Ring-LWE over two-to-power cyclotomics is not hard

Hao Chen [*]

March 29, 2021

Abstract

The Ring-LWE over two-to-power cyclotomic integer rings has been the hard computational problem for lattice cryptographic constructions. Its hardness and the conjectured hardness of approximating ideal-SIVP for ideal lattices in two-to-power cyclotomic fields have been the fundamental open problems in lattice cryptography and the complexity theory of computational problems of ideal lattices. In this paper we present a general theory of sublattice attack on the Ring-LWE with not only the Gaussian error distribution but also general error distributions. By the usage of our sublattice attack we prove that the decision Ring-LWE over two-to-power cyclotomic integer rings with certain polynomially bounded modulus parameters when degrees $d_n = 2^{n-1}$ going to the infinity can be solved by a polynomial (in d_n) time algorithm for wide error distributions with widths in the range of Peikert-Regev-Stephens-Davidowitz hardness reduction results in their STOC 2017 paper. Hence we also prove that approximating ideal-$SIVP_{poly(d_n)}$ with some polynomial factors for ideal lattices in two-to-power cyclotomic fields can be solved within quantum polynomial time. Therefore the lattice cryptographic constructions can not be based on the "hardness" of Ring-LWE over two-to-power cyclotomic integer rings even in the classical computational model.

Keywords: Ring-LWE, Width of error distribution, Sublattice attack, Sublattice pair with an ideal, Two-to-power cyclotomic field.

[*] Hao Chen is with the College of Information Science and Technology/Cyber Security, Jinan University, Guangzhou, Guangdong Province, 510632, China, haochen@jnu.edu.cn. This research is supported by the NSFC Grant 62032009.

1 Introduction

1.1 SVP and SIVP

A lattice $\mathbf{L}$ is a discrete subgroup in $\mathbf{R}^n$ generated by several linear independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m$ over the ring of integers, where $m \leq n$, $\mathbf{L} := \{a_1\mathbf{b}_1 + \cdots + a_m\mathbf{b}_m : a_1 \in \mathbf{Z}, \ldots, a_m \in \mathbf{Z}\}$. The volume $vol(\mathbf{L})$ of this lattice is $\sqrt{det(\mathbf{B} \cdot \mathbf{B}^\tau)}$, where $\mathbf{B} := (b_{ij})$ is the $m \times n$ generator matrix of this lattice, $\mathbf{b}_i = (b_{i1}, \ldots, b_{in}) \in \mathbf{R}^n$, $i = 1, \cdots, m$, are base vectors of this lattice. The length of the shortest non-zero lattice vectors is denoted by $\lambda_1(\mathbf{L})$. The well-known shortest vector problem (SVP) is defined as follows. Given an arbitrary $\mathbf{Z}$ basis of an arbitrary lattice $\mathbf{L}$ to find a lattice vector with length $\lambda_1(\mathbf{L})$ (see [36]). The approximating shortest vector problem $SVP_{f(m)}$ is to find some lattice vectors of length within $f(m)\lambda_1(\mathbf{L})$ where $f(m)$ is an approximating factor as a function of the lattice dimension m (see [36]). The Shortest Independent Vectors Problem ($SIVP_{\gamma(m)}$) is defined as follows. Given an arbitrary $\mathbf{Z}$ basis of an arbitrary lattice $\mathbf{L}$ of dimension m, to find m independent lattice vectors such that the maximum length of these m lattice vectors is upper bounded by $\gamma(m)\lambda_m(\mathbf{L})$, where $\lambda_m(\mathbf{L})$ is the m-th Minkowski's successive minima of lattice $\mathbf{L}$ (see [36]). A breakthrough result of M. Ajtai [5] showed that SVP is NP-hard under the randomized reduction. Another breakthrough proved by Micciancio asserts that approximating SVP within a constant factor is NP-hard under the randomized reduction (see [36]). For the latest development we refer to Khot [25]. It was proved that approximating SVP within a quasi-polynomial factor is NP-hard under the randomized reduction. For the hardness results about SVP and $SIVP$ we refer to [25, 26, 47].

1.2 Algebraic number fields

The Ring-LWE was introduced in [31] and has been the computational hard problem for lattice cryptography. It was suggested in [31] that the Ring-LWE over the integer ring $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_n(x))$ of n-th cyclotomic fields, where $\Phi_n(x) = \prod_{\gcd(n,j)=1}(x - \xi_n^j)$ is a cyclotomic polynomial, ξ_n is a primitive n-th root of unity, can be used for lattice-based cryptographic constructions. For example homomorphic encryption standard suggested in [3] was based on Ring-LWE over two-to-power cyclotomic rings. Cyclotomic number fields was first originated from Kummers pioneering work on Fermats last Theorem, we refer to [48]. In general an algebraic number field is a finite degree extension of the rational number field $\mathbf{Q}$. Let $\mathbf{K}$ be an algebraic number field and $\mathbf{R}_\mathbf{K}$ be its ring of integers in $\mathbf{K}$. From the primitive element theorem there exists an element $\theta \in \mathbf{K}$ such that $\mathbf{K} = \mathbf{Q}[x]/(f) = \mathbf{Q}[\theta]$, where $f(x) \in \mathbf{Z}[x]$ is an irreducible monic polynomial satisfying $f(\theta) = 0$ (see [18, 7]). It is well-known there is a positive definite inner product on $\mathbf{K} \otimes \mathbf{C}$ defined by $< u, v >= \Sigma_{i=1}^{d} \sigma_i(u)\widetilde{\sigma_i(v)}$, where σ_i, $i = 1, \ldots, d$, are d embedings of $\mathbf{K}$ in $\mathbf{C}$, and $\tilde{v}$ is complex conjugate. Sometimes we use $||u||_{tr}$ to represent $(\Sigma_{i=1}^{d} \sigma_i(u)\widetilde{\sigma_i(u)})^{1/2}$. This is also the norm with respect to the canonical embedding (see [31]). An ideal in $\mathbf{R_K}$ is a subset of $\mathbf{R_K}$ which is closed under ring addition and multiplication by an arbitrary element in $\mathbf{R_K}$. An ideal is a sub-lattice in $\mathbf{R_K}$ of dimension $deg(\mathbf{K}/\mathbf{Q})$. For an ideal $\mathbf{I} \subset \mathbf{R_K}$, the (algebraic) norm of ideal $\mathbf{I}$ is defined by the cardinality $N(\mathbf{I}) = |\mathbf{R_K}/\mathbf{I}|$, we have $N(\mathbf{I} \cdot \mathbf{J}) = N(\mathbf{I})N(\mathbf{J})$. For a principal ideal $\mathbf{xR_K}$ generated by an element $\mathbf{x}$, then $N(\mathbf{x}) = N(\mathbf{xR_K})$, we refer to [7, 17] for the detail. The dual of a lattice $\mathbf{L} \subset \mathbf{K}$ of rank deg($\mathbf{K}/\mathbf{Q}$) is defined by $\mathbf{L}^\vee = \{\mathbf{x} \in \mathbf{K}, tr_{K/Q}(\mathbf{ax}) \in \mathbf{Z}, \forall \mathbf{a} \in \mathbf{L}\}$. An order $\mathbf{O} \subset \mathbf{K}$ in a number field $\mathbf{K}$ is a subring of $\mathbf{K}$ which is a lattice with rank equal to deg($\mathbf{K}/\mathbf{Q}$). We refer to [17, 18, 7] for number theoretic properties of orders in number fields.

Let ξ_n be a primitive n-th root of unity, the n-th cyclotomic polynomial Φ_n is defined as $\Phi_n(x) = \prod_{j=1,\gcd(j,n)=1}^{n}(x - \xi_n^j)$. This is a monic irreducible polynomial in $\mathbf{Z}[x]$ of degree $\phi(n)$, where ϕ is the Euler function. The n-th cyclotomic field is $\mathbf{Q}(\xi_n) = \mathbf{Q}[x]/(\Phi_n(x))$. When $n = p$ is an odd prime $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ and when $n = p^m$, $\Phi_{p^m}(x) = \Phi_p(x^{p^{m-1}}) = (x^{p^{m-1}})^{p-1} + \cdots + x^{p^{m-1}} + 1$. The ring of integers in $\mathbf{Q}(\xi_n)$ is exactly $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_n(x))$ (see Theorem 2.6 in [50]). Hence the cyclotomic number field $\mathbf{Q}[\xi_n]$ is a monogenic field. The discriminant of the cyclotomic field (also the discriminant of the cyclotomic polynomial Φ_n) is

$$(-1)^{\frac{\phi(n)}{2}} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}}.$$

A polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbf{Z}[X]$ satisfies the condition of the Eisenstein criterion at a prime p, if $p|a_i$ for $0 \leq i \leq n-1$ and p^2 not dividing a_0. A polynomial satisfying this condition is irreducible in $\mathbf{Z}[x]$ from the Eisenstein criterion (see [7, 18]).

1.3 Gaussian and discrete Gaussian

Set $\rho_{s,\mathbf{c}}(\mathbf{x}) = e^{-\pi||\mathbf{x}-\mathbf{c}||^2/s^2}$ for any vector $\mathbf{c}$ in $\mathbf{R}^n$ and any $s > 0$, $\rho_s = \rho_{s,\mathbf{0}}$, $\rho = \rho_1$. The Gaussian distribution around $\mathbf{c}$ with width s is defined by its probability density function $D_{s,\mathbf{c}} = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{s^n}, \forall \mathbf{x} \in \mathbf{R}^n$.

1.3.1 Discretization

For any discrete subset $\mathbf{A} \subset \mathbf{R}^n$ we set $\rho_{s,\mathbf{c}}(\mathbf{A}) = \Sigma_{\mathbf{x}\in\mathbf{A}}\rho_{s,\mathbf{c}}(\mathbf{x})$ and $D_{s,\mathbf{c}}(\mathbf{A}) = \Sigma_{\mathbf{x}\in\mathbf{A}}D_{s,\mathbf{c}}(\mathbf{x})$. Let $\mathbf{L} \subset \mathbf{R}^n$ be a dimension n lattice, the discrete Gaussian distribution over $\mathbf{L}$ is the probability distribution over $\mathbf{L}$ defined by

$$\forall \mathbf{x} \in \mathbf{L}, D_{\mathbf{L},s,\mathbf{c}} = \frac{D_{s,\mathbf{c}}(\mathbf{x})}{D_{s,\mathbf{c}}(\mathbf{L})} = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\mathbf{L})}.$$

When $\mathbf{c} = \mathbf{0}$, the discrete Gaussian distribution is denoted by $\mathbf{D_{L,s}}$. We refer to [35] for the properties of discrete Gaussian distributions.

1.3.2 Width with the canonical embedding

The Gaussian distribution depends on coordinates and the norm. We need to pay special attention to coordinates (or the basis with which coordinates are obtained) and the norm used when we say the "width" of a Gaussian distribution. The "canonical embedding' was used to define the Gaussian distribution on $\mathbf{K} \otimes \mathbf{R}$ (see [31, 32, 41, 10]). We recall the analysis in [10]. Set $\Phi : \mathbf{K} \longrightarrow \mathbf{H}$ the canonical embedding defined on the number field $\mathbf{K} = \mathbf{Q}[x]/(f)$ where f is a degree n irreducible polynomial over $\mathbf{Q}$ and $\alpha_1, \ldots, \alpha_n$ in $\mathbf{C}$ are n roots of f. We refer the definition of the space $\mathbf{H}$ to Subsection 2.2 in [32]. Set $\mathbf{N}_f$ the inverse of the Vandermonde matrix $(\alpha_i^{j-1})_{1\leq i,j\leq n}$ and $\mathbf{B}$ the following matrix.

$$\begin{pmatrix} \mathbf{I}_{s_1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \frac{1}{\sqrt{2}}\mathbf{I}_{s_2} & \frac{i}{\sqrt{2}}\mathbf{I}_{s_2} \\ \mathbf{0} & \frac{1}{\sqrt{2}}\mathbf{I}_{s_2} & \frac{-i}{\sqrt{2}}\mathbf{I}_{s_2} \end{pmatrix}$$

Here there are s_1 real roots of f and $2s_2$ conjugate complex roots of f. Hence $s_1 + 2s_2 = n$. Let $\mathbf{r} = (r_1, \ldots, r_n)$ where $r_1, \ldots, r_n$ are n positive real numbers. If x_i, $i = 1, \ldots, n$, is sampled independently from the Gaussian distribution with width r_i, then coordinate vector with respect to the polynomial base $1, x, \ldots, x^n$ of $\mathbf{K} \otimes \mathbf{R}$ from the Gaussian distribution with parameter $\mathbf{r}$ (with respect to the canonical embedding Φ) is $\mathbf{N}_f \cdot \mathbf{B} \cdot (x_1, \ldots, x_n)^\tau$. Set $||\mathbf{N}_f||_2 = \max \frac{||\mathbf{N}_f \cdot \mathbf{x}||}{||\mathbf{x}||}$ where $\mathbf{x} \in \mathbf{R}^d$ takes all non-zero vectors. In the case $\mathbf{r} = (\sigma', \ldots, \sigma')$, if in the dual form of the Ring-LWE problem we set the width of the Gaussian distribution with respect to the canonical embedding is σ, then $\sigma' \leq ||\mathbf{N}_f||_2 \cdot \max\{|f'(\alpha_1)|, \ldots, |f'(\alpha_n)|\} \cdot \sigma$. Here f' is the derivative of the defining equation $f(x)$ of the number field.

1.4 Plain LWE, Ring-LWE, LWE over number field lattices and module-LWE

Plain LWE

O. Regev proposed the plain LWE and lattice-based cryptographic construction based on it in his paper [45]. We also refer to [46] for a survey. Let n be the security parameter, q be an integer modulus and χ be an error distribution over $\mathbf{Z}_q$. Let $\mathbf{s} \in \mathbf{Z}_q^n$ be a secret chosen uniformly at random. Given access to d samples of the form

$$(\mathbf{a}, [\mathbf{a} \cdot \mathbf{s} + e]_q) \in \mathbf{Z}_q^n \times \mathbf{Z}_q,$$

or

$$(\mathbf{a}, \frac{1}{q}[\mathbf{a} \cdot \mathbf{s} + e]_q) \in \mathbf{Z}_q^n \times \mathbf{R}/\mathbf{Z},$$

where $\mathbf{a} \in \mathbf{Z}_q^n$ are chosen uniformly at random and $\mathbf{e}$ are sampled from the error distribution χ, the search LWE is to recover the secret $\mathbf{s}$. In general χ is the discrete Gaussian distribution with the width σ. Here $\mathbf{a} \cdot \mathbf{s} = \Sigma a_i s_i$ is the inner product of two vectors in $\mathbf{Z}_q^n$. Solving decision $LWE_{n,q,d,\chi}$ is to distinguish with non-negligible probability whether $(\mathbf{A}, \mathbf{b}) \in \mathbf{Z}_q^{n \times d} \times \mathbf{Z}_q^d$ is sampled uniformly at random, or if it is of the form $(\mathbf{A}, \mathbf{A}^\tau \cdot \mathbf{s} + \mathbf{e})$ where $\mathbf{e}$ is sampled from the distribution χ. Here $[\mathbf{a} \cdot \mathbf{s} + e]_q$ is the residue class in the interval $(-\frac{q}{2}, \frac{q}{2}]$. We refer to [46] for the detail and the background.

Ring-LWE

In [33] the algebraic structure of ring was first considered for the hardness of computational problems of lattices, we also refer to [29, 30]. This Ring-SIS (Short Integer Solution over Ring, see [33]) is an analogue of Ajtai's SIS problem. The one-wayness of some function was proved in [33] by assuming the hardness of some computational problems of ideal lattices (cyclic lattices). In their Eurocrypt 21010 paper [31] the Ring-LWE was proposed and then extended in [32]. We refer to the nice survey [40] for the history of development, the theory and cryptographic constructions based on Ring-LWE and Ring-SIS. In particular suggested homomorphic encryption standard [3] was based on Ring-LWE over two-to-power cyclotomic integer rings.

If the $\mathbf{Z}_q^n$ in plain LWE is replaced by $\mathbf{P}_q = \mathbf{P}/q\mathbf{P}$ where $\mathbf{P} = \mathbf{Z}[x]/(f)$, $f(x)$ is a monic irreducible polynomial of degree n in $\mathbf{Z}[x]$, this is the polynomial learning with errors (PLWE). The inner product $\mathbf{a} \cdot \mathbf{s} = \Sigma a_i s_i$ is replaced by the multiplication $\mathbf{a} \cdot \mathbf{s}$ in the ring $\mathbf{P}_q$. The error distribution χ is defined as the discrete Gaussian distributions with respect to the basis $1, x, x^2, \ldots, x^{n-1}$ (see [23, 10]). We refer to [49] for relations and reductions between Ring-LWE and PLWE.

If the $\mathbf{Z}_q^n$ is replaced by $(\mathbf{R_K})_q = \mathbf{R_K}/q\mathbf{R_K}$ where $\mathbf{R_K}$ is the ring of integers in an algebraic number field $\mathbf{K}$ of degree n, this is the Ring-LWE, learning with errors over the ring $\mathbf{R_K}$. The secret $\mathbf{s}$ is in the dual $(\mathbf{R_K}^\vee)_q = \mathbf{R_K}^\vee/q\mathbf{R_K}^\vee$ and $\mathbf{a} \in \mathbf{R_K}_q$ is chosen uniformly at random. The inner product $\mathbf{a} \cdot \mathbf{s} = \Sigma a_i s_i$ is replaced by the multiplication $\mathbf{a} \cdot \mathbf{s}$ in $(\mathbf{R_K}^\vee)_q$. The error $\mathbf{e}$ is in $(\mathbf{R_K}^\vee)_q = \mathbf{R_K}^\vee/q\mathbf{R_K}^\vee$. In this case the width of error distribution is defined by the trace norm on $\mathbf{K} \otimes \mathbf{R}$ via the canonical embedding (see [31, 10]). This is called the dual form of Ring-LWE problem . When $\mathbf{s} \in (\mathbf{R_K})_q$ and $\mathbf{e} \in (\mathbf{R_K})_q$ are assumed it is called the non-dual form of Ring LWE problem. As indicated in [41] page 10 in monogenic case a "tweak factor" $f'(\theta)$ can be used to make two versions equivalent.

LWE over number field lattice

Learning with errors over a number field lattice was introduced in [42]. Let $\mathbf{L} \subset \mathbf{K}$ be a rank deg($\mathbf{K}$) lattice and

$$\mathbf{O^L} = \{x \in \mathbf{K} : x \cdot \mathbf{L} \subset \mathbf{L}\}.$$

Then $\mathbf{O^L}$ is an order.

$$\mathbf{L}^\vee{}_q = \mathbf{L}^\vee/q\mathbf{L}^\vee.$$

Then $\mathbf{O^L} \cdot \mathbf{L}^\vee \subset \mathbf{L}^\vee$. Set $\mathbf{O^L}_q = \mathbf{O^L}/q\mathbf{O^L}$ and $(\mathbf{L}^\vee)_q = \mathbf{L}^\vee/q\mathbf{L}^\vee$. The secret vector $\mathbf{s}$ is in $(\mathbf{L}^\vee)_q$ and $\mathbf{a}$ is in $\mathbf{O^L}_q$. Here we notice that $\mathbf{O} \cdot \mathbf{L}^\vee \subset \mathbf{L}^\vee$. Then the error $\mathbf{e} \in (\mathbf{L}^\vee)_q$. Samples from LWE over number field lattice $\mathbf{L}$ is

$(\mathbf{a}, \mathbf{b}) \in \mathbf{O^L}_q \times (\mathbf{L}^\vee)_q$, where $\mathbf{a}$ is uniformly chosen in $\mathbf{O^L}_q$, the error vector $\mathbf{e}$ is chosen in $(\mathbf{L}^\vee)_q$ according to a Gaussian distribution with the width σ, then $\mathbf{b} \in \mathbf{L}^\vee)_q$ is from the LWE equation. The decisional LWE over $\mathbf{L}$ is to distinguish these samples from uniformly chosen $(\mathbf{a}, \mathbf{b}) \in \mathbf{O^L}_q \times (\mathbf{L}^\vee)_q$. For the detail and hardness reduction we refer to [42]. We refer to [11] for the sublattice attack on LWE over number field lattices.

Module-LWE

Let $\mathbf{M} = \mathbf{R_K}^d$, for $\mathbf{s} \in (\mathbf{R_K}_q^\vee)^d$, and an error distribution ψ over $\mathbf{K} \otimes \mathbf{R}$, we sample the module learning with error distribution $A^{(R)}_{d,q,s,\psi}$ over $\mathbf{R_K}^d \times \mathbf{T}(\mathbf{R_K}^\vee)$ by outputting $(\mathbf{a}, < \mathbf{a}, \mathbf{s} > + \frac{1}{q} e \ mod \ \mathbf{R_K}^\vee)$, where $\mathbf{a} \longleftarrow \mathbf{U}(\mathbf{R_K}_q^d)$ and $e \longleftarrow \psi$. The decision module learning with errors problem Module-LWE over $\mathbf{M}$ is to distinguish uniform samples $\mathbf{U}(\mathbf{R_K}^d \times \mathbf{T}(\mathbf{R_K}^\vee)$ and samples from $A^{(R)}_{d,q,s,\psi}$. Here ψ is the Gaussian distribution with width σ.

We refer to [4] for the detail.

1.5 Hardness reduction

The reduction results from approximating ideal-$SIVP_{poly(d)}$ (or approximating ideal-$SVP_{poly(d)}$) to Ring-LWE were first given in [31, 32] for search version and then a general form from to decision version was proved for arbitrary number fields in [43]. We refer to [43] Corollary 6.3 for the following hardness reduction result.

Hardness reduction for decision Ring-LWE. *Let* $\mathbf{K}$ *be an arbitrary number field of degree* n *and* $\mathbf{R} = \mathbf{R_K}$*. Let* $\alpha = \alpha(n) \in (0, 1)$*, and let* $q = q(n)$ *be an integer such that* $\alpha q \geq 2\omega(1)$*. Then there exists a polynomial-time quantum reduction from* $\mathbf{K} - SIVP_\gamma$ *to average-case, decision* $\mathbf{R} - LWE_{q,\Upsilon_\alpha}$*, for any* $\gamma = \max\{\frac{\eta(\mathbf{I}) \cdot 2}{\alpha \cdot \omega(1)}, \frac{\sqrt{2n}}{\lambda_1(\mathbf{I})}\} \leq \max\{\omega(\sqrt{nlogn}/\alpha), \sqrt{2}n\}$*. Here* $\mathbf{K} - SIVP_\gamma$ *is the Shortest Independent Vector Problems for any fractional ideal lattice in* $\mathbf{K}$*.* $\mathbf{I}$ *is any ideal lattice and* $\eta(\mathbf{I})$ *is the smoothing parameter of* $\mathbf{I}$*.*

Approximating SVP and $SIVP$ restricted to ideal lattices in number fields with degrees going to the infinity are called approximating ideal-SVP and ideal-$SIVP$, we refer to [19, 20, 21, 44, 28, 37] for the latest development on this topic.

1.6 Known attacks

The famous Blum-Kalai-Wasserman (BKW) algorithm in [6] was improved in [1, 27]. On the other hand some provable weak instances of Ring-LWE was given in [22, 23, 16] and analysed in [10, 41]. As showed in [41, 10] these instances of Ring-LWE can be solved by polynomial time algorithms main because the widths of Gaussian distributions of errors are too small or Gaussian distributions of errors are too skew. In [13] these attacks were improved for these modulus parameters which are factors of $f(u)$, where f is the defining equation of the number field and u is an arbitrary integer. However the Gaussian distribution is still required to be narrow such that this type of attack can be succeed. We refer to [2] for the dual lattice attack to LWE with small secrets and refer to [19, 20, 21, 28, 37] for the latest development in algorithms on approximating ideal-SVP.

2 Sublattice attacks

Sublattice attacks was proposed in [11] and extended in [12]. It achieves successful attacks on Ring-LWE with wide Gaussian error distributions. However it works even for other wide error distributions provided that suitable sublattice pairs can be constructed. It is a theory in essence and not an algorithm. The main point of the sublattice attack as follows. For the decision Ring-LWE with *arbitrarily polynomially bounded* width Gaussian error distributions over some number field sequences $\mathbf{K}_n$ including two-to power cyclotomic fields, for some large polynomially bounded modulus parameters (depending on the width bound), by constructing suitable sublattices $\mathbf{L}_n$ in the cycolotomic integer rings $\mathbf{R}_{\mathbf{K_n}}$, the samples from the Ring-LWE equations can be distinguished from the uniform distribution in the quotient $\mathbf{R}_{\mathbf{K_n}}/\mathbf{L}_n$ very efficiently. From this point of view we believe that the learning with errors problem over algebraically-structured objects perhaps can be solved within polynomial times in many settings.

2.1 The motivation of sublattice attacks

In previous attacks on Ring-LWE, when polynomially bounded many samples $(\mathbf{a}, \mathbf{b}) \in \mathbf{R}_{\mathbf{K}}/q\mathbf{R}_{\mathbf{K}} \times \mathbf{R}_{\mathbf{K}}/q\mathbf{R}_{\mathbf{K}}$ are given, only the distributions of these samples over $\mathbf{R_K}/\mathbf{I}$ for some **ideals** satisfying $q\mathbf{R_K} \subset \mathbf{I} \subset \mathbf{R_K}$ and $|\mathbf{R_K}/\mathbf{I}| \leq poly(d)$ have been checked. This is not natural and not sufficient. We need to check the distributions of samples in $\mathbf{R_K}/\mathbf{L}$ where $\mathbf{L}$ takes over **all sublattices** satisfying

$$q\mathbf{R_K} \subset \mathbf{L} \subset \mathbf{R_K}$$

and

$$|\mathbf{R_K}/\mathbf{L}| \leq poly(d).$$

This is the motivation of sublattice attack in our previous paper [11]. In general when the learning with error problems with algebraic structures are used to improve the efficiency, sublattice attacks as above to analysis the distributions of samples over $\mathbf{M}/\mathbf{L}$ should be considered, where $\mathbf{M}$ is module over which the module-LWE is defined and $\mathbf{L}$ takes over all sublattices of $\mathbf{M}$ satisfying

$$q\mathbf{M} \subset \mathbf{L} \subset \mathbf{M}$$

and

$$|\mathbf{M}/\mathbf{L}| \leq poly(d).$$

The previous attacks where $\mathbf{L}$ is restricted to ideals or sub-modules are special, not natural and not sufficient to guarantee the security, we refer to our next paper [15].

The basic point here is as follows. When we want to use the algebraic structure to improve the efficiency of lattice-based cryptographic constructions. The adversary is not so restricted to only check the distributions of samples over algebraic-structured object, the adversary can attack the problem by using lattices without any algebraic structure. In 2019 we proposed the sublattice attack on LWE over number field lattices and suggested some conditions such that sublattice attack can success in [11]. In the sublattice attacks presented in [12] and this paper the sublattice pair with an ideal is introduced the sublattice attacks from sublattice pairs with ideals are given. The adversary can indeed distinguish the Ring-LWE equation samples from the samples uniform distributed in $\mathbf{R_K}/\mathbf{L}$ when sublattices are carefully constructed.

2.2 Sublattice pairs with ideals are needed

When $\mathbf{L}$ is just a sublattice of $\mathbf{R_K}$ satisfying $|\mathbf{R_K}/\mathbf{L}| \leq poly(d)$, for an uniformly distributed $\mathbf{a} \in \mathbf{R_K}$, $\mathbf{a} \cdot \mathbf{L} \subset \mathbf{L}$ is not valid. We even proved in

[12] if $\mathbf{L}_1 \cdot \mathbf{L}_2 \subset \mathbf{L}_3$ where

$$|\mathbf{R_K}/\mathbf{L}_i| \leq poly(d),$$

where $i = 1, 2, 3$, then the length $\lambda_1(\mathbf{L}_3^\vee)$ of the shortest nonzero lattice vectors in the dual $\mathbf{L}_3^\vee$ can not be very small. Hence we need to find an ideal $\mathbf{Q} \subset \mathbf{L}$ satisfying $|\mathbf{R_K}/\mathbf{Q}| \leq poly(d)$, then $\mathbf{s}$ satisfies $\mathbf{s} \in \mathbf{Q}$ with a probability $\frac{1}{poly(d)}$. Therefore we have $\mathbf{a} \cdot \mathbf{s} \in \mathbf{Q} \subset \mathbf{L}$ with a probability $\frac{1}{poly(d)}$ of secrets for uniformly distributed $\mathbf{a} \in \mathbf{R_K}$. Hence if $\mathbf{e} \in \mathbf{L}$ is satisfied with a probability

$$Prob(\mathbf{e} \in \mathbf{L}) \geq \frac{d^c}{|\mathbf{R_K}/\mathbf{L}|}$$

where c is a fixed positive integer, we can distinguish samples $\mathbf{b}$ from Ring-LWE equations and uniformly distributed samples.

The condition

$$Prob(\mathbf{e} \in \mathbf{L}) \geq Prob(\mathbf{e} \in \mathbf{L}_1) \geq \frac{d^c}{|\mathbf{R_K}/\mathbf{L}|}$$

is achieved by an auxiliary sublattice $\mathbf{L}_1 \subset \mathbf{L}$ from the probability computation about $Prob(\mathbf{e} \in \mathbf{L}_1)$ in Theorem 4.1. Hence we need sublattice pairs $(\mathbf{L}_1, \mathbf{L})$ with ideals $\mathbf{Q}$ to mount our sublattice attack.

2.3 Construction of sublattice pairs

We consider the decisional Ring-LWE over two-to-power cyclotomic integers with width satisfying $\sigma \leq d^C$ where C is an arbitrary fixed positive integer. The sublattice pair $(\mathbf{L}_1, \mathbf{L})$ with an ideal $\mathbf{Q}$ will be constructed as follows. We take polynomially bounded modulus parameters q_m such that $q \equiv 1 \ mod \ 2^{m-1}$. Hence q_m is completely split in each two-to-power cyclotomic field of degree 2^{m-1} in the sequence. In general both sublattices $\mathbf{L}_1$ and $\mathbf{L}$ are of the form

$$\{\mathbf{y} : Tr(\mathbf{x}_i, \mathbf{y}) \equiv 0 modq, \mathbf{y} \in \mathbf{R_{K_m}}\}, \tag{1}$$

where $\mathbf{x}_i$'s are fixed elements in $\mathbf{R_{K_m}}$. Notice that these sublattices only depend on the residue classes of $\mathbf{x}_i$'s in $\mathbf{R_{K_m}}/q_m\mathbf{R_{K_m}}$.

In the two-to-power cyclotomic field case, $\mathbf{L}$ is defined by one vector

$$\mathbf{x} = \Sigma_{i=1}^{C_1} m_i \mathbf{x}_i,$$

where $\mathbf{x}_i$ are fixed elements in $\mathbf{R}_{\mathbf{K_m}}$ with fixed bounded norm, m_i's are integers and C_1 is a fixed positive integer. We need this $\mathbf{x}$ satisfies $|\mathbf{R}_{\mathbf{K_m}}/\mathbf{L}| = q_m$. Since the cyclotomic fields are monogenic this is not a strong restriction on $\mathbf{x}$. The sublattice $\mathbf{L}_1$ defined by

$$\{\mathbf{y} : Tr(\mathbf{x}_i, \mathbf{y}) \equiv 0 mod q, \mathbf{y} \in \mathbf{R}_{\mathbf{K_m}}, i = 1, \dots, C_1\}$$

is a sublattice of $\mathbf{L}$. Since $x^{2^{m-1}}+1$ can be factorized to linear factors module q_m, we take $\mathbf{x}$ contains exactly $2^{m-1} - C_2$ factors and $\mathbf{Q}$ is generated by q_m and the product of the remaining C_2 factors. Here C_2 is a fixed positive integer when m goes to the infinity. Then sublattice pairs with ideals can be constructed. The requirement

$$Prob(\mathbf{e} \in \mathbf{L}_1) \geq \frac{d^c}{|\mathbf{R}_\mathbf{K}/\mathbf{L}|}$$

is satisfied from Theorem 4.1 Theorem 4.2 and Theorem 6.1, the condition $\sigma \leq d^C$ the upper bound on norms of $\mathbf{x}_i$'s and the number of $\mathbf{x}_i$'s, and a suitable large polynomially bounded modulus parameter. Therefore the modulus parameter can be taken depending on 2^{m-1} and the fixed positive integers C, C_1, C_2, when m goes to the infinity, such that a sublattice pair with an ideal can be constructed.

The existence of the desired $\mathbf{x}$ with a fixed positive integer C_1 and bounded norm $\mathbf{x}_i$'s when m goes to the infinity is equivalent to some bounded (when m goes to the infinity) finite term linear recurrence relations on some degree $2^{m-1} - C_2$ factors of $x^{2^m-1} + 1$. We refer to Section 6 and the proof of Theorem 3.2 for the detail. Hence from the view of the sublattice attack the hardness of decision Ring-LWE in some number fields is essentially an algebraic problem.

3 Our contribution

3.1 Sublattice pair with an ideal

Let $\mathbf{K} = \mathbf{Q}[x]/(f(x)) = \mathbf{Q}[\theta]$ be a degree d extension field of the rational field $\mathbf{Q}$, where f is a monic irreducible polynomial in $\mathbf{Z}[x]$ and $\theta \in \mathbf{C}$ is a root of f. Let $\mathbf{R}_\mathbf{K}$ be its ring of integers. We consider the non-dual Ring-LWE over $\mathbf{R}_\mathbf{K}$ with a modulus parameter q.

Definition 3.1. *We assume that the modulus parameter q satisfies $d^{C_1} \leq q < d^{C_2}$ where C_1 and C_2 are two fixed positive integers. Let $\mathbf{L}_i \subset \mathbf{R_K}$ be a sublattice in $\mathbf{R_K}$ for $i = 1, 2$ and $\mathbf{Q} \subset \mathbf{R_K}$ is an ideal. They satisfy the following properties.*
1) $q\mathbf{R_K} \subset \mathbf{L}_i \subset \mathbf{R_K}$ for $i = 1, 2$ and $q\mathbf{R_K} \subset \mathbf{Q} \subset \mathbf{R_K}$;
2) $\mathbf{L}_1, \mathbf{L}_2, \mathbf{Q}$ are polynomially indexed in $\mathbf{R_K}$, that is, there exists a fixed positive integer C_3 such that $|\mathbf{R_K}/\mathbf{L}_i| \leq d^{C_3}$ for $i = 1, 2$ and $|\mathbf{R_K}/\mathbf{Q}| \leq d^{C_3}$;
3) $\mathbf{Q} \subset \mathbf{L}_2$ and $\mathbf{L}_1 \subset \mathbf{L}_2$;
4) The probability $Prob(\mathbf{e} \in \mathbf{L}_1)$ that $\mathbf{e} \in \mathbf{L}_1$ satisfies the inequality $Prob(\mathbf{e} \in \mathbf{L}_1) \geq \frac{d^{C_4}}{|\mathbf{R_K}/\mathbf{L}_2|}$ where C_4 is a fixed positive integer. We call $(\mathbf{L}_1, \mathbf{L}_2)$ a sublattice pair with the ideal $\mathbf{Q}$ for the Ring-LWE over $\mathbf{K}$ with the modulus parameter q.

In general if we can construct such lattice pair with an ideal for a Ring-LWE over $\mathbf{R_K}$ with the polynomially bounded modulus parameter q, then the decision version of this Ring-LWE can be solved by a polynomial in d time algorithm. Moreover we notice that the error distribution is only involved in 4), it is not assumed Gaussian. The property 4) is sufficient for a polynomial time attack on the general Ring-LWE with an error distribution satisfying the property 4).

3.2 Main results

The following result is for the Ring-LWE with general error distributions over general number fields with a sublattice pair defined as above.

Theorem 3.1. *We consider the decision Ring-LWE over $\mathbf{R_K}$ with a general error distribution and a modulus parameter q satisfying $d^{C_1} \leq q < d^{C_2}$ where C_1 and C_2 are two fixed positive integers. Suppose that there exists a sublattice pair with an ideal as above. Then the decision Ring-LWE over $\mathbf{R_K}$ with the modulus parameter q can be solved within time complexity $O(d^{4C_2C_3})$.*

Let $\mathbf{K}_n = \mathbf{Q}[x]/(f_n) = \mathbf{Q}[\xi_{2^n}]$, where $f_n = x^{2^{n-1}} + 1$, $d_n = \phi(2^n) = 2^{n-1}$, and ξ_{2^n} is a primitive 2^n-th root of unity. This is a monogenic number field. It is easy to verify that the boundness $||\xi_{2^n}^j||_{tr} \leq \sqrt{d}$ for any integer j and the boundness of the size of "tweak factors" $|f'(\xi_{2^n}^j)| \leq d$ where $\xi_{2^n}^j$ takes over all 2^n-th roots of unity. We can construct sublattice pairs with ideals for two-to-power cyclotomic number fields. Then from Theorem 3.1 the following result can be proved.

Theorem 3.2. *Let C be an arbitrary fixed positive integer. We consider the non-dual decision Ring-LWE over $\mathbf{R_{K_n}} = \mathbf{Z}[\xi_{2^n}]$. Suppose that the width σ of the error distribution over $\mathbf{R_{K_n}}$ satisfies $\frac{\sqrt{d_n}}{\lambda_1(\mathbf{Z}[\xi_{2^n}]^\vee)} \leq \sigma \leq d_n^C$. Then there exists a sequence of polynomially bounded modulus parameters $q_n \leq poly(d_n)$ only depending on d_n and C such that the the decision Ring-LWE over $\mathbf{Z}[\xi_{2^n}]$ with the modulus parameter q_n can be solved in polynomial time (in d_n).*

Corollary 3.1. *Let C be an arbitrary fixed positive integer. We consider the dual decision Ring-LWE over $\mathbf{R_{K_n}}^\vee = \mathbf{Z}[\xi_{2^n}]^\vee$. Suppose that the width σ of the error distribution over $\mathbf{R_{K_n}}^\vee$ satisfies $\frac{\sqrt{d_n}}{\lambda_1(\mathbf{Z}[\xi_{2^n}])} \leq \sigma \leq d_n^C$. Then there exists a sequence of polynomially bounded modulus parameters q_n only depending on d_n and C such that the the decision Ring-LWE over $\mathbf{Z}[\xi_{2^n}]^\vee$ with the modulus parameter q_n can be solved in polynomial time (in d_n).*

From the hardness reduction result Theorem 6.2 and Corollary 6.3 in [43] we have the following result.

Corollary 3.2. *Let $\mathbf{K}_n$, $d_n = 2^{n-1}$, be the sequence of two-to-power cyclotomic fields with their degrees $d_n \longrightarrow \infty$. Then there exists a fixed positive integer c such that approximating $SIVP_{d_n^c}$ with approximating factor d^c for ideal lattices in $\mathbf{K}_{d_n}$ can be solved by a polynomial (in d_n) time quantum algorithm.*

The similar results in the case of two-to-power cyclotomic fields and more general fields were proved in our preprint [13, 14] in 2019.

Corollary 3.3. *Let C be an arbitrary fixed positive integer and m be a fixed positive integer. We consider the Module-LWE over $\mathbf{R_{K_n}}^m = \mathbf{Z}[\xi_{2^n}]^m$. Suppose that the width σ of the error distribution satisfies $\frac{\sqrt{d_n}}{\lambda_1(\mathbf{Z}[\xi_{2^n}])} \leq \sigma \leq d_n^C$. Then there exists a sequence of polynomially bounded modulus parameters q_n only depending on d_n and m, C such that the the decision Module-LWE over $\mathbf{Z}[\xi_{2^n}]^m$ with the modulus parameter q_n can be solved in polynomial time (in d_n).*

3.3 Practical sublattice attack

In this paper by using the construction of sublattice pairs with ideals, we prove that for the decision Ring-LWE over $\mathbf{Z}[\xi_{2^m}]$ with Gaussian error distribution of width σ satisfying $\frac{\sqrt{d_m}}{\lambda_1(\mathbf{Z}[\xi_{2^m}]^\vee)} \leq \sigma \leq d_m^C$, where $d_m = 2^{m-1}$ and C is an arbitrary fixed positive integer. There exists a sequence of polynomially bounded modulus parameters $q_m \leq poly(d_m)$ only depending on d_m and C such that the the decision Ring-LWE over $\mathbf{Z}[\xi_{2^m}]$ with the modulus parameter q_m can be solved in polynomial time (in d_m). For practical lattice cryptographic constructions based on Ring-LWE over the concrete two-to-power cyclotomic integer ring $\mathbf{Z}[\xi_{2^m}]$, we suggest to find suitable sublattice pairs with ideals as required in Theorem 3.2, and then to test samples in $\mathbf{Z}[\xi_{2^m}]/\mathbf{L}_2$, where $\mathbf{L}_2$ is the large sublattice in $\mathbf{Z}[\xi_{2^m}]$ of the sublattice pair with ideal constructed according to the width and the requirement in the proof of Theorem 3.2.

3.4 Cryptographic and algorithmic implications

We prove that the decision Ring-LWE over two-to-power cyclotomic integer rings can be solved within classical polynomial time even for error distributions with the widths in the range of Peikert-Regev-Stephens-Davidowitz hardness reduction results in Corollary 3.2. This is a serious difficulty in lattice-based cryptographic constructions based on Ring-LWE over two-to-power cyclotomic integers. For the complexity theory of computational problems of ideal lattices, our main result Corollary 3.2 and the main results in [13, 14] indicate that approximating ideal-$SIVP$ problems with a polynomial factor for cyclotomic fields are easy in quantum computation model. We refer to other proofs of this kind of results in our preprints [13, 14] in 2019.

4 Probability computation

We need the following computation of probability in Theorem 3.2.

Theorem 4.1. *Let $\mathbf{L}$ be a rank d number field lattice in a degree d number field $\mathbf{K}$. Let $\mathbf{L}_1$ be rank d sublattice of $\mathbf{L}^\vee$ satisfying that $q\mathbf{L}^\vee \subset \mathbf{L}_1 \subset \mathbf{L}^\vee$ and the cardinality $|\mathbf{L}^\vee/\mathbf{L}_1|$ is polynomially bounded. Suppose that the width of the Gaussian distribution of errors $\mathbf{e}$ satisfying $\frac{\sqrt{d}}{\lambda_1(\mathbf{L})} \leq$*

$\sigma \leq \frac{\sqrt{c_1}}{\sqrt{\pi}\lambda_1(\mathbf{L}_1^\vee)}$ and moreover there are at least $\frac{|\mathbf{L}^\vee/\mathbf{L}_1|}{q^{c_2}}$ lattice vectors in $\mathbf{L}_1^\vee$ satisfying $||\mathbf{x}||_{tr} \leq \frac{\sqrt{c_1}}{\sqrt{\pi}\sigma}$, where c_1 and c_2 are fixed positive real numbers. Then the probability $\mathbf{e} \in \mathbf{L}_1$ is

$$Prob(\mathbf{e} \in \mathbf{L}_1) = \frac{\Sigma_{\mathbf{x}\in\mathbf{L}_1} e^{-\pi(\frac{||\mathbf{x}||_{tr}}{\sigma})^2}}{\Sigma_{\mathbf{x}\in\mathbf{L}^\vee} e^{-\pi(\frac{||\mathbf{x}||_{tr}}{\sigma})^2}}.$$

It satisfies

$$Prob(\mathbf{e} \in \mathbf{L}_1) \geq \frac{1}{e^{c_1} q^{c_2}}$$

when q is sufficiently large.

Proof. We calculate the probability $Prob(\mathbf{e} \in \mathbf{L}_1)$ of the condition $\mathbf{e} \equiv 0$ *mod* $\mathbf{L}_1$. It is clear

$$Prob(\mathbf{e} \in \mathbf{L}_1) = \frac{\Sigma_{\mathbf{x}\in\mathbf{L}_1} e^{-\pi(\frac{||\mathbf{x}||_{tr}}{\sigma})^2}}{\Sigma_{\mathbf{x}\in\mathbf{L}^\vee} e^{-\pi(\frac{||\mathbf{x}||_{tr}}{\sigma})^2}}.$$

Set $Y_3(0) = \frac{\Sigma_{\mathbf{x}\in\mathbf{L}^\vee} e^{-\pi(\frac{||\mathbf{x}||_{tr}}{\sigma})^2}}{\sigma^n}$ and $Y_4(0) = \frac{\Sigma_{\mathbf{x}\in\mathbf{L}_1} e^{-\pi(\frac{||\mathbf{x}||_{tr}}{\sigma})^2}}{\sigma^n}$. From the Poisson summation formula (see [35]) we have

$$Y_3(0) = \frac{1}{\det(\mathbf{L}^\vee)} \Sigma_{\mathbf{x}\in\mathbf{L}} e^{-\pi(||\mathbf{x}||_{tr}\sigma)^2}.$$

and

$$Y_4(0) = \frac{1}{\det(\mathbf{L}_1)} \Sigma_{\mathbf{x}\in(\mathbf{L}_1)^\vee} e^{-\pi(||\mathbf{x}||_{tr}\sigma)^2}.$$

Since $\sigma \geq \frac{\sqrt{d}}{\lambda_1(\mathbf{L})}$ then $\Sigma_{\mathbf{x}\in\mathbf{L}-\mathbf{0}} e^{-\pi(||\mathbf{x}||_{tr}\sigma)^2} \leq 1 + \frac{1}{2^d}$ from Lemma 3.2 in [35]. For lattice vectors $\mathbf{x} \in \mathbf{L}_1^\vee$ satisfying

$$||\mathbf{x}||_{tr} \leq \frac{\sqrt{c_1}}{\sqrt{\pi}\sigma}$$

we have

$$e^{-\pi(||\mathbf{x}||_{tr}\sigma)^2} \geq e^{-c_1}.$$

Hence $Prob(\mathbf{e} \in \mathbf{L}_1) \geq \frac{1}{|\mathbf{L}^\vee/\mathbf{L}_1|}(1 + \frac{1}{e^{c_1}} \cdot \frac{|\mathbf{L}^\vee/\mathbf{L}_1|}{q^{c_2}})$. The conclusion follows directly.

From Theorem 4.1 we give a general criterion about the existence of sublattice pairs with ideals for the Ring-LWE with the wide Gaussian error distribution.

Theorem 4.2. *Let* $\mathbf{K}_n = \mathbf{Q}[x]/(f_n) = \mathbf{Q}[\theta_n]$ *be a sequence of degree* d_n *monogenic extension fields of the rational field* $\mathbf{Q}$ *and* $\{f_n\} \in \mathbf{Z}[x]$ *be a sequence of monic irreducible degree* d_n *polynomials. We consider the non-dual Ring-LWE over* $\mathbf{R_{K_n}}$ *with the Gaussian error distribution of width* $\frac{\sqrt{d_n}}{\lambda_1(\mathbf{R_{K_n}}^\vee)} \leq \sigma \leq d_n^{C_3}$*. Let* q_n *be a sequence of modulus parameters satisfying* $d_n^{C_1} \leq q_n < d_n^{C_2}$*. Suppose that* $f_n^1(\theta_n)f_n^2(\theta_n) \in q_n\mathbf{R_{K_n}}$*, where* f_n^1 *and* f_n^2 *are two polynomials in* $\mathbf{Z}/q_n\mathbf{Z}[x]$*, and* $\deg(f_n^1) \leq C$ *where* C *is a fixed positive integer when* d_n *goes to the infinity. Suppose that* f_n^2 *is in the form* $f_n^2 = \Sigma_{i=1}^s m_i \mathbf{x}_n^i$ *where* s *is a fixed positive integer (when* d_n *goes to the infinity) satisfying* $sC_3 < C_1$*,* $m_1, \ldots, m_s$ *are in* $\mathbf{Z}/q_n\mathbf{Z}$*, and* $\mathbf{x}_n^1, \ldots, \mathbf{x}_n^s$ *are elements in* $\mathbf{R_{K_n}}$ *satisfying*
1) $Tr(\mathbf{x}_n^i \cdot \mathbf{y}) \equiv 0$ *mod* q_n *for* $i = 1, \ldots, s$*, and* $\mathbf{y} \in \mathbf{R_{K_n}}$ *define a sublattice* $\mathbf{L}_1$ *of* $\mathbf{R_{K_n}}$ *satisfying* $|\mathbf{R_{K_n}}/\mathbf{L}_1| = q_n^s$*;*
2) $\prod_{i=1}^s s^s ||\mathbf{x}_n^i||_{tr} \leq d_n^{C_1 - sC_3 - C_4}$ *where* C_4 *is a fixed positive real number.*
Set $\mathbf{Q}$ *the ideal generated by* q_n *and* f_n^1 *and* $\mathbf{L}_2$ *the sublattice of* $\mathbf{R_{K_n}}$ *defined by* $Tr(f_n^2 \cdot \mathbf{y}) \equiv 0$ *mod* q_n*.*
3) We assume the index $|\mathbf{R_{K_n}}/\mathbf{L}_2| = q_n$*.*
Then $(\mathbf{L}_1, \mathbf{L}_2)$ *is a sublattice pair with the ideal* $\mathbf{Q}$ *for this Ring-LWE.*

Proof. It is clear for each element $q\mathbf{h_1} + f_n^1\mathbf{h_2} \in \mathbf{Q}$, where $\mathbf{h}_i \in \mathbf{R_{K_n}}$, $Tr((f_n^2(q_n\mathbf{h_1} + f_n^1\mathbf{h}_2)) = Tr(q_n f_n^2 \mathbf{h}_1 + f_n^1 f_n^2 \mathbf{h}_2) \equiv 0$ *mod* q_n, since $f_n^1 f_n^2 \in q_n\mathbf{R_{K_n}}$. Then $\mathbf{Q} \subset \mathbf{L}_2$. Since $f_n^2 = \Sigma_{i=1}^s m_i \mathbf{x}_n^i$ is a linear combination of $\mathbf{x}_n^1, \ldots, \mathbf{x}_n^s$ with integer coefficients, then $Tr(\mathbf{x}_n^i \cdot \mathbf{y}) \equiv 0$ *mod* q_n, for $i = 1, \ldots, s$, implies that $Tr(f_n^2 \mathbf{y}) \equiv 0$ *mod* q_n. Then $\mathbf{L}_1 \subset \mathbf{L}_2$. The probability $Prob(\mathbf{e} \in \mathbf{L}_1)$ that $\mathbf{e} \in \mathbf{L}_1$ can be lower bounded by Theorem 4.1 since $\frac{\mathbf{x}_n^s}{q_n}$, $i = 1, \ldots, s$ are in $\mathbf{L}_1^\vee$. The inequality $Prob(\mathbf{e} \in \mathbf{L}_1) \geq \frac{d_n^{C_4}}{|\mathbf{R_{K_n}}/\mathbf{L}_2|}$ follows from the conditions 1), 2) and 3). Here the key point of applying Theorem 4.1 is as follows. The number of $\mathbf{x} \in \mathbf{L}_1$ satisfying the condition

$$||\mathbf{x}||_{tr} \leq \frac{\sqrt{c_1}}{\sqrt{\pi}\sigma}$$

can be counted directly and at least $\frac{q^s}{d^w}$ where w is a fixed positive integer depending on s, C and $\prod_{i=1}^s s^s ||\mathbf{x}_n^i||_{tr}$.

5 Number theory

The following proposition is useful in this paper. Please refer to [18, 7] for the proof.

Proposition 5.1. *Let $\mathbf{K} = \mathbf{Q}[\alpha]$ be a number field of degree n and $f(T) \in \mathbf{Q}[T] = a_n T^n + a_{n-1}T^{n-1} + \cdots + a_T + a_0$ be the minimal polynomial of α. Write*

$$f(T) = (T - \alpha)(c_{n-1}T^{n-1} + \cdots + c_1(\alpha)T + c_0(\alpha))$$

where $c_j(\alpha) = \Sigma_{i=j+1}^{n} a_i \alpha^{i-j-1}$. The dual base of $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ relative to the trace product is

$$\{\frac{c_0(\alpha)}{f'(\alpha)}, \frac{c_1(\alpha)}{f'(\alpha)}, \ldots, \frac{c_{n-1}(\alpha)}{f'(\alpha)}\}$$

.

Proposition 5.2. *Let $\mathbf{K} = \mathbf{Q}[\theta]$ be a number field, where θ is an algebraic integer whose monic minimal polynomial is denoted by $f(X)$. Then for any prime p not dividing $|\mathbf{R_K}/\mathbf{Z}[\theta]|$ one can obtain the prime decomposition of $p\mathbf{R_K}$ as follows. Let $f(X) \equiv \prod_{i=1}^{g} f_i(X)^{e_i}$ mod p be the decomposition of $f(X)$ module p into irreducible factors in $\mathbf{F}_p[X]$ where f_i are taken to be monic. Then*

$$p\mathbf{R_K} = \prod_{i=1}^{g} \mathbf{P}_i^{e_i},$$

where

$$\mathbf{P}_i = (p, f_i(\theta)) = p\mathbf{R_K} + f_i(\theta)\mathbf{R_K}.$$

Furthermore the residual index of $\mathbf{P}_i$ is equal to the degree of f_i.

The main construction in Theorem 3.2 is as follows. There should be many very short lattice vectors in the dual $\mathbf{L}_1^{\vee}$ of the number field lattice $\mathbf{L}_1$ satisfying $q\mathbf{R}_{\mathbf{K_d}} \subset \mathbf{L}_1 \subset \mathbf{R}_{\mathbf{K_q}}$. Let $\mathbf{x}_1, \ldots, \mathbf{x}_t$ are t elements in $\mathbf{R_K}^{\vee}/q\mathbf{R_K}^{\vee}$, we define a number field lattice $\mathbf{L}(\mathbf{x}_1, \ldots, \mathbf{x}_t)$ by the equations $Tr(\mathbf{x}_i \cdot \mathbf{y}) \equiv 0$ *mod* q, where $\mathbf{y} \in \mathbf{R_K}$, and $i = 1, \ldots, t$. It is obvious $q\mathbf{R_K} \subset \mathbf{L}(\mathbf{x}_1, \ldots, \mathbf{x}_t) \subset \mathbf{R_K}$. Moreover it is clear the definition of $\mathbf{L}(\mathbf{x}_1, \ldots, \mathbf{x}_t)$ only depends on the residue classes of $\mathbf{x}_i$'s in $\mathbf{R_K}^{\vee}/q\mathbf{R_K}^{\vee}$.

Proposition 5.3. *The vectors $\frac{\mathbf{x}_1}{q}, \ldots, \frac{\mathbf{x}_t}{q}$ are in the dual lattice*

$$\mathbf{L}(\mathbf{x}_1, \ldots, \mathbf{x}_t)^{\vee} \subset \frac{\mathbf{R_K}}{q}.$$

If $\mathbf{a} \in \mathbf{R_K}/q\mathbf{R_K}$ *is an invertible element, then there is a* $\mathbf{Z}/q\mathbf{Z}$ *linear isomorphism from* $\mathbf{L}(\mathbf{x}_1, \ldots, \mathbf{x}_t)$ *to* $\mathbf{L}(\mathbf{a}^{-1}\mathbf{x}_1, \ldots, \mathbf{a}^{-1}\mathbf{x}_t)$ *defined by* $\mathbf{y} \longrightarrow \mathbf{ay}$*. In particular the cardinalities of*

$$\mathbf{R_K}/\mathbf{L}(\mathbf{x}_1, \ldots, \mathbf{x}_t)$$

and

$$\mathbf{R_K}/\mathbf{L}(\mathbf{a}^{-1}\mathbf{x}_1, \ldots, \mathbf{a}^{-1}\mathbf{x}_t)$$

are the same.

Proof. The first conclusion is direct from the definition. The second conclusion is a simple computation.

Proposition 5.4 (from Theorem 2.13 in [50]). *Suppose that* p *is an odd prime and* f *is the smallest positive integer such that* $p^f \equiv 1 \bmod 2^n$*. Then* p *splits to* $\frac{2^{n-1}}{f}$ *distinct prime ideals in* $\mathbf{Q}(\xi_{2^n})$ *and each has residue degree* f*.*

Proposition 5.5. *Let* $\mathbf{C}$ *be the following circulant matrix over a finite ring* $\mathbf{R}$ *as follows*

$$\begin{pmatrix} c_0 & c_1 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-3} & c_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ c_1 & c_2 & \cdot & c_{n-1} & c_0 \end{pmatrix}$$

Let ω *be a* n*-th root of unity in* $\mathbf{R}$*. Set* $\mathbf{v} = (1, \omega, \omega^2, \ldots, \omega^{n-1})^\tau$*. Then* $\mathbf{C} \cdot \mathbf{v} = (c_0 + c_1\omega + c_2\omega^2 + \cdots + c_{n-1}\omega^{n-1})\mathbf{v}$*.*

Proof. It is easy to verify the following identity $(c_i, c_{i+1}, \ldots, c_{n-1}, c_0, \ldots, c_{i-1}) \cdot \mathbf{v} = c_i + c_{i+1}\omega + \cdots + c_{n-1}\omega^{n-i-1} + c_0\omega^{n-i} + \cdots + c_{i-1}\omega^{n-1} = (c_0 + c_1\omega + \cdots + c_{n-1}\omega^{n-1}) \cdot \omega^{n-i}$. The conclusion follows directly.

6 Ring-LWE and linear recurrence relations

From Theorem 4.2 the explicit construction of sublattice pairs with an ideal is equivalent to the problem about the special formation of some elements in the ideal $\mathbf{I}$ in the quotient ring $\mathbf{R}_q = \mathbf{F}_q[x]/(x^d + 1)$, where the dimension of $\mathbf{R}_q/\mathbf{I}$ over $\mathbf{F}_q$ is upper bounded by a positive integer. This is equivalent to a problem about the form of codewords in some nega-cyclic codes in $\mathbf{F}_q[x]/(x^d+1)$ with constant codimension over large but polynomially bounded finite fields $\mathbf{F}_q$. In coding theory and practice cyclic codes and quasi-cyclic code over small finite fields have been studied extensively. We refer to [15] for this problem and sublattice attacks on other number field sequences.

From Proposition 5.4 the two-to-power cyclotomic polynomial $x^{2^{n-1}}+1$ *mod* p where p is an odd prime satisfying that $p \equiv 1$ *mod* 2^n, has 2^{n-1} distinct roots in $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, these are primite 2^n-th root of unity in $\mathbf{F}_p$. Set a such a primitive 2^n-th root of unity in $\mathbf{F}_p$, then all primitive 2^n-th roots are the form a^j *mod* p where j takes over all odd positive integer in the range $1 \leq j \leq 2^n - 1$. Then we have

$$x^{2^{n-1}}+1 \equiv \prod_{1\leq j \leq 2^n, j odd} (x-a^j).$$

From Theorem 4.2 again when $f_n(x) = x^{2^{n-1}}+1$, $d = 2^{n-1}$ goes to the infinity if we can find $d - H_1$ factors among $x-a$, $x-a^3$, $x-a^5$, $\ldots$, $x - a^{2^n-1}$, where H_1 is a fixed positive integer not depending on n, such that the product $F_n = u(x)\prod_{i=1}^{d-C}(x-a^{j_i})$, where $u(x)$ is a degree u polynomial in $\mathbf{F}_p[x]$ such that $u(a^j)$'s are not zero in $\mathbf{F}_p$ for $j = 1, 3, \ldots, 2^n-1$, satisfying the following condition, then the desired f_1 and f_2 in Theorem 3.2 can be constructed.

Condition A. There exists a polynomial $T_n(x) \in \mathbf{F}_p[x]$ such that
1.The degree of T_n is bounded, that is, $\deg(T_n) \leq H_2$, where H_2 is a fixed positive integer;
2. T_nF_n is not zero in $\mathbf{F}_p[x]/(f_n(x))$;
3.T_nF_n can be expressed as a linear combination over $\mathbf{F}_p$ of bounded number H_3 of terms x^{l_i}, where $l_i \in \{0, 1, \ldots, x^{2^{n-1}}\}$. That is

$$T_n(x)F_n(x) = \Sigma_{i=1}^{H_3} m_i x^{l_i},$$

where $1 \leq l_i \leq 2^{n-1}$ and H_3 is a fixed positive integer.

The condition 3 is equivalent to a linear recurrence relation of the coefficients of F_n. The condition 2 is equivalent to a non-trivial linear recurrence relation that T_n can not contain all factors $x - a^{j'}$ where j' takes over all elements of the set $\mathbf{C} = \{1, 3, \ldots, 2^n-1\} - \{j_1, \ldots, j_{d-C}\}$. When such F_n is constructed, we take $f_2(x)$ in Theorem 3.1 as $T_n(x)F_n(x)$. Then

$f_1(x) \equiv \prod_{j'_i \mathbf{C}}(x - a^{j'_i})$ *mod* p. It is easy to verify that $f_1(\xi_{2^n})$ and $f_2(\xi_{2^n})$ satisfy the condition of Theorem 3.2, if $Tr(F_n(\xi_{2^n})T_n(\xi_{2^n}) \cdot \mathbf{x}) \equiv 0$ *mod* p for $\mathbf{x} \in \mathbf{R_{K_n}}$, defines an index p sublattice in $\mathbf{R_{K_n}}$. This will be achieved by the property $m_1, \ldots, m_{H_3}$ are not zero in $\mathbf{F}_p$.

Let $\mathbf{K}_n = \mathbf{Q}[x]/(f_n(x)) = \mathbf{Q}[\theta_n]$, where f_n is a monic irreducible polynomial in $\mathbf{Z}[x]$ with degrees $d_n = \deg(f_n)$ goes to the infinity, be a sequence of monogenic number fields. The ring of integers in number field $\mathbf{K_n}$ is denoted by $\mathbf{R_{K_n}}$. We observe that the following conditions are satisfied for the cyclotomic number fields.

Condition B. $||\theta_n||_{tr} \leq d_n^{C_1}$ where C_1 is a fixed positive integer;

Condition C. $|f'_n(\theta_{n,j}| \leq d_n^{C_2}$, where $\theta_{n,j}$, $j = 1, 2, \ldots, d_n$ are d_n roots of f_n in the complex number field, and C_2 is a fixed positive integer.

Theorem 6.1. *Let $\mathbf{K}_n = \mathbf{Q}[x]/(f_n(x))$, where f_n is a monic irreducible polynomial in $\mathbf{Z}[x]$ with degrees $d_n = \deg(f_n)$ goes to the infinity, be a sequence of monogenic number fields satisfying the above Condition B and C. We consider the decision dual Ring-LWE over $\mathbf{R_{K_n}}^{\vee}$ and suppose that the width of the Gaussian distribution of errors satisfies $\frac{\sqrt{d_n}}{\lambda_1(\mathbf{R_{K_n}})} \leq \sigma \leq d_n^{C_3}$, where C_3 is a fixed positive integer. Let $d_n^{C_4} \leq p_n \leq d_n^{C_5}$ be a sequence of polynomially bounded prime modulus parameters, where C_4 and C_5 are two fixed positive integers. If there exists a non-zero*

$$F_n(x) = x^{d_n+u-H_1} + a_{d_n-H_1-1} + \cdots + a_0$$

of $\mathbf{F}_{p_n}[x]/(f_n(x))$ satisfying $F_nG_n = 0$ in $\mathbf{F}_{p_n}[x]/(f_n(x))$, where G_n is a polynomial satisfying $\deg(G_n) \leq H_4$, H_4 is a fixed positive integer. Suppose that
1) For each n, F_n satisfies Condition A;
2) $Tr(\theta_n^{l_i} \cdot \mathbf{x}) \equiv 0$ mod p_n, $\mathbf{x} \in \mathbf{R_{K_n}}$, $i = 1, \ldots, H_3$ define an index $p_n^{H_3}$ sublattice $\mathbf{L}_{n.1}$ of $\mathbf{R_{K_n}}$;
3) $Tr(T_n(\theta_n)F_n(\theta_n) \cdot \mathbf{x}) \equiv 0$ mod p_n defines an index p_n sublattice $\mathbf{L}_{n,2}$ of $\mathbf{R_{K_n}}$;
4) $H_3^{H_3} \prod_{i=1}^{H_3} ||\theta_n^{l_i}||_{tr} \leq d_nC_4 - H_3C_1 - C_2 - C_6$ where C_6 is a fixed positive integer.

Then $(\mathbf{L}_{1,n}, \mathbf{L}_{n,2})$ is a sublattice pair with an ideal $\mathbf{Q}_n = (p_n, G_n(\theta_n))$ to the dual Ring-LWE over $\mathbf{R_{K_n}}^{\vee}$. Moreover Condition A means a bound-

ed (by H_2) term non-trivial linear recurrence relation on the coefficients $a_{d_n-H_1-1}, \dots, a_0$.

Proof. Set $T_n(x) = c_{H_2}x^{H_2} + c_{H_2-1}x^{H_2-1} + \cdots + c_1x + c_0$. Then the coefficient of $x^{d_n+u-H_1-i}$, $1 \leq i \leq d_n - H_1 - H_2$, in $T_n(x)F_n(x)$ is

$$c_0a_{d_n+u-H_1-i} + c_1a_{d_n+u-H_1-i-1} + \cdots + c_{H_2}a_{d_n+u-H_1-H_2-i}.$$

If these coefficients $c_0a_{d_n+u-H_1-i}+c_1a_{d_n+u-H_1-i-1}+\cdots+c_{H_2}a_{d_n+u-H_1-H_2-i} \equiv 0 \ mod \ p_n$, are vanished except the first H_3 terms or last H_3 terms, then the condition 3 in Condition A is automatically satisfied. The condition 2 in Condition A means that such linear recurrence relations do not lead to a factor f_n in T_nF_n. The other conclusions follows from Theorem 3.2 and Condition C about "tweak factors" between dual and non-dual version directly.

From Theorem 6.1 the existence of a sublattice pair with an ideal for the dual Ring-LWE over monogenic number fields satisfying Condition B+C can be proved from a non-trivial bounded term linear recurrence relation in $\mathbf{F}_{p_n}$ for the coefficients of some $d_n - H_1$ degree factor $F_n(x)$ of $f_n(x) \in \mathbf{F}_{p_n}[x]$, where H_1 is a fixed positive integer when d_n goes to the infinity. Hence from Theorem 3.1 decision dual Ring-LWE can be solved in (classical) polynomial time if such a non-trivial bounded term linear recurrence relation can be constructed. These linear recurrence relations are not so difficult for monogenic number fields. Hence the decision dual Ring-LWE over monogenic number fields are not so hard from the view of our sublattice pair attack.

Lemma 6.1 *We consider the modulus parameter $p_n \equiv 1 \ mod \ 2^n$ and $a \in \mathbf{F}_{p_n}$ is a primitive 2^n-th root of unity in $\mathbf{F}_{p_n}$ as above. Set*

$$F_{n,i_i,t_i} = \frac{x^{2^{n-1}} - a^{2^{n-1}}}{x^{2^{t_i}} - a^{j_i2^{t_i}}},$$

where j_i's are odd positive integers, t_i's are smaller than a fixed positive integer. Let

$$F_n(x) = w_{j_1}F_{n,j_1,t_1} + \cdots + w_{H_1}F_{n,j_{H_1},t_{H_1}}$$

be a linear combination of H_1 non-zero polynomials $F_{n,j_1,t_1}, F_{n,j_2,t_2}, \dots,$ $F_{n,j_{H_1},t_{H_1}} \in \mathbf{F}_{p_n}[x]/(f_n(x))$ with invertible elements $w_1, \dots, w_{j_{H_1}} \in \mathbf{R_{K_n}}/p_n\mathbf{R_{K_n}}$. We assume that one root ω of one denominator $x^{2^{t_1}} - a^{j_12^{t_1}}$ is not root of other denominators $x^{2^{t_2}} - a^{j_22^{t_2}}, \dots, x^{2^{t_{H_1}}} - a^{j_12^{t_{H_1}}}$. Then $F_n(x)$ is a non-zero element in $\mathbf{F}_{p_n}[x]/(f_n(x))$. If $T_n(x)$ is a polynomial in $\mathbf{F}_{p_n}[x]$ such that

$T_n(\omega)$ is not zero in $\mathbf{F}_{p_n}$, then $T_n(x)F_n(x)$ is not zero in $\mathbf{F}_{p_n}[x]/(f_n(x))$.

Proof. ω is not a root of $F_{n,j_1,t_1}(x)$. However it is a root of all $F_{n,j_2,t_2}, F_{n,j_3,t_3}, \ldots, F_{n,j_{H_1},t_{H_1}}$ in $\mathbf{F}_{p_n}$ since ω is not a root of denominators $x^{2^{t_2}} - a^{j_2 2^{t_2}}, \ldots, x^{2^{t_{H_1}}} - a^{j_1 2^{t_{H_1}}}$. Then this root is not a root of $F_n(x)$ and F_n is not zero in $\mathbf{F}_{p_n}[x]/(f_n(x))$.

On the other hand, if $T_n(x)$ is a polynomial in $\mathbf{F}_{p_n}[x]$ such that $T_n(\omega)$ is not zero in $\mathbf{F}_{p_n}$, then $T_n(x)F_n(x)$ is not zero in $\mathbf{F}_{p_n}[x]/(f_n(x))$. Actually we have $T_n(\omega)F_n(\omega) = w_{j_1}T_n(\omega)F_{n,j_1,t_1}(\omega)$. This is not zero in $\mathbf{F}_{p_n}$. Hence $T_n(x)F_n(x)$ can not have all $a, a^3, \ldots, a^{2^n-1}$ as its roots. This leads to non-trivial linear recurrence relations.

If we want a linear recurrence relation on a degree $2^{n-1}-1$ factor

$$F_{n,j}(x) = \frac{x^{2^{n-1}} - a^{j2^{n-1}}}{x - a^j} = x^{2^{n-1}-1} + a^j x^{2^{n-1}-2} + \cdots + a^{j(2^{n-1}-2)}x + a^{j(2^{n-1}-1)}$$

of $f_n(x)$, where j is a positive odd number $1 \leq j \leq 2^n - 1$, it is a trivial linear recurrence relation. Suppose that we have a $T_n(x) = c_{H_2}x^{H_2} + \cdots + c_0$ satisfying the linear recurrence relation

$$c_0 a^{j(2^{n-1}-i-1)} + c_1 a^{j(2^{n-1}-i-2)} + \cdots + c_{H_2} a^{j(2^{n-1}-i-1-H_2)} = 0,$$

then $T_n(a^j) = 0$. Hence this linear recurrence relation leads to a factor $x^{2^{n-1}} + 1$ of $T_n(x)F_n(x)$. This is a trivial linear recurrence relation.

We observe the case of the linear combination of several degree $2^{n-1}-1$ factors $F_n(x) = w_1F_{n,j_1} + \cdots + w_hF_{n,j_h}$, where $w_1, \ldots, w_h \in \mathbf{F}_{p_n}$. Suppose that there exists an odd positive integer j_0 in the range $1 \leq j_0 \leq 2^n - 1$ satisfying that $j_l - j_0$ can be divisible by 2^{n-C}, where C is a fixed positive integer and $l = 1, \ldots, h$. We want to check a linear recurrence relation $T_n(x)$ on this $F_n(x)$ using 2^C coefficients. First of all the coefficient of $F_n(x)$ is of the form

$$(w_1 a^{(j_1-j_0)i} + \cdots + w_h a^{(j_h-j_0)i})a^{j_0 i},$$

where i takes positive integers from 1 to $2^{n-1}-1$. We observe that

$$w_1 a^{(j_1-j_0)i} + \cdots + w_h a^{(j_h-j_0)i}$$

is of period 2^C from the condition than $j_i - j_0$ can be divisible by 2^{n-C}. Hence a linear recurrence relation $T_n(x)$ on these coefficients $(w_1 a^{(j_1-j_0)i} +$

$\cdots + w_h a^{(j_h-j_0)i})a^{j_0 i}$ corresponds to a non-zero solution of the following circulant $2^C \times 2^C$ matrix $\mathbf{C}$ over $\mathbf{F}_{p_n}$.

$$\begin{pmatrix} \Sigma_{l=1}^h w_i & \Sigma_{l=1}^h w_l a^{j_l-j_0} & \cdots & \Sigma_{l=1}^h w_l a^{(j_l-j_0)(2^C-1)} \\ \Sigma_{l=1}^h w_l a^{(j_l-j_0)(2^C-1)} & \Sigma_{l=1}^h w_l & \cdots & \Sigma_{l=1}^h w_l a^{(j_l-j_0)(2^C-2)} \\ \cdots & \cdots & \cdots & \cdots \\ \Sigma_{l=1}^h w_l a^{j_l-j_0} & \Sigma_{l=1}^h w_l a^{2(j_l-j_0)} & \cdots & \Sigma_{l=1}^h w_l \end{pmatrix}$$

If $\mathbf{c}' = (c'_{2^C-1}, c_{2^C-2}, \ldots, c'_0)^\tau$ is a non-zero solution of the equation $\mathbf{C} \cdot \mathbf{c}' = 0$, set $c_i = \frac{c'_i}{a^{j_0 i}}$, then $T_n(x) = \Sigma_{i=0}^{2^C-1} c_i x^i$ is such a linear recurrence relation.

Set $\omega \in \mathbf{F}_{p_n}$ a primitive 2^C-th root of unity in $\mathbf{F}_{p_n}$, when $p_n \equiv 1$ *mod* 2^C. Then 2^C vectors $(1, \omega^i, \omega^{2i}, \ldots, \omega^{((2^C-1)i})^\tau$, $i = 0, 1, \ldots, 2^C-1$ are linear independent and span the space $\mathbf{F}_{p_n}^{2^C}$. From Proposition 5.5 over $\mathbf{F}_{p_n}$ the linear space *span*$(\mathbf{C})$ spanned by the rows of $\mathbf{C}$ is orthogonal to these vectors $(1, a^s, \ldots, a^{s(2^C-1)})$ where s takes over all integers which can be divisible by 2^{n-C} and not of the form $j_0 - j_l$, $l = 1, \ldots, h$. From Proposition 5.5 over $\mathbf{F}_{p_n}$ again, the dimension of *span*$(\mathbf{C})$ is h, then *span*$(\mathbf{C})$ is the linear span of h vectors $(1, a^{j_0-j_l}, \ldots, a^{(j_0-j_l)(2^C-1)})$, $l = 1, \ldots, h$. Unfortunately h vectors $(1, a^{j_l-j_0}, \ldots, a^{(j_l-j_0)(2^C-1)})$, $l = 1, \ldots, h$ are in the linear space *span*$(\mathbf{C})$ spanned by the rows of $\mathbf{C}$. Hence we conclude that $T_n(a^{j_l}) = 0$ in $\mathbf{F}_{p_n}$ for $l = 1, \ldots, h$. Then only a trivial linear recurrence relation such that $T_n(x)F_n(x)$ containing $f_n(x)$ as a factor can be found in this case.

7 Proofs of main results

Proof of Theorem 3.1. First of all the probability that uniformly chosen $\mathbf{a} \in \mathbf{R_K}/q\mathbf{R_K}$ is in the ideal $\mathbf{Q}/q\mathbf{R_K}$ is at least $\frac{1}{d^{C_3}}$ from the condition 2 of the sublattice pair with the ideal $\mathbf{Q}$. We take the d^C samples $(\mathbf{a}, \mathbf{b})$'s from the Ring-LWE equation satisfy $\mathbf{a} \in \mathbf{Q}/q\mathbf{R_K}$. This can be achieved within time complexity $O(d^{2(C+C_3)})$ by checking the algebraic condition $\mathbf{a} \in \mathbf{Q}/q\mathbf{R_K}$ when $\mathbf{Q}$ is explicitly given.

Since $\mathbf{a} \in \mathbf{Q}/q\mathbf{R_K}$ then $\mathbf{a} \cdot \mathbf{s} \in \mathbf{Q}/q\mathbf{R_K} \subset \mathbf{L}_2/q\mathbf{R_K}$ for arbitrary unknown secret $\mathbf{s}$ from the condition 3) of the sublattice pair. Hence for the d^C samples

$(\mathbf{a},\mathbf{b})$'s from the Ring-LWE equation satisfy $\mathbf{a} \in \mathbf{Q}/q\mathbf{R_K}$, the probability that $\mathbf{b} \in \mathbf{L}_2$ is bigger than the probability $Prob(\mathbf{e} \in \mathbf{L}_1)$, since $\mathbf{L}_1 \subset \mathbf{L}_2$ and $\mathbf{a}\cdot\mathbf{s}+\mathbf{e} \in \mathbf{L}_2$ from the fact $\mathbf{a}\cdot\mathbf{s} \in \mathbf{L}_2$. Then for these d^C samples $(\mathbf{a},\mathbf{b})$'s from the Ring-LWE equation satisfy $\mathbf{a} \in \mathbf{Q}/q\mathbf{R_K}$, the probability that $\mathbf{b} \in \mathbf{L}_2$ is bigger than

$$Prob(\mathbf{e} \in \mathbf{L}_1) \geq \frac{d^{C_4}}{|\mathbf{R_K}/\mathbf{L}_2|} \geq \frac{2}{|\mathbf{R_K}/\mathbf{L}_2|}.$$

One the other hand we look at $(\mathbf{a},\mathbf{b})$ uniformly distributed samples in

$$\mathbf{R_K}/\mathbf{Q} \times \mathbf{R_K}/\mathbf{L}_2.$$

For any fixed first coset, the second components $\mathbf{b}$'s have to be equally distributed in $\mathbf{R_K}/\mathbf{L}_2$. Therefore by checking the algebraic condition $\mathbf{b} \in \mathbf{L}_2$ for these d^C samples $(\mathbf{a},\mathbf{b})$'s from the Ring-LWE equation satisfy $\mathbf{a} \in \mathbf{Q}/q\mathbf{R_K}$, we can distinguish from these uniformly chosen $(\mathbf{a},\mathbf{b})$ within time complexity $O(d^{4C_3})$.

Another proof can be given as follows. We consider the secret $\mathbf{s} \in \mathbf{Q}$, this happens with a probability at least $\frac{1}{d^{C_3}}$. For such a secret, given d^C samples $(\mathbf{a},\mathbf{b})$, we have

$$\mathbf{a} \cdot \mathbf{s} \in \mathbf{Q} \subset \mathbf{L}_2.$$

The probability that $\mathbf{b} \in \mathbf{L}_2$ is bigger than the probability $Prob(\mathbf{e} \in \mathbf{L}_1)$ that $\mathbf{e} \in \mathbf{L}_1$ since $\mathbf{L}_1 \subset \mathbf{L}_2$. Then for these d^C samples $(\mathbf{a},\mathbf{b})$'s, the probability that $\mathbf{b} \in \mathbf{L}_2$ is bigger than

$$Prob(\mathbf{e} \in \mathbf{L}_1) \geq \frac{d^{C_4}}{|\mathbf{R_K}/\mathbf{L}_2|} \geq \frac{2}{|\mathbf{R_K}/\mathbf{L}_2|}.$$

This can be distinguished from the uniformly distributed d^C samples.

Proof of Theorem 3.2. We consider the two-to-power cyclotomic field $\mathbf{K}_n = \mathbf{Q}[\xi_{2^n}] = \mathbf{Q}[x]/(f_n)$, $f_n = x^{2^{n-1}} + 1$. Let p_n be an sufficiently large polynomially bounded odd prime number satisfying $p_n \equiv 1 \ mod\ 2^n$, where we will control its size later. From Proposition 5.4 there exists a $a \in \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ such that $a^{2^{n-1}}+1 \equiv 0 \ mod\, p$. Hence it is easy to verify that $a^j \in \mathbf{F}_{p_n}$, where j is an odd positive integer, satisfies $(a^j)^{2^{n-1}} \equiv -1 \ mod\, p_n$. There are $d_n = 2^{n-1}$ such odd positive integers and the ideal $p_n\mathbf{R_{K_n}}$ is completely splits to the product of d_n prime ideals $(p_n, x-a^j)$, $j = 1, 3, \ldots, 2^n-1$.

We use non-zero elements of the forms

$$F_n(x) = w_1 F_{n,j_1}(x) + \cdots + w_h F_{n,j_h}(x) \in \mathbf{F}_{p_n}[x]/(f_n(x)),$$

where $w_1, \ldots, w_h$ are h constants in $\mathbf{F}_{p_n}$, and there exists an odd positive integer j_0 in the range $1 \leq j_0 \leq 2^n - 1$ satisfying that $j_l - j_0$ can be divisible by 2^{n-C}, C is a fixed positive integer and $l = 1, \ldots, h$ to construct linear recurrence relations of period $2^C + 1$. As indicated in Lemma 6.1 $F_n(x)$ is a non-zero element in $\mathbf{F}_{p_n}[x]/(f_n(x))$ and contains a factor of $f_n(x)$ with degree bigger than or equal $2^{n-1} - C$ from Lemma 6.1. Hence the element $G_n(x)$ in Theorem 6.1 can be constructed directly from these primitive 2^n-th roots of unity in $\mathbf{F}_{p_n}$.

Set

$$A_0 = \Sigma_{l=1}^{h} w_i,$$

$$A_1 = \Sigma_{l=1}^{h} w_l a^{j_l - j_0},$$

$$\cdots,$$

$$A_{2^C-1} = \Sigma_{l=1}^{h} w_l a^{(j_l - j_0)(2^C-1)}.$$

Comparing with the argument in the previous section, we use $2^C + 1$ coefficients. The $2^C \times (2^C + 1)$ matrix $\mathbf{D}$ defining the linear recurrence relation is as follows.

$$\begin{pmatrix} A_0 & A_1 & \cdots & A_{2^C-1} & A_0 \\ A_{2^C-1} & A_0 & \cdots & A_1 & A_{2^C-1} \\ \cdots & \cdots & \cdots & \cdots & \\ A_1 & A_2 & \cdots & A_0 & A_1 \end{pmatrix}$$

It is clear that for a non-zero vector $\mathbf{c} = (c_{2^C-1}, \ldots, c_1, c_0)^\tau$ satisfying

$$\mathbf{C} \cdot c = 0,$$

where $\mathbf{C}$ is the following matrix as in Section 5.

$$\begin{pmatrix} A_0 & A_1 & \cdots & A_{2^C-1} \\ A_{2^C-1} & A_0 & \cdots & A_1 \\ \cdots & \cdots & \cdots & \cdots \\ A_1 & A_2 & \cdots & A_0 \end{pmatrix}$$

The vector $\mathbf{u} = (u_{2^C}, u_{2^C-1}, \ldots, u_0, u_1)^\tau$ satisfying

$$u_{2^C} + u_0 = c_{2^C-1},$$

$$u_{2^C-1} = c_{2^C-2},$$

$$\cdots\cdots,$$

$$u_1 = c_0.$$

is a solution of

$$\mathbf{D} \cdot \mathbf{u} = 0.$$

Set $u'_i = \frac{u_i}{a^{j_0 i}}$ as in Section 5, the polynomial $T'_n(x) = \Sigma_{i=0}^{2^C} u'_i x^i$ is a linear recurrence on $F_n(x)$. Though $T_n(a^{j_l}) = 0$ for $l = 1, 2, \ldots, h$. From the above relation we can choose suitable u_{2^C} and u_0 such that

$$T'_n(a^{j_l}) \neq 0$$

for $l = 1, 2, \ldots, h$. Hence we get a non-trivial linear recurrence relation of period $2^C + 1$.

The conditions 1) and 2) in Theorem 6.1 are satisfied automatically since p_n is a prime number and the formation of $T_n(x)F_n(x)$. Since we only require that p_n is a prime number satisfying $p_n \equiv 1 \ mod \ 2^n$, we can find a sufficiently large polynomially bounded prime number p_n satisfying the condition 3) and 4) in Theorem 6.1. Hence sublattice pairs claimed in Theorem 6.1 can be constructed. The degree of $G_n(x)$ is denoted by t_1 and the number of terms in the $T_n(x)F_n(x)$ is denoted by t_2. From the above argument these two numbers can be independent of p_n when a suitable h and C are fixed.

8 The algorithm

We give the algorithm combining Theorem 3.1 and Theorem 3.2.

From given C_1, C_2 in Conditions B and C, in the case of two-to-power cyclotomic polynomial $f_n(x) = x^{2^{n-1}} + 1$, $C_1 = C_2 = 1$, and given C_3 determining the width of the error distribution, fix t_1 and t_2 as in the proof of Theorem 6.1, we calculate a large C_4 to satisfy the condition 3) and 4) in Theorem 6.1. Then for an polynomially bonded prime number $d_n^{C_4} \leq p_n$ satisfying $p_n \equiv 1 \ mod \ 2^n$ we execute the following algorithm.

Step 1. Find a non-trivial linear recurrence relation $T_n'(x)$ as in the proof of Theorem 6.1. Set $\mathbf{y} = T_n'(x)(F_n(x)$. Find $G_n(x)$ as in Theorem 6.1. Set $\mathbf{Q}_n$ the ideal generated by $G_n(x)$ and p_n. This can be done within time complexity $O(2^{2t_3})$.

Step 2. Define the sublattice $\mathbf{L}_2 \subset \mathbf{R}_{\mathbf{K_n}}$ by $Tr(\mathbf{x} \cdot \mathbf{y}) \equiv 0 \ mod \ p_n$ for $\mathbf{x} \in \mathbf{R}_{\mathbf{K_n}}$ and the auxiliary sublattice $\mathbf{L}_1 \subset \mathbf{R}_{\mathbf{K_n}}$ by $Tr(\mathbf{x} \cdot \xi_{2^n}^{j_i}) \equiv 0 \ mod$ p_n for $\mathbf{x} \in \mathbf{R}_{\mathbf{K_n}}$, where j_i are the degrees of monomials x_i^j appearing in the polynomial $T_n(x)'F_n(x)$.

Step 3. For given polynomially bounded many samples $(\mathbf{a}_1, \mathbf{b}_i)$, $i = 1, \ldots, p_n^{2+t_1}$, we find at least $\frac{p_n^{2+t_1}}{p_n^{t_1}}$ samples $\mathbf{a}_i$'s which are in the ideal $\mathbf{Q}_n$. It is within the time $O(p_n^{2t_1})$.

Step 4. For these p_n^2 samples $(\mathbf{a}, \mathbf{b})$'s with the first component $\mathbf{a} \in \mathbf{Q}_n$ we check the probability $\mathbf{b} \in \mathbf{L}_2$. If these samples are not from the Ring-LWE equation this probability is $\frac{1}{|\mathbf{R}_{\mathbf{K_n}}/\mathbf{L}_2|} = \frac{1}{p_n}$. If it is from the Ring-LWE equation, this probability is bigger than the probability $Prob(\mathbf{e} \in \mathbf{L}_1)$ that $\mathbf{e} \in \mathbf{L}_1$. Since

$$Prob(\mathbf{e} \in \mathbf{L}_1) \geq \frac{2}{|\mathbf{R}_{\mathbf{K}}/\mathbf{L}_2|},$$

we can distinguish within time complexity $O(p_n^8)$.

Important notice for implementation. To implement this algorithm we need to construct the sublattice pair with the ideal **explicitly**. Then we choose a secret in the ideal and to test samples from the Ring-LWE equations module the sublattice $\mathbf{L}_2$. Here a large polynomially bounded module parameter should be chosen according to the requirement of Theorem 3.2.

9 Conclusion

In this paper we propose a general theory of sublattice pair attacks on the Ring-LWE with arbitrary error distributions. This sublattice pair attack is applied to the Ring-LWE with Gaussian error distributions over two-to-power fields. Then it is proved that for two-to-power cyclotomic fields such sublattice pairs can be constructed and hence sublattice attacks from sublattice pairs can be achieved. We prove that the decision Ring-LWE over two-to-power fields with wide error distributions of widths in the range of Peikert-Regev-Stephens-Davidowitz hardness reduction results can be solved by a polynomial time algorithm. Then from the hardness reduction results the approximating ideal-$SIVP_{poly(d)}$ with some polynomial factors for ideal lattices in two-to-power cyclotomic fields can be solved within quantum polynomial time. Therefore lattice based cryptographic constructions can not be based on the "hardness" of the present form Ring-LWE over two-to-power cyclotomic integers even in the classical computation model. The further sublattice attacks on Ring-LWE over general cyclotomic fields with wide errors will be presented in [15]. Practical sublattice attack can be adapted from the construction of sublattice pairs with ideals according to the width and the construction in the proof of Theorem 6.1 and Theorem 3.2. The optimization of the lower bounds in Theorem 4.1 and Theorem 6. 1 and the better polynomially bounded modulus parameters will be given in [15].

References

[1] S. Arora and R. Ge, New algorithms for learning in the presence of errors, ICALP 2010, LNCS 6755, 403-415, 2011.

[2] M. R. Albrecht, On dual lattice attack against small-secret LWE and parameter choices in HElib and SEAL, Eurocrypt 2017, LNCS 10211, 103-219, 2017.

[3] M. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, S. Halevi, J. Hoffstein, K. Laine, K. Lauter, S. Lokam, D. Micciancio, D. Moody, T. Morrison, A. Sahai and V. Vaikuntanathan, Homomorphic encryption standard, Cryptology ePrint, 2019/939, 2019.

[4] M. R. Albrecht and A. Deo, Large Modulus Ring-LWE Module-LWE. Asiacrypt 2017, 267-296, 2017.

[5] M. Ajtai, The shortest vector problem in L_2 is NP-hard for randomized reduction, STOC 1998, 10-19, 1998.

[6] A. Blum, A. Kalai and H. Wasserman, Noise-tolarant learning, the parity problem, and statistical query model, J. ACM, **50**, no.4, 506-519, 2003.

[7] A. I. Borevich and I. R. Shafarevich, Number theory, Transalted from the Russian by Newcomb Greenleaf, Pure and Applied Mathematics,Vol. 20, Academic Press, New York, London, 1966.

[8] Z. Brakerski, A. Langlois, C. Peikert, O. Regev and D. Stehlé, Classical hardness of learning with errors, STOC 2013, 575-584, 2013.

[9] Z. Brakerski and R. Perlman, Order-LWE and hardness of Ring-LWE with entropic secrets, Cryptology ePrint Archive 2018/494, 2018.

[10] W. Castryck, I. Illashenko and F. Vercauteren, Provable weak instances of Ring-LWE revisted, Eurcocrypt 2016, 147-167, 2016.

[11] Hao Chen, Sublattice attacks on LWE over arbitrary number field lattices, Cryptology ePrint Achive 2019/791, 2019.

[12] Hao Chen, Sublattice attacks on Ring-LWE with wide error distributions I, Cryptology ePrint Achive 2020/440, 2020.

[13] Hao Chen, Approximating ideal-$SVP_{poly(n)}$ with preprocessing in two-to-power cyclotomics is not hard in quantum computation model, Preprint 2019.

[14] Hao Chen, On approximation $SVP_{poly(n)}$ with preprocessing for ideal lattices in quantum computation model, Preprint 2019.

[15] Hao Chen, Sublattice attacks on Ring-LWE with wide error distributions III, in preparation, 2020.

[16] H. Chen, K. Lauter and K. E. Stange, Security consideration for Galois non-dual RLWE families, SAC 2061, LNCS, 10532, pp. 432-462, and the full version: Vulnerable Galois RLWE families and improved attackes, Cryptology ePrint Achive 2016/193.

[17] H. Cohen, A course in computational number theory, GTM 138, Springer-Verlag, 1993.

[18] K. Conrad, The different ideal, http://www.math.uconn.edu/kconrad/.

[19] R. Cramer, L. Ducas, C. Peikert and O.Regev, Recovering short generators of principle ideals in cyclotomic rings, Eurocrypt 2016, 559-585, 2016.

[20] R. Cramer, L. Ducas and B. Wesolowski, Short Stickelberger relations and application to ideal-SVP, Eurocrypt 2017, 324-348, 2017.

[21] L. Ducas, M. Plançon and B. Wsolowski, On the shortness of vectors to be found by the ideal-SVP quantum algorithm, Cryoto 2019, 322-351, 2019.

[22] Y. Eisentrage, S. Hallgren and K. Lauter, Weak instances of PLWE, SAC 2014, 183-194, 2014.

[23] Y. Elias, K. Lauter, E. Ozman and K. E. Stange, Provable weak instances of Ring-LWE, Crypto 2015, 63-92, 2015.

[24] P. M. Gruber, Convex and Discrete Geometry, Gurndlehren der mathematischen Wissenschaften 336, Springer-Verlag, Birlin Heidelberg 2007.

[25] S. Khot, Hardness of approximating the shortest vector problem, J. ACM, **52**, 789-808, 2005.

[26] S. Khot, Inapproximability results for computational problems of lattice, 453-473, The LLL algorithm, survey and application, edited by P. Q. Nguyen and B. Vallée, Springer, 2010.

[27] P. Kirchner and P-A. Fouque, An improved BKW algorithm for LWE with applications to cryptography and lattices, Crypto 2015, 43-62, 2015.

[28] C. Lee, A. Pellet-Mary, D. Stehlé and A. Wallet, An LLL algorithm for modulus lattices, Cryptology ePrint Archive 2019/1035, 2019.

[29] V. Lyubashevsky and D. Micciancio, Generalized compact knapsacks are collision ressitant, ICALP (2), 37-54, 2006.

[30] V. Lyubashevsky, D. Micciancio, C. Peikert and A. Rosen, SWIFT: A modest proposal for FFT hashing, FSE, 54-72, 2008.

[31] V. Lyubashevsky, C. Peikert and O. Regev, On ideal lattices and learning with errors over rings, J. ACM, **60**, 1-43, 2013, preliminary version, Eurocrypt 2010, 1-23, 2010.

[32] V. Lyubashevsky and C. Peikert and O. Regev, A toolkit for ring-LWE cryptography, Eurocrypt 2013, 35-54, 2013.

[33] D. Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one-way fucntions, Comp. Complex., 16(4), 365-411, 2007.

[34] D. Micciancio and O. Regev, Lattice-based cryptography, Book Chapter in Post-quantum Cryptography, D. J. Bernstein and J. Buchmann (eds.), Springer (2008).

[35] D. Micciancio and O. Regev, Worst-case to average-case reduction based on Gaussian measures, FOCS 2004, 372-381, 2004.

[36] D. Micciancio and S. Goldwasser, Complexity of lattice problems, A cryptographic perspective, Kluwer Academic Publishers.

[37] T. Mukherjee and N. Stephens-Davidowitz, Lattice reduction for modules, or how to reduce moduleSVP to moduleSVP, Crypto 2020, 213-242, 2020.

[38] C. Peikert, Public-key cryptosystmes from the worst case shortest lattice vector problem, STOC 2009, 333-342, 2009.

[39] C. Peikert, An efficient and parallel Gaussian sampler for lattices, Crypyo 2010, 80-97, 2010.

[40] C. Peikert, A decade of lattice cryptography, Cryptology ePrint Archive 2015/939, 2015, Foundations and Trends in Theoretical Computer Science 10:4, now Publishers Inc., 2016.

[41] C. Peikert, How (not) to instanaite Ring-LWE, Cryptology ePrint Achive 2016/351, 2016.

[42] C. Peikert and Z. Pepin, Algebraically structured LWE, revisited, TCC 2019, 1-23, 2019.

[43] C. Peikert, O. Regev and N. Stephens-Davidowitz, Pseudorandomness of Ring-LWE for any ring and modulus, STOC 2017, 461-473, 2017.

[44] A. Pellet-Mary, G. Hanrot and D. Stehlé, Approx-SVP in ideal lattices with pre-processing, Cryptology ePrint Achive 2019/215, Eurocrypt 2019, 685-716, 2019.

[45] O. Regev, New lattice-based cryptographic constructions, J. ACM, vol.**51**, 899-942, 2004.

[46] O. Regev, On lattices, learning with errors, random linear codes, J. ACM, **56**, 1-40, 2009.

[47] O. Regev, On the complexity of lattice problems with polynomial approximation factor, 475-496, The LLL algorithm, survey and application, edited by P. Q. Nguyen and B. Vallée, Springer, 2010.

[48] P. Ribenboinm, 13 lectures on Fermats last theorem, Springer-Verlag, New Tork, 1979.

[49] M. Rosca, D. Stehlé and A. Wallet, On the Ring-LWE and polynomial-LWE problems, Eurocrypt 2018, 146-173, 2018.

[50] L. Washington, Introduction to cyclotomic fields, Graduate Texts in Mathematics 83, Springer-Verlag 1997.