Solving Algebraically Structured LWE in Arbitrary Number Fields

Hao Chen *

September 17, 2019

Abstract

Learning with errors (LWE) have been used to construct many lattice-based crypto-systems. For the efficiency consideration learning with errors over algebraic integer rings (Ring-LWE) were introduced by Lyubashevsky, Peikert and Regev in Eurocrypt 2010. In recent years variants of algebraically structured learning with errors such as order-LWE, module-LWE and LWE over number field lattices have been introduced. In this paper we prove that for these algebraically structured LWE in *an arbitrary number field* there are infinitely many algebraically weak modulus parameters such that the problem can be transformed to distinguishing the discretization of one-dimensional continuous Gaussian distribution from the uniform distribution. Hence for these algebraically weak modulus parameters these LWE over *arbitrary number fields* can be solved within a polynomial time for a suitable large width. While for plain LWE there is no such algebraically weak modulus parameters.

Secondly we prove that for LWE over a number field lattice $\mathbf{L}$ in *arbitrary number fields*, when the width is smaller than $O(\frac{\sqrt{logn}}{\lambda_1(\mathbf{L}_1^\vee)})$ for some polynomially bounded cardinality $|\mathbf{L}^\vee/\mathbf{L}_1|$ sublattice $\mathbf{L}_1 \subset \mathbf{L}^\vee$, then the LWE over $\mathbf{L}$ can be solved by a polynomial time algorithm for some modulus parameters. This leads to new sub-lattice bounds on widths of solvable Ring-LWE instances.

Keywords: Ring-LWE, Order LWE, LWE over a number field lattice, Width of the Gaussian of error distribution.

*Hao Chen is with the College of Information Science and Technology/Collage of Cyber Security, Jinan University, Guangzhou, Guangdong Province, 510632, China, haochen@jnu.edu.cn. This research is supported by the NSFC Grant 11531002.

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 [40]). 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 [40]). A breakthrough result of M. Ajtai [4] 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 [40]). For the latest development we refer to Khot [28]. It was proved that approximating SVP within a quasi-polynomial factor is NP-hard under the randomized reduction. 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 minimum of lattice $\mathbf{L}$ (see [40]). For the hardness results about SVP and $SIVP$ we refer to [28, 29, 49].

1.2 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 $D_{s,\mathbf{c}} = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{s^n}, \forall \mathbf{x} \in \mathbf{R}^n$.

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 $\mathbf{L} \subset \mathbf{R}^n$ is a dimension n lattice, the discrete Gaussian distribution over $\mathbf{L}$ is the probability distribu-

tion 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 $\mathbf{D}_{\mathbf{L},\mathbf{s}}$. We refer the following properties of discrete Gaussian distributions to [37].
1) If $\mathbf{x}$ is distributed according to $\mathbf{D}_{s,\mathbf{c}}$ and conditioned on $\mathbf{x} \in \mathbf{L}$, the conditional distribution of $\mathbf{x}$ is $D_{\mathbf{L},s,\mathbf{c}}$.
2) For any lattice $\mathbf{L}$ and any vector $\mathbf{c} \in \mathbf{R}^n$ we have $\rho_{s,\mathbf{c}}(\mathbf{L}) \leq \rho_s(\mathbf{L})$.
3) Set $C = c\sqrt{2\pi e}e^{-\pi c^2} < 1$ for any $c > \frac{1}{\sqrt{2\pi}}$, and n dimensional lattice $\mathbf{L}$ and $\mathbf{v} \in \mathbf{R}^n$, $\rho(\mathbf{L} - c\sqrt{n}\mathbf{B}_n) \leq C^n\rho(\mathbf{L})$, $\rho((\mathbf{L} + \mathbf{v}) - c\sqrt{n}\mathbf{B}_n) \leq C^n\rho(\mathbf{L})$, where $\mathbf{B}_n$ is the unit-ball centered at the origin.
4 If a $\mathbf{e} \in \mathbf{R}^n$ is sampled according to a Gaussian distribution with width σ, then the Euclid norm $||\mathbf{e}||$ of $\mathbf{e}$ satisfies $||\mathbf{e}|| \leq \sqrt{3n}\sigma$ with an overwhelming probability.

1.3 Algebraic number fields

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 $\mathbf{R_K}$ is its ring of integers in $\mathbf{K}$. From the primitive element theorem there exits 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 [16]). It is well-known there is a positive definite inner product on the lattice $\mathbf{R_K}$ defined by $< u, v >= tr_{K/Q}(u\tilde{v})$ where $\tilde{v}$ is its complex conjugate (see [8, 16]). Sometimes we use $||u||_{tr}$ to represent $tr_{K/Q}(u\tilde{u})^{1/2}$. This is also the norm with respect to the canonical embedding (see [31]). The number field $\mathbf{K}$ is called monogenic, if the ring $\mathbf{R_K}$ of integers is of the form $\mathbf{R_K} = \mathbf{Z}[x]/(f) = \mathbf{Z}[\theta]$. This is equivalent to that $\mathbf{R_K}$ has a power base (see [22]). In this case the discriminant of the number field $\mathbf{K}$ (see [16]) is the same as the discriminant of the minimal polynomial f, $\Delta_{\mathbf{K}} = \Delta_f$. For a monic degree m polynomial f with m roots $\theta_1, \theta_2, \ldots, \theta_m$, then the discriminant of the polynomial f is $\Delta_f = \prod_{i \neq j}(\theta_j - \theta_i)^2$. For an ideal $\mathbf{I} \subset \mathbf{R_K}$ if we can find one generator $\mathbf{g}$, this ideal is called a principal ideal generated by $\mathbf{g}$. Any ideal in $\mathbf{R_K}$ is a lattice of dimension $deg(\mathbf{K}/\mathbf{Q})$. For an ideal $\mathbf{I} \subset \mathbf{R_K}$, its dual $\mathbf{I}^\vee$ is defined as $\mathbf{I}^\vee = \{\mathbf{x} \in \mathbf{K}, tr_{K/Q}(\mathbf{ax}) \in \mathbf{Z}, \forall \mathbf{a} \in \mathbf{I}\}$. 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 [16, 17, 10] 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 $\mathbf{Q}(\xi_n) = \mathbf{Q}[x]/(\Phi_n(x))$ and the ring of integers in $\mathbf{Q}(\xi_n)$ is exactly $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_n(x))$ (see [53]). For example when $n = 2^m$, the n-th cyclotomic polynomial is $\Phi_{2^m}(x) = x^{2^{m-1}} + 1$. 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 cyclotomic number field $\mathbf{Q}[\xi_n]$ is a monogenic field. The discriminant of the cyclotomic field (also the discriminant if the cyclotomic polynomial Φ_n) is

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

For example when $n = 2^m$ the discriminant is $2^{(m-1)2^{m-1}}$. When $n = p$ is an odd prime the discriminant is $(-1)^{\frac{p-1}{2}} p^{p-2}$. Hence

$$\prod (\xi_j - \xi_i)^2 = (-1)^{\frac{\phi(n)}{2}} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}},$$

where $\xi_1, \xi_2, \ldots, \xi_{\phi(n)}$ are n-the primitive roots of unity, from the equality $\Delta_{\mathbf{Q}[\xi_n]} = \Delta_{\Phi_n}$.

We consider the field $\mathbf{K}_q = \mathbf{Q}[x]/(f_q)$ where $f_q(x) = x^n + q$, q has a prime factor with exponent 1. Then $f_q(x)$ is irreducible from the Eisenstein criterion. It is known that when n is a power of a prime l, q is squrefree and l^2 can not divide $((-q)^n + q)$, the field $\mathbf{K}_q$ is monogenic (see [23], Proposition 5.1). The discriminant of $\mathbf{K}_q$ is $(-1)^{\frac{n^2-n}{2}} n^n q^{n-1}$ (see [23]).

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

1.4.1 Plain LWE

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

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

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 $\mathbf{Z}_q^n$.

Write the d coefficient vectors $\mathbf{a}_1, \ldots, \mathbf{a}_d$ as columns of a matrix $\mathbf{A} \in \mathbf{Z}_q^{n \times d}$, Then the search LWE problem $LWE_{n,q,d,\chi}$ is to recover the secret from $\mathbf{A}^\tau \cdot \mathbf{s} + \mathbf{e} = \mathbf{b}$ *mod* q from public $(\mathbf{A}, \mathbf{b})$. Here τ is the transposition of a matrix and $(\mathbf{s}, \mathbf{e})$ is an unknown vector.

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 [48] for the detail and the background. When q is prime and polynomial bounded by $poly(n)$, there is a polynomial-time reduction between the search and decision LWE (see [48]). For this LWE without ring structure the reduction results from approximating SVP to plain LWE were given in [48, 41, 9].

1.4.2 Ring-LWE

If the $\mathbf{Z}_q^n$ 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 problem. 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 [22, 23]).

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 $\mathbf{K}$, this is the Ring-LWE, learning with errors problem 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, 11]). 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 [12, 44] these two forms of Ring-

LWE problem can be converted with a scale factor $|\Delta_{\mathbf{K}}|^{\frac{1}{n}}$ on the width of the Gaussian distribution of errors. In [12] and [44] page 10 it was indicated in monogenic case a "tweak factor" $f'(\theta)$ can be used to make two versions equivalent. The reduction result from approximating ideal-SVP to Ring-LWE over arbitrary number fields were give in [31, 32, 46].

Remark 1.1. First of all the hardness of approximating SVP to some almost polynomial factors under the randomized reduction was proved for all lattices ([28, 29, 49]), while the hardness of some Ring-LWE is based on $SVP_{poly(n)}$ or $SIVP_{poly(n)}$ for fractional ideal lattices as proved in the above result (see [48, 41, 31, 46]). People do not have any evidence that approximating SVP for ideal lattices is hard or not (see [44, 48]). Secondly the approximating factor has to be small if we want the hardness of LWE or Ring-LWE from the hardness of $SVP_{poly(n)}$ or $SIVP_{poly(n)}$, since when the approximating factor is as large as exponential of lattice dimensions, the LLL algorithm can be used to give the desired lattice vectors (see [34]).

1.4.3 LWE over number field lattices

Learning with errors over a number field lattice was introduced in [45]. 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.

$$\mathbf{L}^\vee = \{y \in \mathbf{K} : Tr_{\mathbf{K/Q}}(xL) \subset \mathbf{Z}\}.$$

$\mathbf{O^L}_q = \mathbf{O^L}/q\mathbf{O^L}$, $\mathbf{L}_q^\vee = \mathbf{L}^\vee/q\mathbf{L}^\vee$. The secret vector $\mathbf{s}$ is in $\mathbf{L}_q^\vee$ 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 $\mathbf{e} \in \mathbf{L}_q^\vee$.

When $\mathbf{L} = \mathbf{R_K}$, it is the dual form of Ring-LWE. When $\mathbf{L} = \mathbf{O}^\vee$ for an order $\mathbf{O} \subset \mathbf{K}$, this is the order LWE introduced in [10]. This form was indicated in [45]. For example for a number field $\mathbf{K} = \mathbf{Q}[\theta]$, $\mathbf{O} = \mathbf{Z}[\theta]$, this is order LWE over $\mathbf{Z}[\theta]$. In this case $\mathbf{Z}[\theta]^\vee = \frac{1}{f'(\theta)}\mathbf{Z}[\theta]$ (see [17]), then $\mathbf{O}^{\mathbf{Z}[\theta]^\vee} = \mathbf{Z}[\theta]$. Hence $\mathbf{s} \in (\mathbf{Z}[\theta])_q$, $\mathbf{a} \in (\mathbf{Z}[\theta])_q$ and $\mathbf{e} \in (\mathbf{Z}[\theta])_q$.

For MP LWE (middle-product LWE) and relations of widths in the reduction between different learning with errors we refer to [50, 51, 45]. We refer to [10, 50, 51] for hardness reduction results.

1.4.4 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, 44, 11]). We recall the analysis in [11]. 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.

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

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.

1.5 Known attacks

We refer to [6, 27] for the attack to LWE from the Blum-Kalai-Wasserman algorithm and its improvement. In [34] a probabilistic polynomial time algorithm was given to recover the secret key of LWE over $\mathbf{Z}_q^n$ when $\frac{nq}{\sigma}$ is very large. On the other hand Ring-LWE problems over integer rings of some algebraic number fields or polynomial rings $\mathbf{P}_q^n$ were attacked in [21, 23, 14, 15, 11, 14]. In [44, 11] the above attack was analysed. The attacks can succeed because the width of the Gaussian distribution over $\mathbf{K} \otimes \mathbf{R}$ is too small, often smaller than a constant not depending on q only depending on the lattice dimension d, or the shape of the Gaussian distribution on

$\mathbf{P}_q$ with respect to the base $1, x, \ldots, x^{u-1}$ is too "skewed" (see [44, 12]).

When the width is too small, with high probabilities the errors are within some range $z+(-\frac{1}{2}, \frac{1}{2})$ with a fixed integer z, the Ring-LWE can be reduced to an errorless problem (see [44]). One of the attack in [21, 23, 14, 15, 11, 14] is based on a homomorphism $\mathbf{R_K} \longrightarrow \mathbf{R_K}/\rho = \mathbf{F}_{q^\mu}$, where ρ is the ideal over q and μ is one or two. Then the Ring-LWE can be "transformed" to a LWE over $\mathbf{F}_{q^f}$. If the "error distribution"over $\mathbf{F}_{q^f}$ from the errors sampled according to some Gaussian distribution is concentrated, then it leads to a complexity $O(q^3 n)$ attack. Over 2-power cyclotomic integer rings, the above "error distribution" is indistinguishable from the uniform distribution under a suitable condition(see [15], section 4). Then their attack can not be applied to cyclotomic integer rings. Their method can also be applied to some polynomial LWE problems as described in [22, 23].

In [18] approximating SVP with approximating factor $2^{O(\sqrt{nlogn})}$ for principal ideals in cyclotomic integer rings with $n = p^m$ can be found from an arbitrary generator within polynomial time by an efficient bounded distance decoding algorithm for the log-unit lattice. This work was extended in [19] and [47] such that sub-exponential complexity algorithms with some pre-processing for approx-SVP in ideal lattices have been achieved. The analysis of the approximating factor was recently published in [20].

The bounded distance decoding problem (BDD) for a lattice $\mathbf{L}$ is as follows. Given any $\mathbf{x}$ to find a lattice vector $\mathbf{v} \in \mathbf{L}$ such that $||\mathbf{x}-\mathbf{v}|| \leq B$ where B is a fixed bound. In many applications $B = \gamma\lambda_1(\mathbf{L})$ is assumed. Attacks on LWE and Ring-LWE by bounded distance decoding with pruning were given in [35]. For algebraic attacks on LWE we refer to [1]. As indicated in [38], a polynomial time algorithm to find the secret key in the binary LWE can be obtained by the method in [1] when n^2 samples are available. For binary LWE and Ring-LPN (learning parity with errors over ring) we refer to [27] for sub-exponential attacks. We refer to [10] for solving Ring-LWE under some conditions about samples and secret distributions and [52] for algebraic structure improvement on the Blum-Kalai-Wasserman algorithm.

2 Our contribution

2.1 Main results

We consider the LWE over a number field lattice $\mathbf{L}$. Let q be a modulus parameter. $\mathbf{a}$ and $\mathbf{s}$ are taken uniformly in $\mathbf{O}_q^{\mathbf{L}} = \mathbf{O}^{\mathbf{L}}/q\mathbf{O}^{\mathbf{L}}$ and $\mathbf{L}_q^{\vee} = \mathbf{L}^{\vee}/q\mathbf{L}^{\vee}$. The error $\mathbf{e}$ is sampled in $\mathbf{L}_q^{\vee} = \mathbf{L}^{\vee}/q\mathbf{L}^{\vee}$ according to a discrete Gaussian distribution.

Let $f(x) \in \mathbf{Z}[x]$ be an irreducible polynomial with degree n and $\mathbf{K} = \mathbf{Q}[x]/(f) = \mathbf{Q}[\theta]$ be an algebraic number field. Let $\mathbf{b}_1^{\vee}, \ldots, \mathbf{b}_n^{\vee}$ be a base of $\mathbf{L}^{\vee}$. Let $h(\mathbf{L}^{\vee}) \in \mathbf{R_K}$ be the element satisfying that $h(\mathbf{L}^{\vee})\mathbf{b}_i^{\vee} \in \mathbf{Z}[\theta]$, $i = 1, \ldots, n$. We set $|h(\mathbf{L}^{\vee})| = \max\{|\delta_1(h(\mathbf{L}^{\vee}))|, \ldots, |\delta_n(h(\mathbf{L}^{\vee}))|\}$ where $\delta_1, \ldots, \delta_n$ are n embeddings of $\mathbf{K}$ in $\mathbf{C}$. It is clear that there exists such an element since $\mathbf{b}_i^{\vee} \in \mathbf{Q}[\theta]$, $i = 1, \ldots, n$. For example in the case $\mathbf{K}$ is monogenic then $\mathbf{R_K} = \mathbf{Z}[\theta]$, we can set $h(\mathbf{R_K}^{\vee}) = f'(\theta)$. Here $f'(x)$ is the derivative polynomial of $f(x)$. $\mathbf{O}^{\mathbf{R_K}} = \mathbf{R_K}$, and $h(\mathbf{O}^{\mathbf{R_K}}) = 1$. When $\mathbf{L} = \mathbf{Z}[\theta])^{\vee}$, this is the order LWE over $\mathbf{Z}[\theta]$. $\mathbf{s} \in (\mathbf{Z}[\theta])_q$, $h(\mathbf{Z}[\theta]) = h(\mathbf{O}^{\mathbf{Z}[\theta])^{\vee}}) = 1$.

From $\mathbf{a} \cdot \mathbf{s} + \mathbf{e} = \mathbf{b}$ *mod* q,

$$h(\mathbf{O}^{\mathbf{L}})\mathbf{a} \cdot h(\mathbf{L}^{\vee})\mathbf{s} + h(\mathbf{O}^{\mathbf{L}})h(\mathbf{L}^{\vee})\mathbf{e} = h(\mathbf{O}^{\mathbf{L}})h(\mathbf{L}^{\vee})\mathbf{b}.$$

We have the following result.

Theorem 2.1. *Let* $\mathbf{K}$ *and* $\mathbf{L}$ *be as above and we consider the LWE over* $\mathbf{L}$. *We assume that the polynomially bounded modulus parameter* $q \leq n^{c_1}$ *(*c_1 *is an arbitrary fixed positive integer) is a factor of* $f(0)$. *f the width* σ *with respect to the canonical embedding satisfies* $\sigma \leq \frac{c_2\sqrt{logn}}{||\mathbf{N}_f||_2 \cdot |h(\mathbf{O}^{\mathbf{L}})| \cdot |h(\mathbf{L}^{\vee})|}$, *where* c_2 *is another arbitrary fixed positive integer, then LWE over the number field lattice* $\mathbf{L}$ *can be solved by a* $O(n^{4c_2^2})$ *complexity algorithm.*

It is clear $f(x+u)$, h is an arbitrary integer, is also a defining equation of the number field $\mathbf{K}$. It has n roots $\theta - u, \theta_2 - u, \ldots, \theta_n - u$. $h(\mathbf{L}^{\vee})\mathbf{e}$ can be expanded in $\mathbf{Z}[\theta - u]$ as follows.

$$h(\mathbf{L}^{\vee})\mathbf{e} = e_0'' + e_1''(\theta - u) + \cdots + e_{n-1}''(\theta - u)^{n-1},$$

where $e_i' \in \mathbf{Z}/q\mathbf{Z}$, $i = 0, 1, \ldots, n-1$.

Corollary 2.1. *Let* $\mathbf{K}$ *and* $\mathbf{L}$ *be as above and we consider the LWE over* $\mathbf{L}$*. We assume that* $q \leq n^{c_1}$ *is a factor of* $f(u)$ *for an arbitrary integer* u *where* c_1 *is an arbitrary fixed positive integer. Then for this modulus parameter* q *if the width* σ *with respect to the canonical embedding satisfies* $\sigma \leq \frac{c_2(\sqrt{logn})q}{||\mathbf{N}_{f(x+u)}||_2 \cdot |h(\mathbf{O}^{\mathbf{L}})| \cdot |h(\mathbf{L}^{\vee})|}$ *where* c_2 *is another arbitrary fixed positive integer, then LWE over the number field lattice* $\mathbf{L}$ *can be solved by a* $O(n^{4c_2^2})$ *complexity algorithm.*

Corollary 2.2. *Let* $\mathbf{K}$, $\mathbf{R}_{\mathbf{K}}$ *and we consider the dual form of Ring-LWE problem as in Section 1. Assume that*
1) $\mathbf{K} = \mathbf{Q}[x]/(f)$ *is monogenic;*
2) $q \leq n_1^c$ *is a polynomially bounded factor of* $f(u)$ *for some integer* u *where* c_1 *is an arbitrary fixed positive integer, we denote the polynomial* $f_u = f(x+u)$*;*
3) The width σ *in the dual form of RING-LWE with respect to the canonical embedding satisfies* $\sigma \leq \frac{c_2(\sqrt{logn})q}{||\mathbf{N}_{f_u}||_2 \cdot \max f'}$*, where* c_2 *is an arbitrary fixed positive constant. Here we recall* $\max f' = \max\{|f'(\theta_1)|, \ldots, |f'(\theta_n)|\}$*, where* $\theta_1, \ldots, \theta_n$ *are* n *roots of the defining equation* f*.*
Then when n *is sufficiently large, for a non-negligible probability* $\frac{1}{q} \geq \frac{1}{n^{c_1}}$ *of secrets* $\mathbf{s}$*, the decision version of the dual form of Ring-LWE over* $\mathbf{R}_{\mathbf{K}}$ *can be solved within a polynomial time* $O(n^{4c_2^2})$*.*

Corollary 2.3. *Let* $\mathbf{K}_q = \mathbf{Q}[x]/(f_q)$*,* $f_q(x) = x^n + q$ *and we consider the dual form of Ring-LWE. Assume that*
1) q *has a prime factor with exponent* 1*.* n *is a two–to-power of* 2^k*,* q *is square-free and* 4 *can not divide* $((-q)^n + q)$*;*
2) $q \leq n^{c_1}$ *where* c_1 *is an arbitrary fixed positive integer;*
2) The width σ *in the dual form of RING-LWE with respect to the canonical embedding satisfies* $\sigma \leq c_2\sqrt{\frac{logn}{n}}q^{1/n}$ *where* c_2 *is another arbitrary fixed positive integer.*
Then when n *is sufficiently large, for a non-negligible probability* $\frac{1}{q} \geq \frac{1}{n^c}$ *of secrets* $\mathbf{s}$*, the decision version of the dual form of Ring-LWE for modulus parameter* q *over* $\mathbf{R}_{\mathbf{K}}$ *can be solved within a polynomial time* $O(n^{4c_2^2})$*.*

The following result is to transform the learning with errors equation $\mathbf{a} \cdot \mathbf{s} + \mathbf{e} \equiv \mathbf{b}$ *mod* q to a weaker equation $\mathbf{a} \cdot \mathbf{s} + \mathbf{e} \equiv \mathbf{b}$ *mod* $\mathbf{L}_1$ where $\mathbf{L}_1$ is a sub-lattice of $\mathbf{L}^{\vee}$ containing $q\mathbf{L}^{\vee}$. In previous works [22, 11, 44] only the case $\mathbf{L}$ is an ideal was considered.

Theorem 2.2. *Let* $\mathbf{K}$ *be a degree* n *extension field of* $\mathbf{Q}$ *and* $\mathbf{L} \subset \mathbf{K}$ *be a number field lattice. We consider the LWE over the number field lattice* $\mathbf{L}$*. Suppose that* $\mathbf{L}_1$ *is a sub-lattice of* $\mathbf{L}^\vee$ *satisfying* $q\mathbf{L}^\vee \subset \mathbf{L}_1 \subset \mathbf{L}^\vee$ *and the cardinality* $|\mathbf{L}^\vee/\mathbf{L}_1| \leq n^{c_1}$ *where* c_1 *is an arbitrary fixed positive integer.* $\mathbf{L}_1^\vee \subset \mathbf{K}$ *is the dual lattice of* $\mathbf{L}_1$ *under the trace inner product. If the width* σ *of Gaussian with respect to the canonical embedding satisfies* $\sigma \leq \frac{c_2\sqrt{logn}}{\lambda_1(\mathbf{L}_1^\vee)}$*, then for* $\mathbf{a} \in \mathbf{O}^{\mathbf{L}}$ *satisfying the following property A)*

A) There exist $\mathbf{a}_1$ *and* $\mathbf{a}_2$ *in* $\mathbf{O}^{\mathbf{L}}$ *satisfying* $\mathbf{a}\mathbf{a}_1 + q\mathbf{a}_2 = 1$ *and* $\mathbf{a}_1\mathbf{L}_1 \subset \mathbf{L}_1$*,*

$\mathbf{s}$ *mod* $\mathbf{L}_1$ *can be determined with a probability greater than* $\frac{1}{|\mathbf{L}^\vee/\mathbf{L}_1|} + \frac{1}{n^{4c_2^2}|\mathbf{L}^\vee/\mathbf{L}_1|}$ *from the LWE equation in a* $O(n^2)$ *complexity.*

The following Corollary 2.4 is direct application of Theorem 2.2 in the case $\mathbf{L} = \mathbf{R_K}^\vee$.

Corollary 2.4. *Let* $\mathbf{K}$ *be a degree* n *extension field of* $\mathbf{Q}$*. We consider the non-dual form of Ring-LWE over* $\mathbf{K}$*. Suppose that* $\mathbf{L} \subset \mathbf{R_K}$ *is a rank* n *lattice satisfying* $q\mathbf{R_K} \subset \mathbf{L} \subset \mathbf{R_K}$ *and the cardinality* $|\mathbf{R_K}/\mathbf{L}| \leq n^{c_1}$*, where* c_1 *is an arbitrary fixed positive integer. If the width* σ *of Gaussian with respect to the canonical embedding satisfies* $\sigma \leq \frac{c_2\sqrt{logn}}{\lambda_1(\mathbf{L}^\vee)}$ *where* $\mathbf{L}^\vee \subset \mathbf{K}$ *is the dual lattice of* $\mathbf{L}$ *under the trace inner product, then for* $\mathbf{a} \in \mathbf{R_K}$ *satisfying the following property A)*

A) There exist $\mathbf{a}_1$ *and* $\mathbf{a}_2$ *in* $\mathbf{R_K}$ *satisfying* $\mathbf{a}\mathbf{a}_1 + q\mathbf{a}_2 = 1$ *and* $\mathbf{a}_1\mathbf{L} \subset \mathbf{L}$*,*

$\mathbf{s}$ *mod* $\mathbf{L}$ *can be determined with a probability greater than* $\frac{1}{|\mathbf{R_K}/\mathbf{L}|} + \frac{1}{n^{4c_2^2}|\mathbf{R_K}/\mathbf{L}|}$ *from the non-dual Ring-LWE equation in a* $O(n^2)$ *complexity.*

We should notice that for hard algebraically structured LWE instances, $\mathbf{s}$ *mod* $\mathbf{L}_1$ for uniformly distributed $\mathbf{s} \in \mathbf{L}^\vee/q\mathbf{L}^\vee$ is uniformly distributed in $\mathbf{L}^\vee/\mathbf{L}_1$ for any sub-lattice $\mathbf{L}_1 \subset \mathbf{L}^\vee$ containing $q\mathbf{L}^\vee$. That is for each possibility of $\mathbf{L}^\vee/\mathbf{L}_1$, $\mathbf{s}$ *mod* $\mathbf{L}_1$ occurs with a probability $\frac{1}{|\mathbf{L}^\vee/\mathbf{L}_1|}$. Hence if elements satisfying the condition A) is non-negligible Theorem 2.2 and Corollary 2.4 show that decision LWE can be solved within a polynomial time.

From Theorem 2.2 we have the following result about the solvable algebraically structured LWE over ideals. In particular when $N(\mathbf{I})$ is exponential large the bound on the width about solvable LWE instances are quite large since $\lambda_1(\mathbf{J}^\vee)$ can be quite large.

Corollary 2.5. *Let* $\mathbf{K}$ *be a degree* n *extension field of* $\mathbf{Q}$ *and* $\mathbf{L} = \mathbf{I} \subset \mathbf{R_K}$ *be an ideal in* $\mathbf{R_K}$*. Suppose* $\mathbf{J}$ *is a fractional ideal satisfying* $\mathbf{I} \subset \mathbf{J} \subset \frac{1}{q}\mathbf{I}$ *and* $N(\mathbf{J}/\mathbf{I}) \leq n^{c_1}$ *where* c_1 *is an arbitrary fixed positive integer. If the width* σ *of Gaussian with respect to the canonical embedding satisfies* $\sigma \leq \frac{c_2\sqrt{logn}}{\lambda_1(\mathbf{J})}$*, then for* $\mathbf{a} \in \mathbf{R_K}$ *which is coprime to* q*,* $\mathbf{s}$ *mod* $\mathbf{J}^\vee$ *can be determined with a probability greater than* $\frac{1}{N(\mathbf{J}/\mathbf{I})} + \frac{1}{n^{4c_2^2}N(\mathbf{J}/\mathbf{I})}$ *from the LWE equation in a* $O(n^2)$ *complexity.*

For a sub-lattice $\mathbf{L} \subset \mathbf{R_K}$ we define a new sub-lattice $m(\mathbf{L}) = \mathbf{L} + \mathbf{L} \cdot \mathbf{L} + \cdots + \mathbf{L} \cdots \mathbf{L} + \cdots$. Since each element in $\mathbf{R_K}$ is an algebraic integer with degree at most n, then $\mathbf{b}_{i_1}^{j_1} \cdots \mathbf{b}_{i_t}^{j_t}$, $i_1, \ldots, i_t \in \{1, 2, \ldots, n\}$, $j_1, \ldots, j_t \leq n-1$ span the lattice $m(\mathbf{L})$ where $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ is a base of the lattice $\mathbf{L}$. If $\mathbf{L}$ is in some integral lattice $\mathbf{I}$, it is obvious $m(\mathbf{L}) \subset \mathbf{I}$. We also have $\mathbf{L} \cdot m(\mathbf{L}) \subset m(\mathbf{L})$.

Corollary 2.6. *Let* $\mathbf{K}$ *be a degree* n *extension field of* $\mathbf{Q}$*. We consider the non-dual form of Ring-LWE over* $\mathbf{K}$*. Suppose that* $\mathbf{L} \subset \mathbf{R_K}$ *is a sub-lattice satisfying* $q\mathbf{R_K} \subset \mathbf{L} \subset \mathbf{R_K}$ *and the cardinality* $|\mathbf{R_K}/\mathbf{O}| \leq n^{c_1}$*, where* c_1 *is an arbitrary fixed positive integer. If the width* σ *of Gaussian with respect to the canonical embedding satisfies* $\sigma \leq \frac{c_2\sqrt{logn}}{\lambda_1((m(\mathbf{L}))^\vee)}$*, then for a probability at least* $\frac{1}{n^{c_1}}$ *of* $\mathbf{s} \in \mathbf{R_K}$ *the decision non-dual Ring-LWE can be solved in a* $O(n^{4c_2^2+c_1})$ *complexity.*

Corollary 2.7. *Let* $\mathbf{K}$ *be a degree* n *extension field of* $\mathbf{Q}$*. We consider the non-dual form of Ring-LWE over* $\mathbf{K}$*. Suppose thta* $\mathbf{L} \subset \mathbf{R_K}$ *is a sub-lattice satisfying*
1) $\mathbf{L} \cdot \mathbf{L} \subset \mathbf{L}$*;*
2) $q\mathbf{R_K} \subset \mathbf{L} \subset \mathbf{R_K}$*;*
3) the cardinality $|\mathbf{R_K}/\mathbf{O}| \leq n^{c_1}$ *where* c_1 *is an arbitrary fixed positive integer.*
If the width σ *of Gaussian with respect to the canonical embedding satisfies* $\sigma \leq \frac{c_2\sqrt{logn}}{\lambda_1(\mathbf{L}^\vee)}$*, then for a probability at least* $\frac{1}{n^{c_1}}$ *of* $\mathbf{s} \in \mathbf{R_K}$ *the decision non-*

dual Ring-LWE can be solved in a $O(n^{4c_2^2+c_1})$ complexity.

2.2 Comparison with bounds in Crypto 2015 and Eurocrypt 2016 papers

In Theorem 2.1 conditions on the width do not lead to the case that the width σ' of the error distribution $e_0, \ldots, e_{n-1}$ is too small or skew such that the instance can be reduced to the errorless case. For example for the number fields in Corollary 2.3, in previous Crypto 2015 paper and Eurocrypt 2016 paper [23, 11] the width σ with respect to the canonical embedding has to satisfy

$$\sigma \leq \frac{q}{4\sqrt{\pi}n^2(q-1)^{\frac{3}{2}-\frac{3}{2n}}}$$

in [23] Theorem 5.3 (notice that the defining polynomial in [23] is of the form $x^n + q - 1$) and

$$\sigma \leq \frac{(q-1)^{1/n}}{n}$$

in [11] Subsection 3.3. It is clear that the bound on the width σ

$$\sigma \leq c\sqrt{\frac{logn}{n}}q^{1/n}$$

in Corollary 2.3 is better. The distinguishing from the uniform distribution in [23] was realized by χ statistic test or by a theoretical argument in [23, 11, 44]. In this paper the distinguishing is proved by a direct probability computation.

In Corollary 2.4 if $\mathbf{L}$ is required to be an ideal in $\mathbf{R_K}$, then from the inequality $\lambda_1(\mathbf{L}^\vee) \geq \sqrt{n}(N(\mathbf{L}^\vee)^{1/n}$ and $N(\mathbf{L}^\vee) \geq \frac{1}{n^{c_1}}$, we have

$$\frac{c_2\sqrt{logn}}{\lambda_1(\mathbf{L}^\vee)} \leq c_3\sqrt{\frac{logn}{n}}$$

for sufficiently large n and a suitable positive constant c_3. This conclusion in Corollary 2.4 is similar as the result of Corollary 2.3. This can be compared with Theorem 5.2 in page 25 of [44]. However if $\mathbf{L}$ is only required as a rank n sublattice containing $q\mathbf{R_K}$, $\lambda_1(\mathbf{L}^\vee)$ can be quite small and the bound on the width σ might be better as Corollary 2.6.

2.3 Theoretical implications

In this paper we distinguish factors of $f(u)$, where $f \in \mathbf{Z}[x]$ is the defining equation and u is an arbitrary integer, as **algebraically weak** modulus parameters. For these modulus parameters Ring-LWE, Order-LWE, Polynomial LWE and generally LWE over number field lattices problems can be transformed to distinguish the discretization of one-dimensional continuous Gaussian from the uniform distribution, that is, only the term e_0 of error distribution is involved in the problem (see Proof of Theorem 2.1). This leads to a better bound on widths of solvable instances of Ring-LWE as showed in Corollary 2.3. On the other hand there is no such algebraically weak modulus parameters for plain LWE problems.

Secondly we give a lower bound on widths of "hard" instances of learning with errors problems over number field lattices. In the case of non-dual form of Ring-LWE this new lower bound is better than previous works and analysis in [23, 11, 44].

2.4 Practical attacks

For non-dual form of Ring-LWE in an arbitrary number field $\mathbf{K}$ we need to check $\lambda_1((m(\mathbf{L})^\vee)$ for these sub-lattice $\mathbf{L}$ satisfying $q\mathbf{R_K} \subset \mathbf{L} \subset \mathbf{R_K}$ and $|\mathbf{R_K}/\mathbf{L}| \leq M$ at least for some fixed positive constant M. If the width is smaller than the bound $\frac{1}{\lambda_1((m(\mathbf{L}))^\vee)}$ both search and decision versions of Ring-LWE can be solved from Theorem 2.2, Corollary 2.6.

2.5 An open problem

For a sub-lattice $\mathbf{L} \subset \mathbf{R_K}$ satisfying $q\mathbf{R_K} \subset \mathbf{L} \subset \mathbf{I}$, where $\mathbf{I}$ is an ideal, and the cardinality $|\mathbf{R_K}/\mathbf{L}| \leq poly(n)$ (then $|\mathbf{R_K}/\mathbf{I}| \leq poly(n)$ and $\lambda_1(\mathbf{I}^\vee)$ can not be very small), if $\lambda_1((m(\mathbf{L}))^\vee)$ is very small then it follows from Corollary 2.6 a new very large bound on the width of solvable Ring-LWE can be obtained. It is natural to ask the following question. Notice that $m(\mathbf{L}) \subset \mathbf{I}$ and $\lambda_1((m(\mathbf{L}))^\vee) \leq \lambda_1(\mathbf{I}^\vee)$.

Problem I. *Is there a sub-lattice $\mathbf{L} \subset \mathbf{R_K}$ with a polynomially bounded cardinality $|\mathbf{R_K}/\mathbf{L}| \leq poly(n)$ satisfying $\mathbf{L} \cdot \mathbf{L} \subset \mathbf{L}$ and very small $\lambda_1((\mathbf{L}^\vee)$? In particular is there such a sub-lattice with very small $\lambda_1(\mathbf{L}^\vee)$ leading to a*

bound about width in the range of hardness reduction results in [46]?

3 Algebraic and probability computation

3.1 Algebraic reduction

We consider the LWE over number field lattice $\mathbf{L} \subset \mathbf{K}$, where $\mathbf{K} = \mathbf{Q}[\theta]$ is a number field. $\mathbf{a} \cdot \mathbf{s}$ can be expressed as $(1, \theta, \ldots, \theta^{n-1}) \cdot \mathbf{A}^\tau \cdot \mathbf{s}$, where $\mathbf{a} = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}, \mathbf{s} = s_0 + s_1\theta + \cdots + s_{n-1}\theta^{n-1}$. Here we assume $\mathbf{s} = (s_0, s_1, \ldots, s_{n-1})^\tau \in (\mathbf{Z}/q\mathbf{Z})^n$. By multiplying a suitable factor $h(\mathbf{L}^\vee)$ this is always true. $\mathbf{A}^\tau$ is the matrix form of the multiplication of $\mathbf{a}$ in $\mathbf{K}$. The entries of the matrix $\mathbf{A}$ are from the coefficients of the polynomial f and $\mathbf{a}$. The computation of $\mathbf{A}$ is from the relation $f(\theta) = 0$ reducing the term θ^j, $j \geq n$ to a linear combination of lower power terms $1, \theta, \ldots, \theta^{n-1}$. We have the following result.

Theorem 3.1. *The matrix $\mathbf{A}^\tau$ has n distinct eigenvalues $a_0 + a_1\theta_t + \cdots + a_{n-1}\theta_t^{n-1}$ with eigenvector $\mathbf{U}_t = (1, \theta_t, \ldots, \theta_t^{n-1})$, where $\theta_1, \ldots, \theta_n$ are n roots of $f(x)$. That is, we have*

$$\mathbf{U}_t \cdot \mathbf{A}^\tau = (a_0 + a_1\theta_t + a_2\theta_t^2 + \cdots + a_{n-1}\theta_t^{n-1})\mathbf{U}_t.$$

Proof. We have $\mathbf{U}_t \cdot \mathbf{A}^\tau \cdot \mathbf{s} = \mathbf{a} \cdot \mathbf{s} = (a_0 + a_1\theta_t + \cdots + a_{n-1}\theta_t^{n-1})(s_0 + s_1\theta_t + \cdots + s_{n-1}\theta_t^{n-1}) = (a_0 + a_1\theta_t + \cdots + a_{n-1}\theta_t^{n-1})\mathbf{U}_t \cdot \mathbf{s}$ for any possible $\mathbf{s}$, since θ_t is a root of the polynomial f. Then

$$(\mathbf{U}_t \cdot \mathbf{A}^\tau - (a_0 + a_1\theta_t + \cdots + a_{n-1}\theta_t^{n-1})\mathbf{U}_t) \cdot \mathbf{s} = 0$$

for any possible $\mathbf{s}$. Thus $\mathbf{U}_t \cdot \mathbf{A}^\tau - (a_0 + a_1\theta_t + \cdots + a_{n-1}\theta_t^{n-1})\mathbf{U}_t = 0$. The conclusion is proved.

Theorem 3.2. *Let q be a positive integer such that $w \in \mathbf{Z}/q\mathbf{Z}$ is a root of $f(x)$ module q. Set $\mathbf{w} = (1, w, \ldots, w^{n-1})$. Then $\mathbf{w} \cdot \mathbf{A}^\tau \equiv (a_0 + a_1w + a_2w^2 + \cdots + a_{n-1}w^{n-1})\mathbf{w}$ mod q.*

Proof. Since $f(w) \equiv 0$ *mod* q, then taking the congruence module q, w^j, $j \geq n$ can also be represented as a linear combination of lower power terms $1, w, \ldots, w^{n-1}$ by the same relation as $f(w) = 0$ *mod* q. We have

$\mathbf{w}\cdot\mathbf{A}^\tau\cdot\mathbf{s} \equiv (a_0+a_1w+\cdots+a_{n-1}w^{n-1})(s_0+s_1w+\cdots+s_{n-1}w^{n-1})$ *mod* q. That is for any $\mathbf{s} \in (\mathbf{Z}/q\mathbf{Z})^n$, we have $(\mathbf{w}\cdot\mathbf{A}^\tau-(a_0+a_1w+\cdots+a_{n-1}w^{n-1})\mathbf{w})\cdot\mathbf{s} \equiv 0$ *mod* q. Then $\mathbf{w}\cdot\mathbf{A}^\tau \equiv (a_0+a_1w+a_2w^2+\cdots+a_{n-1}w^{n-1})\mathbf{w}$ *mod* q.

For example when $n=2^m$, $d=2^{m-1}$, the cyclotomic polynomial $\Phi_{2^m}(x) = x^{2^{m-1}}+1$. Then $\xi_n^d=-1$ and $\xi_n^j\mathbf{a} = -a_{d-j}-a_{d-j+1}\xi_n-\cdots-a_{d-1}\xi_n^{j-1}+a_0\xi_n^j+\cdots+a_{d-j-1}\xi_n^{d-1}$. Thus the matrix $\mathbf{A}$ is a $d\times d$ matrix of the following form.

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{d-1} \\ -a_{d-1} & a_0 & a_1 & \cdots & a_{d-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -a_2 & -a_1 & -a_0 & \cdots & a_3 \\ -a_1 & -a_2 & -a_3 & \cdots & a_0 \end{pmatrix}$$

3.2 Probability computation

For the discretization to $\mathbf{Z}$ of Gaussian distribution of the width σ, the probability at x is

$$p_{\sigma,discrete}(x) = \frac{e^{-\pi(\frac{x}{\sigma})^2}}{1+2e^{-\pi(\frac{1}{\sigma})^2}+2e^{-4\pi(\frac{1}{\sigma})^2}+2e^{-9\pi(\frac{1}{\sigma})^2}+\cdots+}.$$

Then after taking module q, the probability at $x \in (-\frac{q}{2}, \frac{q}{2}]$ is

$$P_{\sigma,discrete,modq}(x) = \frac{e^{-\pi(\frac{x}{\sigma})^2}+\Sigma_{k=1}^{\infty}(e^{-\pi(\frac{x+kq}{\sigma})^2}+e^{-\pi(\frac{x-kq}{\sigma})^2})}{1+2e^{-\pi(\frac{1}{\sigma})^2}+2e^{-4\pi(\frac{1}{\sigma})^2}+2e^{-9\pi(\frac{1}{\sigma})^2}+\cdots+}.$$

Theorem 3.3. *Let $q=q(n)$ be a positive integer sequence tending to the infinity. Suppose that $\mathbf{e}$ is a continuous random variable over $\mathbf{R}$ satisfying the Gaussian distribution of the width $\sigma(n) \le c\sqrt{logn}q$ where c is an arbitrary fixed positive integer. Then the discrete random variable over $\mathbf{Z}/q\mathbf{Z}$ from $\mathbf{e}$ satisfies*
1)

$$P_{\sigma,discrete,modq}(0) \ge \frac{1}{q}+\frac{1}{n^{\pi c^2+1}}.$$

if $\sigma(n)$ is not bounded and n is sufficiently large.
2)

$$P_{\sigma,discrete,modq}(0) \ge \frac{1}{1+\Sigma_{k=\pm1}^{\pm\infty}e^{-(kM)^2}} \ge c(M)$$

if $\sigma(n)$ is upper bounded by a positive constant M, where $c(M)$ is a small positive constant only depending on M.

Proof. The second conclusion is direct. We prove the first conclusion. Set $Y_1(0) = \frac{1+\Sigma_{k=\pm 1}^{\pm\infty} e^{-\pi(\frac{k}{\sigma})^2}}{\sigma}$ and $Y_2(0) = \frac{1+\Sigma_{k=\pm 1}^{\pm\infty} e^{-\pi(\frac{kq}{\sigma})^2}}{\sigma}$, from the Poisson summation formula (see [37]) we have

$$Y_1(0) = 1 + \Sigma_{k=\pm 1}^{\pm\infty} e^{-\pi(k\sigma)^2}.$$

and

$$Y_2(0) = \frac{1}{q} + \Sigma_{k=\pm 1}^{\pm\infty} e^{-\pi(k\frac{q}{\sigma})^2}.$$

Since $\Sigma_{k=\pm 1}^{\pm\infty} e^{-\pi(k\sigma)^2} \leq \Sigma_{k=\pm 1}^{\pm\infty} e^{-k\pi(\sigma)^2} = 2\frac{e^{-\pi\sigma^2}}{1-e^{-\pi\sigma^2}}$,

$$1 + e^{-\pi\sigma^2} \leq Y_1(0) \leq \frac{1 + e^{-\pi\sigma^2}}{1 - e^{-\pi\sigma^2}}.$$

On the other hand $Y_2(0) \geq \frac{1}{q}(1 + e^{-\pi(\frac{\sigma}{q})^2}) \geq \frac{1}{q}(1 + \frac{1}{n^{\pi c^2}})$ from the condition $\sigma(n) \leq c\sqrt{logn}q$. The conclusion follows directly.

3.3 Gautschi's bound on the ∞ norm of inverses of Vandermonde matrices

Since the estimation of the bound $||\mathbf{N}_f||_2$ for the inverse of Vandermonde matrix $\mathbf{N}_f$ is needed in our results, we recall th Gautschi bound in [24].

Let

$$\mathbf{V}(x_1, \ldots, x_n) = (a_{ij})_{1\leq i\leq n, 0\leq j\leq n-1} = (x_i^j)_{1\leq i\leq n, 0\leq j\leq n-1}$$

be a Vandermonde matrix and $\mathbf{V}^{-1}$ be its inverse. Here $x_1, \ldots, x_n$ are distinct complex numbers. The following result in [24] Theorem 4.4 is useful to give bounds on $||\mathbf{N}_f||_\infty$. We recall that the

$$||\mathbf{A}||_\infty = \max_{1\leq \nu n} \Sigma_{\mu=1}^{n} |a_{\nu\mu}|,$$

where $\mathbf{A} = (a_{\nu\mu})_{1\leq\nu\leq n, 1\leq\mu\leq n}$. It is clear $\frac{1}{\sqrt{n}}||\mathbf{A}||_\infty \leq ||\mathbf{A}||_2 \leq \sqrt{n}||\mathbf{A}||_\infty$.

Gautschi Theorem. *Set* $p(x) = \prod_{i=1}^{n}(x - x_i)$. *Suppose that* $x_{n+1-i} = \bar{x_i}$, *where* $\bar{x_i}$ *is the conjugate of* x_i, *and* $x_{\frac{n+1}{2}} = 0$ *if* n *is odd. If* $Re(x_i) \geq 0$ *or* $Re(x_i) \leq 0$ *for all* $i = 1, \ldots, n$. *Then*

$$\frac{|p(-1)|}{\min_i\{\frac{|1+x_i|^2}{|1-|x_i||}|p'(x_i)|\}} \leq ||\mathbf{V}^{-1}||_\infty \leq \frac{|p(-1)|}{\min_i\{\frac{|1+x_i|^2}{1+|x_i|}|p'(x_i)|\}}$$

if $Re(x_i) \geq 0$ *for all* $i = 1, \ldots, n$ *and*

$$\frac{|p(1)|}{\min_i\{\frac{|1-x_i|^2}{|1-|x_i||}|p'(x_i)|\}} \leq ||\mathbf{V}^{-1}||_\infty \leq \frac{|p(1)|}{\min_i\{\frac{|1-x_i|^2}{1+|x_i|}|p'(x_i)|\}}$$

if $Re(x_i) \leq 0$ *for all* $i = 1, \ldots, n$, *where the minimum is taken over all* i *with* $1 \leq i \leq \frac{n}{2}$.

4 Proofs and Algorithms

4.1 Proof of main results

Proof of Theorem 2.1. We first consider the situation that $\mathbf{s}, \mathbf{a}, \mathbf{e}$ are in $\mathbf{R}_{\mathbf{K}q}$. Let w be a root of the equation $f(x) \equiv 0 \ mod\ q$. From Theorem 3.1 we have $\mathbf{w} \cdot \mathbf{A}^\tau \equiv (a_0 + a_1 w + a_2 w^2 + \cdots + a_{n-1} w^{n-1})\mathbf{w} \ mod\ q$, where $\mathbf{w} = (1, w, \ldots, w^{n-1})$. Then for an unknown secret vector $\mathbf{s}$, $\mathbf{w}\cdot\mathbf{A}^\tau\cdot\mathbf{s} \equiv (a_0+a_1w+a_2w^2+\cdots+a_{n-1}w^{n-1})(s_0+s_1w+\cdots+s_{n-1}w^{n-1})\ mod\ q$. From the sample $(\mathbf{A}, \mathbf{b})$ satisfying $\mathbf{A}^\tau\cdot\mathbf{s}+\mathbf{e} \equiv \mathbf{b}\ mod\ q$, $\mathbf{w}\cdot\mathbf{A}^\tau\cdot\mathbf{s}+\mathbf{w}\cdot\mathbf{e} \equiv \mathbf{w}\cdot\mathbf{b}$ $mod\ q$. That is, $(a_0+a_1w+a_2w^2+\cdots+a_{n-1}w^{n-1})(s_0+s_1w+\cdots+s_{n-1}w^{n-1})+(e_0 + e_1w + \cdots + e_{n-1}w^{n-1}) \equiv b_0 + b_1w + \cdots + b_{n-1}w^{n-1}\ mod\ q$. Then the equality $e_0 + e_1w + \cdots + e_{n-1}w^{n-1} \equiv b_0 + b_1w + \cdots + b_{n-1}w^{n-1}\ mod\ q$ holds for secret vectors satisfying $s_0 + s_1w + \cdots + s_{n-1}w^{n-1} \equiv 0\ mod\ q$. Since q is bounded by a polynomial function of n, then for a non-negligible probability $\frac{1}{q}$ of secret vectors, $e_0 + e_1w + \cdots + e_{n-1}w^{n-1} \equiv b_0 + b_1w + \cdots + b_{n-1}w^{n-1}$ $mod\ q$.

Since $w = q$ is a root of $f(x) \equiv 0\ mod\ q$, then if $(\mathbf{a}, \mathbf{b})$ is a sample from the Ring-LWE euqation, $e_0+e_1q+\cdots+e_{n-1}q^{n-1} \equiv b_0+b_1q+\cdots+b_{n-1}q^{n-1}$ $mod\ q$, that is, $e_0 \equiv b_0\ mod\ q$ for a non-negligible probability $\frac{1}{q}$ of secrets. We only need to test if $b_0\ mod\ q$ is a uniform distribution on $(-\frac{q}{2}, \frac{q}{2}] \bigcap \mathbf{Z}$. From Theorem 3.3 e_0 as a discrete random variable differing with the uniform distribution with a term $\frac{1}{n^{4c^2}}$ at zero or bigger than a positive constant.

Then the LWE problem can be solved by testing the probability of b_0 at zero. This can be achieved by testing $O(n^{4c^2})$ samples within $O(n^{4c^2})$ time. Since $h(\mathbf{O^L})\mathbf{a}, h(\mathbf{L}^\vee)\mathbf{s}, h(\mathbf{O^L})h(\mathbf{L}^\vee)\mathbf{e}$ are in $\mathbf{R}_{\mathbf{K}q}$, we get the conclusion of Theorem 2.1.

Another simple proof of Theorem 2.1. We observe the product $\mathbf{a}\cdot\mathbf{s}$ *mod* q. Since the constant term of the defining equation $f(x)$ *mod* q is zero, then $(\theta)^j$ *mod* q, for $j \geq n$, is only $\mathbf{Z}/q\mathbf{Z}$ linear combination of $\theta^{n-1}, \ldots, \theta$ *mod* q. Then $a_0 s_0 + e_0 \equiv b_0$ *mod* q from the Ring-LWE equaition $\mathbf{a}\cdot\mathbf{s}+\mathbf{e} \equiv \mathbf{b}$ *mod* q. For a probability $\frac{1}{q}$ of secrets $s_0 \equiv 0$ *mod* q. Then $e_0 \equiv b_0$ *mod* q for a probability $\frac{1}{q}$ of secrets. From Theorem 3.3 the conclusion of Theorem 2.1 follows.

Proof of Corollary 2.1 It follows from Theorem 2.1 directly.

Proof of Corollary 2.2. This statement follows from Corollary 2.1 and Subsubsection 1.4.4.

Proof of Corollary 2.3. The n roots are $q^{1/n}\xi_j$, where ξ_j, $j = 1, 2, \ldots, n = 2^k$ are 2^k primitive 2^{k+1}-th root of unity. Here we notice $(\xi_j)^{2^k} = -1$. Then the conclusion of Corollary 2.3 follows from Corollary 2.2 and $||\mathbf{N}_f||_2 = \frac{1}{\sqrt{n}}$ (see [11]).

Proof of Theorem 2.2. We consider the secret $\mathbf{s} \in \mathbf{L}_1/q\mathbf{L}_1$, since the cardinality $|\mathbf{L}^\vee/\mathbf{L}_1| \leq n^{c_1}$, these secrets occurs with a non-negligible probability $\frac{1}{n^{c_1}}$. From the equation $\mathbf{a}\cdot\mathbf{s}+\mathbf{e} \equiv \mathbf{b}$ *mod* q, where $\mathbf{a} \in (\mathbf{O^L})_q$, $\mathbf{s} \in \mathbf{L}_1$, $\mathbf{eb} \in (\mathbf{L}^\vee)_q$ and $q\mathbf{L}^\vee \subset \mathbf{L}_1$, we have $\mathbf{e} \equiv \mathbf{b}$ *mod* $\mathbf{L}_1$. Set the probability that $\mathbf{b} \equiv 0$ *mod* $\mathbf{L}_1$ as $P_{\mathbf{b}}$. Then $\mathbf{b}$ *mod* $\mathbf{L}_1$ is a uniform distribution if $(\mathbf{a}, \mathbf{b})$ is not from the LWE equation, that is, $P_{\mathbf{b}} = \frac{1}{|\mathbf{L}^\vee/\mathbf{L}_1|}$ if $(\mathbf{a}, \mathbf{b})$ is not from the LWE equation. We calculate the probability $P_{\mathbf{e}}$ of the condition $\mathbf{e} \equiv 0$ *mod* $\mathbf{L}_1$. It is clear

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

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 [37]) we have

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

and

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

Then a similar argument as the proof of Theorem 3.3 gives the conclusion $P_{\mathbf{e}} \geq \frac{1}{|\mathbf{L}^\vee/\mathbf{L}_1|} + \frac{1}{n^{4c_2^2}|\mathbf{L}^\vee/\mathbf{L}_1|}$. Then $\mathbf{a} \cdot \mathbf{s} \equiv \mathbf{b}$ *mod* $\mathbf{L}_1$ holds for a probability greater than $\frac{1}{|\mathbf{L}^\vee/\mathbf{L}_1|} + \frac{1}{n^{4c_2^2}|\mathbf{L}^\vee/\mathbf{L}_1|}$.

We have $\mathbf{a} \cdot \mathbf{a}_1 + q\mathbf{a}_2 = 1$ for some $\mathbf{a}_1$ and $\mathbf{a}_2$ in $\mathbf{O}^{\mathbf{L}}$ such that $\mathbf{a}_1\mathbf{L}_1 \subset \mathbf{L}_1$. It follows $\mathbf{a}_1\mathbf{a}\mathbf{s} = \mathbf{s} - q\mathbf{a}_2\mathbf{s} \equiv \mathbf{a}_1\mathbf{b}$ *mod* $\mathbf{a}_1\mathbf{L}_1$. Since $\mathbf{a}_1\mathbf{L}_1 \subset \mathbf{L}_1$ and $q\mathbf{a}_2\mathbf{s} \in q\mathbf{L}^\vee \subset \mathbf{L}_1$ we have $\mathbf{s} \equiv \mathbf{a}_1\mathbf{b}$ *mod* $\mathbf{L}_1$. The conclusion follows directly.

Proof of Corollary 2.4. Corollary 2.4 follows from Theorem 2.2 directly.

Proof of Corollary 2.5. Corollary 2.5 follows from Theorem 2.2. directly.

Proof of Corollary 2.6. When the secret $\mathbf{s} \in \mathbf{L}$ with a probability at least $\frac{1}{n^{c_1}}$, for $\mathbf{a} \in \mathbf{L}$ with a probability at least $\frac{1}{n^{c_1}}$, $\mathbf{as} \in m(\mathbf{L})$. Then $\mathbf{e} \equiv \mathbf{b}$ *mod* $m(\mathbf{L})$ is a uniform distribution. From Theorem 2.2 $P_{\mathbf{e}} \geq \frac{1}{|\mathbf{R}_\mathbf{K}/m(\mathbf{L})|} + \frac{1}{n^{4c_2^2}|\mathbf{R}_\mathbf{K}/m(\mathbf{L})|}$. Then the conclusion follows directly.

Proof of Corollary 2.7. It follows from Corollary 2.6 directly.

4.2 Algorithms

The algorithm for Theorem 2.1 is as follows. For given samples $(\mathbf{a}, \mathbf{b})$, we test the probability of $(\mathbf{b})_q \equiv \mathbf{b}_0$ *mod* q. If it is not from the Ring-LWE equation $\mathbf{a}\cdot\mathbf{s}+\mathbf{e} = \mathbf{b}$, it is $\frac{1}{q}$. If the sample is from the equation $\mathbf{a}\cdot\mathbf{s}+\mathbf{e} = \mathbf{b}$, then for a non-negligible probability of $\frac{1}{q}$ of $\mathbf{s}$, the probability $P((\mathbf{b})_q = 0) \geq \frac{1}{q} + \frac{1}{n^{\pi c_2^2+1}}$. This can be tested from $O(n^{4c_2^2})$ samples within $O(n^{4c_2^2})$ time complexity. The algorithm for Corollary 2.6 is to test the probability of $\mathbf{e} \equiv 0$ *mod* $m(\mathbf{L})$. The similar process gives the distinguishing from the uniform distribution.

5 More solvable instances of Ring-LWE

Our main result Theorem 2.1 can be applied to LWE over arbitrary lattices in arbitrary number fields. In this section we give some applications in two-to-power cyclotomic fields and order LWE problems.

5.1 Two-to-power cyclotomic fields

In many cases the condition in Theorem 2.1 can be satisfied for infinitely many modulus parameter q. For example when $\mathbf{K}_t = \mathbf{Q}[x]/(\Phi_{2^t})$, where $\Phi_{2^t} = x^{2^{t-1}} + 1$ is the 2^t-th cyclotomic polynomial, then for any odd prime modulus parameter $q \equiv 1 \ mod \ 2^t$, there exists a integer h such that $h^{2^{t-1}} + 1 \equiv 0 \ mod \ q$ (see Proposition 2.10 in page 13 of [53]). Therefore there exists a $1 \leq h \leq q-1$ such that $h^{2^{t-1}} + 1 \equiv 0 \ mod \ q$. Then we have the following result from Theorem 2.1.

Corollary 5.1. *Let $\mathbf{K} = \mathbf{Q}[x]/(\Phi_n)$ where $n = 2^t$, $\mathbf{R_K} = \mathbf{Z}[x]/(\Phi_n)$ and the dual form of Ring-LWE over $\mathbf{R_K}$ be as above, c_1 be an arbitrary fixed positive integer, $q \leq n^{c_1}$ be a odd prime modulus parameter satisfying $q \equiv 1 \ mod \ n$. We assume that the width σ in the dual form of Ring-LWE with respect to the canonical embedding satisfies $\sigma \leq \frac{c_2\sqrt{logn}q}{2(|h|+1)^{n/2}n}$ where c_2 is another arbitrary fixed positive integer.*
Then when n is sufficiently large, for a non-negligible probability $\frac{1}{q} \geq \frac{1}{n^{c_1}}$ of secrets $\mathbf{s}$, the decision version of the above non-dual form of Ring-LWE over $\mathbf{R_K}$ can be solved within a polynomial time $O(n^{4c_2^2})$.

Proof. The conclusion follows from Corollary 2.2 and Gautschi's bound.

The following result about the dual form of Ring-LWE over two-to-power cyclotomic fields is from Theorem 2.2 and Corollary 2.5.

5.2 Order LWE

In this subsection we give applications to order LWE in an arbitrary number field $\mathbf{K} = \mathbf{Q}[x]/(f)$ where $f \in \mathbf{Z}[x]$ is an irreducible monic polynomial.

Corollary 5.2. *Let $\mathbf{K}_n = \mathbf{Q}[x]/(f) = \mathbf{Q}[\theta]$ be an number field and we consider the order LWE over the order $\mathbf{Z}[\theta]$. Assume that*

1) The modulus parameter $q \leq n^{c_1}$ where c_1 is an arbitrary fixed positive integer and q is a factor of $f(u)$ for some integer u, set $f_u = f(x+u)$;
2) The width σ of error distribution with respect to the canonical embedding satisfies $\sigma \leq \frac{c_2\sqrt{logn}}{||\mathbf{N}_{f_u}||_2}$. where c_2 is another arbitrary fixed positive constant. Then when n is sufficiently large, for a non-negligible probability $\frac{1}{n}$ of secrets $\mathbf{s}$, the decision version of the order LWE over $\mathbf{Z}[\theta]$ can be solved within a polynomial time $O(n^{4c_2^2})$.

Proof. The conclusion follows from Theorem 2.1 directly.

6 Values of irreducible polynomials in $\mathbf{Z}[x]$

The possible modulus parameters satisfying the condition 2) in Theorem 2.2 have to be factors of $f(h)$ for some integer h. We recall some results to show that this condition is not a strong restriction on modulus parameters.

First of all the following result in page 13 of [53] indicates that in cyclotomic polynomial case, the probability that a prime modulus parameter satisfying the condition 2) in Theorem 2.2 is $\frac{1}{n}$.

Proposition 5.1. *Let n be a positive integer and p be an odd prime satisfying that p is not a factor of n. Then there exists an integer h such that $\Phi_n(h) \equiv 0$ mod p if and only if $p \equiv 1$ mod n.*

The following Bouniakowsky conjecture made in 1857 [7] also suggests that there are infinitely many prime modulus parameters satisfying the condition 2 in Theorem 2.2.

Bouniakowsky conjecture. *Let $f(x) \in \mathbf{Z}[x]$ be an irreducible polynomial satisfying $\gcd(f(1), f(2), \ldots,) = 1$, then there are infinitely many integers m such that $f(m)$ is prime.*

The following result in [5] suggests that the prime factors of $f(m)$ are quite large.

Proposition 5.2. Assume that the abc conjecture is true. Suppose that $f(x) \in \mathbf{Z}[x]$ has no repeated roots. Fix $\epsilon > 0$. Then $\prod_{prime-factor-p-of-f(m)} p \gg$

$|m|^{\deg(f)-1-\epsilon}$, *where the constant implied by* $\gg$ *depends on* f *and* ϵ.

7 Conclusion

In this paper we give two types of bound on width (with respect to the canonical embedding) of solvable algebraically structured learning with errors problems in arbitrary number fields. For an arbitrary number field $\mathbf{K} = \mathbf{Q}(f)$ factors of $f(u)$ for arbitrary integer u are algebraically weak modulus parameters such that the LWE for these modulus parameters can be solved within a polynomial time for a larger bound on width. Then some better bounds on widths for provable weak instances of Ring-LWE were proved. Secondly we give sub-lattice and sub-order attacks on algebraically structured learning with errors problems in arbitrary number fields. From these attacks we need to check polynomially bounded cardinalities sub-lattices $\mathbf{L}_1 \subset \mathbf{L}^{\vee}$ for LWE over number field lattice $\mathbf{L}$ or sub-lattices $\mathbf{L} \subset \mathbf{R_K}$ for non-dual form of Ring-LWE problems. In practice this means that widths have to be at least as large as $\max_{|\mathbf{L}^{\vee}/\mathbf{L}_1| \leq poly(n)} \{\frac{1}{\lambda_1(\mathbf{L}_1^{\vee})}\}$ if $\mathbf{O}^{\mathbf{L}_1}$ is non-negligible or at least as large as $\max_{|\mathbf{R_K}/\mathbf{L}| \leq poly(n)} \{\frac{1}{\lambda_1((m(\mathbf{L}))^{\vee})}\}$.

Acknowledgement. The author is grateful to Professor Chris Peikert for indicating the mistake in the previous version of this paper.

References

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

[2] M. R. Albrecht, R. Player and S. Scott, On the concrete hardness of learning with errors, Journal of Mathematical Cryptology, **9**, 169-203, 2015.

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

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

[5] A. D. Barry, The abc conjecture and k-free numbers, Master's thesis, Mathematical Institute, Universiteit Leiden, 2007.

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

[7] V. Bouniakowsky, Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la de composition des entiers en facteurs, Sc. Math. Phys. **6**, 305-329, 1857.

[8] Z. Brakerski, C. Gentry and V. Vaikuntanathan, (leveled) fully homomorphic encryption without bootstrapping, Proc. 3rd Innovations in Theoretical Computer Sciences, 2012.

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

[10] Z. Brakerski and R. Perlman, Order-LWE and the hardness of ring-lwe with entropic secrets, Cryptology ePrint Archive, Report 2018/494, 2018.

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

[12] W. Castryck, I. Illashenko and F. Vercauteren, On error distribution of Ring-based LWE, Cryptology ePrint Achive, 2016/240, LMS Journal of Computation and Mathematics, vol. 19 (Special Issue A), pp.130-145, 2016.

[13] Hao Chen, On approximating SVP with pre-processing for ideal lattices, in preparation.

[14] H. Chen, K. Lauter and K. E. Stange, Attackes on search RLWE. iacr e-print 2015/971, SIAM Journal on Applied Algebra and Geometry, vol.1,665-682, 2019.

[15] 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.

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

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

[18] R. Cramer, L. Ducas, C. Peikert and O.Regev, Recovering short generators of principle ideals in cyclotomic rings, iacr e-print 2015, Eurocrypt 2016.

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

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

[21] Y. Eisentrage, S. Hallgen and K. Lauter, Weak instances of PLWE, SAC 2014.

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

[23] Y. Elias, K. Lauter, E. Ozman and K. E. Stange, Ring-LWE cryptography for the number theorist, Women in Numbers 3: Research Directions in Number Theory.

[24] W. Gautschi, Norm estimation for inverse of Vandermonde matrices, Numer. Math., vol. 23, 337-347, 1975.

[25] C. Gentry, Fully homomorphic encryption using ideal lattices, STOC 2009, 167-178.

[26] S. Garg, C. Grag and S. Halevi, Candidate multilinear maps from ideal lattices, Eurocrypt 2013, 1-17, 2013.

[27] P. Kirchner and P-A. Fouque, An improved BKW algorithm for L-WE with applications to cryptography and lattices, Cryptology ePrint Achive, 2015/552, Crypto 2015.

[28] S. Khot, Hardness of approximating the shortest vector problem, Journal of ACM, vol.52 (2005), 789-808.

[29] 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.

[30] R. Lindner and C. Peikert, Better key sizes (and attacks) for LWE-based encryption, CT-RSA, 2011, LNCS 6558, 319-339, 2011.

[31] V. Lyubashevsky, C. Peikert and O. Regev, On ideal lattices and learning with errors over rings, J. ACM, 60(6), 1-43, nov., 2013, preliminary version, Eurocrypt 2010.

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

[33] V. Lyubashevsky, Ideal lattices, tutorial in MIT, http://people.casil.mit.edu/joanne/idealtutorial.pdf

[34] K. Laine and K. Lauter, Key recovery for LWE in polynomial time, Cryptology ePrint Achive, 2015/176.

[35] M. Liu and P. Q. Nguyen, Solving BDD by enumeration, CT-RSA, 2013, LNCS 7779,293-309, 2013.

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

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

[38] D. Micciancio and C. Peikert, Hardness of SIS and LWE with small parameters, Crypto2013.

[39] D. Micciancio and M. Walter, Practial, predictable lattice basis reduction, Eurocrypt 2016.

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

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

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

[43] C. Peikert, A decade of lattice cryptography, iacr e-print, 2015/939, 2015, now Publishers Inc., 2016.

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

[45] C. Peikert and Z. Pepin, Algebraically structured LWE, revisited, Cryptology ePrint Achive, 2019/878, 2019.

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

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

[48] O. Regev, On lattices, learning with errors, random linear codes, Journal of ACM, **56**, no.6, 2009.

[49] 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.

[50] M. Roşca, A. Aakzad, D. Stehlé and R. Steinfeld, Middle-product learning with errors, Crypto 2017, 283-297, 2017.

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

[52] K. Stange, Algebraic aspects of solving Ring-LWE, includin ring-based improvement in the Blum-Kalai-Wasserman algorithm, Cryptology ePrint Archive, Report 2019/183, 2019.

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