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

Hao Chen *

May 21, 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 computational number theory. In our previous paper we presented a general theory of subset attack on the Ring-LWE with not only the Gaussian error distribution but also general error distributions. By the usage of our subset attack from sublattice quadruples we prove that the decision (then the search version) Ring-LWE over two-to-power cyclotomic integer rings with certain sufficiently large 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 post-quantum 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, Subset attack, Feasible non-negligible subset quadruple, Sublattice quadruple, 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 [37]). 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 [37]). 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 [37]). 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 [37]). 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, 48].

1.2 Algebraic number fields

The Ring-LWE was introduced in [32] and has been the computational hard problem for lattice cryptography. It was suggested in [32] 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 [49]. 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 $\mathbf{R_K}$ 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 $< u, v >= \Sigma_{i=1}^{d} \sigma_i(u)\tilde{\sigma_i(v)}$, 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 $(\Sigma_{i=1}^{d} \sigma_i(u)\tilde{\sigma_i(u)})^{1/2}$. This is also the norm with respect to the canonical embedding (see [32]). 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 algebraic number field has the nice symmetry property reflected in the following lower bound (see [32] Lemma 2.9) for a fraction ideal $\mathbf{I}$,

$$\sqrt{d} N(\mathbf{I})^{1/d} \leq \lambda_1(\mathbf{I}).$$

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 [52]). 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 $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbf{Z}[X]$ 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 [36] 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 [32, 33, 42, 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 [33]. 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 [46]. We also refer to [47] 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 [47] for the detail and the background.

Ring-LWE

In [34] the algebraic structure of ring was first considered for the hardness of computational problems of lattices, we also refer to [30, 31]. This Ring-SIS (Short Integer Solution over Ring, see [34]) is an analogue of Ajtai's SIS problem. The one-wayness of some function was proved in [34]

by assuming the hardness of some computational problems of ideal lattices (cyclic lattices). In their Eurocrypt 21010 paper [32] the Ring-LWE was proposed and then extended in [33]. We refer to the nice survey [41] 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 [50] for relations and reductions between Ring-LWE and PLWE. In general arbitrary number of samples can be accessed to distinguish the the samples from the the Ring-LWE equation and the uniformly distributed samples. In the hardness reduction result in [**?**] only polynomially many samples are allowed for the adversary.

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 [32, 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 [42] 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 [43]. 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 [43].

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 [32, 33] for search version and then a general form from to decision version was proved for arbitrary number fields in [44]. We refer to [44] 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, 45, 28, 38] 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, 42]. As showed in [42, 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, 38] for the latest development in algorithms on approximating ideal-SVP.

2 Subset attacks

2.1 The ideal attack is very restricted

In previous attacks on Ring-LWE in [23] (then analysed in [10, 42]) the Ring-LWE equation $\mathbf{a}\cdot\mathbf{s}+\mathbf{e}\equiv\mathbf{b}$ mod q was transformed to consider $\mathbf{a}\cdot\mathbf{s}+\mathbf{e}\equiv\mathbf{b}$ mod $\mathbf{P}$, where $\mathbf{P}$ is a prime ideal factor of the modulus parameter q with a polynomially bounded algebraic norm $N(\mathbf{P})$. This kind of attack initiated in [23] and then analysed in [10, 42] can be called ideal attack on Ring-LWE. In ideal attack on Ring-LWE $\lambda_1(\mathbf{P}^\vee)$ satisfies

$$\lambda_1(\mathbf{P}^\vee)\geq\sqrt{d}N(\mathbf{P}^\vee)^{1/d}\geq d^{1/2-c/d}\frac{1}{|\Delta_{\mathbf{K}}|^{1/d}}.$$

Since $\mathbf{P}$ has a polynomially bounded algebraic norm, the width has a small upper bound for solvable instances for some fixed positive integer c .

When the modulus parameter q is a prime number such that $q\mathbf{R}_{\mathbf{K}}$ is a prime ideal in $\mathbf{R}_{\mathbf{K}}$, it is obvious we get nothing from the ideal attack. In our sublattice attack and subset attack we propose to find subtle polynomially bounded index sublattices $\mathbf{L}$ or feasible non-negligible subsets $\mathbf{B}$, then

to test the samples from the Ring-LWE equation in $\mathbf{R_K/L}$ or the feasible subset $\mathbf{B}$. Sublattice attacks was proposed in [13]. In this paper we extend it to subset attacks.

2.2 The motivation of subset attacks

In previous attacks on Ring-LWE, when polynomially bounded many samples $(\mathbf{a}, \mathbf{b}) \in \mathbf{R_K}/q\mathbf{R_K} \times \mathbf{R_K}/q\mathbf{R_K}$ 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 $\mathbf{A} \subset \mathbf{R_K}/q\mathbf{R_K}$ where $\mathbf{A}$ can be any feasible non-negligible subsets, that is, the condition

$$\mathbf{a} \in \mathbf{A}$$

can be computed within polynomial time and the size of $\mathbf{A}$ satisfies

$$\frac{|\mathbf{A}|}{|\mathbf{R_K}/q\mathbf{R_K}|} \geq \frac{1}{d^c},$$

where c is a fixed positive integer. In general when the learning with error problems with algebraic structures are used to improve the efficiency, subset attacks as above to analysis the distributions of samples over $\mathbf{A} \subset \mathbf{M}/q\mathbf{M}$ should be considered, where $\mathbf{M}$ is module over which the module-LWE is defined and $\mathbf{A}$ takes over all feasible subsets of $\mathbf{M}/q\mathbf{M}$ satisfying

$$\frac{|\mathbf{A}|}{|\mathbf{M}/q\mathbf{M}|} \geq \frac{1}{poly(d)}.$$

The previous attacks where $\mathbf{A}$ is restricted to ideals or sub-modules are not natural, special and not sufficient to guarantee the security, we refer to our next paper [14].

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 restricted to only check the distributions of samples over algebraic-structured object, the adversary can attack the problem by using feasible non-negligible subsets without any structure.

2.3 Subset quadruples are needed

We need to find three non-negligible subsets $\mathbf{A}_i$, $i = 1, 2, 3$ satisfying that

$$\frac{|\mathbf{A}_i|}{|\mathbf{R_K}/q\mathbf{R_K}|} \geq \frac{1}{d^c},$$

and $\mathbf{A}_1$ and $\mathbf{A}_3$ are feasible, that is the condition $\mathbf{a} \in \mathbf{A}_i$, $i = 1, 2$, can be checked within polynomial time. Here

$$\mathbf{A}_1 \cdot \mathbf{A}_2 = \{\mathbf{as} : \mathbf{a} \in \mathbf{A}_1, \mathbf{s} \in \mathbf{A}_2\}.$$

For two subsets $\mathbf{A}$ and $\mathbf{B}$ in $\mathbf{R_K}/q\mathbf{R_K}$ we define a subset $\mathbf{A} + \mathbf{B} = \{\mathbf{a} + \mathbf{b} : \mathbf{a} \in \mathbf{A}, \mathbf{b} \in \mathbf{B}\}$ in $\mathbf{R_K}/q\mathbf{R_K}$. A subset $\mathbf{A}_4 \subset \mathbf{R_K}/q\mathbf{R_K}$ is needed to satisfy that $\mathbf{A}_1 \cdot \mathbf{A}_2 + \mathbf{A}_4 \subset \mathbf{A}_3$ and

$$Prob(\mathbf{e} \in proj^{-1}(\mathbf{A}_4)) \geq \frac{d^C|\mathbf{A}_3|}{|\mathbf{R_K}/q\mathbf{R_K}|},$$

where C is a fixed positive integer and $proj$ is the natural mapping

$$\mathbf{R_K} \longrightarrow \mathbf{R_K}/q\mathbf{R_K}.$$

Then the samples from the Ring-LWE equations can be distinguished from uniformly distributed samples. Hence it is important to calculate the error distributions over these feasible non-negligible subsets.

In the case that $\mathbf{A}_1$ and $\mathbf{A}_2$ are additive, that is,

$$\mathbf{A}_i + \mathbf{A}_i \subset \mathbf{A}_i,$$

we recover the sublattice pair attack in [13] and the previous versions of this paper. We call $(\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4)$ a sublattice quadruple when $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$ and $\mathbf{A}_4$ are images of sublattices. In the sublattice quadruple case if $\mathbf{A}_1$ is the whole ring and $\mathbf{A}_2$ is an ideal it is the sublattice pair with an ideal introduced in the previous version of this paper. In the case that $\mathbf{A}_i$ is an ideal, it is the very restricted case of ideal attack considered in [23, 10] and analysed in [42]. The "sublattice pair with ideal" construction for the required sublattices proposed in the previous versions of the paper can not work for number field case as indicated in [42]. However the comment in [42] can not apply to the general sublattice attack or its extended version of subset attack (for general structured LWE) considered in this version. The only problem in previous versions is the usage of polynomially bounded index ideals in the construction of the required sublattices for number field case.

2.4 Subset attacks on other algebraically structured LWE

Some generalizations of Ring-LWE to other learning with errors problems over algebraically structured objects were presented in literature, even for some non-commutative algebras or rings with suitable positive inner products. It has been realized that LWE is indeed a good framework to construct cryptographic constructions since the pioneering work in [46]. However the cryptanalysis of LWE over algebraically structured objects are obviously not sufficient. Feasible non-negligible subset quadruples or sublattice quadruples are general framework to analysis the hardness of these LWE over algebraically structured objects. We believe that these problems are not hard in many settings. **The main point is the existence of feasible non-negligible subset quadruples or sublattice quadruples is equivalent to some algebraic conditions from the computation of error distribution in Theorem 4.1.** In Galois extension number field case there are so many prime numbers with various decomposition properties, then we can find suitable polynomially bounded prime modulus parameters to satisfy the required algebraic conditions.

3 Our contribution

3.1 Subset quadruples

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 $\mathbf{R_K}$ be its ring of integers. We consider the non-dual Ring-LWE over $\mathbf{R_K}$ 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 $\mathbf{A}_i \subset \mathbf{R_K}/q\mathbf{R_K}$, $i = 1, 2, 3, 4$, be four subsets in $\mathbf{R_K}/q\mathbf{R_K}$ satisfying the following conditions.*
1) $\frac{|\mathbf{A}_i|}{|\mathbf{R_K}/q\mathbf{R_K}|} \geq \frac{1}{d^{C_3}}$ for $i = 1, 2, 3$, where C_3 is fixed positive integer;
2) $\mathbf{A}_1 \cdot \mathbf{A}_2 + \mathbf{A}_4 \subset \mathbf{A}_3$;
3) The set $\mathbf{A}_1$ and $\mathbf{A}_3$ are feasible, that is, the condition $\mathbf{a} \in \mathbf{A}_1$ and the condition $\mathbf{b} \in \mathbf{A}_3$ for $\mathbf{a} \in \mathbf{R_K}/q\mathbf{R_K}$ and $\mathbf{b} \in \mathbf{R_K}/q\mathbf{R_K}$ can be checked within polynomial time;
4) The probability $Prob(\mathbf{e} \in proj^{-1}(\mathbf{A}_4)) > \frac{d^{C_4}|\mathbf{A}_3|}{|\mathbf{R_K}/q_{\mathbf{R_K}}|}$, where C_4 is a fixed positive integer.

In general if we can construct such subset quadruples 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). We do not require that $\mathbf{A}_4$ to be non-negligible in the uniform distribution.

3.2 Main results

In case that $\mathbf{A}_1$ and $\mathbf{A}_2$ come from sublattice. We denote the set of all elements of $\mathbf{R_K}$ of the form

$$\Sigma_{i=1}^{C_5} m_i \mathbf{b}_i,$$

where C_5 is a fixed positive integer when d goes to the infinity, $||\mathbf{b}_i|| \leq d^{C_6}$ for a fixed positive integer C_6, by $\mathbf{B}$.

Condition. Let $\mathbf{K}_d$ be a sequence of Galois extension fields of the rational number field $\mathbf{Q}$ with degree d going to the infinity, and $\mathbf{B}_d$ be the set described as above. For any given fixed positive integer C_7 we assume that there exists a sufficiently large polynomially bounded un-ramified prime $d^{C_7} \leq p(d)$ satisfying $\gcd(p(d), d) = 1$, such that $\mathbf{R_{K_d}}/p(d)\mathbf{R_{K_d}}$ is isomorphic to the product of bounded (by a fixed positive integer C_8) number of $\mathbf{F}_{p(d)^{f(d)}}$,

$$\mathbf{R_{K_d}}/p(d)\mathbf{R_{K_d}} = \mathbf{F}_{p(d)^{f(d)}} \times \cdots \times \mathbf{F}_{p(d)^{f(d)}},$$

(C_8 copies of $\mathbf{F}_{p(d)^{f(d)}}$, $C_8 f(d) = d$), and there exist $\mathbf{F}_{p(d)}$ linear subspaces $\mathbf{A}_1^j$ and $\mathbf{A}_2^j$ in $\mathbf{F}_{p(d)^{f(d)}}$ for $j = 1, 2, \ldots, C_8$, with dimensions

$$\dim(\mathbf{A}_i^j) \geq d - C_9$$

for $i = 1, 2$, where C_9 is a fixed positive integer when d goes to the infinity, and an element $\mathbf{b} \in \mathbf{B}_d$, such that $\Sigma_{j=1}^{8} Tr_{\mathbf{F}_{p(d)^{f(d)}}/\mathbf{F}_{p(d)}}(\mathbf{b} \cdot \mathbf{x}_1^j \mathbf{x}_2^j) \equiv 0$ *mod* p_d satisfied for any $\mathbf{x}_i^j \in \mathbf{A}_i^j$ for $i = 1, 2, j = 1, 2, \ldots, C8$. Here $Tr_{\mathbf{F}_{p(d)^{f(d)}}/\mathbf{F}_{p(d)}} = x + x^{p(d)} + \cdots + x^{p(d)^{f(d)-1}}$ is the trace mapping from the finite field $\mathbf{F}_{p(d)^{f(d)}}$ to $\mathbf{F}_{p(d)}$.

Theorem 3.1. *If $\mathbf{K}_d$ is a sequence of Galois number fields with degree d going to the infinity and the above condition is satisfied. Let σ_d be the sequence of the widths of Gaussian error distributions over $\mathbf{R_{K_d}}$. Suppose that $\frac{\sqrt{d}}{\lambda_1(\mathbf{R_{K_d}}^\vee)} \leq \sigma_d \leq d^{C_9}$, where C_9 is a fixed positive integer when d goes to the infinity. Then the decision non-dual Ring-LWE over $\mathbf{R_{K_d}}$ for certain polynomially bounded prime modulus parameters can be solved within the polynomial (in d) time.*

Notice that the above condition depends on the number fields only with the element $\mathbf{b} \in \mathbf{B}_d$. Hence we believe that if we can prove the existence of such an element, it should work for many number field sequences. The above condition will be analysed in Section 5. In the above case that $p(d)\mathbf{R_K}$ is the product of bounded number of prime ideals, no ideal factor of $p(d)$ has polynomially bounded index when d goes to the infinity, then the analysis in [42] does not work in this situation. However this is not the only approach to construct sublattices for sublattice attacks or feasible non-negligible subset quadruples for subset attacks. The above result Theorem 3.1 was proved in [12].

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 quadruples for two-to-power cyclotomic number fields.

Theorem 3.2. *Let C be an arbitrary large 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 sequence σ_n of the error distribution sequences over $\mathbf{R_{K_n}}$ satisfies $\frac{\sqrt{d_n}}{\lambda_1(\mathbf{Z}[\xi_{2^n}]^\vee)} \leq \sigma_n \leq d_n^C$. 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 we can construct sublattice quadruple sequences for the the decision Ring-LWE over $\mathbf{Z}[\xi_{2^n}]$ with the modulus parameter q_n.*

From Theorem 3.2 the following result can be proved.

Corollary 3.1. *Let C be an arbitrary large 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 widths σ_n of the error distribution over $\mathbf{R_{K_n}}^\vee$ satisfies $\frac{\sqrt{d_n}}{\lambda_1(\mathbf{Z}[\xi_{2^n}])} \leq \sigma_n \leq$*

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 dual decision Ring-LWE over* $\mathbf{Z}[\xi_{2^n}]^\vee$ *with the modulus parameter* q_n *can be solved in the polynomial time (in* d_n*).*

From the hardness reduction result Theorem 6.2 and Corollary 6.3 in [44] 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 by different method.

Corollary 3.3. *Let* C *be an arbitrary fixed positive integer and* m *be a fixed positive integer. We consider the Module-LWE over* ${\mathbf{R}_{\mathbf{K_n}}}^m = \mathbf{Z}[\xi_{2^n}]^m$. *Suppose that the width sequences* σ_n *of the error distribution sequence satisfies* $\frac{\sqrt{d_n}}{\lambda_1(\mathbf{Z}[\xi_{2^n}])} \leq \sigma_n \leq d_n^C$. *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 the polynomial time (in* d_n*).*

3.3 Cryptographic and algorithmic implications

We prove that the decision Ring-LWE over two-to-power cyclotomic integer rings (then the search version) 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. Then post-quantum lattice cryptographic constructions can not be based on the hardness of Ring-LWE. 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 can be solved in the polynomial time in the quantum computation model. Further results about other Galois number field sequences will be presented in [15].

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 [36]) 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 [36]. 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.

5 Number theory

5.1 Basic facts

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 $q\mathbf{R_{K_d}} \subset \mathbf{L}_1 \subset \mathbf{R_{K_q}}$. 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.

The following result about the factorization of a prime number in the cyclotomic fields is useful in the sublattice construction, we refer to [52].

Proposition 5.4 *Let* $n=2^m$ *be a two-to-power and* $d=\phi(n)=2^{m-1}$ *be its Euler function. Let* p *be an odd prime. Set* f *the order of* p *in* $(\mathbf{Z}/2^m\mathbf{Z})^*$, *that is,* f *is the smallest positive integer such that* $p^f\equiv 1\ mod\ n$. *Then* p *factorized to* $M=\frac{2^{m-1}}{f}$ *prime ideals in* $\mathbf{Z}[\xi_n]$,

$$p\mathbf{Z}[\xi_n]=\mathbf{P_1}\cdots\mathbf{P}_M.$$

Moreover $\mathbf{Z}[\xi_n]/\mathbf{P}_i$ *is isomorphic* $\mathbf{F}_{p^f}$.

We refer to [51] for the following general result about decomposition groups of prime ideals.

Proposition 5.5. *Let* $\mathbf{K}$ *be a degree* n *Galois extension of the rational number field with the Galois group* $\mathbf{G}$. *Suppose that* p *is an un-ramified prime in* $\mathbf{R_K}$. *Let* $p\mathbf{R_K}=\mathbf{P}_1\cdots\mathbf{P}_t$ *be its decomposition of the product*

of prime ideals, $\mathbf{R_K}/\mathbf{P}_i = \mathbf{F}_{p^{f_i}}$. *Then* G *acts on* $\mathbf{P}_1, \ldots, \mathbf{P}_t$ *transitively and all residual class degrees* f_i*'s,* $i = 1, 2, \ldots, t$ *are the same* f. *We have* $n = |\mathbf{G}| = tf$. *Let*

$$\mathbf{G}_{\mathbf{P}_1} = \{g \in G : g(\mathbf{P}_1) = \mathbf{P}_1\}$$

be the decomposition subgroup of the prime ideal $\mathbf{P}_1$ *in the Galois group* $\mathbf{G}$. *Then the decomposition subgroup* $\mathbf{G}_{\mathbf{P}_i}$ *of* $\mathbf{P}_i$, $i = 2, \ldots, t$, *is the conjugate* $g_i \mathbf{G}_{\mathbf{P}_1} g_i^{-1}$ *of* $\mathbf{G}_{\mathbf{P}_1}$. *The Galois group* $\mathbf{G}$ *is the sum of these decomposition subgroups. Moreover* $\mathbf{G}_{\mathbf{P}_i}$ *is isomorphic to the automorphism group of the extension* $\mathbf{F}_{p^f}$ *of* $\mathbf{F}_p$ *generated by the Frobenius element* $x \longrightarrow x^p$.

5.2 Trace functions and adjoint linearized polynomials over $\mathbf{F}_{q^n}$

In the follow part we recall some basic facts about linearized polynomials (q polynomials) and trace functions over $\mathbf{F}_{q^n}$. Let $L(x) = \Sigma_{i=0}^{n-1} a_i x^{q^i}$, where $a_i \in \mathbf{F}_{q^n}$. It is clear $L : \mathbf{F}_{q^n} \longrightarrow \mathbf{F}_{q^n}$ is a linear mapping of n dimensional linear space over $\mathbf{F}_q$. The polynomial $l(x) = \Sigma_{i=0}^{n-1} a_i x^i$ is called the conventional q-associate of $L(x)$. The polynomial $L(x)$ is called the linearized associate of $l(x)$. The following proposition is well-known , we refer to [29].

Proposition 5.6. *Let* $L_1(x) = \Sigma_{i=0}^{n-1} a_i x^{q^i}$, $L_2(x) = \Sigma_{i=0}^{n-1} b_i x^{q^i}$ *be two linearized polynomials with coefficients* $a_i \in \mathbf{F}_q$ *and* $b_i \in \mathbf{F}_q$. *The polynomial* $l_1(x) = \Sigma_{i=0}^{n-1} a_i x^i$ *and* $l_2(x) = \Sigma_{i=0}^{n-1} b_i x^i$ *in* $\mathbf{F}_q[x]$ *are their conventional* q*-associates. The conventional* q*-associate of* $L_1(L_2(x)) = L_2(L_1(x))$ *is the product* $l_1(x) l_2(x)$.

Proof. $L_1(L_2(x)) = \Sigma_{j=0}^{n-1} a_j (\Sigma_{i=0}^{n-1} b_i x^{q^i})^{q^j} = \Sigma_{j=0}^{n-1} (\Sigma_{i=0}^{n-1} b_i^{q^i} x^{q^{i+j}})$. Since $b_i^{q^i} = b_i$ for any $i = 1, 2, \ldots, n-1$ from the condition $b_i \in \mathbf{F}_q$, we have $L_1(L_2(x)) = \Sigma_{j=0}^{n-1} a_j (\Sigma_{i=0}^{n-1} b_i x^{q^{i+j}}) = \Sigma_{j=0}^{n-1} \Sigma_{i=0}^{n-1} a_j b_i x^{q^{i+j}}$. The conclusion follows directly.

For the linearized polynomial $L(x) = \Sigma_{i=0}^{n-1} a_i x^{q^i} \in \mathbf{F}_{q^n}[x]$, the adjoint polynomial of L is the linearized polynomial $\hat{L}(x) = \Sigma_{i=0}^{n-1} a_i^{q^{n-i}} x^{q^{n-i}}$.

Proposition 5.7. *We have* $Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q}(yL(z)) = Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q}(z\hat{L}(y))$ *for* $y, z \in \mathbf{F}_{q^n}$.

Proof. It is clear that $Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q}(yaz^{q^i}) = Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q}(za^{q^{n-i}}y^{q^{n-i}})$ for $z, y, a \in \mathbf{F}_{q^n}$. Then the conclusion follows from the additivity directly.

We set $n = 2^{m-1}$ and $L_1(x) = x^{q^4} - x$ and $L_2(x) = x^{q^{n-4}} + x^{q^{n-8}} + \cdots + x^{q^8} + x^{q^4} + x + w(x)$, where f is a linearized polynomial with degree at most q^{16}.

Proposition 5.8. *The kernels of L_1 and L_2 as F_q linear mappings of $\mathbf{F}_{q^n}$ have their dimensions at most* 20.

Proof. The dimension of L_1 is at most 4 since its degree is at most 4. Let $Tr_{\mathbf{F}_{q^n}/\mathbf{F}_{q^4}} : \mathbf{F}_{q^n} \longrightarrow \mathbf{F}_{q^4}$ be the trace function from $\mathbf{F}_{q^n}$ to $\mathbf{F}_{q^4}$ defined by $x + x^{q^4} + x^{q^8} + \cdots + x^{q^{n-4}}$. The codimension of its kernel as a $\mathbf{F}_q$ linear space is at most 4. For $y \in \ker(L_2) \bigcap \ker(Tr_{\mathbf{F}_{q^n}/\mathbf{F}_{q^4}})$, it is clear that y satisfies $w(x) = 0$. Since the codimension of the kernel of $Tr_{\mathbf{F}_{q^n}/\mathbf{F}_{q^4}}$ is at most 4. The conclusion follows directly.

6 Proof of the main results

Proof of Theorem 3.1. We prove that feasible non-negligible subset quadruples grantee the polynomial time solvability. The probability that uniformly chosen $\mathbf{a} \in \mathbf{R_K}/q\mathbf{R_K}$ is in the subset $\mathbf{A}_1$ is at least $\frac{1}{d^{C_3}}$, the probability $\mathbf{s} \in \mathbf{A}_2$ is at least $\frac{1}{d^{C_3}}$ for uniformly distributed $\mathbf{s} \in \mathbf{R_K}/q\mathbf{R_K}$. We check the probability $(\mathbf{a}, \mathbf{b}) \in (\mathbf{A}_1, \mathbf{A}_3)$ for $d^{C_{11}}$ samples $(\mathbf{a}, \mathbf{b})$'s where C_{10} is a fixed sufficiently large positive integer. Since both $\mathbf{A}_1$ and $\mathbf{A}_3$ are feasible, this can be done within a polynomial time. When these samples are uniformly distributed, the probability that

$$(\mathbf{a}, \mathbf{b}) \in (\mathbf{A}_1, \mathbf{A}_3)$$

is exactly

$$\frac{|\mathbf{A}_1|}{|\mathbf{R_K}/q\mathbf{R_K}|} \cdot \frac{|\mathbf{A}_3|}{|\mathbf{R_K}/q\mathbf{R_K}|}.$$

Since $\mathbf{a} \cdot \mathbf{s} \in \mathbf{A}_1 \cdot \mathbf{A}_2$ for the fixed unknown secret $\mathbf{s} \in \mathbf{A}_2$, when $\mathbf{a} \in \mathbf{A}_1$. Then the probability $\mathbf{b} \in \mathbf{A}_3$ is bigger than or equal to $Prob(\mathbf{e} \in proj^{-1}(\mathbf{A}_4))$ from the condition 2)

$$\mathbf{A}_1 \cdot \mathbf{A}_2 + \mathbf{A}_4 \subset \mathbf{A}_3$$

in the definition of subset quadruples. Then we have

$$Prob((\mathbf{a},\mathbf{b}) \in (\mathbf{A}_1,\mathbf{A}_3)) \geq \frac{|\mathbf{A}_1|}{|\mathbf{R_K}/q\mathbf{R_K}|} \cdot Prob(\mathbf{e} \in proj^{-1}(\mathbf{A}_4)).$$

From the condition 4) of the subset quadruple we have

$$Prob((\mathbf{a},\mathbf{b}) \in (\mathbf{A}_1,\mathbf{A}_3)) > \frac{|\mathbf{A}_1|}{|\mathbf{R_K}/q\mathbf{R_K}|} \cdot \frac{2|\mathbf{A}_3|}{|\mathbf{R_K}/q\mathbf{R_K}|},$$

when samples are from the Ring-LWE equations. Hence for non-negligible secrets $\mathbf{s} \in \mathbf{A}_2$, the $d^{C_{11}}$ samples $(\mathbf{a},\mathbf{b})$'s from the Ring-LWE equation are not uniformly distributed and can be tested within a polynomial time.

The Tr_d of the extension $\mathbf{K}_d/\mathbf{Q}$ has a natural projection $Tr_{d,p(d)}$: $\mathbf{R_{K_d}}/p(d)\mathbf{R_{K_d}} = \mathbf{F}_{p(d)^{f(d)}} \times \cdots \times \mathbf{F}_{p(d)^{f(d)}} \longrightarrow \mathbf{Z}/p(d)\mathbf{Z} = \mathbf{F}_{p(d)}$. From Proposition 5.5, this $Tr_{d,p(d)}$ function of $\mathbf{R_{K_d}}/p(d)\mathbf{R_{K_d}} = \mathbf{F}_{p(d)^{f(d)}} \times \cdots \times \mathbf{F}_{p(d)^{f(d)}}$ is the sum

$$Tr_{d,p(d)}(x_1,\ldots,x_{C_8}) = Tr_{\mathbf{F}_{p(d)^{f(d)}}/\mathbf{F}_{p(d)}}(x_1) + \cdots + Tr_{\mathbf{F}_{p(d)^{f(d)}}/\mathbf{F}_{p(d)}}(x_{C_8}).$$

Here $f(d)C_8 = d$. We take $\mathbf{A}_1$ and $\mathbf{A}_2$ the sum of $\mathbf{A}_1^j$, $j = 1,2,\ldots,C_8$, $\mathbf{A}_4$ the subspace in $\mathbf{R_{K_d}}/p(d)\mathbf{R_{K_d}}$ defined by $Tr(\mathbf{b}\cdot\mathbf{x}) \equiv 0 \ mod\ p(d)$. Then $\mathbf{A}_1 \cdot \mathbf{A}_2 \subset \mathbf{A}_4$. $\mathbf{A}_3$ is the same as the $\mathbf{A}_4$. From Theorem 4.1 the condition 4) of subset quadruple is satisfied. The conclusion follows directly.

We give the proof of Theorem 3.2.

Proof of Theorem 3.2. First of all we can find $p(d)$ from Proposition 5.4. It is well-known that 3 is an order 2^{m-2} element in $(\mathbf{Z}/2^m\mathbf{Z})^*$. Then for any odd prime satisfying $p \equiv 3 \ mod\ 2^m$, its order in $(\mathbf{Z}/2^m\mathbf{Z})^*$ is 2^{m-2}. From Proposition 5.4 the suitable sufficiently large polynomially bounded un-ramified prime $p(d)$ such that $\mathbf{Z}[\xi_n]/p\mathbf{Z}[\xi_n]$ factorized to the product of 2 prime ideals can be found directly from Dirichlet's Theorem (by an argument of Dirichlet's density). Then $C_8 = 2$ in the Condition of Theorem 3.1.

Set $\mathbf{b} = 1$. Let $\mathbf{A}_1^j$ be the image of the linearized polynomial $G^j(x)$ and $\mathbf{A}_2$ be the image of of the linearized polynomial $L^j(x)$ for $j = 1,2$. Hence

$$Tr_{\mathbf{F}_{q^{f(d)}}/\mathbf{F}_q}(G^1(y)L^1(z)) + Tr_{\mathbf{F}_{q^{f(d)}}/\mathbf{F}_q}(G^2(y)L^2(z)) = Tr_{\mathbf{F}_{q^{f(d)}}/\mathbf{F}_q}(z(\hat{L^1}(G^1(y)) + \hat{L^2}(G^2(y)))$$

from Proposition 5.7. We only need to find linearized $p(d)^4$ polynomials G^1, G^2, L^1, L^2 such that $g^1l^1 + g^2l^2$ is of the form $x^d - 1$ where g^j, l^j, $j = 1,2$,

are the conventional associates of G^j, L^j from Proposition 5.6. This can be constructed from Proposition 5.8 directly. The conclusion follows from Theorem 3.1.

Proof of Corollary 3.1, 3.2 and 3.3. The conclusions follows from Theorem 3.2 directly by the results in [32, 44].

7 Conclusion

In this paper we construct sublattice quadruples for the Ring-LWE over the two-to-power cyclotomics such that the samples from the Ring-LWE equations can be distinguished from the uniformly distributed samples. The main point of our subset or sublattice attack is to find carefully constructed polynomially bounded index sublattices or feasible non-negligible subsets and check samples from the Ring-LWE equations in the quotients of such lattices or these feasible non-negligible subsets. The sublattice attack from sublattice quadruples is applied to the Ring-LWE with arbitrary polynomially bound width Gaussian error distributions over two-to-power fields. We prove that the decision (then search) Ring-LWE over two-to-power fields with wide error distributions of widths in the range of Peikert-Regev-Stephens-Davidowitz hardness reduction results for certain sufficiently large polynomially bounded modulus parameters 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. The construction of suitable sublattice quadruples for many Galois number field sequences will be presented in [15].

Acknowledgement. I am grateful to Chris Peikert for his comment in [42] on my effort to understand the hardness of the Ring-LWE. I also thank these friends for their interest and comment on the previous versions of this paper and my other ePrints on related problems.

The Twitter claim in [42] "entire approach cannot possibly work against the targeted Ring-LWE parameters" is exaggerating. This claim can only apply to the minor error of "sublattice pairs with ideals" construction for the required sublattice in the sublattice attack for the number field case, not the whole theory of sublattice attack on Ring-LWE. Even for polynomial ring

LWE with some special inner products the sublattice pair with ideals can be used to construct the required sublattices as in [12]. In previous cryptanalysis of Ring-LWE in [23, 10] only samples from Ring-LWE equations in quotients of ideals were considered. This kind of ideal attack was analysed in [42], which was emphasized in Chris Twitter comment. When polynomially bounded index ideals are not used in our sublattice attack construction or the inner product has no the symmetric property

$$\sqrt{d}N(\mathbf{I})^{1/d} \leq \lambda_1(\mathbf{I}),$$

actually there is no previous results can be used to say anything about the sublattice attack.

The sufficiently large polynomially bounded prime numbers which are completely split in the cyclotomic rings were used in the 1st version as modulus parameters. Then there are $poly(d)$ many polynomially bounded index ideal factors of this prime modulus parameters. Hence the construction of "sublattice pair with an ideal" in the 1st version is incorrect in the number field case as indicated in [42]. In this version un-ramified sufficiently large polynomially bounded primes with very high residual class degrees f are used as modulus parameters, that is, d/f is bounded when d goes to the infinity. Then no ideal factors of these modulus parameters have polynomially bounded indices. In the proof of Theorem 3.2 all ideal factors of the modulus parameters are of exponential indices in $\mathbf{Z}[\xi_{2^m}]$.

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, Subset attacks on Ring-LWE with wide error distributions I, Cryptology ePrint 2020/440.

[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, Subset attacks on Ring-LWE with wide error distributions II, in preparation 2021.

[16] H. Chen, K. Lauter and K. E. Stange, Security consideration for Galois non-dual RLWE families, SAC 2016, 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.

[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] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Cambridge University Press, Cambridge, 1997.

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

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

[32] 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.

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

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

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

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

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

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

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

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

[41] 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.

[42] C. Peikert, How (not) to instanaite Ring-LWE, SCN 2016, 411-430, 2016, Private communications, Twitter explaination of the 1st version of ePrint 2021/418 on 3, 2021.

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

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

[45] 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.

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

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

[48] 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.

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

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

[51] W. Stein, Introduction of algebraic number theory, 2005.

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