From Learning with Errors (LWE) problem to CLWE problem

Jiankai Zhao

Faculty of Computational Mathematics and Cybernetics, Shenzhen MSU-BIT University, Shenzhen, China, 518172

243791757@qq.com

Abstract. The main purpose of this paper is to introduce the learning with errors problem on cyclic algebras, i.e., the CLWE problem, and to fully discuss and utilize the well-proven LWE-related conclusions and assumptions in cryptography theory. Firstly, this paper provides the basic framework of Learning with Errors (LWE) problems for cyclic algebra samples. Then lattices generated by the two-sided ideal of cyclic algebra with natural order are applied to cryptography. Based on the above contents, the so-called CLWE problem is introduced to point out the dimensions and structures suitable for constructing cryptographic systems for explicit algebra, and the security of corroding problems is discussed in the CLWE samples. Finally, this paper also discusses some possible future research directions, some natural routes to further research the construction and application of CLWE problems, for example, how to choose parameters for a specific security level, so as to offer some references for future study.

Keywords: Learning with Errors(LWE), cyclic algebra, CLWE, lattice problem

1. Introduction

Advances in quantum computer technology threaten the structure of most existing ciphers. In this context, cryptography based on lattice has slowly become an effectively secure cryptography theory. The so-called Learning with Errors (LWE) problem has been determined that it can be widely used as the basic theory for chosen-ciphertext attack [1-3] (It's worth pointing out that lattice-based cryptography has some attractive characteristics: for example, the best attack in terms of security requires exponential $2^{(n)}$time spent in the security parameter *n*, even for quantum attacks. In terms of efficiency and algorithm implementation, lattice-based encryption can be simple and parallelized) and secure public-key encryption under chosen-plaintext attack [4] (Lattice attack on the LWE problem combining reduction with an enumeration admitting a time or success tradeoff), fully homomorphic encryption [5-7] (The FHE method can significantly improve performance and base security on weaker assumptions), encryption based on identity [8], and so more. Cryptography based on lattice has been greatly aided by the use of the short integer solution introduced by literature *Generating hard instances of lattice problems* [9] and the learning with errors problem by the paper *On lattices, learning with errors, random linear codes, and cryptography* [10]. The practical hardness of LWE problems against attacks isn't settled issue, which means hard to assess the efficiency and security of plans. And then the intention of this paper is to clarify further this theme by analyzing variants of

© 2023 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

known schemes and estimated security and their consequences of sizes. Now pay attention to the famous LWE problem.

Firstly, let $p(n) \leq poly(n)$be a prime number and there exists a equation list with some errors: $\langle a_1, s\rangle \approx \chi b1(\text{mod}\, p(n))\ \langle a_2, s\rangle \approx \chi\, b2(\text{mod} p(n)),\cdots$,where $s \in \mathbb{Z}_p^n, b_i \in \mathbb{Z}_p$, a a_i are chosen uniformly and independently from the sample space $\mathbb{Z}_p^n$. The error is a probability distribution $X\colon \mathbb{Z}_p \to \mathbb{R}^+$. And $(\forall i)\colon b_i = \langle a_i, s\rangle + e_i$ is satisfied, where arbitrary element $e_i \in \mathbb{Z}_p$ is chosen independently depending on probability distribution X. The problem to find elements from above equations by LWE problem can be called learning with error.

It is worth mentioning that, the first subexponential algorithm as a special case of this problem, given $X(0) = 1 - \varepsilon,\ X(1) = \varepsilon, p(n) = 2$ was obtained by Blum, Kalai, and Wasserman [11]. In addition, two other valuable variants over rings and modules are noted, which be called RLWE problem [12] and MLWE problem [13].

2. Basic theory

2.1. LWE Problems on Lattices

Advances in quantum computer technology threaten the structure of most existing ciphers. In this context, cryptography based on lattice has slowly become an effectively secure cryptography theory. The so-called LWE problem has been determined that it can be widely used as the basic theory for chosen-ciphertext attack [14-16] (It's worth pointing out that lattice-based cryptography has some attractive characteristics: for example, the best attack in terms of security requires exponential $2^{(n)}$ time spent in the security parameter n, even for quantum attacks. In terms of efficiency and algorithm implementation, lattice-based encryption can be simple and parallelized) and secure public-key encryption under chosen-plaintext attack [17] (Lattice attack on the LWE problem combining reduction with an enumeration admitting a time or success tradeoff), fully homomorphic encryption [6, 7, 9] (The FHE method can significantly improve performance and base security on weaker assumptions), encryption based on identity [8], and so more.

Cryptography based on lattice has been greatly aided by the use of the short integer solution introduced by Chris Peikert and Brent Waters [1] and the learning with errors problem by literature *An efficient and parallel gaussian sampler for lattices* [18]. The practical hardness of LWE problems against attacks isn't a settled issue, which means it hard to assess the efficiency and security of plans. And then the intention of this paper is to clarify further this theme by analyzing variants of known schemes and estimated security and their consequences of sizes. Now pay attention to the famous LWE problem.

Firstly, let $p(n) \leq poly(n)$be a prime number, and there exists an equation list with some errors: $\langle a_1, s\rangle \approx \chi b1(\text{mod}\, p(n))\ \langle a_2, s\rangle \approx \chi\, b2(\text{mod} p(n)),\cdots$, where $s \in \mathbb{Z}_p^n, b_i \in \mathbb{Z}_p,$ a a_i are chosen uniformly and independently from the sample space $\mathbb{Z}_p^n$. The error is a probability distribution$X\colon \mathbb{Z}_p \to \mathbb{R}^+$. And $(\forall i)\colon b_i = \langle a_i, s\rangle + e_i$ is satisfied,
where arbitrary element $e_i \in \mathbb{Z}_p$ is chosen independently depending on probability distribution X. The problem to find element s from above equations by LWE problem can be called learning with error.

It is worth mentioning that, the first subexponential algorithm as a special case of this problem, given $X(0) = 1 - \varepsilon,\ X(1) = \varepsilon, p(n) = 2$ was obtained by Blum, Kalai, and Wasserman [4]. In addition, two other valuable variants over rings and modules are noted, which be called RLWE problem [19] and MLWE problem [20].

2.2. Order

Now introduce some basic definitions and results of the maximal order and natural theory. Let Λ be a non-commutative ring, then point 3 different types of ideals of the ring Λ. A so-called left ideal I of the ring Λ is an Abelian subgroup of ring Λ. The situation about right ideal is symmetrical. Note that $(\forall_i \in)(\forall_r \in \Lambda): r_i \in I$. In fact, A so-called two-sided ideal of Λ is an Abelian subgroup closed under left and right scaling by the ring Λ. For two-sided ideals, the concept of fractional ideals was defined as shown:

Definition 1. Let I be an ideal. If relation $(\exists c \in K): cI = J$is satisfied for a two-sided ideal J, then I can be called a fractional ideal of Λ.

In what follows, the Definition 1 is always restricted to two-sided ideals. The prime ideals of an order Λ are defined as the maximal two-sided ideals. Then the inverse of an ideal $I \subset \Lambda$ can be defined as $I^{-1} = \{\alpha \in \mathcal{A} | I\alpha I \subset I\}$ (It's worth mentioning that $II^{-1} = I^{-1}I = \Lambda$ in the two-sided case).

Codifferent ideal for an order Λ is defined as $\Lambda^{\vee} = \{\alpha \in \mathcal{A} | (Tr(\alpha\Lambda) \subset \mathbb{Z})\}$, where operation Tr is the trace operation given by $Tr(\alpha) = Tr_{K/Q}$. Note that if a dual ideal and above codifferent ideal are fractional, it's better than they are full ideals satisfying $\Lambda^{\vee} I^{-1} = I^{\vee}$ for arbitrary ideal I.

The structure of two-sided ideals' natural order isn't as simple as for $\mathcal{O}_K$ or an any maximal order. The group of two-sided ideals in a maximal order is a free Abelian group generated by the prime ideals, then definitions of inverse ideals and coprime ideals can be clearly deduced [21].

Example 1. The ring of integers $\mathcal{O}_k$ over the number field K denotes a unique maximal order (It's worth to point that the maximal order isn't necessarily unique for cyclic algebra). Considering the natural order for the LWE problem, defined as $\Lambda = \bigoplus_{i=0}^{d-1} \mu^i \mathcal{O}_L$ is paid attention. Differently this order isn't necessarily maximal order of $\mathcal{O}_k$. (But that natural orders are also maximal will be pointed out later.) But it's worth mentioning that under multiplication γ lies in the ring $\mathcal{O}_k$.

2.3. *Cyclic Algebra*

Now the theory on cyclic algebra has been emphasized in the coding theory filed [22, 23], therefore based on some previous work, the LWE problem on cyclic algebra over noncommutative rings was considered.

Consider restating the LWE problem like Definition 2. For details of the definition expansions of above problems over number fields restriction or over modules restriction, see the associated papers *Cyclic division algebras: A tool for space--time coding* [19] and *Maximal orders*[20] respectively.

Definition 2. Let $\mathrm{n}, \mathrm{q} \in \mathbb{Z}^+$ and positive number $\alpha > 0$ be an error parameter. The unit ring $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ is defined for a sample $(a, b) \leftarrow A_{s,\alpha}$ obtained by an uniformly random vector $\alpha \in \mathbb{Z}_q^n$, a secret $\mathrm{s} \in \mathbb{Z}_q^n$, element $\mathrm{e} \leftarrow D_\alpha$. Then the equation $(a, b) = (a, \langle a, s \rangle / q + e mod \mathbb{Z})$ is outputted.

From above distribution this problem stem form two problem forms, so-called "search problem" and "decision problem". These "search problem" and "decision problem" both are underlied on above LWE distribution. The "search Learning with Errors" problem is to find the secret s from a sample set, where secret s is sampled uniformly and randomly from sample space $\mathbb{Z}_q^n$. But the "decision Leaning with Errors" problem on inputting a sample set on $\mathbb{Z}_q^n \times \mathbb{T}$ is for determining whether samples are taken from the set $A_{s,\alpha}$ for the secret s or are uniform.

In generally, this number of samples given in any of above problems need to be attended in the truthful case. In consideration of a probabilistic factor of these decision LWE problems, the merit of the algorithms that can solve the above problems is important and deserves attention, as the difference between a uniform distribution and the acceptable probability on samples from the LWE distribution $A_{s,\alpha}$.

Considering the work of this paper, it involves many cross-cutting areas: lattice-based cryptography theory, number theory, information theory, and so on. It is necessary to give some basic, necessary concepts. At first, the relevant definitions of cyclic algebra are given from the literature *On lattices, learning with errors, random linear codes, and cryptography* [10].

Definition 3. Assuming a number field with degree n denoted by K, the Galois expansion of above number field K with degree d denoted by L, where the Galois group of the Galois expansion over the number field K is cyclic group with degree d, relation $\langle\theta\rangle = Gal(L/K)$ was obtained. Then the cyclic algebra can be defined as shown:

$$L \oplus \mu L \oplus c^2 L \ldots \oplus \mu^{d-1} L = \left(\frac{K}{L}, \theta, \gamma\right) = \mathcal{A} \tag{1}$$

Where $\gamma \in K$ is non-zero element, μ belonging to cyclic algebra $\mathcal{A}$ is the auxiliary generating element of the cyclic algebra, which satisfies $(\forall\alpha \in L): \alpha\mu = \mu\theta(\alpha)$ and $\mu^d = \gamma$. The number d can be called by degree of above cyclic algebra $\mathcal{A}$. If $(\forall\alpha \in \mathcal{A})(\exists\alpha^{-1} \in \mathcal{A}): \alpha\alpha^{-1} = 1$, the algebra $\mathcal{A}$ is said to be a division algebra.

Due to the fact that θ determines the number filed K, then the number filed K is center of the cyclic algebra. It is common to replace $\gamma \in K$ by $\gamma \in \mathcal{O}_K$, which will be used in guaranteeing existence of some given subring (natural order). In general, the property about division can't use to any γ value.

If the elements of $\mathcal{A}$ are represented by a matrix 2.1, then matrix 2.1 can be shown to valid for computing multiplication in the cyclic algebra. It is natural to think that $\alpha \in \mathcal{A}$ as a vector with d dimension $V(\alpha)$ over L. Thus define a mapping $f: \mathcal{A} \to M_{d\times d}(L), \alpha = \alpha_0 + \mu\alpha_1 + \cdots + \mu^{d-1}\alpha_{d-1} \in \mathcal{A} \longmapsto f(\alpha)$, where $(\forall i): \alpha_i \in L$

$$f(\alpha) = \left\{\begin{matrix} \alpha_0\ \theta(\alpha_{d-1})\gamma\ \theta^2(\alpha_{d-2})\gamma \ldots\ \theta^{d-1}(\alpha_1)\gamma \\ \alpha_1\ \ \theta(\alpha_0)\quad \theta^2(\alpha_{d-1})\gamma \ldots\ \theta^{d-1}(\alpha_2)\gamma \\ \alpha_2\ \theta(\alpha_1)\qquad \theta^2(\alpha_0)\ \ \ldots\ \ \theta^{d-1}(\alpha_3)\gamma \\ . \\ . \\ . \\ \alpha_{d-1}\ \theta(\alpha_{d-2})\quad \theta^2(\alpha_{d-3}) \ldots\ \theta^{d-1}(\alpha_0) \end{matrix}\right. \tag{2}$$

The mapping 2.1 can be called a left regular representation, due to relation $(\forall\alpha,\beta \in \mathcal{A}): \left[f(\alpha)V(\beta) = V(\alpha\beta) \land \left(f(\alpha\beta) = f(\alpha)f(\beta)\right)\right]$. Then any $f(\alpha)$ matrix is invertible when A is a division algebra. Considering on $L_{\mathbb{R}}$ the θ is well-defined, the mapping to $f: \oplus_{i=0}^{d-1}\mu L_{\mathbb{R}} \to M_{d\times d}(L_{\mathbb{R}})$ is extended. By vectorizing the images of subrings of an algebra under mapping f, lattices are obtained.

2.4. Division Algebra

Given a division algebra $\mathcal{D}$, whose center $C(\mathcal{D})$ is the set $C(\mathcal{D}) = \{x \in \mathcal{D} | (\forall d \in \mathcal{D})(xd = dx)\}$, it's easy to see that $C(\mathcal{D})$ is a field and $\mathcal{D}$ has a structure as a vector space over the set $C(\mathcal{D})$. And in this paper only division algebras are considered, which have finite dimension as a vector space over the center.

Definition 4. Given a field K, $\mathcal{D}$ whose center is precisely K can be called a division algebra $\mathcal{D}$ over the filed K. In virtue of the dimension $[\mathcal{D}: \mathrm{K}]$ that's always a perfect square, if there is $[\mathcal{D}: \mathrm{K}] = n^2$, thus the square root n of the dimension is called the degree of above division algebra $\mathcal{D}$.

Given a division algebra $\mathcal{D}$ over the field K and a field F satisfying $\mathrm{K} \subset \mathrm{F} \subset \mathrm{D}$, F is a subspace of the K-vector space over division algebra $\mathcal{D}$, if the field F is a subfield of division algebra $\mathcal{D}$ and $[F: K]$ can divide $[\mathcal{D}: K] = n^2$ (If the field F is a subfield of the division algebra $\mathcal{D}$, the maximum value of $[F: K]$ is n obviously, and the subfield F can be called by a maximal subfield of the division algebra $\mathcal{D}$). More details on division algebra can be found in the literature *On ideal lattices and learning with errors over rings* [12].

2.5. Cyclic Division Algebra and Non-norm Condition

Definition 5. Presume a cyclic division algebra $(L/K,\theta,\gamma)=\mathcal{A}$ and let a certain integer order Λ in algebra $\mathcal{A}$ be a finitely generated $\mathbb{Z}$-module satisfying $\Lambda\mathbb{Q}=\mathcal{A}$, where apparently Λ is a subring of cyclic division algebra $\mathcal{A}$ holding the equal identity element with the algebra $\mathcal{A}$. order Λ is called by maximal order, if no integer order Γ satisfying $\Lambda\subsetneq\Gamma\subsetneq\mathcal{A}$, where $\Lambda\mathbb{Q}=\{\sum\alpha_i k_i|(\alpha_i\in\Lambda)(k_i\in\mathbb{Q})\}$.

This paper just consider deal with cases under $\mathbb{Z}$-orders, thus refer to them as orders. However, the existence of a well-structured cyclic division algebra or order isn't obvious. The existence of γ in the condition provides the main point for constructing such objects. The literature [24] states that γ only needs to satisfy a specific non-norm condition, as shown by following:

Lemma 1. Let L/K denote a cyclic extension of number fields and $\langle\sigma\rangle=Gal(L/K)$ be cyclic with the order n. Let the parameter $\gamma\in K^*$ be any element of the smaller number field. Considering a set E satisfying γ^t belongs to the norm group $N_{L/K}(L^*)$, the set E is an Abelian subgroup of $\mathbb{Z}$ and holds relation $E=c\mathbb{Z}$ where c is a factor of n.

Proof. Let $h:\mathbb{Z}\to K^*$ be the homomorphic mapping from the Abelian group containing integers to the group, K^* which is obtained in the formula $\gamma^t=f(t)$. As a result, the set $E=f^{-1}\left(N_{L/K}(L^*)\right)$ is a demanding subgroup of $(\mathbb{Z})$. From knowledge of group theory there exists a unique non-negative integer k satisfying relation $\mathrm{E}=k\mathbb{Z}$, mainly because of relations $N_{L/K}(\gamma)=\gamma^n, n\in E$. Therefore, number n is divided by the generator k of the set E.

Proposition 1. A cyclic algebra $(L/K,\sigma,\gamma)=\mathcal{A}$ with degree n is a cyclic division algebra when and only when n is the smallest factor $\mathrm{t}\in\mathbb{Z}^+$ of n satisfying γ^t is the norm of L^*.

Proof. Let $\mathrm{t}(0<t<n)$ be some integers satisfying exponent γ^t is a norm. Using above Lemma 1 the smallest factor t is a factor of n, hence it can use factors of n instead of integers up to $n-1$. Thus this proposition was proved.

Proposition 2. A cyclic algebra $(L/K,\sigma,\gamma)=\mathcal{A}$ with degree n is a cyclic division algebra when and only when for arbitrary prime divisor p of n, the $\gamma^{\frac{n}{p}}$ isn't the norm of L^*.

Proof. Forms of some integer multiple of t is like fractional forms $\frac{n}{p}$ for some prime factor p of n, if exponent γ^t is a norm for divisor t of n. Let $kt=\frac{n}{p}, k\in\mathbb{Z}^+$, hence it can valid the exponents of this form above. There would be $\gamma^{\frac{n}{p}}=\gamma^{kt}=(\gamma^t)^k$, if γ^t were a norm. The proposition was proved.

The above lemma 1 and propositions 1 and 2 can be rewritten as the following proposition 3, i.e., the non-norm condition as mentioned above.

Proposition 3. (Non-norm condition): A cyclic algebra $(L/K,\sigma,\gamma)=\mathcal{A}$ with degree n is a cyclic division algebra when and only when there not is element of $\gamma^t, 1\le t\le n-1$, occurring in $H_{L/K}(L)$ where $H_{L/K}$ means a norm of L into K.

A simple example of cyclic division algebra is given below:

Example 2. The so-called Hamilton's quaternion is the four-dimensional vector space over the real field $\mathbb{R}$ with basis system $\{1,\hat{\imath},\hat{\jmath},\hat{k}\}$, which satisfies $\hat{\imath}^2=\hat{\jmath}^2=-1$ and $\hat{\imath}\hat{\jmath}=-\hat{\imath}\hat{\jmath}=k$. Obviously, the center of the Hamilton's quaternion H can be denoted by $\{a\cdot 1+0\cdot\hat{\imath}+0\cdot\hat{\jmath}+0\cdot\hat{k}\}$, thus the center is $\mathbb{R}$. Because the dimension of Hamilton's quaternion H is 4=22 over center $\mathbb{R}$, the degree of H is 2.

Consider that the subset $\{a\cdot 1+0\cdot\hat{\imath}+c\cdot\hat{\jmath}+0\cdot\hat{k}|(a,c\in\mathbb{R})\}$ is an isomorphic to complex field $\mathbb{C}$. It's known that the dimension of complex filed $\mathbb{C}$ is 2 over the center real field $\mathbb{R}$, thus complex field $\mathbb{C}$ is a maximal subfield of the Hamilton's quaternion H. Then $\mathbb{C}/\mathbb{R}$ is a Galois extension, whose Galois group is $\{1,\omega\}$, where ω denotes complex conjugation. Hence Hamilton's quaternion H is a cyclic division algebra.

Consider that the natural order $\Lambda$of algebra $\mathcal{A}$ is also a maximal order. Using the natural order, it's simple to construct and represent, and computing a maximal order is slow. The natural order is orthogonal in some places, thus considering the MLWE problem, it's better.

Example 3. Hamilton's quaternion over $\mathbb{Q}$ is defined by $\left\{a \cdot 1 + 0 \cdot \hat{\imath} + c \cdot \hat{\jmath} + 0 \cdot \hat{k} \middle| (a, c \in \mathbb{R})\right\}$ with relations a $\hat{\imath}^2 = \hat{\jmath}^2 = -1$ and $-\hat{\jmath}\hat{\imath} = \hat{\jmath}\hat{\imath}$. A quaternion can be represented by a matrix: $\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$

Thus, a cyclic division algebra $\left(\mathbb{Q}(\hat{\imath})/\mathbb{Q}, \overline{(\cdot)}, -1\right)$ is given, where -1 is a non-norm element and operation $\overline{(\cdot)}$ is the complex conjugate. The Lipschitz integers $L \subset H$form the non-maximal natural order L $= \{a + c\hat{\jmath} | (a, c \in \mathbb{Z}[\hat{\imath}])\}$. The maximal Hurwitz order is given by formula 2.2.

$$\mathrm{H} = \left\{a + b \cdot \hat{\imath} + c \cdot \hat{\jmath} + \frac{1}{2} d \cdot (-1 + \hat{\imath} + \hat{\jmath} + \hat{\imath}\hat{\jmath}) \middle| (a, b, c, d \in \mathbb{Z})\right\} \tag{3}$$

The dimension of $\mathbb{Z}$ is 4 and the degree of this order is 2. The Lipschitz order is a sublattice of the Hurwitz order.

The following are the three computational problems on ideal lattices that this paper mainly deals with, which seem to be difficult. These problems can be restricted to integral ideals in $\mathcal{O}_k$ because if ideal I is fractional with $g \in \mathcal{O}_k$ satisfying $gI \in \mathcal{O}_k$ is integral, the scaled ideal $N(g)I \subset \mathcal{O}_k$ as result of $N(g) \in \langle g \rangle$.

Definition 6. Shortest Vector Problem (SVP): Let operation $\|\cdot\|$ be a norm on $\mathbb{R}^n$. Let approximate factor $\xi \geq 1$ and L be a lattice, thus the approximate SVP on L means to discover a non-zero vector x satisfying relation $\xi\lambda_1(\mathcal{L}) \geq \|x\|$.

Definition 7. Shortest Independent Vectors Problem (SIVP): Let operation $\|\cdot\|$ be a norm on $\mathbb{R}^n$. Let approximate factor $\xi \geq 1$ and L be a lattice, thus the approximate SIVP on L means to discover n linearly independent non-zero vectors $x_1, \cdots, x_n$ satisfying relation $\xi\lambda_n(L) \geq \max_i(|x_i|)$.

Definition 8. Bounded Distance Decoding problem (BDD problem) Let operation $\|\cdot\|$ be a norm on $\mathbb{R}^n$. Let approximate facto $\xi \geq 1$ and L be a lattice, and there is relation $\mathrm{d} < 1/2\lambda_1(\mathcal{L})$. Thus, the BBD problem on inputting $y = x + z$ for vector $x \in \mathrm{L}$, where $\|z\| \leq d$ means to compute x (Of course or equivalently to compute z).

These lattice problems have been studied by previous researchers to be considered sufficiently difficult to be used as a basic theory for quantum cryptographic security. No current algorithms for polynomial-time runs in dimension n for any of them. And similar problems on lattices and ideals are shown by the following:

Definition 9. Let algebra $\mathcal{A}$ be a cyclic algebra. The $\mathcal{A} - SVP$ means to discover a nonzero element a belonging to an ideal I with the natural order Λ and satisfying $\xi\lambda_1(I) \geq \|\sigma_{\mathcal{A}}(a)\|_2 = |a|$, where approximate facto $\xi \geq 1$ and $\lambda_1(I)$ represents the minimal length of nonzero elements of ideal I in given norm.

Note that the solution of above $\mathcal{A} - SVP$ on the fractional ideal I can be given on integral ideal gI, where $g \in \mathrm{K}$ satisfying gI is integral. Thus, without loss of generality, when considering problems in security reductions, one can actually presume that above ideal is integral. There is an analogous about extension of SIVP.

Definition 10. Let algebra $\mathcal{A}$ be a cyclic algebra and $\lambda_1\left(\frac{I}{2}\right) > \delta$, where I is an ideal with a maximal $\mathbb{Z}$ -order Λ. Hence the $\mathcal{A} - BBD$ problem on inputting $y = x + z$, where $x \in I, z \in \bigoplus_{i=0}^{d-1} \mu^i L_{\mathbb{R}}$ and to compute x *satisfying* $|z| \leq \delta$.

3. CLWE Problems

3.1. Basic Definitions

The following is the definition of the LWE problem on cyclic algebras. Later such problems will be named CLWE problems, and two variants of these problems are indicated [10].

Definition 11. CLWE problem: Let a Galois extension of number fields be denoted by L/K, which satisfy relations $d = [L: K]$ and $n = [K: \mathbb{Q}]$. And let an algebra $(L/K, \theta, \gamma) = \mathcal{A}$ be the obtained cyclic algebra with the center K and μ satisfying $\gamma = \mu^d \in \mathcal{O}_k$, an order of the cyclic algebra Λ and cyclic Galois group generated by θ. A sample from the CLWE distribution $\prod_{q,s,\sum}$ is given by sampling $\alpha \leftarrow \Lambda_q$ randomly and uniformly and $e \leftarrow \sum$, where $q \geq 2$, distribution $\sum$ is an error distribution over $\oplus_{i=0}^{d-1} \mu^i L_{\mathbb{R}}$ and $s = \Lambda_q^{\vee}$ is a secret.

$$(a, b) = \left(a, \frac{as}{q} + emod\Lambda^{\vee}\right) \in \frac{\left(\Lambda_q, \oplus_{i=0}^{d-1} \mu^i L_{\mathbb{R}}\right)}{\Lambda^{\vee}} \tag{4}$$

If replace $(a \cdot s)$ with $(s \cdot a)$ in the definition, the security of the problem remains unchanged. Similar to LWE problem, two variants of CLWE problem are given, i. e., search problem and decision problem.

Definition 12. (Search CLWE problem) Let a family of error distributions over $\oplus_{i=0}^{d-1} \mu^i L_{\mathbb{R}}$ be denoted by $\sum_{\alpha}$.

CLWE problem can be defined as to discover element s from a set of independent samples from a CLWE distribution $\prod_{q,s,\sum}$ for any secret $s = \Lambda_q^{\vee}$ and $\sum \in \sum_{\alpha}$, where $q \geq 2$ is an integer modulus, $\sum$ is an error distribution over $\oplus_{i=0}^{d-1} \mu^i L_{\mathbb{R}}$.

Definition 13. (Decision CLWE problem) Let a family of error distributions over $\oplus_{i=0}^{d-1} \mu^i L_{\mathbb{R}}$ be denoted by $\sum_{\alpha}$ and $\Psi \in \sum_{\alpha}$. So-called decision CLWE problem can be defined as inputting a set of independent samples from CLWE distribution $\prod_{q,s,\sum}$

For any secret $s = \Lambda_q^{\vee}$ and $\sum \in \sum_{\alpha}$, where $q \geq 2$ is an integer modulus, $\sum$ is an error distribution over $\oplus_{i=0}^{d-1} \mu^i L_{\mathbb{R}}$, then decide which is the advantage case for a random choice from $(s, \sum) \leftarrow D(\Lambda_q^{\vee}) \times \Psi$ or from distribution D_{Λ}, where D_{Λ} is an uniform distribution over $\left(\Lambda_q, \left(\oplus_{i=0}^{d-1} \mu^i L_{\mathbb{R}}\right) / \Lambda^{\vee}\right)$.

3.2. Algebraic structure for CLWE Problems

For applying the assumption of CLWE in a cryptosystem families of algebras suiting for CLWE problem must be chosen, which allow for different security levels and asymptotic analysis. Cyclic division algebras are considered, which have the properties below:

- The non-norm parameter γ must exist in ring $\mathcal{O}_k$ to make the natural order be closed under multiplication operation, where parameter γ may have $(\forall i): |\sigma_i(\gamma)| = 1$ for maintaining sub-multiplicative properties of above norm and coordinate independence.
- The degree $d = [L: K]$ may be small enough. The dimension $n = [K: \mathbb{Q}]$ may be large enough. And q may split completely in the basic field K.

In CLWE problem parameter γ is selected such that $\mathcal{A}$ is a division algebra in order to avoiding attacks on the m-RLWE protocol pointed by literature [5].

The non-norm condition of γ excluded the existence of a homomorphism removing the module structure by taking a cyclic algebra $(L/K, \theta, \gamma) = \mathcal{A}$. Search of algebra $\mathcal{A}$ just needs to be restricted to maximal subfields, so by virtue of the proof from literature [10] attacks on the m-RLWE protocol pointed out by literature *Fully homomorphic encryption without bootstrapping* [5] can't defeat the above structure.

Cyclic division algebras satisfying various conditions have been obtained by experts in the field of coding theory who have spent a lot of effort to construct them, for example in the literature *Worst-case to average-case reductions for module lattices* [13]. In the following, the relevant theorems that are valuable in the literature are pointed out:

Theorem 1. Let the number $m = p^{\alpha}$ be a prime power and $\mathbb{Q}(\zeta_m) = K$ be the basic field. Thus there are infinitely many cyclic Galois extensions M/K with degree $p^{\alpha} = m$, satisfying

$\zeta_m^i(0 < i < m)$ isn't a norm belonging to M/K, where $\varphi(m) = n$ is the degree of the basic field $\mathbb{Q}(\zeta_m) = K$ and ζ_m is a mth primitive root of unity.

Firstly, consider find a prime number q' satisfying $q' \neq 1 mod\, p^{a+1}$ and $q' = 1 mod\, p^a$. Then let $K(\zeta_{q'}) = M'$, thus $K(\zeta_{mq'}) = M'$ by coprimality. Hence the Galois extension $Gal(M'/K)$ is a cyclic group with order $q' - 1$, generated by automorphism σ. Let M be the subfield belonging to M' fixed by mapping σ^m. Therefore $[M{:}\,K] = m$ can be obtained and the extension is cyclic and Galois in virtue of the Fundamental Theorem of Galois Theory, as from the Localization Theorem powers of ζ_m are not norms in the cyclic Galois extension.

Let a Galois field extension with non-norm $\gamma \in \mathcal{O}_{k'}$ be denoted by L'/K', whose Galois group is cyclic Galois group with degree d. Let a field F be another Galois field such that $L' \cap F = \mathbb{Q}$. Therefore $Gal(L'F/K'F)$ is congruent with $Gal(L'/K')$. Additionally, the element γ is non-norm in $L'F/K'F$.

In following that the extension is denoted by L/K newly. Let the cyclic generator of above Galois group be denoted by symbol θ, which offers a cyclic field extension with γ satisfying $d = [L{:}\,K]$and $[F{:}\,\mathbb{Q}][K'{:}\,\mathbb{Q}] = [K{:}\,\mathbb{Q}]$. This method may be extended to cases that the basic field may not be simply denoted by a compositum of two fields [10].

Then L'/K' can be assumed as a cyclic Galois extension with degree d and γ is non-norm. And Let the field K be another Galois field that holds the field K', hence extension KL'/K is cyclic Galois with degree k, where the number $k$can divide the number d. $K'L' \cap K \Longrightarrow (d = k)$, because these fields are linear independent on the field K'.

Theorem 2. Let $\mathbb{Q}(\zeta_n) = K$, where $n = p^r$ and number p is a prime number. And presume that a finite cyclic extension with degree d be denoted by L/K satisfying relations Gal(L/Q) is Abelian, $\langle\theta\rangle = Gal(L/K)$ and $\mathbb{Q}(\zeta_{q^t}) = F$, where $L \cap F = \mathbb{Q}$. Presume the natural order $\Lambda \subset \left(\frac{L}{K}, \theta, \zeta_n\right) = \mathcal{A}$ is maximal order. The natural order Λ' of the cyclic division algebra $(LF/KF, \theta', \zeta_n) = \mathcal{A}$ is maximal order, if number $[F{:}\,\mathbb{Q}]$ and degree d are coprime.

Details of the proof process of Theorem 2 can be found in the paper *On lattices, learning with errors, random linear codes, and cryptography* [10].

3.3. Hardness of CLWE Problems

3.3.1. Hardness of Search CLWE Problems. Let $\mathcal{A}$ be a cyclic division algebra over a given number field L with its center K and natural, maximal order Λ such that $(\forall \mathrm{i}){:}\, |\sigma_\mathrm{i}(\gamma)| = 1$. Then, let $\mathrm{q} \geq 2$, unramified in the number field L and $\alpha = \alpha(\mathrm{n}) \in (0; 1)$, which satisfies $\omega\left(\sqrt{\mathrm{logN}}\right) \leq \alpha\mathrm{q}$, where $\mathrm{N} = \mathrm{nd}^2$is the total dimension of the cyclic division algebra $\mathcal{A}$. Thus so-called $\mathcal{A} - \mathrm{DGS}_\xi$ problem can be denoted to sample a discrete Gaussian distribution $\mathrm{D}_{\mathrm{I},\xi}$, where ideal I is with the order Λ.

Definition 14. For arbitrary $q \geq 2$ so-called $q\mathcal{A} - BDD_{I,\delta}$ problem can be denoted as: given an $\mathcal{A} - BDD_{I,\delta}$ problem and the relation $y = x + z$, whose solution $x \in$ I and error $z \in \bigoplus_{i=0}^{d-1} \mu^i L_\mathbb{R}$, output x mod qI, where $\delta \geq \|e\|_{2,\infty}$.

Lemma 2. Let L be a lattice, $d < \frac{\lambda_1(L)}{2}$ and $q \geq 2$. Given an oracle for $CVP_{L,d}^{(q)}$ an algorithm solving $CVP_{L,d}$ exists.

Proof. Assume a point a and the distance d over the lattice L, A sequence constructed by points is defined as: $a = a_1, a_2, a_3, \cdots$. Then the coefficient vector of the closest lattice point to a_i is denoted by $\beta_i = L^{-1}K_L(a_i) \in \mathbb{Z}^n$. And let $\frac{1}{q}\left(a_i - L(\beta_i \bmod q)\right) = a_{i+1}$. Then $L(\beta_i - (\beta_i \bmod p)/q) \in L$ is the closest lattice point to a_{i+1}. Thus $\frac{1}{q}\left(\beta_i - (\beta_i \bmod q)\right) = \beta_{i+1}$, and notice that the distance of the point x_{i+1} is at most $\frac{d}{q^i}$. After n steps point a_{n+1} whose distance is at most $\frac{d}{q^i}$ was obtained [2]. This obtains a lattice point $L\beta$ with distance $2^n \frac{d}{q^i} \leq d < \frac{\lambda_1(L)}{2}$ of the point a_{n+1}. Thus, the point $L\beta$ is the lattice point that is closest to a_{n+1}. Using vector β_{n+1} and vector $\beta_n \bmod q$, by using the given oracle find $\beta_n = q\beta_{n+1} + (\beta_n \bmod p)$. Repeating the process, vectors $\beta_{n-1}, \beta_{n-2}, \cdots, \beta_1$ are obtained. Above algorithm since $L\beta_1$ gives the closest point to a_1.

Lemma 3. Given an instance y of the $q - BDD_{I^\vee,d}$ problem the reduction is defined as following:

- **STEP 1**: Find an element $g \in I$ satisfying $\langle q \rangle$ and gI^{-1} are coprime.
- **STEP 2**: Take a sample $h \leftarrow D_{I,r}$ from a Gaussian oracle for any sample requested by the lattice L. Give lattice L the pair $(a, b) \in R_q \times \mathbb{G}$, found by assuming $a = \theta_g^{-1}(h \bmod qI) \in R_q, e' \leftarrow D_{\alpha/\sqrt{2}}, b = (hy)/q + e' mod R^\vee$.
- **STEP 3**: If L generated a solution $t \in R_q^\vee$, then output $\theta_g^{-1}(t) \in I_q^\vee$.

Let y be an instance of $BDD_{I^\vee,d}$ problem with relation $y = x + z$, where x belongs to $I^\vee, d \geq |e|_\infty$. Then every pair (a, b) generated by this reduction can be depicted by distribution $A_{s,\Sigma}$, where $\sum \in \sum_\alpha$and $s = \theta_g(x \bmod qI^\vee) = gx \in R_q^\vee$.

It is worth mentioning that the validity of the reduction of the algorithm in lemma 3 is guaranteed by lemma 3.6 in the literature [18] and lemma 4.7 in the literature [19].

Lemma 4. For any $q \geq 2$ from $\mathcal{A} - BDD_{I,\delta}$ to $q\mathcal{A} - BDD_{I,\delta}$ there exist a deterministic polynomial time reduction. The lemma 4 is obtained by using the lemma 2 and the algorithm in the lemma 3.

Lemma 5. A algorithm running probabilistic polynomial time can be given as follows [10, 20]: input a parameter $r \geq \sqrt{2}q\eta(I)$, where $q \geq 2$ is a prime integer, a instance of $q\mathcal{A} - BDD_{I^\vee,\alpha q\omega(\sqrt{\log(nd)})/r\sqrt{2nd}}$ problem $y = x + z$, where $I^\vee \subset \Lambda$ is a fractional ideal, x belongs to $I^\vee$, and samples from the discrete Gaussian distribution $D_{I,r'}.$, where $r \leq r'$.

Output samples from distribution $\Pi_{q,s,\Sigma}$for a secret $s = f_g(x \bmod qI^\vee) \in \Lambda_q^\vee$, where $f_g: \mathcal{A} \to \mathcal{A}, f_g(x) = gx$ and distribution Σ is an error distribution. When $|\gamma| = 1$ the distribution of the resulting error e' is marginal, which is Gaussian distribution with the parameter $r_{i,j} \leq \alpha$.

Definition 15. The set constructed of all Gaussian distributions over the lattice $\bigoplus_{i=0}^{d-1} u^i L_\mathbb{R}$ whose marginal distribution is Gaussian distribution with the parameter $r_{i,j} \leq \alpha$ can be defined as the family of error distributions Σ_α.

Theorem 3. There is an oracle solving $CLWE_{q,\Sigma_\alpha}$ problem for inputting $\alpha \in (0;1)$, an ideal $I \subset \Lambda$, an integer $q \geq 2$, a parameter $r \geq \sqrt{2}q\eta_\varepsilon(I)$ with $\sqrt{2N}/\lambda_1(I^\vee) < r\omega((\sqrt{\log N})/(\alpha q) = r'$, and samples from the discrete Gaussian distribution $D_{I,r'}$. Then an algorithm on quantum outputting an independent sample from the discrete Gaussian distribution $D_{I,r'}$ was obtained.

Using the reduction process from Lemma 5, the quantum step from *An efficient and parallel gaussian sampler for lattices*[18], in the form of $\mathcal{A} - BDD_{I\delta}$ problem pointed by *Maximal orders* [20], which the offset is bounded in the norm $\|e\|_{2,\infty} \leq \delta$, theorem 3 was obtained.

Theorem 4. There exists quantum reduction process running in a polynomial time for arbitrary $\omega r\sqrt{d}(\sqrt{\log(dn)})/q\alpha = \xi$, where $\sqrt{2}q\eta_\varepsilon(I) < r$ from the $\mathcal{A} - DGS_\xi$ problem to the search $CLWE_{q,\Sigma_\alpha}$ problem.

Corollary 1. There exists quantum reduction process running in a polynomial time for arbitrary $\xi\sqrt{8Nd} = (\omega(\sqrt{dn})/\alpha)$ from the $\mathcal{A} - SIVP_\xi$ to the search $CLWE_{q,\Sigma_\alpha}$ problem.

3.3.2. Search CLWE Problems to Decision CLWE Problems. **Lemma 6.** Let $(\mathrm{L/K}, \theta, \gamma) = \mathcal{A}$ be a cyclic division algebra with a natural order Λ. And let I be an ideal of the ring $\mathcal{O}_\mathrm{K}$ splitting completely as $\mathrm{q_1 \cdots q_n = I}$ [25]. Thus, an isomorphism is obtained as shown:

$$\mathscr{R}_I \times \cdots \times \mathscr{R}_n \cong \frac{\Lambda}{I\Lambda} \tag{5}$$

where $R_i = \bigoplus_{i=0}^{d-1} \mu^i(\mathcal{O}_L/q_i\mathcal{O}_L)$ is the ring satisfying $u(\theta(\ell) + q_i\mathcal{O}_L) = u(\ell + q_i\mathcal{O}_L)$ and $\gamma + q_i = u^d$.

Definition 16. So-called $R_i - CLWE_{q,\Sigma_\alpha}$problem can be defined as discovering $s \bmod R_i$from CLWE distribution $\Pi_{q,s,\Sigma}$ for any distribution Σ belonging to Σ_α.

Consider use some automorphisms of K on rings R_i. Because automorphisms σ_i of K effect on ideals q_i, where K is a Galois extension of $\mathbb{Q}$. At first, these automorphisms are extended to automorphisms α_i of L by a specific method. Thus these automorphisms can be extended to isomorphisms $\alpha_i: \mathcal{A} \to \mathcal{A}' = (L/K, \theta, \gamma') = \mathcal{A}'$, agreeing with α_i on L and sending element u to new element u' satisfying $u'^d = \alpha_i(\gamma)$ and $(\forall x \in L): u'\theta(x) = xu'$.

From *Cyclic division algebras: A tool for space--time coding* [19], element $\alpha_i(\gamma)$ is non-norm, thus the algebra $\mathcal{A}'$ is a division algebra. The function α_i is an isomorphism sending the algebra $\mathcal{A}$ to the new algebra $\mathcal{A}'$. The extended isomorphism α_i sends the $R_i - CLWE_{q,\Sigma_\alpha}$ problem in the algebra $\mathcal{A}$ to identical problem in the new algebra $\mathcal{A}'$, because the error distribution family Σ_α is fixed.

Lemma 7. There exists a reduction process running in indeterministic polynomial time from the $CLWE_{q,\Sigma_\alpha}$ problem to the $R_i - CLWE_{q,\Sigma_\alpha}$ problem.

Proof. Firstly, an oracle for the $R_i - CLWE_{q,\Sigma_\alpha}$ problem can be denoted by $\mathcal{O}_i$. An isomorphism using the oracle $\mathcal{O}_i$ to work out $R_j - CLWE_{q,\Sigma_\alpha}$ problems for every number j is defined in virtue of Lemma 6. And $\alpha_{j/i}$ is an extension of the automorphism belonging to K sending q_j to q_i existing by transitivity.

Because Λ_q and $\Lambda_q^\vee$ are fixed by every $\alpha_{j/i}$, given the obtained pair the sample $(a, b) \leftarrow \Pi_{q,s,\Sigma}$ is a CLWE sample in algebra $(L/K, \theta, \alpha_{j/i}(\gamma)) = \mathcal{A}'$. Feeding samples into the oracle $\mathcal{O}_i$ output $t_j \bmod R_i$ and consider $\alpha_{j/i}^{-1}(t_j) \bmod R_j$. Every sample (a, b) is mapped to a CLWE sample $(\alpha_{j/i}(a), \alpha_{j/i}(\mathrm{a}s/q + e) \bmod \Lambda^\vee)$ in above algebra $\mathcal{A}'$, because $\alpha_{j/i}$ is an automorphism. Because these automorphisms inject the uniform distribution to uniform distribution and determine the family constructed of error distribution family Σ_α and, it's a CLWE instance with the error distribution Σ' belonging Σ_α and the secret $\alpha_{j/i}(s)$. Therefore discovering $s = \alpha_{j/i}^{-1}(t) \bmod R_j$, $t = \alpha_{j/i}(s) \bmod R_i$ is given by the oracle $\mathcal{O}_i$.

Definition 17. For a secret $s \in \Lambda_q^\vee$ and a distribution Σ over $\bigoplus_i \mu^i L_\mathbb{R} (i \in [n])$, a sample is defined by sampling $(a, b) \leftarrow \Pi_{q,s,\Sigma}$ and $h \in \Lambda_q^\vee$, which's independent and uniformly random mod $R_j (j \leq i)$ and 0 mod $R_j (j > i)$, from the distribution $\Pi_{q,s,\Sigma}^i$ over $\Lambda_q \times (\bigoplus_{i=0}^{d-1} \mu^i L_\mathbb{R})/\Lambda^\vee$ and outputting $(a, b + h/q)$.

Let $i = 0$, then $\Pi_{q,s,\Sigma} = \Pi_{q,s,\Sigma}^0$ is defined. The Hybrid LWE distribution is defined in [19], in following that a worst-case decision problem using the distribution relatives to R_i, reduced to search $R_i - CLWR$ problem.

Definition 18. The $W - D - CLWE_{q,\Sigma_\alpha}^i$ problem is defined as problems to find $j \in \{i - 1; i\}$ given access to $\Pi_{q,s,\Sigma}^j$ and to valid CLWE error distribution Σ belonging Σ_α and secret s.

Lemma 8. Let d be a constant and secret s. A reduction process running in probabilistic polynomial time from $R_i - CLWE_{q,s,\Sigma_\alpha}$ problem to $W - D - CLWE_{q,\Sigma_\alpha}^i$ problem for arbitrary $i \in [n]$ exists.

Proof. Consider that possible values of secret $s \bmod R_i$ bounded above by q^{d^2} and polynomial in n. Thus, the possible values can be enumerated. The transform is defined by mapping $\Pi_{q,s,\Sigma}$ to $\Pi_{q,s,\Sigma}^{i-1}$ and taking a value $g \in \Lambda_q^\vee$ (if $s \bmod R_i = g$ or $\Pi_{q,s,\Sigma}^i$). The pair can be outputted below by inputting a CLWE sample $(a, b) \leftarrow \Pi_{q,s,\Sigma}$:

$$\left(a + v, b + \frac{h + vg}{q}\right) \in \Lambda_q \times \frac{\left(\bigoplus_{i=0}^{d-1} \mu^i L_\mathbb{R}\right)}{\Lambda^\vee} = (a', b') \tag{6}$$

where element $h \in \Lambda_q^\vee$ is independent, uniformly random $R_j(j \geq i)$ and otherwise 0 mod $R_j(j < i)$. Element $v \in \Lambda_q$ is uniformly random mod R_i and otherwise 0 mod $R_j(j \neq i)$. Then for a fixed value of a'

$$\frac{a^{'}s + h + v(g-s)}{q} + e = \frac{as + h + vg}{q} + e = b + \frac{h + vg}{q} = b^{'} \tag{7}$$

where the element e is sampling from the distribution Σ belonging to Σ_α. If $g = s$ mod R_i thus $0 = (g-s)v$ mod R_i and the distribution of pair (a', b') is the distribution $\Pi_{q,s,\Sigma}^{i-1}$. Otherwise, $(g-s)v$ is uniformly random mod R_i by assumption and 0 mod $R_j(j \neq i)$. Thus let $v(g-s) + h = h'$ and $\Pi_{q,s,\Sigma}^{i}$ is the distribution of (a', b').

Removing the restriction, there are better framework of RLWE search-decision reduction.

Definition 19. The error distribution Υ_α on the error distribution family is sampled by choosing an error distribution Σ belonging to Σ_α and adding it to D_r, where arbitrary $r_i = \alpha\left((nd^2)^{\frac{1}{4}}\sqrt{y_i}\right)$ for $y_1, \cdots, y_{nd^2}$ is sampled from $\Gamma(2,1)$.

Definition 20. There is an algorithm solving the $D - CLWE_{q,\Upsilon_\alpha}^{i}$ problem for an error distribution Υ_α and $i \in [n]$. There is a non-negligible difference in acceptable probability on inputting from distributions $\Pi_{q,s,\Sigma}^{i}$ and $\Pi_{q,s,\Sigma}^{i-1}$, if it's with a non-negligible probability over pairs (s, Σ) from $U(\Lambda_q^\vee) \times \Upsilon_\alpha$.

The choice of error distribution should be randomized by sampling from error distributions Υ_α in some worst-case to the average-case reduction process.

Lemma 9. There exists a reduction process running in randomized polynomial time from $W - D - CLWE_{q,\Sigma_\alpha}^{i}$ problem to $D - CLWE_{q,\Upsilon_\alpha}^{i}$ problem for arbitrary $\alpha > 0$ and $i \in [n]$ [19].

This choice of distribution Υ_α shows that in decision problem the error covariance matrix is closer to diagonal matrix than that in corresponding search problem.

Lemma 10. Given a secret $s \in \Lambda_q^\vee$and an oracle $\mathcal{O}_i$ solving the $D - CLWE_{q,\Upsilon_\alpha}$ problem, there is an valid algorithm solving $D - CLWE_{q,\Upsilon_\alpha}$ problem for $i \in [n]$ using the oracle $\mathcal{O}$ [26].

The search CLWE problem can be denoted by the $CLWE_{q,\Sigma_\alpha,G}$, where element $s \in G$ for any fixed $G \subset \Lambda_q^\vee$. Overall, the main theorem was obtained:

Theorem 5. Let order Λ be the natural order of a cyclic algebra $(L/K, \theta, \gamma) = \mathcal{A}$, d be constant and $q \in poly(n)$. Then let $\eta_\varepsilon(\Lambda^\vee)$for a negligible $\varepsilon = \varepsilon(n)$. Thus, there is a probabilistic reduction from the $CLWE_{q,\Sigma_\alpha,G}$ problem for arbitrary pairwise different $G \subset \Lambda_q^\vee$ to the $D - CLWE_{q,\Upsilon_\alpha}$ problem spending in time polynomial in n.

4. Conclusion

In recent research, the most important problem to be solved about the CLWE problem may be whether the search problem and the decision problem are equivalent in polynomial time, or whether the difficulty of the decision problem can be directly based on the lattice problem through other methods. It is worth mentioning that the effectiveness of the technique of decision problem difficulty depends on the modulus q. If CLWE is not considered, the method for the difficulty of the decision RLWE problem gives a more general security proof of the decision problem, which is suitable for a wider range of cyclic division algebras. Abandoning some restrictions to expand the possibility of cyclic algebras that support the difficulty of decision problems can provide a larger framework for CLWE-based cryptography [23].

There are some natural routes to further research the construction and application of CLWE problems. Some obvious directions are how to choose parameters for a specific security level, such as NewHope's RLWE scheme and Kyber's MLWE scheme for NIST processes [11]. The formal representation is required to select K, L, γ matrix representation, error distribution, error correction code, and actual security measures. Only after the parameterization scheme is proposed can the actual efficiency of CLWE be compared with the existing LWE structure.

It may also consider whether some restrictions on γ can continue to be canceled. However, according to the previous discussion, it's unlikely to give up the limitation that γ is a non-norm element under the premise of security. In addition, in the paper *Construction of multiblock space--time codes from division algebras with roots of unity as nonnorm elements* [27], the researchers introduced the concept of the coefficient ring, which is also a relatively new and possibly applicable structure.

References

[1] Chris Peikert and Brent Waters. (2008) Lossy trapdoor functions and their applications. In Proceedings of the fortieth annual ACM symposium on Theory of computing, pp. 187-196.

[2] Chris Peikert. (2009) Public-key cryptosystems from the worst-case shortest vector problem. In Proceedings of the forty-first annual ACM symposium on Theory of computing, pp. 333-342.

[3] Daniele Micciancio and Chris Peikert. (2012) Trapdoors for lattices: Simpler, tighter, faster, smaller. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp. 700-718.

[4] Richard Lindner and Chris Peikert. (2011) Better key sizes (and attacks) for lwe-based encryption. In Cryptographers' Track at the RSA Conference, Springer, pp. 319-339.

[5] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (2014) (leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory (TOCT), 6(3):1-36.

[6] Craig Gentry. (2009) Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing, pp. 169-178.

[7] Zvika Brakerski and Vinod Vaikuntanathan. (2012) Efficient fully homomorphic encryption from (standard) LWE. SIAM Journal on computing, 43(2):831-871.

[8] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. (2012) Bonsai trees, or how to delegate a lattice basis. Journal of cryptology, 25(4):601-639.

[9] Miklós Ajtai. (1996) Generating hard instances of lattice problems. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 99-108.

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

[11] Avrim Blum, Adam Kalai, and Hal Wasserman. (2003) Noise-tolerant learning, the parity problem, and the statistical query model. Journal of the ACM (JACM), 50(4):506-519.

[12] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. (2013) On ideal lattices and learning with errors over rings. Journal of the ACM (JACM), 60(6):1-35.

[13] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography, 75(3):565- 599, 2015.

[14] Gilbert Baumslag, Nelly Fazio, Antonio R Nicolosi, Vladimir Shpilrain, and William E Skeith. (2011) Generalized learning problems and applications to non-commutative cryptography. In International Conference on Provable Security, Springer, pp.324-339.

[15] Roope Vehkalahti, Camilla Hollanti, Jyrki Lahtonen, and Kalle Ranto. (2009) On the densest mimolattices from cyclic division algebras. IEEE Transactions on Information Theory, 55(8):3751-3780.

[16] Frederique Oggier and BA Sethuraman. (2012) Quotients of orders in cyclic algebras and space-time codes. arXiv preprint arXiv:1210.7044.

[17] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. (2017) Pseudorandomness of ring-lwe for any ring and modulus. In Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, pp. 461-473.

[18] Chris Peikert. (2010) An efficient and parallel gaussian sampler for lattices. In Annual Cryptology Conference, Springer, pp. 80-97.

[19] Frédérique Oggier, Jean-Claude Belfiore, Emanuele Viterbo, et al. (2007) Cyclic division algebras: A tool for space--time coding. Foundations and Trends® in Communications and Information Theory, 4(1):1-95.

[20] Irving Reiner. (1975) Maximal orders. New York-London.

[21] Charles Everitt Grover. (2020) LWE over cyclic algebras: A novel structure for lattice cryptography.

[22] Charles Grover, Andrew Mendelsohn, Cong Ling, and Roope Vehkalahti. (2022) Non-commutative ring learning with errors from cyclic algebras. Journal of Cryptology, 35(3):1-67.

[23] László Babai. (1986) On lovász'lattice reduction and the nearest lattice point problem. Combinatorica, 6(1):1-13.

[24] Chris Peikert and Zachary Pepin. (2019) Algebraically structured LWE, revisited. In Theory of Cryptography: 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I 17, Springer, pp. 1-23.

[25] Nathan Jacobson. (2009) Finite-dimensional division algebras over fields. Springer Science & Business Media.

[26] Carl Bootland, Wouter Castryck, and Frederik Vercauteren. (2020) On the security of the multivariate ring learning with errors problem. Open Book Series, 4(1):57-71.

[27] Jyrki Lahtonen, Nadya Markin, and Gary McGuire. (2008) Construction of multiblock space--time codes from division algebras with roots of unity as nonnorm elements. IEEE transactions on information theory, 54(11):5231-5235.