Sublattice Attack on Poly-LWE with Wide Error Distributions

Hao Chen *

November 25, 2021

Abstract

The fundamental problem in lattice-based cryptography is the hardness of the Ring-LWE, 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 is no sufficient attacks proposed and considered. In this paper we propose the subset quadruple attack on general structured LWE problems over any ring endowed with a positive definite inner product and an error distribution. Hence from the view of subset quadruple attacks, the error distributions of feasible non-negligible subset quadruples should be calculated to test the hardness. Sublattice pair with an ideal attack is a special case of subset quadruple attack. A lower bound for the Gaussian error distribution is proved to construct suitable feasible non-negligible sublattices. From the sublattice pair with an ideal attack we prove that the decision Poly-LWE over $\mathbf{Z}[x]/(x^n - p_n)$ with certain special inner products and arbitrary polynomially bounded widths of Gaussian error distributions can be solved with the polynomial time for the sufficiently large polynomially bounded modulus parameters p_n.

Keywords: Poly-LWE, Ring-LWE, Wide Error distribution, Subset quadruple attack, Sublattice pair with an ideal.

*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 was supported by the NSFC Grant 62032009.

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, 7]). It is well-known there is a positive definite inner product on $\mathbf{K} \otimes \mathbf{C}$ defined by $< u, v >= \Sigma_{i=1}^{d} \sigma_i(u)\widetilde{\sigma_i(v)}$, where σ_i, $i = 1, \ldots, d$, are d embedings of $\mathbf{K}$ in $\mathbf{C}$, and $\tilde{v}$ is complex conjugate. Sometimes we use $||u||_{tr}$ to represent 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 [7, 12] for the detail. The canonical norm of an algebraic number field has the nice symmetry property reflected in the following lower bound ([26] Lemma 2.9) for a fraction ideal $\mathbf{I}$,

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

The dual of a lattice $\mathbf{L} \subset \mathbf{K}$ of rank deg$(\mathbf{K}/\mathbf{Q})$ is defined by $\mathbf{L}^\vee = \{\mathbf{x} \in \mathbf{K}, tr_{K/Q}(\mathbf{ax}) \in \mathbf{Z}, \forall \mathbf{a} \in \mathbf{L}\}$. An order $\mathbf{O} \subset \mathbf{K}$ in a number field $\mathbf{K}$ is a subring of $\mathbf{K}$ which is a lattice with rank equal to deg$(\mathbf{K}/\mathbf{Q})$. We refer to [12, 13, 7] for number theoretic properties of orders in number fields.

A polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbf{Z}[X]$ satisfies the condition of the Eisenstein criterion at a prime p, if $p|a_i$ for $0 \leq i \leq n-1$ and p^2 not dividing a_0. A polynomial satisfying this condition is irreducible in $\mathbf{Z}[x]$ from the Eisenstein criterion (see [7, 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, 37, 9]). We refer the further analysis to [9, 39].

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 [5] showed that SVP is NP-hard under the randomized reduction. Another breakthrough proved by Micciancio asserts that approximating SVP within a constant factor is NP-hard under the randomized reduction (see [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, 43, 2], we refer to [19] for Minkowski's first and second theorems on successive minima of lattices.

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

Plain LWE

Plain LWE and its lattice-based cryptographic construction was originated from [41]. We refer to [42] 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 [42] 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 [42]). For plain LWE without the ring structure the reduction results from approximating SIVP to plain LWE were given in [42, 34, 8].

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 [36] for a survey of the history of development, the theory and cryptographic constructions based on Ring-LWE and Ring-SIS. In particular suggested homomorphic encryption standard in [4] was based on Ring-LWE over two-to-power cyclotomic integer rings.

If the $\mathbf{Z}_q^n$ in plain LWE is replaced by $\mathbf{P}_q = \mathbf{P}/q\mathbf{P}$ where $\mathbf{P} = \mathbf{Z}[x]/(f)$, $f(x)$ is a degree n monic irreducible polynomial of degree n in $\mathbf{Z}[x]$, this is the polynomial learning with errors (Poly-LWE). 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, 9]).

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, 9]). 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 [37] page 10 in monogenic case a "tweak factor" $f'(\theta)$ can be used to make two versions equivalent.

We refer to [44] for relations and reductions between Ring-LWE and Poly-LWE. In the Poly-LWE case if we use the norm from the canonical embedding from the ring $\mathbf{Z}[x]/(f(x)) = \mathbf{Z}[\theta]$ to the complex number field $\mathbf{C}$, where θ is a root in $\mathbf{C}$ of $f(x)$, it is equivalent to the non-dual Ring-LWE in the monogenic extension case. The Gaussian error distribution is defined from this canonical norm. However if we use some different norm, for example, the norm under which $1, x, \ldots, x^{n-1}$ is the unit orthogonal base, that is, $< x^i, x^j >= 1$ when $i = j$ or 0 when $i \neq j$. The corresponding learning with errors problem is quite different. We will prove that the decision Poly-LWE with this norm and arbitrary polynomially (in n) bounded widths can be solved within the polynomial time for certain sufficiently large polynomially (in n) bounded modulus parameters in Corollary 3.2.

LWE over number field lattice

Learning with errors over a number field lattice was introduced in [38]. Let $\mathbf{L} \subset \mathbf{K}$ be a rank deg($\mathbf{K}$) lattice and

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

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

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

Then $\mathbf{O}^{\mathbf{L}} \cdot \mathbf{L}^{\vee} \subset \mathbf{L}^{\vee}$. Set $\mathbf{O}^{\mathbf{L}}{}_q = \mathbf{O}^{\mathbf{L}}/q\mathbf{O}^{\mathbf{L}}$ and $(\mathbf{L}^{\vee})_q = \mathbf{L}^{\vee}/q\mathbf{L}^{\vee}$. The secret vector $\mathbf{s}$ is in $(\mathbf{L}^{\vee})_q$ and $\mathbf{a}$ is in $\mathbf{O}^{\mathbf{L}}{}_q$. Here we notice that $\mathbf{O} \cdot \mathbf{L}^{\vee} \subset \mathbf{L}^{\vee}$. Then the error $\mathbf{e} \in (\mathbf{L}^{\vee})_q$. Samples from LWE over number field lattice $\mathbf{L}$ is $(\mathbf{a}, \mathbf{b}) \in \mathbf{O}^{\mathbf{L}}{}_q \times (\mathbf{L}^{\vee})_q$, where $\mathbf{a}$ is uniformly chosen in $\mathbf{O}^{\mathbf{L}}{}_q$, the error vector $\mathbf{e}$ is chosen in $(\mathbf{L}^{\vee})_q$ according to a Gaussian distribution with the width σ, then $\mathbf{b} \in \mathbf{L}^{\vee})_q$ is from the LWE equation. The decisional LWE over $\mathbf{L}$ is to distinguish these samples from uniformly chosen $(\mathbf{a}, \mathbf{b}) \in \mathbf{O}^{\mathbf{L}}{}_q \times (\mathbf{L}^{\vee})_q$. For the detail and hardness reduction we refer to [38].

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 [39]. We refer to [39] 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 [6] was improved in [1, 22]. On the other hand some provable weak instances of Ring-LWE was given in [17, 18, 11] and analysed in [9, 37]. As showed in [37, 9] these instances of Ring-LWE can be solved by polynomial time algorithms mainly because the widths of Gaussian distributions of errors are too small or Gaussian distributions of errors are too skew. In [**?**] 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 [3] 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 [40] 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, 33].

1.7 The ideal attack is very restricted

In previous attacks on Ring-LWE in [18] (then analysed in [9, 37]) 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 [9, 37] can be called ideal attack on Ring-LWE. In ideal attack on Ring-LWE $\lambda_1(\mathbf{P}^\vee)$ satisfies

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

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

When the modulus parameter q is a prime number such that $q\mathbf{R_K}$ is a prime ideal in $\mathbf{R_K}$, it is obvious we get nothing from the ideal attack. In our sublattice attack and subset attack we propose to find subtle polynomially bounded index sublattices $\mathbf{L}$ or feasible non-negligible subsets $\mathbf{B}$, then to test the samples from the Ring-LWE equation in $\mathbf{R_K}/\mathbf{L}$ or the feasible subset $\mathbf{B}$. Sublattice with an ideal attack was proposed in [10]. In this paper we extend it to subset attacks.

2 Subset quadruple attack

2.1 The motivation of subset attack

In previous attacks on Ring-LWE, when polynomially bounded many samples $(\mathbf{a},\mathbf{b}) \in \mathbf{R_K}/q\mathbf{R_K} \times \mathbf{R_K}/q\mathbf{R_K}$ are given, only the distributions of these samples over $\mathbf{R_K}/\mathbf{I}$ for some **ideals** satisfying $q\mathbf{R_K} \subset \mathbf{I} \subset \mathbf{R_K}$ and $|\mathbf{R_K}/\mathbf{I}| \leq poly(d)$ have been checked. This is not natural and not sufficient. We need to check the distributions of samples in $\mathbf{A} \subset \mathbf{R_K}/q\mathbf{R_K}$ where $\mathbf{A}$ can be any feasible non-negligible subsets, that is, the condition

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

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

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

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

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

The previous attacks where $\mathbf{A}$ is restricted to ideals or sub-modules are not natural, special and not sufficient to guarantee the security.

The basic point here is as follows. When we want to use the algebraic structure to improve the efficiency of lattice-based cryptographic constructions. The adversary is not restricted to only check the distributions of samples over algebraic-structured object, the adversary can attack the problem by using feasible non-negligible subsets without any structure.

2.2 Subset quadruples are needed

Let $\mathbf{R}$ be a ring which contains the ring of integers $\mathbf{Z}$ as a subring and $\mathbf{R} \otimes_{\mathbf{Z}} \mathbf{Q}$ is a d dimensional linear space over the rational field $\mathbf{Q}$. Suppose that there is a positive definite inner product $< \cdot, \cdot >$ on $\mathbf{R} \otimes_{\mathbf{Z}} R$ where R is the field of real numbers. Assume that $\mathbf{R}$ is a rank d lattice with respect to this positive definite inner product. Let $\mathbf{e}$ be an error distribution over $\mathbf{R} \otimes_Q R$. Let q be a modulus parameter. For the structured LWE over $\mathbf{R}$ with the modulus parameter q, the samples are from the structured LWE equation $\mathbf{a} \cdot \mathbf{s} + \mathbf{e} \equiv \mathbf{b}\ mod\ q$, where $\mathbf{s} \in \mathbf{R}/q\mathbf{R}$ is an arbitrary nonzero secret vector and uniformly chosen, and $\mathbf{a} \in \mathbf{R}/q\mathbf{R}$ are uniformly distributed public vectors.

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

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

and $\mathbf{A}_1$ and $\mathbf{A}_3$ are feasible, that is, the condition $\mathbf{a} \in \mathbf{A}_1$ and the condition $\mathbf{b} \in \mathbf{A}_3$ for $\mathbf{a}, \mathbf{b} \in \mathbf{R}/q\mathbf{R}$ can be checked within polynomial (in d) time. Here

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

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

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

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

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

Then the samples from the structured LWE equations can be distinguished from uniformly distributed samples. Hence it is important to calculate the error distributions over these feasible non-negligible subsets. In summary we introduce the following subset quadruple attack.

Definition 3.1. *We assume that the modulus parameter q satisfies $d^{C_1}\leq q<d^{C_2}$ where C_1 and C_2 are two fixed positive integers. Let $\mathbf{A}_i\subset\mathbf{R}/q\mathbf{R}$, $i=1,2,3,4$, be four subsets in $\mathbf{R}/q\mathbf{R}$ satisfying the following conditions.*
1) $\frac{|\mathbf{A}_i|}{|\mathbf{R}/q\mathbf{R}|}\geq\frac{1}{d^{C_3}}$ for $i=1,2,3$, where C_3 is fixed positive integer;
2) $\mathbf{A}_1\cdot\mathbf{A}_2+\mathbf{A}_4\subset\mathbf{A}_3$;
3) The set $\mathbf{A}_1$ and $\mathbf{A}_3$ are feasible;
4) The probability $Prob(\mathbf{e}\in proj^{-1}(\mathbf{A}_4))>\frac{d^{C_4}|\mathbf{A}_3|}{|\mathbf{R_K}/q\mathbf{R_K}|}$, where C_4 is a fixed positive integer.

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

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

we recover the sublattice pair attack in [**?**]. We call $(\mathbf{A}_1,\mathbf{A}_2,\mathbf{A}_3,\mathbf{A}_4)$ a sublattice quadruple when $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$ and $\mathbf{A}_4$ are images of sublattices. In the sublattice quadruple case if $\mathbf{A}_1$ is the whole ring $\mathbf{R}$ and $\mathbf{A}_2$ is an ideal, it is the sublattice pair with an ideal introduced in [10]. In the case that $\mathbf{A}_1$ is the whole ring $\mathbf{R}$ and $\mathbf{A}_2=\mathbf{A}_3=\mathbf{A}_4$ is an ideal, it is the very restricted case of ideal attack considered in [18, 9] and analysed in [37]. The "sublattice pair with ideal" construction for the required sublattices proposed in [10] can not work for number field case as indicated in [37]. However the comment in [37] can not apply to the general sublattice attack or its extended version of subset attack on general structured LWE proposed in this paper. The only problem in sublattice with an ideal attack on Ring-LWE in [10] is the usage of polynomially bounded index ideals in the construction of the required sublattices for number field case.

2.3 Subset attacks on general structured LWE

As showed in Theorem 3.1, we need to check all feasible non-negligible subset quadruples to test the hardness of the structured LWE. Let us consider the special case sublattice pair with an ideal attack on the Poly-LWE as follows.

The positive definite inner product on the ring $\mathbf{Z}[x]/(x^n - p_n)$ is defined as follows. The base elements $1, x, \ldots, x^{n-1}$ are the orthogonal norm 1 vectors. Here p_n is a sequence of sufficiently large polynomially bounded prime numbers when n goes to the infinity. From Theorem 3.1 and Theorem 4.1 it can be proved the Poly-LWE for the modulus parameters p_n can be solved within the polynomial time. The basic point here is that for this inner products on $\mathbf{Z}[x]/(x^n - p_n)$ and an ideal $\mathbf{I}$ we do not have the lower bound $\sqrt{n}vol(\mathbf{I})^{1/n} \leq \lambda_1(\mathbf{I})$ as for the canonical norm for the number field case. Hence the smoothing argument for the polynomially bounded index ideals for number fields in [37] is not valid in this case. Actually the dual lattice with respect to this inner product of the ideal generated by x is spanned by $\frac{1}{p_n}, x, x^2, \ldots, x^{n-1}$, which has a very short vector $\frac{1}{p_n}$ in the dual lattice.

3 Our contribution

Let $\mathbf{R}_n$ be a sequence of rings over $\mathbf{Z}$ with the dimension d_n, where d_n goes to the infinity, endowed with a sequence of positive definite inner products and a sequence of error distributions $\mathbf{e}_n$. Assume that $\mathbf{R}_n$ is a rank d_n lattice with respect to the above positive definite inner product. Let q_n be a sequence of polynomially bounded modulus parameters. In general if we can construct a sequence of subset quadruples for this structured LWE over $\mathbf{R}_n$, then the decision version of this structured LWE can be solved by a polynomial in d_n time algorithm. Moreover we notice that the error distribution is only involved in 4), it is not assumed Gaussian. The property 4) is sufficient for a polynomial time attack on the general structured LWE with an error distribution satisfying the property 4). We do not require that $\mathbf{A}_4$ to be non-negligible in the uniform distribution.

Theorem 3.1. *We consider the decision structured LWE over $\mathbf{R}_n$ with a sequence of error distributions and a modulus parameter q_n satisfying $d_n^{C_1} \leq q_n < d_n^{C_2}$ where C_1 and C_2 are two fixed positive integers. Suppose that there exists a sequence of subset quadruples as in Definition 2.1. Then the decision structured LWE over $\mathbf{R}_n$ with the modulus parameter q_n can be solved within the polynomial (in d_n) time.*

Hence the central problem for the hardness for the Ring-LWE over the ring of cyclotomic integers is if we can construct such subset quadruples. The following example of Poly-LWE over $\mathbf{Z}[x]/(x^n - p_n)$ with a special positive definite inner product shows that such subset quadruples are easy to construct. Actually in this case subset quadruple become the sublattice pair with an ideal.

Let p_n be a sequence of sufficiently large polynomially bounded prime numbers when n goes to the infinity. The polynomial $x^n - p_n$ is irreducible from the Eisenstein criterion. We use the inner product on $\mathbf{Z}[x]/(x^n - p_n)$ by defining $< x^i, x^j >= 1$ when $i = j$ and 0 when $i \neq j$, $i, j \in \{0, 1, \ldots, n-1\}$. The Gaussian error distribution is defined according to this inner product. The decision Poly-LWE problem as in the number filed case can be considered. From Theorem 3.1 we can prove the following result.

Corollary 3.1. *Let C_{10} be an arbitrary fixed positive integer. Let σ_n be the sequence of the widths of Gaussian error distributions over $\mathbf{Z}[x]/(x^n - p_n)$ with respect to the above inner product. Suppose that $\sqrt{n} \leq \sigma_n \leq n^{C_{10}}$. Then there exists a sequence of sufficiently large polynomially bounded prime numbers p_n (determined by C_{10} and n), such that the decision Poly-LWE over $\mathbf{Z}[x]/(x^n - p_n)$ for modulus parameters p_n can be solved within the polynomial time.*

The basic point here is that for this inner products on $\mathbf{Z}[x]/(x^n - p_n)$ and an ideal $\mathbf{I} \subset \mathbf{Z}[x]/(x^n - p_n)$ we do not have the lower bound $\sqrt{n}vol(\mathbf{I})^{1/n} \leq \lambda_1(\mathbf{I})$ with respect to the above positive definite inner product. This is not as the number field endowed with the canonical norm case. Hence the smoothing argument for the polynomially bounded index ideals in number field case is not valid in this case. The comment in [37] only works for the number field case, not other learning with errors problems over other rings without the property $\sqrt{n}vol(\mathbf{I})^{1/n} \leq \lambda_1(\mathbf{I})$. For general inner products on rings we get nothing about the $\lambda_1(\mathbf{I})$ even for a polynomially bounded index ideal $\mathbf{I}$. Therefore the sublattice pairs with ideals approach in previous versions works for this case without the symmetric property $\sqrt{n}vol(\mathbf{I})^{1/n} \leq \lambda_1(\mathbf{I})$.

We consider the irreducible polynomial $f_n(x) = x^n + a_1x^{n-1} + \cdots + a_n$, where $a_1, \cdots, a_n$ can be divisible by a sufficiently large polynomially (in n) bounded prime p_n, and the ring $\mathbf{Z}[x]/(f_n(x))$. We use the standard inner product on the base $1, x, \ldots, x^{n-1}$ as in the Corollary 3.2 case. The Gaussian error distribution is defined according to this inner product and we have the decision Poly-LWE problem as in the number filed case. From Theorem 3.1 we can prove the following result.

Corollary 3.2. *Let C_{11} be an arbitrary fixed positive integer. Let σ_n be the sequence of the widths of Gaussian error distributions over $\mathbf{Z}[x]/(f_n(x))$ with respect to the above inner product. Suppose that $\sqrt{n} \leq \sigma_n \leq n^{C_{11}}$. Then there exists a sequence of sufficiently large polynomially bounded prime numbers p_n (determined by C_{11} and n), such that the decision Poly-LWE over $\mathbf{Z}[x]/(f_n(x))$ for modulus parameters p_n can be solved within the polynomial time.*

Notice that the case in Corollary 3.2 is similar to the case of p-th cyclotomic polynomial, except that in Corollary 3.2 case the modulus parameter p_n is sufficiently larger (but polynomially bounded in d_n) than the degree or the lattice dimension d_n. In the cyclotomic polynomial case $p_n = d_n + 1$.

4 Probability computation and number theory

We need the following computation of probability. Let $\mathbf{R}$ be a ring which contains the ring of integers $\mathbf{Z}$ as a subring and $\mathbf{R} \otimes_{\mathbf{Z}} \mathbf{Q}$ is a d dimensional linear space over the rational field $\mathbf{Q}$. Suppose that there is a positive definite inner product $< \cdot, \cdot >$ on $\mathbf{R} \otimes_{\mathbf{Z}} R$ where R is the field of real numbers. Assume that $\mathbf{R}$ is a rank d lattice with respect to this positive definite inner product. Let $\mathbf{e}$ be an error distribution over $\mathbf{R} \otimes_Q R$.

Theorem 4.1. *Let $\mathbf{L}$ be a rank d sublattice in $\mathbf{R}$. Let $\mathbf{L}_1$ be rank d sublattice of $\mathbf{L}^\vee \subset \mathbf{R}^{vee}$ satisfying that $q\mathbf{L}^\vee \subset \mathbf{L}_1 \subset \mathbf{L}^\vee$. Suppose that the width of the Gaussian distribution of errors $\mathbf{e}$ satisfying $\frac{\sqrt{d}}{\lambda_1(\mathbf{L})} \leq \sigma \leq \frac{\sqrt{c_1}}{\sqrt{\pi}\lambda_1(\mathbf{L}_1^\vee)}$. Moreover there are at least $\frac{|\mathbf{L}^\vee/\mathbf{L}_1|}{q^{c_2}}$ lattice vectors in $\mathbf{L}_1^\vee$ satisfying $||\mathbf{x}|| \leq \frac{\sqrt{c_1}}{\sqrt{\pi}\sigma}$, where c_1 and c_2 are fixed positive real numbers. Then the* *probability* $\mathbf{e} \in \mathbf{L}_1$ *is*

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

It satisfies

$$\mathbf{P}_{\mathbf{L}_1} \geq \frac{1}{e^{c_1} q^{c_2}}$$

when q *is sufficiently large.*

Proof. We calculate the probability $\mathbf{P}_{\mathbf{L}_1}$ of the condition $\mathbf{e} \equiv 0 \ mod \ \mathbf{L}_1$. It is clear

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

Set $Y_3(0) = \frac{\Sigma_{\mathbf{x}\in\mathbf{L}^\vee} e^{-\pi(\frac{||\mathbf{x}||}{\sigma})^2}}{\sigma^n}$ and $Y_4(0) = \frac{\Sigma_{\mathbf{x}\in\mathbf{L}_1} e^{-\pi(\frac{||\mathbf{x}||}{\sigma})^2}}{\sigma^n}$. From the Poisson summation formula in [31] we have

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

and

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

Since $\sigma \geq \frac{\sqrt{d}}{\lambda_1(\mathbf{L})}$ then $\Sigma_{\mathbf{x}\in\mathbf{L}-\mathbf{0}} e^{-\pi(||\mathbf{x}||\sigma)^2} \leq 1 + \frac{1}{2^d}$ from Lemma 3.2 in [31]. For lattice vectors $\mathbf{x} \in \mathbf{L}_1^\vee$ satisfying

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

we have

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

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

The following result follows from Theorem 4.1 immediately.

Corollary 4.1. *Let* $\mathbf{L} \subset \mathbf{R}$ *be a rank* d *sublattice satisfying* $q\mathbf{R} \subset L \subset \mathbf{R}$. *Suppose that the width of the Gaussian distribution of errors* $\mathbf{e}$ *satisfying* $\frac{\sqrt{d}}{\lambda_1(\mathbf{R}^\vee)} \leq \sigma \leq \frac{\sqrt{c_1}}{\sqrt{\pi}\lambda_1(\mathbf{L}^\vee)}$. *Moreover there are at least* $\frac{|\mathbf{R}/\mathbf{L}|}{q^{c_2}}$ *lattice vectors in*

$\mathbf{L}^\vee$ *satisfying* $||\mathbf{x}|| \leq \frac{\sqrt{c_1}}{\sqrt{\pi}\sigma}$, *where* c_1 *and* c_2 *are fixed positive real numbers. Then the probability* $\mathbf{e} \in \mathbf{L}$ *is*

$$\mathbf{P_L} = \frac{\Sigma_{\mathbf{x}\in\mathbf{L}} e^{-\pi(\frac{||\mathbf{x}||}{\sigma})^2}}{\Sigma_{\mathbf{x}\in\mathbf{R}} e^{-\pi(\frac{||\mathbf{x}||}{\sigma})^2}}.$$

It satisfies

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

when q *is sufficiently large.*

Proposition 4.1. *If* $\mathbf{I} \subset \mathbf{R_K}$ *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 4.1 only few ideals $\mathbf{I}$ satisfy the condition $q\mathbf{R}_K \subset \mathbf{I}$ and $|\mathbf{R_K}/\mathbf{I}| \leq poly(d)$. When $p\mathbf{R_K}$ is a prime ideal, it is obvious that there is no non-trivial ideal satisfying the above two conditions. Hence in sublattice attack or subset attack it is not natural to require a sublattice $\mathbf{L}$ or the feasible non-negligible subsets to be an ideal.

Theorem 4.2. *Let* $\mathbf{L}_1, \mathbf{L}_2$ *and* $\mathbf{L}_3$ *be three polynomially bounded index 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* $\lambda_1(\mathbf{L}_1^\vee) \geq \Omega(\frac{1}{|\Delta_\mathbf{K}|^{\frac{3}{2d}} d^{\frac{2c}{d}}})$.

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 $\mathbf{B}(\mathbf{L}^\vee)$ to be the matrix representation of $\mathbf{L}^\vee$ with respect to this fixed base of $\mathbf{R_K}$. Then

$$|\det(\mathbf{B}(\mathbf{L}_2^\vee))| = |\Delta_\mathbf{K}|^{-1} \cdot |(\det(\mathbf{B}(\mathbf{L}_2)))^{-1}| \geq \frac{1}{|\Delta_\mathbf{K}|^{3/2} d^c}$$

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

$$|\det(\mathbf{X})| \geq |\det(\mathbf{M})| \cdot \frac{1}{|\Delta_\mathbf{K}|^{3/2} d^{2c}} \geq \frac{1}{|\Delta_\mathbf{K}|^{3/2} d^{2c}}$$

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

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

The conclusion follows directly.

From Theorem 4.2 if a sublattice $\mathbf{L}$ in $\mathbf{R}_\mathbf{K}$ contains the product of two polynomially bounded cardinality sublattices, the $\lambda_1(\mathbf{L}^\vee)$ is lower bounded by $\Omega(\frac{1}{|\Delta_\mathbf{K}|^{\frac{3}{2d}} d^{\frac{2c}{d}}})$ when d is sufficiently large. In particular if both $\mathbf{L}$ and $\mathbf{O}^\mathbf{L}$ satisfy

$$|\mathbf{R}_\mathbf{K}/\mathbf{L}| \leq poly(d),$$

and

$$|\mathbf{R}_\mathbf{K}/\mathbf{O}^\mathbf{L}| \leq poly(d),$$

$\lambda_1(\mathbf{L}^\vee)$ can not be very small. Therefor the sublattice attack with non-negligible $\mathbf{L}$ and $\mathbf{O}^\mathbf{L}$ has the strong restriction on the bound of width as the attack when $\mathbf{L}$ is required to be an ideal as in [18, 9, 37].

5 Proofs of main results

Proof of Theorem 3.1. The probability that uniformly chosen $\mathbf{a} \in \mathbf{R}/q\mathbf{R}$ is in the subset $\mathbf{A}_1$ is at least $\frac{1}{d^{C_3}}$, the probability $\mathbf{s} \in \mathbf{A}_2$ is at least $\frac{1}{d^{C_3}}$ for uniformly distributed $\mathbf{s} \in \mathbf{R}/q\mathbf{R}$. We check the probability $(\mathbf{a}, \mathbf{b}) \in (\mathbf{A}_1, \mathbf{A}_3)$ for $d^{C_{12}}$ samples $(\mathbf{a}, \mathbf{b})$'s where C_{12} is a fixed sufficiently large positive integer. Since both $\mathbf{A}_1$ and $\mathbf{A}_3$ are feasible, this can be done within a polynomial time. When these samples are uniformly distributed, the probability that

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

is exactly

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

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

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

in the Definition 2.1 of subset quadruples. Then we have

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

From the condition 4) of the subset quadruple we have

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

when samples are from the structured LWE equations. Hence for non-negligible secrets $\mathbf{s} \in \mathbf{A}_2$, the $d^{C_{12}}$ samples $(\mathbf{a}, \mathbf{b})$'s from the structured LWE equation are not uniformly distributed and can be tested within a polynomial time.

Proof of Corollary 3.1. Set $\mathbf{A}_1 = \mathbf{Z}[x]/(x^n - p_n)$ and $\mathbf{A}_2 = \mathbf{A}_3 = \mathbf{A}_4$ the image in $\mathbf{Z}/p_n\mathbf{Z}[x]/(x^n)$ of the ideal generated by the element x. Then $\mathbf{A}_2$, $i = 2, 3, 4$, is defined by $< 1, y > \equiv 0 \ mod \ p_n$, $y \in \mathbf{Z}[x]/(x^n - p_n)$. That is, $\mathbf{A}_2 = \mathbf{A}_3 = \mathbf{A}_4$ is the set

$$\{p_n a_0 + a_1 x + \cdot + a_{n-1} x^{n-1} : a_i \in \mathbf{Z}\}.$$

Then $\frac{1}{p_n}$ is in the dual lattice of the ideal $\mathbf{A}_2 = \mathbf{A}_3 = \mathbf{A}_4$ generated by x. From Corollary 4.1 it can be verified that $(\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4)$ is a sublattice quadruple or $(\mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4)$ is a sublattice pair with an ideal, when p_n is a sufficiently large polynomially bounded prime. Actually from Corollary 4.1 the condition 4) in Definition 2.1 is true when the sequence of prime modulus parameters p_n is chosen sufficiently large. Hence the Poly-LWE for the modulus parameters p_n can be solved within the polynomial time from Theorem 3.1. Actually the dual lattice with respect to the endowed positive definite inner product of the ideal generated by x is spanned by $\frac{1}{p_n}, x, x^2, \ldots, x^{n-1}$, which has a very short vector $\frac{1}{p_n}$ in the dual lattice.

Proof of Corollary 3.2. Similar to the proof of Corollary 3.1

6 Conclusion

In this paper we propose a general method of subset quadruple attack on the structured LWE to test its hardness. From the point view of subset quadruple attack on the Ring-LWE, the error distributions over feasible non-negligible subsets in $\mathbf{R_K}/q\mathbf{R_K}$ should be calculated and checked. From the sublattice pair with an ideal attack we prove that the decision Poly-LWE over $\mathbf{Z}[x]/(x^n - p_n)$ endowed with the special positive definite inner product and arbitrary polynomially bounded widths error distributions can be solved within the polynomial in n time for the sufficiently large polynomially bounded modulus parameters p_n.

References

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

[2] D. Aggarwal, D. Dadush and N. Stephens-Davidowitz, Solving the Closest Vector Problem in 2^n Time: the discrete Gaussian strikes again, FOCS, 563-582, 2015.

[3] 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.

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

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

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

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

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

[9] W. Castryck, I. Illashenko and F. Vercauteren, Provable weak instances of Ring-LWE revisted, Eurcocrypt 2016, LNCS 9665, 147-167, 2016.

[10] Hao Chen, Ring-LWE over two-to-power cyclotomics is not hard, Cryptology ePrint Achive 2021/418, 2021, with the serious error as indicated in [37], work in progress, 2021.

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

[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, LNCS 9666, 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, LNCS 11694, 322-351, 2019.

[17] Y. Eisentrage, S. Hallgren and K. Lauter, Weak instances of PLWE, SAC 2014, LNCS 8781, 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, J. ACM, **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, LNCS 9215, 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), LNCS 4051, 144-155, 2006.

[25] V. Lyubashevsky, D. Micciancio, C. Peikert and A. Rosen, SWIFT: A modest proposal for FFT hashing, FSE 2008, LNCS 5086,, 54-72, 2008.

[26] V. Lyubashevsky, C. Peikert and O. Regev, On ideal lattices and learning with errors over rings, J. ACM, **60**, 1-43, 2013, preliminary version, Eurocrypt 2010, LNCS 6110, 1-23, 2010.

[27] V. Lyubashevsky and C. Peikert and O. Regev, A toolkit for ring-LWE cryptography, Eurocrypt 2013, LNCS 7881, 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] T. Mukherjee and N. Stephens-Davidowitz, Lattice reduction for modules, or how to reduce moduleSVP to moduleSVP, Crypto 2020, LNCS 12172, 213-242, 2020.

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

[35] C. Peikert, An efficient and parallel Gaussian sampler for lattices, Crypyo 2010, LNCS 6223, 80-97, 2010.

[36] 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.

[37] C. Peikert, How (not) to instanaite Ring-LWE, SCN 2016, LNCS 9841, 411-430, 2016, Chris Twitter comment on April 3, 2021.

[38] C. Peikert and Z. Pepin, Algebraically structured LWE, revisited, TCC 2019, LNCS 11891, 1-23, 2019.

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

[40] A. Pellet-Mary, G. Hanrot and D. Stehlé, Approx-SVP in ideal lattices with pre-processing, Cryptology ePrint Achive 2019/215, Eurocrypt 2019, LNCS 11478, 685-716, 2019.

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

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

[43] 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.

[44] M. Rosca, D. Stehlé and A. Wallet, On the Ring-LWE and polynomial-LWE problems, Eurocrypt 2018, LNCS 10820, 146-173, 2018.