Solving Ring-LWE over Algebraic Integer Rings

Hao Chen *

July 5, 2019

Abstract

Many cryptographic schemes have been proposed from learning with errors problems over some rings (Ring-LWE). Polynomial time quantum reduction from the approximating Shortest Independent Vectors Problem ($SIVP_\gamma$) for fractional ideal lattices in *any algebraic number field* to the average-case decision Ring-LWE for any modulus over the integer ring in this number field was established in the Peikert-Regev-Stephens-Davidowitz STOC 2017 paper. However the hardness of approximating $SIVP_{poly(n)}$ in quantum computing was only a folklore conjecture. In this paper we prove that decision Ring-LWE for arbitrary number fields can be solved within polynomial time for infinitely many modulus parameters under a suitable bound on widths (with respect to the canonical embedding). We construct some algebraic number fields such that the decision versions of Ring-LWE with parameters in the range of Peikert-Regev-Stephens-Davidowitz $\mathbf{K} - SIVP$ to Ring-LWE reduction result can be solved within polynomial time. Our results indicate that approximating $SIVP_{poly(n)}$ for fractional ideal lattices in these algebraic number fields can be solved by a polynomial time quantum algorithm.

Keywords: Ring-LWE, Algebraic Integer Ring, $SIVP_{poly(n)}$ for ideal lattices.

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

1 Introduction

1.1 SVP and SIVP

A lattice $\mathbf{L}$ is a discrete subgroup in $\mathbf{R}^n$ generated by several linear independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m$ over the ring of integers, where $m \leq n$, $\mathbf{L} := \{a_1\mathbf{b}_1 + \cdots + a_m\mathbf{b}_m : a_1 \in \mathbf{Z}, \ldots, a_m \in \mathbf{Z}\}$. The volume $vol(\mathbf{L})$ of this lattice is $\sqrt{det(\mathbf{B} \cdot \mathbf{B}^\tau)}$, where $\mathbf{B} := (b_{ij})$ is the $m \times n$ generator matrix of this lattice, $\mathbf{b}_i = (b_{i1}, \ldots, b_{in}) \in \mathbf{R}^n$, $i = 1, \cdots, m$, are base vectors of this lattice. The length of the shortest non-zero lattice vectors is denoted by $\lambda_1(\mathbf{L})$. The well-known shortest vector problem (SVP) is defined as follows. Given an arbitrary $\mathbf{Z}$ basis of an arbitrary lattice $\mathbf{L}$ to find a lattice vector with length $\lambda_1(\mathbf{L})$ (see [47]). 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 [47]). A breakthrough result of M. Ajtai [4] showed that SVP is NP-hard under the randomized reduction. Another breakthrough proved by Micciancio asserts that approximating SVP within a constant factor is NP-hard under the randomized reduction (see [47]). For the latest development we refer to Khot [34]. It was proved that approximating SVP within a quasi-polynomial factor is NP-hard under the randomized reduction. The Shortest Independent Vectors Problem ($SIVP_{\gamma(m)}$) is defined as follows. Given an arbitrary $\mathbf{Z}$ basis of an arbitrary lattice $\mathbf{L}$ of dimension m, to find m independent lattice vectors such that the maximum length of these m lattice vectors is upper bounded by $\gamma(m)\lambda_m(\mathbf{L})$, where $\lambda_m(\mathbf{L})$ is the m-the Minkowski's minimum of lattice $\mathbf{L}$ (see [47]). For the hardness results about SVP and $SIVP$ we refer to [34, 35, 55].

Since the publication of [24], BKZ (block Korkine-Zolotarev) type algorithms with extreme pruning enumerations of large blocksizes $50 - 150$ as subroutines were proposed such that relative "shorter" lattice bases can be reduced from arbitrary given lattice bases. BKZ type algorithms in [24, 46] have been served as main algorithms to get short vectors in high dimensional lattices related to Ring-LWE problems and to check the hardness of the Ring-LWE problems (see [2, 37]).

1.2 Gaussian and discrete Gaussian

Gaussian distribution. 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 $D_{s,\mathbf{c}} = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{s^n}, \forall \mathbf{x} \in \mathbf{R}^n$. n random variables with density functions $\rho_1, \ldots, \rho_n$ are said mutually independent if their joint probability distribution has the density function $\rho = \prod_{i=1}^{n} \rho_n$. Notice that $D_{s,\mathbf{c}}$ can be expressed as the product of n independent 1-dimension Gaussian distributions. A n dimensional random variable according to a Gaussian distribution on $\mathbf{R}^n$ has the density function

$$\rho(\mathbf{\Sigma}, \mathbf{c}) = \frac{1}{(2\pi)^{n/2}(det(\Sigma))^{1/2}} e^{-\frac{1}{2}(\mathbf{x}-\mathbf{c})\cdot(\Sigma)^{-1}(\mathbf{x}-\mathbf{c})^{\tau}},$$

where $\mathbf{c} \in \mathbf{R}^n$ and Σ is a positive definite matrix. The coordinate random variables $X_1, \ldots, X_n$ of the n dimensional random variable $\mathbf{X} = (X_1, \ldots, X_n)$ with the above density function are mutually independent if Σ is a diagonal matrix.

Discretization. For any discrete subset $\mathbf{A} \subset \mathbf{R}^n$ we set $\rho_{s,\mathbf{c}}(\mathbf{A}) = \Sigma_{\mathbf{x}\in\mathbf{A}}\rho_{s,\mathbf{c}}(\mathbf{x})$ and $D_{s,\mathbf{c}}(\mathbf{A}) = \Sigma_{\mathbf{x}\in\mathbf{A}} D_{s,\mathbf{c}}(\mathbf{x})$. Let $\mathbf{L} \subset \mathbf{R}^n$ is a dimension n lattice, the discrete Gaussian distribution over $\mathbf{L}$ is the probability 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 the following properties of discrete Gaussian distributions to [44].
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.

Remark 1.1. If x is a continuous random variable over $\mathbf{R}$ according to a Gaussian distribution with the width σ, then ux is a continuous random variable according to a Gaussian distribution with the width $u\sigma$, where u is a positive integer. Let x_{dis} be the discretization of x valued in $\mathbf{Z}$. Then the discrete random variable ux_{dis} is not the discretization $(ux)_{dis}$ of the continuous random variable ux. The density function of the discrete random

variable ux_{dis} at $z \in \mathbf{Z} - u\mathbf{Z}$ is zero. However the density function of $(ux)_{dis}$ at $z \in \mathbf{Z}$ is

$$\frac{e^{-\pi(\frac{z}{u\sigma})^2}}{\Sigma_{y\in\frac{1}{u}\mathbf{Z}}e^{-\pi(\frac{y}{\sigma})^2}}.$$

In particular the density function of $(ux)_{dis}$ is not zero at $z \in \mathbf{Z} - u\mathbf{Z}$.

If we consider the discrete random variable ux_{dis} module q valued in $(-\frac{q}{2}, \frac{q}{2}] \bigcap \mathbf{Z}$ and $(ux)_{dis}$ module q valued in $(-\frac{q}{2}, \frac{q}{2}]$, the difference is much bigger. Set $uw' \equiv w \ mod \ q$, where w and w' are two integers in $(-\frac{q}{2}, \frac{q}{2}]$. The density function of ux_{dis} at w is

$$\frac{\Sigma_{k=\pm 1}^{\pm\infty} e^{-\pi(\frac{w'+kq}{\sigma})^2}}{\Sigma_{z\in\mathbf{Z}}e^{-\pi(\frac{z}{\sigma})^2}}.$$

The density function of $(ux)_{dis}$ is

$$\frac{\Sigma_{k=\pm 1}^{\pm\infty} e^{-\pi(\frac{w'+\frac{kq}{u}}{\sigma})^2}}{\Sigma_{y\in\frac{1}{u}\mathbf{Z}}e^{-\pi(\frac{y}{\sigma})^2}}.$$

That is, when u is large, $(ux)_{dis}$ module q is very close to a uniform distribution on $(-\frac{q}{2}, \frac{q}{2}]$ and ux_{dis} is not.

In the practical scenario of attacking a decisional Ring-LWE problem, the errors in samples obtained by attackers are discrete random variables over $\mathbf{Z}/q\mathbf{Z}$ according to the discretizations of Gaussian distributions. However in some analysis these errors were treated as continuous random variables. In particular the width of a linear combination of errors (as discrete random variables) was treated according to the formula of a linear combination of continuous random variables satisfying Gaussian distributions. This is not mathematically rigorous and sometimes far away from a real linear combination of discrete errors over $\mathbf{Z}/q\mathbf{Z}$. We refer to [49] subsection 4.1 and [39] subsection 2.4.2 for the detail.

1.3 Algebraic number fields

An algebraic number field is a finite degree extension of the rational number field $\mathbf{Q}$. Let $\mathbf{K}$ be an algebraic number field and $\mathbf{R_K}$ is its ring of integers in $\mathbf{K}$. From the primitive element theorem there exits an element $\theta \in \mathbf{K}$ such

that $\mathbf{K} = \mathbf{Q}[x]/(f) = \mathbf{Q}[\theta]$ where $f(x) \in \mathbf{Z}[x]$ is an irreducible polynomial (see [21]). It is well-known there is a positive definite inner product on the lattice $\mathbf{R_K}$ defined by $< u, v >= tr_{K/Q}(u\tilde{v})$ where $\tilde{v}$ is its complex conjugate (see [8, 16]). Sometimes we use $||u||_{tr}$ to represent $tr_{K/Q}(u\tilde{u})^{1/2}$. This is also the norm with respect to the canonical embedding (see [39]). The number field $\mathbf{K}$ is called monogenic, if the ring $\mathbf{R_K}$ of integers is of the form $\mathbf{R_K} = \mathbf{Z}[x]/(f) = \mathbf{Z}[\theta]$. This is equivalent to that $\mathbf{R_K}$ has a power base (see [26]). In this case the discriminant of the number field $\mathbf{K}$ (see [21]) is the same as the discriminant of the minimal polynomial f, $\Delta_{\mathbf{K}} = \Delta_f$. We recall for a monic degree m polynomial f with m roots $\theta_1, \theta_2, \ldots, \theta_m$, then the discriminant of the polynomial f is $\Delta_f = \prod_{i \neq j}(\theta_j - \theta_i)^2$. For an ideal $\mathbf{I} \subset \mathbf{R_K}$ if we can find one generator $\mathbf{g}$, this ideal is called a principal ideal generated by $\mathbf{g}$. Any ideal in $\mathbf{R_K}$ is a lattice of dimension $deg(\mathbf{K}/\mathbf{Q})$. For an ideal $\mathbf{I} \subset \mathbf{R_K}$, its dual $\mathbf{I}^\vee$ is defined as $\mathbf{I}^\vee = \{\mathbf{x} \in \mathbf{K}, tr_{K/Q}(\mathbf{ax}) \in \mathbf{Z}, \forall \mathbf{a} \in \mathbf{I}\}$.

Let ξ_n be a primitive n-th root of unity, the n-th cyclotomic polynomial Φ_n is defined as $\Phi_n(x) = \prod_{j=1,\gcd(j,n)=1}^{n}(x - \xi_n^j)$. This is a monic irreducible polynomial in $\mathbf{Z}[x]$ of degree $\phi(n)$, where ϕ is the Euler function. The n-th cyclotomic field is $\mathbf{Q}(\xi_n) = \mathbf{Q}[x]/(\Phi_n(x))$ and the ring of integers in $\mathbf{Q}(\xi_n)$ is exactly $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_n(x))$ (see [58]). For example when $n = 2^m$, the n-th cyclotomic polynomial is $\Phi_{2^m}(x) = x^{2^{m-1}} + 1$. When $n = p$ is an odd prime $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ and when $n = p^m$, $\Phi_{p^m}(x) = \Phi_p(x^{p^{m-1}}) = (x^{p^{m-1}})^{p-1} + \cdots + x^{p^{m-1}} + 1$.

The cyclotomic number field $\mathbf{Q}[\xi_n]$ is a monogenic field. The discriminant of the cyclotomic field (also the discriminant if the cyclotomic polynomial Φ_n) is

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

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

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

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

1.4 LWE and Ring-LWE

LWE.

Let n be the security parameter, q be an integer modulus and χ be an error distribution over $\mathbf{Z}_q$. Let $\mathbf{s} \in \mathbf{Z}_q^n$ be a secret chosen uniformly at random. Given access to d samples of the form

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

where $\mathbf{a} \in \mathbf{Z}_q^n$ are chosen uniformly at random and $\mathbf{e}$ are sampled from the error distribution χ, the search LWE is to recover the secret $\mathbf{s}$. In general χ is the discrete Gaussian distribution with the width σ. Here $\mathbf{a} \cdot \mathbf{s} = \Sigma a_i s_i$ is the inner product of two vectors in $\mathbf{Z}_q^n$.

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

Solving decision $LWE_{n,q,d,\chi}$ is to distinguish with non-negligible probability whether $(\mathbf{A}, \mathbf{b}) \in \mathbf{Z}_q^{n \times d} \times \mathbf{Z}_q^d$ is sampled uniformly at random, or if it is of the form $(\mathbf{A}, \mathbf{A}^\tau \cdot \mathbf{s} + \mathbf{e})$ where $\mathbf{e}$ is sampled from the distribution χ.

Here $[\mathbf{a} \cdot \mathbf{s} + e]_q$ is the residue class in the interval $(-\frac{q}{2}, \frac{q}{2}]$. We refer to [54] 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 [54]).

For this LWE without ring structure, the following reduction results (see [54, 48, 15]) give reductions from approximating SVP to LWE.

Reduction from $GapSVP_{\tilde{O}(nq/\sigma)}$ to search $LWE_{n,d,D_{Z,s}}$.
Regev [54]. If $q = poly(n)$ and $\sigma > \sqrt{n/(2\pi)}$, then there exists a quantum polynomial time reduction from worst-case $GapSVP_{\tilde{O}(nq/\sigma)}$ the search $LWE_{n,q,d,D_{Z,\sigma}}$.

Peikert [48]. If $q \geq 2^{n/2}$, $\sigma > \sqrt{n/(2\pi)}$ and $d = poly(n)$, then there exists a classical polynomial time reduction from worst-case $GapSVP_{\tilde{O}(nq/\sigma)}$ to search $LWE_{n,q,d,D_{Z,\sigma}}$.

Brakerski-Langlois-Peikert-Regev-Stehlé [15]. If If $q \leq poly(n)$, $\sigma > \sqrt{n/(2\pi)}$ and $d = poly(n)$, then there exists a polynomial time classical reduction from worst-case $GapSVP_{\tilde{O}(nq/\sigma)}$ in dimension $\sqrt{n}$ to search $LWE_{n,q,d,D_{Z,\sigma}}$.

Hence if the hardness of LWE is based on the hardness of approximating SVP, the ratio $\frac{nq}{\sigma}$ has to be small, for related result we refer to [42]. On the other hand, the equivalence of Decision LWE and Search LWE was proved in [54] (Lemma 4.2 in [54]) when $2 \leq q \leq poly(n)$ and q is a prime. (or see [2], Lemma 3).

Ring-LWE.

If the $\mathbf{Z}_q^n$ is replaced by $\mathbf{P}_q = \mathbf{P}/q\mathbf{P}$ where $\mathbf{P} = \mathbf{Z}[x]/(f)$, $f(x)$ is a monic irreducible polynomial of degree n in $\mathbf{Z}[x]$, this is the polynomial learning with errors problem. The inner product $\mathbf{a} \cdot \mathbf{s} = \Sigma a_i s_i$ is replaced by the multiplication $\mathbf{a} \cdot \mathbf{s}$ in the ring $\mathbf{P}_q$. The error distribution χ is defined as the discrete Gaussian distributions with respect to the basis $1, x, x^2, \ldots, x^{n-1}$ (see [26, 27]).

If the $\mathbf{Z}_q^n$ is replaced by $(\mathbf{R_K})_q = \mathbf{R_K}/q\mathbf{R_K}$ where $\mathbf{R_K}$ is the ring of integers in an algebraic number field $\mathbf{K}$, this is the Ring-LWE, learning with errors problem over the ring $\mathbf{R_K}$. The secret $\mathbf{s}$ is in the dual $(\mathbf{R_K}^\vee)_q = \mathbf{R_K}^\vee/q\mathbf{R_K}^\vee$ and $\mathbf{a} \in \mathbf{R_K}_q$ is chosen uniformly at random. The inner product $\mathbf{a} \cdot \mathbf{s} = \Sigma a_i s_i$ is replaced by the multiplication $\mathbf{a} \cdot \mathbf{s}$ in $(\mathbf{R_K}^\vee)_q$. The error $\mathbf{e}$ is in $(\mathbf{R_K}^\vee)_q = \mathbf{R_K}^\vee/q\mathbf{R_K}^\vee$. In this case the width of error distribution is defined by the trace norm on $\mathbf{K} \otimes \mathbf{R}$ via the canonical embedding (see [39, 17]). 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 [17, 18, 26] these two forms of Ring-LWE problem are equivalent with a scale factor $|\Delta_\mathbf{K}|^{\frac{1}{n}}$ on the width of the Gaussian distribution of errors.

The following reduction result is from [39, 40].

Hardness reduction for Ring-LWE 1: *Let $\mathbf{K}$ be the m-th cyclotomic field of degree $n = \phi(m)$. Let $\alpha = \alpha(n) > 0$ and $q = q(n) \geq 2$, $q \equiv 1$ mod m be a polynomial bounded prime such that $\alpha q \geq \omega(\sqrt{logn})$. Then there exists a polynomial time quantum reduction from $GapSVP_{\tilde{O}(\sqrt{n}/\alpha)}$ (or $GapSIVP_{\tilde{O}(\sqrt{n}/\alpha)}$) on any ideal lattices in $\mathbf{R_K}$ to the decision Ring-LWE*

over $\mathbf{R_K}$ *given* l *samples, with the discrete Gaussian distribution with width* $q\alpha(\frac{nl}{log(nl)})^{1/4}$.

Here we know that the approximating factor is $\tilde{O}(\frac{\sqrt{n}q(\frac{nl}{log(nl)})^{1/4}}{\sigma})$ where $\sigma = q\alpha(\frac{nl}{log(nl)})^{1/4}$ is the width of the Gaussian distribution. As explained in [39, 25] when $\mathbf{K}$ is Galois and q is a prime number that splits into prime ideals in $\mathbf{R_K}$ with $poly(n)$ algebraic norms, the decision version and the search version of the Ring-LWE problem over $\mathbf{R_K}$ are equivalent.

For efficient implementation of recent cryptography breakthrough fully homomorphic encryption (FHE) and cryptographic multilinear mappings in [30, 31] it was suggested based on the hardness of Ring-LWE problems over integer rings in cyclotomic number fields with degree $\phi(n) = 2^{k-1}, n = 2^k$ (see [43]). For more cryptographic primitives based on Ring-LWE we refer to [40, 41, 51, 50, 48, 54].

The following reduction was proved in [39] section 4 for general number fields. For the detail of the *discrete Gaussian sampling* problem $\mathbf{K} - DGS_\gamma$ for fractional ideals and the reduction from $\tilde{O}(\frac{\sqrt{n}}{\alpha})$-approximate SIVP to $\mathbf{K} - DGS_\gamma$, we refer to [39].

Hardness reduction for Ring-LWE 2: *Let* $\mathbf{K}$ *be an arbitrary number field of degree* n. *Let* $\alpha = \alpha(n) > 0$ *and* $q = q(n) \geq 2$ *be such that* $\alpha q \geq \omega(\sqrt{logn})$. *Then there exists a probabilistic polynomial-time quantum reduction from* $\mathbf{K} - DGS_\gamma$ *to the search version* $\mathbf{R} - LWE_{q,\Psi<\alpha}$, *where* $\gamma = \frac{\eta_\varepsilon(\mathbf{I})\cdot\omega(\sqrt{logn})}{\alpha}$ *for some negligible* $\varepsilon = \varepsilon(n)$. *Here* $\mathbf{K} - DGS_\gamma$ *is the discrete Gaussian sampling problem.* $\mathbf{I}$ *is any ideal and* $\eta_\varepsilon(\mathbf{I})$ *is the smoothing parameter of* $\mathbf{I}$.

Actually this was extended to decision Ring-LWE in [52] in the following results (Theorem 6.2 and Corollary 6.3 in [52]).

Hardness reduction for Ring-LWE 3: *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* $\mathbf{K} - DGS_\gamma$ *to average-case, decision* $\mathbf{R} - LWE_{q,\Upsilon_\alpha}$, *for any* $\gamma = \max\{\frac{\eta(\mathbf{I})\cdot 2}{\alpha\cdot\omega(1)}, \frac{\sqrt{2n}}{\lambda_1(\mathbf{I})}\}$. *Here* $\mathbf{K} - DGS_\gamma$ *is the discrete Gaussian sampling problem.* $\mathbf{I}$ *is any ideal lattice and* $\eta(\mathbf{I})$ *is the smoothing parameter of* $\mathbf{I}$.

Hardness reduction for Ring-LWE 4: *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* $\mathbf{I}$.

Remark 1.2. First of all the hardness of approximating SVP to some almost polynomial factors under the randomized reduction was proved for all lattices ([32, 35, 55]), while the hardness of some Ring-LWE is based on $SVP_{poly(n)}$ or $SIVP_{poly(n)}$ for fractional ideal lattices as proved in the above result (see [54, 48, 39, 52]). People do not have any evidence that approximating SVP for ideal lattices is hard or not (see [51, 54]). Secondly the approximating factor has to be small if we want the hardness of LWE or Ring-LWE from the hardness of $SVP_{poly(n)}$ or $SIVP_{poly(n)}$, since when the approximating factor is as large as exponential of lattice dimensions, the LLL algorithm can be used to give the desired lattice vectors (see [42]).

Remark 1.3. The Gaussian distribution depends on coordinates and the norm. We need to pay special attention to coordinates (or the basis with which coordinates are obtained) and the norm used when we say the "width" of a Gaussian distribution. The "canonical embedding' was used to define the Gaussian distribution on $\mathbf{K} \otimes \mathbf{R}$ (see [39, 40, 51, 17]). We recall the analysis in [17]. Set $\Phi : \mathbf{K} \longrightarrow \mathbf{H}$ the canonical embedding defined on the number field $\mathbf{K} = \mathbf{Q}[x]/(f)$ where f is a degree n irreducible polynomial over $\mathbf{Q}$ and $\alpha_1, \ldots, \alpha_n$ in $\mathbf{C}$ are n roots of f. We refer the definition of the space $\mathbf{H}$ to Subsection 2.2 in [40]. Set $\mathbf{N}_f$ the inverse of the Vandermonde matrix $(\alpha_i^{j-1})_{1\leq i,j\leq n}$ and $\mathbf{B}$ the following matrix.

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

Here there are s_1 real roots of f and $2s_2$ conjugate complex roots of f. Hence $s_1 + 2s_2 = n$. Let $\mathbf{r} = (r_1, \ldots, r_n)$ where $r_1, \ldots, r_n$ are n positive real numbers. If x_i, $i = 1, \ldots, n$, is sampled independently from the Gaussian distribution with width r_i, then coordinate vector with respect to the polynomial base $1, x, \ldots, x^n$ of $\mathbf{K} \otimes \mathbf{R}$ from the Gaussian distribution with parameter

$\mathbf{r}$ (with respect to the canonical embedding Φ) is $\mathbf{N}_f \cdot \mathbf{B} \cdot (x_1, \ldots, x_n)^\tau$. Set $||\mathbf{N}_f||_2 = \max \frac{||\mathbf{N}_f \cdot \mathbf{x}||}{||\mathbf{x}||}$ where $\mathbf{x} \in \mathbf{R}^d$ takes all non-zero vectors. In the case $\mathbf{r} = (\sigma', \ldots, \sigma')$, if in the dual form of the Ring-LWE problem we set the width of the Gaussian distribution with respect to the canonical embedding is σ, then $\sigma' \leq ||\mathbf{N}_f||_2 \cdot |\Delta_{\mathbf{K}}|^{\frac{1}{n}} \cdot \sigma$. Here $\Delta_{\mathbf{K}}$ is the discriminant of the algebraic number field $\mathbf{K}$.

In the plain LWE over $\mathbf{Z}_q^n$, if the secret $\mathbf{s}$ is chosen uniformly at random from $\{-1, 0, 1\}^n$ or $\{0, 1\}^n$, the corresponding LWE is called binary LWE. The binary LWE was introduced and some hardness results were proved in [15, 45]. In [5] a lattice decoding attack on this binary LWE was presented. It was proved that the worst-case GapSVP of some lattices of dimensions $n/logq$ can be reduced to binary LWE in [15, 45].

1.5 Known attacks

We refer to [12, 33] for the attack to LWE from the Blum-Kalai-Wasserman algorithm and its improvement. In [42] a probabilistic polynomial time algorithm was given to recover the secret key of LWE over $\mathbf{Z}_q^n$ when $\frac{nq}{\sigma}$ is very large. On the other hand Ring-LWE problems over integer rings of some algebraic number fields or polynomial rings $\mathbf{P}_q^n$ were attacked in [25, 27, 19, 20, 17, 19]. In [51, 17, 18] the above attack was analysed. The attacks can succeed because the width of the Gaussian distribution over $\mathbf{K} \otimes \mathbf{R}$ is too small, often smaller than a constant not depending on q only depending on the lattice dimension d, or the shape of the Gaussian distribution on $\mathbf{P}_q$ with respect to the base $1, x, \ldots, x^{u-1}$ is too "skewed" (see [51, 18]).

When the width is too small, with high probabilities the errors are within some range $z + (-\frac{1}{2}, \frac{1}{2})$ with a fixed integer z, the Ring-LWE can be reduced to an errorless problem (see [51]). One of the attack in [25, 27, 19, 20, 17, 19] is based on a homomorphism $\mathbf{R}_{\mathbf{K}} \longrightarrow \mathbf{R}_{\mathbf{K}}/q\mathbf{R}_{\mathbf{K}} = \mathbf{F}_{q^\mu}$, where $q\mathbf{R}_{\mathbf{K}}$ is an ideal over q and μ is one or two. Then the Ring-LWE can be "transformed" to a LWE over $\mathbf{F}_{q^f}$. If the "error distribution"over $\mathbf{F}_{q^f}$ from the errors sampled according to some Gaussian distribution is concentrated, then it leads to a complexity $O(q^3 n)$ attack. Over 2-power cyclotomic integer rings, the above "error distribution" is indistinguishable from the uniform distribution (see [20], section 4). Then their attack can not be applied to cyclotomic integer rings. Their method can also be applied to some polynomial LWE

problems as described in [26, 27].

In [22] approximating SVP with approximating factor $2^{O(\sqrt{nlogn})}$ for principal ideals in cyclotomic integer rings with $n = p^m$ can be found from an arbitrary generator (see [11, 7, 8, 9, 10]) within polynomial time by an efficient bounded distance decoding algorithm for the log-unit lattice. Thus the [56] version of FHE can be broken within sub-exponential complexity or quantum polynomial complexity. This work was extended in [23] and [53] such that sub-exponential complexity algorithms with sub-exponential pre-processing for approx-SVP in ideal lattices have been achieved.

The bounded distance decoding problem (BDD) for a lattice $\mathbf{L}$ is as follows. Given any $\mathbf{x}$ to find a lattice vector $\mathbf{v} \in \mathbf{L}$ such that $||\mathbf{x} - \mathbf{v}|| \leq B$ where B is a fixed bound. In many applications $B = \gamma\lambda_1(\mathbf{L})$ is assumed. Attacks on LWE and Ring-LWE by bounded distance decoding with pruning were given in [38, 5]. For algebraic attacks on LWE we refer to [1]. As indicated in [45], a polynomial time algorithm to find the secret key in the binary LWE can be obtained by the method in [1] when n^2 samples are available. For binary LWE and Ring-LPN (learning parity with errors over ring) we refer to [33] for sub-exponential attacks.

We refer to [16, 57] for recent developments in solving Ring-LWE under some conditions about samples and secret distributions.

2 Our contribution

2.1 Main results

Polynomial time quantum reductions from approximating $SIVP_{poly(n)}$ for fractional ideal lattices in any algebraic number field to the average-case decision Ring-LWE problem for any modulus over the integer ring in this number field was established in [52]. In this paper we show that for modulus parameter q such that $f(q) \equiv 0 \ mod \ q$, the decision Ring-LWE problems over integer rings in some algebraic number fields can be solved efficiently. However this condition is not so restrictive as the first glance. Because the defining equation $f(x)$ can be replaced by $f(x + h)$ where h can be any integer. Therefore any factor of $f(h)$ where h is an arbitrary integer, can be the modulus parameter satisfying this condition.

Let $f(x) \in \mathbf{Z}[x]$ be an irreducible polynomial with degree n and $\mathbf{K} = \mathbf{Q}[x]/(f)$ be an algebraic number field such that the ring of integers in $\mathbf{K}$ is $\mathbf{R_K} = \mathbf{Z}[x]/(f)$. That is, the number field $\mathbf{K}$ is monogenic. We consider the non-dual form of the Ring-LWE problem over $\mathbf{R_K}$. Let q be a modulus parameter. $\mathbf{a}$ and $\mathbf{s}$ are taken uniformly in $\mathbf{R}_{\mathbf{K},q} = \mathbf{R_K}/q\mathbf{R_K}$ and the error $\mathbf{e}$ is taken in $\mathbf{R}_{\mathbf{K},q}$ according to a discrete Gaussian distribution. The sample from the Ring-LWE over $\mathbf{R_K}$ is $(\mathbf{a}, \mathbf{b})$, $\mathbf{a}\cdot\mathbf{s}+\mathbf{e} = \mathbf{b}$ *mod* q. Let θ be a root of f in the algebraic closure of $\mathbf{Q}$ and then $\mathbf{K} = \mathbf{Q}(\theta)$ and the ring of integers in $\mathbf{K}$ is $\mathbf{R_K} = \mathbf{Z}[\theta]$. We can set the error vector $\mathbf{e} = e_0+e_1\theta+\cdots+e_{n-1}\theta^{n-1}$, where $e_0, e_1, \ldots, e_{n-1}$ are discretizations from continuous random variables over real numbers satisfying the Gaussian distribution width σ'. Let the width of the Gaussian distribution with respect to the canonical embedding be σ. Then $\sigma' \leq ||\mathbf{N}_f||_2 \cdot |\Delta_{\mathbf{K}}|^{\frac{1}{n}} \cdot \sigma = ||\mathbf{N_f}||_2 \cdot |\Delta_f|^{\frac{1}{n}} \cdot \sigma$. Here Δ_f is the discriminant of the polynomial f. We refer to [39, 17, 18] for the detail.

The main results of this paper are as follows.

Theorem 2.1. *Let* $\mathbf{K}$, $\mathbf{R_K}$ *and the non-dual form of Ring-LWE problem be as above. Assume that*
1) $\mathbf{K} = \mathbf{Q}[x]/(f)$ *is monogenic;*
2) f *and* q *satisfy* $f(q) \equiv 0$ *mod* q*;*
3) q *and the width* σ' *are bounded by* n^c *where* c *is a fixed positive integer;*
4) $q \geq n$ *and* $q^{3/2+\epsilon} \leq \sigma'$ *where* ϵ *is an arbitrary small positive real number. Then when* n *is sufficiently large, for a non-negligible probability* $\frac{1}{q} \geq \frac{1}{n^c}$ *of secrets* $\mathbf{s}$*, the decision version of the above non-dual form of Ring-LWE over* $\mathbf{R_K}$ *can be solved within a polynomial time* $O(n^{2c})$*.*

In the above result the Ring-LWE is transformed to one-dimensional case, however the condition that σ' is polynomially bounded is essentially necessary. In Theorem 2.1 the width σ' is coordinate-depending, we need the following result in which the condition is about the width with respect to the canonical embedding.

Theorem 2.2. *Let* $\mathbf{K}$, $\mathbf{R_K}$ *and the non-dual form of Ring-LWE problem be as above. Assume that*
1) $\mathbf{K} = \mathbf{Q}[x]/(f)$ *is monogenic;*
2) $q \geq n$ *is a factor of* $f(h)$ *for some integer* h*, we denote the polynomial* $f_h = f(x+h)$*;*
3) q *is bounded by* n^c *and the width* σ *with respect to the canonical em-*

bedding satisfies $\frac{q^{3/2+\epsilon}}{\min||\mathbf{N}_{f_h}|||\Delta_f|^{\frac{1}{n}}} \leq \sigma \leq \frac{n^c}{||\mathbf{N}_{f_h}||_2 \cdot |\Delta_f|^{\frac{1}{n}}}$, *where* $\min||\mathbf{N}_{f_h}|| = \min\frac{||\mathbf{N}_{\mathbf{f_h}} \cdot \mathbf{x}||}{||\mathbf{x}||}$, ϵ *is an arbitrary small positive real number and* c *is a fixed positive integer.*
Then when n *is sufficiently large, for a non-negligible probability* $\frac{1}{q} \geq \frac{1}{n^c}$ *of secrets* $\mathbf{s}$*, the decision version of the above non-dual form of Ring-LWE over* $\mathbf{R_K}$ *can be solved within a polynomial time* $O(n^{2c})$*.*

Corollary 2.1. *Let* $\mathbf{K}$, $\mathbf{R_K}$ *and the non-dual form of Ring-LWE problem be as above. Assume that*
1) $\mathbf{K} = \mathbf{Q}[x]/(f)$ *is monogenic;*
2) $q \geq n$ *is a factor of* $f(h)$ *for some integer* h*;*
3) q, $||\mathbf{N}_{f_h}||_2$, $|\Delta_f|^{\frac{1}{n}}$ *and* $\frac{q^{3/2+\epsilon}}{\min||\mathbf{N}_{f_h}|||\Delta_f|^{\frac{1}{n}}} \leq \sigma$ *are bounded by* n^c*, where* ϵ *is an arbitrary small positive real number and* c *is a fixed positive integer.*
Then when n *is sufficiently large, for a non-negligible probability* $\frac{1}{q} \geq \frac{1}{n^c}$ *of secrets* $\mathbf{s}$*, the decision version of the above non-dual form of Ring-LWE over* $\mathbf{R_K}$ *can be solved within a polynomial time* $O(n^{6c})$*.*

Corollary 2.2. *Let* $\mathbf{K}_n = \mathbf{Q}[x]/(f_n)$, $\mathbf{R}_{\mathbf{K}_n}$ *be a sequence of monogenic algebraic number fields and their rings of integers, with their degrees tending to the infinity, and* c *be a fixed large positive integer. We assume that*
1) There exists a sequence of modulus parameters q_n *satisfying* $n \leq q_n \leq n^c$ *and* q_n *is a factor of* $f_n(h_n)$ *for some integer* h_n*, we denote the polynomial* $f_n(x + h_n)$ *by* $g_n(x)$*;*
2) $||\mathbf{N}_{g_n}||_2$ *and* $|\Delta_{f_n}|^{\frac{1}{n}}$ *are bounded by* n^c*.*
Then the approximating SIVP for fractional ideals in $\mathbf{K}_n$ *with a polynomial factor can be solved within a polynomial time (in* n*) quantum algorithm.*

In Theorem 2.2, Corollary 2.1 and 2.2 the key point is if we could find a polynomially bounded q as a factor of $f(x + h)$, can the $||\mathbf{N}_{f(x+h)}||_2$ be polynomially bounded?

In many cases the condition 2) in Theorem 2.2 can be satisfied for infinitely many modulus parameter q. For example when $\mathbf{K}_t = \mathbf{Q}[x]/(\Phi_{2^t})$, where $\Phi_{2^t} = x^{2^{t-1}} + 1$ is the 2^t-th cyclotomic polynomial, then for any odd prime modulus parameter $q \equiv 1 \ mod\ 2^t$, there exists a integer h such that $h^{2^{t-1}} + 1 \equiv 0 \ mod\ q$ (see Proposition 2.10 in page 13 of [58]). Therefore there exists a $1 \leq h \leq q - 1$ such that $h^{2^{t-1}} + 1 \equiv 0 \ mod\ q$. Then we have the following result from Theorem 2.2.

Corollary 2.3. *Let* $\mathbf{K} = \mathbf{Q}[x]/(\Phi_n)$ *where* $n = 2^t$, $\mathbf{R_K} = \mathbf{Z}[x]/(\Phi_n)$ *and the non-dual form of Ring-LWE over* $\mathbf{R_K}$ *be as above, c be a fixed positive integer,* $n \leq q \leq n^c$ *be a odd prime modulus parameter satisfying* $q \equiv 1$ *mod n. We assume that the width* σ *with respect to the canonical embedding satisfies* $\frac{q^{3/2+\epsilon}}{(|h|+1)^{n/2}\sqrt{n}} \leq \sigma \leq \frac{n^c}{2(|h|+1)^{n/2}\sqrt{n}}$, *where* ϵ *is an arbitrary small positive real number.*
Then when n is sufficiently large, for a non-negligible probability $\frac{1}{q} \geq \frac{1}{n^c}$ *of secrets* $\mathbf{s}$, *the decision version of the above non-dual form of Ring-LWE over* $\mathbf{R_K}$ *can be solved within a polynomial time* $O(n^{2c})$.

Let $f_n(x) = x^n + u_n \in \mathbf{Z}[x]$, $n = 2^t$, where u is an positive integer, if u_n has a prime factor with exponent 1, it is an irreducible polynomial in $\mathbf{Z}[x]$ from the Eisenstein criterion. There exists an odd prime u_n satisfying $n \leq u_n \leq 3n$ and $u_n \equiv 3$ *mod* 4 from the Dirichlet density Theorem. As stated in [26, 17] the number field $\mathbf{K}_n = \mathbf{Q}[x]/(f_n)$ is a monogenic field. Then $\Delta_{\mathbf{K}_n} = \Delta_{f_n} = n^n u_n^{n-1}$ and $|\Delta_{f_n}|^{\frac{1}{n}} = n u_n^{\frac{n-1}{n}}$. In this case $\mathbf{N}_{f_n}$ can be nd can be calculated explicitly as in [17]. The two important quantities $||\mathbf{N}_{f_n}||_2$ and $\min \mathbf{N}_{f_n}$ are polynomially bounded. We have the following result from Corollary 2.1.

Corollary 2.4. *Let* $\mathbf{K}_n = \mathbf{Q}[x]/(f_n)$ *where* $n = 2^t$, $\mathbf{R}_{\mathbf{K}_n} = \mathbf{Z}[x]/(f_n)$ *and the non-dual form of Ring-LWE over* $\mathbf{R}_{\mathbf{K}_n}$ *be as above, c be a fixed positive integer. We take* u_n *as the modulus parameter. Assume that the width* σ *with respect to the canonical embedding satisfies* $3n^{1+\epsilon} \leq \sigma \leq n^c$, *where* ϵ *is an arbitrary small positive real number.*
Then when n is sufficiently large, for a non-negligible probability $\frac{1}{n}$ *of secrets* $\mathbf{s}$, *the decision version of the above non-dual form of Ring-LWE over* $\mathbf{R_K}$ *can be solved within a polynomial time* $O(n^{4c})$.

It is clear that we can choose a suitable constant positive integer c such that the above case of solvable decision Ring-LWE is in the parameter range of Hardness reduction for Ring-LWE 4 in Subsection 1.4. From Corollary 2.2 and Hardness reduction for Ring-LWE 4 we have the following result.

Corollary 2.5. *The approximating SIVP for fractional ideals with some polynomial factors in* $\mathbf{K}_n = \mathbf{Q}[x]/(f_n)$ *as in Corollary 2.4 can be solved within a polynomial time (in n) quantum algorithm.*

2.2 Comparison with previous works

In Theorem 2.1 conditions on the width do not lead to the case that the width σ' of the error distribution $e_0, \ldots, e_{n-1}$ is too small or skew such that the instance can be reduced to the errorless case. In previous works [19, 20, 26] the width of error distribution is too small or skew such that the RING-LWE can be reduced to the errorless case. The distinguishing from the uniform distribution was realized by χ statistic test or by a theoretical argument as in [26, 17, 51]. In this paper the distinguishing is proved by a probability argument. In Corollary 2.4 our bound on the width σ with respect to the canonical embedding for solvable Ring-LWE is much better than the same bound in the Crypto 2015 paper [26]. The parameters in Corollary 2.4 are in the range of hardness reduction results in Subsection 1.4.

2.3 Cryptographic implications

Almost all lattice-based crypto-systems are based on Ring-LWE problems over cyclotomic integer rings $\mathbf{Z}[x]/(\Phi_{2^t})$. The security is established from the conjectured quantum hardness about approximating $SIVP_{poly(n)}$ or $SVP_{poly(n)}$ for ideal lattices in $\mathbf{Z}[x]/(\Phi_{2^t})$. More generally it was widely conjectured that the $SVP_{poly(n)}$ for ideal lattices in general algebraic number fields is hard, we refer to [41].

Corollary 2.2 suggests that approximating SIVP problems for fractional ideals in some algebraic number fields with special number-theoretical structures are not hard in quantum computing. Corollary 2.4 gave a sequence of number fields in which $SIVP_{poly(n)}$ can be solved by a polynomial time quantum algorithm. In Theorem 2.2 and Corollary 2.2 the requirement about the width σ with respect to the canonical embedding is a bound by a polynomial of n, the main difficult part is to bound $||\mathbf{N}_{f_h}||_2$ in Theorem 2.2 and $||\mathbf{N}_{g_n}||_2$ in Corollary 2.2. Algebraic number fields satisfying conditions 1) and 2) in Corollary 2.2 are in the range of Hardness reduction 3 and 4, and their $SIVP_{poly(n)}$ is not hard in quantum computing, as illustrated in Corollary 2.4-2.5. Hence we believe that the hardness of Ring-LWE and approximating $SIVP_{poly(n)}$ or $SVP_{poly(n)}$ for fractional ideals depends essentially on concrete number-theoretical structures of number fields. From the point of cryptographic view people need a strong evidence or a proof for the hardness of $SIVP_{poly(n)}$ ($SVP_{poly(n)}$) for ideal lattices in $\mathbf{Q}[x]/(\Phi_n)$, $n = 2^t$. In this respect Corollary 2.3 shows that when σ is exponentially

small the Ring-LWE over these cyclotomic integer rings is easy for infinitely many primes. We give more results about cyclotomic number fields in Section 6.

3 Preparation

3.1 Matrix form

For a Ring-LWE problem over the integer ring $\mathbf{Z}[\theta]$, where $\mathbf{K} = \mathbf{Q}[\theta]$ is a monogenic number field, $\mathbf{a} \cdot \mathbf{s}$ can be expressed as $(1, \theta, \ldots, \theta^{n-1}) \cdot \mathbf{A}^\tau \cdot \mathbf{s}$, where $\mathbf{a} = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}, \mathbf{s} = s_0 + s_1\theta + \cdots + s_{n-1}\theta^{n-1}$. Here we also refer $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in (\mathbf{Z}/q\mathbf{Z})^n, \mathbf{s} = (s_0, s_1, \ldots, s_{n-1})^\tau \in (\mathbf{Z}/q\mathbf{Z})^n$. $\mathbf{A}^\tau$ is the matrix form of the multiplication of $\mathbf{a}$ in $\mathbf{K}$. The entries of the matrix $\mathbf{A}$ are from the coefficients of the polynomial f and $\mathbf{a}$. The computation of $\mathbf{A}$ is from the relation $f(\theta) = 0$ reducing the term θ^j, $j \geq n$ to a linear combination of lower power terms $1, \theta, \ldots, \theta^{n-1}$. We have the following result.

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

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

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

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

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

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

Proof. Since $f(w) \equiv 0 \ mod \ q$, then taking the congruence module q, w^j, $j \geq n$ can also be represented as a linear combination of lower power terms $1, w, \ldots, w^{n-1}$ by the same relation as $f(w) = 0 \ mod \ q$. We have $\mathbf{w} \cdot \mathbf{A}^\tau \cdot \mathbf{s} \equiv (a_0 + a_1 w + \cdots + a_{n-1} w^{n-1})(s_0 + s_1 w + \cdots + s_{n-1} w^{n-1}) \ mod \ q$. That is for any $\mathbf{s} \in (\mathbf{Z}/q\mathbf{Z})^n$, we have $(\mathbf{w} \cdot \mathbf{A}^\tau - (a_0 + a_1 w + \cdots + a_{n-1} w^{n-1})\mathbf{w}) \cdot \mathbf{s} \equiv 0 \ mod \ q$. Then $\mathbf{w} \cdot \mathbf{A}^\tau \equiv (a_0 + a_1 w + a_2 w^2 + \cdots + a_{n-1} w^{n-1})\mathbf{w} \ mod \ q$.

We consider the Ring-LWE over the cyclotomic integer ring $\mathbf{Z} = \mathbf{Z}(\xi_n) = \mathbf{Z}[x]/(\Phi_n)$, where ξ_n is a primitive n-th root of unity. For an element $\mathbf{a} \in \mathbf{Z}[\xi_n]$ with the form $\mathbf{a} = a_0 + a_1 \xi_n + \cdots + a_{d-1} \xi_n^{d-1}$ and a secret $\mathbf{s} = s_0 + s_1 \xi_n + \cdots + s_{d-1} \xi_n^{d-1} \in \mathbf{R_K}/q\mathbf{R_K}$, where $d = \phi(n)$. $\mathbf{a} \cdot \mathbf{s}$ can be expressed as $(1, \xi_n, \ldots, \xi_n^{d-1}) \cdot \mathbf{A}^\tau \cdot \mathbf{s}$. Here $\mathbf{A}^\tau$ is the matrix form of the multiplication $\mathbf{a}\cdot$ in $\mathbf{K} = \mathbf{Q}[x]/(\Phi_n)$.

Set $a_{0j} = a_j$ for $j = 0, \ldots, d-1$. Set $\Sigma_{j=0}^{d-1} a_{1j} \xi_n^j = \xi_n \cdot \mathbf{a}, \ldots, \Sigma_{j=0}^{d-1} a_{d-1,j} \xi_n^j = \xi_n^{d-1} \cdot \mathbf{a}$, where $\cdot$ is the multiplication in $\mathbf{K}$. Then $\mathbf{a} \cdot \mathbf{s} = \Sigma_{j=0}^{d-1} s_j \xi_n^j \cdot \mathbf{a} = \Sigma_{j=0}^{d-1} s_j (\Sigma_{l=0}^{d-1} a_{jl} \xi_n^l)$. Hence

$$\mathbf{a} \cdot \mathbf{s} = \Sigma_{l=0}^{d-1} (\Sigma_{j=0}^{d-1} s_j a_{jl}) \xi_n^l.$$

The matrix $\mathbf{A}$ is $(a_{lj})_{0 \leq l \leq d-1, 0 \leq j \leq d-1}$. That is the j-th row of the matrix $\mathbf{A}$ is the expansion with the base $(1, \xi_n, \ldots, \xi_n^{d-1})$ of the element $\xi_n^j \cdot \mathbf{a}$.

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

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

3.2 Probability theory

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

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

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

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

Theorem 3.3. *Let $q = q(n)$ be a positive integer sequence tending to the infinity. Suppose that $\mathbf{e}$ is a continuous random variable over $\mathbf{R}$ satisfying the Gaussian distribution of polynomially bounded width $\sigma \geq q^{\frac{3}{2}+\epsilon}$ where ϵ is an arbitrary small positive real number. Then the discrete random variable over $\mathbf{Z}/q\mathbf{Z}$ from $\mathbf{e}$ satisfies that when q is sufficiently large,*

$$P_{\sigma,discrete,modq}(0) \leq \frac{1}{q} - \frac{c_1 q}{\sigma^2}$$

for a fixed positive constant c_1.

Proof. The probability at $x \in \mathbf{Z}/q\mathbf{Z} = (-\frac{q}{2}, \frac{q}{2}] \bigcap \mathbf{Z}$,

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

Here we denote the denominator by $\mathbf{D}(0)$ and the numerator by $\mathbf{N}(x)$.

We have $\mathbf{D}(0) - \Sigma_{j=0}^{q-1} e^{-(\frac{x-j}{\sigma})^2} = \Sigma_{k=1}^{\infty} e^{-(\frac{-kq+x}{\sigma})^2} \Sigma_{j=0}^{q-1} e^{\frac{-(-kq-j+x)^2+(-kq+x)^2}{\sigma^2}} +$
$\Sigma_{k=1}^{\infty} e^{-(\frac{kq+x}{\sigma})^2} \Sigma_{j=0}^{q-1} e^{\frac{-(kq-j+x)^2+(kq+x)^2}{\sigma^2}} = \Sigma_{k=1}^{\infty} e^{-(\frac{-kq+x}{\sigma})^2} \Sigma_{j=0}^{q-1} e^{-\frac{j(2kq-2x+j)}{\sigma^2}} +$
$\Sigma_{k=1}^{\infty} e^{-(\frac{kq+x}{\sigma})^2} \Sigma_{j=0}^{q-1} e^{\frac{j(2kq-j+2x)}{\sigma^2}}$.

We set $x = 0$ in $\mathbf{N}(x)$ then

$$\mathbf{D}(0) - \Sigma_{j=0}^{q-1} e^{-(\frac{j}{\sigma})^2} = \Sigma_{k=1}^{\infty} e^{-(\frac{kq}{\sigma})^2} (\Sigma_{j=0}^{q-1} e^{-\frac{j(2kq+j)}{\sigma^2}} + \Sigma_{j=0}^{q-1} e^{\frac{j(2kq-j)}{\sigma^2}}).$$

We expand $\Sigma_{j=0}^{q-1} e^{-\frac{j(2kq+j)}{\sigma^2}}$ and $\Sigma_{j=0}^{q-1} e^{\frac{j(2kq-j)}{\sigma^2}}$ as follows.
$\Sigma_{j=0}^{q-1} e^{-\frac{j(2kq+j)}{\sigma^2}} = q - \Sigma_{j=0}^{q-1} \frac{j(2kq+j)}{\sigma^2} + \Sigma_{j=0}^{q-1} \frac{(-\frac{j(2kq+j)}{\sigma^2})^2}{2} + \Sigma_{j=0}^{q-1} \frac{(-\frac{j(2kq+j)}{\sigma^2})^3}{6} + \cdots +$
$\Sigma_{j=0}^{q-1} \frac{(-\frac{j(2kq+j)}{\sigma^2})^m}{m!} + \cdots$
$\Sigma_{j=0}^{q-1} e^{\frac{j(2kq-j)}{\sigma^2}} = q + \Sigma_{j=0}^{q-1} \frac{j(2kq-j)}{\sigma^2} + \Sigma_{j=0}^{q-1} \frac{(\frac{j(2kq-j)}{\sigma^2})^2}{2} + \Sigma_{j=0}^{q-1} \frac{(\frac{j(2kq-j)}{\sigma^2})^3}{6} + \cdots +$
$\Sigma_{j=0}^{q-1} \frac{(\frac{j(2kq-j)}{\sigma^2})^m}{m!} + \cdots$.

Then $\Sigma_{j=0}^{q-1} e^{-\frac{j(2kq+j)}{\sigma^2}} + \Sigma_{j=0}^{q-1} e^{\frac{j(2kq-j)}{\sigma^2}} = 2q - \frac{(q-1)q(2q-1)}{3\sigma^2} + \cdots + \Sigma_{j=0}^{q-1}(\frac{(-\frac{j(2kq+j)}{\sigma^2})^m}{m!} + \frac{(\frac{j(2kq-j)}{\sigma^2})^m}{m!}) + \cdots$.

Hence we have $\mathbf{D}(0) + (q - 1 - \Sigma_{j=1}^{q-1} e^{-(\frac{j}{\sigma})^2}) = q\mathbf{N}(0) - \frac{(q-1)q(2q-1)}{3\sigma^2} \times \Sigma_{k=1}^{\infty} e^{-(\frac{kq}{\sigma})^2} + \Sigma_{k=1}^{\infty}[e^{-(\frac{kq}{\sigma})^2} \Sigma_{j=0}^{q-1} \frac{j^2(4k^2q^2+j^2)}{\sigma^4}] + \Sigma_{m\geq 3} \Sigma_{k=1}^{\infty}[\Sigma_{j=0}^{q-1}(\frac{(-\frac{j(2kq+j)}{\sigma^2})^m}{m!} + \frac{(\frac{j(2kq-j)}{\sigma^2})^m}{m!}) \times e^{-(\frac{kq}{\sigma})^2}]$.

Lemma 3.1. *1) Let s be an non-negative integer and q be a fixed positive real number. Then $\mathbf{D}_s = \Sigma_{k=1}^{\infty} e^{-(\frac{kq}{\sigma})^2} k^s$ satisfies $c(\frac{\sigma}{q})^{s+1} \leq \mathbf{D}_s \leq Cs^2(\frac{\sigma}{q})^{s+1}$, where c and C are two universal positive real constants.*
2) When $\frac{\sigma}{q}$ is sufficiently large,

$$\Sigma_{k=1}^{\infty} e^{-(\frac{kq}{\sigma})^2} < 2\Sigma_{k=1}^{\infty} e^{-(\frac{kq}{\sigma})^2} (\frac{kq}{\sigma})^2$$

Proof. Let $\mathbf{S}_{m,s} = \Sigma_{\sqrt{m-1}\frac{\sigma}{q} \leq k < \sqrt{m}\frac{\sigma}{q}} k^s$ be the sum of k^s for k satisfying

$$(m-1) \leq (\frac{k}{\sigma})^2 \leq m$$

Then

$$\Sigma_{m=1}^{\infty} \mathbf{S}_{m,s} e^{-m} \leq \mathbf{D}_s \leq \Sigma_{m=1}^{\infty} \mathbf{S}_{m,s} e^{-(m-1)}$$

On the other hand it is well-known from Faulhaber's formula (Bernoulli's formula)

$$\frac{n^{s+1}}{s+1} \leq \Sigma_{k=1}^{n} k^s \leq n^{s+1}$$

Then it is clear we have

$$\frac{1}{m}(\frac{\sigma}{q})^{s+1} \leq \mathbf{S}_{m,s} \leq m^{\frac{s+1}{2}}(\frac{\sigma}{q})^{s+1}$$

Then the conclusion 1) follows directly.

We can compute $\Sigma_{0<\frac{kq}{\sigma})^2 \leq 1} e^{-(\frac{kq}{\sigma})^2}$ by considering $\frac{1}{m+1} < (\frac{kq}{\sigma})^2 \leq \frac{1}{m}$ for $m = 1, 2, \ldots$, as follows. Set S_m the number of positive integers satisfying $\frac{\sigma}{q\sqrt{m+1}} < k \leq \frac{\sigma}{q\sqrt{m}}$, then

$$\Sigma_{0<\frac{kq}{\sigma})^2 \leq 1} e^{-(\frac{kq}{\sigma})^2} \leq \Sigma_{m=1}^{\infty} e^{-\frac{1}{m+1}} S_m$$

The same method can be used to compute $\Sigma_{n<(\frac{kq}{\sigma})^2\le 1+n} e^{-(\frac{kq}{\sigma})^2}[2(\frac{kq}{\sigma})^2-1]$ for $n=1,2,\ldots,$ as follows.

$$\Sigma_{n<(\frac{kq}{\sigma})^2\le 1+n} e^{-(\frac{kq}{\sigma})^2}[2(\frac{kq}{\sigma})^2-1] \ge \Sigma_{m=1}^{\infty}(2n-1+\frac{1}{m+1})e^{-n-\frac{1}{m}}S_m$$

Then the coefficient of $\frac{\sigma}{q}$ on the left side is smaller then the coefficient of $\frac{\sigma}{q}$ on the right side. The conclusion 2) is proved.

Lemma 3.2. *For a fixed positive integer m*

$$\Sigma_{k=1}^{\infty} e^{-(\frac{kq}{\sigma})^2}[\Sigma_{j=0}^{q-1}(\frac{(-\frac{j(2kq+j)}{\sigma^2})^m}{m!}+\frac{(\frac{j(2kq-j)}{\sigma^2})^m}{m!})] \le \frac{3^{m+1}m}{(m-1)!}\cdot\frac{q^m}{\sigma^{m-1}}$$

Proof. It is clear $\Sigma_{k=1}^{\infty} e^{-(\frac{kq}{\sigma})^2}(\Sigma_{j=0}^{q-1}\frac{(-\frac{j(2kq+j)}{\sigma^2})^m}{m!}) \le \frac{2\cdot 3^m m^2}{m!}\cdot\frac{q^{m+m+1}}{\sigma^{2m}}\cdot(\frac{\sigma}{q})^{m+1}$ from Lemma 3.1. Then the conclusion follows directly.

When $m\ge 3$,

$$\Sigma_{k=1}^{\infty} e^{-(\frac{kq}{\sigma})^2}(\Sigma_{j=0}^{q-1}(\frac{(-\frac{j(2kq+j)}{\sigma^2})^m}{m!}+\frac{(\frac{j(2kq-j)}{\sigma^2})^m}{m!})) \le \frac{C}{q^{(m-1)\epsilon+\frac{m-3}{2}}}$$

where C is a universal positive constant and $\sigma=q^{\frac{3}{2}+\epsilon}, \epsilon>0$.

It is obvious $q-1-\Sigma_{j=1}^{q-1}e^{-(\frac{j}{\sigma})^2} \le \Sigma_{j=1}^{q-1}(\frac{j}{\sigma})^2 \le \frac{q^3}{3\sigma^2}$. Here the inequality $e^x\ge 1+x$ is used.

Thus in the above expansion $\mathbf{D}(0)+(q-1-\Sigma_{j=1}^{q-1}e^{-(\frac{j}{\sigma})^2}) = q\mathbf{N}(0) - \frac{(q-1)q(2q-1)}{3\sigma^2}\times\Sigma_{k=1}^{\infty}e^{-(\frac{kq}{\sigma})^2}+\Sigma_{k=1}^{\infty}[e^{-(\frac{kq}{\sigma})^2}\Sigma_{j=0}^{q-1}\frac{j^2(4k^2q^2+j^2)}{\sigma^4}]+\Sigma_{m\ge 3}\Sigma_{k=1}^{\infty}(\Sigma_{j=0}^{q-1}(\frac{(-\frac{j(2kq+j)}{\sigma^2})^m}{m!}+\frac{(\frac{j(2kq-j)}{\sigma^2})^m}{m!}))\times e^{-(\frac{kq}{\sigma})^2}$, we have

$$\Sigma_{k=1}^{\infty}e^{-(\frac{kq}{\sigma})^2}\Sigma_{j=0}^{q-1}\frac{j^2(4k^2q^2+j^2)}{\sigma^4} \ge \Sigma_{k=1}^{\infty}e^{-(\frac{kq}{\sigma})^2}(\frac{kq}{\sigma})^2\frac{4q^3}{3\sigma^2}.$$

Then $\frac{q^3}{\sigma^2}\Sigma_{k=1}^{\infty}e^{-(\frac{kq}{\sigma})^2}$ is the largest term and we estimate its coefficient from Lemma 3.1 2). Hence we have

$$\mathbf{D}(0)-c_1\frac{q^2}{\sigma} \ge q\mathbf{N}(0)$$

for some positive constant c_1. The conclusion of Theorem 3.3 follows directly.

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

Let

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

be a Vandermonde matrix and $\mathbf{V}^{-1}$ be its inverse. Here $x_1,\ldots,x_n$ are distinct complex numbers. The following result in [29] Theorem 4.4 is useful to give bounds on $||\mathbf{N}_f||_\infty$. We recall that the

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

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

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

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

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

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

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

4 Proofs and Algorithms

4.1 Proof of main results

Proof of Theorem 2.1. Let w be a root of the equation $f(x)\equiv 0\ mod\ q$. From Theorem 3.1 we have $\mathbf{w}\cdot\mathbf{A}^\tau\equiv(a_0+a_1w+a_2w^2+\cdots+a_{n-1}w^{n-1})\mathbf{w}$ *mod* q, where $\mathbf{w}=(1,w,\ldots,w^{n-1})$. Then for an unknown secret vector $\mathbf{s}$, $\mathbf{w}\cdot\mathbf{A}^\tau\cdot\mathbf{s}\equiv(a_0+a_1w+a_2w^2+\cdots+a_{n-1}w^{n-1})(s_0+s_1w+\cdots+s_{n-1}w^{n-1})\ mod\ q$. From the sample $(\mathbf{A},\mathbf{b})$ satisfying $\mathbf{A}^\tau\cdot\mathbf{s}+\mathbf{e}\equiv\mathbf{b}\ mod\ q$, $\mathbf{w}\cdot\mathbf{A}^\tau\cdot\mathbf{s}+\mathbf{w}\cdot\mathbf{e}\equiv\mathbf{w}\cdot\mathbf{b}$ *mod* q. That is, $(a_0+a_1w+a_2w^2+\cdots+a_{n-1}w^{n-1})(s_0+s_1w+\cdots+s_{n-1}w^{n-1})+(e_0+e_1w+\cdots+e_{n-1}w^{n-1})\equiv b_0+b_1w+\cdots+b_{n-1}w^{n-1}\ mod\ q$. Then the

equality $e_0+e_1w+\cdots+e_{n-1}w^{n-1} \equiv b_0+b_1w+\cdots+b_{n-1}w^{n-1}\ mod\ q$ holds for secret vectors satisfying $s_0+s_1w+\cdots+s_{n-1}w^{n-1} \equiv 0\ mod\ q$. Since q is bounded by a polynomial function of n, then for a non-negligible probability $\frac{1}{q}$ of secret vectors, $e_0+e_1w+\cdots+e_{n-1}w^{n-1} \equiv b_0+b_1w+\cdots+b_{n-1}w^{n-1}$ $mod\ q$.

Since $w=q$ is a root of $f(x) \equiv 0\ mod\ q$, then if $(\mathbf{a},\mathbf{b})$ is a sample from the Ring-LWE euqation, $e_0+e_1q+\cdots+e_{n-1}q^{n-1} \equiv b_0+b_1q+\cdots+b_{n-1}q^{n-1}$ $mod\ q$, that is, $e_0 \equiv b_0\ mod\ q$ for a non-negligible probability $\frac{1}{q}$ of secrets. We only need to test if $b_0\ mod\ q$ is a uniform distribution on $(-\frac{q}{2},\frac{q}{2}]\bigcap\mathbf{Z}$. From Theorem 3.3 e_0 as a discrete random variable differing with the uniform distribution with a term $\frac{c_1q}{\sigma'^2}$ at zero. Then the Ring-LWE can be solved by testing the probability of b_0 at zero. This can be achieved by testing $O(n^{2c})$ samples within $O(n^{2c})$ time. The conclusion is proved.

Proof of Theorem 2.2. It is clear that $\mathbf{K}=\mathbf{Q}[x]/(f_h)$ and $\mathbf{R_K}=\mathbf{Z}[x]/(f_h)$. Then $f_h(0) \equiv 0\ mod\ q$ and the condition 1) and 2) in Theorem 2.1 are satisfied. The conclusion follows from $\min||\mathbf{N}_{f_h}|||\Delta_f^{\frac{1}{n}} \leq \sigma' \leq ||\mathbf{N}_{f_h}||_2\sigma$ and Theorem 2.1 directly.

Proof of Corollary 2.1 It follows from Theorem 2.2 directly.

Proof of Corollary 2.2. This statement follows from Corollary 2.1 and Hardness reduction for Ring-LWE 4.

Proof of Corollary 2.3. We consider the polynomial $\Phi_{2^t,h}=(x+h)^{2^{t-1}}+1$. It is clear $h \leq -2$ or $h \geq 2$. Then the polynomial $\Phi_{2^t,h}$ satisfies the condition of the Gautschi Theorem. The conclusion follows from the estimation about $||\mathbf{N}_{\Phi_{2^t,h}}||_2$ in the Gautschi Theorem.

Proof of Corollary 2.4. As computed in [26, 17], the number field $\mathbf{K}_n=\mathbf{Q}[x]/(f_n)$ is a monogenic field. We have $\Delta_{\mathbf{K}_n}=\Delta_{f_n}=n^nu_n^{n-1}$. It is easy to check n roots of f_n are $u_n^{\frac{1}{n}}\zeta_j$, where ζ_j, $j=1,2,\ldots,n$, are n roots of $x^n+1=0$. From Subsection 3.3 of [17], $||\mathbf{N}_{f_n}||_2=\frac{1}{\sqrt{n}}$ and $\min||\mathbf{N}_{f_n}||=\frac{1}{\sqrt{n}u_n^{\frac{n-1}{n}}}$. The conclusion follows directly from Corollary 2.1.

Proof of Corollary 2.5. This conclusion follows from Corollary 2.2 directly.

4.2 The algorithm

For given samples $(\mathbf{a}, \mathbf{b})$, we test the probability of $(\mathbf{b})_q \equiv \mathbf{b}_0 \ mod\ q$. If it is not from the Ring-LWE equation $\mathbf{a} \cdot \mathbf{s} + \mathbf{e} = \mathbf{b}$, it is $\frac{1}{q}$. If the sample is from the equation $\mathbf{a} \cdot \mathbf{s} + \mathbf{e} = \mathbf{b}$, then for a probability of $\frac{1}{q}$ of $\mathbf{s}$, the probability $P((\mathbf{b})_q = 0) \leq \frac{1}{q} - \frac{c_1 q}{\sigma'^2}$. This can be tested from $O(n^{2c})$ samples within $O(n^{2c})$ time.

Here we should notice that the time consuming of the above algorithm depends on the polynomially bounded width σ', because the non-negligible difference is $\frac{c_1 q}{\sigma'^2}$.

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

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

First of all the following result in page 13 of [58] indicates that in cyclotomic polynomial case, the probability that a prime modulus parameter satisfying the condition 2) in Theorem 2.2 is $\frac{1}{n}$.

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

The following Bouniakowsky conjecture made in 1857 [13] also suggests that there are infinitely many prime modulus parameters satisfying the condition 2 in Theorem 2.2.

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

The following result in [6] suggests that the prime factors of $f(m)$ are quite large.

Proposition 5.2. Assume that the abc conjecture is true. Suppose that $f(x) \in \mathbf{Z}[x]$ *has no repeated roots. Fix* $\epsilon > 0$. *Then* $\prod_{prime-factor-p-of-f(m)} p \gg |m|^{\deg(f)-1-\epsilon}$, *where the constant implied by* $\gg$ *depends on* f *and* ϵ.

6 Ring-LWE and $SIVP_{poly(n)}$ for cyclotomic number fields

We consider the family of cyclotomic number fields $\mathbf{Q}[\xi_p] = \mathbf{Q}[x]/(\Phi_p)$ where $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, p is an odd prime tending to the infinity. In this case the degree is $n = p - 1$, $\Phi_p(1) = p$ is a prime number. Consider $f(x) = \Phi_p(1 + x)$, then $f(0) \equiv 0 \ mod \ p$. From Theorem 2.2 we have the following result.

Corollary 6.1. *If the width* σ *with respect to the canonical embedding satisfies*

$$\frac{p^{3/2+\epsilon}}{2^{p-1}p^{\frac{p-2}{p-1}}} \leq \sigma \leq \frac{p^c}{2^p \cdot p^{\frac{p-2}{p-1}}}$$

where c *is an arbitrary fixed positive integer and* ϵ *is an arbitrary small positive real number, for the modulus parameter* p, *the Ring-LWE over* $\mathbf{Z}[\xi_p]$ *can be solved within polynomial time* $O(n^{2c})$ *for a non-negligible probability* $\frac{1}{p}$ *of secrets.*

Proof. We get an estimation about $||\mathbf{N}_f||_2$ and $\min ||\mathbf{N}_f||$ from the Gautschi bound in Subsection 3.3. The condition $\sigma \leq \frac{p^c}{2^{p-1} \cdot p^{\frac{p-2}{p-1}}}$ should be satisfied such that σ' is upper bounded by a polynomial of $n = p - 1$. Hence the width with respect to the canonical embedding has to be very small when $n = p - 1$ tends to the infinity.

For general cyclotomic number fields the following result transform the hardness of $SIVP_{poly(n)}$ to a problem about number-theoretic properties of cyclotomic polynomials.

Theorem 6.1. *If there is a sequence of cyclotomic polynomials* Φ_{m_n}, *where* m_n *tending to the infinity, a sequence of prime numbers* q_n *tending to the infinity and a sequence of integers* h_n, *satisfying*
1) $q_n \equiv 1 \ mod \ m_n$ *and* $\Phi_{m_n}(h_n) \equiv 0 \ mod \ q_n$;

2) $q_n \leq m_n^c$, $|\Phi_{m_n}(h_n+1)| \leq m_n^c$ *if* $h_n \geq 1$ *or* $|\Phi_{m_n}(h_n-1)| \leq m_n^c$ *if* $h_n \leq -1$, *where* c *is a fixed positive integer;*
then $SIVP_{poly(n)}$ *with some polynomial approximating factor for fraction ideals in cyclotomic number fields* $\mathbf{K}_n = \mathbf{Q}[x]/(\Phi_{m_n})$ *can be solved by a polynomial time (in* m_n*) quantum algorithm.*

Proof. It is clear $|\Delta_{\Phi_{m_n}}|^{1/m_n} \leq m_n$ from the formula in subsection 1.3. From Proposition 2.10 in page 13 of [58], the condition $q_n \equiv 1 \ mod \ m_n$ implies the existence of non-zero h_n such that $\Phi_{m_n}(h_n) \equiv 0 \ mod \ q_n$. It is clear that the condition in the Gautschi bound is satisfied since $h_n + \xi_{m_n}$ has a non-negative real part of $h_n \geq 1$ or a non-positive real part if $h_n \leq -1$. The conclusion follows from Theorem 2.2 and the estimation of $||\mathbf{N}_{\Phi_{m_n,h_n}}||_2$ directly. Here Φ_{m_n,h_n} is the polynomial $\Phi_{m_n}(x+h_n)$.

7 Conclusion

Though the hardness of $SIVP_{poly(n)}$ or $SVP_{poly(n)}$ for ideal lattice are widely conjectured and this folklore conjecture has been served as the base of the security of lattice-based crypto-systems, there is no conclusive result about this problem since the active development of lattice-based cryptography. From the hardness reduction results proved in [52] the approximating $SIVP_\gamma$ for fractional ideals in any algebraic number field can be reduced to the average decision Ring-LWE. In this paper we proved that decision versions of Ring-LWE over integer rings of arbitrary number fields with a suitable condition on the width can be solved within polynomial time for infinitely many modulus parameters. Hence we construct some monogenic number fields such that $SIVP_{poly(n)}$ for ideal lattices in these number fields are not hard in quantum computing. This gives an strong evidence that the hardness of Ring-LWE and related $SIVP_{poly(n)}$ for ideal lattices essentially depends on concrete number-theoretic structures of an algebraic number field.

References

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

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

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

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

[5] S. Bai and S. D. Galbraith, Lattice decoding attacks on binary LWE, Information Security and Privacy, Cryptology ePrint Achive, Report 2013/839.

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

[7] J.-F. Biasse and C. Fieker, Sub-exponential class group and uint group computation in large degree number fields, LMS J. Comput. Math., 17 (suppl. A), 385-403, 2014.

[8] J.-F. Biasse, Subexponential time relations in the class group of large degree number fields, Adv. Math. Commun., 8(4), 407-425, 2014.

[9] J.-F. Biasse and F. Song, Efficient quantum algorithm for computing class groups and solving the principal ideal problem in arbitrary degree number fields, 893-902, SODA 2016.

[10] J.-F. Biasse, Approximate short vectors in ideal lattices of $\mathbf{Q}[\xi_{p^n}]$ with precomputation of $Cl(O_k)$, 374-393, SAC2017.

[11] J.-F. Biasse, T. Espitau, P-A. Fouque, A. Gélin and P. Kirchner, Computing generator in cycltomic integer ringes, Eurocrypt 2017, 60-88, 2017.

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

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

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

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

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

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

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

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

[20] 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.

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

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

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

[24] Y. Chen and P. Q. Nguyen, BKZ2.0: Better lattice security estimates, 1-20, Asiacrypt 2011, full version, http://www.di.ens.fr/ ychen/research/

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

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

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

[28] J. Fan and F. Vercauteren, Somewhat practical fully homomorphic encrytion, Cryptology ePrint Achive, 2012/144, 2012.

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

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

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

[32] I. Haviv and O. Regev, Tensor-based hardness of the shortest vector problem to within almost polynomial fasctors, STOC 2007, Theory of Computing 8 (23), 513-531, 2012.

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

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

[35] 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.

[36] A.K.Lenstra, H.W. Lenstra and L.Lovàsz, Factoring polynomials with rational coefficients, Math.Ann., **261**, 513-524, 1982.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[55] 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.

[56] N. Smart and F. Vercauteren, Fully homomorphic encryption scheme with relatively small key size and ciphertext sizes, PKC 2010.

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

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