証明可能であるが，IND-CCA2 安全でないことおよび NM-CPA 安全でないことを以下のように示すことができる．

**命題 4.4.** *ElGamal* 暗号は $(t, q_d, \epsilon)$-*IND-CCA2* 安全な公開鍵暗号方式ではない．

攻撃者 $\mathcal{A}$ が $m_0, m_1 \in \mathbb{Z}_q$ を選び，どちらかの平文 $m_b$ が暗号化されたチャレンジ暗号文 $c^* := (c_0, c_1)$ を受け取ったとする．その後，攻撃者が任意の平文 $m' \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ を選び $(c_0, c_1 \cdot m')$ を復号オラクルに聞いた場合，返答される値は $m := m_b \cdot m'$ という値であり，$m/m'$ を計算することにより $m_0, m_1$ のどちらが暗号化されていたのかを求めることができる．よって $\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ は満たされないので ElGamal 暗号は IND-CCA2 安全ではない．

**命題 4.5.** *ElGamal* 暗号は *INM-CPA* 安全な公開鍵暗号方式ではない.

具体的に ElGamal 暗号の INM-CPA 安全性を破る攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ を以下のように構成しよう.

| $\underline{\mathcal{A}_1(pk)}$ | $\underline{\mathcal{A}_2(c^*, s)}$ | $\underline{\mathcal{A}_3(d_1, s_2)}$ |
|---|---|---|
| $m_0, m_1 \xleftarrow{\cup} \mathcal{M}$; | $(c_0, c_1) := c^*$; | $d_1 = m_1$ ならば 1 を出力 |
| $s_1 := (m_0, m_1)$: | $c' := (c_0^2, c_1^2)$; | $d_1 = m_0$ ならば 0 を出力 |
| $(m_0, m_1, s_1)$ を出力 | $s_2 := s_1$: | |
| | $(c', s_2)$ を出力 | |

$\mathcal{A}_2$ はチャレンジ暗号文 $c^* = (c_0, c_1)$ を受け取ったとき $c' := (c_0^2, c_1^2)$ を出力しており, $c'$ を復号すると元の平文に復号される. そして, $\mathcal{A}_3$ はその平文が $m_1, m_0$ どちらであるかを識別してビットを出力している.

そのため, INM-CPA-0 の実験が行われた場合は常に 0 が出力され, INM-CPA-1 の実験が行われた場合は常に 1 が出力されるため, $\mathsf{Adv}_{\Pi,\mathcal{A}}^{\mathsf{INM\text{-}CPA}}(k) < \epsilon(k)$ とはならない. 従って ElGamal 暗号は INM-CPA 安全な公開鍵暗号方式ではない.

# 5 公開鍵暗号の安全性の関係と歴史

4.2 節で述べた大まかに分けた 3 つの安全性の達成度と 3 つの攻撃法に関して, 現在の研究では表 1 のような関係にあることが示されている. なお, 図では強秘匿性や頑強性に関して細かく分類したものを取り上げる. 表 1 における 2 つの安全性 A

表 1: 公開鍵暗号の安全性の関係

| 攻撃法 | 安全性の関係<br>('=' は等価を, '<' は差が存在することを示す) |
|---|---|
| CPA | $\mathrm{OW} < \mathrm{SS} = \mathrm{IND} < \mathrm{INM} = \mathrm{SNM} < \mathrm{INM}' = \mathrm{SNM}'$ |
| CCA1 | $\mathrm{OW} < \mathrm{SS} = \mathrm{IND} < \mathrm{INM} = \mathrm{SNM} < \mathrm{INM}' < \mathrm{SNM}'$ |
| CCA2 | $\mathrm{OW} < \mathrm{SS} = \mathrm{IND} = \mathrm{INM} = \mathrm{SNM} = \mathrm{INM}' < \mathrm{SNM}'$ |

と安全性 B に関して, A=B はその攻撃の種類に関しては 2 つの安全性が等価であることを示す. 一方, A<B はその攻撃の種類に関してある公開鍵暗号方式 Π が B を満たす場合必ず Π は A を満たすが, A を満たし B を満たさない公開鍵暗号方式が存在することを示すものである. 主に, OW<IND<NM の順に安全性が強くなり, CPA<CCA1<CCA2 の順に安全性が強くなり, 上記に挙げた安全性のうち OW-CPA が一番弱く, SNM′-CCA2 が一番強い安全性である. ただし, 一般的な公開鍵暗号に

おける安全性は SNM-ATK や INM-ATK で捉えることができ，その場合 IND-CCA2 は INM-CCA2 や SNM-CCA2 と等価な安全性である．また，公開鍵暗号および公開鍵暗号の安全性に関する定式化の歴史は以下の通りである．

1976 年: Diffie, Hellman (公開鍵暗号，Diffie-Hellman 鍵配送) [9]

1978 年: Rivest, Shamir, Adleman (RSA 暗号) [43]

1979 年: Rabin (OW-CPA) [41]

1982 年: Goldwasser, Micali (IND-CPA) [17]

1990 年: Naor, Yung (IND-CCA1) [36]

1991 年: Rackoff, Simons (IND-CCA2) [42]

1991 年: Dolev, Dwork, Naor (NM-CCA2) [10]

1998 年: Bellare, Desai, Poincheval, Rogaway (IND-CCA2 と NM-CCA2 の等価性の証明) [1]

1999 年: Bellare, Sahai (SNM と INM の等価性の証明) [4]

2003 年: Watanabe，Shikata, Imai (SS と IND の CCA1，CCA2 における等価性の証明) [46]

2007 年: Pass, Shelat, Vaikuntanathan (SNM′，INM′，SNM と INM に関する関係の証明) [38]

# 6 安全性の定義の関係

## 6.1 一方向性と強秘匿性の関係

**定理 6.1.** いかなる攻撃の種類 $ATK \in \{CPA, CCA1, CCA2\}$ に対しても，ある公開鍵暗号 $\Pi$ が *IND-ATK* 安全であるならば，$\Pi$ は *OW-ATK* 安全である．

証明. いかなる IND-ATK 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ に対しても $\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{B}}(k) < \epsilon(k)$ であると仮定するならば，いかなる OW-ATK 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対しても $\mathsf{Adv}^{\mathsf{OW\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ であることをゲーム列を用いて示す．なお，それぞれのゲーム Game $i$ において 1 が出力される事象を $S_i$ と置くことにする．

**Game 0:** Game 0 は OW-ATK 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ との通常の OW-ATK における実験とする．
Game 0 は $\Pr[S_0] = \Pr[\mathsf{Exp}^{\mathsf{OW\text{-}ATK}}_{\Pi,\mathcal{A}}(k) \to 1]$ である．

**命題 6.1.** $|\Pr[S_0] - 1/|\mathcal{M}_{pk}|| \leq \mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{B}}(k)$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. 具体的に $\mathcal{B}$ が内部で $\mathcal{A}$ を利用して以下の動作を行っている場合を考える．

| $\underline{\mathcal{B}_1^{\mathcal{O}_1}(pk)}$ | $\underline{\mathcal{B}_2^{\mathcal{O}_2}(c^*, s')}$ |
|---|---|
| $s \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $m' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$; |
| $m_0, m_1 \xleftarrow{\mathsf{U}} \mathcal{M}_{pk}$; | $m' = m_1$ ならば $b' := 1$; |
| $s' := (m_0, m_1, s)$: | $m' = m_0$ ならば $b' := 0$; |
| $(m_0, m_1, s)$ を出力 | そうでなければ $b' \xleftarrow{\mathsf{U}} \{0,1\}$: |
| | $b'$ を出力 |

上記のように $\mathcal{B}$ を構成した場合，$c^*$ が $m_0$ の暗号文であったときに $b' = 0$ が出力されるのは，$\mathcal{A}$ が $m' = m_0$ を出力するかあるいは $m' \notin \{m_0, m_1\}$ を出力した場合に $\mathcal{B}$ が $b' = 1$ となる値を $1/2$ の確率で選ぶかのいずれかである．よって

$$\Pr[\mathcal{B} \text{ が } 0 \text{ を出力} \mid b = 0] = \Pr[S_0] + \frac{1}{2}\Pr[\neg S_0 \wedge m' \neq m_1 \mid b = 0]$$

と表される．ただし，$\mathcal{A}$ からみて $m_0$ の暗号文を受け取っている場合に (つまり $b = 0$)，$\mathcal{B}$ が選んだ別の平文を $m' = m_1$ と当てることができる確率は高々$1/|\mathcal{M}_{pk}|$ であるので

$$\begin{aligned}\Pr[\neg S_0 \wedge m' \neq m_1 \mid b = 0] &= 1 - \Pr[S_0 \vee m' = m_1 \mid b = 0] \\ &= 1 - \Pr[S_0] - \frac{1}{|\mathcal{M}_{pk}|}\end{aligned}$$

表される．また，$c^*$ が $m_1$ の暗号文であったときに $b' = 1$ が出力される確率も $m_0$ の暗号文の時と同様に考えることができ

$$\begin{aligned}&\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{B}}(k) \\ &= |2 \cdot \Pr[b = b'] - 1| \\ &= |\Pr[\mathcal{B} \text{ が } 0 \text{ を出力} \mid b = 0] + \Pr[\mathcal{B} \text{ が } 1 \text{ を出力} \mid b = 1] - 1| \\ &= \left| \begin{array}{l} \Pr[S_0] + \frac{1}{2}\left(1 - \Pr[S_0] - \frac{1}{|\mathcal{M}_{pk}|}\right) \\ + \Pr[S_0] + \frac{1}{2}\left(1 - \Pr[S_0] - \frac{1}{|\mathcal{M}_{pk}|}\right) - 1 \end{array} \right| \\ &= \left|\Pr[S_0] - \frac{1}{|\mathcal{M}_{pk}|}\right|\end{aligned}$$

となる． ■

命題 6.1 より $\Pr[S_0] - 1/|\mathcal{M}_{pk}| \leq \mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\mathcal{B}}(k)$ であるので

$$\mathsf{Adv}^{\mathsf{OW\text{-}ATK}}_{\Pi,\mathcal{A}}(k) = \left|\Pr[S_0] - \frac{1}{|\mathcal{M}_{pk}|}\right| < \mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{B}}(k)$$

が得られる． □

## 6.2 強秘匿性の等価性

**定理 6.2.** いかなる攻撃の種類 $ATK \in \{CPA, CCA1, CCA2\}$ に対しても，公開鍵暗号が *SS-ATK* 安全であることと，*IND-ATK* 安全であることは等価である．

この定理は補題 6.1 および補題 6.2 から導くことができる．

**補題 6.1.** いかなる攻撃の種類 $ATK \in \{CPA, CCA1, CCA2\}$ に対しても，ある公開鍵暗号 $\Pi$ が *IND-ATK* 安全であるならば，$\Pi$ は *SS-ATK* 安全である．

証明. いかなる IND-ATK 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ に対しても $\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{B}} < \epsilon(k)$ であると仮定するならば，いかなる SS-ATK-1 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対してもアルゴリズム $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ が存在し，$\mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},h} < \epsilon(k)$ であることをゲーム列を用いて示す．なお，それぞれのゲーム Game $i$ において 1 が出力される事象を $S_i$ と置くことにする．

**Game 0:** Game 0 は SS-ATK 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ との通常の SS-ATK-0 における実験とする．
**Game 1:** Game 0 は $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ として $pk$ の下で行われているゲームであるが，新たに $(pk', sk') \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ を生成し $pk'$ の下で行われているゲームへと変更する．そのため，$\mathcal{A}_1$ に入力する値を $pk'$ に変更し，チャレンジ暗号文を $pk'$ を用いて生成し，$\mathcal{A}$ が利用する復号オラクル $\mathcal{O}'_1, cO'_2$ は $sk'$ の下で復号するオラクルとする．また，便宜上 $m_0 \xleftarrow{\mathsf{U}} \mathcal{M}$ を $m_0, m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$ と別の $m_1$ が選ばれているゲームとする．
**Game 2:** Game 1 において $m_0 \xleftarrow{\mathsf{U}} \mathcal{M}$ から生成しているチャレンジ暗号文 $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk', m_0)$ を $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk', m_1)$ へと変更する．
**Game 3:** Game 3 はアルゴリズム $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ との $pk$ の下での通常の SS-ATK-1 の実験とし，このとき $\mathcal{S}$ は内部で $\mathcal{A}$ を表 2 下部のように動作させているものとする．

それぞれ Game 0 から Game 3 までのゲームを表 2 に示す．
Game 0 は通常の SS-ATK-0 における実験であるので $\Pr[S_0] = \Pr[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A},h}(k) \to 1]$ である．よってその他のゲーム間における関係を以下の命題を用いて示す．

**命題 6.2.** $\Pr[S_1] = \Pr[S_0]$.

証明. Game 1 は $(pk', sk')$ の下で SS-ATK-1 の実験に $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ が追加されているだけであり，攻撃者には $(pk, sk)$ は一切入力されていない．また，$m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$ として選ばれた $m_1$ は攻撃者には一切入力されていないため，そのため攻撃者から見て Game 1 は通常の SS-ATK-1 による実験と識別不可能である．よって

$$\Pr[S_1] = \Pr[S_0]$$

が成り立つ． ■

表 2: 補題 6.1 の証明の流れと $\mathcal{S}$ の構成

| Game 0 (SS-ATK-0) | Game 1 |
|---|---|
| $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; |
| | $(pk', sk') \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; |
| $(\mathcal{M}, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $(\mathcal{M}, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}'_1}(pk')$; |
| $m_0 \xleftarrow{\mathsf{U}} \mathcal{M}$; | $m_0, m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$; |
| $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$; | $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk', m_0)$; |
| $(v, f) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m_0), s)$: | $(v, f) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), s)$: |
| $v = f(m_0)$ ならば 1 を出力 | $v = f(m_0)$ ならば 1 を出力 |
| $v \neq f(m_0)$ ならば 0 を出力 | $v \neq f(m_0)$ ならば 0 を出力 |
| **Game 2** | **Game 3** |
| $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; |
| $(pk', sk') \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ | |
| $(\mathcal{M}, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}'_1}(pk')$; | $(\mathcal{M}, s') \xleftarrow{\mathsf{R}} \mathcal{S}_1(pk)$; |
| $m_0, m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$; | $m_0 \xleftarrow{\mathsf{U}} \mathcal{M}$; |
| $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$; | |
| $(v, f) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m_0), s)$: | $(v, f) \xleftarrow{\mathsf{R}} \mathcal{S}_2(h(m_0), s')$: |
| $v = f(m_0)$ ならば 1 を出力 | $v = f(m_0)$ ならば 1 を出力 |
| $v \neq f(m_0)$ ならば 0 を出力 | $v \neq f(m_0)$ ならば 0 を出力 |
| **$\mathcal{S}_1(pk)$** | **$\mathcal{S}_2(h(m_0), s')$** |
| $(pk', sk') \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | $m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$; |
| $(\mathcal{M}, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}'_1}(pk')$; | $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk', m_1)$; |
| $s' := (s, pk', sk')$: | $(v, f) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_0), s)$: |
| $(\mathcal{M}, s')$ を出力 | $(v, f)$ を出力 |

**命題 6.3.** $|\Pr[S_2] - \Pr[S_1]| \leq \Pr[\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{B}}(k)]$ を満たす *IND-ATK* 攻撃者 $\mathcal{B}$ が存在する．

証明. Game 2 において 1 が出力される確率 $\Pr[S_2]$ と Game 1 において 1 が出力される確率 $\Pr[S_1]$ の差が $\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{B}}(k)$ で抑えられることを示そう．

公開鍵暗号 $\Pi$ において $(pk', sk')$ の下での IND-ATK-$b$ の実験を考えたときに，IND-ATK 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ が $\mathcal{A}$ を内部で以下のように利用した場合を考える．

| $\underline{\mathcal{B}_1^{\mathcal{O}'_1}(pk')}$ | $\underline{\mathcal{B}_2^{\mathcal{O}'_2}(c^*, s')}$ |
|---|---|
| $(\mathcal{M}, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}'_1}(pk')$; | $(v, f) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}'_2}(c^*, h(m_1), s)$; |
| $m_0, m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$; | $b' := 1$ if $v = f(m_0)$; |
| $s' := (m_0, m_1, s)$: | $b' := 0$ if $v \neq f(m_0)$: |
| $(m_0, m_1, s')$ を出力 | $b'$ を出力 |

IND-ATK-0 の実験において $\mathcal{B}$ が 1 を出力するのは，内部で利用している $\mathcal{A}_2$ が $m_0$ の暗号文を受け取っている状態で $v = f(m_0)$ なる $(v, f)$ を出力する場合であり，これは Game 2 において 1 が出力される場合と等価である．よって $\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B}}(k) \to 1] = \Pr[S_2]$ である．一方，IND-ATK-1 の実験において $\mathcal{B}$ が 1 を出力するのは，内部で利用している $\mathcal{A}_2$ が $m_1$ の暗号文を受け取っている状態で $v = f(m_0)$ なる $(v, f)$ を出力する場合であり，これは Game 3 において 1 が出力される場合と等価である．よって $\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{B}}(k) \to 1] = \Pr[S_3]$ である．つまり，

$$
\begin{aligned}
|\Pr[S_2] - \Pr[S_1]| &\leq \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{B}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B}}(k) \to 1\right] \end{array} \right| \\
&= \mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{B}}(k)
\end{aligned}
$$

である． ■

**命題 6.4.** $\Pr[S_3] = \Pr[S_2]$.

証明. Game 3 において，$\mathcal{S}$ は $\mathcal{A}$ を用いて表 2 下部のように動作している．このときの $\mathcal{S}$ の出力が Game 2 における $\mathcal{A}$ の出力と等価であることを示そう．Game 3 は $pk$ の下での通常の SS-ATK-1 の実験であるので $\mathcal{S}$ には復号オラクルは与えられない．しかし，$\mathcal{S}$ は内部で $(pk', sk')$ を生成しており $\mathcal{A}$ には Game 2 のように $pk'$ を入力するため，$\mathcal{A}$ が復号オラクルにクエリを聞いてきた場合は $sk'$ を用いることで正しく返答することができる．$\mathcal{S}$ は内部で生成した $m_1$ の暗号文を $\mathcal{A}_2$ に入力しており，$\mathcal{A}_2$ の出力 $(v, f)$ を最終的な出力としているため，Game 3 における $\mathcal{S}$ の出力は Game 2 における $\mathcal{A}$ の出力と等価な分布である．よって $S_3$ が起きる確率は Game 2 において 1 が出力される確率，つまり $S_2$ が起きる確率と同じであるため

$$\Pr[S_3] = \Pr[S_2]$$

表 3: 補題 6.2 の証明の流れ

| Game 0 (IND-ATK-0) | Game 1 |
|---|---|
| $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; |
| $(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; |
| $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$; | $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$; |
| $b' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$: | $b' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$: |
| $b'$ を出力 | $b'$ を出力 |

が得られる． ■

なお，Game 3 は SS-ATK-1 の実験としているので，$\Pr[S_3] = \Pr[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},h}(k) \to 1]$ と表される．最終的に

$$\begin{aligned}\mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},h}(k) &= \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A},h}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}',h}(k) \to 1\right] \end{array} \right| \\ &= |\Pr[S_0] - \Pr[S_3]| \\ &\leq \mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(k)\end{aligned}$$

が得られ，$\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ であることを仮定していたので，$\mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},h}(k) < \epsilon(k)$ となる．よって補題 6.1 が証明された． □

**補題 6.2.** いかなる攻撃の種類 $ATK \in \{CPA, CCA1, CCA2\}$ に対しても，ある公開鍵暗号 $\Pi$ が *SS-ATK* 安全であるならば，$\Pi$ は *IND-ATK* 安全である．

証明. ゲーム列を用いて，いかなる SS-ATK-1 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ に対してもあるアルゴリズム $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ が存在し $\mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{B},\mathcal{S},h} < \epsilon(k)$ であると仮定するならば，いかなる IND-ATK 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対しても $\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}} < \epsilon(k)$ であることを示す．なお，それぞれのゲーム Game $i$ において 1 が出力される事象を $S_i$ と置くことにする．

**Game 0:** Game 0 は IND-ATK 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ との通常の IND-ATK-0 における実験とする．
**Game 1:** Game 1 では Game 0 におけるチャレンジ暗号文を $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$ から $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$ へと変更する．それぞれの Game 0 と Game 1 は表 3 のように表される．

Game 0 は通常の IND-ATK-0 における実験であり Game 1 は IND-ATK-1 と等価であるので，$\Pr[S_0] = \Pr[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B}}(k) \to 1]$，$\Pr[S_1] = \Pr[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{B}}(k) \to 1]$

と表される．そこで，この 2 つのゲームにおける出力の差が SS-ATK ゲームにおける優位性で抑えられることを示そう．

**命題 6.5.** *SS-ATK-0* の実験において平文空間が $\mathcal{M} := \{m_0, m_1\}$ とされ $m_b$ からチャレンジ暗号文が生成されたものとする．このとき，$\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1] = \Pr[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B},h}(k) \to 1 \mid b = 0]$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. 具体的に，Π に対する SS-ATK-0 の実験を行う $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ が内部で $\mathcal{A}$ を以下のように動作させている場合を考える．なお，ここでは SS-ATK-0 に用いられている $h$ は何も出力しない関数とし，$\mathcal{B}_2$ にはいかなる部分情報も入力されないものとする．

| | |
|---|---|
| $\underline{\mathcal{B}_1^{\mathcal{O}_1}(pk)}$ | $\underline{\mathcal{B}_2^{\mathcal{O}_2}(c^*, s')}$ |
| $(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $b' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$; |
| $\mathcal{M} := \{m_0, m_1\}$; | $v := m_{1-b'}$, $f$ : 恒等写像: |
| $s' := (m_0, m_1, s)$: | $(v, f)$ を出力 |
| $(\mathcal{M}, s')$ を出力 | |

攻撃者 $\mathcal{B}_1$ が $\mathcal{M} := \{m_0, m_1\}$ とした平文空間の中から $m_0$ が選ばれてチャレンジ暗号文 $c^*$ が生成された場合，$\mathcal{A}$ からみてこれは IND-ATK-0 そのものである．また，上記の SS-ATK-0 の実験において 1 が出力されるのは $\mathcal{B}$ が $v = f(m_0)$ を満たす $(v, f)$ を出力する場合であり，それは $\mathcal{A}$ が $b' := 1$ を出力するときのみである．よって

$$\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{Pi,\mathcal{A}}(k) \to 1] = \Pr[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}0}}_{\mathcal{B},h}(k) \to 1 \mid b = 0]$$

となる． ■

**命題 6.6.** *SS-ATK-0* の実験において平文空間が $\mathcal{M} := \{m_0, m_1\}$ とされ $m_b$ からチャレンジ暗号文が生成されたものとする．このとき，$\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1] = \Pr[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B}',h}(k) \to 1 \mid b = 1]$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}'$ が存在する．

証明. 命題 6.5 と同様に，Π に対する SS-ATK-1 の実験を行う $\mathcal{B}' = (\mathcal{B}'_1, \mathcal{B}'_2)$ が内部で $\mathcal{A}$ を以下のように動作させている場合を考える．なお，ここでは SS-ATK に用いられている $h$ は何も出力しない関数とし，$\mathcal{B}'_2$ にはいかなる部分情報も入力されないものとする．

| | |
|---|---|
| $\underline{\mathcal{B}_1'^{\mathcal{O}_1}(pk)}$ | $\underline{\mathcal{B}_2'^{\mathcal{O}_2}(c^*, s')}$ |
| $(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $b' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$; |
| $\mathcal{M} := \{m_0, m_1\}$; | $v := m_{b'}$, $f$ : 恒等写像: |
| $s' := (m_0, m_1, s)$: | $(v, f)$ を出力 |
| $(\mathcal{M}, s)$ を出力 | |

上記の構成が命題 6.5 のものと異なるのは $v$ の値を $v := m_{b'}$ としている点である．もし $\mathcal{B}_1'$ が $\mathcal{M} := \{m_0, m_1\}$ とした平文空間の中から $m_1$ が選ばれてチャレンジ暗号文 $c^*$ が生成された場合，$\mathcal{A}$ からみてこれは IND-ATK-1 そのものである．また，上記の SS-ATK-0 実験において 1 が出力されるのは $\mathcal{B}'$ が $v = f(m_1)$ を満たす $(v, f)$ を出力する場合であり，それは $\mathcal{A}$ が $b' := 1$ を出力するときのみである．よって

$$\Pr[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\mathsf{IND\text{-}ATK\text{-}1}}(k) \to 1] = \Pr[\mathsf{Exp}_{\Pi,\mathcal{B}',h}^{\mathsf{SS\text{-}ATK\text{-}0}}(k) \to 1 \mid b = 1]$$

である． ■

なお，$\Pi$ は SS-ATK 安全であることを仮定しているので，あるアルゴリズム $\mathcal{S}, \mathcal{S}'$ が存在して

$$\left| \begin{array}{l} \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B},h}^{\mathsf{SS\text{-}ATK\text{-}0}}(k) \to 1 \mid b = 0\right] \\ -\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{S},h}^{\mathsf{SS\text{-}ATK\text{-}1}}(k) \to 1 \mid b = 0\right] \end{array} \right| = \mathsf{Adv}_{\Pi,\mathcal{B},\mathcal{S},h}^{\mathsf{SS\text{-}ATK}}(k)$$

$$\left| \begin{array}{l} \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}',h}^{\mathsf{SS\text{-}ATK\text{-}0}}(k) \to 1 \mid b = 1\right] \\ -\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{S}',h}^{\mathsf{SS\text{-}ATK\text{-}1}}(k) \to 1 \mid b = 1\right] \end{array} \right| = \mathsf{Adv}_{\Pi,\mathcal{B}',\mathcal{S}',h}^{\mathsf{SS\text{-}ATK}}(k)$$

である．ただし，このとき SS-ATK-1 の実験を考えると，$\mathcal{S}$ には $m_1, m_0$ の部分情報は一切入力されていないため，$\mathcal{S}$ からみて $m_0$ が選ばれたときに $v = f(m_0)$ なる $(v, f)$ を出力する確率も $m_1$ が選ばれたときに $v = f(m_1)$ なる $(v, f)$ を出力する確率も $1/2$ である．つまり

$$\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{S},h}^{\mathsf{SS\text{-}ATK\text{-}1}}(k) \to 1 \mid b = 1\right] = \frac{1}{2}$$
$$\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{S}',h}^{\mathsf{SS\text{-}ATK\text{-}1}}(k) \to 1 \mid b = 0\right] = \frac{1}{2}$$

である．よって

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(k) &= \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1\right] \end{array} \right| \\
&= \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B},h}(k) \to 1 \mid b=0\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B}',h}(k) \to 1 \mid b=1\right] \end{array} \right| \\
&\leq \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},h}(k) \to 1 \mid b=0\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{SS\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S}',h}(k) \to 1 \mid b=1\right] \end{array} \right| \\
&\quad + \mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{B},\mathcal{S},h}(k) + \mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{B}',\mathcal{S}',h}(k) \\
&= \mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{B},\mathcal{S},h}(k) + \mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{B}',\mathcal{S}',h}(k)
\end{aligned}
$$

が得られる．仮定より $\Pi$ は SS-ATK 安全であるので $\mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{B},\mathcal{S},h}(k) < \epsilon(k)$ および $\mathsf{Adv}^{\mathsf{SS\text{-}ATK}}_{\Pi,\mathcal{B}',\mathcal{S}',h}(k) < \epsilon(k)$ であるので $\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ である． □

## 6.3 強秘匿性と頑強性の関係

まずは，強秘匿性における IND-ATK と，頑強性における INM-ATK の関係について議論しよう．

INM-ATK が 4.3.2 節の IND-ATK と異なる点は，最終的な出力がチャレンジ暗号文 $c^*$ の平文 $m_b$ を推測するためのビット $b'$ ではなく暗号文の集合となっていることである．もし IND-ATK を破ることができる攻撃者 $\mathcal{B}$ が存在するならば，その攻撃者を内部で利用することで $\mathcal{B}$ が出力したビット $b'$ から $m_{b'}$ を暗号化したものを $c_1 := \mathsf{Enc}(pk, m_{b'})$ として出力するアルゴリズム $\mathcal{B}'$ は INM-ATK を破ることができる．つまり，ある公開鍵暗号方式が INM-ATK 安全であるならば，IND-ATK 安全であることが以下の定理を証明することで示すことができる．

**定理 6.3.** 攻撃の種類 $ATK \in \{CPA, CCA1, CCA2\}$ に関して，ある公開鍵暗号方式 $\Pi$ が *INM-ATK* 安全であるならば，$\Pi$ は *IND-ATK* 安全である．

証明. ゲーム列を用いて，いかなる INM-ATK 攻撃者 $\mathcal{B}$ に対しても $\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{B}} < \epsilon$ であると仮定するならば，いかなる IND-ATK 攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}} < \epsilon$ であることを示す．なお，それぞれのゲーム Game $i$ において 1 が出力される事象を $S_i$ と置くことにする．

**Game 0:** Game 0 は IND-ATK 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対する通常の IND-ATK-0 の実験とする．

**Game 1:** Game 0 における $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$ を $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$ へと置き換える．

それぞれ Game 0 と Game 1 は以下のように表される．

| Game 0 (IND-ATK-0) | Game 1 |
|---|---|
| $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; |
| $(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; |
| $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$; | $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$; |
| $b' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$; | $b' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$; |
| $b'$ を出力 | $b'$ を出力 |

Game 0 は通常の IND-ATK-0 の実験であり，Game 0 から $c^*$ を $m_0$ の暗号文から $m_1$ の暗号文へと変更した Game 1 は IND-ATK-1 の実験そのものであるので $S_0 = \Pr[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\mathsf{IND\text{-}ATK\text{-}0}}(k) \to 1]$，$S_1 = \Pr[\mathsf{Exp}_{\Pi,\mathcal{A}}^{\mathsf{IND\text{-}ATK\text{-}1}}(k) \to 1]$ である．そこで，Game 0 と Game 1 において 1 が出力される確率の差が INM-ATK の実験における優位性 $\mathsf{Adv}_{\Pi,\mathcal{B}}^{\mathsf{INM\text{-}ATK}}(k)$ で抑えられることを示そう．

**命題 6.7.** $|\Pr[S_1] - \Pr[S_0]| < \mathsf{Adv}_{\Pi,\mathcal{B}}^{\mathsf{INM\text{-}ATK}}(k)$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. 命題 6.7 を証明するため，Π に対しての INM-ATK-$b$ の実験を考える．そして，このとき INM-ATK 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ が内部で IND-ATK 攻撃者 $\mathcal{A}$ を以下のように利用しているとする．

| $\mathcal{B}_1^{\mathcal{O}_1}(pk)$ | $\mathcal{B}_2^{\mathcal{O}_2}(c^*, s_1)$ |
|---|---|
| $(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $b' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$; |
| $s_1 := (s, m_0, m_1)$: | $c_{b'} \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_{b'})$; |
| $(m_0, m_1, s_1)$ を出力 | $s_2 := (m_0, m_1)$: |
| $\mathcal{B}_3(d_1, s_2)$: | $(c_{b'}, s_2)$ を出力 |
| $d_1 = m_1$ ならば 1 を出力 | |
| $d_1 \neq m_1$ ならば 0 を出力 | |

もし INM-ATK-0 の実験が行われていたならば，$\mathcal{B}_3$ が 1 を出力するのは $\mathcal{A}_2$ が $m_0$ の暗号文 $c^*$ を受け取っているときに $b' = 1$ を出力した場合であり，これは Game 0 において 1 が出力される場合と等価である．よって $\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\mathsf{INM\text{-}ATK\text{-}0}}(k) \to 1\right] = \Pr[S_0]$ である．

一方，INM-ATK-1 の実験が行われていたならば，$\mathcal{B}_3$ が 1 を出力するのは $\mathcal{A}_2$ が $m_1$ の暗号文 $c^*$ を受け取っているときに $b' = 1$ を出力した場合であり，これは Game 1 において 1 が出力される場合と等価である．よって $\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\mathsf{INM\text{-}ATK\text{-}1}}(k) \to 1\right] = \Pr[S_1]$ である．

よって

$$
\begin{aligned}
|\Pr[S_1] - \Pr[S_0]| &\leq \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{B}}(k) \to 1\right] \end{array} \right| \\
&= \mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{B}}(k)
\end{aligned}
$$

となる．■

最終的に，

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(k) &= \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1\right] \end{array} \right| \\
&= |\Pr[S_0] - \Pr[S_1]| \\
&\leq \mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{B}}(k)
\end{aligned}
$$

が得られる．$\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{B}}(k) < \epsilon(k)$ であることを仮定しているので $\mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ が満たされる．□

次に，公開鍵暗号方式 Π が IND-CCA2 安全であるならば INM-CCA2 安全であること，そして攻撃の種類が ATK ∈ {CCA1, CPA} の場合は IND-ATK 安全であったとしても INM-ATK 安全ではない方式の具体例を示す．

**定理 6.4.** ある公開鍵暗号方式 Π が *IND-CCA2* 安全であるならば，Π は *INM-CCA2* 安全である．

証明．ゲーム列を用いて，いかなる IND-CCA2 攻撃者 $\mathcal{B}$ に対しても $\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\mathcal{B}}(k) < \epsilon(k)$ が満たされていると仮定するならば，いかなる INM-CCA2 攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}^{\mathsf{INM\text{-}CCA2}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ であることを示す．なお，それぞれのゲーム Game $i$ において 1 が出力される事象を $S_i$ と置くことにする．

**Game 0:** Game 0 は INM-CCA2 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ との通常の INM-CCA2-0 の実験とする．
**Game 1:** Game 1 は Game 0 における $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$ を $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$ に置き換えたものとする．

それぞれ Game 0 と Game 1 は以下のように表される．

Game 0 (INM-CCA2-0)
$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$;
$(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$;
$\mathbf{c} \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$;
$(c_1, \ldots, c_n) := \mathbf{c}$;
  $d_i := \mathsf{Dec}(pk, c_i)$;
$b' \xleftarrow{\mathsf{R}} \mathcal{A}_3(d_1, \ldots, d_n)$:
$b'$ を出力

Game 1
$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$;
$(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$;
$\mathbf{c} \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s)$;
$(c_1, \ldots, c_n) := \mathbf{c}$;
  $d_i := \mathsf{Dec}(pk, c_i)$;
$b' \xleftarrow{\mathsf{R}} \mathcal{A}_3(d_1, \ldots, d_n)$:
$b'$ を出力

Game 0 は通常の INM-CCA2-0 の実験であり，Game 0 から $c^*$ を $m_0$ の暗号文から $m_1$ の暗号文へと変更した Game 1 は INM-CCA2-1 の実験そのものであるので $S_0 = \Pr[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1]$，$S_1 = \Pr[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1]$ である．そこで，Game 0 と Game 1 において 1 が出力される確率の差が IND-CCA2 の実験における優位性 $\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\mathcal{B}}(k)$ で抑えられることを示そう．

**命題 6.8.** $|\Pr[S_1] - \Pr[S_0]| < \mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\mathcal{B}}(k)$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. 命題 6.8 を証明するため，Π に対しての IND-ATK-$b$ の実験を考える．そして，このとき IND-ATK 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ が内部で $\mathcal{A}$ を以下のように動作させているとする．

$\mathcal{B}_1^{\mathcal{O}_1}(pk)$
$(m_0, m_1, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$s := s_1$:
$(m_0, m_1, s)$ を出力

$\mathcal{B}_2^{\mathcal{O}_2}(c^*, s)$
$(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s_1)$;
$(c_1, \ldots, c_n) := \mathbf{c}$;
  $c_i = c^*$ ならば $d_i := \perp'$;
  そうでなければ $d_i := \mathcal{O}_2(\cdot, c_i)$;
$b' \xleftarrow{\mathsf{R}} \mathcal{A}_3(d_1, \ldots, d_n, s_2)$:
$b'$ を出力

IND-CCA2-0 の実験が行われていたときに $\mathcal{B}$ が 1 を出力するのは，内部で動作している $\mathcal{A}_2$ が $m_0$ の暗号文 $c^*$ を受け取っているときに出力した値の ($c^*$ を除いた) 復号結果を $\mathcal{A}_3$ に入力したとき，$\mathcal{A}_3$ が $b' = 1$ を出力した場合である．これは Game 0 において 1 が出力される場合と等価であるので，$\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B}}(k) \to 1\right] = \Pr[S_0]$ である．

一方，INM-CCA2-1 の実験が行われていたときに $\mathcal{B}$ が 1 を出力するのは，内部で動作している $\mathcal{A}_2$ が $m_1$ の暗号文 $c^*$ を受け取っているときに出力した値の ($c^*$ を除いた) 復号結果を $\mathcal{A}_3$ に入力したとき，$\mathcal{A}_3$ が $b' = 1$ を出力した場合である．これは Game 1 にお

いて 1 が出力される場合と等価であるので，よって $\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{B}}(k) \to 1\right] = \Pr[S_1]$ である．

よって

$$\begin{aligned}|\Pr[S_1] - \Pr[S_0]| &\leq \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}CCA2\text{-}1}}_{\Pi,\mathcal{B}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}CCA2\text{-}0}}_{\Pi,\mathcal{B}}(k) \to 1\right] \end{array} \right| \\ &= \mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{B}}(k)\end{aligned}$$

となる． ■

最終的に，

$$\begin{aligned}\mathsf{Adv}^{\mathsf{INM\text{-}CCA2}}_{\Pi,\mathcal{A}}(k) &= \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{INM\text{-}CCA2\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{INM\text{-}CCA2\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1\right] \end{array} \right| \\ &= |\Pr[S_0] - \Pr[S_1]| \\ &\leq \mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\mathcal{B}}(k)\end{aligned}$$

が得られる．$\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\mathcal{B}}(k) < \epsilon(k)$ であることを仮定していたので，$\mathsf{Adv}^{\mathsf{INM\text{-}CCA2}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ が得られる． □

前述の定理 6.3 および定理 6.4 により，IND-CCA2 と INM-CCA2 は等価であることが示された．一方，ATK $\in \{\mathrm{CPA}, \mathrm{CCA1}\}$ に関しては IND-ATK と INM-ATK には安全性に差があることを示そう．

**定理 6.5.** 攻撃の種類 $ATK \in \{\mathrm{CPA}, \mathrm{CCA1}\}$ に関して，*IND-ATK* 安全かつ *INM-ATK* 安全ではない公開鍵暗号方式が存在する．

証明. 定理 6.5 は以下に示す補題 6.3 から導くことができる． □

**補題 6.3.** ある公開鍵暗号方式 $\Pi$ が *IND-CCA1* 安全性を満たす場合，*IND-CCA1* 安全かつ *INM-CPA* 安全ではない公開鍵暗号方式 $\Pi'$ が存在する．

証明. ある公開鍵暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が IND-CCA1 安全である場合に，以下のような公開鍵暗号方式 $\Pi'$ を考え，$\Pi'$ が IND-CCA1 安全かつ INM-CPA 安全でないことを示す．

$\mathsf{Gen}'(1^k)$**:** $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ を行い，$pk' := pk, sk' := sk$ として $(pk', sk')$ を出力する．

$\mathsf{Enc}'(pk', m)$**:** $m$ の各ビットを反転させた平文を $\bar{m}$ と置く．$c_1 \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m), c_2 \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \bar{m})$ を求め，$c := c_1 \| c_2$ を出力する．

$\mathsf{Dec}'(sk', c)$: $m' := \mathsf{Dec}(sk, c_1)$ を出力する．

上記の公開鍵暗号方式 $\Pi'$ に対して，補題 6.4 および補題 6.5 を示すことで，補題 6.3 は証明される． □

**補題 6.4.** $\Pi$ が *IND-CCA1* 安全ならば $\Pi'$ は *IND-CCA1* 安全な公開鍵暗号方式である．

証明. ゲーム列を用いて，$\Pi$ に対するいかなる IND-CCA1 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ に対しても $\mathsf{Adv}^{\mathsf{IND\text{-}CCA1}}_{\Pi,\mathcal{B}} < \epsilon(k)$ であるならば，$\Pi'$ に対するいかなる IND-CCA1 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対しても $\mathsf{Adv}^{\mathsf{IND\text{-}CCA1}}_{\Pi',\mathcal{A}} < \epsilon(k)$ であることを示す．なお，それぞれのゲーム Game $i$ において 1 が出力される事象を $S_i$ と置くことにする．

**Game 0:** Game 0 は通常の $\Pi'$ に対しての攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ との IND-CCA1-0 の実験とする．
**Game 1:** Game 1 は Game 0 における $c_2^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \bar{m_0})$ を，$c_2^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \bar{m_1})$ へと変更する．
**Game 2:** Game 2 では，Game 1 における $c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$ を $c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$ へと変更する．

それぞれ Game 0 から Game 2 までのゲームは以下のように表される．

| Game 0 (IND-ATK-0) | Game 1 |
|---|---|
| $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}'(1^k)$;<br>$(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;<br>$c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$;<br>$c_2^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \bar{m_0})$;<br>$c^* := (c_1^*, c_2^*)$;<br>$b' \xleftarrow{\mathsf{R}} \mathcal{A}_2(c^*, s)$:<br>$b'$ を出力 | $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}'(1^k)$;<br>$(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;<br>$c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$;<br>$c_2^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \bar{m_1})$;<br>$c^* := (c_1^*, c_2^*)$;<br>$b' \xleftarrow{\mathsf{R}} \mathcal{A}_2(c^*, s)$:<br>$b'$ を出力 |
| Game 2 | |
| $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$;<br>$(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;<br>$c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$;<br>$c_2^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \bar{m_1})$;<br>$c^* := (c_1^*, c_2^*)$;<br>$b' \xleftarrow{\mathsf{R}} \mathcal{A}_2(c^*, s)$:<br>$b'$ を出力 | |

Game 0 は通常の IND-CCA1-0 の実験であるので

$$\Pr[S_0] = \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}CCA1\text{-}0}}_{\Pi',\mathcal{B}'}(k) \to 1\right]$$

である．よってその他のゲーム間での関係について以下の命題を証明する．

**命題 6.9.** $|\Pr[S_1] - \Pr[S_0]| \leq \mathsf{Adv}^{\mathsf{IND\text{-}CCA1}}_{\Pi,\mathcal{B}}(k)$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. $\Pi$ に対して攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ との IND-CCA1-$b$ の実験を考え，$\mathcal{B}$ が $\mathcal{B}'$ を以下のように利用している場合を考える．

| | |
|---|---|
| $\underline{\mathcal{B}_1^{\mathcal{O}_1}(pk)}$ | $\underline{\mathcal{B}_2(c_2^*, s)}$ |
| $(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{B}_1'^{\mathcal{O}_1}(pk)$: | $c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$; |
| $(\bar{m_0}, \bar{m_1}, s)$ を出力 | $c^* := (c_1^*, c_2^*)$; |
| | $b' \xleftarrow{\mathsf{R}} \mathcal{B}_2'(c^*, s)$: |
| | $b'$ を出力 |

IND-CCA1-0 の実験が行われたときに $\mathcal{B}$ が 1 を出力するのは，内部で動作している $\mathcal{A}$ が $c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0), c_2^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \bar{m_0})$ としてチャレンジ暗号文を受け取っているときに 1 を出力した場合である．$\mathcal{A}$ からみてこれは Game 0 における動作と等価であるので $\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA1\text{-}0}}_{\Pi,\mathcal{B}} \to 1] = \Pr[S_0]$ である．一方，IND-CCA1-1 の実験が行われたときに $\mathcal{B}$ が 1 を出力するのは，内部で動作している $\mathcal{A}$ が $c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0), c_2^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \bar{m_1})$ としてチャレンジ暗号文を受け取っているときに 1 を出力した場合である．$\mathcal{A}$ からみてこれは Game 1 における動作と等価であるので $\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA1\text{-}1}}_{\Pi,\mathcal{B}} \to 1] = \Pr[S_1]$ である．よって

$$\begin{aligned} |\Pr[S_1] - \Pr[S_0]| &\leq \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}1}}_{\Pi,\mathcal{B}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B}}(k) \to 1\right] \end{array} \right| \\ &\leq \mathsf{Adv}^{\mathsf{IND\text{-}ATK}}_{\Pi,\mathcal{B}}(k) \end{aligned}$$

が成り立つ． ■

**命題 6.10.** $|\Pr[S_2] - \Pr[S_1]| \leq \mathsf{Adv}^{\mathsf{IND\text{-}CCA1}}_{\Pi,\mathcal{B}}(k)$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}$ が存在する．

証明. これは命題 6.9 の証明方針と同様であり，$\mathcal{B}$ に対するチャレンジ暗号文を $c_1^*$ とすれば明らかである． ■

最終的に，

$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{IND\text{-}CCA1}}_{\Pi',\mathcal{A}}(k) \\
&= \left|\left[\mathsf{Exp}^{\mathsf{IND\text{-}CCA1\text{-}0}}_{\Pi',\mathcal{A}}(k) \to 1\right] - \left[\mathsf{Exp}^{\mathsf{IND\text{-}CCA1\text{-}1}}_{\Pi',\mathcal{A}}(k) \to 1\right]\right| \\
&= |\Pr[S_0] - \Pr[S_3]| \\
&\leq 2 \cdot \mathsf{Adv}^{\mathsf{IND\text{-}CCA1}}_{\Pi,\mathcal{B}}(k)
\end{aligned}$$

が得られる．$\mathsf{Adv}^{\mathsf{IND\text{-}CCA1}}_{\Pi,\mathcal{B}}(k) < \epsilon(k)$ であることを仮定していたので，$\mathsf{Adv}^{\mathsf{IND\text{-}CCA1}}_{\Pi',\mathcal{A}}(k) < \epsilon(k)$ である． □

**補題 6.5.** $\Pi'$ は *INM-CPA* 安全な公開鍵暗号方式ではない．

証明．$\Pi'$ に対する INM-CPA 攻撃者 $\mathcal{A}$ が以下のような動作を行っている場合を考える．

| | |
|---|---|
| $\underline{\mathcal{A}_1(pk)}$ | $\underline{\mathcal{A}_2(c^*, s)}$ |
| $m_0, m_1 \xleftarrow{\mathsf{U}} \mathcal{M}_{pk}$; | $c_1^* \| c_2^* := c^*$; |
| $s_1 := m_1$: | $c_1 := c_2^* \| c_1^*$; |
| $(m_0, m_1, s_1)$ を出力 | $s_2 := m_1$; |
| $\underline{\mathcal{A}_3(d_1, s_2)}$ | $(c_1, s_2)$ を出力 |
| $d_1 = \bar{m_1}$ ならば 1 を出力 | |
| $d_1 \neq \bar{m_1}$ ならば 0 を出力 | |

INM-CPA-0 の実験が行われていた場合，$\mathcal{A}_2$ に入力される $c^*$ は $c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$, $c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \bar{m_0})$ として求められた $c^* := c_1^* \| c_2^*$ が入力される．つまり $c' = c_2^* \| c_1^*$ の $\mathsf{Dec}'$ による復号結果は $\bar{m_0}$ であり，$\mathcal{A}_3$ の構成からこの場合常に 0 が出力される．

一方，INM-CPA-1 の実験が行われていた場合，$c^*$ は $c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$，$c_1^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \bar{m_1})$ として求められた $c^* := c_1^* \| c_2^*$ となったものが入力され，$c' = c_2^* \| c_1^*$ の $\mathsf{Dec}'$ による復号結果は $\bar{m_1}$ である．そのため $\mathcal{B}_3$ は常に 1 を出力する．

よって $\mathsf{Adv}^{\mathsf{INM\text{-}CPA}}_{\Pi',\mathcal{A}}(k) < \epsilon(k)$ とはならないので $\Pi'$ は INM-CPA 安全ではない． □

## 6.4 頑強性の関係

表 1 にあるように，頑強性として定義される 4 つの安全性 (SNM, SNM′, INM, INM′) は攻撃法によって安全性が異なる．今回は，一般的な公開鍵暗号についての安全性として考えられている SNM-ATK と INM-ATK に関してのみに焦点を当て，この 2 つの定義が等価であることを証明しよう．

**定理 6.6.** 攻撃の種類 $ATK \in \{CPA,\ CCA1,\ CCA2\}$ において，ある公開鍵暗号 $\Pi$ が *INM-ATK* 安全であるならば $\Pi$ は *SNM-ATK* 安全である．

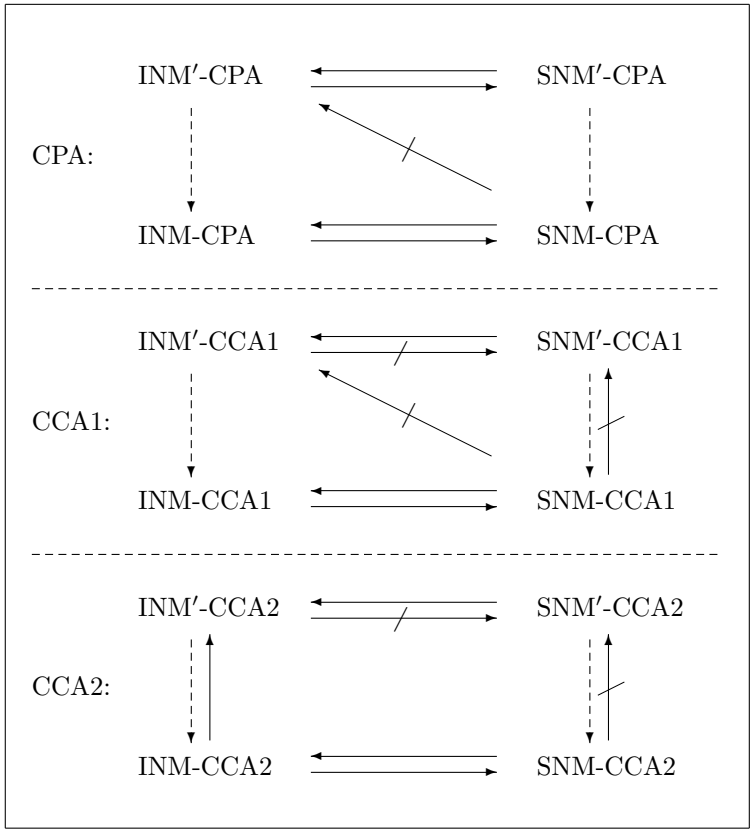


図 7: Non-Malleability の関係

証明. ゲーム列を用いて，いかなる INM-ATK 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ に対しても $\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{B}}(k) < \epsilon(k)$ が満たされているならば，いかなる SNM-ATK 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対してもアルゴリズム $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ が存在し，$\mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{R},h}(k) < \epsilon(k)$ であることを示す．なお，それぞれのゲーム Game $i$ において 1 が出力される事象を $S_i$ と置くことにする．

**Game 0:** Game 0 は SNM-CPA 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ との通常の SNM-ATK-0 における実験とする．
**Game 1:** Game 1 は $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ として $pk$ の下で行われているゲームであるが，新たに $(pk', sk') \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ を生成し $pk'$ の下で行われているゲームへと変更する．そのため，$\mathcal{A}_1$ に入力する値を $pk'$ に変更し，チャレンジ暗号文を $pk'$ を用いて生成し，$\mathcal{A}$ が復号オラクルを利用した場合は $sk'$ の下で復号したものを返答する．また，便宜上 $m_0 \xleftarrow{\mathsf{U}} \mathcal{M}$ を $m_0, m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$ と別の $m_1$ が選ばれているゲームとする．
**Game 2:** Game 1 において入力されている暗号文 $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$ を $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$ へと変更する．
**Game 3:** Game 3 はアルゴリズム $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ との SNM-CPA-1 の実験とし，このとき $\mathcal{S}$ が $\mathcal{A}$ を内部で表 5 のように利用している場合を考える．

Game 0 は通常の SNM-ATK-0 における実験であり $\Pr[S_0] = \Pr[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A},\mathcal{R},h}(k) \to 1]$ と表される．よってその他のゲーム間における関係を以下の命題を用いて示す.

**命題 6.11.** $\Pr[S_1] = \Pr[S_0]$.

証明. Game 1 は $(pk', sk')$ の下での SS-ATK-1 の実験に $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ が追加されているだけであり，攻撃者には $(pk, sk)$ は一切入力されていない．また，$m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$ として選ばれた $m_1$ は攻撃者には一切入力されていないため，そのため攻撃者から見て Game 1 は Game 0 と完全に識別不可能である．よって

$$\Pr[S_1] = \Pr[S_0]$$

が成り立つ． ■

**命題 6.12.** $|\Pr[S_2] - \Pr[S_1]| \leq \Pr[\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{B}}(k)]$ を満たす *INM-ATK* 攻撃者 $\mathcal{B}$ が存在する．

証明. Game 2 において 1 が出力される確率 $\Pr[S_2]$ と Game 1 において 1 が出力される確率 $\Pr[S_1]$ の差が $\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{B}}(k)$ で抑えられることを示そう．

公開鍵暗号 $\Pi$ において $(pk', sk')$ の下での INM-ATK-$b$ の実験を考えたときに，IND-ATK 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$ が $\mathcal{A}$ を内部で以下のように利用した場合を考える．

表 4: 定理 6.6 の証明の流れ

| Game 0 (SNM-ATK-0) | Game 1 |
|---|---|
| $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; |
| | $(pk', sk') \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; |
| $(\mathcal{M}, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $(\mathcal{M}, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}'_1}(pk')$; |
| $m_0 \xleftarrow{\mathsf{U}} \mathcal{M}$; | $m_0, m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$; |
| $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$; | $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk', m_0)$; |
| $(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_"}(c^*, h(m_0), s_1)$; | $(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2(c^*, h(m_0), s_1)$; |
| $(c_1, \ldots, c_n) := \mathbf{c}$; | $(c_1, \ldots, c_n) := \mathbf{c}$; |
| $d_i := \mathsf{Dec}(pk, c_i)$; | $d_i := \mathsf{Dec}(pk, c_i)$; |
| $b' := \mathcal{R}(\mathcal{M}, m_0, d_1, \ldots, d_n, s_2)$: | $b' := \mathcal{R}(\mathcal{M}, m_0, d_1, \ldots, d_n, s_2)$: |
| $b'$ を出力 | $b'$ を出力 |
| **Game 2** | **Game 3** |
| $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; |
| $(pk', sk') \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | |
| $(\mathcal{M}, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}'_1}(pk')$; | $(\mathcal{M}, s_1) \xleftarrow{\mathsf{R}} \mathcal{S}_1(pk)$; |
| $m_0, m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$; | $m_0 \xleftarrow{\mathsf{U}} \mathcal{M}$; |
| $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk', m_1)$; | |
| $(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m_0), s_1)$; | $(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{S}_2(c^*, h(m_0), s_1)$; |
| $(c_1, \ldots, c_n) := \mathbf{c}$; | $(c_1, \ldots, c_n) := \mathbf{c}$; |
| $d_i := \mathsf{Dec}(pk, c_i)$; | $d_i := \mathsf{Dec}(pk, c_i)$; |
| $b' := \mathcal{R}(\mathcal{M}, m_0, d_1, \ldots, d_n, s_2)$: | $b' := \mathcal{R}(\mathcal{M}, m_0, d_1, \ldots, d_n, s_2)$: |
| $b'$ を出力 | $b'$ を出力 |

表 5: 定理 6.6 の Game 3 における $\mathcal{S}$ の構成

| $\mathcal{S}_1(pk)$ | $\mathcal{S}_2(h(m_0), s_1)$ |
|---|---|
| $(pk', sk') \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | $m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$; |
| $(\mathcal{M}, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk')$: | $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$; |
| $(\mathcal{M}, s_1)$ を出力 | $(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, h(m_0), s_1)$: |
| | $(\mathbf{c}, s_2)$ を出力 |

| | |
|---|---|
| $\underline{\mathcal{B}_1^{\mathcal{O}_1'}(pk')}$ | $\underline{\mathcal{B}_2^{\mathcal{O}_2'}(c^*, s_1')}$ |
| $(\mathcal{M}, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1'}(pk')$; | $(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2'}(c^*, h(m_0), s)$; |
| $m_0, m_1 \xleftarrow{\mathsf{U}} \mathcal{M}$; | $s_2' := (s_2, m_0, m_1, \mathcal{M})$: |
| $s_1' := (s_1, m_0, m_1, \mathcal{M})$: | $(\mathbf{c}, s_2')$ を出力 |
| $(m_0, m_1, s_1)$ を出力 | $\underline{\mathcal{B}_3(d_1, \ldots, d_n, s_2')}$ |
| | $b' := \mathcal{R}(\mathcal{M}, m_0, d_1, \ldots, d_n, s_2)$: |
| | $b'$ を出力 |

INM-ATK-0 の実験において最終的に 1 が出力されるのは，内部で動作している $\mathcal{A}$ に $m_0$ の暗号文 $c^*$ を入力し，$\mathcal{A}$ が出力した暗号文の集合を復号した結果を $\mathcal{R}$ に入力したときに $\mathcal{R}$ が 1 を出力する場合である．これは Game 1 における出力と等価であるので $\Pr[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\mathsf{INM\text{-}ATK\text{-}0}}(k) \to 1] = \Pr[S_1]$ となる．一方，INM-ATK-1 の実験において最終的に 1 が出力されるのは，内部で動作している $\mathcal{A}$ に $m_1$ の暗号文 $c^*$ を入力し，$\mathcal{A}$ が出力した暗号文の集合を復号した結果を $\mathcal{R}$ に入力したときに $\mathcal{R}$ が 1 を出力する場合である．これは Game 2 における出力と等価であるので $\Pr[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\mathsf{INM\text{-}CPA\text{-}1}}(k) \to 1] = \Pr[S_2]$ となる．よって

$$
\begin{aligned}
|\Pr[S_2] - \Pr[S_1]| &\leq \left| \begin{array}{l} \Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\mathsf{INM\text{-}ATK\text{-}1}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}_{\Pi,\mathcal{B}}^{\mathsf{INM\text{-}ATK\text{-}0}}(k) \to 1\right] \end{array} \right| \\
&= \mathsf{Adv}_{\Pi,\mathcal{B}}^{\mathsf{INM\text{-}ATK}}(k)
\end{aligned}
$$

である． ■

**命題 6.13.** $\Pr[S_3] = \Pr[S_2]$.

証明. Game 3 において，$\mathcal{S}$ は $\mathcal{A}$ を用いて表 5 のように動作している．Game 3 は $pk$ の下での通常の SS-ATK-1 の実験であるので $\mathcal{S}$ には復号オラクルは与えられない．しかし，$\mathcal{S}$ は内部で $(pk', sk')$ を生成しており $\mathcal{A}$ には Game 2 のように $pk'$ を入力するため，$\mathcal{A}$ が復号オラクルにクエリを聞いてきた場合は $sk'$ を用いることで正しく返答することができる．$\mathcal{S}$ は内部で生成した $m_1$ の暗号文を $\mathcal{A}_2$ に入力しており，$\mathcal{A}_2$ の出力 $(\mathbf{c}, s_2)$ を最終的な出力としているため，Game 3 における $\mathcal{S}$ の出力は Game 2 における $\mathcal{A}$ の出力と等価な分布である．よって $S_3$ が起きる確率は Game 2 において 1 が出力される確率，つまり $S_2$ が起きる確率と同じであるため

$$\Pr[S_3] = \Pr[S_2]$$

が得られる． ■

表 6: 定理 6.7 の証明の流れ (Game 0-1)

| Game 0 (INM-ATK-1) | Game 1 |
|---|---|
| $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; | $(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$; |
| $(m_0, m_1, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; |
| $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$; | $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$; |
| $(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s_1)$; | $(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s_1)$; |
| $(c_1, \ldots, c_n) := \mathbf{c}$; | $(c_1, \ldots, c_n) := \mathbf{c}$; |
| $d_i := \mathsf{Dec}(pk, c_i)$; | $d_i := \mathsf{Dec}(pk, c_i)$; |
| $b' \xleftarrow{\mathsf{R}} \mathcal{A}_3(d_1, \ldots, d_n, s_2)$: | $b' \xleftarrow{\mathsf{R}} \mathcal{A}_3(d_1, \ldots, d_n, s_2)$: |
| $b'$ を出力 | $b'$ を出力 |

なお，Game 3 は SNM-ATK-1 の実験であるため $\Pr[S_3] = \Pr[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{R},h}(k) \to 1]$ と表され，最終的に

$$\begin{aligned}\mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{R},h}(k) &= \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A},\mathcal{R},h}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{R},h}(k) \to 1\right] \end{array} \right| \\ &= |\Pr[S_0] - \Pr[S_3]| \\ &\leq \mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{B}}(k)\end{aligned}$$

が得られる．$\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{B}}(k) < \epsilon(k)$ であることを仮定していたので，$\mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{R},h}(k) < \epsilon(k)$ となる．よって補題 6.6 が証明された． □

**定理 6.7.** 攻撃の種類 $ATK \in \{CPA, CCA1, CCA2\}$ において，ある公開鍵暗号 $\Pi$ が *SNM-ATK (SNM-ATK)* 安全であるならば $\Pi$ は *INM-ATK (INM-ATK)* 安全である．

証明. ゲーム列を用いて，いかなる SNM-ATK-1 攻撃者 $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ に対してもアルゴリズム $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ が存在し，いかなる関係 $\mathcal{R}$ に対しても $\mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{B},\mathcal{S},\mathcal{R},h}(k) < \epsilon(k)$ が満たされているならば，いかなる INM-ATK 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ に対しても $\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ であることを示す．なお，それぞれのゲーム Game $i$ において 1 が出力される事象を $S_i$ と置くことにする．

**Game 0:** Game 0 は INM-ATK 攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ との通常の INM-ATK-0 における実験とする．
**Game 1:** Game 1 では Game 0 におけるチャレンジ暗号文を $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_0)$ から $c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m_1)$ へと変更する．それぞれの Game 0 と Game 1 は表 6 のように表される．

Game 0 は通常の INM-ATK-0 における実験であり Game 1 は INM-ATK-1 と等価であるので，$\Pr[S_0] = \Pr[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1]$，$\Pr[S_1] = \Pr[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1]$ と表すことができる．そこで，この 2 つのゲームにおける出力の差が SNM-ATK ゲームにおける優位性で抑えられることを示そう．

**命題 6.14.** *SNM-ATK-0* の実験において平文空間を *2* つの平文の集合 $\mathcal{M} := \{m_0, m_1\}$ としたときに $m_b$ からチャレンジ暗号文が生成された場合を考える．このとき，

$$\Pr[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1] = \Pr[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{R},h}(k) \to 1 \mid b = 0]$$
$$\Pr[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1] = \Pr[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{R},h}(k) \to 1 \mid b = 1]$$

を満たす確率的多項式時間アルゴリズム $\mathcal{B}$ および関係 $\mathcal{R}$ が存在する．

証明. 具体的に，$\Pi$ に対する SNM-ATK-0 の実験を行う $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ および関係 $\mathcal{R}$ が $\mathcal{A}$ を用いて以下のように動作している場合を考える．なお，ここでは SNM-ATK-0 に用いられている $h$ は何も出力しない関数とし，$\mathcal{B}_2$ にはいかなる部分情報も入力されないものとする．

| | |
|---|---|
| $\underline{\mathcal{B}_1^{\mathcal{O}_1}(pk)}$ | $\underline{\mathcal{B}_2^{\mathcal{O}_2}(c^*, s_1')}$ |
| $(m_0, m_1, s_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$; | $(\mathbf{c}, s_2) \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(c^*, s_1)$; |
| $\mathcal{M} := \{m_0, m_1\}$; | $s_2' := s_2$: |
| $s_1' := (m_0, m_1, s_1)$: | $(\mathbf{c}, s_2')$ を出力 |
| $(\mathcal{M}, s')$ を出力 | $\underline{\mathcal{R}(\mathcal{M}, m_0, d_1, \ldots, d_n, s_2')}$ |
| | $b' \xleftarrow{\mathsf{R}} \mathcal{A}_3(d_1, \ldots, d_n, s_2)$: |
| | $m_1 = m_{b'}$ ならば 1 を出力 |
| | $m_1 \neq m_{b'}$ ならば 1 を出力 |

攻撃者 $\mathcal{B}_1$ が $\mathcal{M} := \{m_0, m_1\}$ とした平文空間の中から $m_0$ が選ばれてチャレンジ暗号文 $c^*$ が生成された場合，これは $\mathcal{A}$ からみたとき INM-ATK-0 の実験そのものである．また，$m_1$ が選ばれてチャレンジ暗号文 $c^*$ が生成された場合は，これは $\mathcal{A}$ からみたとき INM-ATK-1 の実験そのものである．また，上記の SNM-ATK-0 の実験において 1 が出力されるのは $\mathcal{R}$ が $m_1 = m_{b'}$ を満たす場合であり，それはどちらの場合も $\mathcal{A}$ が $b' := 1$ を出力するときのみである．よって

$$\Pr[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1] = \Pr[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{R},h}(k) \to 1 \mid b = 0]$$
$$\Pr[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1] = \Pr[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{R},h}(k) \to 1 \mid b = 1]$$

となる． ■

なお，$\Pi$ は SNM-ATK 安全であることを仮定しているので，あるアルゴリズム $\mathcal{S}$ が存在して

$$\left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{R},h}(k) \to 1 \mid b = 0\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{R},h}(k) \to 1 \mid b = 0\right] \end{array} \right| = \mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{B},\mathcal{S},\mathcal{R},h}(k)$$

$$\left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{R},h}(k) \to 1 \mid b = 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{R},h}(k) \to 1 \mid b = 1\right] \end{array} \right| = \mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{B},\mathcal{SR},h}(k)$$

である．ただし，このとき SNM-ATK-1 の実験を考えると，$\mathcal{S}$ には $m_1, m_0$ の部分情報は一切入力されていないため，$\mathcal{S}$ からみて $m_1$ が選ばれたときに関係 $\mathcal{R}$ を満たす暗号文を出力する確率も $m_0$ が選ばれたときに関係 $\mathcal{R}$ を満たす暗号文を出力する確率も $1/2$ である．つまり

$$\Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{S},\mathcal{R},h}(k) \to 1 \mid b = 1\right] = \frac{1}{2}$$
$$\Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{S},\mathcal{R},h}(k) \to 1 \mid b = 0\right] = \frac{1}{2}$$

である．よって

$$\begin{aligned} \mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{A}}(k) &= \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{INM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1\right] \end{array} \right| \\ &= \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{R},h}(k) \to 1 \mid b = 0\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{R},h}(k) \to 1 \mid b = 1\right] \end{array} \right| \\ &\leq \left| \begin{array}{l} \Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{R},h}(k) \to 1 \mid b = 0\right] \\ -\Pr\left[\mathsf{Exp}^{\mathsf{SNM\text{-}ATK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{R},h}(k) \to 1 \mid b = 1\right] \end{array} \right| \\ &\quad + 2 \cdot \mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{B},\mathcal{S},\mathcal{R},h}(k) \\ &= 2 \cdot \mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{B},\mathcal{S},\mathcal{R},h}(k) \end{aligned}$$

となる．仮定から $\mathsf{Adv}^{\mathsf{SNM\text{-}ATK}}_{\Pi,\mathcal{B},\mathcal{S},R,h}(k) < \epsilon(k)$ であるため $\mathsf{Adv}^{\mathsf{INM\text{-}ATK}}_{\Pi,\mathcal{A}}(k) < \epsilon(k)$ が導かれる．□

# 7 IND-CCA2 安全を満たす効率的な公開鍵暗号方式

## 7.1 Cramer-Shoup 暗号

Cramer-Shoup 暗号は Cramer, Shoup が 1998 年に提案したもので，ランダムオラクルモデルを用いずに IND-CCA2 安全であることが証明された初の実用的な公開鍵暗号方式である [7] [8]．Cramer-Shoup 暗号は以下のようなものである．

**Gen:** $1^k$ ($k$ : セキュリティパラメータ) を入力とし，素数位数 $q$ の乗法群 $\mathbb{G}$ を $|q| = k$ となるように定める．$g$ を群 $\mathbb{G}$ の生成元とし，$w \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ から $\hat{g} := g^w$ とする．$x_1, x_2, y_1, y_2, z_1, z_2 \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ から

$$e := g^{x_1}\hat{g}^{x_2}, f := g^{y_1}\hat{g}^{y_2}, h := g^{z_1}\hat{g}^{z_2}$$

を求め，標的衝突困難ハッシュ関数族 HF のためのパラメータ hk を選ぶ ($\mathsf{HF}_{\mathsf{hk}} : \mathbb{G}^3 \to \mathbb{Z}_q$)．それぞれ公開鍵と秘密鍵を $pk := (q, \mathsf{hk}, g, \hat{g}, e, f, h)$，$sk := (x_1, x_2, y_1, y_2, z_1, z_2)$ とする．

$$pk = (q, \mathsf{hk}, g, \hat{g}, e, f, h),\ sk = (x_1, x_2, y_1, y_2, z_1, z_2)$$

**Enc:** 公開鍵 $pk$ および平文 $m \in \mathbb{G}$ を入力として，

E1: $u \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ を選ぶ．

E2: $a := g^u$ を求める．

E3: $\hat{a} := \hat{g}^u$ を求める．

E4: $c := h^u \cdot m$ とする．

E5: ハッシュ関数 $\mathsf{HF}_{\mathsf{hk}}$ を用いて $v := \mathsf{HF}_{\mathsf{hk}}(a, \hat{a}, c)$ を求める．

E6: $d := e^u f^{uv}$ を求める．

E7: $C := (a, \hat{a}, c, d) \in \mathbb{G}^4$ を暗号文として出力する．

**Dec:** 公開鍵 $pk$ と秘密鍵 $sk$ と暗号文 $C$ を入力とし，

D1: 暗号文のフォームが正しいかどうか ($\mathbb{G}$ の要素が 4 つであるか) の確認を行う．フォームが間違っていれば $\perp$ を出力する．

D2: $a, \hat{a}, c \in G$ であるかを確認する．もしそうでないならば $\perp$ を出力する．

D3: ハッシュ関数 $\mathsf{HF}_{\mathsf{hk}}$ を用いて $v' := \mathsf{HF}_{\mathsf{hk}}(a, \hat{a}, c)$ を求める．

D4: $d = a^{x_1+y_1v'}\hat{a}^{x_2+y_2v'}$ であるかを確認する．もしそうでないならば $\perp$ を出力する．

D5: $m' := c \cdot (a^{z_1}\hat{a}^{z_2})^{-1}$ を復号結果として出力する．

Cramer-Shoup 暗号において平文が正しく暗号化されていれば $v = v'$ であり，

$$\begin{aligned} d &= e^u f^{uv} = (g^{x_1}\hat{g}^{x_2})^u \cdot (g^{y_1}\hat{g}^{y_2})^{uv} = g^{u(x_1+vy_1)} \cdot \hat{g}^{u(x_2+vy_2)} \\ &= a^{x_1+y_1v}\hat{a}^{x_2+y_2v} \end{aligned}$$

により検証に通り，

$$m' = c \cdot (a^{z_1}\hat{a}^{z_2})^{-1} = (g^{z_1}\hat{g}^{z_2})^u \cdot m \cdot (g^{uz_1}\hat{g}^{uz_2})^{-1} = m$$

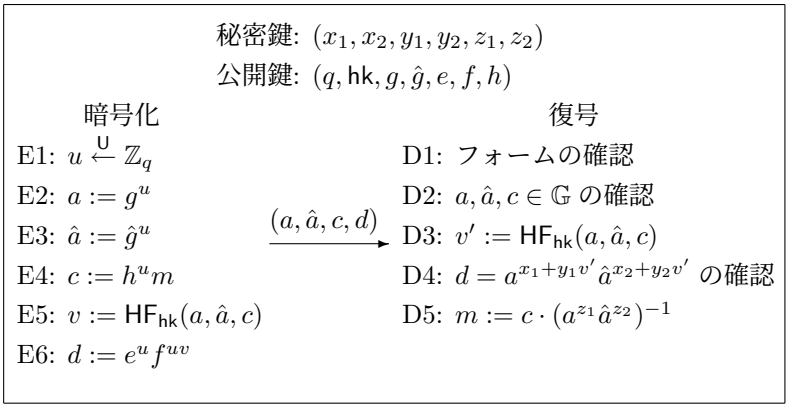


図 8: Cramer-Shoup 暗号

となることから元の平文を得ることができる.

Cramer-Shoup 暗号の安全性は DDH 仮定とハッシュ関数の標的衝突困難性の下で成り立っている. なお, 39 ページで述べた DDH 仮定は $\mathbb{F}_p^\times$ 上で定義したものであるが, 一般の群 $\mathbb{G}$ についても DDH 仮定を同様に定義することができる.

**定理 7.1.** $\mathbb{G}$ 上において *DDH* 仮定が成り立っており, ハッシュ関数族 $\mathsf{HF}$ が標的衝突困難性を満たしているならば, *Cramer-Shoup* 暗号 $\Pi$ は *IND-CCA2* 安全な公開鍵暗号方式である. 特に, いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対してもある確率的多項式時間アルゴリズム $\mathcal{B}_1, \mathcal{B}_2$ が存在し

$$\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\mathcal{A}}(k) \leq \mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{B}_1}(k) + \mathsf{Adv}^{\mathsf{TCR}}_{\mathcal{B}_2}(k) + (q_d + 4)/q$$

を満たす.

証明. まず, Cramer-Shoup 暗号に対して通常の IND-CCA2 ゲームが行われた場合攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ と挑戦者の間でどのようなやりとりが行われるかを示しておく.

**Setup:** $\mathsf{Gen}$ アルゴリズムから $pk = (q, \mathsf{hk}, g, \hat{g}, e, f, h)$ および $sk = (x_1, x_2, y_1, y_2, z_1, z_2)$ を求め, $pk$ を攻撃者 $\mathcal{A}_1$ に入力する.

**Phase 1:** 攻撃者 $\mathcal{A}_1$ が $c_i = (a_i, \hat{a}_i, c_i, d_i)$ を復号オラクルに問い合わせた場合,

D1: 暗号文のフォームが正しいかどうか ($\mathbb{G}$ の要素が 4 つであるか) の確認を行う. フォームが間違っていれば $\perp$ を出力する.

D2: $a_i, \hat{a}_i, c_i \in \mathbb{G}$ であるかを確認する. もしそうでないならば $\perp$ を出力する.

D3: ハッシュ関数 $\mathsf{HF}_{\mathsf{hk}}$ を用いて $v_i := \mathsf{HF}_{\mathsf{hk}}(a_i, \hat{a}_i, c_i)$ を求める.

D4: $d_i = a_i^{x_1+y_1v_i}\hat{a}_i^{x_2+y_2v_i}$ であるかを確認する．もしそうでないならば $\perp$ を出力する．

D5: $m_i := c_i \cdot (a_i^{z_1}\hat{a}_i^{z_2})^{-1}$ を復号結果として返答する．

という動作が行われる．

**Challenge:** 攻撃者 $\mathcal{A}_1$ が $(m_0, m_1, s)$ を出力したならば，$b \xleftarrow{\mathsf{U}} \{0,1\}$ として

E1: $u \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ を選ぶ．

E2: $a^* := g^u$ を求める．

E3: $\hat{a}^* := \hat{g}^u$ を求める．

E4: $c^* := h^u \cdot m_b$ とする．

E5: ハッシュ関数 $\mathsf{HF}_{\mathsf{hk}}$ を用いて $v^* := \mathsf{HF}_{\mathsf{hk}}(a^*, \hat{a}^*, c^*)$ を求める．

E6: $d^* := e^u f^{uv^*}$ を求める．

E7: $C^* := (a^*, \hat{a}^*, c^*, d^*) \in \mathbb{G}^4$ を暗号文として攻撃者 $\mathcal{A}_2$ に返答する．

**Phase 2:** 攻撃者 $\mathcal{A}_2$ が暗号文を復号オラクルに聞いてきたら，Phase 1 と同様の操作を行い平文あるいは $\perp$ を返答する．ただし，チャレンジ暗号文 $C^*$ が復号オラクルに聞くことは禁止するものとする．

**Guess:** 攻撃者 $\mathcal{A}_2$ はビット $b$ に対する推測 $b'$ を出力する．

上記の動作でゲームが行われることを踏まえて，Cramer-Shoup 暗号に対する IND-CCA2 安全性が以下のゲームの変換によって DDH 問題に帰着される事を示そう．

**Game 0:** Game 0 は通常の Cramer-Shoup 暗号に対しての攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対しての IND-CCA2 ゲームとする．
**Game 1:** Game 1 では，Game 0 の Challenge における E4 と E6 をそれぞれ

E4′: $c^* := (a^*)^{z_1}(\hat{a}^*)^{z_2} \cdot m_b$

E6′: $d^* := (a^*)^{x_1+y_1v^*}(\hat{a}^*)^{x_2+y_2v^*}$

へと変換する．
**Game 2:** Game 2 では，Game 1 における Challenge における E3 を

E3′: $\hat{u} \xleftarrow{\mathsf{U}} \mathbb{Z}_q \setminus \{u\}, \hat{a}^* := \hat{g}^{\hat{u}}$

へと変換する．
**Game 3:** Game 3 では，$x := x_1 + wx_2 \bmod q, y := y_1 + wy_2 \bmod q, z := z_1 + wz_2 \bmod q$ とし，Game 2 の Phase 1 および Phase 2 における D4 と D5 をそれぞれ

D4′: $\hat{a}_i = a_i^w, d_i = a_i^{x+yv_i}$ であるかを確認する．もしそうでないならば $\perp$ を出力する．

D5′: $m_i' := c_i \cdot (a^z)^{-1}$ を復号結果として返答する．

へと変換する．

**Game 4:** Game 4 では，Game 3 における E4′ を

E4″: $r \xleftarrow{\mathsf{U}} \mathbb{Z}_q,\ c^* := g^r$

へと変換する．

**Game 5:** Game 5 では，チャレンジ暗号文に含まれる $(a^*, \hat{a}^*, c^*)$ と復号オラクルに聞かれた $(a_i, \hat{a}_i, c_i)$ に関して $(a^*, \hat{a}^*, c^*) \neq (a_i, \hat{a}_i, c_i)$ かつ $\mathsf{HF}_{hk}(a^*, \hat{a}^*, c^*) = \mathsf{HF}_{hk}(a_i, \hat{a}_i, c_i)$ が満たされているならばゲームを中止する．

それぞれのゲーム Game $i$ において 1 が出力される事象を $S_i$ と置くことにする．Game 0 は通常の IND-CCA2 ゲームであるので Game 0 において $b' = b$ となる事象 $S_0$ は

$$|2 \cdot \Pr[S_0] - 1| = \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}CCA2}}(k)$$

と表される．よってその他のゲーム間における関係を以下の命題を用いて示す．

**命題 7.1.** $\Pr[S_1] = \Pr[S_0]$ が成り立つ．

証明. チャレンジ暗号文を生成する際に E4 および E6 を Game 1 のように変更したとしても，この変換は単に式変形を行っただけなので攻撃者から見て Game 1 と Game 0 は完全に識別不可能である．よって

$$\Pr[S_1] = \Pr[S_0]$$

である． ■

**命題 7.2.** $|\Pr[S_2] - \Pr[S_1]| \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{DDH}}(k) + 3/q$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}_1$ が存在する．

証明. もし Game 2 において 1 が出力される確率と Game 1 において 1 が出力される確率の差が無視できない値であるのならば，DDH 仮定を破ることができるアルゴリズム $\mathcal{B}_1$ が構成できることを示す．アルゴリズム $\mathcal{B}_1$ は DDH 問題の入力として $(q, g', g_1', g_2', g_3')$ を受け取り，以下のように内部で $\mathcal{A}$ を動作させる．

$\underline{\mathcal{B}_1(g', g'_1, g'_2, g'_3)}$
$\mathsf{hk}$ を選ぶ; $g := g'$; $\hat{g} := g'_1$;
$x_1, x_2, y_1, y_2, z_1, z_1 \xleftarrow{\mathsf{U}} \mathbb{Z}_q$;
$e := g^{x_1}\hat{g}^{x_1}$; $f := g^{y_1}\hat{g}^{y_1}$; $h := g^{z_1}\hat{g}^{z_1}$;
$pk := (q, \mathsf{hk}, g, \hat{g}, e, f, h)$;
$(m_0, m_1, s) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}_1}(pk)$;
$b \xleftarrow{\mathsf{U}} \{0, 1\}$; $a^* := g'_2$; $\hat{a}^* := g'_3$;
$c^* := (a^*)^{z_1}(\hat{a}^*)^{z_2} \cdot m_b$; $v^* := \mathsf{HF}_{\mathsf{hk}}(a^*, \hat{a}^*, c^*)$
$d^* := (a^*)^{x_1+y_1v^*}(\hat{a}^*)^{x_2+y_2v^*}$;
$C^* := (a^*, \hat{a}^*, c^*, d^*)$;
$b' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}_2}(C^*, s)$:
$b' = b$ ならば 1 を出力
$b' \neq b$ ならば 0 を出力

この識別器アルゴリズムは Game 1 と Game 2 の中間に位置するもので，実際のゲームと違うのは $(g, \hat{g}, a^*, \hat{a}^*)$ を入力とされている組 $(q, g', g'_1, g'_2, g'_3)$ に置き換えているのみである．また，$\mathcal{B}_1$ は自身で秘密鍵を生成しているため $sk$ を用いて $\mathcal{A}$ の復号オラクルに対して正しく返答することができる．

もし $\mathcal{B}_1$ への入力が $\{(q, g', g'_1, g'_2, g'_3) \mid x, y \xleftarrow{\mathsf{U}} \mathbb{Z}_q, g'_1 := g^x, g'_2 := g^y, g'_3 := g^{xy}\}$ ならば $\mathcal{D}$ の動作は Game 1 と同じになるため，$\mathcal{D}$ が 1 を出力する確率は事象 $S_1$ が起きる確率と同じであり

$$\Pr\left[\mathcal{B}_1(q, g', g'_1, g'_2, g'_3) \to 1 \;\middle|\; \begin{array}{l} x, y \xleftarrow{\mathsf{U}} \mathbb{Z}_q;\ g'_1 := g^x; \\ g'_2 := g^y;\ g'_3 := g^{xy} \end{array}\right] = \Pr[S_1]$$

となる．一方，$\mathcal{B}_1$ への入力が $\{(q, g', g'_1, g'_2, g'_3) \mid x, y, z \xleftarrow{\mathsf{U}} \mathbb{Z}_q, g'_1 := g^x, g'_2 := g^y, g'_3 := g^z\}$ かつ $x \neq 0, z \not\equiv xy \pmod q$ を満たすならば $\mathcal{B}_1$ の動作は Game 2 と同じになるため，$\mathcal{B}_1$ が 1 を出力する確率は事象 $S_2$ が起きる確率と同じである．なお，$x \neq 0$ かつ $z \not\equiv xy \pmod q$ を満たさない確率は高々$3/q$ であるので

$$\Pr\left[\mathcal{B}_1(q, g', g'_1, g'_2, g'_3) \to 1 \;\middle|\; \begin{array}{l} x, y, z \xleftarrow{\mathsf{U}} \mathbb{Z}_q;\ g'_1 := g^x; \\ g'_2 := g^y;\ g'_3 := g^z \end{array}\right] = \Pr[S_2] - \frac{3}{q}$$

となる．よって

$$|\Pr[S_2] - \Pr[S_1]| \leq \mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{B}_1}(k) + 3/q$$

となる． ■

**命題 7.3.** *Game $i$* において *$D_4$* の検証に通り *$D_4'$* の検証に通らない暗号文が復号オラクルに聞かれた場合を事象 $F_i$ と定義する．このとき $|\Pr[S_3] - \Pr[S_2]| \leq \Pr[F_3]$ となる．

証明. 事象 $F_3$ が起きなければ Game 2 と Game 3 は等価なゲームとなるため $\Pr[S_2 \wedge \neg F_3] = \Pr[S_3 \wedge \neg F_3]$ である．よって 2 章で述べた difference lemma を用いることで $|\Pr[S_3] - \Pr[S_2]| \leq \Pr[F_3]$ が導かれる． ■

**命題 7.4.** $\Pr[S_4] = \Pr[S_3]$ かつ $\Pr[F_4] = \Pr[F_3]$ が成り立つ.

証明. Game 3 における $c^*$ は $c^* := (a^*)^{z_1}(\hat{a}^*)^{z_2} \cdot m_b$ で表されており，攻撃者 $\mathcal{A}$ から見て $z_1, z_2$ の情報として得ているものは公開鍵 $h = g^{z_1}\hat{g}^{z_2}$ のみである．このとき，$(a^*)^{z_1}(\hat{a}^*)^{z_2}$ および $h$ に対して $g$ を底とした離散対数を考えると

$$\begin{pmatrix} \log_g (a^*)^{z_1}(\hat{a}^*)^{z_2} \\ \log_g h \end{pmatrix} \equiv \begin{pmatrix} u & \omega\hat{u} \\ 1 & \omega \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \pmod{q} \tag{2}$$

表される．式 (2) における $2 \times 2$ 行列を $M_1$ とすると行列式は $|M_1| = \omega(\hat{u} - u) \neq 0$ となるので，$(a^*)^{z_1}(\hat{a}^*)^{z_2}$ は $h$ からみて線形独立な値であり，$\mathbb{G}$ 上一様分布な値である．つまり，$c^*$ を $r \xleftarrow{\cup} \mathbb{Z}_q$ から $c^* := g^r$ と置き換えたとしても攻撃者から見て識別不可能である．よって $\Pr[S_4] = \Pr[S_3]$ かつ $\Pr[F_4] = \Pr[F_3]$ が成り立つ. ■

**命題 7.5.** $\Pr[S_4] = 1/2$ が成り立つ.

証明. Game 4 においては $c^* = g^r$ となっており，攻撃者が入力した平文 $m_0, m_1$ とは完全に独立な値である．そのため攻撃者が $m_b$ の値を $1/2$ 以上の確率で推測することは不可能であるため

$$\Pr[S_4] = \frac{1}{2}$$

となる． ■

**命題 7.6.** *Game 5* においてゲームが中止されるという事象を $C_5$ と置く．このとき $|\Pr[F_5] - \Pr[F_4]| \leq \Pr[C_5]$ が成り立つ.

証明. Game 5 においてゲームが中止されなければ Game 4 と Game 5 は等価であるため，$\Pr[F_5 \wedge \neg C_5] = \Pr[F_4 \wedge \neg C_5]$ である．従って 2 章で述べた difference lemma を用いることにより

$$\Pr[F_5] - \Pr[F_4]| \leq \Pr[C_5]$$

が得られる． ■

**命題 7.7.** $Pr[C_5] \leq \mathsf{Adv}^{\mathsf{TCR}}_{\mathcal{B}_2}(k) + 1/q$ を満たす確率的多項式時間アルゴリズム $\mathcal{B}_2$ が存在する.

証明．もし事象 $C_5$ が起きるならば，ハッシュ関数の標的衝突困難性を破ることができるアルゴリズム $\mathcal{B}_2$ を構成することができることを示そう．

$\mathcal{B}_2$ は $\mathsf{hk}$ および $(a^*, \hat{a}^*, c^*) \xleftarrow{\mathsf{U}} \mathbb{G}^3$ を受け取り，入力されている $\mathsf{hk}$ 以外の公開鍵及び秘密鍵を Cramer-Shoup 暗号の鍵生成アルゴリズムを用いて生成する．攻撃者が 2 つの平文を出力してきたら，$\mathcal{B}_2$ は入力された $(a^*, \hat{a}^*, c^*) \in \mathbb{G}^3$ を用いて

$$v^* := \mathsf{HF}_{\mathsf{hk}}(a^*, \hat{a}^*, c^*),\ d^* := (a^*)^{x_1 + y_1 v^*} (\hat{a}^*)^{x_2 + y_2 v^*}$$

を求め，$(a^*, \hat{a}^*, c^*, d^*)$ をチャレンジ暗号文とする．攻撃者 $\mathcal{A}$ が復号オラクルを聞いていた場合は Game 5 における条件に沿って復号を行い，事象 $C_5$ が起きた場合 $\mathcal{B}_2$ は $\mathcal{A}$ とのゲームを中止し (標的衝突困難ハッシュ関数の) 挑戦者に対して $(a_i, \hat{a}_i, c_i)$ を出力する．

上記のように $\mathcal{B}_2$ が動作した場合，$\log_g a^* \neq \log_{\hat{g}} \hat{a}^*$ であるならば $\mathcal{B}_2$ の動作は Game 4 において事象 $C_5$ が起きた場合と等価であるため標的衝突困難ハッシュ関数の安全性を破ることができる．なお，$\log_g a^* \neq \log_{\hat{g}} \hat{a}^*$ であるかは標的衝突困難ハッシュ関数の入力に依存し，$(a^*, \hat{a}^*, c^*)$ はいずれも $\mathbb{G}$ 上ランダムに選ばれた要素であって Game 2 のような制約はない．ただし，$\log_g a^* = \log_{\hat{g}} \hat{a}^*$ となる確率は高々$1/q$ であるので，この確率を除けば $\mathcal{B}_2$ はハッシュ関数の標的衝突困難性を破ることができる．よって

$$\Pr[C_5] \leq \mathsf{Adv}^{\mathsf{TCR}}_{\mathcal{B}_2}(k) + 1/q$$

となる． ■

**命題 7.8.** $\Pr[F_5] \leq q_d/q$ が成り立つ．

証明．事象 $F_5$ が起きるというのは，$1 \leq i \leq q_d$ において $\mathcal{A}$ が $a_i := g^{u_i}, \hat{a}_i := \hat{g}^{\hat{u}_i}$ $(u_i \neq \hat{u}_i)$ となる値で復号オラクルに暗号文 $(a_i, \hat{a}_i, c_i, d_i)$ を聞いてきた際に検証に通る場合である．このとき $e, f, d^*, d_i$ に対して $g$ を底とした離散対数を考えると

$$\log_g e \equiv x_1 + \omega x_2 \pmod{q} \tag{3}$$
$$\log_g f \equiv y_1 + \omega y_2 \pmod{q} \tag{4}$$
$$\log_g d^* \equiv u(x_1 + v^* y_1) + \omega \hat{u}(x_2 + v^* y_2) \pmod{q} \tag{5}$$
$$\log_g d_i \equiv u_i(x_1 + v_i y_1) + \omega \hat{u}_i(x_2 + v_i y_2) \pmod{q} \tag{6}$$

となる．式 (3) から (6) を行列を用いて表すと

$$\begin{pmatrix} \log_g e \\ \log_g f \\ \log_g d^* \\ \log_g d_i \end{pmatrix} \equiv \begin{pmatrix} 1 & \omega & 0 & 0 \\ 0 & 0 & 1 & \omega \\ u & \omega\hat{u} & uv^* & \omega\hat{u}v^* \\ u_i & \omega\hat{u}_i & u_i v_i & \omega\hat{u}_i v_i \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ y_1 \\ y_2 \end{pmatrix} \pmod{q} \tag{7}$$

である．式 (7) における $4\times4$ の行列を $M_2$ と置いたとき，行列 $M_2$ の行列式は $|M_2| = w^2(u-\hat{u})(u_i-\hat{u}_i)(v^*-v_i)$ となり，このときこれまでのゲーム変換から $u_i \neq \hat{u}_i, u \neq \hat{u}, v^* \neq v_i$ である．よって $|M_2| \neq 0$ であるため行列 $M_2$ は正則であり，D4′ における検証に通る確率は各々の $i$ に対して高々$1/q$ である．よって $1 \leq i \leq q_d$ であることから，

$$\Pr[F_5] \leq q_d/q$$

となる． ■

以上の命題による確率評価を積み重ねることにより

$$\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\mathcal{A}}(k) \leq \mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{B}_1}(k) + \mathsf{Adv}^{\mathsf{TCR}}_{\mathcal{B}_2}(k) + (q_d+4)/q$$

が得られるため，定理 7.1 が証明された． □

# 付録

## A 計算量的仮定

GDH (Gap Diffie-Hellman) 仮定

$1^k$ ($k$ : セキュリティパラメータ) を入力し，$(p,q,g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k)$ を求める．$x, y \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ から $g_1 := g^x \bmod p, g_2 := g^y \bmod p$ を求める．このとき，$(p,q,g,g_1,g_2)$ が入力されたときに，DDH オラクルとして $(A_1,A_2,A_3)$ を入力すると $\log_g A_1 \cdot \log_g A_2 \equiv \log_g A_3 \pmod q$ であるかの判定結果が返答されるオラクル $\mathcal{O}$ を利用しつつ $g^{xy} \bmod p$ を求める問題を GDH 問題と呼ぶ．あるアルゴリズム $\mathcal{A}$ の GDH 問題に対しての優位性は

$$\mathsf{Adv}^{\mathsf{GDH}}_{\mathcal{A}}(k) := \Pr\left[ g_3 \equiv g^{xy} \pmod p \;\middle|\; \begin{array}{l} (p,q,g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k);\ x,y \xleftarrow{\mathsf{U}} \mathbb{Z}_q; \\ g_1 := g^x \bmod p;\ g_2 := g^y \bmod p; \\ g_3 \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}}(p,q,g,g_1,g_2) \end{array} \right]$$

として定義される．

**定義 A.1.** いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても，*GDH* 問題に対しての優位性が $\mathsf{Adv}^{\mathsf{GDH}}_{\mathcal{A}}(k) < \epsilon(k)$ である場合，*GDH* 仮定が保たれているという．

$\ell$-SDH 仮定

$1^k$ ($k$ : セキュリティパラメータ) を入力し，$\mathbb{G}_1, \mathbb{G}_2$ を素数位数 $q$ の巡回群，$g_2$ を $\mathbb{G}_2$ における生成元とし $g_1 := \phi(g_2)$ とする ($|q| = k$，$\phi : \mathbb{G}_2 \to \mathbb{G}_1$ は効率的に計算可能な写像)．$A_i := g_2^{z^i}$ と定義したとき，($z \in \mathbb{Z}_q$)，$z \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ から $(g_1, \{A_i\}_{0\leq i\leq \ell})$ が与

えられたとき，$(c, g_1^{1/(z+c)})$ $(c \in \mathbb{Z}_q)$ を出力する問題を $\ell$-SDH 問題と呼ぶ．あるアルゴリズム $\mathcal{A}$ の $\ell$-SDH 問題に対しての優位性は

$$\mathsf{Adv}_{\mathcal{A}}^{\ell\text{-}\mathsf{SDH}}(k) := \Pr\left[\mathcal{A}(g_1, \{A_i\}_{0\le i\le \ell}) \to (c, g_1^{1/(z+c)}) \;\middle|\; \begin{array}{l} g_2 \xleftarrow{\mathsf{U}} \mathbb{G}_2;\ g_1 := \phi(g_2); \\ z \xleftarrow{\mathsf{U}} \mathbb{Z}_q; \forall 1 \le i \le \ell, A_i := g_2^{z^i} \end{array}\right]$$

として定義される．

**定義 A.2.** いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても *$\ell$-SDH* 問題に対しての優位性が $\mathsf{Adv}_{\mathcal{A}}^{\ell\text{-}\mathsf{SDH}}(k) < \epsilon(k)$ であるとき，*$\ell$-SDH* 仮定が保たれているという．

Strong RSA 仮定

$1^k$ ($k$：セキュリティパラメータ) を入力し，$(n, p, q) := \mathsf{GenMod}(1^k)$ を求める．$\phi(n) := (p-1)(q-1)$ とし，$y \xleftarrow{\mathsf{U}} \mathbb{Z}_n$ を選ぶ．このとき，$y$ が入力された場合に $x^e \equiv y \pmod n$ を満たす $(x, e)$ $(x \in \mathbb{Z}_n, e \in \mathbb{Z}_{\phi(n)})$ を求める問題を Strong RSA 問題と呼ぶ．このとき，あるアルゴリズム $\mathcal{A}$ の Strong RSA 問題に対しての優位性は

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{sRSA}}(k) := \Pr\left[x^e \equiv y \pmod n \;\middle|\; \begin{array}{l} (n, p, q) \xleftarrow{\mathsf{R}} \mathsf{GenMod}(1^k); \\ \phi(n) := (p-1)(q-1); \\ y \xleftarrow{\mathsf{U}} \mathbb{Z}_n;\ (x, e) \xleftarrow{\mathsf{R}} \mathcal{A}(e, n, y) \end{array}\right]$$

として定義される．

**定義 A.3.** いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても，*Strong RSA* 問題に対しての優位性が $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{sRSA}}(k) < \epsilon(k)$ である場合，*Strong RSA* 仮定が保たれているという．

KEA1 仮定

$1^k$ ($k$：セキュリティパラメータ) を入力し，$(n, p, q) := \mathsf{GenMod}(1^k)$ を求める．$x \xleftarrow{\mathsf{U}} \mathbb{Z}_q$ から $g_1 := g^x \bmod p$ として $(g, g_1)$ が入力されたとき，$\log_g g_2$ の知識なしに $g_3 \equiv g_2^x \pmod p$ を満たす $(g_2, g_3)$ を出力する問題を KEA1 問題と呼ぶ．あるアルゴリズム $(\mathcal{A}, \mathcal{A}')$ の KEA1 問題に対しての優位性は

$$\mathsf{Adv}_{\mathcal{A},\mathcal{A}'}^{\mathsf{KEA1}}(k) := \Pr\left[\begin{array}{c} g_3 \equiv g_2^x \pmod p \wedge \\ g_2 \neq g^y \pmod p \end{array} \;\middle|\; \begin{array}{l} (p, q, g) \xleftarrow{\mathsf{R}} \mathsf{GenG}(1^k);\ x \xleftarrow{\mathsf{U}} \mathbb{Z}_q; \\ g_1 := g^x \bmod p;\ (g_2, g_3) := \mathcal{A}(g, g_1); \\ (g_2, g_3, y) := \mathcal{A}'(g, g_1) \end{array}\right]$$

として定義される．

**定義 A.4.** いかなる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても，別の確率的多項式時間アルゴリズム $\mathcal{A}'$ が存在し，*KEA1* 問題に対しての優位性が $\mathsf{Adv}_{\mathcal{A},\mathcal{A}'}^{\mathsf{KEA1}}(k) < \epsilon(k)$ である場合，*KEA1* 仮定が保たれているという．

# 参考文献


[1] Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among notions of security for public-key encryption schemes. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 26–45. Springer, Heidelberg (1998)

[2] Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: 1st ACM Conference on Computer and Communications Security, pp. 62–73. ACM Press (1993)

[3] Bellare, M., Rogaway, P.: Optimal asymmetric encryption. In: Santis, A.D. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 92–111. Springer, Heidelberg (1994)

[4] Bellare, M., Sahai, A.: Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 519–536. Springer, Heidelberg (1999)

[5] Bleichenbacher, D.: Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 1–12. Springer, Heidelberg (1998)

[6] Blum, M., Micali, S.: How to generate cryptographically strong sequences of pseudo-random bits. SIAM Journal on Computiong 13(4) pp. 850–864 (1984)

[7] Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998)

[8] Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal of Computing 33(1) pp. 167–226 (2002)

[9] Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information Theory IT-22(6) pp. 644–654 (1976)

[10] Dolev, D., Dwork, C., Naor, M.: Non-malleable cryptography (extended abstract). In: 23th Annual ACM Symposium on Theory of Computing, pp. 542–552. ACM Press (1991)

[11] ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1984)

[12] Goldreich, O.: Foundations of Cryptography, vol. 1: Basic Tools. Cambridge University Press (2001)

[13] Goldreich, O.: Foundations of Cryptography, vol. 2: Basic Applications. Cambridge University Press (2004)

[14] Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions (extended abstract). In: 25th Annual Symposium on Foundations of Computer Science. pp. 464–479. (1984)

[15] Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions. Journal of ACM 33(4) pp. 792–807 (1986)

[16] Goldreich, O., Levin, L.A.: A hard-core predicate for all one-way functions. In: Annual ACM Symposium on Theory of Computing, pp. 25–32. ACM Press (1989)

[17] Goldwasser, S., Micali, S.: Probabilistic encryption and how to play mental poker keeping secret all partial information. In: 14th Annual ACM Symposium on Theory of Computing, pp. 365–377. ACM Press (1982)

[18] Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing 17(2) pp. 281–308 (1988)

[19] Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. SIAM Journal of Computing 28(4) pp. 1364–1396 (1999)

[20] Katz, J., Lindell, Y.: INTRODUCTION TO MODERN CRYPTOGRAPHY. CRC Press (2007)

[21] Krawczyk, H.: Simple forward-secure signatures for any signature scheme. In: 7th ACM Conference on Computer and Communications Security, pp. 108–115. ACM Press (2000)

[22] Krawczyk, H.: HMQV: A high-performance secure diffie-hellman protocol. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 546–566. Springer, Heidelberg (2005)

[23] Kurosawa, K., Takagi, T.: New approach for selectively convertible undeniable signature schemes. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 428–443. Springer, Heidelberg (2006)

[24] Laguillaumie, F., Libert, B., Quisquater, J.J.: Universal designated verifier signatures without random oracles or non-black box assumptions. In: Prisco, R.D., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 63–77. Springer, Heidelberg (2006)

[25] Laguillaumie, F., Vergnaud, D.: Time-selective convertible undeniable signatures. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 154–171. Springer, Heidelberg (2005)

[26] Lee, J.Y., Cheon, J.H., Kim, S.: An analysis of proxy signatures: Is a secure channel necessary? In: Joye, M. (ed.) CT-RSA 2003. Lecture Notes in Computer Science, vol. 2612, pp. 68–79. Springer, Heidelberg (2003)

[27] Libert, B., Quisquater, J.J.: Identity based undeniable signatures. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 112–125. Springer, Heidelberg (2004)

[28] Libert, B., Quisquater, J.J., Yung, M.: Forward-secure signatures in untrusted update environments: efficient and generic constructions. In: 14th ACM Conference on Computer and Communications Security, pp. 266–275. ACM Press (2007)

[29] Liu, J.K., Wong, D.S.: Linkable ring signatures: Security models and new schemes. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganà, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3481, pp. 614–623. Springer, Heidelberg (2005)

[30] Lu, S., Ostrovsky, R., Sahai, A., Shacham, H., Waters, B.: Sequential aggregate signatures and multisignatures without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 465–485. Springer, Heidelberg (2006)

[31] Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal of Computing 17(2) pp. 373–386 (1988)

[32] Lysyanskaya, A., Micali, S., Reyzin, L., Shacham, H.: Sequential aggregate signatures from trapdoor permutations. In: Cachin, C., Camenisch, J. (eds.) EUROCYRPT 2004. LNCS, vol. 3027, pp. 74–90. Springer, Heidelberg (2004)

[33] Malkin, T., Micciancio, D., Miner, S.K.: Efficient generic forward-secure signatures with an unbounded. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 400–417. Springer, Heidelberg (2002)

[34] Menezes, A., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press (1996)

[35] Micali, S., Ohta, K., Reyzin, L.: Accountable-subgroup multisignatures: extended abstract. In: 8th ACM Conference on Computer and Communications Security, pp. 245–254. ACM Press (2001)

[36] Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: 22nd Annual ACM Symposium on Theory of Computing, pp. 427–437. ACM Press (1990)

[37] Okamoto, T., Tada, M., Okamoto, E.: Extended proxy signatures for smart cards. In: Mambo, M., Zheng, Y. (eds.) ISW 1999. LNCS, vol. 1729, pp. 247–258. Springer, Heidelberg (1999)

[38] Pass, R., Shelat, A., Vaikuntanathan, V.: Relations among notions of non-malleability for encryption. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 519–535. Springer, Heidelberg (2007)

[39] Pointcheval, D., Stern, J.: Security proofs for signature schemes. In: Guillou, L.C., Quisquater, J.J. (eds.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 387–398. Springer, Heidelberg (1996)

[40] Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. Journal of Cryptology 13(3) pp. 361–396 (2000)

[41] Rabin, M.: Digitalized signatures and publickey functions as intractable as factorization. MIT Laboratory for Computer Science (1979)

[42] Rackoff, C., Simon, D.R.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 433–444. Springer, Heidelberg (1991)

[43] Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(2) pp. 120–126 (1978)

[44] Saeednia, S., Kremer, S., Markowitch, O.: An efficient strong designated verifier signature scheme. In: Lim, J.I., Lee, D.H. (eds.) ICISC 2003. LNCS, vol. 2971, pp. 40–54. Springer, Heidelberg (2003)

[45] Shahandashti, S.F., Safavi-Naini, R.: Construction of universal designated-verifier signatures and identity-based signatures from standard signatures. In: Cramer, R. (ed.) PKC 2008. LNCS, vol. 4939, pp. 121–140. Springer, Heidelberg (2008)

[46] Watanabe, Y., Shikata, J., Imai, H.: Equivalence between semantic security and indistinguishability against chosen ciphertext attacks. In: Desmedt, Y. (ed.) PKC 2003. LNCS, vol. 25678, pp. 71–84. Springer, Heidelberg (2003)

[47] Yao, A.C.: Theory and application of trapdoor functions. In: 23rd IEEE Symposium on Foundations of Computer Science, pp. 80–91. IEEE (1982)