Vol.2019-CSEC-87 No.1
2019/12/3

格子問題に基づくSemi-Adaptive安全な内積暗号

宮澤 智輝[1,a)]　佐藤　慎悟[1,b)]　四方　順司[1,2,c)]

概要：近年，量子コンピュータの開発が活発に行われており，耐量子性を持つ暗号方式の研究が注目されている．格子暗号は格子問題の困難性に基づく暗号であり，耐量子性を持つ暗号であるだけでなく，高機能暗号の構成が可能という特徴を持つ．内積暗号は暗号文と秘密鍵に属性ベクトルを埋め込み，復号条件を指定して暗号化を行うことができる高機能暗号である．2008 年に Katz, Sahai, Waters は内積を述語として扱う内積暗号を提案した．2011 年に Agrawal, Freeman,Vaikuntanathan は格子問題に基づいた内積暗号を提案し，2013 年に草川は鍵長の効率性を改善した構成法を提案しているが，いずれも selective 安全性を達成している．本論文では公開パラメータの値を得てから攻撃対象の属性ベクトルを決定する semi-adaptive 安全な（selective 安全性よりも強い安全性概念）格子問題に基づく内積暗号を構成し，その安全性証明を行う．

Semi-Adaptively Secure Inner-Product Encryption from Lattices

Abstract: Recently, quantum computers have been actively developed, and post-quantum cryptography has been focused on. Lattice-based cryptography is the one based on difficulty of lattice problems, and it is expected to have security against quantum computers as well as providing advanced functionalities in encryption. The inner-product encryption (IPE) is a functional encryption where we can specify decryption conditions by embedding attribute vectors in private keys and ciphertexts. In 2008, Katz, Sahai, and Waters proposed IPE which treats inner-products as predicates. Agrawal, Freeman, and Vaikuntanathan proposed a lattice-based IPE in 2011, and Xagawa proposed an improved lattice-based IPE in terms of key-size in 2013. It should be noted that the previous works achieved selective security for lattice-based IPE. In this paper, we propose a lattice-based IPE with semi-adaptive security, where an adversary can select a target attribute vector after seeing public parameters, which is stronger than IPE with selective security.

1. はじめに

近年，量子コンピュータの開発が活発に行われている．量子コンピュータの実現を考えると，量子コンピュータを用いても破ることが困難な耐量子性を持つ暗号方式の研究が必要である．耐量子性を持つ暗号の 1 つに格子暗号がある．格子暗号は格子問題の困難性に基づく暗号であり，耐量子性に加え，従来の暗号技術に付加機能を追加した高機能暗号の実現が可能という特徴をもつ．

2008 年に Katz, Sahai，Waters は内積を述語として扱う内積暗号 [4] の概念を導入した．内積暗号は暗号文と秘密鍵にそれぞれ属性ベクトルを埋め込んでおき，その内積値によって復号可能かどうかを制御するアクセスコントール機能を持つ公開鍵暗号である．2 つの属性ベクトルによって復号条件を指定して暗号化を行うことができるため，従来の 1 対 1 で公開鍵，秘密鍵のペアを生成する公開鍵暗号と比べて利便性が高いと考えられている．また，述語暗号は暗号文に埋め込んだ属性の情報が得られないという特徴がある．このような特徴から暗号文に埋め込む属性を秘匿するようなファイル管理サービスなどへの応用が期待されている．

2011 年に Agrawal, Freeman, Vaikuntanathan は格子問題に基づく内積暗号 [2] を初めて提案した．2013 年に草川は鍵長の効率性を改善した格子問題に基づく内積暗号 [9] を提案した．これは可逆差分符号化を構成で用いることで効率性を改善している．いずれも selective 安全性を満たし

[1] 横浜国立大学大学院環境情報学府/研究院
Graduate School of Environment and Information Sciences, Yoko hama National University
[2] 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University
a) miyazawa-tomoki-vb@ynu.jp
b) sato-shingo-cz@ynu.jp
c) shikata-junji-rb@ynu.ac.jp

ⓒ 2019 Information Processing Society of Japan

ている．

一方，属性とそのアクセス構造によってアクセスコントロール機能を持つ属性ベース暗号の概念は 2005 年に Sahai, Waters によって導入された [8]．格子問題に基づく属性ベース暗号についても研究がされており，2016 年に Brakerski, Vaikuntanathan は安全性を引き上げた semi-adaptive 安全を達成する格子問題に基づく属性ベース暗号 [3] を提案した．

本論文では semi-adaptive 安全な格子問題に基づく内積暗号を初めて提案する． [3] と比較し，暗号文に埋め込んだ属性の情報が漏れないという利点を持つ．selective 安全性では攻撃者が公開パラメータの値を知る前に攻撃対象の属性ベクトルを決定する攻撃を想定している．これより高い安全性である semi-adaptive 安全性を達成するために，属性ベース暗号において semi-adaptive 安全を達成する構成である [3] の属性と乱数の排他的論理和を属性として暗号化を行う手法を内積暗号に適用する．

2. 準備

PPT は Probabilistic Polynomial Time の略である．$\lfloor x \rceil = \lceil x - 1/2 \rceil$ と定義する．2 つの行列 $X \in \mathbb{R}^{n\times m_1}, Y \in \mathbb{R}^{n\times m_2}$ に対し，$[X|Y] \in \mathbb{R}^{n\times(m_1+m_2)}$ を X と Y の列の連結とする．2 つの行列 $X \in \mathbb{R}^{n_1\times m}, Y \in \mathbb{R}^{n_2\times m}$ に対し，$[X;Y] \in \mathbb{R}^{(n_1+n_2)\times m}$ を X と Y の行の連結とする．$\boldsymbol{x} \in \mathbb{R}^m$ に対して $||\boldsymbol{x}||$ をベクトル $\boldsymbol{x}$ の l_2 ノルムとする．行列 $\boldsymbol{X} \in \mathbb{R}^{m\times n}$ に対して $\tilde{\boldsymbol{X}}$ をグラム・シュミットの正規直交化法で得られる基底とする．行列 $\boldsymbol{X} = [\boldsymbol{x}_1; \cdots; \boldsymbol{x}_m] \in \mathbb{R}^{m\times n}$ に対して，$||\boldsymbol{X}||_{\mathrm{row}}$ を $\max_i ||\boldsymbol{x}_i||$ とする．行列 $\boldsymbol{X} \in \mathbb{R}^{m\times n}$ に対して $s_1(\boldsymbol{X}) = \sup_{\boldsymbol{u}\in\mathbb{R}^n, ||\boldsymbol{u}||=1} ||\boldsymbol{X}\boldsymbol{u}|| = \sup_{\boldsymbol{u}'\in\mathbb{R}^m, ||\boldsymbol{u}'||=1} ||\boldsymbol{X}^\top \boldsymbol{u}'||$ とする．行列 $\boldsymbol{X} \in \mathbb{R}^{n\times m}$，$\boldsymbol{Y} \in \mathbb{R}^{m\times k}$ に対して $s_1(\boldsymbol{XY}) \le s_1(\boldsymbol{X}) \cdot s_1(\boldsymbol{Y})$ である．λ をセキュリティパラメータとし，ある関数 $f(\lambda)$ に対して $f(\lambda) < \lambda^{-c}$ であるとき，関数 $f(\lambda)$ は無視できるほど小さいと定義する．ここで c は任意の定数である．無視できるほど小さい関数を $\mathrm{neg}(\lambda)$ と定義する．ある確率が $1 - \mathrm{neg}(\lambda)$ のとき，圧倒的確率と定義する．確率変数 X, Y，有限集合 I に対し，統計的距離を次のように定義する．

$$\Delta(X,Y) = \frac{1}{2}\sum_{i\in I} |\Pr[X=i] - \Pr[Y=i]|.$$

X, Y の統計的距離が無視できるほど小さいとき $X \approx_s Y$ とする．

有限集合 S に対して，$U(S)$ を S 上の一様分布と定義する．一様分布から $neg(\lambda)$ 離れている分布を $\mathrm{neg}(\lambda)$-uniform と定義する．平均 0，分散 s^2 のガウス分布 $N(0,s^2)$ は $\mathbb{R}$ 上の確率密度関数 $(1/s\sqrt{2\pi}) \cdot \exp(-x^2/2s^2)$ によって定義される．$\alpha \in (0,1)$，正の整数 q に対して離散ガウス $\bar{\Psi}_\alpha$ を $N(0, \alpha^2/2\pi)$ から x をサンプリングし，$\lfloor qx \rceil \bmod q$ を出力する分布として定義する．正の実数 s に対して n 次元ガウス関数を $\rho_s(\boldsymbol{x}) = \exp(-\pi||\boldsymbol{x}||^2/s^2)$ として定義する．正の実数 s，可算集合 A に対して離散ガウス分布 $D_{A,s}$ を $D_{A,s}(\boldsymbol{x}) = \frac{\rho_s(\boldsymbol{x})}{\sum_{\boldsymbol{y}\in A}\rho_s(y)}$ と定義する．

3. 格子

$\mathbb{R}^n$ 上の格子は $\boldsymbol{\Lambda} = \{\Sigma_{i=1}^n x_i \boldsymbol{b}_i : x_i \in \mathbb{Z}\}$ によって定義される．ここで，$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^n$ は $\mathbb{R}^n$ 上の線形独立なベクトルであり，行列 $\boldsymbol{B} = [\boldsymbol{b}_1 \cdots \boldsymbol{b}_n]$ を格子 $\boldsymbol{\Lambda}$ の基底という．$\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}, \boldsymbol{u} \in \mathbb{Z}_q^n$ に対して次の格子を定義する．

$$\boldsymbol{\Lambda}_q(\boldsymbol{A}) = \{\boldsymbol{y} \in \mathbb{Z}^m : \exists \boldsymbol{s} \in \mathbb{Z}_q^n \ \ s.t.\ \boldsymbol{y} \equiv \boldsymbol{A}^\top \boldsymbol{s} \pmod q\},$$
$$\boldsymbol{\Lambda}_q^\perp(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}^m : \boldsymbol{Ae} \equiv \boldsymbol{0} \pmod q\},$$
$$\boldsymbol{\Lambda}_q^{\boldsymbol{u}}(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}^m : \boldsymbol{Ae} \equiv \boldsymbol{u} \pmod q\}.$$

定理 1. ([6], 定理 4.1) 整数 $q \ge 2, n \ge 1, k = \lceil \log q \rceil, \bar{m} = nk$ とし，$\boldsymbol{g}^\top = (1, 2, \ldots 2^{k-1}) \in \mathbb{Z}^k, \boldsymbol{G} = \boldsymbol{I}_n \bigotimes \boldsymbol{g}^\top$ とする．このとき，格子 $\boldsymbol{\Lambda}_q^\perp(\boldsymbol{G})$ は既知の基底 $\boldsymbol{S} \in \mathbb{Z}^{\bar{m}\times\bar{m}}$ を持ち，$||\tilde{\boldsymbol{S}}|| \le \sqrt{5}, ||\boldsymbol{S}|| \le \max\{\sqrt{5}, \sqrt{k}\}$ を満たす．

定義 1. ([6], 定義 5.2) 行列 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}, \boldsymbol{G} \in \mathbb{Z}_q^{n\times w}$ とする．m, w, n は $m \ge w \ge n$ を満たす正の整数である．$\boldsymbol{R} \in \mathbb{Z}^{(m-w)\times w}, \boldsymbol{H} \in \mathrm{GL}_n(\mathbb{Z}_q) \subset \mathbb{Z}_q^{n\times n}$ としたとき，$\boldsymbol{A}[\boldsymbol{R}; \boldsymbol{I}_w] = \boldsymbol{HG}$ となる関係を $\boldsymbol{G}$-トラップドアタグ $\boldsymbol{H}$ という．トラップドアは $s_1(\boldsymbol{R})$ によって評価される．

定理 2. ([6]) $k = \lceil \log q \rceil, m = \bar{m} + nk$ とする．

- $\mathrm{GenTrap}^D(\bar{\boldsymbol{A}}, \boldsymbol{H}) \to (\boldsymbol{A}, \boldsymbol{R})$： GenTrap アルゴリズムは入力として行列 $\bar{\boldsymbol{A}} \in \mathbb{Z}_q^{n\times\bar{m}}$，可逆行列 $\boldsymbol{H} \in \mathrm{GL}_n(\mathbb{Z}_q)$ を入力とし，D を $\mathbb{Z}_q$ 上の確率分布とする．出力として，$\boldsymbol{A} = [\bar{\boldsymbol{A}}|\boldsymbol{HG} - \bar{\boldsymbol{A}}\boldsymbol{R}] \in \mathbb{Z}_q^{n\times(\bar{m}+nk)}$ と，トラップドア $\boldsymbol{R}$ を出力する．ここで，$\boldsymbol{R}$ は確率分布 D から選ばれる．特に q を奇素数とし，$\bar{m} = n\log q + \omega(\log\lambda), D = U(\{-1, +1\})$ として，$\bar{\boldsymbol{A}}$ を $\mathbb{Z}_q^{n\times\bar{m}}$ から一様ランダムに選ぶと，$\boldsymbol{A}$ は $\mathrm{neg}(\lambda)$-uniform であり，圧倒的確率で $s_1(\boldsymbol{R}) \le C(\sqrt{\bar{m}} + \sqrt{nk})$ を満たす．
- $\boldsymbol{x} \leftarrow \mathrm{SampleD}(\boldsymbol{R}, \boldsymbol{A}, \boldsymbol{H}, \boldsymbol{u}, s)$：SampleD アルゴリズムは $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ とそのトラップドア $\boldsymbol{R} \in \mathbb{Z}_q^{\bar{m}\times nk}$ タグ $\boldsymbol{H} \in \mathrm{GL}_n(\mathbb{Z}_q)$，ベクトル $\boldsymbol{u} \in \mathbb{Z}_q^n$，ガウシアンパラメータ $s > \sqrt{s_1(\boldsymbol{R})^2 + 1} \cdot \sqrt{7} \cdot \omega(\sqrt{\log n})$ を入力とする．出力として，統計的に $D_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}),s}$ に近い分布に従って $\boldsymbol{x}$ を出力する．つまり，$\boldsymbol{Ax} = \boldsymbol{u}$ となるように $D_{\mathbb{Z}_q,s}^m$ から $\boldsymbol{x}$ をサンプリングする．

4. Learning With Errors(LWE)

learning with errors (LWE) は [7] によって提案された問題である．ベクトル $\boldsymbol{s} \in \mathbb{Z}_q^n$ と $\mathbb{Z}_q$ 上の確率分布 χ に対して，$\mathbb{Z}_q^n \times \mathbb{Z}_q$ 上の分布 $A(\boldsymbol{s}, \chi)$ は $\boldsymbol{a} \leftarrow \mathbb{Z}_q^n$ と $x \leftarrow \chi$ をサンプリングし，$(\boldsymbol{a}, \boldsymbol{a}^\top \boldsymbol{s} + x)$ を出力する．

定義 2. 整数 $q = q(n), \mathbb{Z}_q$ 上の確率分布 χ から与えられる

LWE 問題 $\mathrm{LWE}(q,\chi)$ は一様ランダムな $\boldsymbol{s}\in\mathbb{Z}_q^n$ が与えられたとき，オラクル $A(\boldsymbol{s},\chi)$ とオラクル $U(\mathbb{Z}_q^n\times\mathbb{Z}_q)$ を識別する問題である．LWE 問題の PPT 攻撃者 $\mathcal{A}$ に対してアドバンテージを次のように定義する．

$$\mathrm{Adv}_{\mathcal{A},\mathrm{LWE}(q,\chi)}(n)=|\Pr[\mathcal{A}^{\mathrm{A(s,\chi)}}(1^n)=1]-\Pr[\mathcal{A}^{U(\mathbb{Z}_q^n\times\mathbb{Z}_q)}(1^n)=1]|.$$

$\mathrm{Adv}_{\mathcal{A},\mathrm{LWE}(q,\chi)}(n)$ が無視できるほど小さいとき，LWE 仮定が成り立つと言う．

5. 述語暗号

ここでは述語暗号について説明する．$P:\Phi\times\Sigma\to\{0,1\}$ を述語とする．ここで，Φ は鍵属性空間，Σ は暗号文属性空間，$\mathcal{M}$ は平文空間を示す．述語 P に対する述語暗号は次の 4 つの多項式時間アルゴリズムからなる．

$(pp,msk)\leftarrow\mathrm{Setup}(1^\lambda)$： Setup アルゴリズムは入力としてセキュリティパラメータ λ を受け取り，公開パラメータ pp とマスター秘密鍵 msk を出力する．

$sk_\phi\leftarrow\mathrm{KeyGen}(msk,\phi)$： KeyGen アルゴリズムは入力として msk，鍵属性 $\phi\in\Phi$ を受け取り，秘密鍵 sk_ϕ を出力する．

$ct\leftarrow\mathrm{Enc}(pp,\sigma,M)$： Enc アルゴリズムは入力として pp，暗号文属性 $\sigma\in\Sigma$，平文 $M\in\mathcal{M}$ を受け取り，暗号文 ct を出力する．

$M\mathrm{or}\perp\leftarrow\mathrm{Dec}(sk_\phi,ct)$： Dec アルゴリズムは入力として秘密鍵 sk_ϕ，暗号文 ct を受け取り，復号結果 $M\in\mathcal{M}$ か復号不可能シンボル $\perp$ を出力する．

定義 3. 述語暗号の正当性を次のように定義する．任意の $\phi\in\Phi,\sigma\in\Sigma$ に対して $(pp,msk)\leftarrow\mathrm{Setup}(1^\lambda)$，$sk_\phi\leftarrow\mathrm{KeyGen}(msk,\phi)$，$ct\leftarrow\mathrm{Enc}(pp,\sigma,M)$，$P(\phi,\sigma)=1$ のとき，

$$\Pr\left[M=\tilde{M}:\tilde{M}\leftarrow\mathrm{Dec}(sk_\phi,ct)\right]$$

を圧倒的確率で満たす．$P(\phi,\sigma)=0$ のとき，

$$\Pr\left[\tilde{M}=\perp:\tilde{M}\leftarrow\mathrm{Dec}(sk_\phi,ct)\right]$$

を圧倒的確率で満たす．

定義 4. 上記の述語暗号の安全性ゲームとして次のものを考える．

(1) 挑戦者は $(pp,msk)\leftarrow\mathrm{Setup}(1^\lambda)$ を生成し，pp を攻撃者へ送信する．

(2) 攻撃者は任意の回数の秘密鍵クエリを発行する．秘密鍵クエリでは，挑戦者に鍵属性 ϕ_i を送信し，それを受信した挑戦者は $sk_{\phi_i}\leftarrow\mathrm{KeyGen}(msk,\phi_i)$ を生成し，sk_{ϕ_i} を攻撃者へ送信する．

(3) 攻撃者は暗号文属性のペア σ_0，σ_1 と平文のペア M_0 と M_1 を挑戦者に送信する．挑戦者は一様ランダムに $b\in\{0,1\}$ を選び，暗号文 $ct=\mathrm{Enc}(pp,\sigma_b,M_b)$ を計算し，ct を攻撃者へ送信する．

(4) 攻撃者はステップ *2* のように任意の回数の秘密鍵クエリを発行する．

(5) 攻撃者は b を推測し，$b'\in\{0,1\}$ を出力する．

攻撃者は $P(\phi_i,\sigma_0)=P(\phi_i,\sigma_1)=0$ の条件を満たすクエリのもとで b を推測する必要がある．安全性ゲームにおいて攻撃者 $\mathcal{A}$ のアドバンテージは $|\Pr[b'=1|b=1]-\Pr[b'=1|b=0]|$ である．上記の安全性ゲームは adaptive 安全性ゲームである．攻撃者が挑戦者に暗号文属性のペア σ_0，σ_1 を送信するタイミングによって別の安全性ゲームが定義される．ステップ *1* の前に攻撃者が暗号文属性のペア σ_0，σ_1 を送信するものを selective 安全性ゲームという．ステップ *2* の前に攻撃者が暗号文属性のペア σ_0，σ_1 を送信するものを semi-adaptive 安全性ゲームという．全ての PPT 攻撃者 $\mathcal{A}$ に対して $\mathcal{A}$ のアドバンテージが無視できるほど小さいとき，述語暗号は wAH- adaptive /selective /semi-adaptive - CPA 安全である．wAH は weakly attribute hiding の略である．

6. 可逆差分符号化の疑似可換性

[9] で提案された任意の a に対し，$H(a)\cdot\mathrm{G}=\mathrm{G}\cdot\mathrm{H_g(a)}$ を満たし，$s_1(H_g(a))$ が小さい H,H_g を定義する．

6.1 可逆差分符号化 H

$H:\mathrm{GF}(q^n)\to\mathbb{Z}_q^{n\times n}$ を用いて符号化を行うことを考える．任意の *2* つの多項式 $a\neq a'\in\mathrm{GF}(q^n)$ に対して，$H(a)-H(a')$ が常に可逆であるとき，H を可逆差分という．

符号化に用いる演算として [5] で提案された Rot を定義する．有限環 $R=\mathbb{Z}_q[X]/\langle g\rangle$ を考える．ここで，$g\in\mathbb{Z}_q[X]$ は n 次モニック多項式である．q が素数かつ，g が $\mathbb{Z}_q$ 上で既約である場合，環 R は $\mathrm{GF}(q^n)$ である．写像 $\tau:R\to\mathbb{Z}_q^n$ を $a=a_0+a_1X+\cdots+a_{n-1}X^{n-1}\mapsto(a_0,\ldots,a_{n-1})^\top$ と定義する．$\mathrm{Rot}:R\to\mathbb{Z}_q^{n\times n}$ を次のように定義する．

$$a=a_0+a_1X+\cdots+a_{n-1}X^{n-1}\mapsto[\tau(a)\ \tau(aX)\ \ldots\tau(aX^{n-1})].$$

$H(a):=\mathrm{Rot}(a)$ とすると，任意の $a\neq a'$ に対して $H(a)-H(a')=H(a-a')$ を満たす．また，任意の定数 $a\in\mathbb{Z}_q\subset\mathrm{GF}(q^n)$ に対して，$H(a)=a\boldsymbol{I}_n$ を満たす．

演算の特徴として次の式が成り立つ．

$$H(a)\cdot H(b)=H(ab),H(a)+H(b)=H(a+b).$$

6.2 符号化 H_g

H_g は $H_g:\mathrm{GF}(q^n)\to\{0,1,\ldots,b-1\}^{nk\times nk}$ で定義される写像であり，$\boldsymbol{G},H$ に対して疑似可換性を持つ．ここで，$b\geq2$ は正の整数であり，$\boldsymbol{B}$ を $\{0,1,\ldots,b-1\}\subset\mathbb{Z}_q$ とす

る．$k = \lceil \log_b q \rceil$，$\boldsymbol{g}^\top = (1, b, \ldots, b^{k-1})$ とすると，[6] で提案されたガジェット行列 $\boldsymbol{G} \in \mathbb{Z}_q^{n \times nk}$ は次のように定義される．

$$\boldsymbol{G} = \boldsymbol{I}_n \otimes \boldsymbol{g}^\top = \begin{bmatrix} 1\ b \cdots b^{k-1} & & & \\ & 1\ b \cdots b^{k-1} & & \\ & & \ddots & \\ & & & 1\ b \cdots b^{k-1} \end{bmatrix}$$

$a \in \mathbb{Z}_q$ に対してその b-ary 分解を $d_g(a) = (a_1, \ldots, a_k)^\top \in \boldsymbol{B}^k$ とすると，$\boldsymbol{g} \cdot d_g(a) = \Sigma_{i=1}^k a_i \cdot b^{i-1} = a$ を満たす．写像 D_g を次のように定義する．

$$D_g : a \in \mathbb{Z}_q \mapsto [d_g(a)\ d_g(ba)\ \ldots\ d_g(b^{k-1}a)] \in \boldsymbol{B}^{k \times k}.$$

D_g の定義から $\boldsymbol{g} \cdot D_g(a) = (a, ba, \ldots, b^{k-1}a) = a \cdot \boldsymbol{g}$ を満たし，疑似可換性を与えている．

D_g を拡張し，$\mathbb{Z}_q^{n \times m}$ を定義域とすると任意の行列 $\boldsymbol{A} = \{a_{i,j}\} \in \mathbb{Z}_q^{n \times m}$ に対して次の式が得られる．

$$D_g(\boldsymbol{A}) = \begin{bmatrix} D_g(a_{1,1}) & D_g(a_{1,2}) & \cdots & D_g(a_{1,m}) \\ D_g(a_{2,1}) & D_g(a_{2,2}) & \cdots & D_g(a_{2,m}) \\ \vdots & \vdots & \ddots & \vdots \\ D_g(a_{n,1}) & D_g(a_{n,2}) & \cdots & D_g(a_{n,m}) \end{bmatrix}$$

H_g を多項式から行列への写像として次のように定義する．

$$H_g : a = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathrm{GF}(q^n) \mapsto D_g(\mathrm{Rot}(a)).$$

写像 H_g は $\boldsymbol{G}, H$ に対して疑似可換性を持つ．

補題 1. ([9]，補題 4.1) $\boldsymbol{G} = \boldsymbol{I}_n \otimes \boldsymbol{g}^\top \in \mathbb{Z}_q^{n \times nk}$ とすると，任意の $a \in \mathrm{GF}(q^n)$ に対して $\boldsymbol{G} \cdot H_g(a) = H(a) \cdot \boldsymbol{G}$ を満たす．

補題 2. ([9]，補題 4.2) 任意の $a \in \mathrm{GF}(q^n)$ に対して，$||H_g(a)||_{\mathrm{row}} \leq (b-1) \cdot \sqrt{nk}$，$s_1(H_g(a)) \leq (b-1)nk$ を満たす．

7. 証明のための補題

ここでは，これまで証明で用いられ，本論文でも利用する補題について述べる．

補題 3. ([1]，補題 12) λ をセキュリティパラメータとする．z を $\mathbb{Z}^m$ 上の任意のベクトルとする．$\alpha \in (0,1), q$ を正の整数とする．$\boldsymbol{e}$ を確率分布 $\bar{\Psi}_\alpha^m$ に従う確率変数とすると，圧倒的確率で次の式が成り立つ．

$$|\langle \boldsymbol{e}, \boldsymbol{z} \rangle| \leq ||\boldsymbol{z}||(q\alpha \cdot \omega(\sqrt{\log \lambda}) + \sqrt{m}/2),$$
$$||\boldsymbol{e}|| \leq \sqrt{m}(q\alpha \cdot \omega(\sqrt{\log \lambda}) + 1/2)$$

ここで，$|\langle \boldsymbol{e}, \boldsymbol{z} \rangle|$ は $[-(q-1)/2, (q-1)/2]$ の整数として扱う．また，確率分布 $\bar{\Psi}_\alpha$ からのサンプルは少なくとも $q\alpha \cdot \omega(\sqrt{\log \lambda}) + 1/2$ の絶対値を圧倒的確率で持つ．

補題 4. ([1]，補題 13，補題 14) q を奇素数とする．$m = (n+t)\log q + \omega(\log q), \boldsymbol{R}$ を $m \times \bar{m}$ の行列とし，それぞれの列が少なくとも m の min-entropy を持つ．$\boldsymbol{A}$，$\boldsymbol{B}$ をそれぞれ $\mathbb{Z}_q^{n \times m}, \mathbb{Z}_q^{n \times \bar{m}}$ から一様ランダムに選んだ行列とする．このとき，任意の正の整数 t と任意の行列 $W \in \mathbb{Z}_q^{m \times t}$ に対して次の式が成り立つ．

$$\Delta((\boldsymbol{A}, (AR), \boldsymbol{R}^\top \boldsymbol{W}), (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{R}^\top \boldsymbol{W})) \leq \frac{\bar{m}}{2} \cdot 2^{-\frac{1}{2}(m-(n+t)\log q)} = 2^{-\omega(\log \lambda)}$$

補題 5. ([1]，補題 15) $R \leftarrow \{-1, +1\}^{n \times m}$ としたとき，圧倒的確率で $s_1(\boldsymbol{R}) \leq C(\sqrt{n} + \sqrt{m})$ を満たす定数 C が存在する．

8. Semi-Adaptive 安全な内積暗号の構成法

8.1 提案構成法

[9] で提案された内積暗号スキームに [3] で提案された Semi-Adaptive 安全を達成するためのテクニック (属性 x を $x \oplus \Delta$ として暗号化し，Δ を暗号文に埋め込む手法) を組み合わせて Semi-Adaptive 安全な内積暗号を構成する．暗号文属性を $\vec{w}$，鍵属性を $\vec{v}$ とする．乱数 $\vec{\Delta}$ を用いて，暗号文属性を $\vec{w} + \vec{\Delta}$ として暗号化を行う．正しく内積暗号として動作するために次式を満たす必要がある．

$$(\vec{w} + \vec{\Delta})^\top \vec{v} = \vec{w}^\top \vec{v}.$$

この条件を満たすため，属性 $\vec{w}, \vec{v}$ に調整要素を加えた $\vec{w'} = [\vec{w}; 0], \vec{v'} = [\vec{v}; v_{\mu+1}]$ を定義する．ここで μ は属性の要素数であり，$v_{\mu+1}$ は $\sum_{i=1}^{\mu+1} v_i \Delta_i = 0$ となるような $v_{\mu+1}$ である．$\vec{w'}, \vec{v'}$ を用いて内積の計算を行うと，

$$(\vec{w'} + \vec{\Delta})^\top \vec{v'} = \vec{w'}^\top \vec{v'} + \vec{\Delta}^\top \vec{v'} = \vec{w}^\top \vec{v}$$

となり，正しく内積の計算を行うことが可能である．

$\vec{\Delta}$ の値は秘密鍵 $sk_{\vec{v}}$ に含まれており，暗号化アルゴリズム Enc では未知の値である．そのため，直接 $\vec{\Delta}$ を利用して暗号化することはできない．この問題を解決するために，ビット分解して暗号化を行い，復号時に再構成する手法を用いて $\vec{\Delta}$ を暗号文に埋め込んでいる．$\vec{\Delta}$ については 0, 1 の両方の場合について暗号文を生成しておき，selective 安全な鍵ポリシー属性ベース暗号 (KP-ABE) を用いて正しい $\vec{\Delta}$ の値に対応する要素のみ復号時に得られる仕組みを用いることで，暗号文属性を $\vec{w} + \vec{\Delta}$ として暗号化した暗号文が得られる．

提案構成法では selective 安全な KP-ABE を使用する．KP-ABE の秘密鍵に埋め込む関数として $\mathrm{BitCheck}_\Delta(l, i, \gamma, b)$ を定義する．ここで $b \in \{0, 1\}$ である．この関数は Δ のビット長 $|\Delta| = l$ かつ，$\Delta_{i,\gamma} = b$ のとき，1 を返し，それ以外のときに 0 を返す関数である．

$k = \lceil \log q \rceil$ としたとき，$a \in \mathrm{GF}(q^n)$ の各ビット $a_\gamma \in$

$\{0,1\}$，$\gamma \in \{1,\ldots,nk\}$ に対して $\mathrm{con}_{\gamma,k} : \mathbb{Z}_q \to \mathrm{GF}(q^n)$ を次のように定義する．

$$\mathrm{con}_{\gamma,k}(a) = 2^{(\gamma-1 \bmod k)} a X^{\lfloor \frac{\gamma-1}{k} \rfloor}$$

$\mathrm{con}_{\gamma,k}$ は $a = \Sigma_{\gamma=1}^{nk} \mathrm{con}_{\gamma,k}(a_\gamma)$ を満たす．$a, b \in \mathrm{GF}(q^n)$ に対して次の式が成り立つ．

$$a + b = \Sigma_{\gamma=1}^{nk} \mathrm{con}_{\gamma,k}(a_\gamma + b_\gamma)$$

パラメータとして，$k = \lceil \log q \rceil$，$\zeta = \omega(\sqrt{\log(2m)})$，$m = 3n \log q$，$s = 3(\mu+1)Cm^{5/2} \cdot \zeta$，$q = 60C^2(\mu+1)^2 \cdot m^6 \cdot \zeta$，$\alpha = (120C^2(\mu+1)^2 m^{11/2} \cdot \zeta^2)^{-1}$ とし，4 つのアルゴリズム Setup，KeyGen，Enc，Dec を次のように構成する．

$(pp, msk) \leftarrow \mathrm{Setup}(1^\lambda)$:

(1) $(\boldsymbol{A}, \boldsymbol{R_A}) \leftarrow \mathrm{GenTrap}(1^\lambda)$

(2) $(abepp, abemsk) \leftarrow \mathrm{ABE.Setup}(1^\lambda)$

(3) $\boldsymbol{B}_{i,\gamma} \xleftarrow{U} \mathbb{Z}_q^{n \times nk}$ for $i = 1,\ldots,\mu+1$, $\gamma = 1,\ldots,nk$

(4) $\boldsymbol{U} = [\boldsymbol{u}_1|\cdots|\boldsymbol{u}_l] \xleftarrow{U} \mathbb{Z}_q^{n \times l}$

(5) $r_i \xleftarrow{U} \mathrm{GF}(q^n)$ for $i = 1,\ldots,\mu+1$ をランダムに選び，$\vec{r} = (r_1,\ldots,r_{\mu+1})$ とする．ただし，$r_{\mu+1} \neq 0$ とする．

(6) $pp = (\boldsymbol{A}, \{\boldsymbol{B}_{i,\gamma}\}_{i \in \{1,\ldots,\mu+1\}, \gamma \in \{1\ldots,nk\}}, \boldsymbol{U}, abepp)$, $msk = (\boldsymbol{R_A}, abemsk, \vec{r})$ を出力する．

$sk_{\vec{v}} \leftarrow \mathrm{KeyGen}(msk, \vec{v} = (v_1,\ldots,v_\mu)^\top \in \mathrm{GF}(q^n)^\mu)$:

(1) $\vec{\Delta} = \vec{r}$ とする．

(2) $v_{\mu+1} \leftarrow -\frac{1}{\Delta_{\mu+1}} \Sigma_{i=1}^{\mu} v_i \Delta_i$ を計算し，$\vec{v'} = [\vec{v}; v_{\mu+1}]$ とする．

(3) $abesk_\Delta \leftarrow \mathrm{ABE.KeyGen}(abemsk, \mathrm{BitCheck}_\Delta)$

(4) $\boldsymbol{B}_{\vec{v}} \leftarrow \Sigma_{i=1}^{\mu+1}(\Sigma_{\gamma=1}^{nk} \boldsymbol{B}_{i,\gamma}) H_g(v'_i) \in \mathbb{Z}_q^{n \times nk}$ を計算し，$\boldsymbol{A}_{\vec{v}} = [\boldsymbol{A}|\boldsymbol{B}_{\vec{v}}] \in \mathbb{Z}_q^{n \times (m+nk)}$ とする．

(5) $\boldsymbol{e}_i \leftarrow \mathrm{SampleD}(\boldsymbol{R_A}, \boldsymbol{A}_{\vec{v}}, \boldsymbol{I}, \boldsymbol{u}_i, s)$ for $i = 1,\cdots,l$ $\boldsymbol{E}_{\vec{v}} = [\boldsymbol{e}_1|\cdots|\boldsymbol{e}_l]$ とする．

(6) $sk_{\vec{v}} = (\vec{v'}, \boldsymbol{E}_{\vec{v}}, \vec{\Delta}, abesk_\Delta)$ を出力する．

ここで，$\boldsymbol{A}_{\vec{v}} \cdot \boldsymbol{E}_{\vec{v}} = \boldsymbol{U}$ である．

$ct \leftarrow \mathrm{Enc}(pp, \vec{w} = (w_1,\ldots,w_\mu)^\top \in \mathrm{GF}(q^n)^\mu, \boldsymbol{M} \in \{0,1\}^l)$:

(1) 属性ベクトルを拡張し，$\vec{w'} = [\vec{w}; 0]$ とする．

(2) $\boldsymbol{s} \xleftarrow{U} \mathbb{Z}_q^n$

(3) $\boldsymbol{c}_0 \leftarrow \boldsymbol{A}^\top \boldsymbol{s} + \boldsymbol{x}_0 \in \mathbb{Z}_q^m$ where $\boldsymbol{x}_0 \leftarrow \chi^m$

(4) $\boldsymbol{c}' \leftarrow \boldsymbol{U}^\top \boldsymbol{s} + \boldsymbol{x}' + \boldsymbol{M}\lfloor q/2 \rfloor \in \mathbb{Z}_q^l$ where $\boldsymbol{x}' \leftarrow \chi^l$

(5) $i = 1,\ldots,\mu+1$，$\gamma = 1,\ldots,nk$，$\beta = 0,1$ に対して，$\boldsymbol{R}_{i,\gamma} \xleftarrow{U} \{-1,1\}^{m \times nk}$ をランダムに選び，
$\boldsymbol{c}_{i,\gamma,\beta} \leftarrow (\boldsymbol{B}_{i,\gamma} + H(\mathrm{con}_{\gamma,k}(w_{i,\gamma} + \beta)) \cdot \boldsymbol{G})^\top \boldsymbol{s} + \boldsymbol{R}_{i,\gamma}^\top \boldsymbol{x}_0 \in \mathbb{Z}_q^{nk}$
$\psi_{i,\gamma,\beta} \leftarrow \mathrm{ABE.Enc}(abepp, (l_\Delta, i, \gamma, \beta), \boldsymbol{c}_{i,\gamma,\beta})$ を計算する．ここで，$l_\Delta = (\mu+1)nk$ である．

(6) $ct = (\boldsymbol{c}_0, \{\psi_{i,\gamma,\beta}\}_{i \in \{1,\ldots,\mu+1\}, \gamma \in \{1,\ldots,nk\}, \beta \in \{0,1\}}, \boldsymbol{c}')$ を出力する．

$\boldsymbol{M}\mathrm{or}\perp \leftarrow \mathrm{Dec}(sk_{\vec{v}}, ct)$:

(1) $\vec{\Delta}$ に対応する暗号文を復号する．
$\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}} \leftarrow \mathrm{ABE.Dec}(abesk_\Delta, (l_\Delta, i, \gamma, \Delta_{i,\gamma}), \psi_{i,\gamma,\Delta_{i,\gamma}})$

(2) $\boldsymbol{c}_i \leftarrow \Sigma_{\gamma=1}^{nk} \boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}}$

(3) $\boldsymbol{c}_{\vec{v}} \leftarrow \Sigma_{i=1}^{\mu+1} H_g(v'_i)^\top \boldsymbol{c}_i$

(4) $\boldsymbol{c} = [\boldsymbol{c}_0; \boldsymbol{c}_{\vec{v}}] \in \mathbb{Z}^{m+\bar{m}}$ とする．

(5) $\boldsymbol{d} \leftarrow \boldsymbol{c}' - \boldsymbol{E}_{\vec{v}} \cdot \boldsymbol{c}$

(6) $\lfloor (2/q)\boldsymbol{d} \rceil \bmod 2$ を計算し，出力する．

8.2 正当性の証明

提案構成法の正当性を以下のように示す．

定理 3. $\chi = \bar{\Psi}_\alpha$ とする．$s > 4Cm \cdot \omega(\sqrt{\log n})$，$(\alpha q \cdot \omega(\log \lambda) + \sqrt{m}/2) \cdot 4C(\mu+1)sm^3 < q/5$ のとき，本構成は正当性を持つ．

証明．平文空間を $\mathcal{M} \in \{0,1\}$ として証明を行う．GenTrap の定義より，$s_1(\boldsymbol{R_A}) \leq C\sqrt{2m}$ である．よって $s > 4Cm\omega(\sqrt{\log n}) > \sqrt{s_1(\boldsymbol{R_A})^2 + 1} \cdot \sqrt{7} \cdot \omega(\sqrt{\log n})$ のため，正しく SampleD を実行することが可能である．

復号では selective 安全な ABE から $\vec{\Delta}$ に対応した $\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}} \leftarrow \mathrm{ABE.Dec}(abesk_\Delta, (l_\Delta, i, \gamma, \Delta_{i,\gamma}), \psi_{i,\gamma,\Delta_{i,\gamma}})$ が得られる．$\boldsymbol{c}_i$ を $\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}}$ から構成すると，

$$\boldsymbol{c}_i = \sum_{\gamma=1}^{nk} \boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}} = (\boldsymbol{B}_i + H(w_i + \Delta_i) \cdot \boldsymbol{G})^\top \boldsymbol{s} + \boldsymbol{R}_i^\top \boldsymbol{x}_0$$

である．ここで，$\boldsymbol{B}_i = \sum_{\gamma=1}^{nk} \boldsymbol{B}_{i,\gamma}$，$\boldsymbol{R}_i = \sum_{\gamma=1}^{nk} \boldsymbol{R}_{i,\gamma}$ とした．$\boldsymbol{c}_{\vec{v}}$ を計算すると，

$$\begin{aligned}
\boldsymbol{c}_{\vec{v}} &= \sum_{i=1}^{\mu+1} H_g(v'_i)^\top \boldsymbol{c}_i \\
&= \sum_{i=1}^{\mu+1} H_g(v'_i)^\top \cdot [(\boldsymbol{B}_i + H(w_i + \Delta_i) \cdot \boldsymbol{G})^\top \boldsymbol{s} + \boldsymbol{R}_i^\top \boldsymbol{x}_0] \\
&= \boldsymbol{B}_{\vec{v}}^\top \boldsymbol{s} + (H(\vec{w'}^\top \vec{v'} + \vec{\Delta}^\top \vec{v'}) \cdot \boldsymbol{G})^\top \boldsymbol{s} + \boldsymbol{R}_{\vec{v}}^\top \boldsymbol{x}_0 \\
&= \boldsymbol{B}_{\vec{v}}^\top \boldsymbol{s} + (H(\vec{w'}^\top \vec{v'}) \cdot \boldsymbol{G})^\top \boldsymbol{s} + \boldsymbol{R}_{\vec{v}}^\top \boldsymbol{x}_0 \\
&= \boldsymbol{B}_{\vec{v}}^\top \boldsymbol{s} + (H(\vec{w}^\top \vec{v}) \cdot \boldsymbol{G})^\top \boldsymbol{s} + \boldsymbol{R}_{\vec{v}}^\top \boldsymbol{x}_0
\end{aligned}$$

である．ここで，$\boldsymbol{R}_{\vec{v}} = \Sigma_{i=1}^{\mu+1} \boldsymbol{R}_i \cdot H_g(v'_i)$ とした．また，$\vec{w}^\top \vec{v} = 0$ のとき，

$$\begin{aligned}
\boldsymbol{c}_{\vec{v}} &= \boldsymbol{B}_{\vec{v}}^\top \boldsymbol{s} + \boldsymbol{R}_{\vec{v}}^\top \boldsymbol{x}_0 \\
\boldsymbol{c} &= [\boldsymbol{c}_0; \boldsymbol{c}_{\vec{v}}] = A_{\vec{v}}^\top \boldsymbol{s} + [\boldsymbol{x}_0; \boldsymbol{R}_{\vec{v}}^\top \boldsymbol{x}_0]
\end{aligned}$$

である．よって d は次のようになる．

$$\begin{aligned}
d &= c' - \boldsymbol{e}_{\vec{v}}^\top \cdot \boldsymbol{c} \\
&= M\lfloor q/2 \rfloor + \boldsymbol{u}^\top \boldsymbol{s} + x' - \boldsymbol{e}_{\vec{v}}^\top \cdot (\boldsymbol{A}_{\vec{v}}^\top \boldsymbol{s} + [\boldsymbol{x}_0; \boldsymbol{R}_{\vec{v}}^\top \boldsymbol{x}_0]) \\
&= M\lfloor q/2 \rfloor + x' - \boldsymbol{e}_{\vec{v}}^\top [\boldsymbol{x}_0; \boldsymbol{R}_{\vec{v}}^\top \boldsymbol{x}_0]
\end{aligned}$$

$\boldsymbol{e}_{\vec{v}} = [\boldsymbol{e}_1; \boldsymbol{e}_2] \in \mathbb{Z}^m \times \mathbb{Z}^{nk}$ とすると，

$$d = M\lfloor q/2 \rfloor + x' - (\boldsymbol{e}_1 + \boldsymbol{R}_{\vec{v}}\boldsymbol{e}_2)^\top \boldsymbol{x}_0$$

である．よって正当性を満たすためには圧倒的確率で次式を満たす必要がある．

$$|x'| + |(\boldsymbol{e}_1 + \boldsymbol{R}_{\vec{v}}\boldsymbol{e}_2)^\top \boldsymbol{x}_0| < q/5$$

$\boldsymbol{e} = \boldsymbol{e}_1 + \boldsymbol{R}_{\vec{v}} \cdot \boldsymbol{e}_2 = \boldsymbol{e}_1 + (\Sigma_{i=1}^{\mu+1}\Sigma_{\gamma=1}^{nk}\boldsymbol{R}_{i,\gamma} \cdot H_g(v_i')) \in \mathbb{Z}^m$ とし，ノルムを計算する．圧倒的確率で $||e_1||, ||e_2|| \leq ||e_{\vec{v}}|| \leq s\sqrt{m+nk} \leq s\sqrt{2m}$，補題 5 より $s_1(\boldsymbol{R}_{i,\gamma}) \leq C(\sqrt{nk} + \sqrt{m}) \leq 2C\sqrt{m}$，$s_1(\boldsymbol{R}_i) = s_1(\Sigma_{\gamma=1}^{nk}\boldsymbol{R}_{i,\gamma}) \leq \Sigma_{\gamma=1}^{nk} s_1(\boldsymbol{R}_{i,\gamma}) \leq 2nkC\sqrt{m} \leq 2mC\sqrt{m}$, 補題 2 より $s_1(H_g(v_i')) \leq nk \leq m$ を満たす．よって，$s_1(\boldsymbol{R}_{\vec{v}}) = s_1(\Sigma_{i=1}^{\mu+1}\boldsymbol{R}_i \cdot H_g(v_i')) \leq \Sigma_{i=1}^{\mu+1} s_1(\boldsymbol{R}_i \cdot H_g(v_i')) \leq 2(\mu+1)Cm^{5/2}$ を圧倒的確率で満たす．よって

$$||\boldsymbol{e}|| = ||\boldsymbol{e}_1 + \boldsymbol{R}_{\vec{v}} \cdot \boldsymbol{e}_2|| \leq (1 + 2(\mu+1)Cm^{5/2}) \cdot s\sqrt{2m}$$

である．補題 3 より，次の式が得られる．

$$\begin{aligned} |\boldsymbol{x}'| + |\boldsymbol{e}^{\mathrm{T}}\boldsymbol{x}_0| &\leq \alpha q \cdot \omega(\log\lambda) + 1/2 \\ &\quad + (1 + 2(\mu+1)Cm^{5/2})s\sqrt{2m} \cdot (\alpha q \cdot \omega(\log\lambda) \\ &\quad + \sqrt{m}/2) \\ &\leq (\alpha q \cdot \omega(\log\lambda) + \sqrt{m}/2) \cdot 4C(\mu+1)sm^3 < q/5 \end{aligned}$$

以上より定理は示された．

8.3 安全性の証明

提案構成法の安全性を以下のように示す．

定理 4. $m \geq 2n\log q + \omega(\log n), s \geq 3(\mu+1)Cm^{5/2} \cdot \omega(\sqrt{\log n})$ のとき，LWE 仮定のもと，本構成は wAH-semi-adaptive-CPA 安全である．

証明．安全性証明は [9] の証明と [3] の安全性証明を組み合わせて行う．シミュレーションで用いる 3 つのアルゴリズム $\overline{\mathrm{Setup}}$，$\overline{\mathrm{KeyGen}}$，$\overline{\mathrm{Enc}}$ を定義する．平文空間を $\mathcal{M} \in \{0,1\}$ として証明を行う．

$(pp, \overline{msk}) \leftarrow \overline{\mathrm{Setup}}(1^\lambda)$:

(1) $\boldsymbol{A} \xleftarrow{U} \mathbb{Z}_q^{n\times m}$，$\boldsymbol{u} \xleftarrow{U} \mathbb{Z}_q^n$

(2) $r_i \xleftarrow{U} \mathrm{GF}(q^n)$ for $i = 1, \ldots, \mu+1$ をランダムに選び，$\vec{r} = (r_1, \ldots, r_{\mu+1})$ とする．ただし，$r_{\mu+1} \neq 0$ とする．

(3) $(\boldsymbol{G}, \boldsymbol{S})$ を設定する．$\boldsymbol{S}$ は $\boldsymbol{G}$ の既知の基底である．

(4) $i = 1, \ldots, \mu+1$，$\gamma = 1, \ldots, nk$ に対して，
$\boldsymbol{R}_{i,\gamma} \xleftarrow{U} \{-1, 1\}^{m\times nk}$
$\boldsymbol{B}_{i,\gamma} \leftarrow \boldsymbol{A}\boldsymbol{R}_{i,\gamma} - H(\mathrm{con}_{\gamma,k}(r_{i,\gamma})) \cdot \boldsymbol{G}$ とする．

(5) $(abepp, abemsk) \leftarrow \mathrm{ABE.Setup}(1^\lambda)$

(6) $pp = (\boldsymbol{A}, \{\boldsymbol{B}_{i,\gamma}\}_{i\in\{1,\ldots,\mu+1\},\gamma\in\{1,\ldots,nk\}}, \boldsymbol{u}, abepp)$，$\overline{msk} = (\boldsymbol{S}, \{\boldsymbol{R}_{i,\gamma}\}_{i\in\{1,\ldots,\mu+1\},\gamma\in\{1,\ldots,nk\}}, abemsk, \vec{r})$ を出力する．

$sk_{\vec{v}} \leftarrow \overline{\mathrm{KeyGen}}(\overline{msk}, \vec{v} \in \mathrm{GF}(q^n)^\mu, \vec{w} \in \mathrm{GF}(q^n)^\mu)$:

(1) $\vec{w'} = [\vec{w}; 0]$，$\vec{\Delta} = \vec{r} - \vec{w'}$ とする．

(2) $v_{\mu+1} \leftarrow -\frac{1}{\Delta_{\mu+1}}\Sigma_{i=1}^{\mu} v_i\Delta_i$ を計算し，
$\vec{v'} = [\vec{v}; v_{\mu+1}]$ とする．

(3) $abesk_\Delta \leftarrow \mathrm{ABE.KeyGen}(abemsk, \mathrm{BitCheck}_\Delta)$

(4) $\boldsymbol{B}_{\vec{v}} \leftarrow \Sigma_{i=1}^{\mu+1}(\Sigma_{\gamma=1}^{nk}\boldsymbol{B}_{i,\gamma})H_g(v_i') \in \mathbb{Z}_q^{n\times nk}$ を計算し，$\boldsymbol{A}_{\vec{v}} = [\boldsymbol{A}|\boldsymbol{B}_{\vec{v}}] \in \mathbb{Z}_q^{n\times(m+nk)}$ とする．

(5) $\boldsymbol{e}_{\vec{v}} \leftarrow \mathrm{SampleD}(\boldsymbol{A}, -H(\vec{w}^\top\vec{v}), -\boldsymbol{R}_{\vec{v}}, \boldsymbol{G}, \boldsymbol{S}, \boldsymbol{u}, s)$

(6) $sk_{\vec{v}} = (\vec{v'}, \boldsymbol{e}_{\vec{v}}, \vec{\Delta}, abesk_\Delta)$ を出力する．

ここで $\boldsymbol{A}_{\vec{v}}$ は次のようになる．

$$\begin{aligned} \boldsymbol{A}_{\vec{v}} &= \left[\boldsymbol{A}|\boldsymbol{A}\boldsymbol{R}_{\vec{v}} - \left(\sum_{i=1}^{\mu+1} H(r_i) \cdot \boldsymbol{G}H_g(v_i')\right)\right] \\ &= \left[\boldsymbol{A}|\boldsymbol{A}\boldsymbol{R}_{\vec{v}} - \left(\sum_{i=1}^{\mu+1} H(w_i' + \Delta_i)H(v_i') \cdot \boldsymbol{G}\right)\right] \\ &= \left[\boldsymbol{A}|\boldsymbol{A}\boldsymbol{R}_{\vec{v}} - H(\vec{w'}^\top\vec{v'} + \vec{\Delta}^\top\vec{v'}) \cdot \boldsymbol{G})\right] \\ &= \left[\boldsymbol{A}|\boldsymbol{A}\boldsymbol{R}_{\vec{v}} - H(\vec{w}^\top\vec{v}) \cdot \boldsymbol{G}\right] \end{aligned}$$

ここで，$\boldsymbol{R}_{\vec{v}} = \Sigma_{i=1}^{\mu+1}(\sum_{\gamma=1}^{nk}\boldsymbol{R}_{i,\gamma})H_g(v_i')$ とする．$-\boldsymbol{R}_{\vec{v}}$ は $\boldsymbol{A}_{\vec{v}}$ のトラップドアタグ $-H(\vec{w}^\top\vec{v})$ である．秘密鍵のシミュレーションである $\boldsymbol{S}, -\boldsymbol{R}_{\vec{v}}$ を用いて $\boldsymbol{e}_{\vec{v}}$ を生成している．

$ct \leftarrow \overline{\mathrm{Enc}}(pp, \vec{w} \in \mathrm{GF}(q^n)^\mu, M \in \{0,1\}, \overline{msk})$:

(1) $\vec{w'} = [\vec{w}; 0]$，$\vec{\Delta} = \vec{r} - \vec{w'}$ とする．

(2) $\boldsymbol{s} \xleftarrow{U} \mathbb{Z}_q^n$

(3) $\boldsymbol{c}_0 \leftarrow \boldsymbol{A}^\top\boldsymbol{s} + \boldsymbol{x}_0 \in \mathbb{Z}_q^m$ *where* $\boldsymbol{x}_0 \leftarrow \chi^m$

(4) $\boldsymbol{c}' \leftarrow \boldsymbol{u}^\top\boldsymbol{s} + \boldsymbol{x}' + M\lfloor q/2 \rfloor \in \mathbb{Z}_q$ *where* $x' \leftarrow \chi$

(5) $i = 1, \ldots, \mu+1$，$\gamma = 1, \ldots, nk$ に対して，
$\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}} \leftarrow (\boldsymbol{B}_{i,\gamma} + H(\mathrm{con}_{\gamma,k}(w_{i,\gamma} + \Delta_{i,\gamma})) \cdot \boldsymbol{G})^\top\boldsymbol{s} + \boldsymbol{R}_{i,\gamma}^\top\boldsymbol{x}_0 \in \mathbb{Z}_q^{nk}$
$\psi_{i,\gamma,\Delta_{i,\gamma}} \leftarrow \mathrm{ABE.Enc}(abepp, (l_\Delta, i, \gamma, \Delta_{i,\gamma}), \boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}})$
$\psi_{i,\gamma,1-\Delta_{i,\gamma}} \leftarrow \mathrm{ABE.Enc}(abepp, (l_\Delta, i, \gamma, 1 - \Delta_{i,\gamma}), \boldsymbol{0})$

(6) $ct = (\boldsymbol{c}_0, \{\psi_{i,\gamma,\beta}\}_{i\in\{1,\ldots,\mu+1\},\gamma\in\{1,\ldots,nk\},\beta\in\{0,1\}}, \boldsymbol{c}')$ を出力する．

ここで，$\boldsymbol{B}_{i,\gamma} = \boldsymbol{A}\boldsymbol{R}_{i,\gamma} - H(\mathrm{con}_{\gamma,k}(r_{i,\gamma})) \cdot \boldsymbol{G}$ であるため，$\boldsymbol{B}_i = \sum_{\gamma=1}^{nk}\boldsymbol{B}_{i,\gamma} = \boldsymbol{A}\boldsymbol{R}_i - H(r_i)\boldsymbol{G} = \boldsymbol{A}\boldsymbol{R}_i - H(w_i' + \Delta_i)\boldsymbol{G}$ である．ここで，$r_i = w_i' + \Delta_i$ であり，$\boldsymbol{R}_i = \sum_{\gamma=1}^{nk}\boldsymbol{R}_{i,\gamma}$ とした．

$\Delta_{i,\gamma} = \beta$ の要素 $\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}}$ を考えると，$\boldsymbol{c}_i = \sum_{\gamma=1}^{nk}\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}} = (\boldsymbol{B}_i + H(w_i' + \Delta_i)\boldsymbol{G})^\top\boldsymbol{s} + \boldsymbol{R}_i^\top\boldsymbol{x}_0 = \boldsymbol{R}_i^\top\boldsymbol{c}_0$ となる．

ゲーム変換を用いて証明を行う．各ゲームの添え字 b は挑戦者が選ぶ $b \in \{0,1\}$ を示している．

ゲーム 0_b

ゲーム 0_b は挑戦者が Setup，KeyGen，Enc アルゴリズムを使用し，b を選ぶ wAH-semi-adaptive-CPA ゲームである．

ゲーム 1_b

ゲーム 1_b では $\vec{\Delta}$ の定義を変更し，$\vec{\Delta} = \vec{r} - \vec{w'}_b$ とする．$\vec{\Delta}$ は最初の秘密鍵クエリに答えるときまで使用されないため，暗号化属性 $\vec{w}_b$ を受け取るタイミングを遅らせてもシミュレートが可能である．$\vec{r}$ は一様ランダムであり，$\vec{r} - \vec{w'}_b$ も一様ランダムであるため，ゲーム 0_b とゲーム 1_b は識別不可能である．

ゲーム 2_b

ここではチャレンジ暗号文を変更し，

$$\psi_{i,\gamma,1-\Delta_{i,\gamma}} \leftarrow \mathrm{ABE.Enc}(abepp, (l_\Delta, i, \gamma, 1-\Delta_{i,\gamma}), \mathbf{0})$$

とする．$\mathbf{0}$ は $\boldsymbol{c}_{i,\gamma,1-\Delta_{i,\gamma}}$ と同じ長さを持つ．全ての l_Δ, i, γ に対して，$\mathrm{BitCheck}_\Delta(l_\Delta, i, \gamma, 1-\Delta_{i,\gamma}) = 0$ のため，秘密鍵 $abesk_\Delta$ は $\psi_{i,\gamma,1-\Delta_{i,\gamma}}$ を復号することができず，ABE の selective 安全性よりゲーム 1_b とゲーム 2_b は識別不可能である．このゲーム変換によって以後は $\Delta_{i,\gamma}$ に対応する $\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}}$ の要素のみを考えることが可能となる．

ゲーム 3_b

ゲーム 3_b では挑戦者の実行するアルゴリズムを $\overline{\mathrm{Setup}}$, $\overline{\mathrm{KeyGen}}$, $\overline{\mathrm{Enc}}$ に変更する．

SampleD が正しく動作する条件を考える．ゲーム 2_b では $s > 4Cm \cdot \omega(\sqrt{\log n})$ $> \sqrt{s_1(\boldsymbol{R_A})^2+1} \cdot \sqrt{7} \cdot \omega(\sqrt{\log n})$ である．ゲーム 3_b では $s_1(\boldsymbol{R}_{\vec{v}}) = s_1(\Sigma_{i=1}^{\mu+1} \boldsymbol{R}_i \cdot H_g(v'_i)) \leq \Sigma_{i=1}^{\mu+1} s_1(\boldsymbol{R}_i \cdot H_g(v'_i)) \leq 2(\mu+1)Cm^{5/2}$ であり，圧倒的確率で $s > \sqrt{s_1(\boldsymbol{R}_{\vec{v}})^2+1} \cdot \sqrt{7} \cdot \omega(\sqrt{\log n})$ を満たす必要がある．よって，$s \geq 3(\mu+1)Cm^{5/2} \cdot \omega(\sqrt{\log n})$ であれば，SampleD が正しく動作する．

SampleD アルゴリズムによって $\boldsymbol{e}_{\vec{v}}$ は $D_{A_q^{\boldsymbol{u}}(\boldsymbol{A}_{\vec{v}}),s}$ から選ばれる．よって $\boldsymbol{A}$ と $\boldsymbol{e}_{\vec{v}}$ はゲーム 2_b とゲーム 3_b においてその差を無視できる．

次に $\boldsymbol{B}_{i,\gamma}$ と暗号文 $\boldsymbol{c}_{i,\gamma,\beta}$ について考える．$m \geq (n+1)\log q + \omega(\log n)$ のとき，補題 4 より，$(\boldsymbol{A}, \boldsymbol{B}_{i,\gamma}, \boldsymbol{R}_{i,\gamma}^\top \boldsymbol{W})$ と $(\boldsymbol{A}, \boldsymbol{AR}_{i,\gamma}, \boldsymbol{R}_{i,\gamma}^\top \boldsymbol{W})$ は統計的に近い．ここで，$\boldsymbol{B}_{i,\gamma}$ はゲーム 2_b において一様ランダムに配られているため，$(\boldsymbol{A}, \boldsymbol{B}_{i,\gamma}, \boldsymbol{R}_{i,\gamma}^\top \boldsymbol{W})$ と $(\boldsymbol{A}, \boldsymbol{AR}_{i,\gamma} - H(\mathrm{con}_{\gamma,k}(r_{i,\gamma}))\boldsymbol{G}, \boldsymbol{R}_{i,\gamma}^\top \boldsymbol{W})$ もまた，統計的に近い．また，$\boldsymbol{R}_{i,\gamma}$ は (i,γ) 毎に独立に選ばれているため，次の式が得られる．

$$(\boldsymbol{A}, \{\boldsymbol{B}_{i,\gamma}, \boldsymbol{R}_{i,\gamma}^\top \boldsymbol{x}_0\}) \approx_s (\boldsymbol{A}, \{\boldsymbol{AR}_{i,\gamma} - H(\mathrm{con}_{\gamma,k}(r_{i,\gamma}))\boldsymbol{G} \ \ , \boldsymbol{R}_{i,\gamma}^\top \boldsymbol{x}_0\}).$$

$(\boldsymbol{B}_{i,\gamma} + H(\mathrm{con}_{\gamma,k}(w_{i,\gamma}+\Delta_{i,\gamma}))\boldsymbol{G})^\top \boldsymbol{s}$ を加えたものについて次の式が得られる．

$$\begin{aligned}&(\boldsymbol{A}, \{\boldsymbol{B}_{i,\gamma}, (\boldsymbol{B}_{i,\gamma} \\ &+H(\mathrm{con}_{\gamma,k}(w_{i,\gamma}+\Delta_{i,\gamma}))\boldsymbol{G})^\top \boldsymbol{s} + \boldsymbol{R}_{i,\gamma}^\top \boldsymbol{x}_0\}) \\ &\approx_s (\boldsymbol{A}, \{\boldsymbol{AR}_{i,\gamma} - H(\mathrm{con}_{\gamma,k}(r_{i,\gamma}))\boldsymbol{G} \\ &\quad , (\boldsymbol{AR}_{i,\gamma} - H(\mathrm{con}_{\gamma,k}(r_{i,\gamma}))\boldsymbol{G} \\ &\quad +H(\mathrm{con}_{\gamma,k}(w_{i,\gamma}+\Delta_{i,\gamma}))\boldsymbol{G})^\top \boldsymbol{s} + \boldsymbol{R}_{i,\gamma}^\top \boldsymbol{x}_0\}).\end{aligned}$$

よってゲーム 2_b とゲーム 3_b において，$(\boldsymbol{A}, \boldsymbol{B}_{i,\gamma}, \boldsymbol{c}_{i,\gamma,\beta})$ の確率分布は統計的に近く識別不可能である．

ゲーム 4_b

ゲーム 4_b では暗号文要素 $\boldsymbol{c}_0$,$\{\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}}\}$,$c'$ をランダムな暗号文に変更する．

ゲーム 3_b とゲーム 4_b を識別可能な攻撃者 $\mathcal{A}$ を利用して，LWE 問題を解く PPT アルゴリズム $\mathcal{B}$ を構成することで証明を行う．与えられた $(\boldsymbol{a_i}, y_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ for $0, \ldots, m$ に対し，次のように定義する．

$$\boldsymbol{A} = [\boldsymbol{a}_1 \cdots \boldsymbol{a}_m] \in \mathbb{Z}_q^{n \times m}, \ \boldsymbol{u} = \boldsymbol{a}_0,$$
$$\boldsymbol{c}_0 = (y_1, \ldots, y_m)^{\mathrm{T}} \in \mathbb{Z}_q^m, \ c' = y_0 + M\lfloor q/2 \rfloor.$$

$\mathcal{B}$ は次のようにゲームをシミュレーションする．まず，$\overline{\mathrm{Setup}}$ を上記の $\boldsymbol{A}$,$\boldsymbol{u}$ を用いて実行する．その後公開鍵 pp を $\mathcal{A}$ に送信し，$\mathcal{B}$ から属性 $\vec{w}_0, \vec{w}_1$ を受け取り，$\vec{w} = \vec{w}_b$ とする．秘密鍵クエリでは $\overline{\mathrm{KeyGen}}$ を実行する．暗号文の生成は $\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}} = \boldsymbol{R}_{i,\gamma}^\top \boldsymbol{c}_0$，$\boldsymbol{c}_{i,\gamma,1-\Delta_{i,\gamma}} = \mathbf{0}$ とし，ABE.Enc を用いて $\psi_{i,\gamma,\beta} \leftarrow \mathrm{ABE.Enc}(abepp, (l_\Delta, i, \gamma, \beta), \boldsymbol{c}_{i,\gamma,\beta})$ として暗号化を行う．ここで $\beta \in \{0,1\}$ である．暗号文として $ct = (\boldsymbol{c}_0, \{\psi_{i,\gamma,\beta}\}_{i \in \{1,\ldots,\mu+1\}, \gamma \in \{1,\ldots,nk\}, \beta \in \{0,1\}}, c')$ を攻撃者 $\mathcal{A}$ に送信する．

LWE 挑戦者のオラクルが $A(\boldsymbol{s}, \chi)$ であった場合，$\boldsymbol{c}_0 = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} + \boldsymbol{x}_0$，$c' = \boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}$ となり，ゲーム 3_b のシミュレーションとなっている．ここで，$\boldsymbol{x}_0 \leftarrow \chi^m$，$x' \leftarrow \chi$ である．

LWE 挑戦者のオラクルが $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ であった場合，$\boldsymbol{A}$,$\boldsymbol{c}_0$ は一様ランダムに選ばれる．よって $m \geq (n+1)\log q + \omega(\log n)$ のとき，補題 4 より $(\boldsymbol{A}, \boldsymbol{c}_0, \boldsymbol{AR}_{i,\gamma}, \boldsymbol{R}_{i,\gamma}^{\mathrm{T}} \boldsymbol{c}_0)$ は統計的に $\mathbb{Z}_q^{(n+1)\times m} \times \mathbb{Z}_q^{(n+1)\times nk}$ 上の一様分布に近い．よって $(\boldsymbol{c}_0, \{\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}}\}, c')$ は $\mathbb{Z}_q^{m+(nk)^2(\mu+1)+1}$ 上において一様分布である．よってゲーム 4_b のシミュレーションとなっている．

次にゲーム 4_0 とゲーム 4_1 の識別不可能性を証明する．ゲーム 4_0 とゲーム 4_1 で $\vec{w}$ は $\vec{\Delta} = \vec{r} - \vec{w'}$ と $\boldsymbol{B}_{i,\gamma} \leftarrow \boldsymbol{AR}_{i,\gamma} - H(\mathrm{con}_{\gamma,k}(r_{i,\gamma}))\boldsymbol{G}$ に含まれている．$\vec{\Delta}$ はゲーム 1_b より統計的に一様ランダムなものと識別不可能であり，統計的に $\vec{w}_0, \vec{w}_1$ を隠している．

ゲーム 3_b の議論より，

$$(\boldsymbol{A}, \{\boldsymbol{B}_{i,\gamma}\}) \approx_s (\boldsymbol{A}, \{\boldsymbol{AR}_{i,\gamma} - H(\mathrm{con}_{\gamma,k}(r_{i,\gamma}))\boldsymbol{G}\}).$$

ⓒ 2019 Information Processing Society of Japan

が得られる．この式は任意のベクトル $\vec{w}$ と行列 G に対して成り立つため，統計的に $\vec{w_0}$ と $\vec{w_1}$ を隠している．よってゲーム 4_0 とゲーム 4_1 は識別不可能である．

以上より定理は示された．

9. まとめ

本論文では格子問題に基づく内積暗号に注目し，semi-adaptive 安全な構成方法を提案した．[3] で提案された semi-adaptive 安全な属性ベース暗号の属性と乱数の排他的論理和を属性として暗号化を行う手法と [9] の内積暗号スキームを組み合わせて構成し，その正当性証明，安全性証明を行った．暗号化属性に乱数を用いた影響を消すための調整要素を加えることで内積暗号に [3] の手法を適用可能なことを示した．

参考文献

[1] S. Agrawal, D. Boneh, X. Boyen, "Efficient Lattice (H)IBE in the Standard Model." EUROCRYPT 2010, pp.553-572.
[2] S. Agrawal, D. M. Freeman, V. Vaikuntanathan, "Functional Encryption for Inner Product Predicates from Learning with Errors." ASIACRYPT 2011, pp.21-40.
[3] Z. Brakerski, V. Vaikuntanathan, "Circuit-ABE from LWE: Unbounded Attributes and Semi-adaptive Security." CRYPTO 2016, pp.363-384.
[4] J. Katz, A. Sahai, B. Waters, "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products." EUROCRYPT 2008, pp.146-162.
[5] D. Micciancio, "Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions." Computational Complexity 2007, pp.365-411.
[6] D. Micciancio, C. Peikert, "Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller." EUROCRYPT 2012, pp.700-718.
[7] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography." STOC 2005, pp.84-93.
[8] A. Sahai, B. Waters, "Fuzzy Identity-Based Encryption." EUROCRYPT 2005, pp.457-473.
[9] K. Xagawa, "Improved (Hierarchical) Inner-Product Encryption from Lattices. " Public key Cryptography 2013, pp.235-252.

付　　録

A.1 属性ベース暗号

ここでは属性ベース暗号として KP-ABE について説明する．X を属性空間，$\mathcal{M}$ を平文空間，$\mathcal{F} \subset X \to \{0,1\}$ としたとき，KP-ABE は次の 4 つのアルゴリズムからなる．

$(pp, msk) \leftarrow \mathrm{Setup}(1^\lambda)$: Setup アルゴリズムは入力としてセキュリティパラメータ 1^λ を受け取り，公開パラメータ pp とマスター秘密鍵 msk を出力する．

$sk_\phi \leftarrow \mathrm{KeyGen}(msk, f)$: KeyGen アルゴリズムは入力として msk，ポリシー $f \in F$ を受け取り，秘密鍵 sk_f を出力する．

$ct \leftarrow \mathrm{Enc}(pp, x, M)$: Enc アルゴリズムは入力として pp，属性 $x \in X$，平文 $M \in \mathcal{M}$ を受け取り，暗号文 ct を出力する．

$\mathrm{Dec}(sk_f, x, ct) \leftarrow M \mathrm{or} \perp$: Dec アルゴリズムは入力として秘密鍵 sk_f，属性 x，暗号文 ct を受け取り，復号結果 $M \in \mathcal{M}$ か復号不可能シンボル $\perp$ を出力する．

属性ベース暗号の正当性を次のように定義する．任意の $x \in X, f \in F$, に対して $(pp, msk) \leftarrow \mathrm{Setup}(1^\lambda), sk_f \leftarrow \mathrm{KeyGen}(msk, f), ct \leftarrow \mathrm{Enc}(pp, x, M)$，$f(x) = 1$ のとき，

$$\Pr\left[M = \tilde{M} : \tilde{M} \leftarrow \mathrm{Dec}(sk_f, x, ct)\right]$$

を圧倒的確率で満たす．$f(x) = 0$ のとき，

$$\Pr\left[\tilde{M} = \perp : \tilde{M} \leftarrow \mathrm{Dec}(sk_f, x, ct)\right]$$

を圧倒的確率で満たす．

A.1.1 属性ベース暗号の安全性

属性ベース暗号の安全性ゲームとして次のものを考える．

(1) 攻撃者は挑戦者に属性 x を送信する．

(2) 挑戦者は $(pp, msk) \leftarrow \mathrm{Setup}(1^\lambda)$ を生成し，pp を攻撃者へ送信する．

(3) 攻撃者は任意の回数の秘密鍵クエリを発行する．秘密鍵クエリでは，挑戦者に $f(x) = 0$ であるポリシー f を送信し挑戦者は $sk_f \leftarrow \mathrm{KeyGen}(msk, f)$ を生成し，sk_f を攻撃者へ送信する．

(4) 平文のペア M_0 と M_1 を挑戦者に送信する．挑戦者は一様ランダムに $b \in \{0,1\}$ を選び，暗号文 $ct = \mathrm{Enc}(pp, x, M_b)$ を計算し，ct を攻撃者へ送信する．

(5) 攻撃者はステップ *2* のように任意の回数の秘密鍵クエリを発行する．

(6) 攻撃者は b を推測し，$b' \in \{0,1\}$ を出力する．

安全性ゲームにおいて攻撃者 $\mathcal{A}$ のアドバンテージは $|\Pr[b' = 1 | b = 1] - \Pr[b' = 1 | b = 0]|$ である．上記の安全性ゲームは selective 安全性ゲームである．全ての PPT 攻撃者 $\mathcal{A}$ に対して $\mathcal{A}$ のアドバンテージが無視できるほど小さいとき，属性ベース暗号は selective-CPA 安全である．

ⓒ 2019 Information Processing Society of Japan