Vol.2020-DPS-182 No.6
Vol.2020-CSEC-88 No.6
2020/3/12

Ring-LWEの定義体の拡張に関する研究

石村 隆晃[1,a)]　奥村 伸也[2,b)]　宮地 充子[2,c)]

概要：Ring-LWE 問題は，大規模な量子コンピュータ完成後も計算困難な問題と考えられ，耐量子暗号や (耐量子) 準同型暗号のみならず (耐量子) 鍵交換方式の構成に利用されている．効率面からの理由により，通常円分体上で Ring-LWE ベースの暗号プロトコルは構成されるが，有田らは分解体と呼ばれる円分体の部分体上で Ring-LWE ベースの準同型暗号を構成し，円分体を用いるよりもより多くの平文を一括で暗号化し準同型処理を施すことができることを示した．また，用途により円分体以外の Ring-LWE に適した代数体を探す研究プロジェクトの提案も存在する．円分体以外の代数体を Ring-LWE に利用する場合は，円分体と同程度の効率を有するように構成しなくてはならず，有田らは分解体を用いる場合には効率面の問題を克服できることを示している．しかし，円分体や分解体以外では効率面の問題を克服できるかは示されていない．本研究では，素数 m に対する円分体 $\mathbb{Q}(\zeta_m)$ の部分体については，効率的な Ring-LWE ベースの暗号プロトコルの構成に利用できる可能性があることを，有田らが分解体の場合に用いた方法に従って示す．

1. はじめに

現代はセキュリティが日常に深く浸透しており，セキュリティが我々の生活を支えるインフラであることに異論はないだろう．このような状況下で企業などが量子コンピュータ開発に力をいれている．量子コンピュータ開発技術の発展により，計算速度が飛躍的に向上し，我々の生活が豊かになることは疑いようもない．その一方で技術の進歩には負の側面もある．それは量子コンピュータを用いたセキュリティへの攻撃が行われうるということである．なぜなら量子コンピュータが大規模化すれば，RSA 暗号や楕円曲線暗号などの現在広く利用されている多くの公開鍵暗号は解読されることがしられている [8]．そこで NIST(アメリカ国立標準技術研究所) は，量子コンピュータ実用化後も安全な暗号 (耐量子暗号) の標準化を目的として耐量子暗号標準化プロジェクト [1] を立ち上げている．

Learning With Errors(LWE) 問題 [7] は量子コンピュータを用いても計算困難と考えられており，耐量子暗号や耐量子鍵交換方式などの構成に利用されており注目を集めている．LWE 問題とはエラーが加えられた有限体上の連立一次方程式を解く問題である． LWE 問題は有限体上で扱われるが，代数体の整数環上で扱われる LWE 問題を Ring-LWE 問題 [3] という．より正確には，素数 q と代数体の整数環 R について，剰余環 $R_q := R/qR$ は乗算も可能な $\mathbb{F}_q$ 上のベクトル空間となるが，Ring-LWE はこの R_q 上で構成される．Ring-LWE 問題は LWE 問題に代数的な構造が付加されることで，LWE よりも効率的な暗号プロトコルを構成できると考えられている．

Ring-LWE 問題に基づく暗号プロトコルでは，R_q の元同士の乗算に最も時間がかかるため，その高速化には，R_q での乗算の効率化が必須である．中国式剰余定理から R_q には，係数ごとの積だけで済む高速乗算に適した $\mathbb{F}_q$ 上の基底が存在する．しかし，そのような基底のみでは Ring-LWE 問題が容易に解けるようになりセキュリティ面に脆弱性を生む．これを解決するために Ring-LWE 問題が困難となるような基底から始め，基底変換を行って乗算しやすい基底に変換し，乗算後に元の基底に逆変換する．このような変換，逆変換が効率的にできる基底の組を見つける必要がある．円分体上には $Powerful$-基底と CRT-基底に代表される前述の条件を満たす基底の組が存在することが知られており [4]，円分体は Ring-LWE を扱う際広く利用されている．

一方，用途に合わせて円分体上だけではなく他の代数体上で Ring-LWE ベースの暗号プロトコルを構成する研究プロジェクトが提案されている [6]．実際に，円分体以外の代数体として，有田らは分解体上で Ring-LWE ベースの準同型暗号を提案し，円分体を用いるよりも多くの平文

[1] 大阪大学工学部
Osaka University
[2] 大阪大学大学院 工学研究科
Osaka University
[a)] ishimura@cy2sec.comm.eng.osaka-u.ac.jp
[b)] okumura@comm.eng.osaka-u.ac.jp
[c)] miyaji@comm.eng.osaka-u.ac.jp

を効率的に一括で暗号化し準同型演算処理が可能であることを示した [2]．有田らは，分解体上でも円分体における $Powerful$-基底と CRT-基底に対応する Ring-LWE に適した基底の組 (η-基底 と ξ-基底 と呼ばれる) が存在することを示している．

今後も暗号プロトコルが応用される場面は増えると考えられるが，代数体の種類は多岐にわたり，興味深い固有の性質を持つものが多い．さらに，円分体や分解体のみの場合，使用できるパラメータ，特に安全性に関わってくる円分体・分解体の $\mathbb{Q}$ 上の拡大次数やモジュラスパラメータ q が限定的になるため，より柔軟なパラメータ設定を可能にすることは重要である．そのため，効率的な Ring-LWE ベースの暗号プロトコルの構成に利用できる円分体以外の代数体を検討することは今後必要になってくると考えられる．

本研究では，効率的な Ring-LWE ベースの暗号プロトコルの構成に利用できる代数体を増やすことを目的とし，まずは素数 m に対する m-th 円分体の部分体について，有田らが η-基底と ξ-基底を構成した方法と同様の方法で，基底の組を構成した．構成した基底の組による乗算計算について実験を行い，提案手法 (基底変換を利用した手法) とそうでない場合とでは，実験したパラメータについては提案手法の方が高速に乗算を行えることを確かめた．

2. 代数体と Ring-LWE 問題

2.1 代数体

Ring-LWE 問題を説明する前に，まずは代数体について簡単に述べる．さらなる詳細については，例えば [5] を参照されたい．

代数体とは，有理数体 $\mathbb{Q}$ の有限次拡大体のことである．(つまり，$\mathbb{Q}$ を部分体として含み，$\mathbb{Q}$-ベクトル空間として有限次元の体である．) 体 K を代数体とする．$a \in K$ が 0 でないモニックな $f(X) \in \mathbb{Z}[X]$ の根である，つまり $f(a) = 0$ が成り立つとき，a を代数的整数といい，K の代数的整数全体の集合 O_K は環となり K の整数環と呼ばれる．K の $\mathbb{Q}$ 上の拡大次数 (K の $\mathbb{Q}$-ベクトル空間としての次元) を n とすると，O_K には n 個の $\mathbb{Z}$-基底が存在する．

整数環 O_K の任意のイデアル $I \subset O_K$ は，一意的に素イデアル分解が可能である．つまり，O_K の素イデアル $\mathcal{P}_1, \ldots, \mathcal{P}_m$ と自然数 $e_i \geq 1$ $(1 \leq i \leq m)$ が存在して，$I = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_m^{e_m}$ と書ける．素数 p について $I = pO_K$ のとき，全ての $1 \leq i \leq m$ について $e_i = 1$ が成り立つなら，p は K で不分岐であるといい，そうでないなら p は K で分岐するという．各素イデアル $\mathcal{P}_i$ について，$O_K/\mathcal{P}_i$ は有限体 $\mathbb{F}_{p^{f_i}}$ となるが，K が $\mathbb{Q}$ のガロア拡大であるとき，$e_1 = \cdots = e_m$, $f_1 = \cdots = f_m$ となる．また，各 e_i, f_i が 1 になるとき，p は K で完全分解するという．

各素イデアル $\mathcal{P}_i$ は O_K の極大イデアルとなるから，$\mathcal{P}_i + \mathcal{P}_j = O_K (i \neq j)$ が成り立つ．(この時，$\mathcal{P}_i$ と $\mathcal{P}_j$ は互いに素という．) よって，中国式剰余定理のイデアル版である以下の環同型が成り立つ：

$$O_K/\mathcal{P}_1 \cdots \mathcal{P}_m \cong O_K/\mathcal{P}_1 \times \cdots \times O_K/\mathcal{P}_m.$$

2.1.1 Ring-LWE Problem

素数 q 及び代数体 K とその整数環 O_K について，$O_{K,q} := O_K/qO_K$ を考える．χ_{secret} と χ_{error} を $O_{K,q}$ 上の確率分布とする．このとき，$a \in O_{K,q}$ を χ_{error} に従ってサンプルすることを $a \leftarrow \chi_{\text{error}}$ と記す．また，$U(O_{K,q})$ を $O_{K,q}$ 上の一様分布とする．このとき，$O_{K,q} \times O_{K,q}$ 上の Ring-LWE サンプルとは，$a \leftarrow U(O_{K,q})$, $s \leftarrow \chi_{\text{secret}}$, $e \leftarrow \chi_{\text{error}}$ に対して $(a, as + e)$ の形をした $O_{K,q} \times O_{K,q}$ からのサンプルのことである．

Ring-LWE 問題には，探索 Ring-LWE 問題と識別 Ring-LWE 問題の 2 つが存在する．探索 Ring-LWE 問題とは，任意個の Ring-LWE サンプル $(a_i, a_i s + e_i) \in O_{K,p} \times O_{K,p}$ に対して，s を計算する問題である．一方，識別 Ring-LWE 問題とは，任意個の $O_{K,p} \times O_{K,p}$ からのサンプル (a_i, b_i) が Ring-LWE サンプルか一様にサンプルされたかを識別する問題である．

代数体 K 上の Ring-LWE ベースの暗号プロトコルでは，$O_{K,q}$ の元同士の乗算と加算の計算が複数回行われるが，特に乗算計算に最も時間がかかる．そのため，高速に乗算計算を行う必要があるが，その際次節で見るように，$O_{K,q}$ の $\mathbb{F}_q$ 上の基底がポイントとなる．

3. 円分体と Ring-LWE

ここでは，円分体について説明し，なぜ円分体が効率的な Ring-LWE ベースの暗号プロトコルの構成に利用されているかを説明する．ここでも円分体に関するさらなる詳細については，[5] を参照されたい．

自然数 m について，ζ_m を 1 の原始 m 乗根とし，$\mathbb{Q}$ に ζ_m を添加した体 ($\mathbb{Q}$ と ζ_m を含む最小の体)$K = \mathbb{Q}(\zeta_m)$ を m-th 円分体という．円分体 K の整数環は，$O_K = \mathbb{Z}[\zeta_m]$ であり，$1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}$ は O_K の $\mathbb{Z}$-基底の 1 つであり，m が素数か素数冪のとき第 1 節で述べた $Powerful$-基底に該当するものである．ここで，$n := \varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$ はオイラー関数である．円分体 K は $\mathbb{Q}$ のガロア拡大であり，そのガロア群 $\mathrm{Gal}(K/\mathbb{Q})$ は $(\mathbb{Z}/m\mathbb{Z})^*$ と同型である．つまり，ガロア理論から K の部分体を定めることは $(\mathbb{Z}/m\mathbb{Z})^*$ の部分群を定めることと同値である．

ガロア群の元 $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ は，ある m と互いに素な自然数 j を用いて $\sigma(\zeta_m) = \zeta_m^j$ を満たす．そのような元を σ_j と書くこととする．このとき，$\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*; \sigma_j \mapsto j \pmod{m}$ が上記の同型を与える．

素数 q が $q \equiv 1 \pmod{m}$ を満たせば，K で完全分解することが知られている．このとき，中国式剰余定理

(のイデアル版) より，環の同型 $O_{K,q} \cong (\mathbb{F}_q)^n$ が存在する．この同型について，$(\mathbb{F}_q)^n$ の $\mathbb{F}_q$ 上の自然な基底 $e_1 = (1,0,\ldots,0), e_2 = (0,1,0,\ldots,0), \ldots, e_n = (0,\ldots,0,1)$ に対応する $c_1,\ldots,c_n \in O_{K,q}$ が第 1 節で述べた CRT-基底と呼ばれるものであり，高速乗算を実現できる基底である．実際，$a = \sum_i a_i c_i$, $b = \sum_i b_i c_i \in O_{K,q} (a_i, b_i \in \mathbb{F}_q)$ とすると，$ab = \sum_i a_i b_i c_i$ となり，係数ごとの乗算で $O_{K,q}$ の元同士の乗算が可能となる．

しかし，CRT-基底で Ring-LWE 問題を考えた場合，例えば，探索 Ring-LWE 問題は，$a = \sum_i a_i c_i$, $s = \sum_i s_i c_i$, $e = \sum_i e_i c_i$ とすると，a_i が既知で s_i, e_i が未知の時に $as + e = \sum_i (a_i s_i + e_i) c_i$ から s_i を求める問題となるが，e_i は q に対して十分小さく取られることから，そのような問題は $(a_1, 0, \ldots, 0), \ldots, (0, \ldots, a_n)$ を基底とする非常に単純な格子から得られる最短/最近ベクトル問題を解くことで解が得られる．

一方，$Powerful$-基底で表現した元同士の乗算は，計算が複雑になるが，Ring-LWE 問題が容易になるという結果は現在までに得られていない．さらに，$Powerful$-基底と CRT-基底の間には，高速フーリエ変換などの手法により高速な基底変換の手法が存在する．よって，円分体上で Ring-LWE 問題を考える場合は，2 つの基底を利用する場合が多い．

4. 分解体と Ring-LWE

ここでは，有田らが Ring-LWE ベースの準同型暗号の構成に利用した，素数 m に対する m-th 円分体 K の部分体としての分解体について述べる．

素数 p を m と異なる素数とする．ガロア理論より p (mod. m) が生成する $(\mathbb{Z}/m\mathbb{Z})^*$ の部分群に対応する K の部分体 Z が存在する．その Z を p に対する K の分解体という．分解体も $\mathbb{Q}$ のガロア拡大であり，そのガロア群は $(\mathbb{Z}/m\mathbb{Z})^*/ < p >$ と同型である．p に対する分解体を Ring-LWE に利用する場合，$q = p^r$ $(r \geq 1)$ を用いて $O_{Z,q}$ 上で演算を行う．分解体 Z 上での Ring-LWE に適した基底の組について説明する [2].

4.1 η-基底

定義 4.1.
m を素数として $K = \mathbb{Q}(\zeta_m)$ を m 次円分体とする．Z を素数 $p(\neq m)$ に対する K の分解体とする．$\mathbb{Z}_m^*/\langle p\rangle \simeq Gal(Z|\mathbb{Q})$ の代表元の任意の組を $\{t_0, \cdots t_{g-1}\}$(代表元の数が g 個) に固定するとき $i = 0, \cdots g-1$ に対して

$$\eta_i = Tr_{K|Z}(\zeta^{t_i}) = \sum_{a\in\langle p\rangle} \zeta^{t_i a}.$$

と定義する．

定義 4.2 (η-基底)**.**
$Z \subset K$ を p に関する分解体とし, 整数環を $R_Z = R \cap Z$ とするとき, $\vec{\eta} = (\eta_0, \cdots \eta_{g-1})$ を R_Z の η- 基底と定義する．任意の $a \in R_Z$ に $a = \vec{\eta^T}\vec{a}$ を満たし対応する $\vec{a} \in \mathbb{Z}^g$ が存在する．このとき $\vec{a}$ を η-$vector$ と呼ぶ.

4.1.1 ξ-基底

代表元 t_i の選択により Z のガロア群 $Gal(Z|\mathbb{Q})$ は以下のように表される．

$$\mathrm{Gal}(Z|\mathbb{Q}) = \{\rho_{t_0}, \cdots, \rho_{t_{g-1}}\}.$$

分解体上の要素 $a \in Z$ は正規の埋め込み σ_Z を通して g 次元の $\mathbb{R}$ ベクトルとして表現され:

$$\sigma_Z : Z \to H_Z(\subset \mathbb{C}^{\mathbb{Z}_m^*/\langle p\rangle});$$
$$a \to (\rho_i(a))_{i\in\mathbb{Z}_m^*/\langle p\rangle}.$$

のようになる．

定義 4.3 (分解体上での正規の埋め込み)**.**
ここで, 写像 $\sigma_Z(Z)$ は以下で定義される g 次元の $\mathbb{R}$ 部分空間 H_Z に含まれている．

$$H_Z \stackrel{\mathrm{def}}{=} \{x \in \mathbb{C}^{\mathbb{Z}_m^*/\langle p\rangle} : x_i = \bar{x}_{m-i} (\forall i \in \mathbb{Z}_m^*/\langle p\rangle)\}$$

このとき分解体上の要素 $a \in Z$ は正規の埋め込みから以下のように表される．

$$\sigma_Z : K \to H_Z \subset \mathbb{C}^{\mathbb{Z}_m^*/\langle p\rangle};$$
$$\sigma_Z(a) = (\rho_i(a))_{i\in\mathbb{Z}_m^*/\langle p\rangle}.$$

定義 4.4 (変換行列 Ω_Z)**.**
$g \times g$ の行列 Ω_Z を以下のように定義する．

$$\Omega_Z = (\rho_{t_i}(\eta_j))_{0\leq i,j<g} (\in R_Z^{g\times g})$$

Ω_Z のそれぞれの列は埋め込み $\sigma_Z(\eta_j)$ である．ガロア群 $\mathrm{Gal}(Z|\mathbb{Q})$ は巡回群であるから代表元 $\{t_0, \cdots, t_{g-1}\}$ が $j = 0, \cdots g-1$ に対して $t_j \equiv t^j (mod\ m)$ のように取れる．また任意の i, j に対して $\eta = Tr_{K|Z}(\zeta)$ から

$$\rho_{t_i}(\eta_j) = \eta_{i+j}$$

が成り立つ．

定理 4.1 (逆変換行列 Γ_Z)**.**
$g \times g$ の Z 上の行列 Γ_Z を

$$\Gamma_Z = (\rho_{t_i}(\bar{\eta_j} - d)/m))_{0\leqq i,j<g} (\in Z^{g\times g}).$$

としたとき $\bar{\Gamma}_Z^T \bar{\Omega}_Z = I$ となる． Ω_Z は対称なので $\Gamma_Z \Omega_Z = \Gamma_Z \Omega_Z = I$ である．

補題 4.1.
任意の $\vec{b} = \Omega_Z \vec{a}$ に対して以下の式が成立する．

$$\vec{a} = \Gamma_Z \vec{b} = 1/m(\bar{\Omega}_Z \vec{b} - d(\textstyle\sum_j b_j) \cdot \vec{1}).$$

ここで r を正の整数として $q = p^r (p : \text{素数})$ とする．また $\mathfrak{q} = \mathfrak{q}_0$ を素イデアル分解 $qR_Z = \mathfrak{q}_0 \cdots \mathfrak{q}_{g-1}$ に現れる最初のイデアルとする．このとき $R_Z/\mathfrak{q} \simeq \mathbb{Z}_q$ であることを考慮すると,

$$\Omega_Z^{(q)} \stackrel{\mathrm{def}}{=} \Omega_Z \ mod\ \mathfrak{q}\ (\in (R_Z)_{\mathfrak{q}}^{g\times g} \simeq \mathbb{Z}_q^{g\times g}).$$

定義 4.5 (ξ-基底)**.**

ξ-基底 $\vec{\xi} = (\xi_0, \cdots, \xi_{g-1}) \in (R_Z)_{\mathfrak{q}}^{(q)}$ は以下のように定義される.

$$\vec{\eta}^T \equiv \vec{\xi}^T \Omega_Z^{(q)} (mod\ \mathfrak{q}).$$

ξ-基底は $(R_Z)_{\mathfrak{q}}$ の $\mathbb{Z}_q$ 上の基底である. 任意の $a \in (R_Z)_{\mathfrak{q}}$ に対して, $a = \vec{\xi}^T \vec{b}$ を満たす $\vec{b} \in \mathbb{Z}_q^g$ が一意的に存在する. この $\vec{b} \in \mathbb{Z}_q^g$ を b の ξ-*vector* と呼ぶ.

補題 4.2.
任意の要素 $a \in R_Z$ は以下の 2 つを満たす.

- $a = \vec{\eta^T} \cdot \vec{a} \Leftrightarrow \sigma_Z(a) = \Omega_Z \vec{a}$,
- $a \equiv \vec{\xi^T} \cdot \vec{b} \Leftrightarrow \sigma_Z(a) \equiv \vec{b} (mod\ \mathfrak{q})$.

補題 4.3.
$a_1 = \vec{\xi^T} \cdot \vec{b_1}, a_2 = \vec{\xi^T} \cdot \vec{b_2}$ ならそのとき $a_1 a_2 = \vec{\xi^T} \cdot (\vec{b_1} \odot \vec{b_2})$($\odot$: 各成分ごとの積).
このことから ξ-基底で扱うと $(R_Z)_{\mathfrak{q}}$ の元同士の乗算が成分ごとの積になるから, η-基底で乗算をするよりも ξ-基底で乗算をするほうが速く計算できる.

4.1.2 $\Omega_Z^{(q)}$ の導出

行列 $\Omega_Z^{(q)}$ は $i+1$ 行は i 行を左に 1 つシフトしたものなので,1 行目を計算すれば後の行は 1 つ上の行を左に 1 つシフトさせていくだけでよく、2 行目以降は求める必要がない.

4.1.3 $\vec{b} = \Omega_Z^{(q)} \cdot \vec{a}$ の計算

$\Omega_Z^{(q)}$ の定義より,$\vec{b} = \Omega_Z^{(q)} \cdot \vec{a}$ の j 番目の要素 b_j は $b_j = \sum_{i=0}^{g-1} a_i \eta_{i+j}$ で表される. これはつまり $\vec{b}$ は $\vec{\eta} = (\eta_i)_{i=0}^{g-1}$ が $\Omega_Z^{(q)}$ の第 1 行目という条件下で, ベクトル $\vec{\eta}$ と $\vec{a} = (a_0, a_{g-1}, a_{g-2}, \cdots, a_1)$ の畳み込み積ということである.

ここで $\mathbb{Z}_q$ 上で以下の 2 つの多項式を定義する:

$$f(X) = \eta_0 + \eta_1 X + \cdots + \eta_{g-1} X^{g-1},$$
$$g(X) = a_0 + a_{g-1} X + \cdots + a_1 X^{g-1}.$$

$\vec{b}$ は $\vec{\eta}$ と $\vec{a}$ の畳み込み積だから

$$f(X)g(X) = b_0 + b_1 X + \cdots + b_{g-1} X^{g-1}\ (mod\ X^g - 1).$$

で表される.

4.1.4 η-*vector* と ξ-*vector* を用いた R_Z 上での演算手法

二つの $(R_Z)_{\mathfrak{q}}$ の元 $a = \vec{\eta}^T \cdot \vec{a}$ と $b = \vec{\eta}^T \cdot \vec{b}$ の乗法を考える. まず, 2 つの η-*vector* $\vec{a}, \vec{b}$ を対応する ξ-*vector* に変換すると,ξ-*vector* 上で要素ごとの乗算ができ, その結果を η-*vector* $(mod\ q)$ に変換する. 以下で詳しく説明する.

mult_eta $(\vec{a}, \vec{b}, q)$:
$\vec{\alpha} = \text{eta\_to\_xi}(\vec{\alpha}, q), \vec{\beta} = \text{eta\_to\_xi}(\vec{b}, q)$,
For $i = 0, \cdots, g-1, \gamma_i = \alpha_i \beta_i\ mod\ q$,
return $\vec{c} = \text{xi\_to\_eta}(\vec{\gamma}, q)$.
関数 eta_to_xi と xi_to_eta は事前に計算できる $\Omega_Z^{(q)}$ と補題 4.1 と補題 4.3 も用いた.

eta_to_xi$(\vec{a}, q)$:
$a(X) = a_0 + a_{g-1} X + \cdots + a_1 X^{g-1}$,
$c(X) = \eta_0 + \eta_1 X + \cdots + \eta_{g-1} X^{g-1}$,
$/((\eta_i)_{i=0}^{g-1}$ は $\Omega_Z^{(q)}$ の第 1 行目である.)
return $\vec{b} = (b_0, \cdots, b_{g-1})$.

xi_to_eta$(\vec{b}, q)$:
$b(X) = b_0 + b_{g-1} X + \cdots + b_1 X^{g-1}$,
$c(X) = \bar{\eta}_0 + \bar{\eta}_1 X + \cdots + \bar{\eta}_{g-1} X^{g-1}$,
$/((\bar{\eta}_i)_{i=0}^{g-1}$ は $\bar{\Omega}_Z^{(q)}$ の第 1 行目である.)
$a(X) = b(X)c(X)\ mod\ (q, X^g - 1)$,
$t = b_0 + \cdots + b_{g-1}\ mod\ q$,
return $\vec{a} = (m^{-1}(a_i - dt)\ mod\ q)_{i=0}^{g-1}$.

5. 提案手法とその結果

上記で説明した有田らの Ring-LWE に適した基底の構成方法は，円分体の部分体のうち，分解体に限定していたが，本研究では，その他の部分体についても η-基底と ξ-基底に対応する基底の構成について考える.

円分体 K, m, q を第 4 節と同様とする. ただし，q は素数冪ではなく素数とする. 部分体 $M \subset K$ について，対応する $(\mathbb{Z}/m\mathbb{Z})^*$ の部分群を H とし，その位数を d_H とする. このとき，詳しい証明は割愛するが第 4 節で定義した Ω_Z や Γ_Z は M についても同様に定義でき，また補題は d を d_H に置き換えても成り立つ. よって，M についても Ring-LWE に適していると期待できる η-基底と ξ-基底に対応する基底の構成は可能である. また，基底間の変換も同様である.

5.1 実験内容

m-th 円分体 $K = \mathbb{Q}(\zeta_m)$ の部分体 M で実験を行う. m が素数なので $(\mathbb{Z}/m\mathbb{Z})^*$ は巡回群となる. よって，M の $\mathbb{Q}$ 上の拡大次数 g から部分群 H は一意的に決定できる. 実験では何も変換を行わず η-基底同士で乗算計算した場合と，η-基底から ξ-基底に変換して乗算計算を行い，その結果を η-基底に戻す場合の時間を測定した.

5.2 実験環境

ここでは本実験で用いた環境を示す.

- Intel(R) Xeon(R) CPU E5-16080v3 @3.20GHz 3.20GHz
- RAM:32.0GB
- 使用した言語:プログラミング言語 magma
- OS:Ubunts 16.04.6 LTS

5.3 実験結果

100 回それぞれの場合について乗算時間 (秒) を測定し，その平均を計算した．それぞれの結果を表 1 に示す．

表 1 実験結果

	η-基底のみでの平均時間 (秒)	提案手法での平均時間 (秒)
$m = 2063$ $q = 12379, g = 1031$	0.55	0.029
$m = 10267$ $q = 10091, g = 1711$	0.0501	0.073
$m = 2081$ $q = 12487, g = 1040$	0.57	0.030
$m = 103049$ $q = 12907, g = 1171$	3.905	0.036

実験結果から提案手法の方が η-基底のみの場合よりも高速に演算が行えていることが分かる．

6. まとめ

様々な代数体上で効率的な Ring-LWE ベースの耐量子暗号プロトコルを構成することを目指す場合，代数体の整数環と素数により得られる有限体上のベクトル空間における乗算演算が高速に行えることを示さなければならない．本研究では，高速乗算が可能な上記ベクトル空間の基底について検討し，その結果，素数 m に対して m-th 円分体の部分体上で高速乗算が可能と期待できる基底の組を構成した．また，その基底の組について基底変換を利用した乗算 (提案手法) と基底変換を利用しない乗算とで計算時間を比較し，基底変換を利用した方が高速に乗算可能であるという結果を得た．

今後の課題としては，素数冪 m について m-th 円分体について Ring-LWE に適した基底の組の構成を検討することが挙げられる．(そのような基底の組が構成できれば，テンソル積を利用することで任意の円分体の部分体上で，Ring-LWE に適した基底が構成可能であると考えられる．) また，有田らの方法以外の既定の組の構成方法の検討や円分体の部分体ではない代数体についても，Ring-LWE に適した基底の組を構成することを検討していく．さらに，効率性のみならず様々な代数体上の Ring-LWE ベースの暗号プロトコルの安全性についても検討する．

謝辞 本研究の一部は，科学技術振興機構（JST）の CREST(JPMJCR1404) 及び文部科学省「Society5.0 に対応した高度技術人材育成事業成長分野を支える情報技術人材の育成拠点の形成 (enPiT)」，さらに文部科学省の平成 30 年度「Society 5.0 実現化研究拠点支援事業」の助成を受けています．

参考文献

[1] National institute of standards and technology (nist), ”post-quantum cryptography standardization”, available at. https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization.

[2] Seiko Arita and Sari Handa. Subring homomorphic encryption. In Howon Kim and Dong-Chan Kim, editors, *Information Security and Cryptology – ICISC 2017*, pages 112–136, Cham, 2018. Springer International Publishing.

[3] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, pages 1–23, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[4] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-lwe cryptography. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, pages 35–54, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[5] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag Berlin Heidelberg, 1999.

[6] Jheyne Nayara Ortiz, Ricardo Dahab, and Diego de Freitas Aranha. Non-cyclotomic number fields for lattice-based cryptography, 2018. https://www.ic.unicamp.br/~ra153618/phd/eqe-jnortiz.pdf.

[7] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.

[8] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 124–134. IEEE Computer Society, 1994.