中央大学数学教室講究録　No.3

# 双線形写像暗号とその発展

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　3

# 双線形写像暗号とその発展

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，2009 年 1 月 28 日から 2 月 5 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，双線形写像暗号とその発展についての様々な解説を行っていただいた．講義は 5 日間に渡って行われ，近年の公開鍵暗号に用いられている双線形写像を用いた公開鍵暗号方式の安全性やその証明，またその発展等，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。

2009 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

双線形写像が暗号に応用されてから 10 年近くが経過し，その応用範囲は暗号全般に及んでいる．本講義では、公開鍵暗号概念の拡張として近年研究されている

- ID ベース暗号 (IBE)
- 階層 ID ベース暗号 (HIBE)
- 属性ベース暗号 (ABE)

やディジタル署名への応用等について，安全性の定式化やそれぞれの方式の構成法，そして安全性の証明に関して取り扱う．

## 1.1　用語及び基本概念

$1^k$: 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

$\{0,1\}^*$: 任意長のバイナリ系列

$\mathbb{N}$: 自然数の集合

$\mathbb{Z}_p$: 0 以上 $p$ 未満の整数の集合

$\mathbb{F}_q$: 位数 $q$ の有限体

$a \mid b$: $a$ は $b$ を割り切る

$a \xleftarrow{\mathsf{U}} \mathbb{Z}_p$: $a$ は一様分布な $\mathbb{Z}_p$ の中からランダムに選ばれた値

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

$a \xleftarrow{\mathsf{R}} X_k$: $a$ は確率変数 $X_k$ の中からランダムに選ばれた値

$a \in X$: $a$ 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 $b$

$A \cap B$: 集合 $A$ と集合 $B$ の共通集合

$a := b$: $a$ に $b$ を代入

$a := b \bmod n$: $b \bmod n$ 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

$a \approx b$: $a$ と $b$ は識別不可能

$a \simeq b$: $b$ は $a$ の近似値

$\Pr[A(x) \to a]$: 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

$\epsilon$: いかなる正整数 $c$ に対しても，十分大きな $k$ に対して $\epsilon(k) < k^{-c}$ 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 楕円曲線と双線形写像

楕円曲線とは，一般的に $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a4x + a_6$ で与えられる $(x, y)$ に関する方程式のことである．このとき，有限体 $\mathbb{F}_q$ の標数 $q$ が 5 以上の場合，有限体上の楕円曲線は $y^2 = x^3 + ax + b$ かつ $4a^2 + 27b^2 \neq 0$ で表され，一般に $E/\mathbb{F}_q$ と書く．楕円曲線上の有利点の集合を $E(\mathbb{F}_q)$ で表したとき，$E(\mathbb{F}_q)$ は群をなし，$\mathbb{Z}/n_1\mathbb{Z}$ と $\mathbb{Z}/n_2\mathbb{Z}$ の直積と同型となる $(n_2 \mid n_1,\ n_2 \mid (q-1))$．ねじれ点を $E[n] := \{P \in E(\overline{\mathbb{F}}_q) \mid nP \in \mathcal{O}\}$ と定義すると，$E[n]$ 上で**ペアリング (pairing)** と呼ばれる双線形写像が定義できる．ペアリングは，$e : E[n] \times E[n] \to \mathbb{F}_{q^k}$ で定義され，

- bilinearity

$$\forall S_1, S_2, T_1, T_2, \quad e(S_1 \cdot S_2, T_1) = e(S_1, T_1) \cdot e(S_2, T_1)$$
$$e(S_1, T_1 \cdot T_2) = e(S_1, T_1) \cdot e(S_1, T_2)$$

- non-degeneracity

$$\forall T \in E[n], \quad e(S, T) = 1 \Leftrightarrow S = 0$$

という 2 つの性質を持ち，Miller のアルゴリズム等によって効率的に計算可能である．

ペアリングは，非対称ペアリングと対称ペアリングの二種類に分けることができる．非対称ペアリングにおける群の記述を，$e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$ とする．$\mathbb{G}$ は基礎体，$\hat{\mathbb{G}}$ は拡大体であり，それぞれ $\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T$ の位数は素数 $p$ であるとする．$g \in \mathbb{G}, \hat{g} \in \mathbb{G}$ としたとき，上記の 2 つの性質は

- bilinearity: $\forall a, b \in \mathbb{Z}_p,\ e(g^a, \hat{g}^b) = e(g, \hat{g})^{ab}$

- non-degeneracy: $e(g, \hat{g}) \neq 1 \in \mathbb{G}_T$

と表される．

楕円曲線をとってきた場合，$\mathbb{G}$ と $\hat{\mathbb{G}}$ の関係において

Type1: $\phi : \hat{\mathbb{G}} \to \mathbb{G}$ および $\phi^{-1} : \mathbb{G} \to \hat{\mathbb{G}}$ が効率的に計算可能

Type2: $\phi : \hat{\mathbb{G}} \to \mathbb{G}$ のみ効率的に計算可能

Type3: $\phi, \phi^{-1}$ 共に効率的に計算不可能

の三種類に分けることができる．Supersingular な楕円曲線を選んできた場合は Type1 の写像を求めることができ，この場合を特に非対称ペアリング $e' : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ と定義する．対称ペアリングと非対称ペアリングの関係において，

$$x \in \mathbb{G}, y \in \hat{\mathbb{G}},\ e'(x, \phi(y)) = e(x, y)$$

が成り立つ．

以降では，この双線形写像を用いた公開鍵暗号の様々な方式について述べ，その安全性についての議論を行う．

# 3 公開鍵暗号

**公開鍵暗号 (PKE: Public Key Encryption)** は，暗号化を行う鍵と復号するための鍵が異なり，暗号化を行う鍵を公開しておく暗号方式である．利用者はある決められた手順で公開鍵 $pk$ と秘密鍵 $sk$ のペアを生成し，公開鍵 $pk$ を Web ページなどに登録しておく．秘密鍵 $sk$ は暗号文を復号する際に利用するため，自身で保持しておく．誰かがその利用者に対して暗号化を行う際には，登録されている公開鍵 $pk$ を用いて暗号化を行い，暗号文を生成する．利用者はその暗号文を受け取ると，自身で秘密にしておいた秘密鍵 $sk$ を用いて復号を行う．

## 3.1 公開鍵暗号の定義

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

$\mathsf{Gen}$ : 鍵生成 - $k$ をセキュリティパラメータとしたとき，$1^k$ を入力とし，公開鍵と秘密鍵のペア $(pk, sk)$ を出力するアルゴリズム．また，このとき平文空間 $\mathcal{M}_{pk}$ が決まる．

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

Enc：暗号化 - 公開鍵 $pk$ と平文空間から取ってきた平文 $m \in \mathcal{M}$ 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 $m$ を出力するアルゴリズム．

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

である．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するものである．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．確定的アルゴリズムとは，同じ値が入力されたときは同じ値を出力するアルゴリズムである．

公開鍵暗号における正当性とは，正しく平文 $m$ を暗号化されている場合に，その復号結果が正しく元の平文に戻ることであり，

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

と表される．

## 3.2 公開鍵暗号の安全性

公開鍵暗号の安全性は 達成度，攻撃法 の二通りから考えられる．

### 3.2.1 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)** - 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)** - ある平文 $m$ に対する暗号文 $c = E(m)$ が与えられたとき，関係 $R$ に関して $R(m, m')$ となる暗号文 $c' = E(m')$ を出力することができないこと．

### 3.2.2 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: Chosen Ciphertext Attack 1)** - 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: Chosen Ciphertext Attack 2)** - 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．

公開鍵暗号の安全性に関して最も望ましい安全性は IND-CCA2 であり，以下の攻撃者 $\mathcal{A} = (\mathcal{A}_1, cA_2)$ と挑戦者 challenger との間のゲーム (IND-CCA2 ゲーム) を行うものである．IND-CCA2 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-CCA2 ゲーム:**

**Setup**: $1^k$ を入力として，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**: 攻撃者 $\mathcal{A}$ 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適応的に何度も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 $(m_0, m_1)$ のうち $b \xleftarrow{\cup} \{0, 1\}$ からどちらか一方の平文 $m_b$ を選び，$c^* := \mathsf{Enc}(pk, m_b)$ 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 $C^*$ 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．

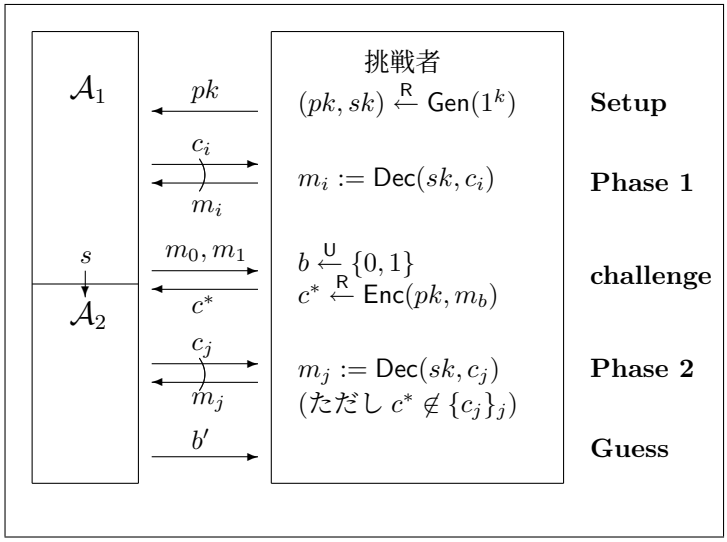


図 1: IND-CCA2

**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．

この IND-CCA2 ゲームは図 1 のように表すことができ，このゲームにおける攻撃者 $\mathcal{A}$ の優位性は

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

で表される．そして，いかなる確率的多項式時間の攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}CCA2}}(k) \leq \epsilon(k)$ が成立する場合，その公開鍵暗号は IND-CCA2 安全であるという．一般に，識別不可能性のゲームにおける攻撃者の優位性は

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}ATK}}(k) := \left| 2 \cdot \Pr \left[ b' = b \mid \begin{array}{l} (pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k); \\ (m_0, m_1) \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}_1}(pk); \\ b \xleftarrow{\mathsf{U}} \{0,1\}; \\ c^* := \mathsf{Enc}(pk, m_b); \\ b' \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}_2}(c^*) \end{array} \right] - 1 \right|$$

と定式化することができ，攻撃法によって

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

と分けることができる．

# 4 ディジタル署名

## 4.1 ディジタル署名の定義

**ディジタル署名 (Digital Signature)** は 3 つのアルゴリズム $(\mathsf{G_{sig}}, \mathsf{S_{sig}}, \mathsf{V_{sig}})$ からなっており，

$\mathsf{G_{sig}}$：鍵生成 - $k$ をセキュリティパラメータとして $1^k$ を入力とし，署名鍵と検証鍵のペア $(sk, vk)$ を出力するアルゴリズム．また，このときメッセージ空間 $\mathcal{M}_{sig}$ が定まる．

$$1^k \rightarrow \boxed{\mathsf{G_{sig}}} \rightarrow (sk, vk)$$

$\mathsf{S_{sig}}$： 署名 - 検証鍵 $vk$ と署名鍵 $sk$ とメッセージ空間から取ってきたメッセージ $m \in \mathcal{M}_{sig}$ を入力とし，署名 $\sigma$ を出力するアルゴリズム．

$$(vk, sk, m) \rightarrow \boxed{\mathsf{S_{sig}}} \rightarrow \sigma$$

$\mathsf{V_{sig}}$：検証 - 検証鍵 $vk$ とメッセージ $m$ と署名 $\sigma$ を入力とし，検証を行うアルゴリズム．検証式を満たす場合は 1 を，そうでなければ 0 を出力する．

$$(vk, m, \sigma) \rightarrow \boxed{\mathsf{V_{sig}}} \rightarrow 1 \text{ or } 0$$

である．ディジタル署名における正当性とは，正しく生成された署名 $\sigma$ を検証した場合に，その検証が正しく通ることであり，

$$\Pr\left[\mathsf{S_{sig}}(vk, \sigma, m) = 1 \mid \begin{array}{l} (sk, vk) \xleftarrow{\mathsf{R}} \mathsf{G_{sig}}(1^k); \\ m \in \mathcal{M}_{sig}; \\ \sigma \xleftarrow{\mathsf{R}} \mathsf{S_{sig}}(vk, sk, m) \end{array}\right] = 1$$

と表される．

## 4.2 ディジタル署名の安全性

ディジタル署名の安全性としては，いかなる文書に対しても偽造が困難であることが求められる．このとき，攻撃者は署名オラクルを利用することで自分で選んだメッセージに対しての署名が得られるものとした場合，

・署名オラクルに何回アクセスできるか

・過去に署名オラクルに聞いたメッセージを用いた新たな署名の偽造を考慮に入れるか

に分類して考える．

2つの分類の中でも，攻撃者の署名オラクルの利用を一度に限定し，過去に署名オラクルに聞いたメッセージを用いた新たな署名の偽造を考慮に入れるものを **one-time strong EUF-CMA** と呼ぶ．この場合の攻撃者 $\mathcal{A}$ の成功確率は

$$\begin{aligned}&\mathsf{Adv}^{\mathsf{OT\text{-}sEUF\text{-}CMA}}_{\mathcal{A}}(k)\\ &:= \Pr\left[\begin{array}{l|l}\mathsf{V}_{\mathsf{sig}}(vk, m', \sigma') = 1 \wedge & (sk, vk) \xleftarrow{\mathsf{R}} \mathsf{G}_{\mathsf{sig}};\ m \xleftarrow{\mathsf{R}} \mathcal{A}(vk);\\ (m', \sigma') \neq (m, \sigma) & \sigma \xleftarrow{\mathsf{R}} \mathsf{S}_{\mathsf{sig}}(vk, sk, m);\ (m', \sigma') \xleftarrow{\mathsf{R}} \mathcal{A}(\sigma)\end{array}\right]\end{aligned}$$

として定式化できる．いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}^{\mathsf{OT\text{-}sEUF\text{-}CMA}}_{\mathcal{A}}(k)$ が negligible ならばそのディジタル署名は one-time strong EUF-CMA であると呼ぶ．

また，署名オラクルを多項式回利用することができ，過去に署名オラクルに聞いたメッセージを用いた偽造を考慮に入れないものを **EUF-CMA** と呼ぶ．この場合の攻撃者 $\mathcal{A}$ の成功確率は

$$\begin{aligned}&\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathcal{A}}(k)\\ &:= \Pr\left[\begin{array}{l|l}\mathsf{V}_{\mathsf{sig}}(vk, m, \sigma) = 1 \wedge m \text{ が署名} & (sk, vk) \xleftarrow{\mathsf{R}} \mathsf{G}_{\mathsf{sig}};\\ \text{オラクルに聞かれていない} & (m, \sigma) \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathsf{S}_{\mathsf{sig}}(vk, sk, \cdot)}(vk)\end{array}\right]\end{aligned}$$

として定式化でき，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathcal{A}}(k)$ が negligible ならばそのディジタル署名は EUF-CMA であると呼ぶ．

# 5 ID ベース暗号

**ID ベース暗号 (IBE: Identity Based Encryption)** は PKE の拡張の一つであり，PKE において利用者は公開鍵を生成していたのに対し，IBE では利用者の ID を公開鍵の代わりに用いる方式である．IBE においてはシステム全体で利用されるシステム公開鍵と，それに対応するマスター秘密鍵が存在し，ID 一つ一つに対応する秘密鍵はマスター秘密鍵から生成される．IBE では利用者にメッセージを暗号化して送りたい場合にシステム公開鍵と ID を入力し，生成された暗号文は対応する秘密鍵を知っている利用者のみが復号することができる．

## 5.1 ID ベース暗号の定義

ID ベース暗号は 4 つのアルゴリズム $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ からなっており，

$\mathsf{Setup}$ : セットアップ - $k$ をセキュリティパラメータとしたとき $1^k$ を入力とし，システム公開鍵とマスター秘密鍵のペア $(pk, mk)$ を出力するアルゴリズム．また，

このとき平文空間 $\mathcal{M}_{IBE}$ が定まる．

$$1^k \rightarrow \boxed{\mathsf{Setup}} \rightarrow (pk, mk)$$

KeyGen：鍵生成 - $mk$ とアイデンティティID を入力とし，その ID に対する個別秘密鍵 $d_{\mathrm{ID}}$ を出力するアルゴリズム．

$$(pk, mk, \mathrm{ID}) \rightarrow \boxed{\mathsf{KeyGen}} \rightarrow d_{\mathrm{ID}}$$

Enc：暗号化 - $pk$ と暗号文を送る相手の ID，平文空間から取ってきた平文 $m \in \mathcal{M}_{IBE}$ を入力とし，暗号文 $c$ を出力するアルゴリズム．

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

Dec：復号 - $pk$ と暗号文 $c$，秘密鍵 $d_{\mathrm{ID}}$ を入力とし，平文 $m$ を出力するアルゴリズム．

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

である．ID ベース暗号における正当性とは，正しく平文 $m$ を暗号化されている場合に，その復号結果が正しく元の平文に戻ることであり，

$$\Pr\left[m' = m \mid \begin{array}{l} (pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k);\ d_{\mathrm{ID}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(pk, mk, \mathrm{ID}); \\ m \in \mathcal{M}_{IBE};\ c \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \mathrm{ID}, m);\ m' := \mathsf{Dec}(pk, d_{\mathrm{ID}}, c) \end{array}\right] = 1$$

と表される．

## 5.2 ID ベース暗号の安全性

ID ベース暗号の安全性は 2 つの達成度と攻撃法 のから考えられる．

### 5.2.1 安全性の達成度 1

ID ベース暗号における安全性の達成度の 1 つ目は公開鍵暗号と同様であり，

- 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)** - 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)** - ある平文 $m$ に対する暗号文 $c = E(m)$ が与えられたとき，関係 $R$ に関して $R(m, m')$ となる暗号文 $c' = E(m')$ を出力することができないこと.

の三種類について分類する.

#### 5.2.2 安全性の達成度 2

ID ベース暗号における安全性の達成度の 2 つ目は，ID ベース特有の達成度で,

- **選択 ID 型 (sID: selective ID)**: 攻撃者があらかじめターゲットとする ID を，公開パラメータが与えられる前に定めておくもの.

- **適応的 ID 型 (aID: adaptive ID)**: 攻撃者がターゲットとする ID を，challenge 暗号文 $c^*$ を受け取る直前に定めるもの.

である．選択 ID 型の安全性は sID と呼ばれるが，適応的 ID 型の場合は単に ID 安全と呼ぶことが多い．ID ベース暗号において望ましい安全性は適応的 ID 型であるが，既存の ID ベース暗号方式の中には選択 ID 型で証明されているものが存在し，それが将来的な発展に繋がっている.

#### 5.2.3 攻撃法

ID ベース暗号における攻撃の種類は公開鍵暗号と同じで,

- **選択平文攻撃 (CPA: Chosen Plaintext Attack)**

- **選択暗号文攻撃 (CCA1: Chosen Ciphertext Attack 1)**

- **適応的選択暗号文攻撃 (CCA2: Chosen Ciphertext Attack 2)**

に分類することができる.

ID ベース暗号において，最も望まれる安全性は IND-ID-CCA2 であり，以下の攻撃者 $\mathcal{A}$ と挑戦者 challenger との間のゲームとして図 2 のように定式化される.

IND-ID-CCA2 ゲームにおける攻撃者 $\mathcal{A}$ の優位性は

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

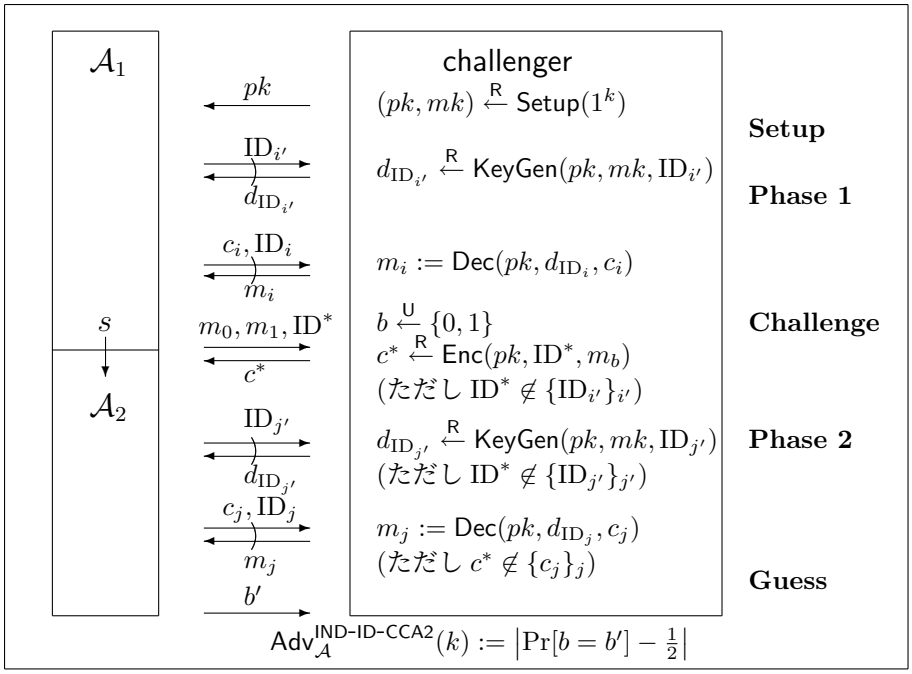


図 2: IND-ID-CCA2

で表され，いかなる確率的多項式時間の攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}^{\mathsf{IND\text{-}ID\text{-}CCA2}}_{\mathcal{A}}(k) \leq \epsilon(k)$ が成立する場合，その ID ベース暗号は IND-ID-CCA2 安全であるという．公開鍵暗号の IND-CCA2 ゲームとは異なり，**Phase 1** および **Phase 2** において KeyGen オラクルを利用することで，ターゲットとする ID 以外に対して秘密鍵を得ることができる．

また，一般に適応的 ID 型の識別不可能性のゲームにおける攻撃者の成功確率は

$$\mathsf{Adv}^{\mathsf{IND\text{-}ID\text{-}ATK}}_{\mathcal{A}}(k) := \left| 2 \cdot \Pr\left[ b' = b \mid \begin{array}{l} (pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k); \\ (m_0, m_1, \mathrm{ID}^*) \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}_1}(pk); \\ b \xleftarrow{\mathsf{U}} \{0,1\}; \\ c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \mathrm{ID}^*, m_b); \\ b' \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}_2}(c^*) \end{array} \right] - 1 \right|$$

と表され，攻撃法によって

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

と分けることができる．

また，ID ベース暗号においては，IND-sID-CPA 安全な方式も重要な役割を持つ．IND-sID-CPA における攻撃者 $\mathcal{A}$ と挑戦者 challenger の間のゲームは図 3 のように定式化される．

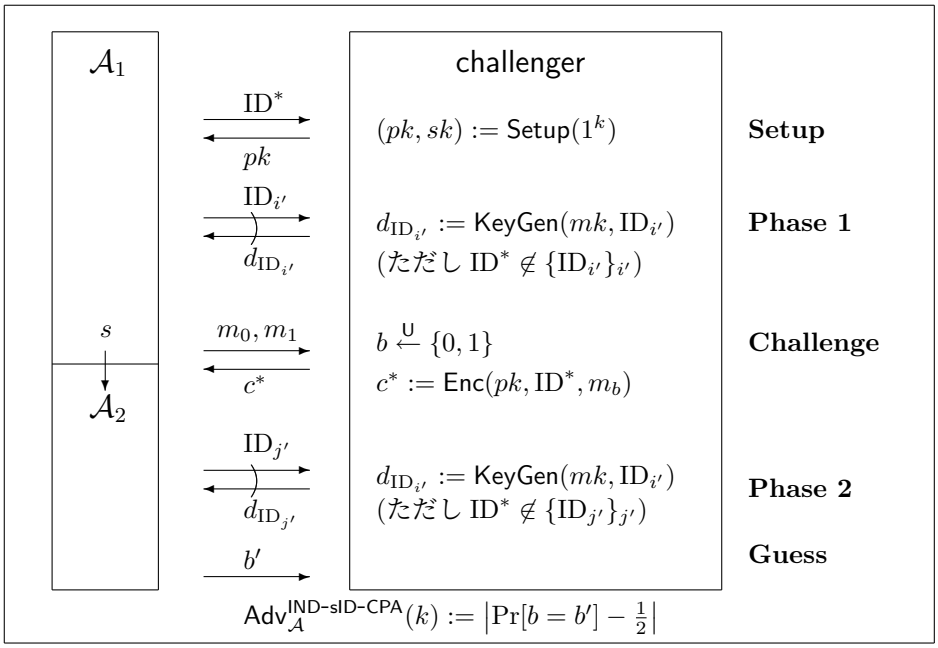


図 3: IND-sID-CPA

図 3 の IND-sID-CPA ゲームにおける攻撃者 $\mathcal{A}$ の優位性は

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

で表され，いかなる確率的多項式時間の攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}^{\mathsf{IND\text{-}sID\text{-}CPA}}_{\mathcal{A}}(k) \leq \epsilon(k)$ が成立する場合，その ID ベース暗号は IND-sID-CPA 安全であるという．IND-ID-CCA2 ゲームと異なる点は，**Phase 1** および **Phase 2** において復号オラクルを利用できないこと，およびターゲットとする $\mathrm{ID}^*$ を **challenge** の時ではなく **Setup** が行われる前段階に宣言することである．

また，一般に sID 型の識別不可能性のゲームにおける攻撃者の成功確率は

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sID\text{-}ATK}}(k) := \left| 2 \cdot \Pr \left[ b' = b \mid \begin{array}{l} \mathrm{ID}^* := \mathcal{A}(); \\ (pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k); \\ (m_0, m_1) \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}_1}(pk); \\ b \xleftarrow{\mathsf{U}} \{0,1\}; \\ c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \mathrm{ID}^*, m_b); \\ b' \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}_2}(c^*) \end{array} \right] - 1 \right|$$

と表され，攻撃法によって

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

と分けることができる．

## 5.3 ペアリングを用いた IBE の分類

効率的な IBE の構成は，2000 年に Sakai-Ohgishi-Kasahara らによってペアリングを用いて提案されたものが始まりとなり，以降様々な IBE の構成が提案されている．既存研究におけるペアリングを用いた IBE の構成方法は，

- **Full Domain Hash IBE**

  Sakai-Ohgishi-Kasahara (2000) [18]

  Boneh-Franclin (2001) [6]

- **Exponent Inversion IBE**

  Sakai-Kasahara (2003) [17]

  Boneh-Boyen (2004) [3]

  Gentry (2006) [12]

- **Commutative Blinding IBE**

  Boneh-Boyen (2004) [4]

  Waters (2005) [19]

と大きく三つの方式に分類することができる．それぞれ分類に応じて個別秘密鍵の構成や安全性の根拠となる数論仮定などが異なる．

## 5.4 Random Oracle Model の下で安全な IBE

上記の三つの分類された方式をそれぞれ比較するため，Random Oracle Model で証明することができる Boneh-Franclin IBE，Sakai-Kasahara IBE，Boneh-Boyen IBE を例として取り上げる．なお，これらはすべて Fujisaki-Okamoto 変換 [11] という変換手法を用いており，IND-ID-CCA2 安全な方式へと変換されている．

### 5.4.1 Random Oracle Model

Random Oracle Model とは，ハッシュ関数を理想的なランダム関数として扱うモデルである．Random Oracle Model においては，理想的ランダムハッシュ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，その出力ビット列をランダムなコイン投げによって決める．通常の暗号学的ハッシュ関数の場合は，入力値に対して効率的な計算により出力が決まるが，理想的ランダム関数では上記のように定められたテーブルにより出力値が決まる．Random Oracle Model においては各ランダム関数 $G$ や $H$ は理想的ランダム関数として定義され全利用者に共有される．従って同じ入力値に対しての出力値は常に同じである．

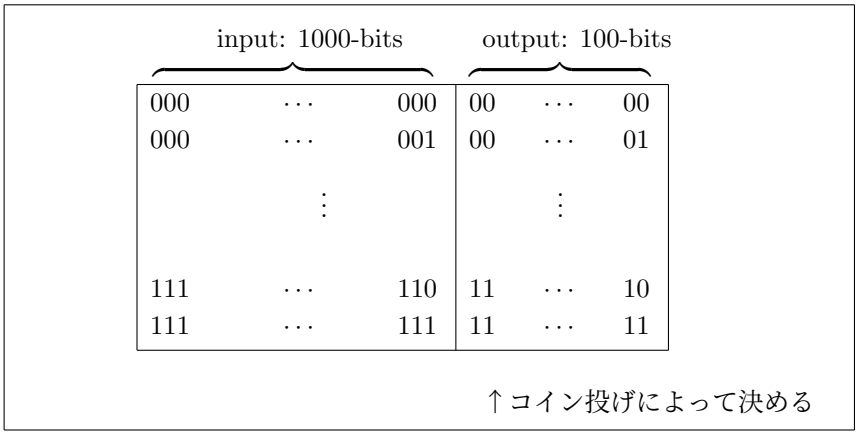


図 4: Random Oracle Model

### 5.4.2 Boneh-Franclin IBE (BF01 IBE)

Full Domain Hash IBE (FDH IBE) に分類される Boneh-Franclin IBE [6] は，非対称ペアリングを用いた場合以下のように構成される．

**Setup:** $\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T$ を素位数 $p$ の群，$g$ を群 $\mathbb{G}$ の生成元とし，$w \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $g_1 := g^w$ を求める．また，ハッシュ関数として $H_1 : \{0,1\}^* \to \hat{\mathbb{G}}$，$H_2 : \mathbb{G}_T \to \{0,1\}^\ell, H_3 : \{0,1\}^\ell \times \{0,1\}^\ell \to \mathbb{Z}_p, H_4 : \{0,1\}^\ell \to \{0,1\}^\ell$ を取ってくる．$pk := (g, g_1, H_1, H_2, H_3, H_4)$，$mk := w$ とする．

$$pk = (g, g_1, H_1, H_2, H_3, H_4),\ mk = w$$

**KeyGen:** ある ID $\in \{0,1\}^*$ に対しての個別秘密鍵を生成する場合，ID と $mk$ を入力とし，$d_{\mathrm{ID}} := H_1(\mathrm{ID})^w \in \hat{\mathbb{G}}$ を求め $d_{\mathrm{ID}}$ を個別秘密鍵とする．

**Enc:** ある ID に対してメッセージ $m \in \{0,1\}^\ell$ を暗号化する場合，

1. $s \xleftarrow{\mathsf{U}} \{0,1\}^\ell$ を選ぶ．
2. $r := H_3(s, m)$ とする．
3. $c_0 := g^r, c_1 := s \oplus H_2(e(g_1, H_1(\mathrm{ID}))^r), c_2 := m \oplus H_4(s)$ を計算する．
4. $C := (c_0, c_1, c_2)$ を暗号文として出力する．

**Dec:** $d_{\mathrm{ID}}$ を用いて暗号文 $C = (c_0, c_1, c_2)$ を復号する場合，

1. $s' := H_2(e(c_0, d_{\mathrm{ID}})) \oplus c_1$ とする．
2. $m' := H_4(s') \oplus c_2$ を求める．
3. $r' = H_3(s', m')$ を求める．
4. $g^{r'} = c_0$ であれば $m'$ を平文として出力し，そうでなければ正しくない暗号文であるとして $\perp$ を出力する．

Boneh-Franclin IBE では，暗号文 $(c_0, c_1, c_2)$ が正しく生成されている場合，

$$\begin{aligned} s' &= H_2(e(c_0, d_{\mathrm{ID}})) \oplus c_1 \\ &= H_2(e(g^r, H_1(\mathrm{ID})^w)) \oplus (s \oplus H_2(e(g_1, H_1(\mathrm{ID}))^r)) \\ &= H_2(e(g_1, H_1(\mathrm{ID})^r)) \oplus s \oplus H_2(e(g_1, H_1(\mathrm{ID}))^r) \\ &= s \end{aligned}$$

という関係が成り立つことで，$H_4(s') \oplus c_2 = m$ として平文を復号している．

Boneh-Franclin IBE の安全性の根拠となる数論仮定は，BDH (Bilinear Diffie-Hellman) 仮定と呼ばれるものである．

対称ペアリングにおける BDH 仮定

$a, b, c \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ として $(g, g^a, g^b, g^c) \in \mathbb{G}^4$ が入力された場合に，$e'(g,g)^{abc} \in \mathbb{G}_T$ を求める問題を対称ペアリングにおける BDH 問題と呼ぶ．そして，いかなる多項式時間

攻撃者に対しても BDH 問題を解くことが困難である場合，その群上において BDH 仮定が保たれているという．

**定義 5.1.** 攻撃者 $\mathcal{A}$ の *BDH* 問題に対する優位性を

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{BDH}}(k) := \Pr\left[\mathcal{A}(g, g^a, g^b, g^c) \to e'(g,g)^{abc} \mid a, b, c \xleftarrow{\mathsf{U}} \mathbb{Z}_p\right]$$

と置いたとき，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても，$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{BDH}}(k) \leq \epsilon(k)$ である場合，その群において *BDH* 仮定が保たれているという．

非対称ペアリングにおける BDH 仮定

$a, b, c \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ として $(g, g^a, g^b, g^c, \hat{g}, \hat{g}^a, \hat{g}^b, \hat{g}^c) \in \mathbb{G}^4 \times \hat{\mathbb{G}}^4$ が入力された場合に，$e(g,\hat{g})^{abc} \in \mathbb{G}_T$ を求める問題を非対称ペアリングにおける BDH 問題と呼ぶ．そして，いかなる多項式時間攻撃者に対しても BDH 問題を解くことが困難である場合，その群上において BDH 仮定が保たれているという．

**定義 5.2.** 攻撃者 $\mathcal{A}$ の *BDH* 問題に対する優位性を

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{BDH}'}(k) := \Pr\left[\mathcal{A}(g, g^a, g^b, g^c, \hat{g}, \hat{g}^a, \hat{g}^b, \hat{g}^c) \to e(g,\hat{g})^{abc} \mid a, b, c \xleftarrow{\mathsf{U}} \mathbb{Z}_p\right]$$

と置いたとき，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{BDH}'}(k) \leq \epsilon(k)$ である場合，その群において *BDH* 仮定が保たれているという．

**定理 5.1.** *Boneh-Franclin IBE* は *Random Oracle Model* において非対称ペアリングにおける *BDH* 仮定の下で *IND-ID-CCA2* 安全な *IBE* である．

### 5.4.3 Sakai-Kasahara IBE (SK03 IBE)

Exponent Inversion IBE に分類される Sakai-Kasahara IBE [17] は，非対称ペアリングを用いた場合以下のように構成される．なお，この IBE の安全性証明は 2005 年 Chen-Cheng によって示された [10].

**Setup:** $\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T$ を素位数 $p$ の群，$g$ を群 $\mathbb{G}$ の生成元，$\hat{g}$ を群 $\hat{\mathbb{G}}$ の生成元とする．$w \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $g_1 := g^w$ を求め，$v_0 := e(g,\hat{g})$ とする．また，ハッシュ関数として $H_1 : \{0,1\}^* \to \mathbb{Z}_p$，$H_2 : \mathbb{G}_T \to \{0,1\}^\ell, H_3 : \{0,1\}^\ell \times \{0,1\}^\ell \to \mathbb{Z}_p, H_4 : \{0,1\}^\ell \to \{0,1\}^\ell$ を取ってくる．$pk := (g, g_1, \hat{g}, v_0, H_1, H_2, H_3, H_4)$，$mk := w$ とする．

$$pk = (g, g_1, \hat{g}, v_0, H_1, H_2, H_3, H_4),\ mk = w$$

**KeyGen:** ある $\mathrm{ID} \in \{0,1\}^*$ に対しての個別秘密鍵を生成する場合，ID と $mk$ を入力とし，$d_{\mathrm{ID}} := \hat{g}^{\frac{1}{w + H_1(\mathrm{ID})}} \in \hat{\mathbb{G}}$ を求め $d_{\mathrm{ID}}$ を個別秘密鍵とする．

**Enc:** ある ID に対してメッセージ $m \in \{0,1\}^\ell$ を暗号化する場合,

1. $s \xleftarrow{\mathsf{U}} \{0,1\}^\ell$ を選ぶ.
2. $r := H_3(s, m)$ とする.
3. $c_0 := (g_1 g^{H_1(\mathrm{ID})})^r, c_1 := H_2(v_0^r), c_2 := m \oplus H_4(s)$ を計算する.
4. $C := (c_0, c_1, c_2)$ を暗号文として出力する.

**Dec:** $d_{\mathrm{ID}}$ を用いて暗号文 $C = (c_0, c_1, c_2)$ を復号する場合,

1. $s' := H_2(e(c_0, d_{\mathrm{ID}})) \oplus c_1$ とする.
2. $m' := H_4(s') \oplus c_2$ を求める.
3. $r' = H_3(s', m')$ を求める.
4. $(g_1 g^{H_1(\mathrm{ID})})^{r'} = c_0$ であれば $m'$ を平文として出力し，そうでなければ正しくない暗号文であるとして $\perp$ を出力する.

Sakai-Kasahara IBE では，暗号文 $(c_0, c_1, c_2)$ が正しく生成されている場合,

$$\begin{aligned} s' &= H_2(e(c_0, d_{\mathrm{ID}})) \oplus c_1 \\ &= H_2(e((g_1 g^{H_1(\mathrm{ID})})^r, \hat{g}^{\frac{1}{w+H_1(\mathrm{ID})}})) \oplus c_1 \\ &= H_2(e(g^{w+H_1(\mathrm{ID})}, \hat{g}^{\frac{1}{w+H_1(\mathrm{ID})}})^r) \oplus c_1 \\ &= H_2(e(g, \hat{g})^r) \oplus s \oplus H_2(v_0^r) \\ &= s \end{aligned}$$

という関係が成り立つことで，$H_4(s') \oplus c_2 = m$ として平文を復号している.

Sakai-Kasahara IBE の安全性の根拠となる数論仮定は，$q$-BDHI (Bilinear Diffie-Hellman Inversion) 仮定と呼ばれるものである.

対称ペアリングにおける $q$-BDHI 仮定

$x \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ として $(g, g^x, g^{x^2}, \ldots, g^{x^q}) \in \mathbb{G}^{q+1}$ が入力された場合に，$e'(g,g)^{1/x} \in \mathbb{G}_T$ を求める問題を $q$-BDHI 問題と呼ぶ．そして，いかなる多項式時間攻撃者に対しても $q$-BDHI 問題を解くことが困難である場合，その群上において $q$-BDHI 仮定が保たれているという.

**定義 5.3.** 攻撃者 $\mathcal{A}$ の *$q$-BDHI* 問題に対する優位性を

$$\mathsf{Adv}_{\mathcal{A}}^{q\text{-}\mathsf{BDHI}}(k) := \Pr\left[\mathcal{A}(g, g^x, g^{x^2}, \ldots, g^{x^q}) \to e(g,\hat{g})^{1/x} \mid x \xleftarrow{\mathsf{U}} \mathbb{Z}_p\right]$$

と置いたとき，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}_{\mathcal{A}}^{q\text{-}\mathsf{BDHI}}(k) \le \epsilon(k)$ である場合，その群において *$q$-BDHI* 仮定が保たれているという.

**定理 5.2.** *Boneh-Franclin IBE* は *Random Oracle Model* において *q-BDHI* 仮定の下で *IND-ID-CCA* 安全な *IBE* である．

### 5.4.4 Boneh-Boyen IBE (BB04 IBE)

Commutative Blinding IBE に分類される Boneh-Boyen IBE [4] は，非対称ペアリングを用いた場合以下のように構成される．なお，この IBE は元々は Random Oracle Model ではなく，Standard Model の下で証明された IBE であるが，比較のため Commutative blinding を用いつつ Random Oracle Model の下で安全性を持つ効率な IBE へと変更したものである [8].

Setup: $\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T$ を素位数 $p$ の群，$g$ を群 $\mathbb{G}$ の生成元，$\hat{g}$ を群 $\hat{\mathbb{G}}$ の生成元とする．$\alpha, \beta, \gamma \xleftarrow{\cup} \mathbb{Z}_p$ から $g_1 := g^\alpha, g_3 := g^\gamma$ を求め，$v_0 := e(g, \hat{g})^{\alpha\beta}$ とする．また，ハッシュ関数として $H_1 : \{0,1\}^* \to \mathbb{Z}_p$，$H_2 : \mathbb{G}_T \to \{0,1\}^\ell, H_3 : \mathbb{G}_T \times \mathbb{G}^2 \to \mathbb{Z}_p$ を取ってくる．$pk := (g, g_1, \hat{g}, v_0, H_1, H_2, H_3)$，$mk := (\alpha, \beta, \gamma)$ とする．

$$pk = (g, g_1, g_3, v_0, H_1, H_2, H_3, H_4),\ mk = (\hat{g}, \alpha, \beta, \gamma)$$

KeyGen: ある ID $\in \{0,1\}^*$ に対しての個別秘密鍵を生成する場合，ID と $mk$ を入力とし，$r \xleftarrow{\cup} \mathbb{Z}_p$ を選んで $(d_0, d_1) := \hat{g}^{\alpha\beta + (\alpha H_1(\mathrm{ID}) + \gamma) r}, \hat{g}^r) \in \hat{\mathbb{G}}^2$ を求め，$d_{\mathrm{ID}} := (d_0, d_1)$ を個別秘密鍵とする．

Enc: ある ID に対してメッセージ $m \in \{0,1\}^\ell$ を暗号化する場合，

1. $s \xleftarrow{\cup} \mathbb{Z}_p$ を選ぶ．
2. $c := m \oplus H_2(v_0^s), c_0 := g^s, c_1 := g_3^s \cdot g_1^{H_1(\mathrm{ID})s}$ を求める．
3. $t := s \oplus H_3(v_0^s, c_0, c_1)$ とする．
4. $C := (c, c_0, c_1, t)$ を暗号文として出力する．

Dec: $d_{\mathrm{ID}}$ を用いて暗号文 $C = (c, c_0, c_1, t)$ を復号する場合，

1. $k' := e(c_0, d_0) \cdot e(c_1, d_1)^{-1}$ を計算する．
2. $m' := c \oplus H_2(k')$ とする．
3. $s' := t \oplus H_3(k', c_0, c_1)$ を求める．
4. $g^{s'} = c_0$ かつ $(g_3 \cdot g_1^{H_1(\mathrm{ID})})^{s'} = c_1$ であれば $m'$ を平文として出力し，そうでなければ正しくない暗号文であるとして $\perp$ を出力する．

Boneh-Boyen IBE では，暗号文 $(c, c_0, c_1, t)$ が正しく生成されている場合，

$$\begin{aligned} e(c_0, d_0) &= e(g^s, \hat{g}^{\alpha\beta+(\alpha H_1(\mathrm{ID})+\gamma)r}) \\ &= e(g, \hat{g})^{s(\alpha\beta+(\alpha H_1(\mathrm{ID})+\gamma)r)} \\ e(c_1, d_1) &= e(g_3^s \cdot g_1^{H_1(\mathrm{ID})s}, \hat{g}^r) \\ &= e(g, \hat{g})^{s(\alpha H_1(\mathrm{ID})+\gamma)\cdot r} \end{aligned}$$

により $k' = e(c_0, d_0) \cdot e(c_1, d_1)^{-1} = e(g, \hat{g})^{s\alpha\beta} = v_0^s$ という関係が成り立つことで，$H_2(k') \oplus c = m$ として平文を復号している．

Boneh-Boyen IBE の安全性の根拠となる数論仮定は，BDH 問題である．

**定理 5.3.** *Boneh-Boyen IBE は Random Oracle Model において BDH 仮定の下で IND-ID-CCA 安全な IBE である．*

## 5.5 Standard Model の下で安全な IBE

### 5.5.1 Boneh-Boyen IBE (BB04a IBE)

上記の Commutative Blinding IBE に分類される Boneh-Boyen IBE [4] は Random Oracle Model で証明される方式であったが，元々は Standard Model の下で証明可能安全性を持つ方式として提案されていた．Standard Model における方式では以下のようになる．なお，以降の方式ではすべて対称ペアリングを用いた構成法を述べる．

**Setup:** $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とする．$g, g_2, h \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$a \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $g_1 := g^a$ を求める．$pk := (g, g_1, g_2, h)$，$mk := g_2^a$ とする．

$$pk = (g, g_1, g_2, h),\ mk = g_2^a$$

**KeyGen:** ある $\mathrm{ID} \in \mathbb{Z}_p$ に対しての個別秘密鍵を生成する場合，ID と $mk$ を入力とし，$r \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選んで $(d_0, d_1) := (g_2^a \cdot (g_1^{\mathrm{ID}} \cdot h)^r, g^r) \in \mathbb{G}^2$ を求め，$d_{\mathrm{ID}} := (d_0, d_1)$ を個別秘密鍵とする．

**Enc:** ある ID に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選ぶ．
2. $c_0 := g^s, c_1 := (g_1^{\mathrm{ID}} \cdot h)^s, c_2 := e'(g_1, g_2)^s \cdot m$ とする．
3. $C := (c_0, c_1, c_2)$ を暗号文として出力する．

**Dec:** 暗号文 $C = (c_0, c_1, c_2)$ および $d_{\mathrm{ID}}$ を入力とし，$m' = c_2 \cdot e'(c_1, d_1) \cdot e'(c_0, d_0)^{-1}$ を出力する．

BB04a IBE において，暗号文 $(c_0, c_1, c_2)$ が正しく生成されているならば，

$$\begin{aligned} m' &= c_2 \cdot \frac{e'(c_1, d_1)}{e'(c_0, d_0)} \\ &= c_2 \cdot \frac{e'((g_1^{\mathrm{ID}} \cdot h)^s, g^r)}{e'(g^s, g_2^a \cdot (g_1^{\mathrm{ID}} \cdot h)^r)} \\ &= m \cdot e'(g_1, g_2)^s \cdot \frac{1}{e'(g^s, g_2^a)} \\ &= m \end{aligned}$$

として平文を復号することができる．

Boneh-Boyen IBE の安全性の根拠となる数論仮定は，DBDH (Decisional Bilinear Diffie-Hellman) 仮定である．

DBDH 仮定

$a, b, c \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ として $(g, g^a, g^b, g^c, Z) \in \mathbb{G}^4 \times \mathbb{G}_T$ が入力された場合に，$Z = e'(g, g)^{abc}$ であるかを判定する問題を DBDH 問題と呼ぶ．そして，いかなる多項式時間攻撃者に対しても DBDH 問題を解くことが困難である場合，その群上において DBDH 仮定が保たれているという．

**定義 5.4.** 攻撃者 $\mathcal{A}$ の *DBDH* 問題に対する優位性を

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DBDH}}(k) := \left| \begin{array}{l} \Pr\left[\mathcal{A}(g, g^a, g^b, g^c, Z) \to 1 \mid a, b, c \xleftarrow{\mathsf{U}} \mathbb{Z}_p; Z := e'(g, \hat{g})^{abc}\right] \\ -\Pr\left[\mathcal{A}(g, g^a, g^b, g^c, Z) \to 1 \mid a, b, c, z \xleftarrow{\mathsf{U}} \mathbb{Z}_p; Z := e'(g, \hat{g})^{z}\right] \end{array} \right|$$

と置いたとき，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DBDH}}(k) \leq \epsilon(k)$ であるならば，その群において *DBDH* 仮定が保たれているという．

**定理 5.4.** *BB04a IBE* は *Standard Model* において *DBDH* 仮定の下で *IND-sID-CPA* 安全な *IBE* である．

*Proof.* BB04a IBE が DBDH 仮定の下で IND-sID-CPA 安全であることを示すために，背理法を用いて BB04a が IND-sID-CPA 安全ではないと仮定した場合に，DBDH 問題が破られることを示す．具体的には，BB04a に対する IND-sID-CPA ゲームにおいて non-negligible な確率で攻撃に成功する攻撃者 $\mathcal{A}$ を仮定した場合に，$\mathcal{A}$ を用いて DBDH 問題を non-negligible な確率で破るアルゴリズム $\mathcal{B}$ を構成する．$\mathcal{B}$ の目標は BB04a のシミュレーションを行うことで，$\mathcal{A}$ の攻撃成功確率から DBDH 問題を破るための優位性を得ることである．$\mathcal{B}$ は図 5 のように動作を行い，BB04a IBE をシミュレートする．

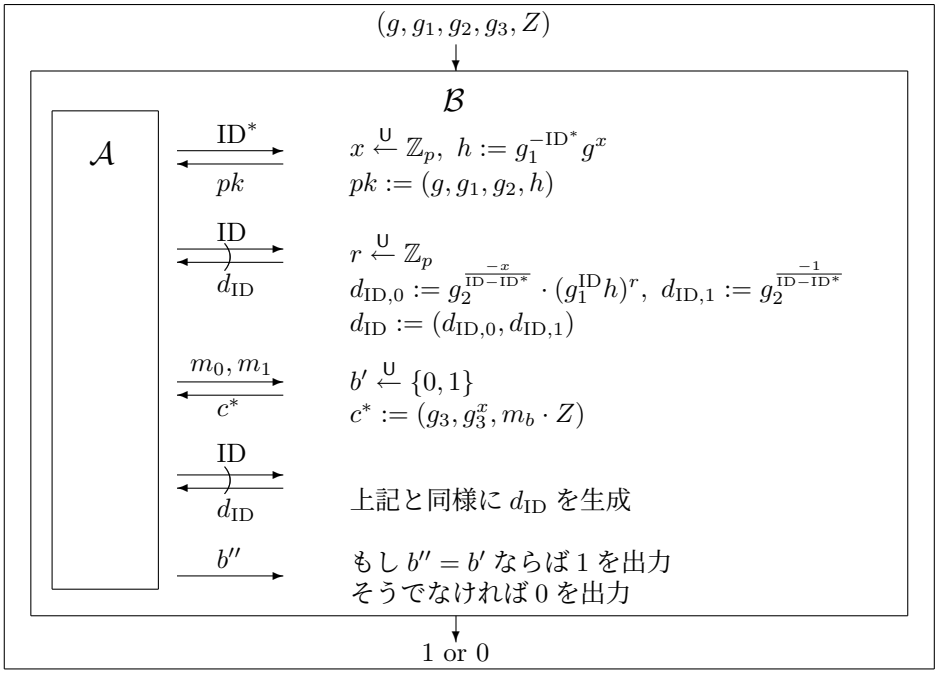


図 5: IND-sID-CPA ゲームの $\mathcal{B}$ によるシミュレート

$\mathcal{B}$ の動作

**Setup:** 最初に，$\mathcal{B}$ は DBDH 問題の入力として $(g, g_1, g_2, g_3, Z) := (g, g^a, g^b, g^c, Z)$ を受け取る．$\mathcal{A}$ を動作させると，$\mathcal{A}$ はターゲットとする $\mathrm{ID}^*$ を送ってくるので，その後で $x \xleftarrow{\cup} \mathbb{Z}_p$ を選び $h := g^{-\mathrm{ID}^*+x}$ として $pk := (g, g_1, g_2, h)$ を $\mathcal{A}$ に返答する．

**Phase 1:** ID に対して KeyGen クエリが行われた場合，$\mathcal{B}$ は $r \xleftarrow{\cup} \mathbb{Z}_p$ を選び，

$$d_{\mathrm{ID},0} := g_2^{\frac{-x}{\mathrm{ID}-\mathrm{ID}^*}} \cdot (g_1^{\mathrm{ID}} h)^r, d_{\mathrm{ID},1} := g_2^{\frac{-1}{\mathrm{ID}-\mathrm{ID}^*}}$$

として $d_{\mathrm{ID}} := (d_{\mathrm{ID},0}, d_{\mathrm{ID},1})$ を返答する．

**Challenge:** 攻撃者 $\mathcal{A}$ から $(m_0, m_1)$ を受け取ると，$b' \xleftarrow{\cup} \{0,1\}$ とし，$c^* := (g_3, g_3^x, m_b \cdot Z)$ を challenge 暗号文として返答する．

**Phase 2:** **Phase 1** と同様の操作を行う．

**Guess:** 攻撃者 $\mathcal{A}$ がビット $b''$ を出力したとする．$\mathcal{B}$ は $b'' = b'$ であれば 1 を出力し，そうでなければ 0 を出力する．

KeyGen クエリにおいて返答している $d_{\mathrm{ID}}$ は，Setup の段階で $h = g^{-\mathrm{ID}^* + x}$ としているので，

$$\begin{aligned}
d_{\mathrm{ID},0} &= g_2^{\frac{-x}{\mathrm{ID}-\mathrm{ID}^*}} \cdot (g_1^{\mathrm{ID}} h)^r \\
&= g_2^{\frac{-x}{\mathrm{ID}-\mathrm{ID}^*}} \cdot (g_1^{\mathrm{ID}} g_1^{-\mathrm{ID}^*} g^x)^r \\
&= \frac{g_1^b}{(g_1^{\mathrm{ID}-\mathrm{ID}^*} g^x)^{\frac{b}{\mathrm{ID}-\mathrm{ID}^*}}} \cdot (g_1^{\mathrm{ID}-\mathrm{ID}^*} g^x)^r \\
&= g_1^b (g_1^{\mathrm{ID}-\mathrm{ID}^*} g^x)^{r - \frac{b}{\mathrm{ID}-\mathrm{ID}^*}} \\
&= g_2^a (g_1^{\mathrm{ID}} h)^{r - \frac{b}{\mathrm{ID}-\mathrm{ID}^*}} \\
d_{\mathrm{ID},1} &= g_2^{\frac{-1}{\mathrm{ID}-\mathrm{ID}^*}} = g^{r - \frac{b}{\mathrm{ID}-\mathrm{ID}^*}}
\end{aligned}$$

となる．これは実際の BB04a IBE における ID に対しての秘密鍵の分布と同じであり，このような構成によって $\mathrm{ID}^*$ 以外に関しては秘密鍵 $d_{\mathrm{ID}^*}$ の生成を行うことができる ($\mathrm{ID}^*$ に関してのみ生成できない)．

もし $\mathcal{B}$ への入力が $Z = e'(g,g)^{abc}$ ならば，このシミュレーションは正しい BB04a における IND-sID-CPA ゲームと等価となる (分布が一致する)．一方，$\mathcal{B}$ への入力が $Z \neq e'(g,g)^{abc}$ である場合，$\mathcal{A}$ に与えられる暗号文 $c_2$ に含まれる平文の情報はこのシミュレーションにおいて受け取っているパラメータとは完全に独立であるため，$\mathcal{A}$ の攻撃成功確率は 1/2 である．よって

$$\begin{aligned}
\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(k) &= \left| \Pr\left[\mathcal{B} \to 1 \mid Z = e'(g,g)^{abc}\right] - \Pr\left[\mathcal{B} \to 1 \mid Z = e'(g,g)^{z}\right] \right| \\
&= \left| 2 \cdot \Pr\left[b'' = b' \mid \text{正しい IND-sID-CPA ゲーム}\right] - 1 \right| \\
&= \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sID\text{-}CPA}}(k)
\end{aligned}$$

となる．今，$\mathcal{A}$ の IND-sID-CPA における攻撃成功確率 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sID\text{-}CPA}}(k)$ は non-negligible であると仮定しているので，$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(k)$ も non-negligible である．よって $\mathcal{B}$ は DBDH 問題を non-negligible な確率で解くことができる． □

### 5.5.2 Boneh-Boyen HIBE(BB04a HIBE)

**HIBE (Hierarchical Identity Based Encryption)** は IBE をより拡張させたものである．HIBE では個別秘密鍵はマスター鍵以外からでも，階層の上位ノードの秘密鍵を持っている状態であれば，下位ノードの個別秘密鍵の生成を行うことができる．5.5.1 節の BB04a IBE を階層化を行った方式 [4] を以下に示す．

**Setup:** $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とする．$g, g_2, h_1, \ldots, h_\ell \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$a \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $g_1 := g^a$ を求める．$pk := (g, g_1, g_2, h_1, \ldots, h_\ell)$，$mk := g_2^a$ とする．

$$pk = (g, g_1, g_2, h_1, \ldots, h_\ell),\ mk = g_2^a$$

KeyGen: ある ID $= (I_1, \ldots, I_j) \in \{0,1\}^j, \{I_i\}_i \in \{0,1\}$ に対しての個別秘密鍵を生成する場合，ID と $mk$ を入力とし，$r_1, \ldots, r_j \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選んで $(d_0, d_1, \ldots, d_j) := (g_2^a \cdot \prod_{k=1}^{j}(g^{I_k} \cdot h_k)^{r_k}, g^{r_1}, \ldots, g^{r_j}) \in \mathbb{G}^{j+1}$ を求め，$d_{\mathrm{ID}} := (d_0, d_1, \ldots, d_j)$ を個別秘密鍵とする．

また，$\mathrm{ID}_{j-1} = (I_1, \ldots, I_{j-1})$ となる ID の個別秘密鍵 $d_{\mathrm{ID}|j-1} = (d'_0, \ldots, d'_{j-1})$ からも $d_{\mathrm{ID}}$ を生成することができる．この場合は，ID と $d_{\mathrm{ID}|j-1}$ を入力とし，$r_j \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選んで $(d_0, d_1, \ldots, d_j) := (d'_0 \cdot (g^{I_j} h_j)^{r_j}, d'_1, \ldots, d'_{j-1}, g^{r_j})$ とする．

Enc: ある ID $= (I_1, \ldots, I_j)$ に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選ぶ．
2. $c_0 := g^s, c_1 := (g_1^{I_1} \cdot h_1)^s, \ldots, c_j := (g_1^{I_j} \cdot h_j)^s, c_{j+1} := e'(g_1, g_2)^s \cdot m$ とする．
3. $C := (c_0, c_1, \ldots, c_j, c_{j+1})$ を暗号文として出力する．

Dec: $d_{\mathrm{ID}}$ を用いて暗号文 $C = (c_0, c_1, \ldots, c_j, c_{j+1})$ を復号する場合，

$$m' = c_{j+1} \cdot \prod_{k=1}^{j} e'(c_k, d_k) \cdot e'(c_0, d_0)^{-1}$$

を出力する．

**定理 5.5.** *Boneh-Boyen HIBE(BB04a HIBE)* は *Standard Model* において *DBDH* 仮定の下で *IND-sID-CPA* 安全な *HIBE* である．

### 5.5.3 Boneh-Boyen IBE(BB04b IBE)

IBE の三つの分類のうち，Exponent Inversion IBE に分類される Boneh-Boyen IBE (BB04b IBE) の方式 [3] を以下に示す．

Setup: $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とする．$g \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$x, y \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $X := g^x, Y := g^y$ を求める．$pk := (g, X, Y)$，$mk := (x, y)$ とする．

$$pk = (g, X, Y),\ mk = (x, y)$$

KeyGen: ある ID $\in \mathbb{Z}_p$ に対しての個別秘密鍵を生成する場合，ID と $mk$ を入力とし，$r \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選んで $(d_0, d_1) := (r, g^{\frac{1}{\mathrm{ID}+x+yr}}) \in \mathbb{Z}_p \times \mathbb{G}$ を求め，$d_{\mathrm{ID}} := (d_0, d_1)$ を出力する．

Enc: ある ID に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選ぶ.
2. $c_0 := g^{s\cdot \mathrm{ID}} X^s, c_1 := Y^s, c_2 := e'(g,g)^s \cdot m$ とする.
3. $C := (c_0, c_1, c_2)$ を暗号文として出力する.

**Dec:** 暗号文 $C = (c_0, c_1, c_2)$ および $d_{\mathrm{ID}}$ を入力とし，$m' = c_2 \cdot e'(c_0 c_1^{d_0}, d_1)^{-1}$ を出力する.

BB04b IBE において，暗号文 $(c_0, c_1, c_2)$ が正しく生成されているならば,

$$\begin{aligned} m' &= c_2 \cdot e'(c_0 c_1^r, g)^{-1} \\ &= c_2 \cdot e'(g^{s\cdot \mathrm{ID}} X^s \cdot (Y^s)^r, g^{\frac{1}{\mathrm{ID}+x+yr}})^{-1} \\ &= c_2 \cdot e'(g^{s(\mathrm{ID}+x+yr)}, g^{\frac{1}{\mathrm{ID}+x+yr}})^{-1} \\ &= m \cdot e'(g,g)^s \cdot e'(g,g)^{-s} \\ &= m \end{aligned}$$

として平文を復号することができる.

BB04b IBE の安全性の根拠となる数論仮定は，$q$-DBDHI(Decisional Bilinear Diffie-Hellman Inversion) 仮定である.

$q$-DBDHI 仮定

$x \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ として $(g, g^x, g^{x^2}, \ldots, g^{x^q}, Z) \in \mathbb{G}^4 \times \mathbb{G}_T$ が入力された場合に，$Z = e'(g,g)^{1/x}$ であるかを判定する問題を $q$-DBDHI 問題と呼ぶ．そして，いかなる多項式時間攻撃者に対しても $q$-DBDHI 問題を解くことが困難である場合，その群上において $q$-DBDHI 仮定が保たれているという.

**定義 5.5.** 攻撃者 $\mathcal{A}$ の *$q$-DBDHI* 問題に対する優位性を

$$\mathsf{Adv}_{\mathcal{A}}^{q\text{-}\mathsf{DBDHI}}(k) := \left| \begin{array}{l} \Pr\left[\mathcal{A}(g, g^x, \ldots, g^{x^q}, Z) \to 1 \mid x \xleftarrow{\mathsf{U}} \mathbb{Z}_p;\ Z := e'(g,g)^{1/x}\right] \\ -\Pr\left[\mathcal{A}(g, g^x, , \ldots, g^{x^q}, Z) \to 1 \mid x, z \xleftarrow{\mathsf{U}} \mathbb{Z}_p, Z := e'(g,g)^z\right] \end{array} \right|$$

と置いたとき，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}_{\mathcal{A}}^{q\text{-}\mathsf{DBDHI}}(k) \leq \epsilon(k)$ である場合，その群において *$q$-DBDHI* 仮定が保たれているという.

**定理 5.6.** *BB04b IBE* は *Standard Model* において *$q$-DBDHI* 仮定の下で *IND-sID-CPA* 安全である.

### 5.5.4 Waters IBE

Waters IBE [19] は Commutative Blinding IBE に分類される IBE で，IBE の中で初めて IND-ID-CPA 安全であることが証明された IBE である.

**Setup:** $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とする．$g, g_2, u', u_1, \ldots, u_k \xleftarrow{\cup} \mathbb{G}$ を選び，$a \xleftarrow{\cup} \mathbb{Z}_p$ から $g_1 := g^a$ を求める．$pk := (g, g_1, g_2, u', u_1, \ldots, u_k)$，$mk := g_2^a$ とする．

$$pk = (g, g_1, g_2, u', u_1, \ldots, u_k),\ mk = g_2^a$$

**KeyGen:** ある ID $= (v_1, \ldots, v_n),\ v_i \in \{0, 1\}$ に対しての個別秘密鍵を生成する場合，ID と $mk$ を入力とし，$r \xleftarrow{\cup} \mathbb{Z}_p$ を選んで $(d_0, d_1) := (g_2^a (u' \prod_{i=1}^k u_i^{v_i})^r, g^r) \in \mathbb{G}^2$ を求め，$d_{\mathrm{ID}} := (d_0, d_1)$ を個別秘密鍵とする．

**Enc:** ある ID に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s \xleftarrow{\cup} \mathbb{Z}_p$ を選ぶ．
2. $c_0 := g^s, c_1 := (u' \prod_{i=1}^k u_i^{v_i})^s, c_2 := e'(g_1, g_2)^s \cdot m$ とする．
3. $C = (c_0, c_1, c_2)$ を暗号文として出力する．

**Dec:** 暗号文 $C = (c_0, c_1, c_2)$ および $d_{\mathrm{ID}}$ を入力とし，$m' = c_2 \cdot e'(c_1, d_1) \cdot e'(c_0, d_0)^{-1}$ を出力する．

Waters IBE において，暗号文 $(c_0, c_1, c_2)$ が正しく生成されているならば，

$$\begin{aligned} m' &= c_2 \cdot \frac{e'(c_1, d_1)}{e'(c_0, d_0)} \\ &= c_2 \cdot \frac{e'((u' \prod_{i=1}^k u_i^{v_i})^s, g^r)}{e'(g^s, g_2^a \cdot (u' \prod_{i=1}^k u_i^{v_i})^r)} \\ &= m \cdot e'(g_1, g_2)^s \cdot \frac{1}{e'(g^s, g_2^a)} \\ &= m \end{aligned}$$

として平文を復号することができる．

BB04a IBE との主な違いは，ID がビット列展開されており，システム公開鍵を多基底にすることで ID を群上の値に埋め込んでいる点である．

**定理 5.7.** *Waters IBE は Standard Model において DBDH 仮定の下で IND-ID-CPA 安全である．*

これまでの Standard Model における方式が selective ID 型の証明であったのに対して，Waters が adaptive ID 型で証明したときの戦略の違いについて解説しておこう．

これまでの selective ID 型の証明では，IBE に対する攻撃者を利用して数論仮定を破るアルゴリズムは，あらかじめ攻撃者が指定した ID に対してのみ個別秘密鍵を生成できないように Setup における公開パラメータを生成していた．しかし，adaptive ID 型の証明では，challenge 暗号文のターゲットとなる ID$^*$ の情報は **Challenge** に

おいて初めて得られるため，Selective ID 型の証明方針のように安全性証明を行うことは難しい．

Waters は上記の問題を回避するため,「ある一定の範囲に対する個別秘密鍵は生成できない」構成を用いて証明を行った．この場合，攻撃者が KeyGen オラクルに聞いてきた ID に関してはすべて個別秘密鍵が生成可能な範囲に含まれており，かつ challenge 暗号文に対しての ID に関しては個別秘密鍵が生成不可能な領域に含まれていれば，攻撃者をうまく利用することができる．

例えば，個別秘密鍵のうち $\frac{1}{n^3}$ 程度が生成できない場合を考える．このとき，KeyGen オラクルへの問い合わせが $n^2$ 回とした場合，すべての KeyGen オラクルに正しく返答できる確率は $(1-\frac{1}{n^3})^{n^2} \simeq 1-\frac{1}{n}$ である．また，challenge 暗号文に対しての ID に関しては個別秘密鍵が生成不可能な領域に含まれる確率は $\frac{1}{n^3}$ であるので，$\frac{1}{n^3}(1-\frac{1}{n})$ の確率で正しくシミュレートを行うことができる．

*Proof.* (sketch) Waters IBE に対して IND-ID-CPA で攻撃に成功する攻撃者 $\mathcal{A}$ を仮定した場合に，$\mathcal{A}$ を用いて DBDH 問題を破るアルゴリズム $\mathcal{B}$ を構成する．

$\mathcal{B}$ の動作

**Setup:** 最初に，$\mathcal{B}$ は DBDH 問題の入力として $(g, g_1, g_2, g_3, Z) := (g, g^a, g^b, g^c, Z)$ を受け取る．攻撃者 $\mathcal{A}$ が KeyGen オラクルを利用できる上限回数を $q_{\mathsf{KG}}$ とする．このとき，$\mathcal{B}$ は以下の動作を行う．

1. $m := 4q_{\mathsf{KG}}$ とする．
2. $P > nm$ となる値を選ぶ ($n$: ID ベクトルの長さ).
3. $k \xleftarrow{\mathsf{U}} \mathbb{Z}_n$ を選ぶ.
4. $x', x_i \xleftarrow{\mathsf{U}} \mathbb{Z}_m$ $(i = 1, \ldots, n)$ を選ぶ.
5. $y', y_i \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ $(i = 1, \ldots, n)$ を選ぶ.
6. $(u', u_1, \ldots, u_n) := (g_2^{p-mk+x'} g^{y'}, g_2^{x_1} g^{y_1}, \ldots, g_2^{x_n} g^{y_n})$ とする．
7. $pk := (g, g_1, g_2, u', u_1, \ldots, u_n)$ をシステム公開鍵として $\mathcal{A}$ に入力する．

また，$\mathrm{ID} = (v_1, \ldots, v_n) \in \{0,1\}^n$ に対し

$$F(\mathrm{ID}) := (p - mk) + x' + \sum_{i=1}^{n} x_i v_i$$

$$J(\mathrm{ID}) := y' + \sum_{i=1}^{n} y_i v_i$$

$$K(\mathrm{ID}) := \begin{cases} 0 & \text{if } x' + \sum_{i=1}^{k} x_i v_i \equiv 0 \pmod{n} \\ 1 & \text{otherwise} \end{cases}$$

という関数を定義する．

**Phase 1:** $\mathrm{ID} = (v_1, \ldots, v_n)$ に対して KeyGen クエリが行われた場合，まず $K(\mathrm{ID}) = 0$ あるかの検証を行い，もし $K(\mathrm{ID}) = 0$ であれば abort する．そうでなければ，$r \xleftarrow{\cup} \mathbb{Z}_p$ から

$$d_0 := g_1^{\frac{J(\mathrm{ID})}{F(\mathrm{ID})}} (u' \prod_{i=1}^{n} u_i^{v_i})^r,$$
$$d_1 := g_1^{\frac{-1}{F(\mathrm{ID})}} g^r$$

を計算し，$d_{\mathrm{ID}} := (d_0, d_1)$ を返答する．

**Challenge:** 攻撃者 $\mathcal{A}$ から $(\mathrm{ID}^*, m_0, m_1)$ が入力されたとき，$F(\mathrm{ID}^*) \not\equiv 0 \pmod p$ であれば abort する．そうでなければ，$b \xleftarrow{\cup} \{0,1\}$ として $C^* := (g_3, g_3^{J(\mathrm{ID}^*)}, Z \cdot m_b)$ を返答する．

**Phase 2: Phase 1** と同様の操作を行う．

**Guess:** 攻撃者 $\mathcal{A}$ がビット $b'$ を出力したとする．$\mathcal{B}$ は $b' = b$ であれば 1 を出力し，そうでなければ 0 を出力する．

アルゴリズム $\mathcal{B}$ が個別秘密鍵を生成できない範囲は $F(\mathrm{ID}) \equiv 0 \pmod p$ のときであるので，先ほど議論したようにすべての KeyGen クエリにおいて $F(\mathrm{ID}) \not\equiv 0 \pmod p$ であり，Challenge 暗号文の ID に対して $F(\mathrm{ID}^*) \equiv 0 \pmod p$ であればシミュレーションをうまく動作させることができる．また，KeyGen クエリの返答は

$$\begin{aligned}
d_0 &= g_1^{\frac{J(\mathrm{ID})}{F(\mathrm{ID})}} (u' \prod_{i=1}^{n} u_i^{v_i})^r \\
&= g_1^{\frac{J(\mathrm{ID})}{F(\mathrm{ID})}} (g_2^{p-mk+x'} g^{y'} \prod_{i=1} (g_2^{x_i} g^{y_i})^{v_i})^r \\
&= g_1^{\frac{J(\mathrm{ID})}{F(\mathrm{ID})}} (g_2^{p-mk+x'+\sum_{i=1}^{n} x_i v_i} \cdot g^{y'+\sum_{i=1}^{n} y_i v_i})^r \\
&= g_1^{\frac{J(\mathrm{ID})}{F(\mathrm{ID})}} (g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})})^r \\
&= g_2^a (g_2^{F(\mathrm{ID}) g^{J(\mathrm{ID})}})^{-\frac{a}{F(\mathrm{ID})}} (g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})})^r \\
&= g_2^a (u' \prod_{i=1}^{n} u_i^{v_i})^{r - \frac{a}{F(\mathrm{ID})}} \\
d_1 &= g_1^{\frac{1}{F(\mathrm{ID})}} g^r = g^{r - \frac{a}{F(\mathrm{ID})}}
\end{aligned}$$

となるため，正しい個別秘密鍵の分布と一致する．

もし $\mathcal{B}$ への DBDH 問題の入力において $Z = e'(g,g)^{abc}$ であり $\mathcal{B}$ がシミュレーションにおいて abort をしなければ，シミュレーションは正しい Waters IBE の IND-ID-CPA ゲームと等価になる．一方，$Z = e'(g,g)^{z}$ が入力されているならば，攻撃者 $\mathcal{A}$ は challenge 暗号文から平文の情報は情報理論的に得られないため，この場合の攻撃者の成功確率は $\frac{1}{2}$ である．よってシミュレーションにおいて abort しない確率を $\Pr[\overline{\mathsf{abort}}]$ とおくと

$$\begin{aligned}
\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(k) &= \left|\Pr\left[Z = e'(g,g)^{abc} : \mathcal{B} \to 1\right] - \Pr\left[Z = e'(g,g)^{z} : \mathcal{B} \to 1\right]\right| \cdot \Pr[\overline{\mathsf{abort}}] \\
&= \left|\Pr\left[\text{正しい IND-sID-CPA ゲーム} : b'' = b'\right] - \frac{1}{2}\right| \cdot \Pr[\overline{\mathsf{abort}}] \\
&= \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}ID\text{-}CPA}}(k) \cdot \Pr[\overline{\mathsf{abort}}]
\end{aligned}$$

となる．また，シミュレーション時に abort する確率に関しては，Waters は $\varepsilon := \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}ID\text{-}CPA}}(k)$ とおくと $O(\varepsilon^{-2} \cdot \ln(\varepsilon^{-1})\lambda^{-1}\ln(\lambda^{-1}))$ $(\lambda = \frac{1}{8(n+1)q})$ の計算時間を利用すると $\Pr[\overline{\mathsf{abort}}]$ は $\frac{1}{32(n+1)q}$ で抑えられることを示しているため (詳細は [19] 参照)，$\mathcal{A}$ の IND-ID-CPA における攻撃成功確率 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}ID\text{-}CPA}}(k)$ が non-negligible であるならば，$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(k)$ も non-negligible となる．よって $\mathcal{B}$ は DBDH 問題を non-negligible な確率で解くことができる． □

### 5.5.5 Gentry IBE

Gentry IBE [12] は Exponent Inversion IBE に分類されるもので，Waters IBE とは異なる方針で IND-ID-CPA 安全であることが証明された IBE である．また，Waters IBE よりも帰着効率がよい安全性証明が行われている．

**Setup:** $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とする．$g, h \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$\alpha \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $g_1 := g^{\alpha}$ を求める．$pk := (g, g_1, h)$，$mk := \alpha$ とする．

$$pk = (g, g_1, h),\ mk = \alpha$$

**KeyGen:** ある $\mathrm{ID} \in \mathbb{Z}_p$ に対しての個別秘密鍵を生成する場合，ID と $mk$ を入力とし，$r_{\mathrm{ID}} \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選んで $h_{\mathrm{ID}} := (hg^{-r_{\mathrm{ID}}})^{\frac{1}{\alpha - \mathrm{ID}}} \in \mathbb{G}$ を求め，$d_{\mathrm{ID}} := (r_{\mathrm{ID}}, h_{\mathrm{ID}})$ を個別秘密鍵とする．

**Enc:** ある $\mathrm{ID} \in \mathbb{Z}_p$ に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選ぶ．
2. $c_0 := g_1^{s} \cdot g^{-s \cdot \mathrm{ID}}, c_1 := e'(g,g)^{s}, c_2 := e'(g,h)^{-s} \cdot m$ とする．
3. $C := (c_0, c_1, c_2)$ を暗号文として出力する．

Dec: 暗号文 $C = (c_0, c_1, c_2)$ および $d_{\mathrm{ID}}$ を入力とし，$m' = c_2 \cdot e'(c_0, h_{\mathrm{ID}}) \cdot c_1^{r_{\mathrm{ID}}}$ を出力する．

Gentry IBE において，暗号文 $(c_0, c_1, c_2)$ が正しく生成されているならば，

$$\begin{aligned} m' &= c_2 \cdot e'(c_0, h_{\mathrm{ID}}) \cdot c_1^{r_{\mathrm{ID}}} \\ &= c_2 \cdot e'(g_1^s \cdot g^{-s \cdot \mathrm{ID}}, (hg^{-r_{\mathrm{ID}}})^{\frac{1}{\alpha - \mathrm{ID}}}) \cdot c_1^{r_{\mathrm{ID}}} \\ &= c_2 \cdot e'(g, (hg^{-r_{\mathrm{ID}}}))^s \cdot c_1^{r_{\mathrm{ID}}} \\ &= m \cdot e'(g,h)^{-s} \cdot e'(g, (hg^{-r_{\mathrm{ID}}}))^s \cdot e'(g,g)^{s \cdot r_{\mathrm{ID}}} \\ &= m \end{aligned}$$

として平文を復号することができる．

Gentry IBE の安全性の根拠となる数論仮定は，trancated decisional $q$-ABDHE(Augmented Bilinear Diffie-Hellman Exponent) 仮定である．

trancated decisional $q$-ABDHE 仮定

$\alpha \overset{\mathsf{U}}{\leftarrow} \mathbb{Z}_p$ として $(g', (g')^{\alpha^{q+2}}, g, g^a, \ldots, g^{a^q}, Z) \in \mathbb{G}^{q+3} \times \mathbb{G}_T$ が入力された場合に，$Z = e'(g, g')^{a^{q+1}}$ であるかを判定する問題を trancated decisional $q$-ABDHE 問題と呼ぶ．そして，いかなる多項式時間攻撃者に対しても trancated decisional $q$-ABDHE 問題を解くことが困難である場合，その群上において trancated decisional $q$-ABDHE 仮定が保たれているという．

**定義 5.6.** 攻撃者 $\mathcal{A}$ の *trancated decisional q-ABDHE* 問題に対する優位性を

$$\mathsf{Adv}_{\mathcal{A}}^{q\text{-}\mathsf{ABDHE}}(k) := \left| \begin{array}{l} \Pr\left[\mathcal{A}(g', (g')^{\alpha^{q+2}}, g, g^a, \ldots, g^{a^q}, Z) \to 1 \mid \alpha \overset{\mathsf{U}}{\leftarrow} \mathbb{Z}_p; Z := e'(g, g')^{\alpha^{q+1}}\right] \\ -\Pr\left[\mathcal{A}(g', (g')^{\alpha^{q+2}}, g, g^a, \ldots, g^{a^q}, Z) \to 1 \mid \alpha, z \overset{\mathsf{U}}{\leftarrow} \mathbb{Z}_p; Z := e'(g, g')^{z}\right] \end{array} \right|$$

と置いたとき，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}_{\mathcal{A}}^{q\text{-}\mathsf{ABDHE}}(k) \leq \epsilon(k)$ である場合，その群において *trancated decisional q-ABDHE* 仮定が保たれているという．

**定理 5.8.** *Gentry IBE* は *Standard Model* において *trancated decisional q-ABDHE* 仮定の下で *IND-ID-CPA* である．

定理を証明するために，基本的な証明のアイデアについて説明を行う．ランダムな $q$ 次多項式 $f(x) := a_0 + a_1 x + \cdots a_q x^q \in \mathbb{F}_p[x]$ を考える．$\alpha \overset{\mathsf{U}}{\leftarrow} \mathbb{F}_p$ から，$h := g^{f(\alpha)}$，$r_{\mathrm{ID}} := f(\mathrm{ID})$ とする．このとき，$h_{\mathrm{ID}} := (hg^{-r_{\mathrm{ID}}})^{\frac{1}{\alpha - \mathrm{ID}}}$ とおくと

$$h_{\mathrm{ID}} = (hg^{-r_{\mathrm{ID}}})^{\frac{1}{\alpha - \mathrm{ID}}} = g^{\frac{f(\alpha) - f(\mathrm{ID})}{\alpha - \mathrm{ID}}}$$

であり，これは $g$ の指数に関して，$q-1$ 次の $\alpha$ に関する多項式で表される．よって，$(g, g^\alpha, \ldots, g^{\alpha^q})$ という入力を用いることで $h_{\mathrm{ID}}$ を求めることができる．つまり，$\alpha$ の値を知らないとしてもすべての ID に対する個別秘密鍵の値をシミュレートできる．

そのため，これまでの証明では，**Challenge** における ID の個別秘密鍵は計算ができないようにシミュレートを構成していたが，今回はすべての ID に対して個別秘密鍵がシミュレートできるように構成を行う．

*Proof.* Gentry IBE に対して IND-ID-CPA で攻撃に成功する攻撃者 $\mathcal{A}$ を仮定した場合に，$\mathcal{A}$ を用いて trancated decisional $q$-ABDHE 仮定を破るアルゴリズム $\mathcal{B}$ を構成する．

$\mathcal{B}$ の動作

**Setup:** $\mathcal{B}$ は trancated decisional $q$-ABDHE 問題の入力として $(g', g'_1, g, g_1, \ldots, g_q, Z) := (g', \mathrm{x}\ (g')^{\alpha^{q+2}}, g, g^a, \ldots, g^{a^q}, Z)$ を受け取る．$\mathcal{B}$ は $q$ 次多項式 $f(x) \in \mathbb{F}_p[x]$ を選び，$h := g^{f(\alpha)}$ とする ($(g, g_1, \ldots, g_q)$ から求める)．$pk := (g, g_1, h)$ として攻撃者 $\mathcal{A}$ に $pk$ を入力する．

**Phase 1:** ID に対して KeyGen クエリが行われた場合，$r_{\mathrm{ID}} := f(\mathrm{ID}), h_{\mathrm{ID}} := g^{\frac{f(\alpha)-f(\mathrm{ID})}{\alpha-\mathrm{ID}}}$ を求める．$d_{\mathrm{ID}} := (r_{\mathrm{ID}}, h_{\mathrm{ID}})$ として $d_{\mathrm{ID}}$ を $\mathcal{A}$ に返答する．

**Challenge:** $\mathcal{A}$ から $m_0, m_1, \mathrm{ID}^*$ を受け取り，$\mathrm{ID}^*$ に対しての個別秘密鍵 $r_{\mathrm{ID}^*} := f(\mathrm{ID}^*), h_{\mathrm{ID}^*} := g^{\frac{f(\alpha)-f(\mathrm{ID}^*)}{\alpha-\mathrm{ID}^*}}$ を求める．このとき，

$$f_2(x) := x^{q+2}$$

$$F_{2,\mathrm{ID}^*}(x) := \frac{f_2(x) - f_2(\mathrm{ID}^*)}{x - \mathrm{ID}^*} : q+1 \text{ 次多項式}$$

と定義する．$F_{2,\mathrm{ID}^*,i}(x)$ を $F_{2,\mathrm{ID}^*}(x)$ における $x^i$ の係数とおくと，

$$F_{2,\mathrm{ID}^*}(x) = F_{2,\mathrm{ID}^*,0} + F_{2,\mathrm{ID}^*,1}x + \cdots + F_{2,\mathrm{ID}^*,q}x^q + x^{q+1}$$

となる．この関数を用い，$b \xleftarrow{\mathsf{U}} \{0,1\}$ として

$$c_0^* := (g')^{f_2(\alpha)-f_2(\mathrm{ID}^*)}$$

$$c_1^* := Z \cdot e'(g', \prod_{i=0}^{q} g^{F_{2,\mathrm{ID}^*,i} \cdot \alpha^i})$$

$$c_2^* := e'(c_0^*, h_{\mathrm{ID}^*})^{-1} \cdot (c_1^*)^{-r_{\mathrm{ID}^*}} \cdot m_b$$

を求め，$C^* := (c_0^*, c_1^*, c_2^*)$ を $\mathcal{A}$ に返答する．

**Phase 2: Phase 1** と同等の操作を行って ID に対しての個別秘密鍵 $d_{\mathrm{ID}}$ を $\mathcal{A}$ に返答する．

**Guess:** 攻撃者 $\mathcal{A}$ がビット $b'$ を出力したならば，$b' = b$ であれば 1 を出力し，そうでなければ 0 を出力する．

Challenge 暗号文に対して，$t = \log_g g' \cdot F_{2,\mathrm{ID}^*}(\alpha)$ とおくと，

$$\begin{aligned} c_0^* = (g')^{f_2(\alpha) - f_2(\mathrm{ID}^*)} &= (g')^{\alpha^{q+2} - (ID^*)^{q+2}} \\ &= (g')^{F_{2,\mathrm{ID}^*}(\alpha)(\alpha - \mathrm{ID}^*)} \\ &= g^{t(\alpha - \mathrm{ID}^*)} \end{aligned}$$

となる．また，$\mathcal{B}$ への入力 $Z$ が $Z = e'(g, g')^{a^{q+1}}$ であれば，

$$\begin{aligned} c_1^* = Z \cdot e'(g', \prod_{i=0}^{q} g^{F_{2,\mathrm{ID}^*,i} \cdot \alpha^i}) = e'(g, g')^{a^{q+1}} \cdot e(g, g')^{\sum_{i=0}^{1} F_{2,\mathrm{ID}^*,i} \cdot \alpha^i} \\ = e'(g, g')^{F_{2,\mathrm{ID}^*}(\alpha)} \\ = e'(g, g)^t \end{aligned}$$

となる．$c_2^*$ は $m_b = c_2^* \cdot e'(c_0^*, h_{\mathrm{ID}^*}) \cdot (c_1^*)^{r_{\mathrm{ID}^*}}$ を満たすように生成しているので，この challenge 暗号文の分布は正しい IND-ID-CPA ゲームにおける challenge 暗号文と一致する．一方，$Z = e'(g, g')^z$ であれば，$\mathcal{A}$ が challenge 暗号文から平文の情報を得ることは情報理論的に不可能であるため，

$$\begin{aligned} \mathsf{Adv}_{\mathcal{B}}^{q\text{-}\mathsf{ABDHE}}(k) &= \left| \Pr\left[\mathcal{B} \to 1 \mid Z = e'(g, g')^{q^{a+1}}\right] - \Pr\left[\mathcal{B} \to 1 \mid Z = e'(g, g)^z\right] \right| \\ &= \left| 2 \cdot \Pr\left[b'' = b' \mid \text{正しい IND-sID-CPA ゲーム}\right] - 1 \right| \\ &= \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}ID\text{-}CPA}}(k) \end{aligned}$$

となる．今，$\mathcal{A}$ の IND-ID-CPA における攻撃成功確率 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}ID\text{-}CPA}}(k)$ は non-negligible であると仮定しているので，$\mathsf{Adv}_{\mathcal{B}}^{q\text{-}\mathsf{ABDHE}}(k)$ も non-negligible である．よって $\mathcal{B}$ は truncated decisional $q$-ABDHE 問題を non-negligible な確率で解くことができる． □

## 5.6 IBE の応用

### 5.6.1 Canetti-Halevi-Katz 変換

5.5.1 節および 5.5.2 節で説明を行った暗号方式はどちらも IND-sID-CPA 安全という弱い安全性での証明が行われているが，2004 年に Canetti, Halevi, Katz は IND-sID-CPA 安全な IBE を one-time sEUF-CMA 安全な署名と組み合わせることにより，IND-CCA2 安全な PKE へと変換する手法 (CHK 変換) を 提案した [9]．これを応用すると，IND-sID-CPA 安全な $\ell$ 階層の HIBE ($\ell$-HIBE) から IND-sID-CCA2 安全な $\ell - 1$ 階層の HIBE を構成することができる．ここでは簡単のため，IND-sID-CPA 安全な IBE を IND-CCA2 安全な PKE に変換する場合の解説を行う．

IND-sID-CPA 安全な IBE のアルゴリズムを $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}', \mathsf{Dec}')$，one-time sEUF-CMA 安全な署名アルゴリズムを $(\mathsf{G_{sig}}, \mathsf{S_{sig}}, \mathsf{V_{sig}})$ として，これらのアルゴリズ

ムを用いて IND-CCA2 安全な PKE のアルゴリズム $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を以下のように構成する．

$\underline{\mathsf{Gen}(1^k)}$

1. $(pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k)$ を動作させる．
2. $pk_{\mathsf{PKE}} := pk$，$sk_{\mathsf{PKE}} := mk$ とする．
3. $(pk_{\mathsf{PKE}}, sk_{\mathsf{PKE}})$ を出力する．

$\underline{\mathsf{Enc}(pk_{\mathrm{PKE}}, m)}$

1. $(vk, sk) \xleftarrow{\mathsf{R}} \mathsf{G}_{\mathsf{sig}}(1^k)$ を動作させる．
2. $c_1 \xleftarrow{\mathsf{R}} \mathsf{Enc}'(pk_{\mathsf{PKE}}, vk, m)$ を求める．このとき，$vk$ を ID とみなして暗号化を行う．
3. $\sigma \xleftarrow{\mathsf{R}} \mathsf{S}_{\mathsf{sig}}(vk, sk, c_1)$ を生成する．
4. $C := (vk, c_1, \sigma)$ とする．
5. $C$ を暗号文として出力する．

$\underline{\mathsf{Dec}(sk_{\mathsf{PKE}}, C)}$

1. $\mathsf{V}_{\mathsf{sig}}(vk, \sigma, c_1) = 0$ であれば $\perp$ を出力する．
2. そうでなければ，$d_{vk} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(sk_{\mathsf{PKE}}, vk)$ を求める．
3. $m' := \mathsf{Dec}'(pk, d_{vk}, c_1)$ を出力する．

**定理 5.9.** *IBE が IND-sID-CPA 安全であり，署名が one-time sEUF-CMA 安全であるならば，上記の構成による PKE は IND-CCA2 安全である．*

*Proof.* 定理 5.9 を証明するため，PKE の IND-CCA2 安全性を non-negligible な確率で破る攻撃者 $\mathcal{A}$ を仮定した場合に，$\mathcal{A}$ を内部で利用することにより IBE の IND-sID-CPA 安全性を破る攻撃者 $\mathcal{A}'$ を構成する．このとき，

Forge: challenge 暗号文 $(vk^*, c^*, \sigma^*)$ を受け取ったとき，署名検証に通る暗号文 $(vk^*, c, \sigma)$ を復号オラクルに聞くイベント $((c, \sigma) \neq (c^*, \sigma^*))$

としたとき，署名の one-time sEUF-CMA 安全性から $\Pr[\mathsf{Forge}] \leq \epsilon(k)$ であることを前提として証明を行う．図 5 に PKE に対する IND-CCA2 攻撃者 $\mathcal{A}$ を用いた IBE に対する IND-sID-CPA 攻撃者 $\mathcal{A}'$ の構成を示す．

$\underline{\mathcal{A}' \text{ の動作}}$

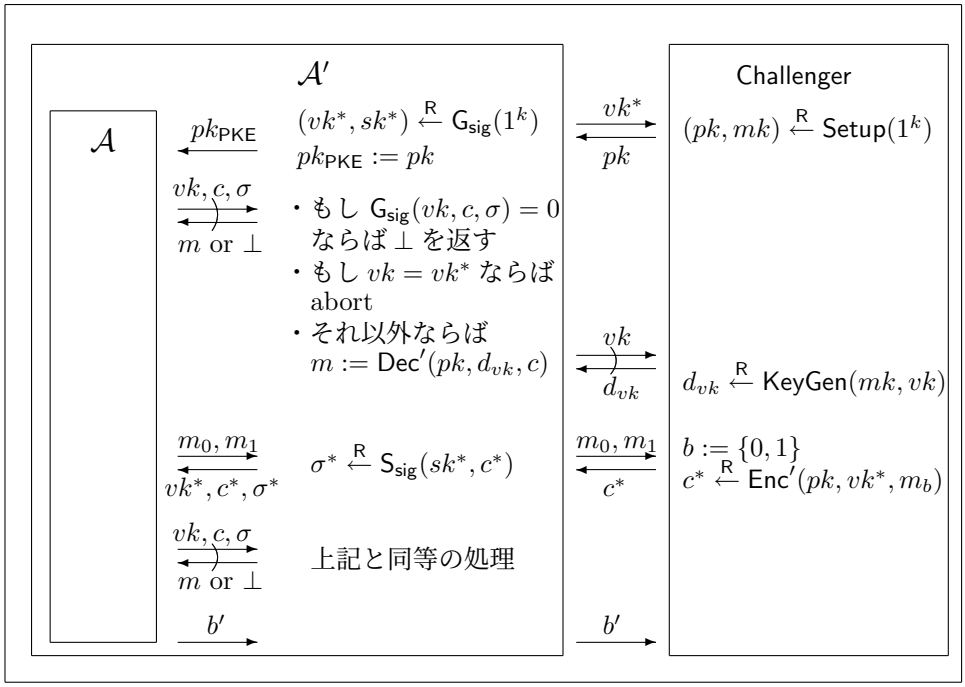


図 6: IND-sID-CPA 攻撃者 $\mathcal{A}'$ の構成

まず，署名の鍵生成アルゴリズムを用いて $(vk^*, sk^*) \xleftarrow{\mathsf{R}} \mathsf{G_{sig}}(1^k)$ を生成し，$vk^*$ をターゲット ID として Challenger に渡す．Challenger からシステム公開鍵 $pk$ を受け取ると，PKE に対しての公開鍵を $pk_{\mathsf{PKE}} := pk$ として $\mathcal{A}$ に入力する．$\mathcal{A}$ から復号オラクルとして $(vk, c, \sigma)$ が入力された場合は，

- 署名検証に失敗するならば (つまり $\mathsf{V_{sig}}(vk, c, \sigma) = 0$)，$\perp$ を出力する．
- 署名検証に通り，$vk = vk^*$ であれば abort する．
- そうでなければ，Challenger に KeyGen クエリを行い個別秘密鍵 $d_{vk}$ を受け取り，暗号文 $c$ を $d_{vk}$ を用いて復号を行い，その復号結果 $m := \mathsf{Dec}'(d_{vk}, c)$ を返す．

まず，署名検証に失敗した場合は，実際の動作と同じように $\perp$ を返せばよい．次に，$vk = vk^*$ となる場合について考える．この場合は，$vk^*$ をターゲットとしているため KeyGen クエリを行うことができない．しかし，署名検証に通る暗号文 $(vk^*, c, \sigma)$ を $\mathcal{A}$ が聞いてくる確率は $\Pr[\mathsf{Forge}]$ と等価であり，この確率は署名の one-time sEUF-CMA 安全性から negligible である．その他の場合は，KeyGen クエリから個別秘密鍵を受け取り IBE における暗号文 $c$ を $d_{vk}$ を用いて復号することができる．

Challenge 暗号文については，$\mathcal{A}$ からメッセージを受け取るとそのメッセージを Challenger に渡し，IBE における challenge 暗号文 $c^*$ を受け取る．PKE における

Challenge 暗号文には $c^*$ 以外に $vk^*$ および $c^*$ に対する署名 $\sigma^*$ が必要であるが，$\mathcal{A}'$ は署名生成のための署名鍵 $sk^*$ を持っているため，$\sigma^* := \mathsf{S_{sig}}(sk^*, c^*)$ を求めることができる．

最終的に，上記の構成における攻撃者 $\mathcal{A}'$ の IND-sID-CPA ゲームにおける成功確率は，

$$\begin{aligned}\mathsf{Adv}^{\mathsf{IND\text{-}sID\text{-}CPA}}_{\mathcal{A}'}(k) &= \left|\Pr\left[\mathcal{A}' \to 1 \mid b = 1\right] - \Pr\left[\mathcal{A}' \to 1 \mid b = 0\right]\right| - \Pr[\mathsf{Forge}] \\ &= \left|\Pr\left[\mathcal{A} \to 1 \mid b = 1\right] - \Pr\left[\mathcal{A} \to 1 \mid b = 0\right]\right| - \Pr[\mathsf{Forge}] \\ &= \mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\mathcal{A}}(k) - \Pr[\mathsf{Forge}]\end{aligned}$$

となる．よって $\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\mathcal{A}}(k)$ が non-negligible であるならば，$\mathsf{Adv}^{\mathsf{IND\text{-}sID\text{-}CPA}}_{\mathcal{A}'}(k)$ も non-negligible であるので，$\mathcal{A}'$ が IND-sID-CPA ゲームを破ることが証明された． □

また，CHK 変換以外の IND-sID-CPA 安全な $\ell$-HIBE を IND-ID-CCA2 安全な $(\ell-1)$-HIBE へと変換する手法として，Boneh-Katz 変換 (BK 変換) が知られている．BK 変換では，署名アルゴリズムの代わりに MAC アルゴリズムと commitment スキームを用いており，CHK 変換よりも効率的に変換することが可能である [7].

### 5.6.2 署名アルゴリズムへの変換

IBE とディジタル署名との関係として，IBE をディジタル署名に変換する手法が知られている．このとき，IBE は OW-ID-CPA 安全であるものであればよい．IBE が OW-ID-CPA 安全であるとは，いかなる多項式時間攻撃者に対しても，

$$\mathsf{Adv}^{\mathsf{OW\text{-}ID\text{-}CPA}}_{\mathcal{A}}(k) := \Pr\left[m' = m \mid \begin{array}{l}(pk, mk) := \mathsf{Setup}(1^k); \\ \mathrm{ID}^* := \mathcal{A}^{\mathsf{KeyGen}(\cdot)}(pk); \\ m := \mathcal{M}; \\ c^* := \mathsf{Enc}(pk, \mathrm{ID}^*, m); \\ m' := \mathcal{A}^{\mathsf{KeyGen}(\cdot)}(c^*)\end{array}\right] - \frac{1}{|\mathcal{M}_{IBE}|} \leq \epsilon(k)$$

であることである．OW-ID-CPA 安全性を満たす IBE から，署名 $(\mathsf{G_{sig}}, \mathsf{S_{sig}}, \mathsf{V_{sig}})$ を以下のように構成する．

$\underline{\mathsf{G_{sig}}(1^k)}$

1. $(pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k)$ を生成する．
2. $vk_{\mathsf{sig}} \xleftarrow{\mathsf{R}} pk, sk_{\mathsf{sig}} := mk$ とする．
3. $(vk_{\mathsf{sig}}, sk_{\mathsf{sig}})$ を出力する．

$\underline{\mathsf{S_{sig}}(sk_{\mathsf{sig}}, m)}$

1. $(d_m) \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(mk, m)$ を生成する．このとき，$m$ を ID とみなして個別秘密鍵の生成を行う．
2. $\sigma := d_m$ を出力する．

$\underline{\mathsf{V}_{\mathsf{sig}}(vk_{\mathsf{sig}}, \sigma, m)}$

1. $m' \xleftarrow{\mathsf{U}} \mathcal{M}_{IBE}$ を選ぶ．
2. $c \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, m, m')$ として $m$ を ID とみなしてメッセージ $m'$ の暗号化を行う．
3. $m'' := \mathsf{Dec}(d_m, c)$ を求める．
4. $m'' = m'$ であれば 1 を出力し，そうでなければ 0 を出力する．

**定理 5.10.** *IBE が OW-ID-CPA であるならば，上記の構成によるディジタル署名は EUF-CMA 安全な署名アルゴリズムである．*

*Proof.* これまでと同様に，上記のディジタル署名を EUF-CMA で破る攻撃者 $\mathcal{A}$ を仮定した場合に，IBE の OW-ID-CPA 安全性を破る攻撃者 $\mathcal{A}'$ の構成方法を図 7 に示す．

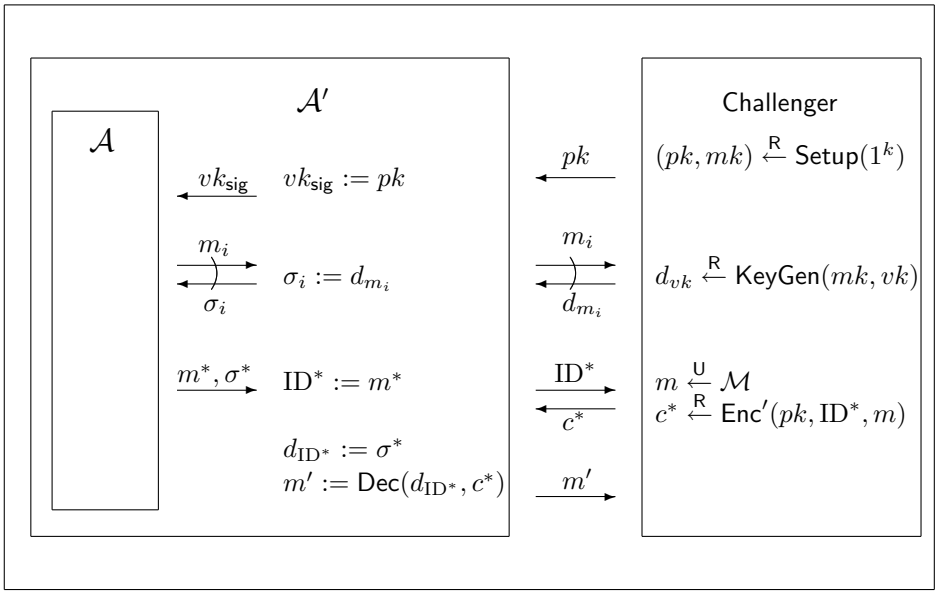


図 7: OW-ID-CPA 攻撃者 $\mathcal{A}'$ の構成

$\underline{\mathcal{A}' \text{ の動作}}$

まず，$\mathcal{A}'$ は Challenger からシステム公開鍵 $pk$ を受け取ると，それを署名の検証鍵として $\mathcal{A}$ に渡す．$\mathcal{A}$ の署名オラクルに対しては，受け取ったメッセージ $m_i$ を ID として Challenger に KeyGen オラクルを聞き，その返答 $d_{m_i}$ を署名として $\mathcal{A}$ に返答する．$\mathcal{A}$ が署名オラクルに聞いていないメッセージ $m^*$ に対する偽造 $(m^*, \sigma^*)$ を返答してきたら，$m^*$ を ID とみなして Challenger に対し $m^*$ に対しての暗号文 $c^*$ を生成させる．このとき，$\mathcal{A}$ が偽造として出力してきた $\sigma^*$ は $m^*$ という ID に対しての個別秘密鍵であるため，$\mathcal{A}'$ は $c^*$ を $d_{\mathrm{ID}^*} := \sigma^*$ として復号することができ，元のメッセージ $m$ を出力することができる．よって，ディジタル署名を EUF-CMA で破る攻撃者 $\mathcal{A}$ を仮定すると場合，$\mathcal{A}'$ は IBE の OW-ID-CPA 安全性を破ることができる． □

### 5.6.3 Boneh-Boyen 署名

5.5.3 節の Boneh-Boyen IBE (BB04b IBE) は，以下の署名方式へと拡張を行うことができる [5].

$\mathsf{G}_{\mathsf{sig}}$: $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とする．$g \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$x, y \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $X := g^x, Y := g^y$ を求める．$vk := (g, X, Y)$，$sk := (x, y)$ とする．

$$vk = (g, X, Y),\ sk = (x, y)$$

$\mathsf{S}_{\mathsf{sig}}$: あるメッセージ $m \in \mathbb{Z}_p$ に対しての署名を行う場合，$r \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選び，$\sigma := g^{\frac{1}{m+x+yr}}$ を出力する．

$\mathsf{V}_{\mathsf{sig}}$: 署名 $\sigma$ を検証する場合，$e'(\sigma, g^m XY^r) = e'(g, g)$ であれば 1 を出力し，そうでなければ 0 を出力する．

Boneh-Boyen 署名の安全性の根拠となる数論仮定は，$q$-SDH(Strong Diffie-Hellman) 仮定と呼ばれるものである．

$q$-SDH 仮定

$x \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ として $(g, g^x, g^{x^2}, \ldots, g^{x^q}) \in \mathbb{G}^{q+1}$ が入力された場合に，$(c, g^{\frac{1}{x+c}}) \in \mathbb{Z}_p \times \mathbb{G}_T$ を求める問題を $q$-SDH 問題と呼ぶ．そして，いかなる多項式時間攻撃者に対しても $q$-SDH 問題を解くことが困難である場合，その群上において $q$-SDH 仮定が保たれているという．

**定義 5.7.** 攻撃者 $\mathcal{A}$ の *$q$-SDH* 問題に対する優位性を

$$\mathsf{Adv}_{\mathcal{A}}^{q\text{-}\mathsf{SDH}}(k) := \Pr\left[\mathcal{A}(g, g^x, \ldots, g^{x^q}) \to (c, g^{\frac{1}{x+c}}) \wedge c \in \mathbb{Z}_p \mid x \xleftarrow{\mathsf{U}} \mathbb{Z}_p\right]$$

と置いたとき，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}_{\mathcal{A}}^{q\text{-}\mathsf{SDH}}(k) \leq \epsilon(k)$ である場合，その群において *$q$-SDH* 仮定が保たれているという．

**定理 5.11.** *Boneh-Boyen* 署名は *Standard Model* において *q-SDH* 仮定の下で *sEUF-CMA* 安全である．

### 5.6.4 Waters 署名

5.5.4 節の Waters IBE は，以下の署名方式へと拡張を行うことができる [19].

$\mathsf{G}_{\mathsf{sig}}$: $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とする．$g, g_2, u', u_1, \ldots, u_k \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$a \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $g_1 := g^a$ を求める．$vk := (g, g_1, g_2, u', u_1, \ldots, u_k)$，$sk := g_2^a$ とする．

$$vk = (g, g_1, g_2, u', u_1, \ldots, u_k),\ sk = g_2^a$$

$\mathsf{S}_{\mathsf{sig}}$: メッセージ $m = (m_1, \ldots, m_k) \in \{0,1\}^n,\ m_i \in \{0,1\}$ に対しての署名を行う場合，$s \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選び，$(\sigma_0, \sigma_1) := (g^s, g_2^a(u' \prod_{i=1}^k u_i^{m_i})^s)$ を求め $\sigma := (\sigma_0, \sigma_1)$ を出力する．

$\mathsf{V}_{\mathsf{sig}}$: 署名 $\sigma$ を検証する場合，$\sigma, m$ および $vk$ を入力とし，$e'(\sigma_1, g)/e'(\sigma_0, u' \prod_{i=1}^k u_i^{m_i}) = e'(g_1, g_2)$ であれば 1 を出力し、そうでなければ 0 を出力する．

**定理 5.12.** *Waters* 署名は *Standard Model* において *BDH* 仮定の下で *sEUF-CMA* 安全である．

# 6 属性ベース暗号

属性ベース暗号 (ABE: Attribute Based Encryption) とは，IBE をさらに拡張した概念として考えられた方式である．IBE における ID が ABE では属性情報へと変わり，ある一定の条件を満たす属性情報を持った利用者はその秘密鍵によって暗号文の復号を行うことができる方式となっている．ABE は大きく二つに分類でき，復号を行えるかの条件が秘密鍵に埋め込まれる **Key Policy ABE (KP-ABE)** と，その条件が暗号文に埋め込まれる **Ciphertext Policy ABE (CP-ABE)** に分けられる．

ABE の構成について述べる前に，いくつかの前提として秘密分散法や Fuzzy IBE と呼ばれる ABE の元となった方式について述べておく．

## 6.1 Shamir の秘密分散法

ある秘密 $s$ を $n$ 個の秘密 $s_1, s_2, \ldots, s_n$ と分割して $n$ 人のパーティへと渡し，分散した秘密を持っているパーティが $d$ 人以上集まれば秘密が復元できるシステムを**秘密分散法 (Secret Sharing Scheme)** という．Shamir が考えた秘密分散法は多項式を利用して $a_1, \ldots, a_{d-1} \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ として $d-1$ 次多項式 $f(x) := a_0 + a_1 x + \cdots + a_{d-1} x^{d-1}$

かつ $a_0 := s$ を考えたとき，$d$ 個の点が集まればその関数の係数が各々ラクランジュ補間によって計算できることから $s$ が復元できる，というものである．分散された秘密を $s_1 := f(1), s_2 := f(2), \ldots, s_n := f(n)$ とし，この中から $d-1$ 個の値 $s_1, \ldots, s_{d-1}$ を集めてきた場合，これらの値は

$$\begin{pmatrix} f(1) \\ f(2) \\ \vdots \\ f(n) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 4 & \cdots & 2^{d-1} \\ & & \vdots & & \\ 1 & d-1 & \cdots & & \end{pmatrix} \begin{pmatrix} s \\ a_1 \\ a_2 \\ \vdots \\ a_{d-1} \end{pmatrix}$$

となる．上式の Vandormorde 行列を $A$ とすると，$A$ の逆行列 $A^{-1}$ を求めることで

$$\begin{pmatrix} s \\ a_1 \\ \vdots \\ a_{d-1} \end{pmatrix} = A^{-1} \begin{pmatrix} f(1) \\ f(2) \\ \vdots \\ f(n) \end{pmatrix}$$

となり，$f(x)$ の各々の係数を求めることが出来る．このとき，$S = (1, \ldots, n), |S| = d$ とすると，行列の係数は $\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$ で決まり (ラグランジュ補間公式)，$f(x) = \sum_{i \in S} \Delta_{i,S}(x) \cdot f(i)$ となる．この関数を用いて $s' := f(0)$ としたとき，$s' = s$ となる．

属性ベース暗号や次の章で紹介するファジー ID ベース暗号は，このラグランジュ補間によってある条件を満たした場合のみ秘密の復元を行え，暗号文を復号できるように構成されている．

## 6.2 ファジー ID ベース暗号

**ファジー ID ベース暗号 (FIBE: Fuzzy Identity Based Encryption)** は 2005 年に Sahai-Waters によって提案されたもので，IBE と ABE との中間に位置する方式である．IBE において暗号文を復号する際には，暗号文を生成する時に用いた ID に対しての秘密鍵 $d_{\mathrm{ID}}$ を持っているパーティのみが復号を行うことが出来た．FIBE では ID を属性を表しているものの集合と捉え，暗号文を生成する時に用いる ID $\omega'$ に対し，あるしきい値 $d$ が個別秘密鍵に設けられており，ID が $|\omega \cap \omega'| \geq d$ なる ID $\omega$ に対する個別秘密鍵を持っていれば暗号文を復号できる方式となっている．

### 6.2.1 FIBE の定義

FIBE は 4 つのアルゴリズム $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ からなっており，

Setup：セットアップ - $k$ をセキュリティパラメータとしたとき $1^k$ を入力とし，システム公開鍵とマスター秘密鍵のペア $(pk, mk)$ を出力するアルゴリズム．このとき平文空間 $\mathcal{M}_{FIBE}$ が定まる．

$$1^k \rightarrow \boxed{\mathsf{Setup}} \rightarrow (pk, mk)$$

KeyGen：鍵生成 - $pk, mk$ と ID の集合 $\omega$ としきい値 $d$ を入力とし，その ID に対する個別秘密鍵 $sk_\omega$ を出力するアルゴリズム．

$$(pk, mk, \omega, d) \rightarrow \boxed{\mathsf{KeyGen}} \rightarrow sk_\omega$$

Enc：暗号化 - $pk$ と暗号文を送る相手の ID の集合 $\omega'$，平文空間から取ってきた平文 $m \in \mathcal{M}_{FIBE}$ を入力とし，暗号文 $c$ を出力するアルゴリズム．

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

Dec：復号 - $pk$ と秘密鍵 $sk_\omega$ と暗号文 $c$ を入力とし，平文 $m$ を出力するアルゴリズム．

$$(pk, sk_\omega, c) \rightarrow \boxed{\mathsf{Dec}} \rightarrow m \quad \text{if} \quad |\omega' \cap \omega| \leq d$$

である．FIBE における正当性とは，正しく平文 $m$ を暗号化されている場合において $|\omega' \cap \omega| \leq d$ ならば秘密鍵 $sk_\omega$ を用いたときに復号結果が正しく元の平文に戻ることであり，

$$\Pr\left[ m' = m \mid \begin{array}{l} (pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k); \\ sk_\omega \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(pk, mk, \omega, d); \\ m \xleftarrow{\mathsf{U}} \mathcal{M}_{FIBE};\ c \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \omega', m); \\ m' := \mathsf{Dec}(pk, sk_\omega, c); \\ |\omega' \cap \omega| \geq d \end{array} \right] = 1$$

である．

### 6.2.2 FIBE の安全性

FIBE における安全性は，IBE と同様に定義されるが，個別秘密鍵を得るための KeyGen クエリにおいて，challenge 暗号文に対する ID とのしきい値が $d$ を越えないという制約条件が課される．IND-sFID-CPA 安全性の場合，攻撃者の IND-sFID-CPA

ゲームに対する優位性は

$$\mathsf{Adv}^{\mathsf{IND\text{-}sFID\text{-}CPA}}_{\mathcal{A}}(k) := \left| 2 \cdot \Pr \left[ b' = b \mid \begin{array}{l} w^* \xleftarrow{\mathsf{R}} \mathcal{A}(); \\ (pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k); \\ (m_0, m_1) \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathsf{KeyGen}(\cdot,\cdot)}(pk); \\ b \xleftarrow{\mathsf{U}} \{0,1\}; \\ c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, w^*, m_b); \\ b' \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathsf{KeyGen}(\cdot,\cdot)}(c^*) \end{array} \right] - 1 \right|$$

で表される．KeyGen オラクルは $(\omega, d)$ が入力されたとき，$|\omega_i \cap \omega^*| \leq d$ の場合のみ個別秘密鍵を返答するオラクルであるとする．

### 6.2.3 Sahai-Waters FIBE (SW05a FIBE)

Sahai-Waters の提案した FIBE (SW05a FIBE) [16] を以下に示す．

**Setup:** $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とし，$\mathcal{U}$ をサイズが $n$ である ID の集合と定義し，$\mathbb{Z}_p$ の部分集合であるとする．$g \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$t_1, \ldots, t_n, y \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $T_1 := g^{t_1}, \ldots, T_n := g^{t_n}, Y := e'(g,g)^y$ を求める．$pk := (g, T_1, \ldots, T_n, Y)$，$mk := (t_1, \ldots, t_n, y)$ とする．

$$pk = (g, T_1, \ldots, T_n, Y),\ mk = (t_1, \ldots, t_n, y)$$

**KeyGen:** ある ID $\omega \subseteq \mathcal{U}$ と $mk$ を入力とし，しきい値が $d$ である個別秘密鍵を生成する場合，$q(0) = y$ となる $d-1$ 次の多項式 $q(x)$ を選んで $\{D_i := g^{\frac{q(i)}{t_i}}\}_{i \in \omega}$ を求め，$sk_\omega := (\omega, \{D_i\}_{i \in \omega})$ を個別秘密鍵とする．

**Enc:** ある ID $\omega'$ に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選ぶ．
2. $c_0 := m \cdot Y^s, \{c_i := T_i^s\}_{i \in \omega'}$ とする．
3. $C := (\omega', c_0, \{c_i\}_{i \in \omega'})$ を暗号文として出力する．

**Dec:** 暗号文 $C = (w', c_0, \{c_i\}_{i \in \omega'})$ および $sk_\omega$ を入力として復号を行う．このとき $|\omega \cap \omega'| \geq d$ が満たされる場合には，$\omega \cap \omega'$ の部分集合の中から適当に $d$ 個の集合 $S$ を取ってくる．そして $m' := c_0 \cdot \prod_{i \in S} (e'(D_i, C_i))^{-\Delta_{i,S}(0)}$ を平文として出力する．

SW05a FIBE において，暗号文 $(c_0, \{c_i\}_{i\in\omega'})$ が正しく生成されているならば，

$$\begin{aligned} m' &= c_0 \cdot \prod_{i\in S}(e'(D_i, c_i))^{-\Delta_{i,S}(0)} \\ &= c_0 \cdot \prod_{i\in S}(e'(g^{\frac{q(i)}{t_i}}, T_i^s))^{-\Delta_{i,S}(0)} \\ &= c_0 \cdot \prod_{i\in S}(e'(g,g))^{-s\cdot q(i)\Delta_{i,S}(0)} \\ &= c_0 \cdot (e'(g,g))^{-s\sum_{i\in S}\Delta_{i,S}(0)q(i)} \\ &= c_0 \cdot (e'(g,g))^{-sy} \\ &= m \end{aligned}$$

として平文を復号することができる．

FW05a FIBE の安全性の根拠となる数論仮定は，DMBDH(Decisional Modified Bilinear Diffie-Hellman) 仮定と呼ばれるものである．

DMBDH 仮定

$a, b, c \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ として $(g, g^a, g^b, g^c, Z) \in \mathbb{G}^4 \times \mathbb{G}_T$ が入力された場合に，$Z = e'(g,g)^{\frac{ab}{c}}$ であるかを判定する問題を DMBDH 問題と呼ぶ．そして，いかなる多項式時間攻撃者に対しても DMBDH 問題を解くことが困難である場合，その群において DMBDH 仮定が保たれているという．

**定義 6.1.** 攻撃者 $\mathcal{A}$ の *DMBDH* 問題に対する優位性を

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DMBDH}}(k) := \left| \begin{array}{l} \Pr\left[\mathcal{A}(g, g^a, g^b, g^c, Z) \to 1 \mid a, b, c \xleftarrow{\mathsf{U}} \mathbb{Z}_p;\ Z := e'(g,\hat{g})^{\frac{ab}{c}}\right] \\ -\Pr\left[\mathcal{A}(g, g^a, g^b, g^c, Z) \to 1 \mid a, b, c, z \xleftarrow{\mathsf{U}} \mathbb{Z}_p;\ Z := e'(g,\hat{g})^{z}\right] \end{array} \right|$$

と置いたとき，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DMBDH}}(k) \leq \epsilon(k)$ である場合，その群において *DMBDH* 仮定が保たれているという．

**定理 6.1.** *SW05a FIBE* は *Standard Model* において *DMBDH* 仮定の下に *IND-sFID-CPA* 安全である．

*Proof.* SW05 FIBE に対して IND-sFID-CPA で攻撃に成功する攻撃者 $\mathcal{A}$ を仮定した場合に，$\mathcal{A}$ を用いて DMBDH 仮定を破るアルゴリズム $\mathcal{B}$ を構成する．

$\mathcal{B}$ の動作

**Setup:** 最初に，$\mathcal{B}$ は DMBDH 問題の入力として $(g, g_1, g_2, g_3, Z) := (g, g^a, g^b, g^c, Z)$ を受け取る．また，$\mathcal{B}$ は $\mathcal{A}$ を動作させ，ターゲット ID $\omega^*$ を受け取る．これら

の値を用いて，

$$i \in \omega^* \Rightarrow \alpha_i \xleftarrow{\mathsf{U}} \mathbb{Z}_p, T_i := g_3^{\alpha_i}$$
$$i \notin \omega^* \Rightarrow \beta_i \xleftarrow{\mathsf{U}} \mathbb{Z}_p, T_i := g_3^{\beta_i}$$

とする．また，$Y := e'(g, g_1)$ とし，$pk := (g, \{T_i\}_{i=1,\ldots,n}, Y)$ を $\mathcal{A}$ に入力する．

**Phase 1:** $(\omega_i, d_i)$ が KeyGen クエリに問われたとする．selective FID ゲームの制約条件から，$|\omega_i \cap \omega^*| < d_i$ である．$\omega_i$ と $\omega^*$ の共通集合を $\Gamma := \omega_i \cap \omega^*$ とおき，これより大きな集合として $\Gamma \subseteq \Gamma' \subseteq \omega$ かつ $|\Gamma'| = d - 1$ となる $\Gamma'$ を取ってくる．$S := \Gamma' \cup \{0\}$ とし，3 つの場合に分けて個別秘密鍵の生成を行う．

Case 1: $i \in \Gamma$

$s_i \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $D_i := g^{s_i}$ とする．

Case 2: $i \notin \Gamma \wedge i \in \Gamma' - \Gamma$

$\lambda_i \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $D_i := g^{\frac{\lambda_i}{\beta_i}}$ とする．

Case 3: $i \notin \Gamma \wedge i \in \omega - \Gamma'$

この場合，$D_i = g^{\frac{q(i)}{\beta_i}}$ となるための $q(i)$ は Case 1 および Case 2 によって $d$ 個の値が定まっているため，ラグランジュ補間によって定まる値となる．よって

$$D_i := (\prod_{j \in \Gamma} g_3^{\omega_i^{-1} \alpha_j s_j \Delta_{j,S}(i)}) \cdot (\prod_{j \in \{\Gamma' - \Gamma\}} g^{\omega_i^{-1} \delta_j \Delta_{j,S}(i)}) \cdot (g_1^{\beta_i^{-1} \Delta_{0,S}(i)})$$

とする．

**Challenge:** 攻撃者 $\mathcal{A}$ から $(m_0, m_1)$ を受け取ると，$b' \xleftarrow{\mathsf{U}} \{0, 1\}$ から $c_0 := m_b \cdot Z, \{c_i := g_2^{\alpha_i}\}_{i \in \omega^*}$ として $C^* := (\omega^*, c_0, \{c_i\}_{i \in \omega^*})$ を返答する．

**Phase 2:** **Phase 1** と同様の操作を行う．

**Guess:** 攻撃者 $\mathcal{A}$ がビット $b''$ を出力したとする．$\mathcal{B}$ は $b'' = b'$ であれば 1 を出力し，そうでなければ 0 を出力する．

もし $\mathcal{B}$ への DMBDH 問題の入力において $Z = e'(g, g)^{\frac{ab}{c}}$ であるならば，シミュレーションは正しい SW05a FIBE の IND-sFID-CPA ゲームと等価になる．一方，$Z = e'(g, g)^z$ が入力されているならば，攻撃者 $\mathcal{A}$ は challenge 暗号文から平文の情報は情報理論的に得られないため，この場合の攻撃者の成功確率は $\frac{1}{2}$ である．よって

$$\begin{aligned}
\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(k) &= \left| \Pr\left[\mathcal{B} \to 1 \mid Z = e'(g, g)^{abc}\right] - \Pr\left[\mathcal{B} \to 1\right] \mid Z = e'(g, g)^z \right| \\
&= \left| 2 \cdot \Pr\left[b'' = b' \mid \text{正しい IND-sFID-CPA ゲーム}\right] - 1 \right| \\
&= \mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sFID\text{-}CPA}}(k)
\end{aligned}$$

となる．初めに，$\mathcal{A}$ の IND-sFID-CPA における攻撃成功確率 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sID\text{-}CPA}}(k)$ は non-negligible であると仮定していたので，$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(k)$ も non-negligible となる．よって $\mathcal{B}$ は DBDH 問題を non-negligible な確率で解くことができる． □

### 6.2.4 Sahai-Waters FIBE (SW05b FIBE)

6.2.3 節の SW05a FIBE では，公開パラメータの長さは $\mathcal{U}$ のサイズによって決まり，すべての ID は $\mathcal{U}$ に含まれる $\mathbb{Z}_p$ の $n$ 個の部分集合で表されていた．Sahai-Waters は ID 空間の制約を緩め，$\mathcal{U}$ を $\mathbb{Z}_p$ 全体とした改良方式を提案した [16]．改良された方式 SW05b FIBE を以下に示す．

**Setup:** $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とし，$\mathcal{U}$ を $\mathbb{Z}_p$ 全体，ID は $\mathbb{Z}_p$ が $n$ 個集まった集合とする．$g, g_2, T_1, \ldots, T_{n+1} \xleftarrow{\mathsf{U}} \mathbb{G}, y \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選んで，$g_1 := g^y$ を求める．$pk := (g, g_1, g_2, T_1, \ldots, T_{n+1})$，$mk := y$ とする．

$$pk = (g, g_1, g_3, T_1, \ldots, T_{n+1}),\ mk = y$$

**KeyGen:** ある ID $\omega \in (\mathbb{Z}_p)^n$ と $mk$ を入力とし，しきい値が $d$ である個別秘密鍵を生成する場合，$q(0) = y$ となる $d-1$ 次の多項式 $q(x)$ を選び $r_i \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を用いて関数

$$T(x) := g_2^{x^n} \cdot \prod_{i=1}^{n+1} T_i^{\Delta_{i,N}(x)}, \quad N = \{1, 2, \ldots, n+1\}$$

から $\{D_i := g_2^{q(i)} T(i)^{r_i}, d_i := g^{r_i}\}_{i \in \omega}$ を求め，$sk_\omega := (\{D_i, d_i\}_{i \in \omega})$ を個別秘密鍵として出力する．

**Enc:** ある ID $\omega'$ に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選ぶ．
2. $c_0 := m \cdot e'(g_1, g_2)^s, c_0' := g^s, \{c_i := T(i)^s\}_{i \in \omega'}$ とする．
3. $C := (\omega', c_0, c_0', \{c_i\}_{i \in \omega'})$ を暗号文として出力する．

**Dec:** 暗号文 $C = (w', c_0, c_0', \{c_i\}_{i \in \omega'})$ および $sk_\omega$ を入力として復号を行う．このとき $|\omega \cap \omega'| \geq d$ であるならば，$\omega \cap \omega'$ の部分集合の中から適当に $d$ 個の集合 $S$ を取ってくる．$m' = c_0 \cdot \prod_{i \in S} \left( \frac{e'(D_i, c_i)}{e'(D_i, c_0')} \right)^{\Delta_{i,S}(0)}$ を平文として出力する．

SW05b FIBE において，暗号文 $(w', c_0, c_1, c_2)$ が正しく生成されているならば，

$$\begin{aligned}
m' &= c_0 \cdot \prod_{i \in S} \left( \frac{e'(d_i, c_i)}{e'(D_i, c_0')} \right)^{\Delta_{i,S}(0)} \\
&= c_0 \cdot \prod_{i \in S} \left( \frac{e'(g^{r_i}, T(i)^s)}{e'(g_2^{q(i)} T(i)^{r_i}, g^s)} \right)^{\Delta_{i,S}(0)} \\
&= c_0 \cdot \prod_{i \in S} (e'(g_2, g))^{-s \cdot q(i) \Delta_{i,S}(0)} \\
&= c_0 \cdot (e'(g_2, g))^{-s \sum_{i \in S} \Delta_{i,S}(0) q(i)} \\
&= c_0 \cdot (e'(g_2, g))^{-sy} \\
&= m
\end{aligned}$$

として平文を復号することができる．

**定理 6.2.** *SW05b FIBE は Standard Model において DBDH 仮定の下に IND-sFID-CPA 安全である．*

## 6.3 アクセス構造

IBE においてはメッセージを暗号化する時の ID と秘密鍵を持っている相手の ID が一致しているときのみ復号可能であり，FIBE においてはメッセージを暗号化する時の ID と秘密鍵を持っている相手の ID の共通部分のしきい値が一定数を越えるときに復号可能であった．これをより一般的にしたものが ABE であり，この場合「一般的なアクセス構造」により復号条件が決定される．

アクセス構造とは，パーティの集合 $\{P_1, \ldots, P_n\}$ に対して秘密 $s$ を $(s_1, \ldots, s_n)$ と分割して $s_i$ を $P_i$ に渡しておいたときに，$s$ を復号できるすべてにパーティの部分集合の集合で表される．例えば，秘密 $s$ の復号条件が「$P_1$ と $P_2$ が集まる」か「$P_1$ と $P_3$ と $P_4$ が集まる」であれば，アクセス構造 $\mathbb{A}$ は $\mathbb{A} = \{\{P_1, P_2\}, \{P_1, P_3, P_4\}\}$ と表される．一般に，このアクセス構造は $\mathbb{A} \subseteq (2^{\{P_1, \ldots, P_n\}} - \{\varphi\})$ で表すことができる．また，アクセス構造を満たしていればその他のいかなるパーティが集まったとしても秘密を復号を行うことができるアクセス構造を monotone とよぶ．

$$\mathbb{A} \text{ が monotone} := \ \forall B, C \quad (B \in \mathbb{A}) \cap (B \subseteq C) \Rightarrow C \in \mathbb{A}$$

また，$\mathbb{A}$ に含まれる部分集合を authorised 集合，$\mathbb{A}$ に含まれない部分集合を unauthorised 集合と呼ぶ．ABE では，パーティの集合 $\{P_1, \ldots, P_n\}$ を属性 $\{A_1, \ldots, A_n\}$ に置き換えて考える．

### 6.3.1 Linear Secret Sharing Scheme (LSSS)

一般のアクセス構造を効率的に実現するための手法として Linear Secret Sharing Scheme (LSSS) が挙げられる．

$\mathbb{K}$ を有限体とし，Secret Sharing Scheme (SSS) を $\pi$ で表すとする．このとき，秘密が $s \in \mathbb{K}$ であり，アクセス構造 $\mathbb{A}$ を実現する $\pi$ が $\mathbb{K}$ 上の LSSS であるとは，

1. 各パーティ $P_i$ の秘密 $s_i$ が $\mathbb{K}$ 上の値であり，$s_i = \{\pi_{i,j}(s^*, r)\}_{j=1,\ldots,d_i}$ で表される ($r$ は $s$ を分割するときに用いた乱数)．

2. authorised 集合 $G \in \mathbb{A}$ に対して $s$ が線形結合によって復元できること．

$$\exists\{\alpha_{i,j} | P_i \in G, 1 \leq i \leq d_i\} \text{ s.t. } s = \sum_{P_i \in G} \sum_{1 \leq i \leq d_i} \alpha_{i,j} \pi_{i.j}(s, r)$$

LSSS の実現例としては，Shamir の SSS や，SSS を階層化させ，分割した秘密鍵をさらにしきい値で分割して秘密分散させているアクセス木と呼ばれるものが挙げられる．アクセス木ではそれぞれのノードにしきい値が割り当てられており，最下位ノードが葉ノードとして属性と対応する形で表現されている．

### 6.3.2 Monotone Span Program (MSP)

先ほどの LSSS を一般的に表現したものが Monotone Span Program (MSP) である．$\mathbb{K}$ を有限体とし，$\{x_1, \ldots, x_n\}$ を変数の集合とする．このとき，$\mathbb{K}$ 上の MSP とは $t \times \ell$ 行列 $M$ と，$M$ の行を $\{x_1, \ldots, x_n\}$ にラベル付けする写像 $\rho$ としたときラベル付けされた行列 $\hat{M}(M, \rho)$ のことをいう．変数の部分集合 $\gamma$ を選んだときに写像 $\rho$ に

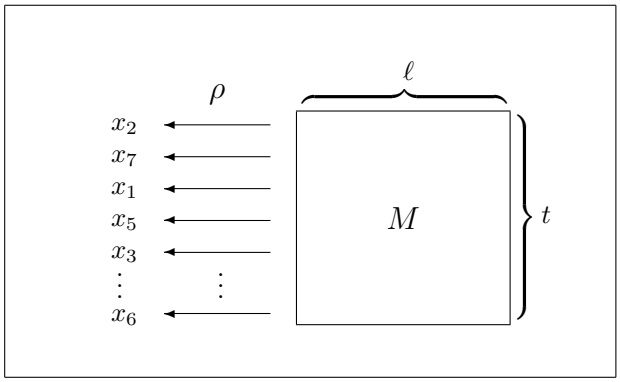


図 8: MSP におけるラベル付け

よって対応する，行列 $M$ の部分行列を $M_\gamma$ で表すとする．このとき，$M_\gamma$ の行ベクトルで張られるベクトル空間 $\mathrm{span}(M_\gamma)$ に 1 の $\ell$ 列ベクトル $\vec{1} := (1, \ldots, 1)$ が含まれて

いるとき，MSP $\hat{M}$ は $\gamma$ を受理するという．つまり，$\sum_{i\in\gamma}\alpha_i M_i = \vec{1}$ となる $\{\alpha_i\}_{i\in\gamma}$ が存在するするとき MSP $\hat{M}$ は $\gamma$ を受理する．

**定理 6.3.** *LSSS は MSP と等価である．*

## 6.4 Key Policy ABE (KP-ABE)

### 6.4.1 KP-ABE の定義

KP-ABE は 4 つのアルゴリズム (Setup, Enc, KeyGen, Dec) からなっており，

Setup：セットアップ - $k$ をセキュリティパラメータとしたとき $1^k$ を入力とし，システム公開鍵とマスター秘密鍵のペア $(pk, mk)$ を出力するアルゴリズム．このとき平文空間 $\mathcal{M}_{ABE}$ が定まる．

$$1^k \to \boxed{\mathsf{Setup}} \to (pk, mk)$$

Enc：暗号化 - $pk$ と属性集合 $\gamma$，平文空間から取ってきた平文 $m \in \mathcal{M}_{ABE}$ を入力とし，暗号文 $c_\gamma$ を出力するアルゴリズム．

$$(pk, \gamma, m) \to \boxed{\mathsf{Enc}} \to c_\gamma$$

KeyGen：鍵生成 - $mk$ と $pk$ とアクセス構造 $\mathbb{A}$ を入力とし，そのアクセス構造にたいする個別秘密鍵 $sk_{\mathbb{A}}$ を出力するアルゴリズム．

$$(pk, mk, \mathbb{A}) \to \boxed{\mathsf{KeyGen}} \to sk_{\mathbb{A}}$$

Dec：復号 - $pk$ と $sk_{\mathbb{A}}$ と暗号文 $c_\gamma$ を入力とし，$\gamma \in \mathbb{A}$ ならば平文 $m$ を出力するアルゴリズム．

$$(pk, sk_{\mathbb{A}}, c_\gamma) \to \boxed{\mathsf{Dec}} \to m \text{ if } \gamma \in \mathbb{A}$$

である．KP-ABE における正当性とは，正しく平文 $m$ を暗号化されている場合において $\gamma \in \mathbb{A}$ ならば秘密鍵 $sk_{\mathbb{A}}$ を用いたときに復号結果が正しく元の平文に戻ることであり，

$$\Pr\left[ m' = m \mid \begin{array}{l} (pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k);\ c_\gamma \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \gamma, m); \\ m \xleftarrow{\mathsf{U}} \mathcal{M}_{ABE};\ sk_{\mathbb{A}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(pk, mk, \mathbb{A}); \\ m' := \mathsf{Dec}(pk, sk_{\mathbb{A}}, c); \gamma \in \mathbb{A} \end{array} \right] = 1$$

である．

### 6.4.2 KP-ABE の安全性

KP-ABE における安全性では，個別秘密鍵を得るための KeyGen クエリにおいて用いられるアクセス構造が，challenge 暗号文における属性集合を含まないという制約条件を課す．IND-sAT-CPA 安全性の場合，攻撃者の成功確率は

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sAT\text{-}CPA}}(k) := \left| 2 \cdot \Pr \left[ b' = b \mid \begin{array}{l} \gamma^* \xleftarrow{\mathsf{R}} \mathcal{A}(); \\ (pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k); \\ (m_0, m_1) \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathsf{KeyGen}(pk,mk,\cdot)}(pk); \\ b \xleftarrow{\mathsf{U}} \{0,1\}; \\ c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \gamma^*, m_b); \\ b' \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathsf{KeyGen}(pk,mk,\cdot)}(c^*) \end{array} \right] - 1 \right|$$

で表され，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sAT\text{-}CPA}}(k)$ が negligible である場合，その方式は IND-sAT-CPA 安全であるという．なお，IND-sAT-CPA 安全性の場合，KeyGen オラクルは $\mathbb{A}$ が入力されたとき，$\gamma^* \notin \mathbb{A}$ の場合のみ個別秘密鍵を返答するオラクルとする．

### 6.4.3 Goyal-Pandey-Sahai-Waters KP-ABE (GPSW KP-ABE)

Goyal, Pandey, Sahai, Waters は初めて Key Policy の ABE を提案した [13]．Goyal-Pandey-Sahai-Waters KP-ABE (GPSW KP-ABE) の構成を，アクセス木を用いた場合と MSP を用いた場合の二種類について示す．

[アクセス木による構成]

**Setup:** $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とし，$\mathcal{U}$ をサイズが $n$ である値の集合とする．$g \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$t_1, \ldots, t_n, y \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $T_1 := g^{t_1}, \ldots, T_n := g^{t_n}, Y := e'(g,g)^y$ を求める．$pk := (g, T_1, \ldots, T_n, Y)$，$mk := (t_1, \ldots, t_n, y)$ とする．

$$pk = (g, T_1, \ldots, T_n, Y),\ mk = (t_1, \ldots, t_n, y)$$

**Enc:** ある属性情報 $\gamma \subseteq \mathcal{U}$ に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選ぶ．
2. $c_0 := m \cdot Y^s, \{c_i := T_i^s\}_{i \in \gamma}$ とする．
3. $C := (\gamma, c_0, \{c_i\}_{i \in \gamma})$ を暗号文として出力する．

KeyGen: あるアクセス木 $\mathbb{T}$ と $mk$ を入力とし，$\gamma \in \mathbb{T}$ ならば暗号文が復号できる個別秘密鍵 $sk_{\mathbb{T}}$ を考える．まず，しきい値 $d_x$ の各ノード $x$ に対して，次数 $d_x - 1$ の多項式 $q_x$ を選ぶ．このとき，ルートノード $r$ に関しては $q_r(0) = y$ となるようにする．アクセス木の最下位の葉ノードが属性 $i$ に対応し，その葉ノードの名前を $\alpha_i$，$\alpha_i$ の親ノードの名前を $\mathrm{parent}(\alpha_i)$ とし $\alpha_i$ が $\mathrm{parent}(\alpha_i)$ の $j$ 番目の子ノードとする．$q_{\alpha_i}(0) := q_{\mathrm{parent}(\alpha_i)}(j)$ とし，$D_{\alpha_i} := g^{\frac{q_{\alpha_i}(0)}{t_i}}$ $(i = 1, \ldots, n)$ を求め，$sk_{\mathbb{T}} := (\{D_{\alpha_i}\}_{i=1,\ldots,n})$ を個別秘密鍵とする．

Dec: 暗号文 $C$ および $sk_{\mathbb{T}}$ を入力として復号を行う．まず，葉ノード $\alpha_i \in \gamma$ に対して $e'(D_{\alpha_i}, c_i)$ を計算する．暗号文に対して秘密鍵のしきい値がノード $x$ のしきい値を越える場合，$d_x$ 個の集合 $S_x$ を取ってくる．$x$ の子ノード $z$ において計算された値を $F_z$ とおいたとき，$F_x := \prod_{z \in S_x} F_z^{\Delta_{i,S_x}(0)}$ を求める．再帰的にルートノードまで繰り返し，$F_r$ を求め，$m' = c_0 \cdot F_r^{-1}$ を平文として出力する．

GPSW KP-ABE において，暗号文 $(c_0, \{c_i\}_{i \in \gamma})$ が正しく生成されているならば，葉ノードに対応する属性の秘密鍵を用いて

$$F_{\alpha_i} = e'(D_{\alpha_i}, c_{\alpha_i}) = e'(g, g)^{s \cdot q_{\alpha_i}(0)}$$

となる．この値を用いて中間ノードの値は

$$\begin{aligned} F_x &= \prod_{z \in S_x} F_z^{\Delta_{z,S_x}(0)} \\ &= \prod_{z \in S_x} (e'(g, g)^{s \cdot q_x(z)})^{-\Delta_{z,S_x}(0)} \\ &= (e'(g, g))^{-\sum_{z \in S_x} s \cdot q_x(z) \Delta_{z,S_x}(0)} \\ &= c_0 \cdot e'(g, g)^{s \cdot q_x(0)} \end{aligned}$$

として計算することが出来る．この計算をルートノードに辿り着くまで繰り返すと $F_z = e'(g, g)^{s \cdot q_r(0)} = e'(g, g)^{sy}$ が得られ，暗号文を復号することができる．

[MSP による構成]

Setup: $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とし，$\mathcal{U}$ をサイズが $n$ である値の集合とする．$g \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$t_1, \ldots, t_n, y \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $T_1 := g^{t_1}, \ldots, T_n := g^{t_n}, Y := e'(g, g)^y$ を求める．$pk := (g, T_1, \ldots, T_n, Y)$，$mk := (t_1, \ldots, t_n, y)$ とする．

$$pk = (g, T_1, \ldots, T_n, Y),\ mk = (t_1, \ldots, t_n, y)$$

Enc: ある属性情報 $\gamma \subseteq \mathcal{U}$ に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選ぶ．

2. $c_0 := m \cdot Y^s, \{c_i := T_i^s\}_{i \in \gamma}$ とする．

3. $C := (\gamma, c_0, \{c_i\}_{i \in \gamma})$ を暗号文として出力する．

KeyGen: MSP $\hat{M}$ と $mk$ を入力とし，$\gamma \in \hat{M}$ ならば暗号文が復号できる個別秘密鍵 $sk_{\mathbb{T}}$ を考える．まず，ベクトル $\vec{u} := (u_1, \ldots, u_t)$ を $\sum_{i=1}^{t} u_i = y$ となるように要素 $u_1, \ldots, u_t \xleftarrow{\cup} \mathbb{Z}_p$ を選ぶ．$t \times \ell$ 行列 $M$ の $i$ 行ベクトルを $\vec{M}_i$ で表したとき，$D_{\alpha_i} := g^{\frac{\vec{M}_i \cdot \vec{u}}{t_{\rho(i)}}}$ $(i = 1, \ldots, n)$ を求め，$sk_{\hat{M}} := (\{D_{\alpha_i}\}_{i=1,\ldots,m})$ を個別秘密鍵とする．

Dec: 暗号文 $C$ および $sk_{\hat{M}}$ を入力として復号を行う．MSP が $\gamma$ を受理する場合，$\sum_{\rho(i) \in \gamma} \alpha_i \vec{M}_i = \vec{1}$ となる $\alpha_i$ が存在するため，$\alpha_i$ を求め，$m' := c_0 \cdot \prod_{\rho(i) \in \gamma} e'(D_{\rho(i)}, c_i)^{-\alpha_i}$ を出力する．

GPSW KP-ABE において，暗号文 $(c_0, \{c_i\}_{i \in \gamma})$ が正しく生成されているならば，

$$
\begin{aligned}
m' &= c_0 \cdot \prod_{\rho(i) \in \gamma} e'(D_{\rho(i)}, c_i)^{-\alpha_i} \\
&= c_0 \cdot \prod_{\rho(i) \in \gamma} e'(g^{\frac{q_i(0)}{t_i}}, T_i^s)^{-\alpha_i} \\
&= c_0 \cdot \prod_{\rho(i) \in \gamma} e'(g, g)^{-s \cdot \alpha_i \cdot \vec{M}_i \cdot \vec{u}} \\
&= c_0 \cdot e'(g, g)^{-s \cdot \sum_{\rho(i) \in \gamma} \alpha_i \vec{M}_i \cdot \vec{u}} \\
&= c_0 \cdot e'(g, g)^{-s \cdot \vec{1} \cdot \vec{u}} \\
&= c_0 \cdot e'(g, g)^{-sy} \\
&= m
\end{aligned}
$$

として暗号文を復号することができる．

**定理 6.4.** *GPSW KP-ABE は Standard Model において DBDH 仮定の下で IND-sAT-CPA 安全である．*

*Proof.* GPSW KP-ABE に対して IND-sAT-CPA で攻撃に成功する攻撃者 $\mathcal{A}$ を仮定した場合に，$\mathcal{A}$ を用いて DBDH 仮定を破るアルゴリズム $\mathcal{B}$ を構成する．

$\mathcal{B}$ の動作

**Setup:** 最初に，$\mathcal{B}$ は DBDH 問題の入力として $(g, g_1, g_2, g_3, Z) := (g, g^a, g^b, g^c, Z)$ を受け取る．攻撃者 $\mathcal{A}$ を動作させて $\gamma^*$ を受け取り，$\gamma^*$ に応じて $1 \leq i \leq n$ に

対して

$$i \in \gamma^* \Rightarrow \gamma_i \xleftarrow{\cup} \mathbb{Z}_p,\ T_i := g^{\gamma_i}$$
$$i \notin \gamma^* \Rightarrow \beta_i \xleftarrow{\cup} \mathbb{Z}_p,\ T_i := g_2^{\beta_i}$$

とする．$Y := e'(g_1, g_2)$ を求め，$pk := (\{T_i\}_{i=1,\ldots,n}, Y)$ を $\mathcal{A}$ に入力する．

**Phase 1:** $\hat{M}$ に対して KeyGen クエリが行われた場合，$t \times \ell$ 行列 $M$ の $j$ 行列目を $\vec{M}_j = (x_{j1}, \ldots, x_{j\ell})$ と表したとき，

Case 1: $\rho(j) \in \gamma^*$

$\lambda_i \xleftarrow{\cup} \mathbb{Z}_p$ を選び，

$$\Phi_1 := \frac{\sum_{i=1}^{\ell} x_{ji}\lambda_i}{\gamma_{\rho(j)}}$$

として $D_j := g_2^{\Phi_1}$ を求める．

Case 2: $\rho(j) \notin \gamma^*$

$M_{\gamma^*}$ は $\vec{1}$ と独立であるので，$M_{\gamma^*} \cdot \vec{w} = 0$ となる $\vec{w}$ が存在する．この $\vec{w} = (w_1, \ldots, w_\ell)$ を求め，$h := \sum_{i=1}^{\ell} w_i$ とする．この値を用いて，

$$\Phi_2 := \frac{\sum_{i=1}^{\ell} x_{ji}}{h\beta_{\rho(j)}},\ \Phi_3 := \frac{\sum_{i=1}^{\ell} x_{ji}(w_i - \sum k = 1^{\ell}\lambda_k)}{h\beta_{\rho(j)}},$$

として $D_j := g_1^{\Phi_2} g^{\Phi_3}$ を求める．

それぞれに対応する $D_j$ を求め，$sk_{\hat{M}} := \{D_i\}_{i=1,\ldots,n}$ を $\mathcal{A}$ に返答する．

**Challenge:** $\mathcal{A}$ から $m_0, m_1$ を受け取ると，$b' \xleftarrow{\cup} \{0,1\}$ を選び $c_0 := m_b \cdot Z, \{c_i := g_3^{\gamma_i}\}_{i\in\gamma^*}$ として $C^* := (\gamma^*, c_0, \{c_i\}_{i\in\gamma^*})$ を $\mathcal{A}$ に返答する．

**Phase 2: Phase 1** と同等の操作を行って $\hat{M}$ に対しての個別秘密鍵 $sk_{\hat{N}}$ を $\mathcal{A}$ に返答する．

**Guess:** 攻撃者 $\mathcal{A}$ がビット $b''$ を出力したならば，$b'' = b'$ であれば 1 を出力し，そうでなければ 0 を出力する．

KeyGen クエリにおける鍵生成に関しての補足説明を行う．まず，$v_i := b\lambda_i$ となるベクトル $\vec{v} := (v_1, \ldots, v_\ell)$ を考える．$\psi := (ab - b\sum_{k=1}^{\ell} \lambda_k) \cdot h^{-1}$ とおき，$\vec{u} := \vec{v} + \psi\vec{w}$

とする．このとき，

$$\begin{aligned}\vec{1}\cdot\vec{u}=\sum_{i=1}^{\ell}(v_i+\psi w_i)&=\sum_{i=1}^{\ell}\left(b\lambda_i+\frac{ab-b\sum_{k=1}^{\ell}\lambda_k}{h}\cdot w_i\right)\\&=b\cdot\sum_{i=1}^{\ell}\lambda_i+\frac{ab-b\sum_{k=1}^{\ell}\lambda_k}{h}\cdot\sum_{i=1}^{\ell}w_i\\&=b\cdot\sum_{i=1}^{\ell}\lambda_i+\frac{ab-b\sum_{k=1}^{\ell}\lambda_k}{h}\cdot h\\&=ab\end{aligned}$$

という関係が成り立つ．Case 1 においては，

$$\begin{aligned}\frac{\vec{M}_j\cdot\vec{u}}{t_{\rho(j)}}&=\frac{\vec{M}_j\cdot(v_i+\psi w_i)}{t_{\rho(j)}}\\&=\frac{\vec{M}_j\cdot v_i+\psi(\vec{M}_j\cdot w_i)}{t_{\rho(j)}}\\&=\frac{\vec{M}_j\cdot v_i+\psi\cdot 0}{t_{\rho(j)}}\\&=b\cdot\frac{\sum_{i=1}^{\ell}x_{ji}\lambda_i}{r_{\rho(j)}}\\&=b\Phi_1\end{aligned}$$

となるため，$D_j=g_2^{\Phi_1}$ は正しい正しい IND-sAT-CPA ゲームにおける個別秘密鍵の分布と同じとなる．また，Case 2 においては

$$\begin{aligned}\frac{\vec{M}_j\cdot\vec{u}}{t_{\rho(j)}}&=\frac{b\sum_{i=1}^{\ell}x_{ji}\left(\lambda_i+\frac{a-\sum_{k=1}^{\ell}\lambda_k}{h}\right)}{b\beta_{\rho(j)}}\\&=a\left(\frac{\sum_{i=1}^{\ell}x_{ji}}{h\beta_{\rho(j)}}\right)+\left(\frac{\sum_{i=1}^{\ell}x_{ji}(h\lambda_i-\sum_{k=1}^{\ell}\lambda_k)}{h\beta_{\rho(j)}}\right)\\&=a\Phi_2+\Phi_3\end{aligned}$$

となるため，$D_j=g_1^{\Phi_2}g^{\Phi_3}$ は正しい IND-sAT-CPA ゲームにおける個別秘密鍵の分布と同じとなる．

$\mathcal{B}$ に入力される値が $Z=e'(g,g)^{abc}$ である場合，challenge 暗号文の分布は正しい IND-sAT-CPA ゲームにおける challenge 暗号文と一致する．一方，$Z=e'(g,g)^{z}$ であれば，$\mathcal{A}$ が challenge 暗号文から平文の情報を得ることは情報理論的に不可能であ

るため，

$$\begin{aligned}\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(k) &= \left|\Pr\left[Z = e'(g,g)^{abc} : \mathcal{B} \to 1\right] - \Pr\left[Z = e'(g,g)^{z} : \mathcal{B} \to 1\right]\right| \\ &= \left|\Pr\left[\text{正しい IND-sAT-CPA ゲーム} : b'' = b'\right] - \frac{1}{2}\right| \\ &= \left|\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sAT\text{-}CPA}}(k)\right|\end{aligned}$$

となる．今，$\mathcal{A}$ の IND-sAT-CPA における攻撃成功確率 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sAT\text{-}CPA}}(k)$ は non-negligible であると仮定しているので，$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DBDH}}(k)$ も non-negligible である．よって $\mathcal{B}$ は DBDH 問題を non-negligible な確率で解くことができる． □

## 6.5 Ciphertext Policy ABE (CP-ABE)

### 6.5.1 CP-ABE の定義

Ciphertext Policy ABE (CP-ABE) は 4 つのアルゴリズム (Setup, Enc, KeyGen, Dec) からなっており，

Setup：セットアップ - $k$ をセキュリティパラメータとしたとき $1^k$ を入力とし，システム公開鍵とマスター秘密鍵のペア $(pk, mk)$ を出力するアルゴリズム．このとき平文空間 $\mathcal{M}_{ABE}$ が定まる．

$$1^k \to \boxed{\mathsf{Setup}} \to (pk, mk)$$

Enc：暗号化 - $pk$ とアクセス構造 $\mathbb{A}$，平文空間から取ってきた平文 $m \in \mathcal{M}_{ABE}$ を入力とし，暗号文 $c_{\mathbb{A}}$ を出力するアルゴリズム．

$$(pk, \mathbb{A}, m) \to \boxed{\mathsf{Enc}} \to c_{\mathbb{A}}$$

KeyGen：鍵生成 - $pk$ と $mk$ と属性情報 $S$ を入力とし，その属性情報に対する個別秘密鍵 $sk_S$ を出力するアルゴリズム．

$$(pk, mk, S) \to \boxed{\mathsf{KeyGen}} \to sk_S$$

Dec：復号 - $pk$ と $sk_S$ と暗号文 $c_{\mathbb{A}}$ を入力とし，$S \in \mathbb{A}$ ならば平文 $m$ を出力するアルゴリズム．

$$(pk, sk_S, c_{\mathbb{A}}) \to \boxed{\mathsf{Dec}} \to m \text{ if } S \in \mathbb{A}$$

である．CP-ABE における正当性とは，正しく平文 $m$ を暗号化されている場合において $\mathbb{A} \in S$ ならば秘密鍵 $sk_{\mathbb{A}}$ を用いたときに復号結果が正しく元の平文に戻ることであり，

$$\Pr\left[m' = m \mid \begin{array}{l} (pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k);\ c_{\mathbb{A}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \mathbb{A}, m); \\ m \xleftarrow{\mathsf{U}} \mathcal{M}_{ABE};\ sk_S \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(pk, mk, S); \\ m' := \mathsf{Dec}(pk, sk_S, c_{\mathbb{A}}); S \in \mathbb{A} \end{array}\right] = 1$$

である．

### 6.5.2 CP-ABE の安全性

KP-ABE における安全性では，個別秘密鍵を得るための KeyGen クエリにおいて用いられるアクセス構造が，challenge 暗号文における属性集合を含まないという制約条件を課す．IND-sAT-CPA 安全性の場合，攻撃者の成功確率は

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sAT\text{-}CPA}}(k) := \left| 2 \cdot \Pr\left[b' = b \mid \begin{array}{l} \mathbb{A}^* \xleftarrow{\mathsf{R}} \mathcal{A}(); \\ (pk, mk) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k); \\ (m_0, m_1) \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathsf{KeyGen}(\cdot)}(pk); \\ b \xleftarrow{\mathsf{U}} \{0,1\}; \\ c^* \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk, \mathbb{A}^*, m_b); \\ b' \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathsf{KeyGen}(\cdot)}(c^*) \end{array}\right] - 1 \right|$$

で表され，KeyGen オラクルは $S$ が入力されたとき，$S \notin \mathbb{A}^*$ の場合のみ個別秘密鍵を返答するオラクルであるとする．

### 6.5.3 Bethencourt-Sahai-Waters CP-ABE (BSW CP-ABE)

Ciphertext Policy における ABE を初めて提案したのは Bethencourt,Sahai,Waters である [2]．Bethencourt-Sahai-Waters CP-ABE (BSW CP-ABE) を以下に示す．

**Setup:** $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とする．$g \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$\alpha, \beta \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $h := g^\beta, f := g^{\frac{1}{\beta}}, Y := e'(g,g)^\alpha$ を求める．ハッシュ関数 $H : \{0,1\}^* \to \mathbb{G}$ を選び，$pk := (g, h, f, Y, H)$，$mk := (\beta, g^\alpha)$ とする．

$$pk = (g, T_1, \ldots, T_n, Y, H),\ mk = (t_1, \ldots, t_n, y)$$

**Enc:** $t \times \ell$ 行列 $M$ からなるアクセス構造 $\hat{M}$ に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s, u_1, \ldots, u_t \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選ぶ.
2. $\vec{u} := (u_1, \ldots, u_t)$ とする.
3. $(s_1, \ldots, s_\ell) := M \cdot \vec{u}$ とする.
4. $c_0 := m \cdot Y^s, c' := h^s, \{c_i := g^{s_i}, c_i' := H(\rho(i))^{s_i}\}_{i=1,\ldots,\ell}$ とする.
5. $C := (\hat{M}, c_0, c', \{c_i, c_i'\}_{i=1,\ldots,\ell})$ を暗号文として出力する.

**KeyGen:** 属性情報 $S$ と $mk$ を入力とし，個別秘密鍵 $sk_S$ を生成する場合，$r, r_j \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ $(j \in S)$ を選び,

$$D := g^{\frac{\alpha+r}{\beta}}, \{D_j := g^r H(j)^{r_j}\}_{j\in S}, \{D_j' := g^{r_j}\}_{j\in S}$$

を求め，$sk_S := (D, \{D_j, D_j'\}_{j\in S})$ を個別秘密鍵とする.

**Dec:** MSP が $S$ を受理する場合，$\sum_{\rho(i)\in S} \alpha_i \vec{M}_i = \vec{1}$ となる $\{\alpha_i\}_{\rho(i)\in S}$ が存在するので，この値 $\{\alpha_i\}_{\rho(i)\in S}$ を求め，暗号文 $C$ および $sk_S$ を入力として，$m' := c_0 \cdot e'(c', D)^{-1} \cdot \prod_{\rho(i)\in S} \left(\frac{e'(D_{\rho(i)}, c_i)}{e'(D'_{\rho(i)}, c_i')}\right)^{\alpha_i}$ を出力する.

BSW CP-ABE において，暗号文 $(c_0, \{c_i\}_{i\in\gamma})$ が正しく生成されているならば,

$$\begin{aligned}
m' &= c_0 \cdot e'(c', D)^{-1} \cdot \prod_{\rho(i)\in S} \left(\frac{e'(D_{\rho(i)}, c_i)}{e'(D'_{\rho(i)}, c_i')}\right)^{\alpha_i} \\
&= c_0 \cdot e'(c', D)^{-1} \cdot \prod_{\rho(i)\in S} \left(\frac{e'(g^r H(\rho(i))^{r_i}, g^{s_i})}{e'(g^{r_i}, H(\rho(i))^{s_i}}\right)^{\alpha_i} \\
&= c_0 \cdot e'(c', D)^{-1} \cdot \prod_{\rho(i)\in S} e(g,g)^{r\cdot s_i \cdot \alpha_i} \\
&= c_0 \cdot e'(h^s, g^{\frac{\alpha+r}{\beta}})^{-1} \cdot e(g,g)^{r\cdot\sum_{\rho(i)\in S} s_i\cdot\alpha_i} \\
&= m \cdot e'(g,g)^{\alpha s} \cdot e'(g,g)^{-\alpha s - rs} \cdot e'(g,g)^{rs} \\
&= m
\end{aligned}$$

として暗号文を復号することができる.

**定理 6.5.** *BSW CP-ABE* は *Generic Group Model* において *IND-AT-CPA* 安全である.

Generic Group Model とは，群上の演算を行う際にオラクルに問い合わせることで結果を受け取るモデルである．Generic Group Model ではそれぞれの群の値はある名前として表現される.

### 6.5.4 Waters CP-ABE

Waters は Ciphtertext Policy ABE に関して，Standard Model によって証明することができる方式を 2008 年に提案した [20]．今回は Waters がにおいて提案した三つ方式のうち効率的な方式について述べる．

**Setup:** $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とする．$g \xleftarrow{\mathsf{U}} \mathbb{G}$ を選び，$\alpha, \beta \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ から $h := g^\beta, h' := g^\alpha, Y := e'(g,g)^\alpha$ を求める．ハッシュ関数 $H : \{0,1\}^* \to \mathbb{G}$ を選び，$pk := (g, h, Y, H)$，$mk := h'$ とする．

$$pk = (g, h, Y, H),\ mk = h'$$

**Enc:** $t \times \ell$ 行列 $M$ からなるアクセス構造 $\hat{M}$ に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s, r_1, \ldots, r_\ell, u_1, \ldots, u_t \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選ぶ．
2. $\vec{u} := (u_1, \ldots, u_t)$ とする．
3. $(s_1, \ldots, s_\ell) := M \cdot \vec{u}$ とする．
4. $c_0 := m \cdot Y^s, c' := g^s, \{c_i := g^{r_i}, c_i' := h^{s_i} \cdot H(\rho(i))^{-r_i}\}_{i=1,\ldots,\ell}$ とする．
5. $C := (\hat{M}, c_0, c', \{c_i, c_i'\}_{i=1,\ldots,\ell})$ を暗号文として出力する．

**KeyGen:** 属性情報 $S$ と $mk$ を入力とし，個別秘密鍵 $sk_S$ を生成する場合，$t \xleftarrow{\mathsf{U}} \mathbb{Z}_p$ を選び，$D := h' \cdot h^t, D_0 := g^t, \{D_j := H(j)^t\}_{j \in S}$ を求め，$sk_S := (D, D_0, \{D_j\}_{j \in S})$ を個別秘密鍵とする．

**Dec:** MSP が $S$ を受理する場合，$\sum_{\rho(i) \in S} \alpha_i \vec{M}_i = \vec{1}$ となる $\{\alpha_i\}_{\rho(i) \in S}$ が存在するので，この値 $\{\alpha_i\}_{\rho(i) \in S}$ を求め，暗号文 $C$ および $sk_S$ を入力として，$m' := c_0 \cdot e'(c', D)^{-1} \cdot \prod_{\rho(i) \in S} (e'(c_i', D_0) \cdot e'(c_i, D_{\rho(i)})^{\alpha_i}$ を出力する．

BSW CP-ABE において，暗号文 $(c_0, c', \{c_i, c_i'\}_{i \in \gamma})$ が正しく生成されているならば，

$$\begin{aligned}
m' &= c_0 \cdot e'(c', D)^{-1} \cdot \prod_{\rho(i) \in S} (e'(c_i', D_0) \cdot e'(c_i, D_{\rho(i)}))^{\alpha_i} \\
&= c_0 \cdot e'(c', D)^{-1} \cdot \prod_{\rho(i) \in S} e'(g^\beta H(\rho(i))^{-r_i}, g^t) \cdot e'(g^{r_i}, H(\rho(i))^t)^{\alpha_i} \\
&= c_0 \cdot e'(c', D)^{-1} \cdot \prod_{\rho(i) \in S} e(g,g)^{\beta t \cdot s_i \cdot \alpha_i} \\
&= c_0 \cdot e'(g^s, g^{\alpha + \beta t})^{-1} \cdot e(g,g)^{\beta t \cdot \sum_{\rho(i) \in S} s_i \cdot \alpha_i} \\
&= m \cdot e'(g,g)^{\alpha s} \cdot e'(g,g)^{-\alpha s - \beta t s} \cdot e'(g,g)^{\beta t s} \\
&= m
\end{aligned}$$

として暗号文を復号することができる．Waters KP-ABE の安全性の根拠となる数論仮定は，decisional $q$-PBDHE(Parallel Bilinear Diffie-Hellman Exponent) 仮定である．

decisional $q$-PBDHE 仮定

$a, s, b_1, \ldots, b_q \xleftarrow{\cup} \mathbb{Z}_p$ として，$(g, g^s, Z) \in \mathbb{G}^2 \times \mathbb{G}_T$ および $A_i := \{g^{a^i}\}_{1 \le i \le q, q+2 \le i \le 2q} \in \mathbb{G}^{2q-1}$ および $B_{i,j} := \{g^{a^i \cdot b_j^{-1}}\}_{1 \le i \le q, q+2 \le i \le 2q, 1 \le j \le q} \in \mathbb{G}^{q(2q-1)}$，そして $C_{i,j} := \{g^{a^i \cdot s \cdot b_k \cdot b_j^{-1}}\}_{1 \le i,j,k \le q, j \ne k} \in \mathbb{G}^{q^2(q-1)}$ が入力された場合に，$Z = e'(g,g')^{a^{q+1}s}$ であるかを判定する問題を decisional $q$-PBDHE 問題と呼ぶ．そして，いかなる多項式時間攻撃者に対しても decisional $q$-PBDHE 問題を解くことが困難である場合，その群上において decisional $q$-PBDHE 仮定が保たれているという．

**定義 6.2.** 攻撃者 $\mathcal{A}$ の *decisional q-PBDHE* 問題に対する優位性を

$$\mathsf{Adv}_{\mathcal{A}}^{q\text{-PBDHE}}(k) := \left| \begin{array}{l} \Pr\left[ \begin{array}{l} \mathcal{A}(g, g^s, \{A_i\}_i, \{B_{i,j}\}_{i,j}, \{C_{i,j}\}_{i,j}, Z) \to 1 \mid \\ a, s, b_1, \ldots, b_q \xleftarrow{\cup} \mathbb{Z}_p; Z := e'(g,g')^{a^{q+1}s} \end{array} \right] \\ -\Pr\left[ \begin{array}{l} \mathcal{A}(g, g^s, \{A_i\}_i, \{B_{i,j}\}_{i,j}, \{C_{i,j}\}_{i,j}, Z) \to 1 \mid \\ a, s, b_1, \ldots, b_q, z \xleftarrow{\cup} \mathbb{Z}_p; Z := e'(g,g')^{z} \end{array} \right] \end{array} \right|$$

と置いたとき，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても $\mathsf{Adv}_{\mathcal{A}}^{q\text{-PBDHE}}(k) \le \epsilon(k)$ である場合，その群において *decisional q-PBDHE* 仮定が保たれているという．

**定理 6.6.** *Waters CP-ABE* は *Standard Model* において *decisional q-PBDHE* 仮定の下で *IND-sAT-CPA* である．

## 6.6 Non-monotone ABE

これまでの ABE は，monotone である場合についてのみ扱ってきた．monotone のアクセス構造では，ある集合に復号可能な属性の部分集合が含まれている場合，必ず復号可能であった．これに対し，non-monotone アクセス構造では，ブラックリストのように復号可能な属性の部分集合にある属性が追加された場合は復号不可能になる構造を持つことができる．

Non-monotone なアクセス構造を実際に構成する場合について考える．まず，アクセス木において，従来の monotone の場合，各ノードに与えられているしきい値について，子ノードの数としきい値が一致している場合は “AND”，しきい値が 1 である場合は “OR” と捉えることができる．Non-monotone を扱う場合，葉ノードに対応する属性 $\{x_1, \ldots, x_n\} \in \{0,1\}^n$ に対してその否定となる値 $\{\bar{x}_1, \cdots, \bar{x}_n\} \in \{0,1\}^n$ を入力することで，“NOT” を付け加えることができる．この場合，ある属性 $x_i$ が 1 から 0 に変化した場合，その否定である $\bar{x}_i$ が 0 から 1 に変化することで復号可能な状態

に変化する可能性が出てくる．つまり，否定となる値の情報によって non-monotone な状態を実現することができる．

一般には，non-monotone アクセス構造は Span Program (SP) で表現することができる．変数の集合が $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$ あり，行列 $M$ の行から変数の集合へラベル付けする写像 $\rho$ が存在し，属性集合が 1 の場合には $x_1$ から $x_n$ の値を，0 の場合は $\bar{x}_1$ から $\bar{x}_n$ の値を取ることで non-monotone な環境を作り出すことができる．

### 6.6.1 Ostrovsky-Sahai-Waters KP-ABE (OSW KP-ABE)

Non-monotone な KP-ABE は Ostrovsky,Sahai,Waters によって始めて構成された [15]．ここでは Span Program における Ostrovsky-Sahai-Waters KP-ABE に関して述べる．なお，この方式では「暗号文はすべて $d$ 個の属性を持つ」ことを前提としている．

**Setup:** $\mathbb{G}, \mathbb{G}_T$ を素位数 $p$ の群とする．$g \xleftarrow{\cup} \mathbb{G}$ を選び，$\beta, y \xleftarrow{\cup} \mathbb{Z}_p$ から $g_1 := g^y, g_2 := g^\beta$ を求める．次数 $d$ の多項式 $h(x), q(x)$ を $q(0) = \beta$ となるように生成する．このとき，関数

$$T(x) := g_2^{x^d} g^{h(x)},\ V(x) := g^{q(x)}$$

を定義する．これらの関数を用いて $\{g_{2,i} := g^{q(i)}, g_{3,i} := g^{h(i)}\}_{i=1,\ldots,d}$ とし，$pk := (g, g_1, g_2, \{g_{2,i}, g_{3,i}\}_{i=1,\ldots,d})$，$mk := y$ とする．

$$pk = (g, g_1, g_2, \{g_{2,i}, g_{3,i}\}_{i=1,\ldots,d}),\ mk = y$$

**Enc:** $d$ 個の属性を持つ属性情報 $S$ に対してメッセージ $m \in \mathbb{G}_T$ を暗号化する場合，

1. $s \xleftarrow{\cup} \mathbb{Z}_p$ を選ぶ．
2. $c_0 := m \cdot e'(g_1, g_2)^s, c' := g^s, \{C_j := T(j)^s, C'_j := V(j)^s\}_{j \in S}$ とする．
3. $C := (S, c_0, c', \{c_j, c'_j\}_{j \in S})$ を暗号文として出力する．

**KeyGen:** アクセス構造 $\hat{M}$ と $mk$ を入力とし，まず $y$ を $\sum_{i=1}^{\ell} s_i = y$ となるように $s_1, \ldots, s_\ell$ に分割する．個別秘密鍵の生成は，行列 $M$ の $i$ 行目からラベル付けされた変数が $x_{\rho(i)}$ であるか $\bar{x}_{\rho(i)}$ であるかで分けて考える．

ラベル付けされた変数が $x_{\rho(i)}$

$r_i \xleftarrow{\cup} \mathbb{Z}_p$ を選び，$\{D_i := g_2^{s_i} T(\rho(i))^{r_i}, D'_i := g^{r_i}\}_{i \in \{1,\ldots,\ell\}}$ として $sk_{\hat{M}} := (\{D_i, D'_i\}_{i \in \{1,\ldots,\ell\}})$ とする．

ラベル付けされた変数が $\bar{x}_{\rho(i)}$

$r_i \xleftarrow{\cup} \mathbb{Z}_p$ を選び，$\{D_i := V(\rho(i))^{r_i}, D_i' := g^{r_i}, D_i'' := g_2^{s_i+r_i}\}_{i\in\{1,\ldots,\ell\}}$ として $sk_{\hat{M}} := (\{D_i, D_i', D_i''\}_{i\in\{1,\ldots,\ell\}})$ とする．

Dec: MSP が $S$ を受理する場合，$\sum_{x_i,\bar{x}_i\in S}\alpha_i s_i = y$ となる $\{\alpha_i\}_{x_i,\bar{x}_i\in S}$ が存在するので，この値 $\{\alpha_i\}_{x_i,\bar{x}_i\in S}$ を求める．そして 暗号文 $C$ および $sk_{\hat{M}}$ を入力として，

$$m' := c_0 \prod_{x_{\rho(i)}\in S}\left(\frac{e'(D_i,c')}{e'(D_i',c_i)}\right)^{-\alpha_i} \prod_{\bar{x}_{\rho(i)}\in S}\left(\frac{e'(D_i'',c')}{e'(D_i', \prod_{x_{\rho(j)}\in S}(c_j')^{\Delta_{x,S'}(0)})\cdot e'(D_i,c')^{\Delta_{\rho(i),S}(0)}}\right)^{-\alpha_i}$$

を出力する．

BSW CP-ABE において，暗号文 $(S, c_0, c', \{c_i, c_i'\}_{i\in\gamma})$ が正しく生成されているならば，

$$\begin{aligned}\prod_{x_{\rho(i)}\in S}\left(\frac{e'(D_i,c')}{e'(D_i',c_i')}\right)^{-\alpha_i} &= \prod_{x_{\rho(i)}\in S}\left(\frac{e'(g_2^{s_i}T(\rho(i))^{r_i}, g^s)}{e'(g^{r_i}, T(\rho(i))^s)}\right)^{-\alpha_i}\\ &= \prod_{x_{\rho(i)}\in S} e'(g_2,g)^{-ss_i\alpha_i}\end{aligned}$$

である．また，$\bar{x}_{\rho(i)} \in S$ においては，属性情報の中で正の属性であるものの集合を $S' \subseteq S$ とおいたとき，$S_i := S' \cup \{\rho(i)\}$ と置くと $(|S_i| = d+1)$,

$$\begin{aligned}&\prod_{\bar{x}_{\rho(i)}\in S}\left(\frac{e'(D_i'',c')}{e'(D_i', \prod_{x_{\rho(j)}\in S'}(c_j')^{\Delta_{x,S'}(0)})\cdot e'(D_i,c')}\right)^{-\alpha_i}\\ &= \prod_{\bar{x}_{\rho(i)}\in S}\left(\frac{e'(g_2^{s_i+r_i}, g^s)}{e'(g^{r_i}, \prod_{x\in S'}V(x)^{s\Delta_{x,S'}(0)})\cdot e'(V(\rho(i))^{r_i}, g^s)^{\Delta_{\rho(i),S}(0)}}\right)^{-\alpha_i}\\ &= \prod_{\bar{x}_{\rho(i)}\in S}\left(\frac{e'(g_2^{s_i+r_i}, g^s)}{e'(g^{r_i}, g^{s\sum_{x\in S'}q(x)\Delta_{x,S'}(0)})\cdot e'(g^{r_i q(\rho(i))}, g^s)^{\Delta_{\rho(i),S}(0)}}\right)^{-\alpha_i}\\ &= \prod_{\bar{x}_{\rho(i)}\in S}\left(\frac{e'(g_2^{s_i+r_i}, g^s)}{e'(g,g)^{r_i s\sum_{x\in S_i}q(x)\Delta_{x,S_i}(0)}}\right)^{-\alpha_i}\\ &= \prod_{\bar{x}_{\rho(i)}\in S}\left(\frac{e'(g_2,g)^{s_i s+r_i s}}{e'(g,g)^{r_i s\beta}}\right)^{-\alpha_i}\\ &= \prod_{\bar{x}_{\rho(i)}\in S} e'(g_2,g)^{-ss_i\alpha_i}\end{aligned}$$

となる．よって

$$\begin{aligned} m' &= c_0 \cdot \prod_{x_{\rho(i)}, \bar{x}_{\rho(i)} \in S} e'(g_2, g)^{-ss_i\alpha_i} \\ &= c_0 \cdot e'(g_2, g)^{\sum_{x_{\rho(i)}, \bar{x}_{\rho(i)} \in S} -ss_i\alpha_i} \\ &= c_0 \cdot e'(g_2, g)^{-sy} \\ &= m \end{aligned}$$

として平文が復号される．

**定理 6.7.** *OSW KP-ABE* は *Standard Model* において *DBDH* 仮定の下で *IND-sAT-CPA* である．

## 6.7 Predicate Encryption

Predicate Encryption は，Attribute Hiding が追加された ABE である．Attribute Hiding とは，暗号文の情報から属性情報等が得られないという性質のことであり，既存の ABE にはこれらの情報が暗号文の中にそのまま埋め込まれているため Attribute Hiding を持ち得ない．既存の研究では，Predicate Encryption は内積述語と呼ばれるアクセス木の葉ノードと属性情報とが重複がないクラスにおいては，Predicate Encryption が作れることが知られている．

## 6.8 Attribute Based Signature

Attribute Based Signature は，ABE の署名版であり利用者の署名がある属性に所属していることを場合のみ署名の検証に通る署名である．Attribute Based Signature では，異なる署名鍵で署名を生成した場合，それらの署名同士が識別不可能であるという性質が求められる．

# 参考文献


[1] 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)

[2] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334. IEEE (2007)

[3] Boneh, D., Boyen, X.: Efficient selective-ID secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)

[4] Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Heidelberg (2004)

[5] Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004)

[6] Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)

[7] Boneh, D., Katz, J.: Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 87–103. Springer, Heidelberg (2005)

[8] Boyen, X.: A tapestry of identity-based encryption: Practical frameworks compared. International Journal of Applied Cryptography 1(1) pp. 3–21 (2008)

[9] Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 207–222. Springer, Heidelberg (2004)

[10] Chen, L., Cheng, Z.: Security proof of sakai-kasahara's identity-based encryption scheme. Cryptology ePrint Archive, Report 2005/226 (2005)

[11] Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (1999)

[12] Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)

[13] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: 13th ACM Conference on Computer and Communications Security, pp. 89–98. ACM Press (2006)

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

[15] Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: 14th ACM Conference on Computer and Communications Security, pp. 195–203. ACM Press (2007)

[16] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)

[17] Sakai, R., Kasahara, M.: ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054 (2003)

[18] Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: Symposium on Cryptography and Information Security. (2000)

[19] Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)

[20] Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Cryptology ePrint Archive, Report 2008/290 (2009)