Vol.2023-DPS-194 No.48
Vol.2023-CSEC-100 No.48
2023/3/7

pqe ベース暗号方式における安全性の証明

佐藤　克洋[1,a)]　Wang Yuntao[1,b)]　宮地 充子[1,2,c)]

概要：
近年使用されている暗号方式は, 現在の計算機システムに対して一定の安全性を持っている. しかし, それらの暗号方式は近い将来量子計算機の実現によって多項式時間で解読される可能性があることがわかっている. それらに備えるべく, 耐量子計算機暗号の候補である格子暗号 (Lattice-based Cryptography) と多変数多項式暗号 (MPKC:Miltivariate Public Key Cryptography) の技術を用いた linear-pqe-method, またそのリング版である ring-pqe method が提案された. 本研究では, linear-pqe-method, ring-pqe method において証明可能安全性を考察する.

キーワード：耐量子計算機暗号，格子暗号，多変数多項式暗号

Proof of Security in pqe-based cryptosystems

Abstract:
The cryptographic schemes used in recent years have a certain degree of security against current computer systems. However, it is known that these cryptographic schemes may be deciphered in polynomial time in the near future when quantum computers are realized. To prepare for them, the linear-pqe method, and its ring versions, the ring-pqe method were proposed using the techniques of lattice-based cryptography and multivariable public-key cryptography (MPKC), which are candidates for quantum computer cryptography. In this study, we examine the provable safety of the linear-pqe-method and the ring-pqe-method, of which safety has not been considered.

Keywords: post-quantum cryptography, lattice-based cryptography, multivariate public-key cryptography

1. はじめに

近年, 一般的に使用されている公開鍵暗号システムは, その安全性が因数分解, 離散対数問題, 楕円曲線問題などの数論的難問に基づいている. しかし, 近い将来に圧倒的な計算力を持つ量子コンピュータが生み出され流と言われている. これらの問題は shor の量子アルゴリズム [5] により多項式時間で解かれる可能性がある. このような背景により, 現在はその量子コンピュータでも多項式時間で解くことができない 耐量子計算機暗号の研究が急務となっている.

現在開発が進められている耐量子計算機暗号の一つとして, 格子暗号がある. 格子暗号で用いられる Learning with errors(LWE) 問題 [4] などの困難性は, 最終的に最短ベクトル問題 (SVP:Shortest Vector Problem) と呼ばれる, 規則的に並んだ点からなる格子の中から最も長さが短いベクトルを求める問題に帰着できる. 格子暗号の中でも LWE ベースの公開鍵暗号は, 他の耐量子計算機暗号と比べて公開鍵, 秘密鍵, 暗号文のサイズが小さく抑えられ, 演算処理も十分に高速になる. 多変数多項式暗号 (MPKC:Miltivariate Public Key Cryptography)[3] もまた主な耐量子計算機暗号の一つである. 多くの MPKC の安全性は, 多変数二次多項式問題 (MQ 問題: Multivariate Quadratic polynomials

[1] 大阪大学
Osaka University
[2] 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology
[a)] sato@cy2sec.comm.eng.osaka-u.ac.jp
[b)] wang@comm.eng.osaka-u.ac.jp
[c)] miyaji@comm.eng.osaka-u.ac.jp

problem) を解くことの難しさに基づく [10]. MPKC 署名方式は小さな数で実行できるため効率的である一方, MPKC は他と比べて計算コストが大きくなってしまい, 一般的には公開鍵暗号には適用できない. しかし, 制約つき多項式写像を用いることで射影トラップドア一方向性関数を容易に構成することができる. その結果. この関数を用いることで, 安全性が制約つき多項式問題を解くことの困難性に基づき, かつコストを抑えられる MPKC 暗号方式を構築することができる.

2018 年, [8] にて pq-method という多変数多項式暗号が提案された. pq-method の安全性は MPKC の難問である制約つき MQ 問題に基づくものである. 実質的に制約つき MQ 問題は格子理論における Inhomogeneous Short Integer Solution(ISIS) 問題の 2 次版と見ることができるため, pq-method を用いた暗号方式は格子と MPKC を組み合わせた最初の公開鍵暗号であると考えられている. さらに, 公開鍵の大きさを減らすために, [9] では暗号化の際にエラーベクトルを用いた pqe-method が提案された. さらに, これらのアルゴリズムをさらに安全で低コストなものにするために, [7] では, pq-method, pqe-method で用いられている二次多項式を線形多項式にしたアルゴリズムである Linear-pq method, Linear-pqe method が提案され, 後者をリングバージョンにすることで鍵長を $O(1/n)$ に抑えた ring-pqe method も提案された. [7] により, それぞれのアルゴリズムで用いられるパラメーター q を比較すると, 線形多項式構造を用いることではるかに小さな q の値を使用し, 線形多項式乗算を行うことで計算のコストが削減された. また, 鍵生成の最後に線型写像マスクを組み込むことで鍵回復攻撃に対して安全な方式を実現した.

本研究では, [7] にて提案された手法である Linear-pqe method, ring-pqe method について, [2] の Frode という鍵交換プロトコルで使用された証明手法を参考にし, IND-CPA 安全の証明をすることを目的とする.

最後に本論文の構成について記載する. 2 章ではセキュリティに関する一般的な内容や, 今回の研究の軸となる簡単な MPKC の内容をまとめる. 3 章では, 安全性の証明の対象となる [7] で提案されたアルゴリズムを記載し, またその IND-CPA 安全性の証明において参考にした [2] にて利用された識別問題の紹介をする. 4 章では, Linear-pqe method と ring-pqe method のそれぞれについて IND-CPA 安全が成り立つことを証明する. 5 章では結論を述べる.

2. 準備

本章ではセキュリティに関する一般的な内容や, 今回の研究の軸となる簡単な MPKC の内容をまとめる.

2.1 公開鍵暗号

公開鍵暗号

暗号化と復号で別の鍵を用いる暗号を公開鍵暗号という. 暗号化に用いる鍵のみを公開することで, 共通鍵暗号に必要な鍵共有が不要になるが, 処理速度が遅い.

公開鍵の安全性

暗号が安全であるとは, 一般に解読の目標となる暗号文からその復号文である平文が解読されないことを意味する. 解読には暗号文から平文が完全に得られる解読から, 平文の部分情報が求められる解読まで色々なレベルが存在する. 一方、解読する際に利用する手段も, 攻撃者にとって有利な手段から非常に困難な手段まで, 色々なレベルが存在する。安全な暗号方式とは, 攻撃者にとって最も有利な手段を用いても, どんな平文の情報も解読できない方式である.

定義 2.1 (選択平文攻撃 (CPA:Chosen-Plaintext Attack))**.** 攻撃者は任意に選択した平文の集合に対する正しい暗号文を利用する攻撃.

定義 2.2 (識別不可能性 (IND:Indistinguishability))**.** 暗号方式が識別不可能性を満たすとは、二つの長さの等しい平文 m_1,m_2 と、そのどちらかの暗号文 c を与えられた攻撃者が、どちらの平文の暗号文であるか識別できないことである.

定義 2.3 (IND-CPA)**.** 暗号方式が選択平文攻撃の下で識別不可能性（頑強性）を満たすとき,*IND-CPA* であるという.

2.2 格子

格子 L は線型独立なベクトルの組 $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{R}^m$ で表される基底 B により生成される. つまり, $L(\mathbf{b}_1, ..., \mathbf{b}_n) := \{\sum_{i=1}^{n} x_i \mathbf{b}_i, x_i \in \mathbb{Z}\}$. 本論文では便宜上整数格子を利用し, この基底を行列形式で書くと, $B = (\mathbf{b}_1, ..., \mathbf{b}_n) \in \mathbb{Z}^{m \times n}$ と表せる. 整数 n はこの格子のランクであり, $m = n$ のときこの格子はフルランク格子と呼ばれる. また, 格子ベクトル $\mathbf{v} \in \mathbb{R}^m$ のユークリッドノルムは $||\mathbf{v}|| := \sqrt{\mathbf{v} \cdot \mathbf{v}}$ で表される.

定義 2.4 (LWE 問題)**.** 素数 p によって作られる体を $\mathbb{Z}/p\mathbb{Z}$, 標準偏差 δ_s, δ_e に従う $\mathbb{Z}$ 上の確率分布を D_s, D_e, 行列 A を $A \in \mathbb{Z}_p^{m \times n}, (m, n \in \mathbb{Z})$ とする. $\mathbf{s} \in D_s^n, \mathbf{e} \in D_e^m$ と行列 A に対して, $(A, \boldsymbol{b} = A\mathbf{s} + \mathbf{e} \pmod p)$ を *LWE* サンプルという.

定義 2.5 (LWE 識別問題)**.** n, q を正の整数とし, χ を $\mathbb{Z}$ 上の分布とする. また, $\mathbf{s} \xleftarrow{\$} \mathcal{U}(\mathbb{Z}_q^n)$ とする.

ここで, 二つのオラクルを定義する.

- $O_{\chi,\mathbf{s}}: \mathbf{a} \xleftarrow{\$} \mathcal{U}(\mathbb{Z}_q^n), e \xleftarrow{\$} \chi(\mathbb{Z}_q)$; *return* $(\mathbf{a}, \mathbf{as}+e)$.
- $U: \mathbf{a} \xleftarrow{\$} \mathcal{U}(\mathbb{Z}_q^n), u \xleftarrow{\$} \mathcal{U}(\mathbb{Z}_q)$; *return* $(\mathbf{a}, u)$.

パラメーター (n, q, χ) における *LWE* 識別問題は,$O_{\chi,\mathbf{s}}$ と U を見分けることである.

この章からは提案方式，既存方式で利用されるセキュリティの内容について定義する.

2.3 記法

- m, n, l を正の整数とする.
- 集合 $[m]$ は {1,...,m} を表す.
- 剰余環 $\mathbb{Z}_l$ は l の剰余環, すなわち $\mathbb{Z}_l$ の要素は 0 から $l-1$ までである.
- ある要素 $a \in \mathbb{Z}_l$ に対し, a のリフト関数を $\mathrm{lift}_l(a) \in I_l := (-l/2, l/2] \in \mathbb{Z}$ で定義する.
- 同時に, 素数 q の有限体を $\mathbb{F}_q$ とする. n 個の独立変数 $x_{i\in[n]}$ を用いて, 行ベクトル $\mathbf{x} = (x_1, ..., x_n)$ を表す.
- $\mathbf{x}$ を変数とし、係数を $\mathbb{F}_q$ から取る多項式の集合を $\mathbb{F}_q[\mathbf{x}]$ とする,
- m 個の (上三角) 行列 $A_1, ..., A_m \in \mathbb{F}_q^{n\times n}$, m 個のベクトル $\mathbf{b}_1, ..., \mathbf{b}_m \in \mathbb{F}_q^n$, m 個の定数 $c_1, ..., c_m$ を用意する. これらを用いて $\mathbb{F}_q[\mathbf{x}]^m$ 中の二次多項式系を $\mathcal{F}(\mathbf{x}) := f_i(\mathbf{x}) := \mathbf{x}A_i\mathbf{x}^T + \mathbf{b}_i\mathbf{x} + c_i$ で定義する. 簡単のためにそのベクトルを $\mathcal{F}(\mathbf{x}) := (f_1(\mathbf{x}), ..., f_m(\mathbf{x})) \in \mathbb{F}_q[\mathbf{x}]^m$ と書く.
- $x \in \mathbb{R}$ より大きい最初の素数を $\mathsf{NextPrime}(x)$ で表す.
- 正の整数 p と行列 $L \in \mathbb{Z}_p^{n\times m}$ に対し $||L||_p := \max_{\mathbf{a}\in I_p^n}\{|\mathbf{a}\cdot L|_\infty\}$ を定義する.

2.4 多変数多項式暗号 (MPKC) の基礎

定義 2.6 (多変数多項式問題 (MP 問題:Multivariate Polynomial problem))**.** n 個の変数を持つ m 個の多項式を持つ多項式系の集合を $\mathbb{F}_q[\mathbf{x}]^m$ とする. $\mathcal{F}(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}]^m$ が与えられたとき, MP 問題は $\mathcal{F}(\mathbf{x}_0) = \mathbf{0}$ を満たすような解 $\mathbf{x}_0 = (x_{01}, ..., x_{0n}) \in \mathbb{F}_q^n$ を求める問題.

定義 2.7 (制約付き MP 問題)**.** パラメータ $L \in \mathbb{Z}_{>0}$ と n 個の変数を持つ m 個の多項式を持つ多項式システム $\mathcal{F}(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}]^m$ が与えられたとき, 制約付き MP 問題は $\mathcal{F}(\mathbf{x}_0) = \mathbf{0}$ を満たすような解 $\mathbf{x}_0 = (x_{01}, ..., x_{0n}) \in \mathbb{F}_L^n$ を求める問題.

定義 2.8 (MQ 問題)**.** MP 問題 (または制約付き MP 問題) において二次多項式のみを用いる場合, その問題は MQ 問題と呼ばれる.

定義 2.9 (MQ 問題に基づく二次 MPKC の一般構成)**.** m, n を整数, q を素数とする. 二次 MPKC において，秘密鍵には反転可能な二次写像 $F: \mathbb{F}_q[\mathbf{x}]^n \to \mathbb{F}_q[\mathbf{x}]^m$ と二つのアフィン写像 $S: \mathbb{F}_q[\mathbf{x}]^n \to \mathbb{F}_q[\mathbf{x}]^n$ と $T: \mathbb{F}_q[\mathbf{x}]^m \to \mathbb{F}_q[\mathbf{x}]^m$ が用いられる. 公開鍵には $P = S\circ F\circ T: \mathbb{F}_q[\mathbf{x}]^n \to \mathbb{F}_q[\mathbf{x}]^m$ が用いられる. 平文 $\mathbf{m} \in \mathbb{F}_q^n$ は $\mathbf{c} = P(\mathbf{m})$ によって暗号化される.$\mathbf{c}$ は $\mathbf{m} = T^{-1}(F^{-1}(S^{-1}(\mathbf{c})))$ によって復号される. MPKC の安全性は公開鍵 P が秘密鍵なしで反転することの困難性に基づく.

3. 既存研究

3.1 Linear-pqe method と ring-pqe method の紹介 [7][6]

本節では, 今回安全性の証明の対象としたアルゴリズム, Linear-pqe method と ring-pqe method のアルゴリズムを記載する.

pqe-method の線形多項式版

[7] では二次多項式を利用している pqe-method[9] の線形多項式版が提案されている. このアルゴリズムは Linear-pqe method と呼ばれている.

鍵生成

p を小さい素数, n を正の整数とする.

(1) $\mathbf{x} = (x_1, ..., x_n)$ とする. 行列 $L_{1,X}, L_{1,Y}, L_{r,X}, L_{r,Y} \in \mathbb{F}_p^{n\times n}$ をランダムにサンプリングする.

(2) $||L_{a,b}||_p \le M_{a,b} (a \in \{1, r\}, b \in \{X, Y\})$ を満たすような正の整数 $M_{1,X}$, $M_{1,Y}$, $M_{r,X}$, $M_{r,Y}$ を選ぶ. また, $M_1 = M_{1,X} + pM_{1,Y}, M_r = M_{r,X} + M_{r,Y}$ とする.

(3) $q \ge 4M_1M_r$ を満たす素数 q を選ぶ.

(4) $2M_1 < \min_{k\in[2M_r]} |\mathrm{lift}_q(r_ik)|_{i\in[n]}$ を満たすように $0 < r_1, ..., r_n < q$ と $k \in [2M_r]$ を定める. 上記を満たす $r_1, ..., r_n$ がサンプリングできなかった場合, 3. に戻る.

(5)

$$L_X = L_{1,X} + \begin{bmatrix} r_1 & & \\ & \ddots & \\ & & r_n \end{bmatrix} L_{r,X} \in \mathbb{Z}^{n\times n},$$

$$L_Y = pL_{1,Y} + \begin{bmatrix} r_1 & & \\ & \ddots & \\ & & r_n \end{bmatrix} L_{r,Y} \in \mathbb{Z}^{n\times n}$$

を計算する.

$L_Y \pmod q \in \mathbb{F}_q^{n\times n}$ が逆行列を持つとき, $T = L_Y^{-1}$ とする. そうでなければ 1. に戻る.

(6) $L_F = T \circ L_X \in \mathbb{F}_q^{n\times n}$ と $L_S = L_{1,X}^{-1} \pmod p$ を計算する.

秘密鍵：L_S, $\{r_i\}_{i\in[n]}$, L_Y

公開鍵：p, q, L_F

暗号化

(1) ランダムに $\mathbf{e} \in I_p^n$ を選ぶ.

(2) 与えられた平文 $\mathbf{m} \in I_p^n$ に対し, 暗号文 $\mathbf{c} = L_F(\mathbf{m}) + \mathbf{e} \in \mathbb{F}_q^n$ を生成する.

復号

(1) $\mathbf{b} = (b_1, ..., b_n) = L_Y \cdot \mathbf{c}$ を計算する.

(2) 任意の $i \in [n]$ について、$|\mathrm{lift}_q(b_i - r_i k_i)| \leq M_1$ と $|k_i| \leq M_r$ を満たすような k_i を見つける. また, $\hat{b}_i = \mathrm{lift}_q(b_i - r_i k_i) \in \mathbb{Z}$ とする.

(3) $\mathbf{u} = \hat{\mathbf{b}} \pmod p \in \mathbb{F}_p^n$ を計算し, $\mathbf{m}' = \mathrm{lift}_p(L_S \cdot \mathbf{u})$ を計算する. これが平文 $\mathbf{m}$ と一致する.

Linear-pqe method のリング版

次に, Linear-pqe method のリングバージョンである ring-pqe method のアルゴリズムを記載する. このアルゴリズムで用いられる鍵の長さは 先ほどの Linear-pqe method に比べて $O(1/n)$ 短い. したがってこのアルゴリズムはより良いパフォーマンスを発揮すると考えられる.

まず多項式環 R を, $R := \mathbb{Z}[x]/(x^n - 1)$ と定義する. また, 正の整数 p と多項式 $L \in R$ について $||L||_p := \max_{\mathbf{a} \in I_p^n}\{|\mathbf{a} \cdot L|_\infty\}$ と定義する. このセクションでは I_p^n を $n-1$ 次かつ係数を I_p 中に持つ多項式の集合として定義する.

鍵生成

p を小さい素数,n を正の整数とする.

(1) 行列 $L_{1,X}$, $L_{1,Y}$, $L_{r,X}$, $L_{r,Y} \in R/pR$ をランダムにサンプリングする.

(2) $||L_{a,b}||_p \leq M_{a,b} (a \in \{1, r\}, b \in \{X, Y\})$ を満たすような正の整数 $M_{1,X}$, $M_{1,Y}$, $M_{r,X}$, $M_{r,Y}$ を選ぶ. また, $M_1 = M_{1,X} + pM_{1,Y}$, $M_r = M_{r,X} + M_{r,Y}$ とする.

(3) $q \geq 4M_1M_r$ を満たす素数 q を選ぶ.

(4) $2M_1 < \min_{k \in [2M_r]} |\mathrm{lift}_q(rk)|_{i \in [n]}$ を満たすように $(0, q)$ から r を定める. 上記を満たす r がサンプリングできなかった場合は 3. に戻り, より大きな q をサンプリングする.

(5) $L_X = L_{1,X} + rL_{r,X}, L_Y = pL_{1,Y} + rL_{r,Y}$ を計算する.
$L_Y \pmod q \in R/qR$ が逆行列を持つとき, $T = L_Y^{-1}$ とする. そうでなければ 1. に戻る.

(6) $L_F = T \cdot L_X \in R/qR$ と $L_S = L_{1,X}^{-1} \pmod p$ を計算する.
秘密鍵：L_S, r, L_Y
公開鍵：p, q, L_F

暗号化

(1) ランダムに $\mathbf{e} \in I_p^n$ を選ぶ.

(2) 与えられた平文 $\mathbf{m} \in I_p^n$ に対し, 暗号文 $\mathbf{c} = L_F(\mathbf{m}) + \mathbf{e} \in R/qR$ を生成する.

復号

(1) $b(\mathbf{x}) = \sum_{i=0}^{n-1} b_i x^i = L_Y \cdot \mathbf{c}$ を計算する.

(2) 任意の $i \in [n]$ について、$|\mathrm{lift}_q(b_i - rk_i)| \leq M_1$ と $|k_i| \leq M_r$ を満たすような k_i を見つける. また, $\hat{b}_i = \mathrm{lift}_q(b_i - rk_i) \in \mathbb{Z}$ とする.

(3) $\mathbf{u} = \hat{\mathbf{b}} \pmod p \in \mathbb{F}_p^n$ を計算し, $\mathbf{m}' = \mathrm{lift}_p(L_S \cdot \mathbf{u})$ を計算する. これが平文 $\mathbf{m}$ と一致する.

3.2 鍵交換プロトコル：Frodo [2]

本研究では, Frodo という鍵交換プロトコル [2] の行われている証明手法を参考にした. このプロトコルは, 以下の定義 3.1 の識別問題が成り立つという仮定のもとに IND-CPA 安全の証明がされている.

定義 3.1 (短い秘密を用いた LWE 識別問題 [1])**.** *n, q を正の整数, χ を $\mathbb{Z}$ 上の分布とし,$\mathbf{s} \xleftarrow{\$} \chi(\mathbb{Z}_q^n)$ とする. また, 定義 2.5 のように $O_{\chi,\mathbf{s}}$ と U を定義する. パラメータを (n, q, χ) とする短い秘密を用いた LWE 識別問題は, $O_{\chi,\mathbf{s}}$ と U を見分けることである. 特に, アルゴリズム $\mathcal{A}$ についてアドバンテージを定義する.*

$$\mathrm{Adv}^{\mathsf{dlwe-ss}}_{n,q,\chi}(\mathcal{A}) = |\Pr(\mathbf{s} \xleftarrow{\$} \chi(\mathbb{Z}_q^n) : \mathcal{A}^{O_{\chi,\mathbf{s}}}() = 1) - \Pr(\mathcal{A}^U() = 1)|$$

補題 3.1 (short LWE [1])**.** *n, q, χ を定義 3.1 と同様とする. アルゴリズム $\mathcal{A}$ を短い秘密を用いた LWE 識別問題 (定義 3.1) を識別するアルゴリズムであるとする. このとき, $\mathcal{A}$ は $\mathcal{A}$ と, オラクルを $O(n^2)$ 回呼び出したときにほぼ同じ時間で動作する LWE 識別問題 (定義 2.5) のアルゴリズム $\mathcal{B}$ を構築でき, $\mathrm{Adv}^{\mathsf{dlwe-ss}}_{n,q,\chi}(\mathcal{B}) = \mathrm{Adv}^{\mathsf{dlwe}}_{n,q,\chi}(\mathcal{A})$ を満たす.*

3.3 既存研究のまとめと本研究の目的

本研究では, 3.1 の二つのアルゴリズムの安全性を証明する. そのために参考にしたのが 3.2 節で紹介した 3.2 である. 3.2 の鍵交換プロトコルの安全性証明では, 定義 3.1 の識別仮定に基づいている. 次の章からは, これらの考え方を参考に 上記二つのアルゴリズムが IND-CPA 安全を満たすことを証明する.

4. 提案手法

この章では, Linear-pqe method, ring-pqe method のそれぞれにおいてアルゴリズムを通して生成される暗号文 $\mathbf{c}$ と一様ランダムに生成される暗号文 $\mathbf{c}'$ を見分けようとする敵対者の存在を考え, その敵対者がそれらの暗号文を見分ける際のアドバンテージが限りなく小さいことを証明

し, それにより二つのアルゴリズムが IND-CPA 安全を満たすことを証明する.

4.1 Linear-pqe method の安全性証明

以下において, n を正の整数, p を小さい素数, χ を $\mathbb{Z}$ 上の分布, $L_{1,X}, L_{1,Y}, L_{r,X}, L_{r,Y}$ を $\mathbb{F}_p^{n\times n}$ からランダムにサンプリングとした行列とし, $q, \{r_i\}_{i\in n}$ は前述のパラメーターを用いて 3.1 のアルゴリズムにしたがってサンプリングしたものとする. また, $\{r_j\}_{j\in n}$ をそれぞれ (j,j) 成分とする行列を $[r_j]$ と表し, 平文 $\mathbf{m}$ は集合 I_p^n から取るものとする.

また, 3 章にて述べた short-LWE 識別問題をこのアルゴリズムに合うように定義し直す.

定義 4.1 (Unique short-LWE 識別問題)**.** 今回の定義では, *short-LWE* 識別問題とは異なり秘密とエラーベクトルを集合 I_p^n から取っているため, 以下のように定義し直し, これを *Unique short-LWE* 識別問題と呼ぶこととする. p を小さい素数,n, q を正の整数, χ を $\mathbb{Z}$ 上の分布とし, 平文 $\mathbf{m}$ は集合 I_p^n からとるものとする. また, $O_{\chi,\mathbf{m}}$ と U を定義する.

- $O_{\chi,\mathbf{m}} : L \xleftarrow{\$} \mathcal{U}(\mathbb{F}_q^{n\times n}), \mathbf{e} \xleftarrow{\$} \chi(I_p^n)$;
  $$return\ (L, L(\mathbf{m}) + \mathbf{e} \pmod q).$$
- $U : L \xleftarrow{\$} \mathcal{U}(\mathbb{F}_q^{n\times n}), \mathbf{u} \xleftarrow{\$} \mathcal{U}(\mathbb{F}_q^{n})$; *return* $(L, \mathbf{u})$.

パラメータを (n,p,q,χ) とする短い秘密を用いた *LWE* 識別問題は, $O_{\chi,\mathbf{m}}$ と U を見分けることである. また, この識別問題が困難であるという仮定を *Unique short-LWE* 識別仮定と呼ぶ. ここで, この識別問題を解くアルゴリズム $\mathcal{A}$ についてアドバンテージを定義する.

$$\mathrm{Adv}^{\mathsf{u-dlwe-ss}}_{n,p,q,\chi}(\mathcal{A}) = |\Pr(\mathbf{m} \xleftarrow{\$} \chi(I_p^n) : \mathcal{A}^{O_{\chi,\mathbf{m}}}() = 1) - \Pr(\mathcal{A}^{U}() = 1)|$$

定義 4.2. 定義 *2.9* にて, *MPKC* の安全性は行列の積 $P = S \circ F \circ T$ で構成される公開鍵 P を秘密鍵なしで反転する困難性に基づくことを述べた. これに加え, *3.1* では, P のみが与えられた場合に S を単位行列に変えても安全性が低下しないことについて述べられている.

したがって, これに関して識別不可能性も成り立つと仮定する. この仮定を, 行列積識別仮定と呼ぶ.

ここで, *Linear-pqe method* 内で生成される行列 T, L_X について, 二つのオラクル O'_{T,L_X} と U' を定義する.

- O'_{T,L_X} : *return* $T \circ L_X \in \mathbb{F}_q^{n\times n}$.
- $U' : U \xleftarrow{\$} \mathcal{U}(\mathbb{F}_q^{n\times n})$ *return* U.

また, O'_{T,L_X} と U' を見分けるアルゴリズム $\mathcal{A}$ について, 以下のアドバンテージを定義する.

$$\mathrm{Adv}^{\mathsf{invert}}(\mathcal{A}) = |\Pr(\mathcal{A}^{O'_{T,L_X}}() = 1) - \Pr(\mathcal{A}^{U'}() = 1)|$$

Linear-pqe method の安全性証明について, 図 1 のゲームの流れで証明をする. また, S_i を Game i で敵対者が b^* と推測することを表す.

Linear-pqe method の安全性を証明するために, このアルゴリズムを通して生成された暗号文 $\mathbf{c}$ と, 一様ランダムに生成された暗号文 $\mathbf{c}'$ を見分ける敵対者の存在を考える. このとき, そのような敵対者 $\mathcal{A}$ のアドバンテージを以下で定義する.

$$\mathrm{Adv}_{n,p,L_{ab},r_i,q,\chi}(\mathcal{A}) = |\Pr[L_F, \mathbf{c}] - \Pr[L_F, \mathbf{c}']|$$

ここで, $L_{ab} = L_{a,b}(a \in \{1,r\}, b \in \{X,Y\})$, $r_i = \{r_i\}_{i\in[n]}$ とする.

定理 4.1. 定義 *4.1* がパラメーター (n,p,q,χ) において困難かつ 定義 *4.2* の識別問題が困難なとき, *Linear-pqe method* はランダムに生成された暗号文と区別がつかない暗号文を得る. つまり, 図 *2* で与えられる削減アルゴリズム $\mathcal{B}_1, \mathcal{B}_2$ について以下が成り立つ.

$$\mathrm{Adv}_{n,p,L_{ab},r_i,q,\chi}(\mathcal{A}) \le \mathrm{Adv}^{\mathsf{invert}}(\mathcal{A}\circ\mathcal{B}_1) + \mathrm{Adv}^{\mathsf{u-dlwe-ss}}_{n,p,q,\chi}(\mathcal{A}\circ\mathcal{B}_2)$$

この定理は, *Unique short-LWE* 識別仮定, 行列積識別仮定のもとで, このアルゴリズムにおいて 敵対者が得られるアドバンテージが 限りなく小さいことを意味する.

Game 0. まず, もととなるゲームについて考える. $\Pr(S_0)$ を求めるために 以下とする.

$$\mathrm{Adv}_{n,p,L_{ab},r_i,q,\chi}(\mathcal{A}) = |\Pr(S_0) - 1/2| \tag{1}$$

Game 1. このゲームでは, 行列 L_F がアルゴリズム中の L_X と $T(L_Y$ の逆行列) の積から計算されるのではなく, 一様ランダムに生成される.

Game 0 と **Game 1** の違い. Game 0 では, L_F は O'_{T,L_X} からサンプリングされる. しかし, Game 1 では L_F は $\mathcal{U}(\mathbb{F}_q^{n\times n})$ からサンプリングされる.

より明確にすると, まず $\mathcal{B}_1$ を図 2 において入力が L のアルゴリズムとする. L が鍵生成の途中で計算された T, L_X を用いて O'_{T,L_X} からサンプリングされると $\mathcal{B}_1$ は Game 0 のような出力結果を得る. L が $\mathcal{U}(\mathbb{F}_q^{n\times n})$ からサンプリングされると Game 1 のような出力結果を得る. ゆえに, もし $\mathcal{A}$ が Game 0 と Game 1 を見分けられるとき, $\mathcal{A}\circ\mathcal{B}_1$ は O'_{T,L_X} からのサンプルと $\mathcal{U}(\mathbb{F}_q^{n\times n})$ からのサンプルを見分けられる. つまり,

$$|\Pr(S_0) - \Pr(S_1)| \le \mathrm{Adv}^{\mathsf{invert}}(\mathcal{A}\circ\mathcal{B}_1) \tag{2}$$

Game 2. このゲームでは, 暗号文 $\mathbf{c}$ は平文 $\mathbf{m}$ から LWE 問題の構造を用いて計算されるのではなく, 一様ランダムに計算される.

Game 0:
input$(n, p, L_{1,X}, L_{1,Y}, L_{r,X}, L_{r,Y}, q, \{r_i\}_{i\in n}, \mathbf{m})$
1. $L_X = L_{1,X} + [r_j]L_{r,X}$
2. $L_Y = pL_{1,Y} + [r_j]L_{r,Y}$
3. $T = L_Y^{-1} \in \mathbf{F}_q^{n\times n}$
4. $L_F = T \circ L_X \in \mathbf{F}_q^{n\times n}$
5. $\mathbf{e} \xleftarrow{\$} \chi(I_p^n)$
6. $\mathbf{c} = L_F(\mathbf{m}) + \mathbf{e} \in \mathbb{F}_q^n$
7. $\mathbf{c}' \xleftarrow{\$} \mathcal{U}(\mathbb{F}_q^n)$
8. $b^* \xleftarrow{\$} \mathcal{U}(\{0,1\})$
9. **if** $b^* = 0$ **return**$(L_F, \mathbf{c})$
10. **else return**$(L_F, \mathbf{c}')$

Game 1:
input$(n, p, L_{1,X}, L_{1,Y}, L_{r,X}, L_{r,Y}, q, \{r_i\}_{i\in n}, \mathbf{m})$
1. $\boxed{L_F \xleftarrow{\$} \mathcal{U}(\mathbb{F}_p^{n\times n})}$
2. $\mathbf{e} \xleftarrow{\$} \chi(I_p^n)$
3. $\mathbf{c} = L_F(\mathbf{m}) + \mathbf{e} \in \mathbb{F}_q^n$
4. $\mathbf{c}' \xleftarrow{\$} \mathcal{U}(\mathbb{F}_q^n)$
5. $b^* \xleftarrow{\$} \mathcal{U}(\{0,1\})$
6. **if** $b^* = 0$ **return**$(L_F, \mathbf{c})$
7. **else return**$(L_F, \mathbf{c}')$

Game 2:
input$(n, p, L_{1,X}, L_{1,Y}, L_{r,X}, L_{r,Y}, q, \{r_i\}_{i\in n}, \mathbf{m})$
1. $L_F \xleftarrow{\$} \mathcal{U}(\mathbb{F}_p^{n\times n})$
2. $\boxed{\mathbf{c} \xleftarrow{\$} \mathcal{U}(\mathbb{F}_q^n)}$
3. $\mathbf{c}' \xleftarrow{\$} \mathcal{U}(\mathbb{F}_q^n)$
4. $b^* \xleftarrow{\$} \mathcal{U}(\{0,1\})$
5. **if** $b^* = 0$ **return**$(L_F, \mathbf{c})$
6. **else return**$(L_F, \mathbf{c}')$

図 1 Linear-pqe method のゲーム

$\mathcal{B}_1(L)$
1. $L_F \leftarrow L$
2. $\mathbf{e} \xleftarrow{\$} \chi(I_p^n)$
3. $\mathbf{c} = L_F(\mathbf{m}) + \mathbf{e} \in \mathbb{F}_q^n$
4. $\mathbf{c}' \xleftarrow{\$} \mathcal{U}(\mathbb{F}_q^n)$
5. $b^* \xleftarrow{\$} \mathcal{U}(\{0,1\})$
6. **if** $b^* = 0$ **return**$(L_F, \mathbf{c})$
7. **else return**$(L_F, \mathbf{c}')$

$\mathcal{B}_2(\mathbf{a})$
1. $\mathbf{c} \leftarrow \mathbf{a}$
2. $\mathbf{c}' \xleftarrow{\$} \mathcal{U}(\mathbb{F}_q^n)$
3. $b^* \xleftarrow{\$} \mathcal{U}(\{0,1\})$
4. **if** $b^* = 0$ **return**$(L_F, \mathbf{c})$
5. **else return**$(L_F, \mathbf{c}')$

図 2 図 1 の削減アルゴリズム

Game 1 と **Game 2** の違い. Game 1 では, $\mathbf{c}$ は $O_{\chi,\mathbf{m}}$ からサンプリングされる. しかし, Game 2 では $\mathbf{c}$ は $\mathcal{U}(\mathbb{F}_q^n)$ からサンプリングされる.

より明確にすると, まず $\mathcal{B}_2$ を図 2 において入力が $\mathbf{a}$ のアルゴリズムとする. $\mathbf{a}$ が平文 $\mathbf{m}$ を用いて $O_{\chi,\mathbf{m}}$ からサンプリングされると $\mathcal{B}_2$ は Game 1 のような出力結果を得る. $\mathbf{a}$ が $\mathcal{U}(\mathbb{F}_q^{n\times n})$ からサンプリングされると Game 2 のような出力結果を得る. ゆえに, もし $\mathcal{A}$ が Game 1 と Game 2 を見分けられるとき, $\mathcal{A}\circ\mathcal{B}_2$ は $O_{\chi,\mathbf{m}}$ からのサンプルと $\mathcal{U}(\mathbb{F}_q^n)$ からのサンプルを見分けられる. つまり,

$$|\Pr(S_1) - \Pr(S_2)| \le \mathrm{Adv}^{\mathsf{u-dlwe-ss}}_{n,p,q,\chi}(\mathcal{A}\circ\mathcal{B}_2) \qquad (3)$$

Game 2 の評価. Game 2 では, 敵対者は b^* を推測し, それによって $\mathbf{c}$ と $\mathbf{c}'$ を見分ける. Game 2 において, $\mathbf{c}, \mathbf{c}'$ は明らかに一様乱数である. したがって,

$$\Pr(S_2) = 1/2 \qquad (4)$$

結論. (1)-(4) により, 定理 4.1 は証明された.

4.2 ring-pqe method の安全性証明

以下において, n を正の整数, p を小さい素数, χ を $\mathbb{Z}$ 上の分布, $L_{1,X}, L_{1,Y}, L_{r,X}, L_{r,Y}$ を多項式環 R において R/pR からランダムにサンプリングとした行列とし, q, r は前述のパラメーターを用いて 3.1 のアルゴリズムにしたがってサンプリングしたものとする. また, 平文 $\mathbf{m}$ は $n-1$ 次かつ係数を I_p 中に持つ多項式の集合 I_p^n から取るものとする.

また, 先ほどの定義 4.1 をリングバージョンに書き直す.

定義 4.3 (Unique ring short-LWE 識別問題)**.** 以下の問題を *Unique ring short-LWE* 識別問題と呼ぶこととする. p を小さい素数,n, q を正の整数, χ を $\mathbb{Z}$ 上の分布とし, 平文 $\mathbf{m}$ は集合 I_p^n からとるものとする. また, $O_{\chi,\mathbf{m}}$ と U を定義する.

- $O_{\chi,\mathbf{m}} : L \xleftarrow{\$} \mathcal{U}(R/qR), \mathbf{e} \xleftarrow{\$} \chi(I_p^n);$ *return* $(L, L(\mathbf{m}) + \mathbf{e} \in R/qR)$.
- $U : L \xleftarrow{\$} \mathcal{U}(R/qR), \mathbf{u} \xleftarrow{\$} \mathcal{U}(R/qR);$ *return* $(L, \mathbf{u})$.

パラメータを (n, p, q, χ) とする短い秘密を用いた *ring-LWE* 識別問題は, $O_{\chi,\mathbf{m}}$ と U を見分けることである. また, この識別問題が困難であるという仮定を *Unique ring short-LWE* 識別仮定と呼ぶ. ここで, この識別問題を解くアルゴリズム $\mathcal{A}$ についてアドバンテージを定義する.

$$\mathrm{Adv}^{\mathsf{u-dRlwe-ss}}_{n,p,q,\chi}(\mathcal{A}) = |\Pr(\mathbf{m} \xleftarrow{\$} \chi(I_p^n) : \mathcal{A}^{O_{\chi,\mathbf{m}}}() = 1) - \Pr(\mathcal{A}^{U}() = 1)|$$

また, 定義 4.2 についても同様に書き直す.

定義 4.4. *ring-pqe method* 内で生成される行列 T, L_X について, 二つのオラクル O'_{T,L_X} と U' を定義する.

- O'_{T,L_X} : *return* $T \circ L_X \in R/qR$.
- $U' : U \xleftarrow{\$} \mathcal{U}(R/qR)$ *return* U.

また, O'_{T,L_X} と U' を見分けるアルゴリズム $\mathcal{A}$ について, 以下のアドバンテージを定義する.

$$\mathrm{Adv}^{\mathsf{R-invert}}(\mathcal{A}) = |\Pr(\mathcal{A}^{O'_{T,L_X}}() = 1) - \Pr(\mathcal{A}^{U'}() = 1)|$$

Linear-pqe method の安全性証明について, 以下の図 3 のゲームの流れで証明をする.

Game 0:
input$(n, p, L_{1,X}, L_{1,Y}, L_{r,X}, L_{r,Y}, q, r, \mathbf{m})$
1. $L_X = L_{1,X} + rL_{r,X}$
2. $L_Y = pL_{1,Y} + rL_{r,Y}$
3. $T = L_Y^{-1} \mod q \in R/qR$
4. $L_F = T \cdot L_X \in R/qR$
5. $\mathbf{e} \xleftarrow{\$} \chi(I_p^n)$
6. $\mathbf{c} = L_F(\mathbf{m}) + \mathbf{e} \in R/qR$
7. $\mathbf{c}' \xleftarrow{\$} \mathcal{U}(R/qR)$
8. $b^* \xleftarrow{\$} \mathcal{U}(\{0,1\})$
9. **if** $b^* = 0$
   return$(L_F, \mathbf{c})$
10. **else**
   return$(L_F, \mathbf{c}')$

Game 1:
input$(n, p, L_{1,X}, L_{1,Y}, L_{r,X}, L_{r,Y}, q, r, \mathbf{m})$
1. $\boxed{L_F \xleftarrow{\$} \mathcal{U}(R/qR)}$
2. $\mathbf{e} \xleftarrow{\$} \chi(I_p^n)$
3. $\mathbf{c} = L_F(\mathbf{m}) + \mathbf{e} \in R/qR$
4. $\mathbf{c}' \xleftarrow{\$} \mathcal{U}(R/qR)$
5. $b^* \xleftarrow{\$} \mathcal{U}(\{0,1\})$
6. **if** $b^* = 0$
   return$(L_F, \mathbf{c})$
7. **else**
   return$(L_F, \mathbf{c}')$

Game 2:
input$(n, p, L_{1,X}, L_{1,Y}, L_{r,X}, L_{r,Y}, q, r, \mathbf{m})$
1. $L_F \xleftarrow{\$} \mathcal{U}(R/qR)$
2. $\boxed{\mathbf{c} \xleftarrow{\$} \mathcal{U}(R/qR)}$
3. $\mathbf{c}' \xleftarrow{\$} \mathcal{U}(R/qR)$
4. $b^* \xleftarrow{\$} \mathcal{U}(\{0,1\})$
5. **if** $b^* = 0$
   return$(L_F, \mathbf{c})$
6. **else**
   return$(L_F, \mathbf{c}')$

図 3 ring-pqe method のゲーム

このアルゴリズムの安全性を証明するために, このアルゴリズムを通して生成された暗号文 $\mathbf{c}$ と, 一様ランダムに生成された暗号文 $\mathbf{c}'$ を見分ける敵対者の存在を考える. このとき, そのような敵対者 $\mathcal{A}$ のアドバンテージを以下で定義する.

$$\mathrm{Adv}_{n,p,L_{ab},r,q,\chi}(\mathcal{A}) = |\Pr[L_F, \mathbf{c}] - \Pr[L_F, \mathbf{c}']|$$

ここで, $L_{ab} = L_{a,b}(a \in \{1, r\}, b \in \{X, Y\})$ とする.

定理 4.2. 定義 *4.3* がパラメーター (n, p, q, χ) において困難かつ 定義 *4.4* の識別問題が困難なとき, *Linear-pqe method* はランダムに生成された暗号文と区別がつかない暗号文を得る. つまり, 図 *4* で与えられる削減アルゴリズム $\mathcal{B}_1, \mathcal{B}_2$ について以下が成り立つ.

$$\mathrm{Adv}_{n,p,L_{ab},r,q,\chi}(\mathcal{A}) \leq \mathrm{Adv}^{\mathsf{R-invert}}(\mathcal{A} \circ \mathcal{B}_1) + \mathrm{Adv}^{\mathsf{u-dRlwe-ss}}_{n,p,q,\chi}(\mathcal{A} \circ \mathcal{B}_2)$$

この定理は, *Unique ring short-LWE* 識別仮定, 行列積識別仮定仮定のもとで このアルゴリズムにおいて 敵対者が得られるアドバンテージが 限りなく小さいことを意味する.

Game 0. まず, もととなるゲームについて考える. $\Pr(S_0)$ を求めるために 以下とする.

$$\mathrm{Adv}_{n,p,L_{ab},r,q,\chi}(\mathcal{A}) = |\Pr(S_0) - 1/2| \tag{1}$$

Game 1. このゲームでは, 行列 L_F がアルゴリズム中の L_X と T の積から計算されるのではなく, 一様ランダムに生成される.

Game 0 と **Game 1** の違い. Game 0 では, L_F は O'_{T,L_X} からサンプリングされる. しかし, Game 1 では L_F は $R/qR)$ からサンプリングされる. より明確にすると, まず $\mathcal{B}_1$ を図 4 において入力が L のアルゴリズムとする. L が鍵生成の途中で計算された T, L_X を用いて O'_{T,L_X} からサンプリングされると $\mathcal{B}_1$ は Game 0 のような出力結果を得る. L が $\mathcal{U}(R/qR)$ からサンプリングされると Game 1 のような出力結果を得る. ゆえに, もし $\mathcal{A}$ が Game 0 と Game 1 を見分けられるとき, $\mathcal{A} \circ \mathcal{B}_1$ は O'_{T,L_X} からのサンプルと $\mathcal{U}(R/qR)$ からのサンプルを見分けられる. つまり,

$$|\Pr(S_0) - \Pr(S_1)| \leq \mathrm{Adv}^{\mathsf{R-invert}}(\mathcal{A} \circ \mathcal{B}_1) \tag{2}$$

Game 2. このゲームでは, 暗号文 $\mathbf{c}$ は平文 $\mathbf{m}$ から LWE 問題の構造を用いて計算されるのではなく, 一様ランダムに計算される.

Game 1 と **Game 2** の違い. Game 1 では, $\mathbf{c}$ は $O_{\chi,\mathbf{m}}$ からサンプリングされる. しかし, Game 2 では $\mathbf{c}$ は $\mathcal{U}(R/qR)$ からサンプリングされる.

より明確にすると, まず $\mathcal{B}_2$ を図 4 において入力が $\mathbf{a}$ のアルゴリズムとする. $\mathbf{a}$ が平文 $\mathbf{m}$ を用いて $O_{\chi,\mathbf{m}}$ からサンプリングされると $\mathcal{B}_2$ は Game 1 のような出力結果を得る. $\mathbf{a}$ が $\mathcal{U}(R/qR)$ からサンプリングされると Game 2 のような出力結果を得る. ゆえに, もし $\mathcal{A}$ が Game 1 と Game 2 を見分けられるとき, $\mathcal{A} \circ \mathcal{B}_2$ は $O_{\chi,\mathbf{m}}$ からのサンプルと $\mathcal{U}(R/qR)$ からのサンプルを見分けられる. つまり,

$$|\Pr(S_1) - \Pr(S_2)| \leq \mathrm{Adv}^{\mathsf{u-dRlwe-ss}}_{n,p,q,\chi}(\mathcal{A} \circ \mathcal{B}_2) \tag{3}$$

Game 2 の評価. Game 2 では, 敵対者は b^* を推測し, それによって $\mathbf{c}$ と $\mathbf{c}'$ を見分ける. Game 2 において, $\mathbf{c}, \mathbf{c}'$ は明らかに一様乱数である. したがって,

$$\Pr(S_2) = 1/2 \tag{4}$$

結論. (1)-(4) により, 定理 4.2 は証明された.

$\underline{\mathcal{B}_1(L)}$
1. $L_F \leftarrow L$
2. $\mathbf{e} \xleftarrow{\$} \chi(I_p^n)$
3. $\mathbf{c} = L_F(\mathbf{m}) + \mathbf{e} \in R/qR$
4. $\mathbf{c}' \xleftarrow{\$} \mathcal{U}(R/qR)$
5. $b^* \xleftarrow{\$} \mathcal{U}(\{0,1\})$
6. **if** $b^* = 0$ **return**$(L_F, \mathbf{c})$
7. **else return**$(L_F, \mathbf{c}')$

$\underline{\mathcal{B}_2(\mathbf{a})}$
1. $\mathbf{c} \leftarrow \mathbf{a}$
2. $\mathbf{c}' \xleftarrow{\$} \mathcal{U}(R/qR)$
3. $b^* \xleftarrow{\$} \mathcal{U}(\{0,1\})$
4. **if** $b^* = 0$ **return**$(L_F, \mathbf{c})$
5. **else return**$(L_F, \mathbf{c}')$

図 4 図 3 の削減アルゴリズム

4.3 安全性の評価

4.1 節では定義 4.1 と定義 4.2, 4.2 節では定義 4.3 と定義 4.4 という識別問題を定義し, その識別問題が困難であるという仮定のもと 4.1 節, 4.2 節の証明をおこなった. この節では, 3.2 節の Frodo と 4.1 節の Linear-pqe method の安全性において, どの程度安全性に違いががあるのか考察する. まず, 3.2 節の Frodo では, その安全性が定義 3.1 に基づいている. これを定義 4.1 と比較する. これらの識別問題の違いは, 小さい正の整数 p と正の整数 n に対し, 秘密ベクトルとエラーベクトルを $\mathbb{Z}_p^n$ から取るか I_p^n を取るかの違いと, 定義 4.1 において秘密ベクトルの積に用いる行列 A が一様ランダムな行列であるかの違いに他ならない.

秘密ベクトル $\mathbf{s}$ とエラーベクトル $\mathbf{e}$ を $\mathbb{Z}_p^n$ から取るか I_p^n を取るかの違いについては, 証明まではしないが, $\mathbb{Z}_p^n$, I_p^n のとる値の範囲は同じであり, 最終的に $B = A\mathbf{s} + \mathbf{e}$ を計算し, 素数 q で法をとっているため B のとる値の範囲は変わらないとみなせる. したがって, 秘密ベクトルとエラーベクトルを $\mathbb{Z}_p^n$ から取るか I_p^n を取るかによって違いは生じないと考えられる.

定義 4.1 において秘密ベクトルの積に用いる行列 A が一様ランダムな行列であるかについて, これは定義 4.2 の識別問題が困難であれば A も一様ランダムに選んだ行列と見分けがつかないことになる. したがって, 定義 4.2 の行列積識別仮定が成り立てば, Frodo と Linear-pqe method の安全性にはそれほど差がないと考察する.

しかし, 今回の提案において, 行列積識別仮定については, 定義 4.2 で述べた内容が実際に識別不可能かまでは証明しきれず, その安全性を完全に示すまでには至れなかった.

5. まとめ

この論文では, Linear-pqe method については Unique short-LWE 識別仮定と行列積識別仮定, ring-pqe method については Unique ring short-LWE 識別仮定と行列積識別仮定仮定のもとで, アルゴリズムを通して生成された暗号文と一様ランダムに生成された暗号文を見分けようとする敵対者 $\mathcal{A}$ が得られるアドバンテージが無視できるほど無視できるほど小さいことが示された. したがって, Unique short-LWE 識別仮定, Unique ring short-LWE 識別仮定, 行列積識別仮定のもとで二つのアルゴリズムが IND-CPA 安全性を満たすことが証明できた.

謝辞

本研究は JSPS 科研費 JP21K11751，JP21H034438 と文部科学省の平成 30 年度「Society 5.0 実現化研究拠点支援事業」の助成を受けたものです.

参考文献

[1] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *Advances in Cryptology-CRYPTO 2009: 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, pages 595–618. Springer, 2009.

[2] Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from lwe. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 1006–1018, 2016.

[3] Jintai Ding and Bo-Yin Yang. Multivariate public key cryptography. *Post-quantum cryptography*, pages 193–241, 2009.

[4] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[5] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[6] Yuntao Wang, Yasuhiko Ikematsu, and Takanori Yasuda. Public key cryptosystems combining lattice and multivariate polynomial. In *SCIS 2021*, 2021.

[7] Yuntao Wang, Yasuhiko Ikematsu, and Takanori Yasuda. Lattice-based public key cryptosystems invoking linear mapping mask. In *Provable and Practical Security: 16th International Conference, ProvSec 2022, Nanjing, China, November 11–12, 2022, Proceedings*, pages 88–104. Springer, 2022.

[8] Takanori Yasuda. Multivariate encryption schemes based on the constrained mq problem. In *Provable Security: 12th International Conference, ProvSec 2018, Jeju, South Korea, October 25-28, 2018, Proceedings 12*, pages 129–146. Springer, 2018.

[9] Takanori Yasuda. Multivariate public key system using noise. In *SCIS 2020*, 2020.

[10] Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, and Kouichi Sakurai. Mq challenge: hardness evaluation of solving multivariate quadratic problems. *Cryptology ePrint Archive*, 2015.