効率的な格子問題に基づくSemi-Adaptive安全な内積暗号

宮澤 智輝[1,a)]　佐藤 慎悟[3,b)]　四方 順司[1,2,c)]

概要：近年，量子コンピュータ開発の影響から，耐量子計算機暗号の研究が盛んに行われている．特に、格子問題の困難性に基づく暗号は注目されており、耐量子性だけでなく多くの高機能暗号の構成にも利用されている．高機能暗号として、2008 年に Katz らは内積暗号を提案した。2011 年に Agrawal ら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た。また、2017 年に Li らはより効率の優れた構成法を提案し，Wang らは属性数にパラメータが依存しない構成を提案した。ただし、これらはいずれも selective 安全性を満たす方式である．semi-adaptive 安全に注目すると，2016 年に Goyal らは関数暗号に対して selective 安全性から semi-adaptive 安全性に変換する一般的手法を提案した．本論文では格子問題に基づく semi-adaptive 安全な内積暗号に注目する．2019 年 11 月の CSEC 研究発表会で著者らは格子問題に基づく semi-adaptive 安全な内積暗号の構成を提案したが，本論文では，その構成法と既存の構成法（格子問題に基づく selective 安全な内積暗号に Goyal らの変換法を適用し semi-adaptive 安全にした方式）との比較を行う．その結果，著者らの提案方式が鍵長および暗号文サイズの点において最も優れていることを示す．

キーワード：内積暗号，格子問題，LWE 問題，Semi-Adaptive 安全性

Efficient Semi-Adaptively Secure Inner-Product Encryption from Lattices

Tomoki Miyazawa[1,a)]　Shingo Sato[3,b)]　Junji Shikata[1,2,c)]

Abstract: Recently, quantum computers have been developed actively, and it is necessary to study post-quantum cryptography (PQC). Lattice-based cryptography is one of PQC. In 2008, Katz, Sahai, Waters proposed inner-product encryption (IPE) which treats inner-product as predicate. IPE provides access control by the relation between attribute vectors embedded in private keys and ciphertexts. As the existing lattice-based constructions of IPE, in 2011, Agrawal, Freeman, Vaikuntanathan proposed the first lattice-based construction. In 2013, Xagawa proposed lattice-based IPE improving efficiency in terms of key size. In 2017, Li et al. improved lattice-based IPE more efficiency, and Wang, Fan, Wang proposed lattice-based IPE where the parameter size does not depend on the number of attributes. However, we note that those constructions guarantee selective security. Focusing on semi-adaptive security, Goyal, Koppula, and Waters proposed a general method to convert selective security into semi-adaptive security for functional encryption. At CSEC in November 2019, the authors proposed lattice-based semi-adaptive secure IPE. In this paper, we compare our construction with constructions obtained by applying the convertion by Goyal et al. to selective secure lattice-based constructions of IPE. Consequently, we show that our proposed IPE is most efficient in terms of key-size and ciphertext-size.

Keywords: Inner Product Encryption, Lattice, LWE, Semi-Adaptive Security

[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, Yokohama 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.
[3] 国立研究開発法人情報通信研究機構. National Institute of Information and Communications Technology.
[a)] miyazawa-tomoki-vb@ynu.jp
[b)] shingo-sato@nict.go.jp

1. はじめに

近年，量子コンピュータの開発が盛んに行われている．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 [5] 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制御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 [1] 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 [13] 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．2017 年には Li，Zhang, Lu, Wang は更に効率性を改善した構成 [7] を提案した．また，同年，Wang, Fan, Wang は属性数が $\log(\lambda)$ の条件（λ はセキュリティパラメータ）のもと, 公開パラメータに属性数に依存した行列が含まれない構成 [12] を提案した．なお，上記の格子問題に基づく構成はいずれも selective 安全性である．

一方，属性とそのアクセス構造によってアクセス制御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 [11]．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．

また, selective 安全な関数暗号を semi-adaptive 安全に変換する一般的手法 [4] は 2016 年に Goyal，Koppula，Waters によって提案された. この変換では公開鍵暗号方式と garbled circuit を用いて semi-adaptive 安全への変換を実現している．

2019 年 11 月の CSEC 研究発表会にて, 著者らは格子問題に基づく semi-adaptive 安全な内積暗号 [14] を提案した．この構成は暗号文に埋め込んだ属性の情報が漏れないという特徴を持つ．この構成では, 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する手法を内積暗号において実現していた．本論文では，その構成法と既存の構成法（格子問題に基づく selective 安全な内積暗号に Goyal らの変換法 [4] を適用し semi-adaptive 安全にした方式）との比較を行う. その結果，著者らの提案方式が鍵サイズおよび暗号文サイズの点において最も優れていることを示す．

c) shikata-junji-rb@ynu.ac.jp

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．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 $D_{A,s}(\boldsymbol{x}) = \frac{\rho_s(\boldsymbol{x})}{\Sigma_{\boldsymbol{y}\in A}\rho_s(y)}$ と定義する．

2.1 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．

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

定理 1. ([9], 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，$||\tilde{\boldsymbol{S}}|| \leq \sqrt{5}, ||\boldsymbol{S}|| \leq \max\{\sqrt{5}, \sqrt{k}\}$ を満たす．

定義 1. ([9], 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 $m \geq w \geq n$ 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. ([9]) $k = \lceil \log q \rceil, m = \bar{m} + nk$ 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 $s_1(\boldsymbol{R}) \leq C(\sqrt{\bar{m}} + \sqrt{nk})$ 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．

2.2 Learning With Errors(LWE)

learning with errors (LWE) は [10] 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．

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

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

2.3 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 $\phi \in \Phi, \sigma \in \Sigma, M \in \mathcal{M}$ 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，

$$M = \mathrm{Dec}(sk_\phi, ct)$$

を圧倒的確率で満たす．$P(\phi, \sigma) = 0$ のとき，

$$\perp = \mathrm{Dec}(sk_\phi, ct)$$

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．

2.4 可逆差分符号化の疑似可換性

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

2.4.1 可逆差分符号化 $\boldsymbol{H}$

$H : \mathrm{GF}(q^n) \to \mathbb{Z}_q^{n\times n}$ 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 [8] 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．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．

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

2.4.2 符号化 $\boldsymbol{H_g}$

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，$b \geq 2$ 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，[9] 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．

$$H_g : a = a_0+a_1x+\cdots+a_{n-1}x^{n-1} \in \mathrm{GF}(q^n) \mapsto D_g(\mathrm{Rot}(a)).$$

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

補題 1. ([13]，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. ([13]，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．

3. Semi-Adaptive 安全な内積暗号の構成法

[14] で提案した Semi-Adaptive 安全な内積暗号の構成について説明する．[13] で提案された内積暗号の方式に [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，乱数 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，乱数 Δ の影響を打ち消し，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．$\vec{\Delta}$ についてはあらかじめ 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．

3.1 構成法

[14] 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．

$\mathrm{con}_{\gamma}:\{0,1\}\to \mathrm{GF}(q^n)$ を次のように定義する．

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

ここで，$k=\lceil\log q\rceil$ とし，$\gamma\in\{1,2,\ldots,nk\}$ とする．$\mathrm{GF}(q^n)$ の γ ビット目の値 $a\in\{0,1\}$ から $\mathrm{GF}(q^n)$ を構成する関数である．

パラメータとして，$k=\lceil\log q\rceil$，$\zeta=\omega(\sqrt{\log(2m)})$，$m=3n\log q$，$s=3kC(\mu+1)Cm^{3/2}$，$q=60kC^2(\mu+1)^2\cdot m^4\cdot\zeta$，$\alpha=(120kC^2(\mu+1)^2m^{7/2}\cdot\zeta^2)^{-1}$ 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 $i=1,\ldots,\mu+1$, $\gamma=1,\ldots,k$

(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) $\boldsymbol{B}_{\vec{v}}\leftarrow\Sigma_{i=1}^{\mu+1}(\Sigma_{\gamma=1}^{k}\boldsymbol{B}_{i,\gamma})H_g(v_i')\in\mathbb{Z}_q^{n\times nk}$ 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，$\boldsymbol{c}_{i,\gamma,\beta}\leftarrow(\boldsymbol{B}_{i,\gamma}+H(\mathrm{con}_{\gamma}(w_{i,\gamma})+\mathrm{con}_{\gamma}(\beta))\cdot\boldsymbol{G})^{\top}\boldsymbol{s}+\boldsymbol{R}_{i,\gamma}^{\top}\boldsymbol{x}_0\in\mathbb{Z}_q^{nk}$
$\psi_{i,\gamma,\beta}\leftarrow\mathrm{ABE.Enc}(abepp,(l_{\Delta},i,\gamma,\beta),\boldsymbol{c}_{i,\gamma,\beta})$ 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．$\boldsymbol{c}_{i,\gamma,\Delta_{i,\gamma}}\leftarrow\mathrm{ABE.Dec}(abesk_{\Delta},\psi_{i,\gamma,\Delta_{i,\gamma}})$ もし，$\perp=\mathrm{ABE.Dec}(abesk_{\Delta},\psi_{i,\gamma,\Delta_{i,\gamma}})$ であれば，$\perp$ を出力し，終了する．

(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．

4. 効率性の比較

本節では，著者らの提案した構成法 [14] と，[4] を利用して構成した semi-adaptive 安全な内積暗号との比較を行う．比較の際には，鍵属性空間，暗号文属性空間を $\mathrm{GF}(q)^{\mu}$ とする．多ビットの構成については，それぞれの selective 安全な構成において漸近的に同じ項に対して平文長の積が追加され，その項が漸近的に無視できることから,1 ビットの平文の場合の比較を行う．ABE.pp，ABE.sk，ABE.ct をそれぞれ KP-ABE の公開パラメータ，秘密鍵，暗号文とする．PKE.pp，PKE.sk，PKE.ct をそれぞれ公開鍵暗号 (PKE) の公開鍵，秘密鍵，暗号文とする．

[4] の変換では，PKE と Garbled Circuit を利用し，selective 安全な内積暗号の $2l$ 個 ($l=|pp|$) の公開鍵 PKE.pk，秘密鍵 PKE.sk，暗号文 PKE.ct を生成する必要があり，暗号文には Garbled Circuit が追加される．また，[13], [7], [12] の公開パラメータ長はそれぞれ $\mathcal{O}(\mu n^2\log^2 q)$，$\mathcal{O}(\mu n^2\log q)$，$\mathcal{O}(n^2\log^2 q)$ である．[12] は属性数が $\log(\lambda)$ の条件を満たす場合の構成であり，公開パラメータに属性数に依存した行列が含まれない特徴を持つ．属性数をパラメータとした比較ができないため，表での比較は行わない．なお，条件を統一し，属性数を $\log q$ として比較をすると，[12]+[4] のパラメータは [7]+[4] のパラメータに一致する．

表 1 に semi-adaptive 安全な内積暗号の構成のパラメータを示す．[14] では公開鍵，秘密鍵には KP-ABE のパラメータが追加されているのに対し，[4] による変換ではそれぞれ公開パラメータ長個の PKE のパラメータが追加されている．また，C は garbled circuit である．

[14] では [13] の方式を利用しているため、まず [14] と [13]+[4] に注目し，比較を行う。[13] の公開鍵長 $\mu n^2\log^2 q$ を基準として比較すると，[14] は公開パラメータ pp に $\log q$ の積と $|\mathrm{ABE.pp}|$ の和が追加されているのに対し，[13]+[4] では $2l$ 個 ($l=|pp|$) の公開鍵長 $|\mathrm{PKE.pk}|$ が積として追加されている．積に注目して比較すると，$\log q$ と $|\mathrm{PKE.pk}|$ がそれぞれ増加しており，$|\mathrm{PKE.pk}|$ が $\log q$ より

漸近的に大きいとき，[14] の公開パラメータ pp が [13]+[4] より小さくなる．

秘密鍵 sk を比較すると，[14] には |ABE.sk| が追加されており，[13]+[4] では [14] の第 2 項に対し，$n^2 \log q$ と PKE の秘密鍵長 |PKE.sk| の積が追加されている．

次に暗号文 ct について比較を行う．garbled circuit サイズ $|C|$ を考慮にいれずに比較を行うと，$|\text{ABE.ct}| < n^2 \log q |\text{PKE.ct}|$ を満たす場合に提案構成法は [13]+[4] より小さくなる．実際には, ここに garbled circuit サイズ $|C|$ の項が追加されることに注意する．

[7]+[4] の構成は [13]+[4] に比べ，公開鍵長の差である $\log q$ サイズが小さくなっている．

実際に LWE 仮定のもと安全な現在最も効率の良い方式としてそれぞれ PKE[6] と KP-ABE[2] を適用したときのパラメータを表 2 に示す．ここでは，$|\text{PKE.pk}| = n^2 \log q$，$|\text{PKE.sk}| = n \log q$，$|\text{PKE.ct}| = n \log q$，$|\text{ABE.pp}| = \mu n^2 \log^2 q$，$|\text{ABE.sk}| = n^2 \log^3 q$，$|\text{ABE.ct}| = n \log^2 q \log(\mu n \log q)$ とした．結論として, 表 2 より，n の次数を比較することにより，提案構成法 [14] が他の構成法に比べて，鍵サイズ及び暗号文サイズの観点から最も優れていることがわかる．

5. まとめ

本論文では, 2019 年 11 月の CSEC 研究発表会において著者らが提案した semi-adaptive 安全な内積暗号の構成 [14] と, 既存技術の組合せによる semi-adaptive 安全な内積暗号の構成（格子問題に基づく selective 安全な内積暗号に Goyal らの変換法 [4] を適用し semi-adaptive 安全にした方式）との比較を行った．その結果，鍵サイズ及び暗号文サイズの観点から, 著者らの構成法が最も優れていることを示した．

表 1 semi-adaptive 安全な内積暗号の公開パラメータ，秘密鍵，暗号文の比較

構成	$\|pp\|$	$\|sk\|$	$\|ct\|$
提案構成法	$\mu n^2 \log^3 q$ + |ABE.pp|	$n \log^2 q + 2\mu \log q$ + |ABE.sk|	$2\mu \log q$ × |ABE.ct|
[13]+[4]	$2\mu n^2 \log^2 q$ × |PKE.pk|	$n \log^2 q$ $+2\mu n^2 \log^2 q$ × |PKE.sk|	$2\mu n^2 \log^2 q$ × |PKE.ct| $+\|C\|$
[7]+[4]	$2\mu n^2 \log q$ × |PKE.pk|	$n \log^2 q$ $+2\mu n^2 \log q$ × |PKE.sk|	$2\mu n^2 \log q$ × |PKE.ct| + $\|C\|$

表 2 パラメータを代入した semi-adaptive 安全な内積暗号の公開パラメータ，秘密鍵，暗号文の比較

構成	$\|pp\|$	$\|sk\|$	$\|ct\|$
提案構成法	$\mu n^2 \log^3 q$ $+\mu n^2 \log^2 q$	$n \log^2 q + 2\mu \log q$ $+n^2 \log^3 q$	$2\mu n \log^3 q$ $\times \log(\mu n \log q)$
[13]+[4]	$2\mu n^4 \log^3 q$	$n \log^2 q$ $+2\mu n^3 \log^3 q$	$2\mu n^3 \log^3 q + \|C\|$
[7]+[4]	$2\mu n^4 \log^2 q$	$n \log^2 q$ $+2\mu n^3 \log^2 q$	$2\mu n^3 \log^2 q + \|C\|$

参考文献

[1] S. Agrawal, D. M. Freeman, V. Vaikuntanathan, "Functional Encryption for Inner Product Predicates from Learning with Errors." ASIACRYPT 2011, pp.21-40.

[2] D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, V. Nikolaenko, G. Segev, V. Vaikuntanathan, D. Vinayagamurthy "Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits." EUROCRYPT 2014, pp.533-55.

[3] Z. Brakerski, V. Vaikuntanathan, "Circuit-ABE from LWE: Unbounded Attributes and Semi-adaptive Security." CRYPTO 2016, pp.363-384.

[4] R. Goyal, V. Koppula, B. Waters, "Semi-adaptive Security and Bundling Functionalities Made Generic and Easy." TCC2016, pp.361-388.

[5] J. Katz, A. Sahai, B. Waters, "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products." EUROCRYPT 2008, pp.146-162.

[6] R. Lindner, C. Peikert, "Better Key Sizes (and Attacks) for LWE-Based Encryption." CT-RSA2011, pp.319-339.

[7] J. Li, D. Zhang, X. Lu, K. Wang, "Compact (Targeted Homomorphic) Inner Product Encryption from LWE." ICICS2017, pp.132-140.

[8] D. Micciancio, "Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions." Computational Complexity 2007, pp.365-411.

[9] D. Micciancio, C. Peikert, "Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller." EUROCRYPT 2012, pp.700-718.

[10] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography." STOC 2005, pp.84-93.

[11] A. Sahai, B. Waters, "Fuzzy Identity-Based Encryption." EUROCRYPT 2005, pp.457-473.

[12] Z. Wang, X.Fan, M.Wang, "Compact Inner Product Encryption from LWE." ICICS2017, pp.141-153.

[13] K. Xagawa, "Improved (Hierarchical) Inner-Product Encryption from Lattices. " Public key Cryptography 2013, pp.235-252.

[14] 宮澤智輝, 佐藤慎悟, 四方順司, "格子問題に基づく semi-adaptive 安全な内積暗号" 2019-CSEC-87，pp.1-8.