Middle-Product LWE仮定に基づく効率的な鍵失効機能付きIDベース暗号の構成

西村 拓海[1,a)]　高安 敦[1,2]

概要：Learning with Errors (LWE) 仮定の派生として Middle-Product LWE (MPLWE) 仮定がある．Gentry らの LWE ベースの ID ベース暗号 (identity-based encryption, IBE) 方式を変形し，Lombardi らはマスタ公開鍵長を削減した MPLWE ベースの IBE 方式を構成した．IBE に効率的な鍵失効機能を付与した暗号技術に鍵失効機能付き IBE (revocable IBE, RIBE) があり，Takayasu の方式は LWE ベースで最も効率的な RIBE 方式である．これまで MPLWE ベース RIBE 方式の具体的な構成は提案されていないが，Lombardi らの IBE 方式に Ma と Lin の一般的変換を適用すると MPLWE ベースの RIBE 方式を得られる．変換後の RIBE 方式は，Takayasu の方式と比べてマスタ公開鍵長が小さいが，暗号文長が大きくなってしまう．本稿で我々は，MPLWE ベースの RIBE 方式を提案する．提案方式は，Lambardi が Gentry らの LWE ベース方式を変形して MPLWE ベース IBE 方式を構成したように，Takayasu の LWE ベース方式を変形することで得られる．提案方式は，Lombardi らの方式と同等のマスタ公開鍵長と Takayasu らの方式と同等の暗号文長を持ち，格子ベースの最も効率的な RIBE 方式である．また，Takayasu の方式と同様，量子ランダムオラクルモデルにおいて緊密な帰着の下で匿名性を満たす．

キーワード：鍵失効機能付き ID ベース暗号，Middle-Product Learning with Errors，格子暗号

Efficient Revocable Identity-Based Encryption from Middle-Product LWE

Takumi Nishimura[1,a)]　Atsushi Takayasu[1,2]

Abstract: The Middle-Product Learning with Errors (MPLWE) assumption is a variant of the Learning with Errors (LWE) assumption. Recent studies have investigated MPLWE assumption-based cryptographic schemes based on LWE assumption. Lombardi et al. proposed an identity-based encryption (IBE) scheme based on MPLWE assumption. This scheme follows Gentry et al.'s IBE scheme based on LWE. Revocable Identity-based Encryption (RIBE) scheme based on MPLWE assumption can be constructed by combining Lombardi et al.'s IBE scheme with Ma and Lin's generic construction. However, this scheme is not efficient due to a large ciphertext. In this paper, we propose an RIBE scheme based on MPLWE assumption using Takayasu's RIBE scheme based on LWE assumption and the Lombardi et at.'s IBE scheme. The proposed method has a shorter master public key compared to the Takayasu's scheme because it is based not on LWE assumption but on MPLWE assumption. In addition, it has a shorter ciphertext compared to the RIBE schemes using Ma and Lin's generic construction. Furthermore, it is the first RIBE scheme based on MPLWE assumption which has a tight reduction in the quantum random oracle model and anonymity.

Keywords: Revocable Identity-based Encryption, Middle-Product Learning with Errors, Lattice-based Cryptography

[1] 東京大学
The University of Tokyo
[2] 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
[a)] takunishi23@g.ecc.u-tokyo.ac.jp

1. 序論

背景. Learning with Errors (LWE) 仮定 [18] に基づく格子暗号は，耐量子性を持ち高機能暗号を構成可能なため，活発に研究されている．Rosca ら [19] は LWE の派生として Middle-Product LWE (MPLWE) 仮定を提案した．MPLWE 問題は polynomial LWE 問題 [21] と同等に困難であり，LWE ベースの暗号方式を効率化できるため，公開鍵暗号 [15], [19] のみならず，電子署名 [3], [9], [14]，リング署名 [6], [14]，ID ベース暗号 (identity-based encryption, IBE) [7], [15]，階層型 IBE [13]，内積暗号 [27], [28] が構成されるなど近年注目を集めている．本稿では特に IBE に注目する．

Lombardi ら [15] は LWE ベースの Gentry らの IBE 方式 (GPV-IBE) [8] と Agrawal らの選択的安全な IBE 方式 [1] を変形し，初めての MPLWE ベース IBE 方式を提案した．Lombardi らは安全性証明を与えていないが，Gentry ら [8] や Agrawal ら [1] の証明技法によって証明可能であるとした．つまり，Lombardi らの第一方式はランダムオラクルモデル (random oracle model, ROM) で緊密ではない帰着の下で適応的匿名性を，第二方式は標準モデルで選択的匿名性を満たす．本稿は第一方式に注目し，LVV-IBE と呼ぶ．GPV-IBE はマスタ公開鍵長が $O(n^2 \log^2 n)$ で暗号文長は $(n \log^2 n)$ であるのに対し，LVV-IBE はマスタ公開鍵長が $O(n \log^2 n)$ で暗号文長は $(n \log^2 n)$ なので，より効率的である．同様に，Fan ら [7] は LWE ベースの Agrawal らの適応的安全な IBE 方式 [1] を変形することで標準モデルで適応的安全な MPLWE ベース IBE 方式を提案したが，Agrawal らと同様, 安全性ゲームにおいて攻撃者の秘密鍵クエリの回数が制限されている．そのため，LVV-IBE は現状唯一の真に適応的安全な MPLWE ベース IBE 方式である．ただし，LVV-IBE は量子 ROM (quantum ROM, QROM) での証明がないため厳密には耐量子性を持つとは限らないことに注意が必要である [26]．GPV-IBE は Katsumata ら [12] によって QROM で緊密な帰着を持つことが証明されているため耐量子性を持つが，Lambardi らは LVV-IBE が同様の証明を持つかを議論していない．

IBE は一般に不正ユーザの鍵を効率的に失効する手段がないという問題があり，Boldyreva ら [4] はこの機能を実現する暗号技術として鍵失効機能付き IBE (revocable IBE, RIBE) を定義した．Chen らによる初めての方式の構成 [5] 以降，様々な LWE ベース RIBE 方式が提案されてきた [10], [23], [24], [25] が，いずれも選択的安全性しか満たさなかった．初の適応的安全な LWE ベース RIBE 方式は，Ma と Lin の一般的変換 [16] に基づく構成である．Ma と Lin の変換は適応的安全性とマスタ公開鍵長を保存するという利点があるが，暗号文長が大きく，帰着損失が ID の記述長 L_{ID} に比例し，匿名性を満たさないという欠点があった．最も効率的な LWE ベース IBE である GPV-IBE に Ma と Lin の変換を適用すると，マスタ公開鍵長が $O(n^2 \log^2 n)$ で n ビット平文の暗号文長が $O(L_{\mathsf{ID}} n \log^2 n)$ である．Takayasu [22] は，GPV-IBE を変形することで，QROM で緊密な帰着の下で適応的匿名性を満たす LWE ベース RIBE 方式を構成した．Takayasu の RIBE 方式が QROM で緊密な帰着を持つのは，Katsumata らによる GPV-IBE の証明技法 [12] を用いていることに起因する．Takayasu の方式はマスタ公開鍵長が $O(n^2 \log^2 n)$ で n ビット平文の暗号文長が $O(L_{\mathsf{ID}} n \log n)$ であり，LWE ベースで最も効率的な RIBE 方式である．

Ma と Lin の変換 [16] が一般的であるため, LVV-IBE [15] に適用することで MPLWE ベース RIBE 方式を得られる．Ma と Lin の変換はマスタ公開鍵長を保存するため，LVV-IBE から得られる RIBE 方式のマスタ公開鍵長 $O(n \log^2 n)$ は LWE ベース既存方式より効率的である．ただし，Ma と Lin の変換は暗号文長が大きくなるため，LVV-IBE から得られる RIBE 方式の n ビット平文の暗号文長は $O(L_{\mathsf{ID}} n \log^2 n)$ であり，Takayasu の RIBE 方式より非効率である．さらに，Ma と Lin の変換を用いているために，帰着損失が ID の記述長 L_{ID} に比例し，匿名性を満たさない．また，LVV-IBE を用いているので，ROM での安全性の議論しかなく真に耐量子性を持つ保証がない．

貢献. 本稿で，我々は MPLWE ベース RIBE 方式を提案する．提案方式の設計思想は，簡潔に言えば Takayasu の RIBE 方式 [22] が GPV-IBE [8] に適用した変更を LVV-IBE [15] に適用することである．この設計思想自体は自然な発想だが，提案方式の安全性証明は自明ではない．より正確には，LVV-IBE と同様，ROM で帰着損失を許すならば容易に証明可能かもしれないが，Takayasu の RIBE 方式と同様，QROM で緊密な帰着を証明するのは技術的に難しい．つまり，Takayasu は提案 RIBE 方式の証明に Katsumata らによる GPV-IBE の証明技法 [12] を用いたが，LVV-IBE ではこれまで同様の証明が与えられていない．そのため, 我々はまず, Katsumata らによる GPV-IBE の証明技法が LVV-IBE にも適用可能であることを確認し，QROM で緊密な帰着を証明する．さらに，同様にして提案 RIBE 方式の QROM で緊密な帰着を証明する．そのため，本研究は MPLWE ベースの新たな RIBE 方式を提案するのみならず，最も効率的な MPLWE ベース IBE である LVV-IBE の改良した証明をも与えていることに注意されたい．

表 1 で，LWE 仮定や MPLWE 仮定に基づく適応的安全な RIBE 方式を比較する．ただし，平文は n ビットとする．効率に関してはマスタ公開鍵長と暗号文長を比較しており，マスタ公開鍵長は LVV-IBE に Ma-Lin 変換を適用した RIBE 方式と提案方式が最も小さく，暗号文長は

表 1　LWE 仮定と MPLWE 仮定に基づく適応的安全な RIBE 方式の比較.

方式	マスタ公開鍵長	暗号文長	仮定	匿名性	帰着損失	モデル
GPV-IBE [8] + Ma-Lin [16]	$O(n^2\log^2 n)$	$O(L_{\mathsf{ID}}n\log^2 n)$	LWE		$O(L_{\mathsf{ID}})$	QROM
Takayasu RIBE [22]	$O(n^2\log^2 n)$	$O(L_{\mathsf{ID}}n\log n)$	LWE	✓	$O(1)$	QROM
LVV-IBE [15] + Ma-Lin [16]	$O(n\log^2 n)$	$O(L_{\mathsf{ID}}n\log^2 n)$	MPLWE		$O(QL_{\mathsf{ID}})$	ROM
提案方式	$O(n\log^2 n)$	$O(L_{\mathsf{ID}}n\log n)$	MPLWE	✓	$O(1)$	QROM

Takayasu の RIBE 方式と提案方式が最も小さい．つまり，提案方式が最も効率的な格子ベース RIBE 方式である．表 1 では議論していないが，秘密鍵長・更新鍵長は全ての方式で同じで，復号鍵長は暗号文長に比例する．LVV-IBE に Ma-Lin 変換を適用した RIBE 方式の帰着損失とモデルは，Lombardi ら [15] の証明に基づいていることに注意されたい．Q は攻撃者のランダムオラクルクエリの回数を表しているが，我々の改良証明に基けば QROM で帰着損失は $O(L_{\mathsf{ID}})$ に改善される．

最後に，本稿で我々は Boldyreva ら [4] が定義した最も単純な安全性モデルを用いるが，RIBE にはより強い安全性モデルがあるのでその点について触れる．Seo と Emura [20] は，復号鍵漏洩耐性 (decryption key exposure resistance, DKER) と呼ばれる安全性を定義した．LWE ベースで DKER を満たす適応的安全な RIBE 方式は構成可能だと考えられているが，これまで具体的な構成が与えられていない．[*1] さらに，DKER を満たす全ての既存の RIBE 方式は匿名性を満たさないので，本稿では扱っていない．ただし，選択的安全な方式ならば，提案方式と既存の MPLWE ベース階層型 IBE 方式 [13] に Katsumata らの変換 [10] を適用することで得られる．Takayasu と Watanabe [23], [24] は，匿名性と DKER を両立させるために回数制限付き DKER を考えた．本稿では紙面の都合で省略するが，Takayasu の RIBE 方式 [22] は匿名性と回数制限付き DKER を両立する RIBE 方式に変形可能であり，提案方式も同様の変形が可能である．

本稿の構成. 前述の通り LVV-IBE の改良した安全性証明を得ているが，紙面の都合で本稿では省略する．第 2 章で数学的準備を行い，第 3 章で RIBE の定義を与える．第 4 章で提案 RIBE 方式の構成を与え，第 5 章で安全性証明を行う．

2. 準備

安全性パラメータを λ とする．$\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ とする．$n, m > 0$ について $[n] = \{1, \ldots, n\}, [n, m] = \{n, \ldots, m\}$ とする．ベクトル $\mathbf{a} \in \mathbb{R}^n$ について $\|\mathbf{a}\|, \|\mathbf{a}\|_\infty$ をそれぞれ $\mathbf{a}$ の L_2 ノルム, L_∞ ノルムとする．実数体上の n 次多項式 a について $\|a\|, \|a\|_\infty$ をそれぞれ, 多項式 a の係数ベクトルの L_2 ノルム, L_∞ ノルムと定義する．$\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ を, 集合 $\mathcal{X}$ から集合 $\mathcal{Y}$ への全ての関数の集合とする．x を確率分布 D に従ってサンプルするとき $x \leftarrow D$ と書く．集合 S から一様にサンプルするとき $x \xleftarrow{\mathrm{U}} S$ と書く．集合 Ω 上の確率分布 χ に対して, X を χ に従う確率分布, $\Omega_+ = \{x \in \Omega \mid \Pr[X = x] > 0\}$ とし，$H_\infty(\chi) = -\log_2 \min_{x \in \Omega_+} \Pr[X = x]$ と定義する．

多項式と行列. 行列 $\mathbf{A} \in \mathbb{R}^{d \times d}$ と $k < d$ に対して $\mathbf{A}^{(k)} \in \mathbb{R}^{k \times d}$ を $\mathbf{A}$ の上 k 行からなる行列とする．行列 $\mathbf{M}$ の最大特異値を $s_1(\mathbf{M})$ と表す．実対称行列 $\mathbf{P} \in \mathbb{R}^{n \times n}$ が任意の $\mathbf{x} \in \mathbb{R}^n$ について $\mathbf{x}^\top \mathbf{P} \mathbf{x} \geq 0$ を満たすとき $\mathbf{P}$ を半正定値行列と呼ぶ.

実数体上の $n-1$ 次多項式 a について，$\mathbf{a} \in \mathbb{R}^n$ を a の係数ベクトルをとする．また，ベクトル $\mathbf{a} \in \mathbb{R}^n$ について，a を係数ベクトルが $\mathbf{a}$ である実数体上の $n-1$ 次多項式とする．環 R に対して $R^{<d}[X]$ を次数が高々 $d-1$ の R 上の多項式の集合とする．

定義 1 ([19]). $d, k > 0$ とする．$a \in R^{<k}[X]$ に対して，$T^{d,k}(a) \in R^{d \times (k+d-1)}$ を，$i = 1, \ldots, d$ について，第 i 行が $x^{i-1} \cdot a$ の係数ベクトルである行列とする．定義から $T^{1,k}(a)$ は a の係数ベクトルである.

定義 2 ([19]). 次数 m の多項式 $f \in \mathbb{Z}[X]$ に対して, $\mathrm{EF}(f)$ を $\mathrm{EF}(f) = \max_{g \in \mathbb{Z}^{<2m-1}[X]} \frac{\|f \mod g\|_\infty}{\|g\|_\infty}$ と定義する.

格子と離散ガウス分布. 線形独立な m 本のベクトル $\mathbf{b}_i \in \mathbb{R}^n$ により生成される n 次元の格子 Λ を $\Lambda = \{\sum_{i=1}^m x_i \mathbf{b}_i \mid x_i \in \mathbb{Z}\}$ と定義する．また, 任意の $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ と $\mathbf{u} \in \mathbb{Z}_q^n$ に対して，$\Lambda_{\mathbf{u}}^\perp(\mathbf{A})$ を $\Lambda_{\mathbf{u}}^\perp(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}_q^m \mid \mathbf{A}\mathbf{z} = \mathbf{u}\}$ と定義する．半正定値行列 $\Sigma \in \mathbb{R}^{n \times n}$ に対して格子 $\Lambda \subset \mathbb{R}^n$ 上の離散ガウス分布 $D_{\Lambda,\Sigma}$ を，サンプルした値が $\mathbf{x}$ となる確率が $\frac{\rho_{\mathbf{\Sigma}}(\mathbf{x})}{\sum_{\mathbf{x} \in \Lambda} \rho_{\mathbf{\Sigma}}(\mathbf{x})}$ である確率分布とする．ただし $\rho_{\mathbf{\Sigma}}(\mathbf{x}) = \exp(-\pi \mathbf{x}^\top \mathbf{\Sigma}^{-1} \mathbf{x})$ とする．特に単位行列 $\mathbf{I}_n$ と実数 σ を用いて $\Sigma = \sigma \mathbf{I}_n$ と書けるならば $D_{\Lambda,\sigma}$ と書く.

補題 1 ([15]). $\varepsilon \in (0, \frac{1}{2})$, $\sigma \geq \sqrt{\ln(1+\varepsilon^{-1})/\pi}$, $t > \omega(\sqrt{\log n})$ とする．$x \leftarrow D_{\mathbb{Z},\sigma}$ とすると，n について圧倒的な確率で $|x| \leq \sqrt{t}\sigma$ が成立する.

補題 2 ([15]). χ を $\mathbb{Z}_q$ 上の確率分布とし, $\delta \in (0, 1)$ に対して $H_\infty(\chi) \geq -\log \delta$ が成立するとする．$a_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n}[X]$ および $r_i \leftarrow \chi^d[X]$ として, $S = (\mathbb{Z}_q^{<n}[X])^t \times \mathbb{Z}_q^{<n+d-1}[X]$ 上の確率分布 $V = ((a_i)_{i \in [t]}, \sum_{i=1}^t a_i r_i)$ を定義する．このとき $d \leq n$, $\delta^t q = o(1)$, $q = \mathsf{poly}(n)$, $\delta^{-1} = \omega(1)$, $\frac{dt}{n} = \Omega(\log n)$

[*1] Wang ら [25] は ROM で適応的安全な LWE ベース階層型 RIBE 方式を提案したと主張しているが，参考にしている Agrawal らの LWE ベース階層型 IBE 方式 [2] が選択的安全であるため，安全証明が疑わしい.

ならば V は $U(S)$ と統計的に識別不能である．

補題 3 ([15])．$\chi = D_{\mathbb{Z},\sigma}$ とし，$\chi_q = \chi \mod q$ とする．$q = \mathsf{poly}(n)$，$q = \omega(\sigma\sqrt{\log n})$，$\sigma = \omega(1)$ ならば，ある定数 c について $H_\infty(\chi_q) \geq \log \frac{q}{c}$ が成立する．

補題 4 ([8], [15])．n, q, d, t, γ, τ を正の整数とし，σ を離散ガウス分布のパラメータとする．以下の確率的多項式時間アルゴリズムが存在する．

- $\mathsf{TrapGen}(1^n) \to ((a_i)_{i\in[t+\gamma\tau]}, (w_{ij})_{(i,j)\in[t]\times[\gamma\tau]})$：$n$ を入力とし $(a_i)_{i\in[t+\gamma\tau]} \in (\mathbb{Z}_q^{<n}[X])^t \times (\mathbb{Z}_q^{<n+d-1}[X])^{\gamma\tau}$ と $(w_{i,j})_{(i,j)\in[t]\times[\gamma\tau]} \in (\mathbb{Z}_q^{<d}[X])^{t\gamma\tau}$ を出力する．$(a_i)_{i\in[t+\gamma\tau]}$ は一様サンプルと統計的に識別不能である．また各 $j \in [\gamma\tau]$ について $a_{t+j} = 2^{j-1-\lfloor\frac{j-1}{\tau}\rfloor\tau} x^{d\lfloor\frac{j-1}{\tau}\rfloor} - \sum_{i=1}^{t} a_i w_{i,j}$ を満たす．
- $\mathsf{SamplePre}((a_i)_{i\in[t+\gamma\tau]}, (w_{i,j})_{(i,j)\in[t]\times[\gamma\tau]}, u, \sigma) \to (r_i)_{i\in[t+\gamma\tau]}$：$(a_i)_{i\in[t+\gamma\tau]}, (w_{i,j})_{(i,j)\in[t]\times[\gamma\tau]}$，$u \in \mathbb{Z}_q^{<n+2d-2}[X], \sigma$ を入力として $(r_i)_{i\in[t+\gamma\tau]} \in (\mathbb{Z}_q^{<2d-1}[X])^t \times (\mathbb{Z}_q^{<d}[X])^{\gamma\tau}$ を出力する．$\mathbf{A} = (T^{2d-1,n}(a_1)^\top | \dots | T^{d,n+d-1}(a_{t+\gamma\tau})^\top)$ とすると $\mathbf{r} = (\mathbf{r}_1 | \dots | \mathbf{r}_{t+\gamma\tau})$ の分布は離散ガウス分布 $D_{\Lambda_{\mathbf{u}}^\perp(\mathbf{A}),\sigma}$ と統計的に識別不能である．各 $i \in [t+\gamma\tau]$ について $T^{2d-1,n}(a_i)^\top T^{1,2d-1}(r_i)^\top = T^{1,n+2d-2}(a_i r_i)^\top$ が成立するため，$\Lambda_{\mathbf{u}}^\perp(\mathbf{A}) = \{\mathbf{r} \mid \sum_{i=1}^{t+\gamma\tau} a_i r_i = u\}$ である．
- $\mathsf{Sample}\mathbb{Z}(\sigma) \to \mathbf{e}$：入力として $\sigma > 16\sqrt{\log 2m/\pi}$ を受け取り，$\mathbf{e} \in \mathbb{Z}^m$ を出力する．$\mathbf{e}$ の分布は $D_{\mathbb{Z}^m,\sigma}$ と統計的に識別不能である．

Middle-Product Learning with Errors．

定義 3 ([19])．d_a, d_b, d, k を $d_a + d_b - 1 = d + 2k$ を満たす正の整数とする．*Middle Product* $\odot_d : R^{<d_a}[X] \times R^{<d_b}[X] \to R^{<d}[X]$ を $a \odot_d b = \left\lfloor \frac{(a\cdot b) \mod x^{k+d}}{x^k} \right\rfloor$ と定義する．この演算は入力多項式の乗算結果の係数の中間 d 個を抜き出す演算である．例えば $(d_a, d_b, d, k) = (3, 5, 3, 2), (a, b) = (x^2 + 2x + 3, x^4 + 2x^3 + 3x^2 + 4x + 5)$ とすると $a \cdot b = x^6 + 4x^5 + 10x^4 + 16x^3 + 22x^2 + 22x + 15$ なので中間の項 3 つを抜き出して $a \odot_3 b = 10x^2 + 16x + 22$ となる．

補題 5 ([19])．$d, k, n > 0$ とする．任意の $r \in R^{<k+1}[X], a \in R^{<n}[X], s \in \mathbb{Z}_q^{<n+d+k-1}[X]$ に対して $r \odot_d (a \odot_{d+k} s) = (ar) \odot_d s$ が成立する．

定義 4 (MPLWE 分布 [3])．$n, d > 0, q \geq 2$ とする．また，χ を $\mathbb{Z}_q$ 上の分布とする．$s \in \mathbb{Z}_q^{<n+d-1}[X]$ に対して，$a \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n}[X], \mathbf{e} \leftarrow \chi^d$ として，$(a, b = a \odot_d s + e) \in \mathbb{Z}_q^{<n}[X] \times \mathbb{Z}_q^{<d}[X]$ の分布を $\mathsf{MP}_{q,n,d,\chi}(s)$ とする．

定義 5 (Degree-Parametrized MPLWE 仮定 [15])．$n > 0$ を偶数，$q \geq 2, m > 0, \mathbf{d} = (d_i)_{i\in[t]} \in [\frac{n}{2}]^t$ とする．また χ_e, χ_s を $\mathbb{Z}_q$ 上の分布とする．$\mathbf{s} \leftarrow \chi^{n-1}$ とする．$i \in [t]$ について，$a_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n-d_i}[X], \mathbf{e}_i \leftarrow \chi_e^{d_i}$ として，$(a_i, b_i = a_i \odot_{d_i} s + e_i)_{i\in[t]}$ の分布を $\mathsf{dpMP}_{q,n,\mathbf{d},\chi_e}(s)$ とする．$i \in [t]$ について，$w_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<d_i}[X], \mathbf{e}_i \leftarrow \chi_e^{d_i}$ を行い，$(a_i, b_i = w_i + e_i)_{i\in[t]}$ として得られる分布からの任意の個数のサンプルと，同じ個数の $\mathsf{dpMP}_{q,n,\mathbf{d},\chi_e}(s)$ からのサンプルを識別する問題が困難である事を $\mathsf{dpMPLWE}_{q,n,\mathbf{d},\chi_e,\chi_s}$ 仮定と呼ぶ．

以下は Katsumata と Yamada [11] の補題を Middle-Product に応用した補題である．

補題 6 ([11])．q, t, L を正の整数とし，各 $i \in [t]$，各 $\ell \in [L]$ について d_i, d_ℓ は $d_i - d_\ell + 1 > 0$ を満たす正の整数とする．$r > \max\{\omega(\sqrt{\log \sum_{i=1}^{t} d_i}), \omega(\sqrt{\log \sum_{\ell=1}^{L} d_\ell})\}$ を正の実数とする．また各 $i \in [t]$ について $w_i \in \mathbb{Z}_q^{<d_i}[X]$ を任意の多項式とし，$\mathbf{e}_i \leftarrow D_{\mathbb{Z}_q^{d_i},r}$ とする．$((v_{\ell,i})_{i\in[t]})_{\ell\in[L]} \in ((\mathbb{Z}_q^{<d_i-d_\ell+1}[X])^t)^L$ と正の実数 $\sigma > \sum_{\ell=1}^{L} s_1([T^{d_\ell,d_1-d_\ell+1}(v_{\ell,1})| \dots | T^{d_\ell,d_t-d_\ell+1}(v_{\ell,t})]) + 1$ に対して，確率的多項式時間アルゴリズム $\mathsf{Rerand}(((v_{\ell,i})_{i\in[t]})_{\ell\in[L]}, (w_i + e_i)_{i\in[t]}, r, \sigma)$ が存在し，$((\bar{b}_i = w_i + \bar{e}_i)_{i\in[t]}, (\bar{b}'_\ell = \sum_{i=1}^{t} v_{\ell,i} \odot_{d_\ell} w_i + \bar{e}'_\ell)_{\ell\in[L]})$ を出力する．ただし，各 $i \in [t]$ について $\bar{\mathbf{e}}_i$ の分布は $D_{\mathbb{Z}^{d_i},2r\sigma}$ と統計的に識別不能であり，各 $\ell \in [L]$ について $\bar{\mathbf{e}}'_\ell$ の分布は $D_{\mathbb{Z}^{d_\ell},2r\sigma}$ と統計的に識別不能である．

3. 鍵失効機能付き ID ベース暗号

本章では，Katsumata ら [10] と Takayasu [22] による定式化をもとに RIBE の定義を与える．既存研究と同様に，RIBE の鍵失効アルゴリズムは新しく失効されたユーザを鍵失効者リストに加える操作とし，リストに加えられたユーザの削除は行わないとする．

シンタックス． RIBE 方式 Π は以下の六つのアルゴリズムから構成される．各 ID は ID 空間 $\mathcal{ID}$ に含まれ，時刻 T の鍵失効者リストを $\mathsf{RL}_\mathsf{T} \subset \mathcal{ID}$ とする．また平文空間を $\mathcal{M}$，時刻空間を $\mathcal{T} = \{1, \dots, T_{\max}\}$，暗号文空間を $\mathcal{CT}$ とする．

- $\mathsf{Setup}(1^n) \to (\mathsf{mpk}, \mathsf{msk})$： 安全性パラメータ 1^λ を入力としマスタ公開鍵 mpk，マスタ秘密鍵 mpk を出力する．
- $\mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID}) \to \mathsf{sk}_\mathsf{ID}$： mpk，msk，$\mathsf{ID} \in \mathcal{ID}$ を入力として，秘密鍵 sk_ID を出力する．
- $\mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T}, \mathsf{RL}_\mathsf{T}) \to \mathsf{ku}_\mathsf{T}$： mpk，msk，時刻 $\mathsf{T} \in \mathcal{T}$，時刻 T での鍵失効者リスト $\mathsf{RL}_\mathsf{T} \subset \mathcal{ID}$ を入力として，時刻 T の更新鍵 ku_T を出力する．
- $\mathsf{DKGen}(\mathsf{mpk}, \mathsf{sk}_\mathsf{ID}, \mathsf{ku}_\mathsf{T}) \to \mathsf{dk}_{\mathsf{ID},\mathsf{T}} / \perp$： $\mathsf{mpk}, \mathsf{sk}_\mathsf{ID}, \mathsf{ku}_\mathsf{T}$ を入力として $(\mathsf{ID}, \mathsf{T})$ の復号鍵 $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ を出力する．ただし ID の鍵が既に失効しているならば $\perp$ を出力する．
- $\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{T}, \mathsf{m}) \to \mathsf{ct}_{\mathsf{ID},\mathsf{T}}$： mpk，ID，T，平文 $\mathsf{m} \in \mathcal{M}$ を入力として，暗号文 $\mathsf{ct}_{\mathsf{ID},\mathsf{T}}$ を出力する．
- $\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}}) \to \mathsf{m}'$： $\mathsf{mpk}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}}$ を入力として，復号結果 m' を出力する．

正当性． 暗号文 $\mathsf{ct}_{\mathsf{ID},\mathsf{T}}$ は，鍵が失効していなければ復号鍵 $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ によって正当に復号される必要がある．この制約を満たすため，全ての復号鍵 $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ 生成の状況を想定

する．すなわち任意の $\lambda \in \mathbb{N}$，$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^n)$，$\mathsf{ID} \in \mathcal{ID}$，$\mathsf{T} \in \mathcal{T}$，$\mathsf{m} \in \mathcal{M}$，$\mathsf{RL_T} \subset \mathcal{ID} \setminus \{\mathsf{ID}\}$ について，以下の操作により得られた m' が $\mathsf{m}' = \mathsf{m}$ を満たす事を要請する：(1) $\mathsf{sk_{ID}} \leftarrow \mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID})$．(2) $\mathsf{ku_T} \leftarrow \mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T}, \mathsf{RL_T})$．(3) $\mathsf{dk_{ID,T}} \leftarrow \mathsf{DKGen}(\mathsf{mpk}, \mathsf{sk_{ID}}, \mathsf{ku_T})$．(4) $\mathsf{ct_{ID,T}} \leftarrow \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{T}, \mathsf{m})$．(5) $\mathsf{m}' \leftarrow \mathsf{Decrypt}(\mathsf{mpk}, \mathsf{dk_{ID,T}}, \mathsf{ct_{ID,T}})$．

安全性． RIBE の安全性は攻撃者 $\mathcal{A}$ とチャレンジャー $\mathcal{C}$ 間の安全性ゲームにより定義される．このゲームには現在時刻を表すカウンタ $\mathsf{T_{cu}}$ が存在し，$\mathsf{T_{cu}} = 1$ により初期化する．本稿で述べる安全性は適応的匿名性である．

安全性ゲームの始めに，$\mathcal{C}$ は $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$ を実行する．さらに，リスト SKList を $\mathsf{SKList} = (\mathsf{ID} = \mathsf{kgc}, \mathsf{msk})$ によって初期化する．加えて，最初の時刻 $\mathsf{T_{cu}} = 1$ における更新鍵 ku_1 を $\mathsf{ku}_1 \leftarrow \mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T} = 1, \mathsf{RL}_1 = \phi)$ によって初期化する．その後，$\mathcal{C}$ は mpk と ku_1 を $\mathcal{A}$ に送る．$\mathcal{A}$ は以下の四つのクエリを適応的に行う．

秘密鍵生成クエリ． $\mathcal{A}$ によるクエリ $\mathsf{ID} \in \mathcal{ID}$ に対して，$\mathcal{C}$ は $(\mathsf{ID}, *) \in \mathsf{SKList}$ であるか確認し，そうならば $\perp$ を $\mathcal{A}$ に返す．そうでないならば $\mathsf{sk_{ID}} \leftarrow \mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID})$ を実行し，$(\mathsf{ID}, \mathsf{sk_{ID}})$ を SKList に加える．ただし，$\mathcal{A}$ には何も返さない．

秘密鍵漏洩クエリ． チャレンジクエリの前は $\mathcal{A}$ によるクエリ $\mathsf{ID} \in \mathcal{ID}$ に対して，$\mathcal{C}$ はある $\mathsf{sk_{ID}}$ が存在し $(\mathsf{ID}, \mathsf{sk_{ID}}) \in \mathsf{SKList}$ であるか確認し，そうならば $\mathsf{sk_{ID}}$ を $\mathcal{A}$ に送る．チャレンジクエリの後は $\mathsf{ID} = \mathsf{ID}^\star$ かつ $\mathsf{T_{cu}} \geq \mathsf{T}^\star$ ならば $\mathcal{A}$ に $\perp$ を返す．そうでなければチャレンジクエリの前と同じ操作により $\mathsf{sk_{ID}}$ を $\mathcal{A}$ に返す．

鍵失効および更新鍵生成クエリ． チャレンジクエリの前は，$\mathcal{A}$ によるクエリ $\mathsf{RL} \subseteq \mathcal{ID}$ に対して，$\mathcal{C}$ は $\mathsf{RL_{T_{cu}}} \subseteq \mathsf{RL}$ と全ての $\mathsf{ID} \in \mathsf{RL}$ に対して $(\mathsf{ID}, *) \in \mathsf{SKList}$ を確認する．成立しないならば $\perp$ を $\mathcal{A}$ に送信する．成立するならば $\mathsf{T_{cu}} \leftarrow \mathsf{T_{cu}} + 1$ および $\mathsf{RL_{T_{cu}}} \leftarrow \mathsf{RL}$ として，$\mathsf{ku_{T_{cu}}} \leftarrow \mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T}, \mathsf{RL_{T_{cu}}})$ を実行する．その後 $\mathsf{ku_{T_{cu}}}$ を $\mathcal{A}$ に送る．チャレンジクエリの後は，$\mathsf{T_{cu}} = \mathsf{T}^\star - 1$ かつ，$\mathcal{A}$ が既にクエリ $\mathsf{ID}^\star$ の秘密鍵漏洩クエリを行っており，$\mathsf{ID}^\star \in \mathsf{RL_T}$ であるか確認する．そうでないならば $\perp$ を $\mathcal{A}$ に返す．この条件が成立するならばチャレンジクエリの前と同じ操作により $\mathsf{ku_{T_{cu}}}$ または $\perp$ を $\mathcal{A}$ に返す．

チャレンジクエリ． $\mathcal{A}$ は安全性ゲーム内で一度だけこのクエリを行う．$\mathcal{A}$ のクエリ $(\mathsf{m}^\star, \mathsf{ID}^\star, \mathsf{T}^\star)$ に対して $\mathcal{C}$ は一様ランダムに $\mathsf{coin} \xleftarrow{\mathrm{U}} \{0,1\}$ を選ぶ．$\mathsf{coin} = 0$ ならばチャレンジ暗号文 $\mathsf{ct}^\star \leftarrow \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}^\star, \mathsf{T}^\star, \mathsf{m}^\star)$ を計算し $\mathcal{A}$ に送る．$\mathsf{coin} = 1$ ならば暗号文空間を $\mathcal{CT}$ としてチャレンジ暗号文 $\mathsf{ct}^\star \xleftarrow{\mathrm{U}} \mathcal{CT}$ を $\mathcal{A}$ に送る．

ある時点で，$\mathcal{A}$ は coin の推定値 $\widehat{\mathsf{coin}} \in \{0,1\}$ を出力し，安全性ゲームを終了する．

この安全性ゲームにおける $\mathcal{A}$ の優位性を $\mathrm{Adv}^{\mathrm{RIBE}}_{\Pi,\mathcal{A}}(\lambda) = |\Pr[\widehat{\mathsf{coin}} = \mathsf{coin}] - \frac{1}{2}|$ と定義する．

定義 6. 任意の確率的多項式時間攻撃者 $\mathcal{A}$ に対して，$\mathrm{Adv}^{\mathrm{RIBE}}_{\Pi,\mathcal{A}}(\lambda) = \mathrm{negl}(\lambda)$ であるとき，*RIBE* 方式 Π は適応的匿名性を満たすという．

4. 提案方式

本章では MPLWE 仮定に基づく RIBE 方式を提案する．

4.1 準備

提案方式で用いるパラメータを説明する．具体的なパラメータ設定については後述する．$n, q, d, t, k, \gamma, \tau, L_{\mathsf{ID}}, \mathsf{T}$ を正の整数とする．q を素数とする．α, α', σ は正の実数で，離散ガウス分布のパラメータである．平文空間，暗号文空間，ID 空間をそれぞれ $\mathcal{M} = \{0,1\}^{k+2}$，$\mathcal{CT} = (\mathbb{Z}_q^{<2d+k}[X])^t \times (\mathbb{Z}_q^{<d+k+1}[X])^{\gamma\tau} \times (\mathbb{Z}_q^{<k+2}[X])^{L_{\mathsf{ID}}+1}$，$\mathcal{ID} = 0\|\{0,1\}^{L_{\mathsf{ID}}}$ と定義する．また，$\mathsf{ID} \in \mathcal{ID}$ について $\mathsf{ID}[\ell]$ を ID の上位 $\ell + 1$ ビットの値と定める．時刻空間を $\mathcal{T} = \{1, \ldots, \mathsf{T}_{\max}\}$ と定義する．ハッシュ関数 $H : \{0,1\}^{\leq L_{\mathsf{ID}}+1} \times [0, \mathsf{T}_{\max}] \to \mathbb{Z}_q^{<n+2d-2}[X]$ を証明中ではランダムオラクルとして扱う．

KGC は $2^{L_{\mathsf{ID}}}$ 個の葉ノードを持つ二分木 BT によりユーザー ID を管理する．BT の深さ i のノードは 1 ビット目が 0 である $i+1$ ビットバイナリ列が割り当てられている．特に，根ノードは 0 が割り当てられる．バイナリビット列 θ が割り当てられているノードの子ノードは左右それぞれ $\theta\|0$ と $\theta\|1$ が割り与えられる．鍵失効を行う際のアルゴリズムは KUNode アルゴリズム [17] を用いる．KUNode アルゴリズムは，葉ノードの集合 $\mathsf{RL_T} = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_R\}$ を入力として，ノードの集合 $\mathcal{KU_T} = \{\theta_1, \ldots \theta_r\}$ を出力する．KUNode アルゴリズムの性質から，$\mathsf{ID} \notin \mathsf{RL_T}$ ならば，ある $\ell \in [0, L_{\mathsf{ID}}]$ について $\mathsf{ID}[\ell] \in \mathcal{KU_T}$ を満たすノード $\mathsf{ID}[\ell]$ が一意に存在し，$\mathsf{ID} \in \mathsf{RL_T}$ ならば，全ての $\ell \in [0, L_{\mathsf{ID}}]$ について $\mathsf{ID}[\ell] \in \mathcal{KU_T}$ を満たすノード $\mathsf{ID}[\ell]$ が存在しない．また $|\mathcal{KU_T}| = O(|\mathsf{RL_T}|(L_{\mathsf{ID}} - \log|\mathsf{RL_T}|))$ である．

4.2 構成

提案 RIBE 方式は以下のアルゴリズムから構成される．

$\mathsf{Setup}(1^n) \to (\mathsf{mpk}, \mathsf{msk})$：
$((a_i)_{i\in[t+\gamma\tau]}, (w_{i,j})_{(i,j)\in[t]\times[\gamma\tau]}) \leftarrow \mathsf{TrapGen}(1^n)$ を実行する．その後マスタ公開鍵 $\mathsf{mpk} = (a_i)_{i\in[t+\gamma\tau]}$ とマスタ秘密鍵 $\mathsf{msk} = (w_{i,j})_{(i,j)\in[t]\times[\gamma\tau]}$ を出力する．

$\mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID}) \to \mathsf{sk_{ID}}$：
$(r_{\mathsf{ID},i})_{i\in[t+\gamma\tau]} \leftarrow \mathsf{SamplePre}(\mathsf{mpk}, \mathsf{msk}, u_{\mathsf{ID}}, \sigma)$ を実行する．ただし，$u_{\mathsf{ID}} = H(\mathsf{ID}, 0)$ とする．SamplePre の性質から，$\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i} = u_{\mathsf{ID}}$ を満たす．秘密鍵 $\mathsf{sk_{ID}} = (r_{\mathsf{ID},i})_{i\in[t+\gamma\tau]}$ を出力する．

$\mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T}, \mathsf{RL}_\mathsf{T}) \to \mathsf{ku}_\mathsf{T}$： $\mathsf{RL}_\mathsf{T} \subset \mathcal{ID}$ を入力として，KUNode アルゴリズムによりノードの集合 $\mathcal{KU}_\mathsf{T} = \{\theta_1, \ldots \theta_r\}$ を得る．各ノード θ_j に対して，$(r_{\mathsf{T},\theta_j,i})_{i\in[t+\gamma\tau]} \leftarrow \mathsf{SamplePre}(\mathsf{mpk}, \mathsf{msk}, u_{\mathsf{T},\theta_j}, \sigma)$ を実行する．ただし，$u_{\mathsf{T},\theta_j} = H(\theta_j, \mathsf{T})$ とする．その後，時刻 T の更新鍵 $\mathsf{ku}_\mathsf{T} = (\mathcal{KU}_\mathsf{T}, (r_{\mathsf{T},\theta_j,i})_{i\in[t+\gamma\tau]})_{\theta_j\in\mathcal{KU}_\mathsf{T}}$ を出力する．更新鍵は $\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{T},\theta_j,i} = u_{\mathsf{T},\theta_j}$ を満たす．

$\mathsf{DKGen}(\mathsf{mpk}, \mathsf{sk}_\mathsf{ID}, \mathsf{ku}_\mathsf{T}) \to \mathsf{dk}_{\mathsf{ID},\mathsf{T}} / \perp$： $\mathcal{KU}_\mathsf{T} = \{\theta_1, \ldots, \theta_r\}$ を入力としてある $\ell \in [L_\mathsf{ID}+1]$ について $\mathsf{ID}[\ell] = \theta_j$ を満たす θ_j を見つける．そのような θ_j が存在しないなら $\perp$ を，存在するなら $(\mathsf{ID}, \mathsf{T})$ の復号鍵 $\mathsf{dk}_{\mathsf{ID},\mathsf{T}} = (d_{\mathsf{ID},\mathsf{T},i})_{i\in[t+\gamma\tau]} = (r_{\mathsf{ID},i} + r_{\mathsf{T},\theta_j,i})_{i\in[t+\gamma\tau]}$ を出力する．復号鍵は $\sum_{i=1}^{t+\gamma\tau} a_i d_{\mathsf{ID},\mathsf{T},i} = \sum_{i=1}^{t+\gamma\tau} a_i(r_{\mathsf{ID},i} + r_{\mathsf{T},\theta_j,i}) = u_{\mathsf{ID}} + u_{\mathsf{T},\theta_j}$ を満たす．

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{T}, \mathsf{m}) \to \mathsf{ct}_{\mathsf{ID},\mathsf{T}}$： $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+2d+k-1}[X]$ をサンプルする．各 $i \in [t]$ について $\mathbf{e}_i \leftarrow D_{\mathbb{Z}_q^{2d+k},\alpha' q}$ をサンプルし，各 $i \in [t+1, t+\gamma\tau]$ について $\mathbf{e}_i \leftarrow D_{\mathbb{Z}_q^{d+k+1},\alpha' q}$ をサンプルする．さらに，各 $\ell \in [L_\mathsf{ID}+1]$ について $\mathbf{e}'_\ell \leftarrow D_{\mathbb{Z}_q^{k+2},\alpha' q}$ をサンプルする．その後，

$b_i = a_i \odot_{2d+k} s + 2e_i \ (i \in [t])$

$b_i = a_i \odot_{d+k+1} s + 2e_i \ (i \in [t+1, t+\gamma\tau])$

$b'_\ell = \mathsf{m} + (u_\mathsf{ID} + u_{\mathsf{T},\mathsf{ID}[\ell]}) \odot_{k+2} s + 2e'_\ell \ (\ell \in [L_\mathsf{ID}+1])$

を計算し暗号文 $\mathsf{ct}_{\mathsf{ID},\mathsf{T}} = ((b_i)_{i\in[t+\gamma\tau]}, (b'_\ell)_{\ell\in[L_\mathsf{ID}+1]})$ を出力する．

$\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}}) \to \mathsf{m}'$： $\sum_{i=1}^{t+\gamma\tau} a_i d_{\mathsf{ID},\mathsf{T},i} = u_\mathsf{ID} + u_{\mathsf{T},\mathsf{ID}[\ell]}$ を満たす $\ell \in [L_\mathsf{ID}+1]$ を見つける．見つけた ℓ を用いて暗号文 $\mathsf{ct}_{\mathsf{ID},\mathsf{T}}$ の復号を

$$\mathsf{m}' = (b'_\ell - \sum_{i=1}^{t+\gamma\tau} b_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \mod q) \mod 2$$

の通りに計算し，復号結果 m' を出力する．

4.3 正当性とパラメータ設定

本節では提案 RIBE 方式の正当性と安全性証明を行うためのパラメータ設定を行う．

定理 1. $\alpha' < (4\sqrt{2}\omega(\log n)\sigma K + 1)^{-1}$ とする．ただし，$K = t(2d-1) + \gamma\tau d$ である．このとき，提案 *RIBE* 方式は圧倒的な確率で正当である．

証明. SKGen，KeyUp アルゴリズムの性質から各 $\ell \in [L_\mathsf{ID}+1]$ について

$$(u_\mathsf{ID} + u_{\mathsf{T},\mathsf{ID}[\ell]}) \odot_{k+2} s = \sum_{i=1}^{t+\gamma\tau} (a_i(r_{\mathsf{ID},i} + r_{\mathsf{T},\mathsf{ID}[\ell],i})) \odot_{k+2} s$$

$$= \sum_{i=1}^{t} (r_{\mathsf{ID},i} + r_{\mathsf{T},\mathsf{ID}[\ell],i}) \odot_{k+2} (a_i \odot_{2d+k} s) + \sum_{i=t+1}^{t+\gamma\tau} (r_{\mathsf{ID},i} + r_{\mathsf{T},\mathsf{ID}[\ell],i}) \odot_{k+2} (a_i \odot_{d+k+1} s) \quad (1)$$

が成立する．最後の等式変形は補題 5 を用いた．特に Decrypt アルゴリズムで見つけた $\ell \in [L_\mathsf{ID}+1]$ について $r_{\mathsf{ID},i} + r_{\mathsf{T},\mathsf{ID}[\ell],i} = d_{\mathsf{ID}+\mathsf{T},i}$ が成り立つので，

$$\begin{aligned} b'_\ell &= \mathsf{m} + (u_\mathsf{ID} + u_{\mathsf{T},\mathsf{ID}[\ell]}) \odot_{k+2} s + 2e'_\ell \\ &= \mathsf{m} + \sum_{i=1}^{t} d_{\mathsf{ID},\mathsf{T},i} \odot_{k+2} (a_i \odot_{2d+k} s) + \sum_{i=t+1}^{t+\gamma\tau} d_{\mathsf{ID},\mathsf{T},i} \odot_{k+2} (a_i \odot_{d+k+1} s) + 2e'_\ell \end{aligned}$$

が成立する．よって

$$\begin{aligned} & b'_\ell - \sum_{i=1}^{t+\gamma\tau} b_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\ &= \mathsf{m} + \sum_{i=1}^{t} d_{\mathsf{ID},\mathsf{T},i} \odot_{k+2} (a_i \odot_{2d+k} s) + \sum_{i=t+1}^{t+\gamma\tau} d_{\mathsf{ID},\mathsf{T},i} \odot_{k+2} (a_i \odot_{d+k+1} s) + 2e'_\ell - \sum_{i=1}^{t+\gamma\tau} b_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\ &= \mathsf{m} + \sum_{i=1}^{t} d_{\mathsf{ID},\mathsf{T},i} \odot_{k+2} (a_i \odot_{2d+k} s - b_i) + \sum_{i=t+1}^{t+\gamma\tau} d_{\mathsf{ID},\mathsf{T},i} \odot_{k+2} (a_i \odot_{d+k+1} s - b_i) + 2e'_\ell \\ &= \mathsf{m} + \underbrace{2(e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i})}_{\text{エラー項}} \end{aligned}$$

が成立する．最終行の式変形は各 $i \in [t]$ について $-e_i = a_i \odot_{2d+k} s - b_i$ が，各 $i \in [t+1, t+\gamma\tau]$ について $-e_i = a_i \odot_{d+k+1} s - b_i$ が成り立つ事を用いた．$\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty < \frac{q}{8}$ が成立するならば提案方式の復号は正当である．

補題 4 より $((r_{\mathsf{ID},i})_{i\in[t+\gamma\tau]}, u_\mathsf{ID})$ は，各 $i \in [t]$ について $r_{\mathsf{ID},i} \leftarrow D_{\mathbb{Z}^{2d-1},\sigma}[X]$ をサンプルし，各 $i \in [t+1, t+\gamma\tau]$ について $r_{\mathsf{ID},i} \leftarrow D_{\mathbb{Z}^d,\sigma}[X]$ をサンプルし，$u_\mathsf{ID} = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i}$ と計算した $((r_{\mathsf{ID},i})_{i\in[t+\gamma\tau]}, u_\mathsf{ID})$ と統計的に識別不能である．同様に $((r_{\mathsf{T},\mathsf{ID}[\ell],i})_{i\in[t+\gamma\tau]}, u_{\mathsf{T},\mathsf{ID}[\ell]})$ は，各 $i \in [t]$ について $r_{\mathsf{T},\mathsf{ID}[\ell],i} \leftarrow D_{\mathbb{Z}^{2d-1},\sigma}[X]$ をサンプルし，各 $i \in [t+1, t+\gamma\tau]$ について $r_{\mathsf{T},\mathsf{ID}[\ell],i} \leftarrow D_{\mathbb{Z}^d,\sigma}[X]$ をサンプルし，$u_{\mathsf{T},\mathsf{ID}[\ell]} = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{T},\mathsf{ID}[\ell],i}$ と計算した $((r_{\mathsf{T},\mathsf{ID}[\ell],i})_{i\in[t+\gamma\tau]}, u_{\mathsf{T},\mathsf{ID}[\ell]})$ と統計的に識別不能である．よって補題 1 より

$$\|\mathbf{r}_{\mathsf{ID},i}\|_\infty \le \omega(\sqrt{\log n})\sigma, \ \|\mathbf{r}_{\mathsf{T},\mathsf{ID}[\ell],i}\|_\infty \le \omega(\sqrt{\log n})\sigma$$

$$\|\mathbf{e}_i\|_\infty \le \omega(\sqrt{\log n})\alpha' q, \ \|\mathbf{e}'_\ell\|_\infty \le \omega(\sqrt{\log n})\alpha' q$$

が圧倒的な確率で成立する．以上より，

$$\begin{aligned} & \|e'_\ell + \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty \\ &\le \|e'_\ell\|_\infty + \|\sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty \\ &\le \omega(\sqrt{\log n})\alpha' q + K(\sqrt{2}\omega(\sqrt{\log n})\sigma)(\omega(\sqrt{\log n})\alpha' q) \end{aligned}$$

が成立する．よって $\alpha' < (8\sqrt{2}\omega(\log n)\sigma K + 1)^{-1}$ ならば，

$\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty < \frac{q}{8}$ が成立する． □

提案 RIBE 方式が正当かつ安全であるために，パラメータが満たすべき条件と必要な仮定は以下の通りである．

- 正当性のため，$\alpha' < (4\sqrt{2}\omega(\log n)\sigma K + 1)^{-1}$.
- 補題 4 より TrapGen アルゴリズムと SamplePre アルゴリズムを用いるため，$q = \mathsf{poly}(n)$，$d \leq n$，$\frac{dt}{n} = \Omega(\log n)$，$\sigma = \omega(\log^2 n)\sqrt{ndt}$，$\gamma = \frac{n+2d-2}{d}$.
- 補題 2，補題 3 より公開鍵が一様分布と統計的に識別不能であるため，q を素数として，$q = \omega(\sqrt{\log n})\sigma$.
- 補題 4 より，Sample$\mathbb{Z}$ アルゴリズムを用いるため，$\sigma > 16\sqrt{\log 2(2d-1)/\pi}$.
- 補題 6 より，ReRand アルゴリズムを用いるため，$\frac{\alpha'}{2\alpha} > \sqrt{2\sigma^2((2d-1)t + d\gamma\tau)(L_{\mathsf{ID}}+1)+1}$ かつ $\alpha q > t(2d+k) + \gamma\tau d + (K+2)(L_{\mathsf{ID}}+1)$.
- $\mathsf{dpMPLWE}_{q,n+2d+k,\mathbf{d},D_{\alpha q},U(\mathbb{Z}_q^{<n+2d+k-1}[X])}$ 仮定.

上記の条件を満たすため，$\delta > 0$ を任意の小さな値として

$$d = \Theta(n),\ k = \Theta(n),\ t = \log n,\ \gamma = \frac{n+2d-2}{d}$$
$$L_{\mathsf{ID}} = \Omega(n),\ q = n^{3.5+\delta},\ \tau = \lceil \log q \rceil,\ \sigma = n^{1+\delta}$$
$$\alpha' = n^{-1+2\delta},\ \alpha = n^{-3}$$

とパラメータを設定する．

5. QROM における安全性

本章では提案方式の QROM における安全性を証明する．

5.1 QROM

$\alpha_x \in \mathbb{C}$ は $\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$ を満たし，$\{|x\rangle\}_{x\in\{0,1\}^n}$ は $\mathbb{C}^{2^n}$ の正規直交基底とする．$\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \in \mathbb{C}^{2^n}$ を n 量子ビットが表す量子状態とする．この量子状態を観測した際にバイナリビット列 x が観測される確率は $|\alpha_x|^2$ である．QROM では，ROM と同様に理想的なハッシュ関数 H をオラクルとみなす．ただし，オラクルへのクエリとして，量子状態 $\sum_{x,y} \alpha_{x,y} |x\rangle |y\rangle$ を受け取り，$\sum_{x,y} \alpha_{x,y} |x\rangle |H(x) \oplus y\rangle$ を出力する．

5.2 安全性

定理 2. 提案 *RIBE* 方式は前章のパラメータと dpMPLWE 仮定のもとで *QROM* において適応的匿名性を満たす．

本稿では，証明の概略を述べる．通常の安全性ゲームではゲームの最初にチャレンジャー $\mathcal{C}$ はハッシュ関数 $H : \{0,1\}^{\leq L_{\mathsf{ID}}+1} \times [0, \mathsf{T}_{\max}] \to \mathbb{Z}_q^{<n+2d-2}[X]$ を選ぶ．提案 *RIBE* 方式を破る攻撃者 $\mathcal{A}$ による量子ランダムオラクルクエリ $\sum_{\mathsf{ID}\|\mathsf{T},y} \alpha_{\mathsf{ID}\|\mathsf{T},y} |\mathsf{ID}\|\mathsf{T}\rangle |y\rangle$ に対して，$\mathcal{C}$ は $\sum_{\mathsf{ID}\|\mathsf{T},y} \alpha_{\mathsf{ID}\|\mathsf{T},y} |\mathsf{ID}\|\mathsf{T}\rangle |H(\mathsf{ID},\mathsf{T}) \oplus y\rangle$ を回答する．他のクエリに対しては，前章で述べた方式の通りに回答する．

通常の安全性ゲームから，量子ランダムオラクルクエリの $H(\mathsf{ID},\mathsf{T})$ の計算方法，秘密鍵生成クエリ，更新鍵生成クエリへの回答を変更する．まず，帰着アルゴリズムは $\hat{H} \xleftarrow{\mathrm{U}} \mathsf{Func}(\mathcal{ID} \times \mathcal{T}, \{0,1\}^\kappa)$ をサンプルする．$H(\mathsf{ID},0)$ に関しては，各 $i \in [t+\gamma\tau]$ について $r_{\mathsf{ID},i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \hat{H}(\mathsf{ID},0))$ をサンプルして，$H(\mathsf{ID},0) = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i}$ を計算するよう変更する．$H(\theta_j,\mathsf{T})$ に関しては，$r_{\mathsf{T},\theta_j,i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \hat{H}(\theta_j,\mathsf{T}))$ をサンプルして，$H(\theta_j,\mathsf{T}) = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{T},\theta_j,i}$ を計算するよう変更する．ここで，$\mathsf{Sample}\mathbb{Z}(\sigma; \hat{H}(\mathsf{ID},0))$ と $\mathsf{Sample}\mathbb{Z}(\sigma; \hat{H}(\theta_j,\mathsf{T}))$ はそれぞれ $\hat{H}(\mathsf{ID},0)$ と $\hat{H}(\theta_j,\mathsf{T})$ をランダムシードとして $\mathsf{Sample}\mathbb{Z}(\sigma)$ アルゴリズムを実行する事を表す．補題 2 と補題 3 より，$H(\mathsf{ID},0)$ や $H(\theta_j,\mathsf{T})$ が一様サンプルと識別不能なので，この変更は統計的に識別不能である．また補題 4 より，変更した際の $(r_{\mathsf{ID},i})_{i\in[t+\gamma\tau]}$ の分布は，SamplePre アルゴリズムで得た $(r_{\mathsf{ID},i})_{i\in[t+\gamma\tau]}$ の分布と統計的に識別不能である．同様に，変更後の $(r_{\mathsf{T},\theta_j,i})_{i\in[t+\gamma\tau]}$ の分布は，SamplePre アルゴリズムで得た $(r_{\mathsf{ID},i})_{i\in[t+\gamma\tau]}$ の分布と統計的に識別不能である．よって $(r_{\mathsf{ID},i})_{i\in[t+\gamma\tau]}$ と $(r_{\mathsf{T},\theta_j,i})_{i\in[t+\gamma\tau]}$ を秘密鍵生成クエリと更新鍵生成クエリへの回答として返すよう変更できる．いま msk は使用されないので mpk を $(a_i)_{i\in[t+\gamma\tau]} \xleftarrow{\mathrm{U}} (\mathbb{Z}_q^{2d-1}[X])^t \times (\mathbb{Z}_q^d[X])^{\gamma\tau}$ に変更しても補題 4 より統計的に識別不能である．

さらに $\mathsf{coin} = 0$ のときのチャレンジ暗号文を変更する．まず $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+2d+k-1}[X]$ をサンプルする．各 $i \in [t]$ について $\mathbf{e}_i \leftarrow D_{\mathbb{Z}_q^{2d+k},\alpha q}$ をサンプルし，各 $i \in [t+1, t+\gamma\tau]$ について $\mathbf{e}_i \leftarrow D_{\mathbb{Z}_q^{d+k+1},\alpha q}$ をサンプルする．その後，

$$b_i = a_i \odot_{2d+k} s + e_i \ (i \in [t])$$
$$b_i = a_i \odot_{d+k+1} s + e_i \ (i \in [t+1, t+\gamma\tau])$$

を計算し，チャレンジ暗号文を

$$((\bar{b}_i)_{i\in[t+\gamma\tau]}, (\bar{b}'_\ell)_{\ell\in[L_{\mathsf{ID}}+1]})$$
$$\leftarrow 2 \cdot \mathsf{ReRand}(((2^{-1}(r_{\mathsf{ID}^\star,i} + r_{\mathsf{T},\mathsf{ID}^\star[\ell],i}))_{i\in[t+\gamma\tau]})_{\ell\in[L_{\mathsf{ID}}+1]},$$
$$(b_i)_{i\in[t+\gamma\tau]}, \alpha q, \frac{\alpha'}{2\alpha})$$

とする．式 (1) と補題 6 より，変更したチャレンジ暗号文は通常の Encrypt アルゴリズムを用いたチャレンジ暗号文と統計的に識別不能である．

加えて，$\mathsf{dpMPLWE}_{q,n+2d+k,\mathbf{d},D_{\alpha q},U(\mathbb{Z}_q^{<n+2d+k-1}[X])}$ 仮定を用いて $\mathsf{coin} = 0$ のときのチャレンジ暗号文をさらに変更する．具体的には，$(w_i)_{i\in[t+\gamma\tau]} \xleftarrow{\mathrm{U}} (\mathbb{Z}_q^{<2d+k}[X])^t \times (\mathbb{Z}_q^{<d+k+1}[X])^{\gamma\tau}$ をサンプルし

$$b_i = w_i + e_i \ (i \in [t])$$
$$b_i = w_i + e_i \ (i \in [t+1, t+\gamma\tau])$$

を計算する．変更した $(b_i)_{i\in[t+\gamma\tau]}$ は変更前の $(b_i)_{i\in[t+\gamma\tau]}$ と計算量的に識別不能である．その後

$$((\bar{b}_i)_{i\in[t+\gamma\tau]}, (\bar{b}'_\ell)_{\ell\in[L_{\mathsf{ID}}+1]})$$
$$\leftarrow 2 \cdot \mathsf{ReRand}(((2^{-1}(r_{\mathsf{ID}^\star,i} + r_{\mathsf{T},\mathsf{ID}^\star[\ell],i}))_{i\in[t+\gamma\tau]})_{\ell\in[L_{\mathsf{ID}}+1]},$$
$$(b_i)_{i\in[t+\gamma\tau]}, \alpha q, \frac{\alpha'}{2\alpha})$$

を実行してチャレンジ暗号文を計算する．

$\mathsf{ID}^\star \in \mathsf{RL}_{\mathsf{T}^\star}$ ならば，*RIBE* の安全性定義と KUNode アルゴリズムの性質から $\mathcal{A}$ は更新鍵として $((r_{\mathsf{T},\mathsf{ID}^\star[\ell],i})_{i\in[t+\gamma\tau]})_{\ell\in[L_{\mathsf{ID}}+1]}$ を得ることができない．また，$\mathsf{ID}^\star \notin \mathsf{RL}_{\mathsf{T}^\star}$ ならば *RIBE* の安全性ゲームの定義から，$\mathcal{A}$ は秘密鍵漏洩クエリにより $(r_{\mathsf{ID}^\star,i})_{i\in[t+\gamma\tau]}$ を得ていない．よって，補題 2，補題 3 より，$\mathsf{ID}^\star \in \mathsf{RL}_{\mathsf{T}^\star}$ の場合は各 $\ell \in [L_{\mathsf{ID}}+1]$ について $\sum_{i=1}^{t} r_{\mathsf{T},\mathsf{ID}^\star[\ell],i}\bar{w}_i$ の分布が．$\mathsf{ID}^\star \notin \mathsf{RL}_{\mathsf{T}^\star}$ の場合は $\sum_{i=1}^{t} r_{\mathsf{ID},i}\bar{w}_i$ の分布が一様分布と統計的に識別不能である．以上より $\sum_{i=1}^{t+\gamma\tau}(r_{\mathsf{ID}^\star,i} + r_{\mathsf{T},\mathsf{ID}^\star[\ell],i}) \odot_{k+2} w_i$ の分布も一様分布と統計的に識別不能で，$\mathsf{coin} = 1$ のときのチャレンジ暗号文と統計的に識別不能である．

謝辞 本研究の一部は JST CREST Grant Number JPMJCR2113 と JSPS KAKENHI Grant Number 24K02939 の助成を受けたものです．

参考文献

[1] Agrawal, S., Boneh, D. and Boyen, X.: Efficient Lattice (H)IBE in the Standard Model, *EUROCRYPT 2010*, LNCS, Vol. 6110, Springer, pp. 553–572 (2010).

[2] Agrawal, S., Boneh, D. and Boyen, X.: Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE, *CRYPTO 2010*, LNCS, Vol. 6223, Springer, pp. 98–115 (2010).

[3] Bai, S., Das, D., Hiromasa, R., Rosca, M., Sakzad, A., Stehlé, D., Steinfeld, R. and Zhang, Z.: MPSign: A Signature from Small-Secret Middle-Product Learning with Errors, *PKC 2020*, LNCS, Vol. 12111, Springer, pp. 66–93 (2020).

[4] Boldyreva, A., Goyal, V. and Kumar, V.: Identity-based encryption with efficient revocation, *ACM CCS 2008*, ACM Press, pp. 417–426 (2008).

[5] Chen, J., Lim, H. W., Ling, S., Wang, H. and Nguyen, K.: Revocable Identity-Based Encryption from Lattices, *ACISP 12*, LNCS, Vol. 7372, Springer, pp. 390–403 (2012).

[6] Das, D., Au, M. H. and Zhang, Z.: Ring Signatures Based on Middle-Product Learning with Errors Problems, *AFRICACRYPT 19*, LNCS, Vol. 11627, Springer, pp. 139–156 (2019).

[7] Fan, J., Lu, X. and Au, M. H.: Adaptively Secure Identity-Based Encryption from Middle-Product Learning with Errors, *ACISP 23*, LNCS, Vol. 13915, Springer, pp. 320–340 (2023).

[8] Gentry, C., Peikert, C. and Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions, *40th ACM STOC*, ACM Press, pp. 197–206 (2008).

[9] Hiromasa, R.: Digital Signatures from the Middle-Product LWE, *ProvSec 2018*, LNCS, Vol. 11192, Springer, pp. 239–257 (2018).

[10] Katsumata, S., Matsuda, T. and Takayasu, A.: Lattice-Based Revocable (Hierarchical) IBE with Decryption Key Exposure Resistance, *PKC 2019*, LNCS, Vol. 11443, Springer, pp. 441–471 (2019).

[11] Katsumata, S. and Yamada, S.: Partitioning via Nonlinear Polynomial Functions: More Compact IBEs from Ideal Lattices and Bilinear Maps, *ASIACRYPT 2016*, LNCS, Vol. 10032, Springer, pp. 682–712 (2016).

[12] Katsumata, S., Yamada, S. and Yamakawa, T.: Tighter Security Proofs for GPV-IBE in the Quantum Random Oracle Model, *Journal of Cryptology*, Vol. 34, No. 1, p. 5 (2021).

[13] Le, H. Q., Duong, D. H., Susilo, W. and Pieprzyk, J.: Trapdoor Delegation and HIBE from Middle-Product LWE in Standard Model, *ACNS 20*, LNCS, Vol. 12146, Springer, pp. 130–149 (2020).

[14] Lin, H., Sun, S., Wang, M., Liu, J. K. and Wang, W.: Shorter Linkable Ring Signature Based on Middle-Product Learning with Errors Problem, *The Computer Journal*, Vol. 66, No. 12, pp. 2974–2989 (2022).

[15] Lombardi, A., Vaikuntanathan, V. and Vuong, T. D.: Lattice Trapdoors and IBE from Middle-Product LWE, *TCC 2019*, LNCS, Vol. 11891, Springer, pp. 24–54 (2019).

[16] Ma, X. and Lin, D.: Generic constructions of revocable identity-based encryption, *Inscrypt 2019*, LNCS, Springer, pp. 381–396 (2020).

[17] Naor, D., Naor, M. and Lotspiech, J.: Revocation and Tracing Schemes for Stateless Receivers, *CRYPTO 2001*, LNCS, Vol. 2139, Springer, pp. 41–62 (2001).

[18] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography, *37th ACM STOC*, ACM Press, pp. 84–93 (2005).

[19] Rosca, M., Sakzad, A., Stehlé, D. and Steinfeld, R.: Middle-Product Learning with Errors, *CRYPTO 2017*, LNCS, Vol. 10403, Springer, pp. 283–297 (2017).

[20] Seo, J. H. and Emura, K.: Revocable Identity-Based Encryption Revisited: Security Model and Construction, *PKC 2013*, LNCS, Vol. 7778, Springer, pp. 216–234 (2013).

[21] Stehlé, D., Steinfeld, R., Tanaka, K. and Xagawa, K.: Efficient Public Key Encryption Based on Ideal Lattices, *ASIACRYPT 2009*, LNCS, Vol. 5912, Springer, pp. 617–635 (2009).

[22] Takayasu, A.: Adaptively secure lattice-based revocable IBE in the QROM: compact parameters, tight security, and anonymity, *DCC*, Vol. 89, No. 8, pp. 1965–1992 (2021).

[23] Takayasu, A. and Watanabe, Y.: Lattice-Based Revocable Identity-Based Encryption with Bounded Decryption Key Exposure Resistance, *ACISP 17*, LNCS, Vol. 10342, Springer, pp. 184–204 (2017).

[24] Takayasu, A. and Watanabe, Y.: Revocable identity-based encryption with bounded decryption key exposure resistance: Lattice-based construction and more, *Theoretical Computer Science*, Vol. 849, pp. 64–98 (2021).

[25] Wang, S., Zhang, J., He, J., Wang, H. and Li, C.: Simplified Revocable Hierarchical Identity-Based Encryption from Lattices, *CANS 19*, LNCS, Vol. 11829, Springer, pp. 99–119 (2019).

[26] Yamakawa, T. and Zhandry, M.: Classical vs Quantum Random Oracles, *EUROCRYPT 2021*, LNCS, Vol. 12697, Springer, pp. 568–597 (2021).

[27] Yang, N., Yang, S., Zhao, Y. and Wu, W.: Inner Product Encryption from Middle-Product Learning with Errors, *SocialSec 2022*, CCIS, Vol. 1663, Springer Nature, pp. 94–113 (2022).

[28] Yang, N., Yang, S., Zhao, Y., Wu, W. and Wang, X.: Inner product encryption from Middle-Product Learning With Errors, *Computer Standards & Interfaces*, Vol. 87, No. C (2024).