Sublattice Attacks on Ring-LWE with Wide Error Distributions I

Hao Chen *

May 27, 2020

Abstract

Since the Lyubashevsky-Peikert-Regev Eurocrypt 2010 paper the Ring-LWE has been the hard computational problem for lattice cryptographic constructions. The fundamental problem is its hardness which has been based on the conjectured hardness of approximating ideal-SIVP or ideal-SVP. Though it is now widely conjectured both are hard in classical and quantum computation model there have no sufficient attacks proposed and considered. In this paper we propose sublattice attacks on Ring-LWE over an arbitrary number field from *sublattice pairs*. We give a sequence of number fields $\mathbf{K}_n$ of degree $d_n \longrightarrow \infty$, such that the decision Ring-LWE with very wide error distributions over integer rings of $\mathbf{K}_n$ can be solved by a polynomial (in d_n) time algorithm from our sublattice attack. The widths of error distributions in our attack is in the range of Peikert-Regev-Stephens-Davidowitz hardness reduction results in their STOC 2017 paper. Hence we also prove that approximating ideal-$SIVP_{poly(d)}$ with some polynomial factor for ideal lattices in these number fields can be solved by a polynomial time quantum algorithm.

Keywords: Ring-LWE, Width of error distribution, Sublattice attack, Sublattice pair.

*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 Algebraic number fields

An algebraic number field is a finite degree d 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 of degree d satisfying $f(\theta) = 0$ (see [13, 5]). It is well-known there is a positive definite inner product on $\mathbf{K} \otimes \mathbf{C}$ defined by $< u, v >= \Sigma_{i=1}^{d} \sigma_i(u)\widetilde{\sigma_i(v)}$, where σ_i, $i = 1, \ldots, d$, are d embedings of $\mathbf{K}$ in $\mathbf{C}$, and $\tilde{v}$ is complex conjugate. Sometimes we use $||u||_{tr}$ to represent the norm $< u, u >^{1/2}$. This is the norm with respect to the canonical embedding (see [26]). 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 [5, 12] for the detail. The dual of a lattice $\mathbf{L} \subset \mathbf{K}$ of rank $\deg(\mathbf{K}/\mathbf{Q})$ is defined by $\mathbf{L}^\vee = \{\mathbf{x} \in \mathbf{K}, tr_{K/Q}(\mathbf{ax}) \in \mathbf{Z}, \forall \mathbf{a} \in \mathbf{L}\}$. An order $\mathbf{O} \subset \mathbf{K}$ in a number field $\mathbf{K}$ is a subring of $\mathbf{K}$ which is a lattice with rank equal to $\deg(\mathbf{K}/\mathbf{Q})$. We refer to [12, 13, 5] 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 [47]). 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 $0 \le i \le n-1$

and p^2 not dividing a_0. A polynomial satisfying this condition is irreducible in $\mathbf{Z}[x]$ from the Eisenstein criterion (see [5, 13]).

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 $\mathbf{L} \subset \mathbf{R}^n$ 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 $\mathbf{D}_{\mathbf{L},\mathbf{s}}$. We refer to [31] for the following properties of discrete Gaussian distributions.
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.

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 $\mathbf{K} \otimes \mathbf{C}$ (see [26, 27, 38, 7]). We refer the further analysis to [7, 40].

1.3 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 [32]). 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 [32]). 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 [32]). A breakthrough result of M. Ajtai [3] 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 [32]). For the latest development we refer to Khot [20]. 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 [20, 21, 44], we refer to [19] for Minkowski's first and second theorems on successive minima of lattices.

1.4 Plain LWE and Ring-LWE

Plain LWE

Plain LWE and its lattice-based cryptographic construction was originated from [42]. We refer to [43] 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

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

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 [43] 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 [43]). For plain LWE without the ring structure the reduction results from approximating SVP to plain LWE were given in [43, 35, 6].

Ring-LWE

The algebraic structure of ring was first introduced to the hardness of computational problems of lattices in [29] (also in [24, 25]) for the consideration of efficiency. This is Ring-SIS (Short Integer Solution over Ring, see [29]) and it is the analogue of Ajtai's SIS problem. The one-wayness of some function was proved in [29] by assuming the hardness of some computational problems of cyclic lattices (ideal lattices). Ring-LWE was originated from 2010 paper [26] and then extended in [27]. We refer to [37] for a survey of the history of development, the theory and cryptographic constructions based on Ring-LWE and Ring-SIS.

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 [18, 7]). We refer to [45] for relations and reductions between Ring-LWE and PLWE.

If the $\mathbf{Z}_q^n$ is replaced by $(\mathbf{R_K})_q = \mathbf{R_K}/q\mathbf{R_K}$ where $\mathbf{R_K}$ is the ring of integers in an algebraic number field $\mathbf{K}$ of degree n, this is the Ring-LWE, learning with errors over the ring $\mathbf{R_K}$. The secret $\mathbf{s}$ is in the dual $(\mathbf{R_K}^{\vee})_q = \mathbf{R_K}^{\vee}/q\mathbf{R_K}^{\vee}$ and $\mathbf{a} \in \mathbf{R_K}_q$ is chosen uniformly at random. The inner product $\mathbf{a} \cdot \mathbf{s} = \Sigma a_i s_i$ is replaced by the multiplication $\mathbf{a} \cdot \mathbf{s}$ in $(\mathbf{R_K}^{\vee})_q$. The error $\mathbf{e}$ is in $(\mathbf{R_K}^{\vee})_q = \mathbf{R_K}^{\vee}/q\mathbf{R_K}^{\vee}$. In this case the width of error distribution is defined by the trace norm on $\mathbf{K} \otimes \mathbf{R}$ via the canonical embedding (see [26, 7]). 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 [38] 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 [39]. 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. Set $\mathbf{O^L}_q = \mathbf{O^L}/q\mathbf{O^L}$, $\mathbf{L}^{\vee}{}_q = \mathbf{L}^{\vee}/q\mathbf{L}^{\vee}$. 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 $\mathbf{e} \in \mathbf{L}^{\vee}{}_q$. For the detail and hardness reduction we refer to [39].

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 [26, 27] for search version and then a general form to decision version was proved for arbitrary number fields in [40]. We refer to [40] Theorem 6.2 and 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* $\mathbf{I}$.

1.6 Known attacks

1.6.1 Attacks on LWE

The famous Blum-Kalai-Wasserman (BKW) algorithm in [4] was improved in [1, 22]. E Stange presented its ring-based adaption in [46]. On the other hand some provable weak instances of Ring-LWE was given in [17, 18, 11] and analysed in [7, 38]. As showed in [38, 7] 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 [8] 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.

1.6.2 Approximating ideal-SVP

In [14] it was proved approximating SVP with factor $2^{O(\sqrt{nlogn})}$ for principal ideals in cyclotomic integer rings $\mathbf{Z}[\xi_n]$ 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 [15] and [41] such that sub-exponential complexity algorithms with some pre-processing for approx-SVP with some sub-exponential factor for ideal lattices can been achieved. The analysis of the approximating factor was recently published in [16]. For the recent developments we refer to [23, 34].

2 Our contribution

2.1 Sublattice pair attack

We consider the decision non-dual Ring-LWE over the integer ring $\mathbf{R_K}$ of a number field $\mathbf{K}$ of degree d. Let q be a modulus parameter. $\mathbf{a}$ and $\mathbf{s}$ are chosen uniformly at random in $(\mathbf{R_K})_q = \mathbf{R_K}/q\mathbf{R_K}$. The error $\mathbf{e}$ is sampled in $(\mathbf{R_K})_q$ according to a discrete Gaussian distribution (with respect to the canonical embedding) with the width σ. We define sublattice pair $(\mathbf{L}_1, \mathbf{L}_2)$ as follows.

Definition. *Let $c, c_1, c_2, c < c_3 < c_4, c_4 + 3 < c_5, c_6$ be given fixed positive real numbers. For the Ring-LWE over $\mathbf{R_K}$ with the modulus parameter q satisfying $d \leq q \leq d^{c_1}$, $(\mathbf{L}_1, \mathbf{L}_2)$ is called a sublattice pair with $q, c, c_1, c_2, c < c_3 < c_4, c_5, c_6$ if the following conditions are satisfied.*
1) $\mathbf{L}_1$ and $\mathbf{L}_2$ are rank d lattices satisfying $q\mathbf{R_K} \subset \mathbf{L}_i \subset \mathbf{R_K}$ and indexes satisfy $|\mathbf{R_K}/\mathbf{L}_1| \leq d^{c_2}$ and $d^{c_3} \leq |\mathbf{R_K}/\mathbf{L}_2| \leq d^{c_4}$;
2) The probability $P_{\mathbf{e}}$ that the error $\mathbf{e} \in \mathbf{L}_1$ is lower bounded by $\frac{1}{d^{c_3-c}}$;
3) We assume that the probability of a uniformly chosen $\mathbf{a} \in \mathbf{R_K}_q$ is invertible is at least $\frac{1}{2}$. For arbitrary uniformly chosen invertible elements $\mathbf{a}_1, ..., \mathbf{a}_{d^{c_5}}$ in $\mathbf{R_K}_q$, we can find $\mathbf{a}_{j_1}, \ldots, \mathbf{a}_{j_{d^{c_4+2}}}$ within a $O(d^{c_6})$ time such that $\mathbf{a}_{j_i}^{-1}\mathbf{L}_1 \subset \mathbf{L}_2$ for $i = 1, \ldots, d^{c_4+2}$.

Here an element $\mathbf{a}$ in $\mathbf{R_K}$ is invertible in $(\mathbf{R_K})_q = \mathbf{R_K}/q\mathbf{R_K}$ if and only if there is an element $\mathbf{a}^{-1} \in \mathbf{R_K}$ such that $\mathbf{a} \cdot \mathbf{a}^{-1} \equiv 1$ *mod* q. The main condition 2) is achieved by the property that there are sufficiently many very short lattice vectors in $\mathbf{L}_1^{\vee}$, we refer to Theorem 3.1. The sublattice pair can be defined for $\mathbf{R_K}^{\vee}$ or more generally defined for LWE over an arbitrary number field lattice.

Please notice that the condition 2)

$$P_{\mathbf{e}} \geq \frac{1}{d^{c_3-c}}$$

and the condition 1)

$$\frac{1}{|\mathbf{R_K}/\mathbf{L}_2|} \leq \frac{1}{d^{c_3}}$$

implies

$$P_{\mathbf{e}} \geq \frac{d^c}{|\mathbf{R_K}/\mathbf{L}_2|}.$$

This is the main point that the samples from Ring-LWE equations can be distinguished from uniformly ones within polynomial time. We refer to the proof of Theorem 2.1.

The following result is to transform the LWE 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* $\mathbf{L}_2$ when $\mathbf{L}_2$ has a sublattice pair. In previous works [18, 7, 38] only the case $\mathbf{L}_2$ is an ideal was considered.

Theorem 2.1. *Let $\mathbf{K}$ be a degree d extension field of $\mathbf{Q}$ with the integer ring $\mathbf{R_K}$. We consider the decision non-dual Ring-LWE over $\mathbf{R_K}$ for a polynomially bounded modulus parameter q satisfying $d \leq q \leq d^{c_1}$. Suppose that* *there exists a sublattice pair* $(\mathbf{L}_1, \mathbf{L}_2)$ *with* $q, c, c_1, c_2, c < c_3 < c_4, c_4 + 3 < c_5, c_6$. *Then the decision non-dual Ring-LWE over* $\mathbf{R_K}$ *for the modulus parameter* q *can be solved in a* $O(d^{c_6+8c_1c_4+c_3})$ *time complexity.*

We consider the following sequence of irreducible polynomials $f_d = x^d - u_d x + u_d(u_d - 1) \in \mathbf{Z}[x]$, where u_d is a polynomially bounded positive integer which contain only prime factors of exponent 1. From the Eisenstein criterion f_d is an irreducible polynomial. Let $\mathbf{K}_d = \mathbf{Q}[x]/(f_d(x))$ be a degree d extension field of $\mathbf{Q}$ with the integer ring $\mathbf{R_{K_d}}$. We will take $u_d = 2p_d$ where p_d is a prime number such that $2p_d - 1$ satisfies the following property.
1) $\gcd(d-1, 2p_d - 1) = 1$;
2) All prime factors of $2p_d - 1$ are distinct and not smaller than $d - 1$.
p_d is assumed polynomially bounded and satisfies other conditions we will give explicitly in Section 5.

Theorem 2.2. *There exist a sequence of polynomially bounded positive integers* $u_d = 2p_d$ *where* p_d *is a suitable polynomially bounded prime number, and a sequence of modulus parameters* $q_d = p_d(2p_d - 1)^3$, *such that if the width of the error distributions satisfies* $\frac{\sqrt{d}}{\lambda_1(\mathbf{R_{K_d}}^\vee)} \leq \sigma \leq \frac{u_d(u_d-1)d^{C+1}}{4}$, *where* C *is an arbitrary large fixed positive integer, we can construct a sequence of sublattice pairs* $(\mathbf{L}_1^d, \mathbf{L}_2^d)$ *satisfying*
1)$|\mathbf{R_{K_d}}/\mathbf{L}_2^d|$ *is polynomially bounded and at least* $\frac{u_d^2(u_d-1)^3}{4}$;
2)The probability $\mathbf{e} \in \mathbf{L}_1^d$ *is lower bounded by* $\frac{1}{64d^{3C+1}u_d^2(u_d-1)^2}$.

The construction in Theorem 2.2 implies that for Ring-LWE over $\mathbf{R_{K_d}}$, we can always have an effective sublattice attack if the upper bound on widths (wider than the range in hardness reduction results in [40]) in Theorem 2.2 is satisfied. We should notice that from the proof of Theorem 2.1 the partial information of the private key $\mathbf{s}$ *mod* $\mathbf{L}_2$ can be found within a polynomial time when polynomially bounded many samples are given, we refer to Section 5.

Corollary 2.1. *We consider the non-dual Ring-LWE over* $\mathbf{R_{K_d}}$ *as above. There exist a sequence of polynomially bounded positive integers* $u_d = 2p_d$ *where* p_d *is a suitable polynomially bounded prime number, and a sequence of modulus parameters* $q_d = p_d(2p_d - 1)^3$, *such that if the width of the error distributions satisfies* $\frac{\sqrt{d}}{\lambda_1(\mathbf{R_{K_d}}^\vee)} \leq \sigma \leq \frac{u_d(u_d-1)d^{C+1}}{4}$ *where* C *is an arbitrary large fixed positive integer, the decision non-dual Ring-LWE with* *modulus parameter q_d can be solved in polynomial time (in d).*

We can consider the attack on the dual form of decision Ring-LWE from Corollary 2.1 since we estimates the size $|f'(\theta)|$ of "tweak factors" in Corollary 4.1. We have the following result.

Corollary 2.2. *We consider the dual form of Ring-LWE over $\mathbf{R_K}^\vee$ for the modulus parameter $q_d = p_d(2p_d - 1)^3$ where $\mathbf{K}$ is the number field as above. Suppose that the width of the error distributions satisfies $\frac{\sqrt{d}}{\lambda_1(\mathbf{R_{K_d}}^\vee)} \leq \sigma \leq d^C$ where C is an arbitrary large fixed positive integer. Then the dual form of the decision Ring-LWE with above modulus parameter q_d can be solved in polynomial time (in d).*

From the hardness reduction result Theorem 6.2 and Corollary 6.3 in [40] we have the following result. We refer to [9] for another proof of similar result without using the reduction to Ring-LWE.

Corollary 2.3. *Let $\mathbf{K}_d$ be a sequence of number field sequence with their degrees $d \longrightarrow \infty$ as in Theorem 2.2. Then approximating $SIVP_{d^{18}}$ with approximating factor d^{18} for ideal lattices in $\mathbf{K}_d$ can be solved by a polynomial (in d) time quantum algorithm.*

2.2 Sublattice attack is natural and necessary

For Ring-LWE over $\mathbf{R_K}$ the equation is $\mathbf{a} \cdot \mathbf{s} + \mathbf{e} \equiv \mathbf{b}$ *mod* q, since the modulus parameter is q, if we check each possibility there are huge exponential q^d possibilities. Therefore it is natural to check each possibility of $|\mathbf{R_K}/\mathbf{L}| \leq poly(d)$ possibilities of the weaker LWE equation $\mathbf{a} \cdot \mathbf{s} + \mathbf{e} \equiv \mathbf{b}$ *mod* $\mathbf{L}$ for each sublattice $\mathbf{L}$ satisfying

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

and

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

From this point of view it is not natural to require $\mathbf{L}$ to be an ideal. The sublattice attack on LWE over arbitrary number lattices was initiated from our previous paper [8] and extended in this paper.

In previous attacks on Ring-LWE in [18] (then analysed in [7, 38]) 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 [18] and then analysed in [7, 38] 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 . In our sublattice attack we propose to consider the equation $\mathbf{a}\cdot\mathbf{s}+\mathbf{e} \equiv \mathbf{b}\ mod\ \mathbf{L}$, where $\mathbf{L}$ is a sublattice with polynomially bounded index $|\mathbf{R_K}/\mathbf{L}|$ and satisfying $q\mathbf{R_K} \subset \mathbf{L}$. Then we find subtle sublattice $\mathbf{L}$ such that $\lambda_1(\mathbf{L}^\vee)$ is very small and there are many very short lattice vectors in $\mathbf{L}^\vee$. From Theorem 3.1 the above equation can be solved for very large widths of error distributions. Our main results indicate that asymptotically our sublattice attack on Ring-LWE is essentially much better than ideal-attack on Ring-LWE at least for certain number fields.

2.3 Sublattice pairs are needed and number-field dependent

In previous ideal-attack in [18, 7] when cosets of $\mathbf{s} \in \mathbf{R_K}/\mathbf{P}$ are checked, since $\mathbf{a} \in \mathbf{O^P} = \mathbf{R_K}$, the multiplication of $\mathbf{a} \in \mathbf{R_K}$ sends a coset to another coset. However when $\mathbf{L}$ is only a sublattice, this is not true. If we want both $\mathbf{L}$ and $\mathbf{O^L} \bigcap \mathbf{R_K}$ are polynomially bounded index in $\mathbf{R_K}$, as proved in Theorem 4.2, $\lambda_1(\mathbf{L}^\vee)$ can not be very small. Hence the sublattice attack with one sublattice as suggest in [8] do not work.

Explicit constructed sublattice pairs can be used for an efficient attack on the Ring-LWE as proved in Theorem 2.1. However these subtle sublattices depend on the number-field structures of sequences of number fields. We refer to [10] for more number fields with sublattice pairs. Sublattice pairs can be defined for LWE (learning from errors) over arbitrary number field lattices and a similar result as Theorem 2.1 can be proved. An essential problem to the Ring-LWE over number fields and the LWE over arbitrary number field lattices is the explicit construction of these subtle sublattice pairs.

2.4 Cryptographic and algorithmic implications

From Corollary 2.1 the decision Ring-LWE over certain number fields can be solved by a polynomial time algorithm in classical computation model even for error distributions with the widths in recommended range of [40]. Now it is absolutely necessary to prove that approximating ideal-$SIVP_{poly(d)}$ for two-to-power cyclotomic fields is hard in quantum and classical computation model, otherwise from our main results it would be possible that the cryptographic constructions based on Ring-LWE over two-to-power cyclotomic fields is not secure even in classical computation model.

For the complexity theory of computational problems for ideal lattices, our main result Corollary 2.2 indicates that approximating ideal-SIVP with a polynomial factor for certain number fields is easy in quantum computation model. It is interesting to know for other number field sequences whether the approximating ideal-$SIVP_{poly(d)}$ is easy or not in quantum computational model.

3 Probability computation

We need the following computation of probability in Theorem 2.2.

Theorem 3.1. *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 (with respect to the canonical embedding) 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*

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

It satisfies

$$P_{\mathbf{e}} \geq \frac{1}{e^{c_1}q^{c_2}}$$

when q *is sufficiently large.*

Proof. 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 [31]) 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 [31]. 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 $P_{\mathbf{e}} \geq \frac{1}{|\mathbf{L}^\vee/\mathbf{L}_1|}(1 + \frac{1}{e^{c_1}} \cdot \frac{|\mathbf{L}^\vee/\mathbf{L}_1|}{q^{c_2}})$. The conclusion follows directly.

4 Number theory

The following proposition is useful in this paper. Please refer to [13, 5] for the proof.

Proposition 4.1. *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

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

.

Let p be a positive integer and $p\mathbf{R}_{\mathbf{K}} = \mathbf{P}^{e_1} \cdots \mathbf{P}_t^{e_t}$ where $\mathbf{P}_i$ are prime ideals and $e_i \geq 1$ are positive integers, is the factorization of the ideal $p\mathbf{R}_{\mathbf{K}}$ to the product of prime ideals.

Proposition 4.2. *If $\mathbf{I} \subset \mathbf{R}_{\mathbf{K}}$ is an ideal containing the positive integer p, then $\mathbf{I}$ is of the form*

$$\mathbf{P}_{j_1}^{e'_1} \cdots \mathbf{P}_{j'_t}^{e'_{t'}}$$

where $t' \leq t$ $e'_i \leq e_{j_i}$.

Proof. Set $\mathbf{I} = \prod_j \mathbf{Q}_j$ the factorization of $\mathbf{I}$ to the product of prime ideals. Then $p \in \mathbf{Q}_j$ and $\mathbf{Q}_j$ is a prime ideal over p. The conclusion follows directly.

From Proposition 4.2 only few ideals $\mathbf{I}$ satisfy the condition $q\mathbf{R}_K \subset \mathbf{I}$. Hence in sublattice attack it is not natural to require a sublattice $\mathbf{L}$ satisfying $q\mathbf{R}_{\mathbf{K}} \subset \mathbf{L} \subset \mathbf{R}_{\mathbf{K}}$ to be an ideal.

We refer to [33] Theorem 1 for the following result, which is useful to estimate the trace norm of an algebraic integer.

Proposition 4.3. *For any positive integer n and $1 \leq k \leq n-1$, let $P(x) = x^n + a_{n-k-1}x^{n-k-1} + \cdots + a_0$ be a complex polynomial such that $a_0 \neq 0$. For any root α of P, we have*

$$|\alpha| \leq (n-k)^{\frac{1}{k+1}} \max_{1 \leq j \leq n} |a_{n-j}|^{\frac{1}{j}}.$$

Here $|\alpha|$ is the absolute value of the complex number α.

Set $f = x^n - ux + u(u-1)$ where u is an positive integer with only prime factors of exponent 1. Then $f(x) \in \mathbf{Z}[x]$ is an irreducible polynomial from the Eisenstein criterion. Let $\theta \in \mathbf{C}$ be a root of f, we have the following result from Proposition 4.3.

Corollary 4.1. *Let u be a positive integer satisfying $n < u \leq n^c$ for some fixed positive integer c. Then $1 < |\theta| \leq \frac{9}{8}$ when n is sufficiently large. We have $||\theta||_{tr} \leq \sqrt{2n}(u(u-1))^{\frac{1}{n}}$ and then*

$$||\theta^{n-1}||_{tr} \leq \sqrt{2n}(u(u-1))$$

and

$$||\theta^{n-2}||_{tr} \leq \sqrt{2n}(u(u-1)).$$

Moreover $f'(\theta) = n\theta^{n-1} - u$ *satisfies*

$$\frac{nu(u-1)}{2} \leq |f'(\theta)| \leq \frac{3nu(u-1)}{2}.$$

Proof. From Proposition 4.3 the inequality $|\theta| \leq \frac{9}{8}$ holds when n is sufficiently large. If $|\theta| < 1$, $|\theta^{n-1}| = |u - \frac{u(u-1)}{\theta}| > \frac{8|u(u-1)|}{9} - u \geq \frac{|u(u-1)|}{2}$. This is a contradiction. Hence $1 < |\theta|$. The other conclusions follows from Proposition 4.3 directly.

The following Kummer lemma (see [12, 5]) is useful for the decomposition of prime numbers to the product of prime ideals in number fields.

Proposition 4.4. *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*.*

We refer to [12] Theorem 6.1.4 for the following Dedekind criterion which is helpful to decide $f = |\mathbf{R_K}/\mathbf{Z}[\theta]|$.

Proposition 4.5 (Dedekind Criterion) *Let* $\mathbf{K} = \mathbf{Q}[\theta]$ *be a number field,* $T(x) \in \mathbf{Z}[x]$ *the monic minimal polynomial of* θ *and* p *be a prime number. Denote by* $\bar{a}$ *the reduction module* p *(in* $\mathbf{Z}$ *or* $\mathbf{Z}[\theta]$*). Let*

$$\bar{T(x)} = \prod_{i=1}^{k} \bar{t_i}^{e_i}$$

be the factorization of $T(x)$ module p in $\mathbf{F}_p[x]$, and set

$$g(x) = \prod_{i=1}^{k} t_i(x),$$

where $t_i \in \mathbf{Z}[x]$ are arbitrary lifts of $\bar{t_i}$. Let $h(x)$ be a monic lift of $\frac{\bar{T(x)}}{g(x)}$ and set $f(x) = \frac{g(x)h(x)-T(x)}{p}$. Then $|\mathbf{R_K}/\mathbf{Z}[\theta]|$ is not divisible by p if and only if $\gcd(\bar{f}, \bar{g}, \bar{h}) = 1$ *in $\mathbf{F}_p[x]$.*

Let $f = x^n - ux + u(u-1)$ where u is a positive integer which has only prime factors of exponent 1. Let $\theta \in \mathbf{C}$ be a root of f, $\mathbf{K} = \mathbf{Q}[\theta] = \mathbf{Q}[x]/(f)$ is the number field. Let $\mathbf{R_K}$ is the ring of integers in $\mathbf{K}$, $\mathbf{Z}[\theta] \subset \mathbf{R_K}$ is an order.

Theorem 4.1. *Let u be a positive integer satisfying*
1) $\frac{u}{p}$ is not zero in $\mathbf{F}_p$ for any prime factor p of u; and
2) All prime factors of $u-1$ are distinct and $\gcd(n-1, p) = 1$ *for any prime factor p of $u-1$.*
Let $f = x^n - ux + u(u-1)$ as above, p be a prime factor of u or $u-1$. Then $|\mathbf{R_K}/\mathbf{Z}[\theta]|$ is not divisible by p.

Proof. First of all we have $f \equiv (x^2 - ux + u^2 - u)(x^{n-2} + ux^{n-3} + ux^{n-4} + \cdots + ux + u)$ *mod* W if W is a factor of $u(u-1)^2$. When p is a factor of u, we can take $g(x) = x$, $h(x) = x^{n-1}$. Then $f(x) = \frac{x^n - (x^n - ux + u(u-1))}{p} = \frac{u}{p}x - \frac{u}{p}(u-1)$. It is easy to verify $\gcd(\bar{f}, \bar{g}, \bar{h}) = 1$ in $\mathbf{F}_p[x]$. The conclusion follows from the Dedekind criterion.

When p is a prime factor of $u-1$ we have $f(x) \equiv x(x-1)(x^{n-2} + x^{n-3} + x^{n-4} + \cdots + x + 1)$ *mod* p. Since $\gcd(n-1, p) = 1$, then $x^{n-1} - 1$ has $n-1$ distinct roots in the algebraic closure of $\mathbf{F}_p$. We can take $g(x) = x(x-1)(x^{n-2} + \cdots + x + 1)$, $h(x) = 1$. Then $f(x) = \frac{x^n - x - (x^n - ux + u(u-1))}{p} = \frac{u-1}{p}x - u\frac{u-1}{p}$. It is easy to verify that $\gcd(\bar{h}, \bar{f}, \bar{g}) = 1$ in $\mathbf{F}_p$ from the condition 2). The conclusion follows from the Dedekind criterion.

The main construction in Theorem 2.2 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 $q\mathbf{R_{K_d}} \subset \mathbf{L}_1 \subset \mathbf{R_{K_d}}$. For given $\mathbf{x}_1, \ldots, \mathbf{x}_t$, 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 $Tr(\mathbf{x}_i\mathbf{y}) \equiv 0$ *mod* q, where $\mathbf{y} \in \mathbf{R_K}$, $i = 1, \ldots, t$. It is obvious

$q\mathbf{R_K} \subset \mathbf{L} \subset \mathbf{R_K}$. 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 4.6. *The vectors $\frac{\mathbf{x}_1}{q}, \ldots, \frac{\mathbf{x}_t}{q}$ are in the dual lattice*

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

If $\mathbf{a} \in \mathbf{R_K}$ is an invertible element in $\mathbf{R_K}/q\mathbf{R_K}$, 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 gives a restriction on the $\lambda_1(\mathbf{L}^\vee)$ of number field lattice $\mathbf{L}$ if $\mathbf{L}$ containing the product of two number field lattices $\mathbf{L}_1$ and $\mathbf{L}_2$ satisfying $|\mathbf{R_K}/\mathbf{L}_i| \leq poly(n)$.

Theorem 4.2. *Let $\mathbf{L}_1, \mathbf{L}_2$ and $\mathbf{L}_3$ be three polynomially bounded cardinality sublattices of rank d in the integer ring $\mathbf{R_K}$ of a degree d number field $\mathbf{K}$. That is $|\mathbf{R_K}/\mathbf{L}_i| \leq d^c$ holds for a fixed positive integer c and $i = 1, 2, 3$. We assume $\mathbf{L}_2 \cdot \mathbf{L}_3 \subset \mathbf{L}_1$. Then $\lambda_1(\mathbf{L}_1^\vee) \geq O(\frac{1}{|\Delta_\mathbf{K}|^{\frac{1}{d}}} d^{\frac{2c}{d}})$.*

Proof. For $\mathbf{x} \in \mathbf{L}_1^\vee$, let $\mathbf{X}$ be the matrix representation of the multiplication of $\mathbf{x}$ with respect to a fixed $\mathbf{Z}$-base of $\mathbf{R_K}$. For a number field lattice $\mathbf{L}$ set $\mathbf{B}(\mathbf{L})$ to be the matrix representation of $\mathbf{L}^\vee$ with respect to this fixed base of $\mathbf{R_K}$. Then

$$|\det(\mathbf{B}(\mathbf{L}_2^\vee))| = |\Delta_\mathbf{K}|^{-1} \cdot |(\det(\mathbf{B}(\mathbf{L}_2)))^{-1}| \geq \frac{1}{|\Delta_\mathbf{K}| d^c}$$

from the definition of dual lattice. Since $\mathbf{x} \in (\mathbf{L}_2 \cdot \mathbf{L}_3)^\vee$, $\mathbf{xy} \in \mathbf{L}_2^\vee$ for each $\mathbf{y} \in \mathbf{L}_3$. Then

$$\mathbf{B}(\mathbf{L}_3) \cdot \mathbf{X} = \mathbf{M} \cdot \mathbf{B}(\mathbf{L}_2^\vee)$$

for some non-singular integer matrix $\mathbf{M}$. We have

$$|\det(\mathbf{X})| \geq |\det(\mathbf{M}| \cdot \frac{1}{|\Delta_{\mathbf{K}}|d^{2c}} \geq \frac{1}{|\Delta_{\mathbf{K}}|d^{2c}}$$

since $|\det(\mathbf{M})| \geq 1$. It is clear

$$||\mathbf{x}||_{tr} = (\Sigma_{i=1}|\sigma_i(\mathbf{x})|^2)^{1/2} \geq \sqrt{d}(\prod_{i=1}^{d} \sigma_i(\mathbf{x}))^{1/d} = \sqrt{d}(N(x\mathbf{R_K}))^{1/d} = \sqrt{d}|\det(\mathbf{X})|^{1/d}.$$

The conclusion follows directly.

From Theorem 4.2 if a sublattice $\mathbf{L}$ in $\mathbf{R_K}$ contains the product of two polynomially bounded cardinality sublattices, the $\lambda_1(\mathbf{L}^\vee)$ is very close to $\frac{\sqrt{d}}{|\Delta_{\mathbf{K}}|^{1/d}}$ when d is sufficiently large. In particular if both $\mathbf{L}$ and $\mathbf{O^L}$ are with polynomially bounded cardinalities, $\lambda_1(\mathbf{L}^\vee)$ can not be very small. The sublattice attack with non-negligible $\mathbf{O^L}$ suggested in [8] has a strong restriction on the bound of width as the attack when $\mathbf{L}_1$ is required to be an ideal as in [18, 7, 38].

5 Proofs of main results

Proof of Theorem 2.1. For any fixed secret $\mathbf{s} \in \mathbf{R_K}_q$, a sublattice pair $(\mathbf{L}_1, \mathbf{L}_2)$ and uniformly chosen polynomially many invertible element $\mathbf{a}_i$ in $\mathbf{R_K}$, we use the property 3) to find $\mathbf{a}_{j_1}, \ldots, \mathbf{a}_{j_{d^{c_4+2}}}$ satisfying

$$a_{j_i}^{-1}\mathbf{L}_1 \subset \mathbf{L}_2$$

within complexity $O(d^{c_6})$. Since we assumed the probability that a uniformly chosen $\mathbf{a} \in \mathbf{R_K}_q$ is not invertible is at most $\frac{1}{2}$. For given uniformly chosen polynomially many samples we can use the property 3) directly.

For these d^{c_4+2} samples $(\mathbf{a}_{j_i}, \mathbf{b}_i)$ we check polynomially many conditions $\mathbf{a}_{j_i}^{-1}\mathbf{b}_i$ in each coset $\mathbf{R_K}/\mathbf{L}_2$. If these samples are from Ring-LWE equations, we have $\mathbf{s} + \mathbf{a}_{j_i}^{-1}\mathbf{e} \equiv \mathbf{a}_{j_i}^{-1}\mathbf{b}_i \ mod \ q$. The probability that $\mathbf{a}_{j_i}^{-1}\mathbf{b}_i$ is in the fixed coset of $\mathbf{R_K}/\mathbf{L}_2$ leading by the secret $\mathbf{s}$ is at least $\frac{1}{d^{c_3-c}} \geq \frac{2}{d^{c_3}} \geq \frac{2}{|\mathbf{R_K}/\mathbf{L}_2|}$ when d is sufficiently large. Actually from the property 2) of sublattice pair the probability that $\mathbf{e} \in \mathbf{L}_1$ is lower bounded by $\frac{1}{d^{c_3-c}}$ and $\mathbf{a}_{j_i}^{-1}\mathbf{e} \in \mathbf{L}_2$ for these error $\mathbf{e} \in \mathbf{L}_1$ from the property 3) of the sublattice pair. Though we do not know which coset of $\mathbf{R_K}/\mathbf{L}_2$ has this property since the secret vector $\mathbf{s}$ is not known, we can find such a coset by checking all polynomially many cosets of $\mathbf{R_K}/\mathbf{L}_2$. Then we can find at least $\frac{2d^{c_4+2}}{|\mathbf{R_K}/\mathbf{L}_2|}$ samples $(\mathbf{a}_{j_i}, \mathbf{b}_i)$ is in a fixed coset of $\mathbf{R_K}/\mathbf{L}_2$ if samples are from Ring-LWE equations. Otherwise there are exactly $\frac{d^{c_4+2}}{|\mathbf{R_K}/\mathbf{L}_2|}$ such $\mathbf{a}_{j_i}^{-1}\mathbf{b}_i$ is each coset. Hence we can distinguish samples from Ring-LWE equations from uniformly chosen ones within a complexity $O(d^{c_6+8c_1c_4+c_3})$.

Proof of Theorem 2.2. First of all we have $x^d - u_dx + u_d(u_d-1) = (x^2 - u_dx + u_d(u_d-1))(x^{d-2} + u_dx^{d-3} + u_dx^{d-4} + \cdots + u_dx + u_d) - u_d(u_d-1)^2(x^{d-3} + \cdots + x^2 + x + 1)$. Then $x^d - u_dx + u_d(u_d-1) \equiv (x^2 - u_dx + u_d(u_d-1) + u_d(u_d-1)^2(\frac{1}{d-1}x - 1))(x^{d-2} + u_dx^{d-3} + \cdots + u_d + u_d(u_d-1)^2(G_3(x) - G_2(x) - \frac{1}{d-1}G_1(x)))\ mod\ u_d(u_d-1)^3$, where

$$G_1(x) = \frac{x^{d-1} - (d-1)x + d - 2}{(x-1)^2},$$

$$G_2(x) = \frac{x^{d-3} - (d-3)x + d - 4}{(x-1)^2},$$

and

$$G_3(x) = \frac{x^{d-2} - (d-2)x + d - 3}{(x-1)^2}.$$

Notice that $\gcd(d-1, u_d-1) = 1$ and then $d-1$ is invertible in the ring $\mathbf{Z}/(u_d-1)\mathbf{Z}$, $G_1(x), G_2(x), G_3(x)$ are polynomials in $\mathbf{Z}/(u_d-1)\mathbf{Z}[x]$. Here we have $x^{d-3} + \cdots + x^2 + x + 1 \equiv (1 - \frac{1}{d-1}x)(x^{d-2} + u_d(x^{d-3} + \cdots + 1)) + (x^2 - u_dx + u_d(u_d-1))(G_2(x) + \frac{1}{d-1}G_1(x) - G_3(x))\ mod\ u_d - 1$, where

$$G_3(x) - G_2(x) - \frac{1}{d-1}G_1(x) = \frac{\frac{-1}{d-1}x^{d-1} + x^{d-2} - x^{d-3} + \frac{1}{d-1}}{(x-1)^2}.$$

From Theorem 4.1 we have

$$\mathbf{R_{K_d}}/W_d\mathbf{R_{K_d}} = \mathbf{Z}[\theta]/W_d\mathbf{Z}[\theta],$$

when $W = p_d(2p_d-1)^3$ and p_d satisfies the conditions before Theorem 2.2 (the conditions in Theorem 4.1). Hence

$$\mathbf{R_{K_d}}^\vee/W_d\mathbf{R_{K_d}}^\vee = \mathbf{Z}[\theta]^\vee/W_d\mathbf{Z}[\theta]^\vee.$$

The modulus parameter is $W_d = p_d(2p_d-1)^3$. Since we will take p_d a sufficiently large prime number then the probability that a uniformly chosen $\mathbf{a} \in \mathbf{R}_{\mathbf{K_d}q}$ is invertible is at least a fixed positive real number. Without loss of generality we assume that these $\mathbf{a}$'s are invertible module $W = p_d(2p_d - 1)^3$.

For any uniformly chosen invertible elements $\mathbf{a}_1, \ldots, \mathbf{a}_{d^{c_5}}$, we consider their images in the residue ring $(\mathbf{Z}/W_d\mathbf{Z})[\theta]/(\theta^4 - u_d\theta^2 + u_d(u_d-1) + u_d(u_d-1)^2(\frac{1}{d-1}\theta - 1))$. It is obvious that $\mathbf{a}_{j_1}, \ldots, \mathbf{a}_{j_{d^{c_4+2}}}$ elements among them can be found within a $O(d^{c_6})$ time, such that the images of these d^{c_4+2} elements $\mathbf{a}_{j_1}, \ldots, \mathbf{a}_{j_{d^{c_4+2}}}$ in the residue ring $(\mathbf{Z}/W_d\mathbf{Z})[\theta]/(\theta^2 - u_d\theta + u_d(u_d - 1) + u_d(u_d-1)^2(\frac{1}{d-1}\theta - 1))$ are the same $\mathbf{a}$. The complexity to find such d^{c_4+2} elements is at most $4W_d^2 d^{c_5}$.

The sublattice pair $(\mathbf{L}_1^d, \mathbf{L}_2^d)$ is defined by six vectors in

$$\mathbf{R}_{\mathbf{K_d}}{}^{\vee}/W_d\mathbf{R}_{\mathbf{K_d}}{}^{\vee} = \mathbf{Z}[\theta]^{\vee}/W_d\mathbf{Z}[\theta]^{\vee}$$

as follows. We set

$$\mathbf{x}_1 = \frac{\theta^{d-1}}{f_d'(\theta)},$$

$$\mathbf{x}_2 = \frac{\theta^{d-2}}{f_d'(\theta)},$$

and

$$\mathbf{x}_3 = \frac{1}{f_d'(\theta)}.$$

Set

$$\mathbf{L}_1^d = \mathbf{L}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3).$$

We consider the following three elements in

$$\mathbf{R}_{\mathbf{K_d}}{}^{\vee}/W_d\mathbf{R}_{\mathbf{K_d}}{}^{\vee} = \mathbf{Z}[\theta]^{\vee}/W_d\mathbf{Z}[\theta]^{\vee}.$$

$$\mathbf{x}_4 = \frac{(u_d-1)(\theta^{d-1} + (u_d-1)\theta^{d-2} - u_d)}{f_d'(\theta)},$$

$$\mathbf{x}_5 = \frac{(u_d-1)^2(\theta^{d-1} - u_d)}{f_d'(\theta)},$$

$$\mathbf{x}_6 = \frac{(u_d-1)((u_d^2 - u_d - 1)\theta^{d-1} - u_d(u_d-1)\theta^{d-2} + u_d(u_d-2))}{f_d'(\theta)}.$$

Notice that $(u_d-1)(\theta-1)(\theta^{d-2}+u_d\theta^{d-3}+\cdots+u_d+u_d(u_d-1)^2(G_3(\theta)-G_2(\theta)-\frac{2}{d-1}G_1(\theta)))\equiv(u_d-1)(\theta^{d-1}+(u_d-1)\theta^{d-2}-u_d)\ mod\ W_d$,
$(u_d-1)^2(\theta-u_d)(\theta^{d-2}+u_d\theta^{d-3}+\cdots+u_d+u_d(u_d-1)^2(G_3(\theta)-G_2(\theta)-\frac{2}{d-1}G_1(\theta)))\equiv(u_d-1)^2(\theta^{d-1}-u_d)\ mod\ W_d$,
and $\theta(\theta-1)^2(\theta^{d-2}+u_d\theta^{d-3}+\cdots+u_d+u_d(u_d-1)^2(G_3(\theta)-G_2(\theta)-\frac{1}{d-1}G_1(\theta)))\equiv(u_d-1)((u_d^2-u_d-1)\theta^{d-1}-u_d(u_d-1)\theta^{d-2}+u_d(u_d-2))\ mod\ W_d$.

Hence $\mathbf{x}_4,\mathbf{x}_5,\mathbf{x}_6$ are in the ideal generated by

$$\frac{\theta^{d-2}+u_d(\theta^{d-3}+\cdots+\theta+1)+u_d(u_d-1)^2(G_3(\theta)-\frac{1}{d-1}G_1(\theta)-G_2(\theta))}{f'(\theta))}.$$

Because $\mathbf{x}_4,\mathbf{x}_5$ and $\mathbf{x}_6$ are linear combinations of $\mathbf{x}_1,\mathbf{x}_2,\mathbf{x}_3$ with integer coefficients, then

$$\mathbf{L}(\mathbf{x}_1,\mathbf{x}_2,\mathbf{x}_3)\subset\mathbf{L}(\mathbf{x}_4,\mathbf{x}_5,\mathbf{x}_6).$$

Then $\mathbf{a}_{j_i}^{-1}\mathbf{L}(\mathbf{x}_1,\mathbf{x}_2,\mathbf{x}_3)\subset\mathbf{L}(\mathbf{a}\mathbf{x}_4,\mathbf{a}\mathbf{x}_5,\mathbf{a}\mathbf{x}_6)$. Actually $\mathbf{x}_4,\mathbf{x}_5$ and $\mathbf{x}_6$ are in the fractional ideal generated by

$$\frac{\theta^{d-2}+u_d(\theta^{d-3}+\cdots+\theta+1)+u_d(u_d-1)^2(G_3(\theta)-\frac{1}{d-1}G_1(\theta)-G_2(\theta))}{f_d'(\theta)},$$

then $\mathbf{a}_{j_i}\cdot\frac{\theta^{d-2}+u_d(\theta^{d-3}+\cdots+\theta+1)+u_d(u_d-1)^2(G_3(\theta)-\frac{1}{d-1}G_1(\theta)-G_2(\theta))}{f_d'(\theta)}$ is completely determined by the image of $\mathbf{a}_{j_i}$ in the residue ring $(\mathbf{Z}/W_d\mathbf{Z})[\theta]/(\theta^2-u_d\theta+u_d(u_d-1)+u_d(u_d-1)^2(\frac{1}{d-1}\theta-1))$. Set

$$\mathbf{L}_2^d=\mathbf{L}(\mathbf{a}\mathbf{x}_4,\mathbf{a}\mathbf{x}_5,\mathbf{a}\mathbf{x}_6).$$

We need to prove the conclusions 1) and 2) in Theorem 2.2.

First of all it is easy to verify the cardinality $|\mathbf{R}_{\mathbf{K_d}}/\mathbf{L}_1^d|=W_d^5$ from Theorem 4.1 and Proposition 4.1. We have

$$||\mathbf{x}_1||_{tr}\leq\frac{2||\theta^{d-1}||_{tr}}{d(u_d(u_d-1))}\leq\sqrt{\frac{8}{d}},$$

$$||\mathbf{x}_2||_{tr}\leq\frac{2||\theta^{d-2}||_{tr}}{d(u_d(u_d-1))}\leq\sqrt{\frac{8}{d}}$$

from Corollary 4.1. It is obvious

$$||\mathbf{x}_3||_{tr} \leq \frac{2}{\sqrt{d}u_d(u_d-1)}$$

from Proposition 4.3. Then the probability that $\mathbf{e} \in \mathbf{L}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$ is at least

$$\frac{1}{64d^{3C+1}u_d^2(u_d-1)^2}$$

by counting the number of lattice vectors $m_1\mathbf{x}_1 + m_2\mathbf{x}_2 + m_3\mathbf{x}_3 \leq \frac{W_d}{\sigma}$ for $m_1, m_2, m_3 \in \mathbf{Z}$ and Theorem 3.1. Actually the number of integers of m_i satisfying $||m_i\mathbf{x}_i||_{tr} \leq \frac{W_d}{3\sigma}$ is at least $\frac{W_d}{4\sigma||\mathbf{x}_i||_{tr}}$, when $\frac{W}{\sigma}$ is sufficiently large. Here we can always chose a polynomially bounded u_d satisfying $\frac{W_d}{\sigma} \geq d^{10}$. Hence there are at least $\frac{W_d 3}{64\sigma^3||\mathbf{x}_1||_{tr}||\mathbf{x}_2||_{tr}||\mathbf{x}_3||_{tr}}$ lattice vectors in the dual lattice $\mathbf{L}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)^\vee$. The lower bound 2) in Theorem 2.2 follows from Theorem 3.1.

We now prove the conclusion 1) of Theorem 2.2. Since the cardinality

$$\mathbf{R}_{\mathbf{K_d}}/\mathbf{L}(\mathbf{a}\mathbf{x}_4, \mathbf{a}\mathbf{x}_5, \mathbf{a}\mathbf{x}_6)$$

is the same as the cardinality of

$$\mathbf{R}_{\mathbf{K_d}}/\mathbf{L}(\mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_6)$$

from Proposition 4.6, we only need to calculate $\mathbf{R}_{\mathbf{K_d}}/\mathbf{L}(\mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_6)$.

The two conditions $Tr(\mathbf{x}_i \cdot \mathbf{y}) \equiv 0 \ mod \ p_d(u_d-1)^3$ for $i = 4, 5$ and $\mathbf{y} \in \mathbf{R}_{\mathbf{K_d}}/W_d\mathbf{R}_{\mathbf{K_d}} = \mathbf{Z}[\theta]/W_d\mathbf{Z}[\theta]$ are equivalent to the two conditions $Tr(\frac{\theta^{d-1}+(u_d-1)\theta^{d-2}-u_d}{f_d'(\theta)} \cdot \mathbf{y}) \equiv 0 \ mod \ p_d(u_d-1)^2$ and $Tr(\frac{\theta^{d-1}-u_d}{f_d'(\theta)} \cdot \mathbf{y}) \equiv 0 \ mod \ p_d(u_d-1)$. These two conditions implies that there are $p_d^2(u_d-1)^2$ residual classes in $\mathbf{R}_{\mathbf{K_d}}/\mathbf{L}(\mathbf{x}_6, \mathbf{x}_7)$. On the other hand from the third new condition $Tr(\mathbf{x}_8 \cdot \mathbf{y}) \equiv 0 \ mod \ p_d(u_d-1)^3$ it is equivalent to $Tr(\frac{(u_d^2-u_d-1)\theta^{d-1}-u_d(u_d-1)\theta^{d-2}+u_d(u_d-2)}{f_d'(\theta)} \cdot \mathbf{y}) \equiv 0 \ mod \ p_d(u_d-1)^2$, we get the conclusion that there are at least $p_d^2(u_d-1)^3$ residual classes in $\mathbf{R}_{\mathbf{K_d}}/\mathbf{L}(\mathbf{x}_6, \mathbf{x}_7, \mathbf{x}_8)$.

Proof of Corollary 2.1. We can take polynomially bounded $p_d \geq d^{5C+2}$ then the constructed sublattices $\mathbf{L}_1^d$ and $\mathbf{L}_2^d$ are indeed a sublattice pair for $q_d = u_d(u_d-1)^3, c, c_1, c_2, c < c_3 < c_4, c_5, c_6$, where $c, c_1, c_2, c_3, c_4, c_5, c_6$

are suitably chosen positive real numbers only depending on the constant C.

Another proof of Theorem 2.2 and Corollary 2.1. In this case we take the modulus parameter $W_d = u_d(u_d-1)^3$. The eight vectors $\mathbf{x}_1, \ldots, \mathbf{x}_8$ are defined as in the proof of Theorem 2.2. We can take samples $(\mathbf{a}, \mathbf{b})$'s with $\mathbf{a} \in \mathbf{I}$, where $\mathbf{I}$ is the ideal in $\mathbf{R_{K_d}}/W\mathbf{R_{K_d}} = \mathbf{Z}[\theta]/W_d\mathbf{Z}[\theta]$ generated by the element $\theta^2 - u_d\theta + u_d^2 - u_d + u_d(u_d-1)^2(\frac{1}{d-1}\theta - 1)$. Actually this ideal $\mathbf{I}$ has index in $\mathbf{R_K}/W_d\mathbf{R_K} = \mathbf{Z}[\theta]/W_d\mathbf{Z}[\theta]$ at most W_d^2. Then $\mathbf{a}\cdot\mathbf{s}$ is automatically in the sublattice $\mathbf{L}_3^d = \mathbf{L}(\mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_6)$ since $\mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_6$ are in the ideal generated by the element $\frac{\theta^{d-2}+u_d\theta^{d-3}+u_d\theta^{d-4}+\cdots+u_d\theta+u_d+u_d(u_d-1)^2(G_3(\theta)-\frac{1}{d-1}G_1(\theta)-G_2(\theta))}{f'(\theta)}$ and $(\theta^2 - u_d\theta + u_d(u_d-1) + u_d(u_d-1)^2(\frac{1}{d-1}\theta - 1))(\theta^{d-2} + u_d\theta^{d-3} + u_d\theta^{d-4} + \cdots + u_d\theta + u_d + u_d(u_d-1)^2(G_3(\theta) - \frac{1}{d-1}G_1(\theta) - G_2(\theta))) \equiv \theta^d - u_d\theta + u_d(u_d-1)$ $mod\ W_d$. It is obvious $\mathbf{L}_1^d = \mathbf{L}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) \subset \mathbf{L}_3^d$ since $\mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_6$ are linear combinations of $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ with integer coefficients. The probability $\mathbf{b} \in \mathbf{L}_3^d$ is bigger than or equal to the probability $\mathbf{P_e}$ of $\mathbf{e} \in \mathbf{L}_1^d$ for these samples $(\mathbf{a}, \mathbf{b})$'s with $\mathbf{a} \in \mathbf{I}$. The index $|\mathbf{R_K}/\mathbf{L}_3^d|$ can be calculated as in the proof of Theorem 2.2 for the modulus parameter $W_d = u_d(u_d-1)^3$, which is at least $u_d^2(u_d-1)^3$.

In this proof we need not to take $\mathbf{a}^{-1}$ $mod\ q$. Hence we need not to take $u_d = 2p_d$ where p_d is an odd prime. We only need to take suitable u_d satisfying the conditions in Theorem 4.1.

Proof of Corollary 2.2. Since we have

$$\mathbf{R_{K_d}}^\vee/W\mathbf{R_{K_d}}^\vee = \mathbf{Z}[\theta]^\vee/W_d\mathbf{Z}[\theta]^\vee$$

when $W = u_d(u_d-1)^3$ and u_d satisfies the conditions of Theorem 4.1. Then

$$\mathbf{R_{K_d}}^\vee/q_d\mathbf{R_{K_d}}^\vee = \mathbf{Z}[\theta]^\vee/q_d\mathbf{Z}[\theta]^\vee.$$

The size $|f'(\theta)|$ was estimated in Corollary 4.1 the conclusion follows from the conversion of dual form Ring-LWE to non-dual form Ring-LWE by by "tweak factors" on the widths.

Proof of Corollary 2.3. We take an arbitrary large positive integer C in Corollary 2.3 then we get a polynomial factor d^{9C} from the Hardness reduction result in Subsection 1.5. To satisfy the main condition in the Hardness reduction result we take $C = 2$ then an approximation factor d^{18} can be achieved.

6 Algorithms

1st algorithm

In this section we summarize the polynomial time algorithms in Theorem 2.1 and 2.2. to solve the decision non-dula Ring-LWE over $\mathbf{R_{K_d}}$ where $\mathbf{K}_d = \mathbf{Q}[x]/(f_d)$, $f_d = x^d - u_d x + u_d(u_d - 1)$. We take $u_d = 2p_d$, where p_d is a prime number such that $2p_d - 1$ satisfies the following conditions.
1) All prime factors of $2p_d - 1$ are distinct and not smaller than $d - 1$, $\gcd(d-1, 2p_d - 1) = 1$;
2) p_d is polynomially bounded and $p_d \geq d^{5C+2}$.
The conditions in Theorem 4.1 are always satisfied. We sample the error according to the Gaussian distribution (with respect to the canonical embedding) of width σ satisfying the condition in Corollary 2.1. $\mathbf{x}_1, \ldots, \mathbf{x}_6$ are defined as in the proof of Theorem 2.2.

Then we set the modulus parameter $W_d = p_d(2p_d - 1)^3$.

Step 1. For given polynomially bounded many $(poly(d))$ samples $(\mathbf{a}_1, \mathbf{b}_i)$, $i = 1, \ldots, W_d^6$, we find these $\mathbf{a}_i$'s which are invertible elements in $\mathbf{R_{K_d}}/W_d\mathbf{R_{K_d}} = \mathbf{Z}[\theta]/W_d\mathbf{Z}[\theta]$ with at least a positive constant probability, where $W_d = p_d(2p_d - 1)^3$. This step is within the polynomial time $O(poly(d)W_d^2)$ by checking the invertibility with the modulus parameter .

Step 2. Find the images of $\mathbf{a}_i$'s in

$$(\mathbf{Z}/W_d)[\theta]/(\theta^2 - u_d\theta + u_d(u_d-1) + u_d(u_d-1)^2(\frac{1}{d-1}\theta - 1))$$

and pick up d^{c_4+2} samples $(\mathbf{a}_{j_i}, \mathbf{b}_i)$'s whose $\mathbf{a}_{j_i}$'s have the same image $\mathbf{a}$. This step is completed within complexity $O(W_d^6)$. Set $\mathbf{L}_2^d = \mathbf{L}(\mathbf{a}\mathbf{x}_4, \mathbf{a}\mathbf{x}_5, \mathbf{a}\mathbf{x}_6)$.

Step 3. Write down the three conditions
$Tr(\mathbf{a}\mathbf{x}_4, \cdot\mathbf{y}) \equiv 0 \ mod\ W_d$;
$Tr(\mathbf{a}\mathbf{x}_5, \cdot\mathbf{y}) \equiv 0 \ mod\ W_d$;
$Tr(\mathbf{a}\mathbf{x}_6, \cdot\mathbf{y}) \equiv 0 \ mod\ W_d$.
This is the lattice $\mathbf{L}_2$ in the sublattice pair. This step is completed within complexity $O(W_d^3)$.

Step 4. Check $\mathbf{a}_{j_i}^{-1}\mathbf{b}_i \ mod\ \mathbf{L}_2^d$, classify them in different cosets of $\mathbf{R_{K_d}}/\mathbf{L}_2^d$. It will be found that there exists at least one coset with at least

$d^{c_4+2}\frac{2}{|\mathbf{R}_{\mathbf{K_d}}/\mathbf{L}_2^d|}$ such $\mathbf{a}_{j_i}^{-1}\mathbf{b}_i$'s if samples are from the Ring-LWE equation, otherwise there are exactly $d^{c_4+2}\frac{1}{|\mathbf{R}_{\mathbf{K_d}}/\mathbf{L}_2^d|}$ such such $\mathbf{a}_{j_i}^{-1}\mathbf{b}_i$'s in each coset. This step is completed within complexity $O(d^{c_4+2}W_d^3)$.

2nd algorithm

In this algorithm we take $W_d = u_d(u_d-1)^3$ and u_d is polynomially bounded and $u_d \geq d^{5C+2}$. The ideal $\mathbf{I}$ in $\mathbf{R}_{\mathbf{K_d}}/W\mathbf{R}_{\mathbf{K_d}} = \mathbf{Z}[\theta]/W\mathbf{Z}[\theta]$ is generated by the element $\theta^2 - u_d\theta + u_d^2 - u_d + u_d(u_d-1)^2(\frac{1}{d-1}\theta - 1)$. $\mathbf{x}_1, \ldots, \mathbf{x}_8$ are defined as in the proof of Theorem 2.2. The sublattice $\mathbf{L}_3^d = \mathbf{L}(\mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_6)$ and the auxiliary sublattice $\mathbf{L}_1^d = \mathbf{L}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$.

Step 1. For given polynomially bounded many samples $(\mathbf{a}_1, \mathbf{b}_i)$, $i = 1, \ldots, W_d^6$, we find at least $\frac{W_d^6}{W_d^2}$ samples $\mathbf{a}_i$'s which are in the ideal $\mathbf{I}$ generated by the element $\theta^2 - u_d\theta + u_d^2 - u_d + u_d(u_d-1)^2(\frac{1}{d-1}\theta - 1)$. It is within the time $O(W_d^8)$.

Step 2. For samples $(\mathbf{a}, \mathbf{b})$'s with the first component $\mathbf{a} \in \mathbf{I}$ we check the probability $\mathbf{b} \in \mathbf{L}_3^d$. If these samples are not from the Ring-LWE equation this probability is $\frac{1}{|\mathbf{R}_{\mathbf{K}}/\mathbf{L}_3^d|}$. If it is from the Ring-LWE equation, this probability is bigger than the probability $P_{\mathbf{e}}$ that $\mathbf{e} \in \mathbf{L}_1^d$. Since $P_{\mathbf{e}} \geq \frac{2}{|\mathbf{R}_{\mathbf{K}}/\mathbf{L}_3^d|}$, we can distinguish within time complexity $O(W_d^8)$.

In this algorithm $\mathbf{a}^{-1}$ is not needed as in 1st algorithm , we only need to check $\mathbf{b}$ *mod* $\mathbf{L}_3^d$ for these samples $(\mathbf{a}, \mathbf{b})$'s with $\mathbf{a} \in \mathbf{I}$.

7 Conclusion

The essence of sublattice attack on Ring-LWE is that the error distributions of sublattices in $\mathbf{R}_{\mathbf{K}}$ should be checked for these polynomially bounded index sublattices $\mathbf{L}$. This gives new large bounds on widths of solvable instances of Ring-LWE, which are closely related to the $\lambda_1(\mathbf{L}^\vee)$ and the number of very short lattice vectors in $\mathbf{L}^\vee$. In this paper we construct a sequence of number fields such that that decision Ring-LWE can be solved within a polynomial time complexity for error distributions with the widths in the range of hardness reduction results in [40]. This is the first sequence of number fields with degrees going to the infinity such that Ring-LWE with large width error distributions can be solved by a polynomial time algorithm. From the hardness reduction results in [40] the approximating $SIVP_{poly(d)}$ for ideal lattices in these number fields can be solved within quantum polynomial time. This is also the first sequence of number fields with degrees going to the infinity such that their approximating ideal-$SIVP_{poly(d)}$ can be solved by a polynomial time quantum algorithm. The sublattice attack on Ring-LWE over cyclotomic integer rings will be presented in [10].

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

[4] 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.

[5] 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.

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

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

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

[9] Hao Chen, On approximating $SVP_{poly(n)}$ with preprocessing for ideal lattices, preprint 2019.

[10] Hao Chen, Sublattice attacks on Ring-LWE with wide error distributions II, In prepration 2020.

[11] 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.

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

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

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

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

[16] 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.

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

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

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

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

[21] 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.

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

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

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

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

[26] V. Lyubashevsky, C. Peikert and O. Regev, On ideal lattices and learning with errors over rings, J. ACM, 60(6), 1-43, 2013, preliminary version, Eurocrypt 2010, 1-23, 2010.

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

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

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

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

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

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

[33] M. Mignotte, Bounds for the roots of lacunary polynomials, Journal of Symbolic Computation, vol. 30, no. 3, 325-327, 2000.

[34] T. Mukherjee and N. Stephens-Davidowitz, Lattice reduction for modules, or how to reduce moduleSVP to moduleSVP, Cryptology ePrint Archive, 2019/1142, 2019.

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

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

[37] 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.

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

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

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

[41] 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.

[42] O. Regev, New lattice-based cryptographic constructions, Journal of ACM, vol.**51** no 6, 899-942, 2004.

[43] O. Regev, On lattices, learning with errors, random linear codes, Journal of ACM, **56**, no.6, 1-40, 2009.

[44] 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.

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

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

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