Noname manuscript No.
(will be inserted by the editor)

The Ring-LWE Problem in Lattice-based Cryptography: In Praise of Twisted Embeddings

Jheyne N. Ortiz (✉) · **Robson R. de Araujo** · **Diego F. Aranha** · **Sueli I. R. Costa** · **Ricardo Dahab**

the date of receipt and acceptance should be inserted later

Abstract Our main result in this work is the extension of the Ring-LWE problem in lattice-based cryptography to include algebraic lattices, realized through twisted embeddings. We define the class of problems *Twisted Ring-LWE*, which replaces the canonical embedding by an extended form. We prove that our generalization for Ring-LWE is secure by providing a security reduction from Ring-LWE to Twisted Ring-LWE in both search and decision forms. It is also shown that the addition of a new parameter, the torsion factor defining the twisted embedding, does not affect the asymptotic approximation factors in the worst-case to average-case reductions. Thus, Twisted Ring-LWE maintains the consolidated hardness guarantee of Ring-LWE and increases the existing scope of algebraic lattices that can be considered for cryptographic applications. Additionally, we expand on the results of Ducas and Durmus (Public-Key Cryptography, 2012) on spherical Gaussian distributions to the proposed class of lattices under certain restrictions. Thus, sampling from a spherical Gaussian distribution can be done directly in the respective number field, while maintaining its shape and standard deviation when seen in $\mathbb{R}^n$ via twisted embeddings.

Keywords Lattice-based cryptography · Twisted embeddings · Ring-LWE · Spherical Gaussian sampling · $\mathbb{Z}^n$-equivalent lattices

Acknowledgements The authors were supported in part by the Brazilian Coordination for the Improvement of Higher Education Personnel Foundation (CAPES) under grant numbers

J.N. Ortiz · R. Dahab
Institute of Computing, University of Campinas, Campinas, Brazil
E-mail: jheyne.ortiz@ic.unicamp.br

R.R. Araujo
Federal Institute of São Paulo, Cubatão, Brazil

D.F. Aranha
Department of Engineering, Aarhus University, Aarhus, Denmark

S.I.R. Costa
Institute of Mathematics, Statistics and Computing Science, University of Campinas, Campinas, Brazil

1591123 and 1540410, the Brazilian National Council for Scientific and Technological Development (CNPq) under grant numbers 164489/2018-5 and 313326/2017-7, and São Paulo Research Foundation under grant number 2013/25977-7.

1 Introduction

Lattice-based cryptography comprehends the class of cryptosystems whose security is based on the conjectured intractability of hard lattice problems such as the Shortest Independent Vectors problem (SIVP), the Shortest Vector Problem (SVP), and the Closest Vector Problem (CVP) [1,23]. The main problem in the foundation of most modern lattice-based cryptosystems is Learning with Errors (LWE) [26]. Since its introduction in the cryptographic realm in 2005, algebraically structured variants have been proposed, such as Learning with Errors over Rings [16], denoted Ring-LWE, and Module-LWE [9,14,2], among others [24].

The usual instantiation of the Ring-LWE problem in lattice-based cryptosystems is over power-of-two cyclotomic number fields, as evidenced by the finalists of NIST's Post-Quantum Cryptography standardization effort [20]. This choice of number field is particularly interesting because its ring of integers is isomorphic to the polynomial ring $R = \mathbb{Z}[x]/(x^n+1)$, for n a power of two. The fact that x^n+1 is maximally sparse allows efficient polynomial multiplication using the number-theoretic transform combined with the negacyclic convolution. In addition to that, the transformation from the ring R to its dual, denoted $R^\vee$, is a simple scaling of the form $R = mR^\vee$, allowing applications to work directly on R, with no loss in their underlying worst-case hardness guarantees [16].

Another advantage of power-of-two cyclotomic number fields is that the sampling of error terms can be performed directly in the ring R considering a power basis, since the transformation to the associated vector subspace H isomorphic to $\mathbb{R}^n$ is just a rigid rotation followed by scaling. Essentially, this occurs because the ideal lattice obtained from the ring of integers of power-of-two cyclotomic number fields is a rotation of the $\mathbb{Z}^n$-lattice. For other choices of cyclotomic fields, sampling from a spherical Gaussian distribution can be done in an extended ring and performing a reduction modulo the cyclotomic polynomial $\Phi_m(x)$, which leads to the desired spherical distribution in the canonical embedding [11]. For general number fields, lattices realized by their ring of integers via canonical embedding do not have to be equivalent to $\mathbb{Z}^n$ and the best option in terms of security still is a sampling from an error distribution in H and computing the inverse transformation with respect to the canonical embedding [16,17].

In this context, we extend the Ring-LWE class of problems to embrace more general algebraic constructions of lattices which allow additional factors on the embedding coordinates. We replace the canonical embedding by *twisted embeddings*, which favors the diversification of security assumptions, by allowing the Ring-LWE Problem to use number fields which realize lattices equivalent to $\mathbb{Z}^n$, in addition to the power-of-two cyclotomic number fields. As a consequence, the error sampling can be performed directly in the polynomial ring without any security loss. For instance, there exists a twisted embedding for which the image of the ring of integers of the maximal real cyclotomic number field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, where $p \geq 5$ is a prime number, is a lattice equivalent to $\mathbb{Z}^{(p-1)/2}$ [7]. Twisted embeddings have been useful in coding theory, since they allow the construction of algebraic lattices with improved properties for Rayleigh fading channels, providing high density, maximum diversity, and great minimum product distance [8,12,5].

This paper is organized as follows. Section 2 is devoted to the introduction of concepts and results on lattices and algebraic number theory to be used throughout the paper. Section 3 introduces the canonical and twisted embeddings. Section 4 approaches the Gaussian measures relevant to the computational reductions which state the hardness of both the original and the Twisted Ring-LWE problems. Section 5 presents the original statement of the Ring-LWE problem in its search and decision variants, and also the computational problems which form the foundation of the (Ring)-LWE hardness. Section 6 generalizes the class of Ring-LWE problems by adopting twisted embeddings. We prove that multiplying the coordinates of vectors in the canonical representation by a twisting factor does not affect the hardness of Ring-LWE. This is shown via a reduction from both search and decision versions of Ring-LWE to their corresponding twisted forms. Moreover, we compute the new approximation factors for the reduction from SIVP to DGS (Discrete Gaussian Sampling problem), and also for the reduction from DGS to Ring-LWE. Since the new approximation factors are simply multiplied by a scalar associated with the lattice dimension n, the asymptotic factors are not affected by the change of embeddings.

Section 7 extends to a more general class of number fields the results of Ducas and Durmus on spherical Gaussian sampling [11]. We show that correct noise sampling can be performed directly in the field representation of lattices equivalent to $\mathbb{Z}^n$ without any increase in the standard deviation. Finally, Section 8 discusses the practical impacts of instantiating the Ring-LWE problem over the ring of integers of the maximal real cyclotomic number field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, where $p \geq 5$ is a prime number. We analyze the main computational operations in the compact public-key cryptosystem of Lyubashevsky, Peikert, and Regev [17], and also the format of the ring's defining polynomial in terms of the expansion factor.

2 Preliminaries on Lattices and Algebraic Number Theory

In this section, we introduce concepts, results and notation to be used throughout the paper. For a positive integer number m, denote by $[m]$ the set $\{1, 2, \ldots, m\}$. For $1 \leq p < \infty$, the ℓ_p-norm of a vector $\mathbf{a}$ in $\mathbb{R}^n$ or $\mathbb{C}^n$ is $\|\mathbf{a}\|_p = \left(\sum_{i=1}^n |a_i|^p\right)^{1/p}$, and the ℓ_∞-norm is $\|\mathbf{a}\|_\infty = \max_{i\in[n]} |a_i|$.

2.1 The Space H

Frequently, lattices are defined in the Euclidean space $\mathbb{R}^n$. However, in the Ring-LWE context, it is more convenient to define lattices in a specific subspace of $\mathbb{C}^n$ isometric to $\mathbb{R}^n$: the *space* H.

Definition 1 (Space H) Let s_1 and s_2 be non-negative integer numbers such that $n = s_1 + 2s_2 > 0$. The *subspace* $H \subseteq \mathbb{C}^n$ is defined as

$$H = \left\{ (a_1, a_2, \ldots, a_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} : a_{j+s_1+s_2} = \overline{a_{j+s_1}},\ \forall\, j \in [s_2] \right\}.$$

We consider H endowed with the inner product obtained as a restriction of the standard inner product of $\mathbb{C}^n$:

$$\langle \mathbf{a}, \mathbf{b} \rangle_H := \sum_{i \in [n]} a_i \overline{b_i} = \sum_{i \in [s_1]} a_i b_i + \sum_{j \in [s_2]} (a_{j+s_1} b_{j+s_1+s_2} + a_{j+s_1+s_2} b_{j+s_1}) \in \mathbb{R}.$$

The norm (usually ℓ_2-norm) of $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in H$ is defined as $\|\mathbf{a}\| = \sqrt{\langle \mathbf{a}, \mathbf{a} \rangle_H}$.

For $i \in [n]$, denote by $\mathbf{u}_i$ the vector with all zero coordinates except for the i-th position, which is equal to one. We consider $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ the canonical basis of $\mathbb{R}^n$ (over $\mathbb{R}$) and $\mathbb{C}^n$ (over $\mathbb{C}$). An orthonormal basis for H can be defined in terms of the canonical basis of $\mathbb{C}^n$:

Definition 2 (Canonical basis of H) Let s_1 and s_2 be non-negative integer numbers such that $n = s_1 + 2s_2 > 0$. For $i \in [s_1]$, define $\mathbf{h}_i = \mathbf{u}_i$. For $i \in [s_2]$, define $\mathbf{h}_{i+s_1} = \frac{1}{\sqrt{2}}(\mathbf{u}_{i+s_1} + \mathbf{u}_{i+s_1+s_2})$ and $\mathbf{h}_{i+s_1+s_2} = \frac{i}{\sqrt{2}}(\mathbf{u}_{i+s_1} - \mathbf{u}_{i+s_1+s_2})$. Then, the set $\mathcal{B} = \{\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n\}$ is an orthonormal basis of H, which we call the *canonical basis* of H as an n-dimensional $\mathbb{R}$-vector space.

Notice that any vector $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in H \subseteq \mathbb{C}^n$ can be written as an $\mathbb{R}$-linear combination of the vectors of the canonical basis $\mathcal{B}$ of H as

$$\mathbf{a} = \sum_{i \in [s_1]} a_i \mathbf{h}_i + \sum_{i \in [s_2]} \sqrt{2} \Re(a_{i+s_1}) \mathbf{h}_{i+s_1} + \sum_{i \in [s_2]} \sqrt{2} \Im(a_{i+s_1}) \mathbf{h}_{i+s_1+s_2},$$

where $\Re(\cdot)$ and $\Im(\cdot)$ denote the real and imaginary parts of a complex number, respectively.

The linear map $\kappa\left(\sum_{i \in [n]} b_i \mathbf{h}_i\right) := \sum_{i \in [n]} b_i \mathbf{u}_i$, with $b_i \in \mathbb{R}$, defines an isomorphism between the $\mathbb{R}$-vector spaces H and $\mathbb{R}^n$, such that $\langle \mathbf{a}, \mathbf{b} \rangle_H = \langle \kappa(\mathbf{a}), \kappa(\mathbf{b}) \rangle$, where $\langle \cdot, \cdot \rangle$ denotes the standard inner product in $\mathbb{R}^n$. Then, it follows that H and $\mathbb{R}^n$ are isometric, that is, H is an Euclidean space, as defined next. In particular, the norm of an element $\mathbf{a} \in H$ coincides with the usual norm (ℓ_2-norm) of $\kappa(\mathbf{a}) \in \mathbb{R}^n$, that is, $\|\mathbf{a}\| = \|\kappa(\mathbf{a})\|_2$.

2.2 Lattices in Euclidean Vector Spaces

An *Euclidean vector space* $(E, \langle \cdot, \cdot \rangle_E)$ is an n-dimensional $\mathbb{R}$-vector space E with an inner product $\langle \cdot, \cdot \rangle_E$, which is isometric to $\mathbb{R}^n$ with the standard inner product. Consider an orthonormal basis $\mathcal{B}(E) = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ of E.

A set $\Lambda \subset E$ is said to be a *full-rank lattice* (or simply *lattice*), if Λ is a discrete additive subgroup of E with rank n. Equivalently, $\Lambda \subset E$ is a lattice if there exists a set of linearly independent vectors $\mathbf{B} = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\} \subset E$ such that

$$\Lambda = \Lambda(\mathbf{B}) = \left\{ \sum_{i \in [n]} a_i \mathbf{v}_i \ : \ a_i \in \mathbb{Z} \right\}.$$

The set $\mathbf{B}$ is called a *basis* (or a $\mathbb{Z}$-basis) of Λ. For each $\mathbf{v}_j \in \mathbf{B}$, it can be written in terms of the orthonormal basis $\mathcal{B}(E)$ as $\mathbf{v}_j = \sum_{i \in [n]} v_{ij} \mathbf{e}_i$ for $v_{ij} \in \mathbb{R}$.

The matrix $\mathbf{M} = [v_{ij}]_{n\times n}$, for which the j-th column is given by the coefficients of $\mathbf{v}_j$ written in the orthonormal basis $\mathcal{B}(E)$, is called a *generator matrix* of Λ. Two basis generate the same lattice if and only if the associated generator matrices $\mathbf{M}$ and $\mathbf{M}'$ are related as $\mathbf{M}' = \mathbf{MU}$, where $\mathbf{U}$ is unimodular (has integer entries and $\det(\mathbf{U}) = \pm 1$). The matrix $\mathbf{G} = \mathbf{M}^t\mathbf{M}$ is called the *Gram matrix* of Λ with respect to $\mathbf{M}$. Since the basis $\mathcal{B}(E)$ of the Euclidean vector space is orthonormal, then $\mathbf{G} = [\langle \mathbf{v}_i, \mathbf{v}_j\rangle_E]_{n\times n}$. The determinant of $\mathbf{G}$ is called the *determinant* of Λ and is denoted by $\det(\Lambda)$. Clearly, $\det(\Lambda) = \det(\mathbf{M})^2$ does not depend of a particular basis of Λ.

The *dual lattice* of Λ is the lattice $\Lambda^* = \{\mathbf{a} \in E \ : \ \langle \mathbf{a}, \mathbf{b}\rangle_E \in \mathbb{Z}, \forall\, \mathbf{b} \in \Lambda\}$ and has generator matrix $(\mathbf{M}^t)^{-1}$. It is known that $(\Lambda^*)^* = \Lambda$ and if Λ has generator matrix $\mathbf{M}$, then $(\mathbf{M}^t)^{-1}$ is a generator matrix for Λ^* and therefore $\det(\Lambda^*) = \det(\Lambda)^{-1}$.

A lattice $\Lambda \subset E$ is called *integral* if $\langle \mathbf{a}, \mathbf{b}\rangle_E \in \mathbb{Z}$ for all $\mathbf{a}, \mathbf{b} \in \Lambda$. Equivalently, Λ is an integral lattice if and only if $\Lambda \subset \Lambda^* \subset (\Lambda/\det(\Lambda))$. An integral lattice is called *unimodular*, or *self-dual*, if $\det(\Lambda) = 1$ or, equivalently, if $\Lambda = \Lambda^*$.

Two lattices Λ and Λ' are said to be *equivalent* if one can be obtained from the other through a rotation, a reflection, or a change of scale. We denote this equivalence by $\Lambda \simeq \Lambda'$. Two Gram matrices $\mathbf{G}$ and $\mathbf{G}'$ of two equivalent lattices Λ and Λ', respectively, are related as $\mathbf{G}' = c^2\mathbf{U}^t\mathbf{G}\mathbf{U}$, where $c \neq 0$ is a real constant and $\mathbf{U}$ is unimodular.

We say that a lattice Λ in $(E, \langle\cdot,\cdot\rangle_E)$ is *orthogonal* if it has a basis $\mathbf{B} = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ such that $\langle \mathbf{v}_i, \mathbf{v}_j\rangle = 0$ if $i \neq j$, for all $i, j \in [n]$. This means that Λ has a diagonal Gram matrix. Moreover, if the basis $\mathbf{B}$ satisfies $\langle \mathbf{v}_i, \mathbf{v}_j\rangle = 0$ if $i \neq j$ and $\langle \mathbf{v}_i, \mathbf{v}_j\rangle = c$ if $i = j$, for all $i, j \in [n]$ and $c \in \mathbb{R}$, then Λ is equivalent to the $\mathbb{Z}^n$-lattice. In this case, Λ has a Gram matrix $\mathbf{G} = c\,\mathbf{Id}_n$. In particular, when $c = 1$, we say that Λ is an *orthonormal* lattice.

2.3 Algebraic Number Theory

In this section, we summarize concepts and results from algebraic number theory, presenting as an example the case of cyclotomic number fields and their maximal real subfields. Details can be found in [28,29].

An (*algebraic*) *number field* K is a finite extension of the field $\mathbb{Q}$. This means that $\mathbb{Q} \subset K$ and K is a $\mathbb{Q}$-vector space with finite dimension. The *degree* of K, denoted $[K : \mathbb{Q}]$, is the dimension of the $\mathbb{Q}$-vector space K. In general, if K and L are number fields such that $K \subset L$, the symbol $[L : K]$ is defined to be the integer number $[L : \mathbb{Q}]/[K : \mathbb{Q}]$ and is called the degree of the extension L/K.

By the Primitive Element Theorem, there exists an element $\theta \in K$ such that $K = \mathbb{Q}(\theta)$, which is equivalent to say that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$, with $n = [K : \mathbb{Q}]$, is a *power basis* of K over $\mathbb{Q}$. Also, if $p(x)$ is the minimal polynomial of θ over $\mathbb{Q}$, then K is isomorphic to $\mathbb{Q}[x]/(p(x))$ and $K = \mathbb{Q}(\theta')$ for every root θ' of $p(x)$. The roots of $p(x)$ are called the conjugates of θ.

Example 1 (Cyclotomic number field) A number field of particular interest is $\mathbb{Q}(\zeta_m)$, the *m-th cyclotomic field*, where $\zeta_m = \exp(2\pi i/m)$ is a primitive m-th root of unity for any integer number $m \geq 1$. The degree of $\mathbb{Q}(\zeta_m)$ is $\varphi(m)$, where $\varphi(\cdot)$ denotes Euler's totient function. The minimal polynomial of ζ_m, called the *m-th cyclotomic polynomial*, is $\Phi_m(x) = \prod_{k\in\mathbb{Z}_m^*}(x - \zeta_m^k)$, where $\mathbb{Z}_m^*$ denotes the group of invertible elements in $\mathbb{Z}_m$.

Example 2 (Maximal real subfield) The number field $\mathbb{Q}(\zeta_m + \zeta_m^{-1}) \subset \mathbb{R} \cap \mathbb{Q}(\zeta_m)$ is the *maximal real subfield* of $\mathbb{Q}(\zeta_m)$ and has degree $\varphi(m)/2$ if $m \geq 3$.

Let K be a number field. A map $\overline{}: K \to K$ is called an *involution* of K if $\overline{a+b} = \overline{a} + \overline{b}$, $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$, and $\overline{\overline{a}} = a$, for all $a, b \in K$. If $K = \mathbb{C}$, the complex conjugation is an example of involution. If $K = \mathbb{Q}(\zeta_n)$ is a cyclotomic number field, then $\overline{\zeta_n} = \zeta_n^{-1}$ is the same involution given by the complex conjugation. In this work, whenever the cyclotomic number field is used, we implicitly assume this involution. For the maximal real subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, we consider the involution restricted over $\mathbb{Q}(\zeta_n)$, which gives the identity map.

The subfield $F = \{a \in K \mid \overline{a} = a\}$, called the fixed field by the involution of K, satisfies $[K : F] \leq 2$. When $[K : F] = 1$ (or $F = K$), we say that the involution is *trivial* (it is the identity); otherwise, the involution is said to be *non-trivial.* If $K = \mathbb{Q}(\zeta_n)$, the fixed field by the involution $\overline{\zeta_n} = \zeta_n^{-1}$ of K is its maximal real subfield [6].

Field monomorphisms. Let K be a number field of degree n. There are exactly n distinct monomorphisms (of fields) from K to $\mathbb{C}$. These monomorphisms are $\mathbb{Q}$-monomorphisms. If $K = \mathbb{Q}(\theta)$ and $p(x)$ is the minimal polynomial of θ, these monomorphisms can be defined as $\sigma_i(\theta) = \theta_i$ for $i \in [n]$, where θ_i are all the distinct roots of $p(x)$.

A monomorphism $\sigma_i : K \to \mathbb{C}$ is said to be *real* if $\sigma_i(K) \subset \mathbb{R}$. Otherwise, it is said to be *complex.* If σ_i is a complex monomorphism, then $\overline{\sigma_i}$ is another complex monomorphism defined by $\overline{\sigma_i}(a) = \overline{\sigma_i(a)}$. So, we can write the degree n as $n = s_1 + 2s_2$, where $s_1 \geq 0$ is the number of real monomorphisms and $2s_2 \geq 0$ is the number of complex monomorphisms from K to $\mathbb{C}$. The pair (s_1, s_2) is called the *signature* of K. We say that K is *totally real* when $s_2 = 0$, and that K is *totally complex* when $s_1 = 0$. The number field K is said to be a *CM-field* if it is totally complex and has degree two over its fixed field by the involution F [6].

Any cyclotomic number field $K = \mathbb{Q}(\zeta_n)$, with $n \geq 3$, is totally complex. Their monomorphisms are defined as $\sigma_i(\zeta_n) = \zeta_n^i$ for each $i \in [n]$ such that $\gcd(i, n) = 1$. In turn, any maximal real cyclotomic subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is totally real. Their monomorphisms are defined as $\sigma_i(\zeta_n + \zeta_n^{-1}) = \zeta_n^i + \zeta_n^{-i}$ for each $i \in [\lfloor n/2 \rfloor]$ such that $\gcd(i, n) = 1$. Note that $\mathbb{Q}(\zeta_n)$ is a CM-field once $\mathbb{Q}(\zeta_n)$ is a totally complex field of degree two over $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

The set of automorphisms $\sigma : K \to K$, where $\sigma(a) = a$ for all $a \in \mathbb{Q}$, constitutes a group under the composition, called *Galois group* of K over $\mathbb{Q}$ and denoted by $\mathrm{Gal}(K/\mathbb{Q})$. It is a fact that $n \leq |\mathrm{Gal}(K/\mathbb{Q})| \leq n!$, where $n = [K : \mathbb{Q}]$. If $|\mathrm{Gal}(K/\mathbb{Q})| = n$, we say that K is a *Galois* number field. If $K \subset \mathbb{C}$ is a Galois number field, then the monomorphisms from K to $\mathbb{C}$ are exactly the elements of $\mathrm{Gal}(K/\mathbb{Q})$. An important fact is that any Galois number field is totally real or totally complex. Cyclotomic number fields and their maximal real subfields are Galois number fields. Specifically, the set $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_n^*$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_n + \zeta_n^{-1})/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_n^*/\{\pm 1\}$.

(Field) trace and norm. Let K be a number field. For every $a \in K$, let $p(x)$ be its minimal polynomial. The *trace* of a in the extension K over $\mathbb{Q}$, denoted $\mathrm{Tr}_{K/\mathbb{Q}}(a)$ or $\mathrm{Tr}_K(a)$, is the sum of all roots of $p(x)$. In turn, the *norm* of a in the extension K over $\mathbb{Q}$, denoted $\mathrm{N}_{K/\mathbb{Q}}(a)$ or $\mathrm{N}_K(a)$, is the product of all roots of $p(x)$. For all

$a \in K$, $\mathrm{Tr}_K(a)$ and $\mathrm{N}_K(a)$ are elements of $\mathbb{Q}$. If K is a Galois number field, the trace and norm of any element $a \in K$ can be defined, respectively, as

$$\mathrm{Tr}_K(a) = \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(a) \qquad \text{and} \qquad \mathrm{N}_K(a) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(a).$$

Ring of integers. The set of all elements in a number field K that are the root of a monic polynomial in $\mathbb{Z}[x]$ is a ring called the *ring of integers* of K, denoted by $\mathcal{O}_K$. If K is a number field of degree n, its ring of integers has a $\mathbb{Z}$-basis with n elements, which is called an *integral basis* of K. If $a \in \mathcal{O}_K$, then $\mathrm{Tr}_K(a)$ and $\mathrm{N}_K(a)$ are elements of $\mathbb{Z}$.

If $\mathcal{I}$ is a nonzero (integral) ideal of $\mathcal{O}_K$, then $\mathcal{I}$ has a $\mathbb{Z}$-basis with n elements. The same holds if $\mathcal{I}$ is a *fractional ideal* of K, which is a subset of K satisfying the condition that $d\mathcal{I} \subset \mathcal{O}_K$ is an integral ideal for some element $d \in \mathcal{O}_K$. Note that every integral ideal is also fractional ($d = 1$). Also, any $\mathbb{Z}$-basis of some nonzero fractional ideal of K, including its ring of integers, is a $\mathbb{Q}$-basis of K. If $K = \mathbb{Q}(\zeta_m)$ is the m-th cyclotomic number field, then $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$, which is the set of all $\mathbb{Z}$-linear combinations of powers of ζ_m. Similarly, the ring of integers of $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$. In general, the ring of integers of a number field $K = \mathbb{Q}(\theta)$ does not have the form $\mathbb{Z}[\theta]$. When this is the case, we say that K is a *monogenic* number field.

The fractional ideal $\mathcal{D}_K^{-1} = \{a \in K : \mathrm{Tr}_K(a\mathcal{O}_K) \subset \mathbb{Z}\}$ is the *codifferent ideal*, that is, the dual ideal of the ring of integers. Frequently, the codifferent ideal is also denoted by $\mathcal{O}_K^\vee$. Note that $\mathcal{O}_K \subset \mathcal{D}_K^{-1}$. If $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in K$, then $\mathcal{O}_K^\vee = (p'(\theta))^{-1}\mathcal{O}_K$, where $p'(x)$ is the derivative of the minimal polynomial $p(x)$ of θ [27, Section 13.2, J]. The inverse ideal of the coddiferent, that is, $\mathcal{D}_K = (\mathcal{D}_K^{-1})^{-1}$, is an ideal of $\mathcal{O}_K$ called *different* of K. In general, the *dual ideal* of any fractional ideal $\mathcal{I}$ of K is the fractional ideal $\mathcal{I}^\vee$ of K, defined as

$$\mathcal{I}^\vee := \{a \in K : \mathrm{Tr}_K(a\mathcal{I}) \subset \mathbb{Z}\} = \mathcal{I}^{-1} \cdot \mathcal{O}_K^\vee.$$

If $\mathcal{I}$ is a nonzero fractional ideal of $\mathcal{O}_K$, the norm of $\mathcal{I}$ is $N(\mathcal{I}) = |\mathcal{O}_K/\mathcal{I}|$ (the cardinality of the quotient of additive groups). If $\mathcal{I}$ and $\mathcal{J}$ are ideals of $\mathcal{O}_K$, then $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})N(\mathcal{J})$, where $\mathcal{I}\mathcal{J}$ denotes the product of $\mathcal{I}$ and $\mathcal{J}$, that is, the set all finite sums of products ab for $a \in \mathcal{I}$ and $b \in \mathcal{J}$. If $\mathcal{I}$ is a principal ideal generated by some $a \in K$, then $\mathrm{N}(\mathcal{I}) = |\,\mathrm{N}_K(a)|$.

3 Embeddings from Number Fields and Algebraic Lattices

In this section consider the following setting. Let K be an algebraic number field with degree n, signature (s_1, s_2), and $\bar{\ }$ a fixed involution. Consider F to be the fixed field by the involution of K. Let σ_i be the real monomorphisms for $i \in [s_1]$, and σ_{i+s_1} be the complex monomorphisms for $i \in [2s_2]$ from K to $\mathbb{C}$, where $\sigma_{i+s_1+s_2} = \overline{\sigma_{i+s_1}}$ for all $i \in [s_2]$. In the following, we define two different embeddings from K into the space $H \subseteq \mathbb{C}^n$: the canonical embedding and the twisted embeddings.

The *canonical embedding* from K into the subspace H is the monomorphism

$$\sigma(a) = (\sigma_1(a), \sigma_2(a), \ldots, \sigma_n(a)) \,.$$

Its image is a lattice, used in the Ring-LWE problem [16,25]. The twisted embeddings defined next are a generalization of the canonical embedding [6]. An element $\tau \in K$ is said to be *totally positive*, if $\tau \in F$ and $\tau_i = \sigma_i(\tau)$ is a positive real number for all $i \in [n]$.

Definition 3 (Twisted embeddings) For any totally positive $\tau \in F$, the τ-*twisted embedding* (or simply *twisted embedding*) is the monomorphism $\sigma_\tau : K \to H$, defined as

$$\sigma_\tau(a) = \Big(\sqrt{\tau_1}\sigma_1(a), \dots, \sqrt{\tau_{s_1}}\sigma_{s_1}(a), \\ \sqrt{\tau_{1+s_1}}\sigma_{1+s_1}(a), \dots, \sqrt{\tau_{2s_2+s_1}}\sigma_{2s_2+s_1}(a)\Big).$$

Since $\tau = 1$ in F is totally positive, then $\sigma_1 = \sigma$, which means that twisted embeddings are generalizations of the canonical embedding. Twisted embeddings provide a way to obtain a variety of lattices in $H \simeq \mathbb{R}^n$ in addition to the ones obtained via canonical embedding, as a consequence of Proposition 1 [6].

Proposition 1 ([6]) *If M is a free $\mathbb{Z}$-module of rank n in K (particularly, if M is the ring of integers of K or any fractional ideal of K), then $\sigma_\tau(M)$ is a full-rank lattice in H.*

Let $K_\mathbb{R}$ denote the tensor product $K \otimes_\mathbb{Q} \mathbb{R}$. Twisted embeddings can be extended from K to $K_\mathbb{R}$ as follows. For any totally positive element $\tau \in F$, the $\mathbb{R}$-vector space $\sigma_\tau(K_\mathbb{R})$ is isomorphic to $H \simeq \mathbb{R}^n$. If $\mathcal{B}$ is a $\mathbb{Q}$-basis of the number field K, then $\mathcal{B}$ is an $\mathbb{R}$-basis of $K_\mathbb{R}$. So, for all totally positive $\tau \in F$, $\sigma_\tau(\mathcal{B})$ is an $\mathbb{R}$-basis of H.

Consider the natural extension of the trace function $\mathrm{Tr}_K : K \to \mathbb{Q}$ to $\mathrm{Tr}_K : K_\mathbb{R} \to \mathbb{R}$. For any totally positive $\tau \in F$, we can define an inner product in $K_\mathbb{R}$ as

$$\langle a, b\rangle_\tau := \langle \sigma_\tau(a), \sigma_\tau(b)\rangle_H = \mathrm{Tr}_K(\tau a\bar{b}), \qquad a, b \in K_\mathbb{R}. \tag{1}$$

By considering the inner product $\langle\cdot,\cdot\rangle_\tau$, the $\mathbb{R}$-vector space $K_\mathbb{R}$ is an Euclidean vector space of dimension n isometric to both $(H, \langle\cdot,\cdot\rangle_H)$ and $(\mathbb{R}^n, \langle\cdot,\cdot\rangle)$.

For each $a \in K_\mathbb{R}$, the ℓ_p-norms of a under the canonical embedding are simply $\|a\|_p = \|\sigma(a)\|_p = \left(\sum_{i\in[n]} |\sigma_i(a)|^p\right)^{1/p}$ for $p < \infty$, and $\max_{i\in[n]} |\sigma_i(a)|$ for $p = \infty$. Similarly, the ℓ_p-norms induced from $\mathbb{C}^n$ under twisted embeddings are defined as

$$\|a\|_{p,\tau} := \|\sigma_\tau(a)\|_p = \left(\sum_{i\in[n]} |\sqrt{\tau_i}\sigma_i(a)|^p\right)^{1/p}$$

for $p < \infty$, and the ℓ_∞-norm is

$$\|a\|_{\infty,\tau} := \|\sigma_\tau(a)\|_\infty = \max_{i\in[n]} |\sqrt{\tau_i}\sigma_i(a)|,$$

where $\tau_i = \sigma_i(\tau)$ for a totally positive element $\tau \in F$. Thus, any free $\mathbb{Z}$-module M of rank n can be seen as a full-rank lattice directly in the Euclidean vector space $(K_\mathbb{R},\langle\cdot,\cdot\rangle_\tau)$, although the image of $\sigma_\tau(M)$ is frequently considered as in $(H, \langle\cdot,\cdot\rangle_H)$.

Using the fact that $\sigma_\tau(a \cdot b) = \sigma(a) \odot \sigma_\tau(b) = \sigma_\tau(a) \odot \sigma(b)$ for any $a, b \in K_\mathbb{R}$, where $\odot$ is the component-wise multiplication in the space H, it follows that

$$\|a \cdot b\|_{p,\tau} \leq \|a\|_\infty \|b\|_{p,\tau} \qquad \text{and} \qquad \|a \cdot b\|_{p,\tau} \leq \|a\|_p \|b\|_{\infty,\tau}. \tag{2}$$

Assuming $b = 1$, from the inequalities in (2), we are able to relate the ℓ_p-norms under twisted embeddings with the infinity norm under the canonical embedding, as

$$\|a\|_\infty \geq \frac{\|a\|_{p,\tau}}{\left(\sum_{i\in[n]} \tau_i^{p/2}\right)^{\frac{1}{p}}}.$$

We can also relate ℓ_p-norms under both embeddings in H as

$$\frac{1}{\max_{i\in[n]} \tau_i} \cdot \|a\|_{p,\tau} \leq \|a\|_p \leq \frac{1}{\min_{i\in[n]} \tau_i} \cdot \|a\|_{p,\tau}. \tag{3}$$

Since $K_\mathbb{R} \simeq \mathbb{R}^n$ under twisted embeddings, it follows that $K_\mathbb{R}$ admits an orthonormal basis. Thus, for any $\mathbb{Z}$-basis $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ of the free $\mathbb{Z}$-module M of rank n in K, the matrix $[\langle v_i, v_j\rangle_\tau]_{n\times n}$ is a Gram matrix of the lattice M in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$, which coincides with the Gram matrix of $\sigma_\tau(M)$ in $(H, \langle\cdot,\cdot\rangle_H)$ with respect to the basis $\{\sigma_\tau(v_1), \sigma_\tau(v_2), \ldots, \sigma_\tau(v_n)\}$. It should be clear that, for different totally positive elements, the lattices obtained from M may not be equivalent, as can be seen below.

Example 3 Let $K = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \ : \ a, b \in \mathbb{Q}\}$ be a totally real number field with degree 2. It follows that the fixed field by the usual involution is $F = K$. For any totally positive element $\tau \in F$, consider the lattice $M_\tau = \mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ in the inner product space $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$. The set $\{1, \sqrt{3}\}$ is a $\mathbb{Z}$-basis of M_τ and the Gram matrix of the lattice M_τ is given by

$$\mathbf{G}_\tau = \begin{bmatrix} \mathrm{Tr}_K(\tau) & \mathrm{Tr}_K(\tau\sqrt{3}) \\ \mathrm{Tr}_K(\tau\sqrt{3}) & \mathrm{Tr}_K(3\tau) \end{bmatrix}. \tag{4}$$

For example, for $\tau = 1$ and $\tau = 2 + \sqrt{3}$, the Gram matrices are given by:

$$\mathbf{G}_1 = \begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix} \quad \text{and} \quad \mathbf{G}_{2+\sqrt{3}} = \begin{bmatrix} 4 & 6 \\ 6 & 12 \end{bmatrix}. \tag{5}$$

Suppose that these two lattices are equivalent. Then, there exists a square matrix $\mathbf{U}$ with integer entries and determinant ± 1, and a real number $k \neq 0$ such that $\mathbf{G}_{2+\sqrt{3}} = k^2 \mathbf{U}^t \mathbf{G}_1 \mathbf{U}$. Since the determinant of both matrices in (5) is equal to 12, then $k = \pm 1$. Now, consider $\mathbf{U}$ to be a matrix for which the rows are given by the vectors $(a, b) \in \mathbb{Z}^2$ and $(c, d) \in \mathbb{Z}^2$. So, the system of equations $\mathbf{G}_{2+\sqrt{3}} = \mathbf{U}^t \mathbf{G}_1 \mathbf{U}$ has no solution $(a, b, c, d) \in \mathbb{Z}^4$ because the equation $2 = a^2 + 3c^2$, provided by the first entry, has no solution $(a, c) \in \mathbb{Z}^2$. This gives a contradiction. Therefore, the lattices given by the same module $M = \mathcal{O}_K$ in the two different inner product spaces $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_1)$ and $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_{2+\sqrt{3}})$ are not equivalent.

Any full-rank lattice M in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$ is said to be an *algebraic lattice*. If $M = \mathcal{I}$ is a fractional ideal in K and the lattice $\mathcal{I}$ is integral (that is, $\langle a, b\rangle_\tau \in \mathbb{Z}$ for all $a, b \in \mathcal{I}$), then $\mathcal{I}$ can be called an *ideal lattice* in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$.

Since $\langle a, b\rangle_\tau = \mathrm{Tr}_K(\tau a\bar{b})$, an ideal $\mathcal{I}$ of K constitutes an ideal lattice in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$ if and only if $\tau\mathcal{I}\bar{\mathcal{I}} \subset \mathcal{D}_K^{-1}$ $(= \mathcal{O}_K^\vee)$. Ideal lattices can be obtained if and only if K is either a totally real number field or a CM-field. In particular, ideal lattices can be obtained via cyclotomic number fields and their maximal real subfields.

Let $\mathcal{I}$ be a fractional ideal of K. It is known that $\sigma(\mathcal{I}^\vee) = \overline{\sigma(\mathcal{I})^*}$ in H under the canonical embedding. However, the same does not hold for twisted embeddings in general, as can be inferred from Proposition 2.

Proposition 2 *Let $\tau \in F$ be a totally positive element and let $\mathcal{I}$ a fractional ideal of K. Then, in the Euclidean vector space $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$, it follows that:*

(i) $\mathcal{I}^* = \tau^{-1}\overline{\mathcal{I}}^\vee$; and
(ii) $\mathcal{I}$ is an unimodular (self-dual) lattice in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$ if and only if $\tau\mathcal{I}\overline{\mathcal{I}} = \mathcal{D}_K^{-1}$.

Proof By definition, $a \in \mathcal{I}^*$ if and only if $\mathrm{Tr}_K(\tau a\overline{\mathcal{I}}) \subset \mathbb{Z}$, which occurs if and only if $\tau a \in \overline{\mathcal{I}}^\vee$, which is equivalent to $a \in \tau^{-1}\overline{\mathcal{I}}^\vee$. This proves (i). Secondly, $\mathcal{I}$ is unimodular when $\mathcal{I}$ is integral and $\mathcal{I} = \mathcal{I}^*$. The lattice $\mathcal{I}$ is integral if and only if $\tau\mathcal{I}\overline{\mathcal{I}}^{-1} \subset \mathcal{D}_K^{-1}$. In turn, by (i), $\mathcal{I} = \mathcal{I}^*$ if and only if $\mathcal{I} = \tau^{-1}\overline{\mathcal{I}}^\vee = \tau^{-1}\overline{\mathcal{I}}^{-1}\mathcal{D}_K^{-1}$, which is equivalent to $\tau\mathcal{I}\overline{\mathcal{I}} = \mathcal{D}_K^{-1}$. Therefore, $\mathcal{I}$ is unimodular if and only if $\tau\mathcal{I}\overline{\mathcal{I}} = \mathcal{D}_K^{-1}$.

4 Gaussian Measures

In this section, we strictly follow the setting of Lyubashevsky et al. [16], adapting the definitions in terms of the twisted embeddings.

For $r > 0$, define the Gaussian function $\rho_{r,\mathbf{c}} : H \to (0,1]$ centered at $\mathbf{c}$ as

$$\rho_{r,\mathbf{c}}(\mathbf{a}) = \exp(-\pi\|\mathbf{a} - \mathbf{c}\|^2/r^2). \tag{6}$$

The subscript $\mathbf{c}$ is taken to be $\mathbf{0}$ when omitted. By normalizing this function, we obtain the continuous Gaussian probability distribution D_r of width r, whose density is given by $r^{-n} \cdot \rho_r(\mathbf{x})$. We extend this definition to elliptical Gaussian distributions in $\{\mathbf{h}_i\}_{i\in[n]}$ (the canonical basis of H) as follows. Let $\mathbf{r} = (r_1, \ldots, r_n) \in (\mathbb{R}^+)^n$ be a vector of positive real numbers such that $r_{j+s_1+s_2} = r_{j+s_1}$ for each $j \in [s_2]$. Then, a sample from the n-dimensional distribution $D_\mathbf{r}$ is given by $\sum_{i\in[n]} x_i\mathbf{h}_i$, where the x_i are chosen independently from the (one-dimensional) Gaussian distribution D_{r_i} over $\mathbb{R}$. Since multiplication of elements in $K_\mathbb{R}$ is mapped to coordinate-wise multiplication in H, we have that for any element $a \in K_\mathbb{R}$, the distribution of $a \cdot D_\mathbf{r}$ is $D_{\mathbf{r}'}$, where $r_i' = r_i \cdot |\sqrt{\tau_i}\sigma_i(a)|$ for $i \in [n]$.

Because of the induced norms from $\mathbb{C}$, which maps elements of K to H, an elliptical distribution defined in the space H can be seen as a distribution directly over $K_\mathbb{R}$. For practical applications, sampling from an error distribution in $K_\mathbb{R}$ is done by generating the error in H and mapping it to its corresponding element in $K_\mathbb{R}$, via twisted embeddings. However, in some special cases, an error can be efficiently sampled directly in $K_\mathbb{R}$ without requiring the computation of the inverse of the Vandermonde matrix with respect to σ_τ [11].

Next, we use the inequalities in (3) to derive upper bounds for the smoothing parameter concerning the ℓ_p-norm under twisted embeddings. The smoothing parameter (Definition 4) is a lattice parameter defining the width beyond which a discrete Gaussian starts to behave similarly to a continuous distribution [19] and has been a subject of study in recent works [13]. The Gaussian mass of a coset $\mathbf{c} + \Lambda$ is defined as $\rho_r(\mathbf{c} + \Lambda) = \sum_{\mathbf{x}\in\mathbf{c}+\Lambda} \rho_r(\mathbf{x})$.

Definition 4 (Smoothing parameter) For an n-dimensional lattice Λ and positive real $\epsilon > 0$, the *smoothing parameter* $\eta_\epsilon(\Lambda)$ is the smallest r such that $\rho_{1/r}(\Lambda^* \setminus \{\mathbf{0}\}) \leq \epsilon$.

The *minimum distance* of a lattice Λ in the ℓ_p-norm under a τ-twisted embedding, denoted $\lambda_1^{(p,\tau)}(\Lambda)$, is the length of a shortest nonzero lattice vector, that is, $\lambda_1^{(p,\tau)}(\Lambda) = \min_{\mathbf{0}\neq\mathbf{x}\in\Lambda} \|\mathbf{x}\|_{p,\tau}$. Similarly, for any $k \leq n$, the k-th *successive minimum* of a lattice Λ, denoted $\lambda_k^{(p,\tau)}(\Lambda)$, is the smallest $\hat{r} > 0$ such that Λ contains at least k linearly independent vectors of norm at most $\hat{r}$. In this setting, Lemmas 1 and 2 present upper bounds for the smoothing parameter associated with twisted embeddings, which are a straightforward adaptation of Lemmas 2.7 and 3.5 from [22], using the inequalities in (3).

Lemma 1 *Let K be an arbitrary number field with fixed field by the involution F and $\tau \in F$ totally positive. For any $p \in [2,\infty]$, any n-dimensional lattice Λ in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$, and any $\epsilon > 0$,*

$$\eta_\epsilon(\Lambda) \leq \lambda_n^{(p,\tau)}(\Lambda) \cdot \frac{n^{1/2-1/p}}{\min_{i\in[n]} \tau_i} \cdot \sqrt{\log(2n(1+1/\epsilon))/\pi}.$$

In particular, for any $\omega(\sqrt{\log n})$ function, there is a negligible function $\epsilon(n)$ for which

$$\eta_\epsilon(\Lambda) \leq \lambda_n^{(p,\tau)}(\Lambda) \cdot \frac{n^{1/2-1/p}}{\min_{i\in[n]} \tau_i} \cdot \omega(\sqrt{\log n}).$$

Lemma 2 *Let K be an arbitrary number field with fixed field by the involution F and $\tau \in F$ totally positive. For any $p \in [1,\infty]$, any n-dimensional lattice Λ in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$, and any $\epsilon > 0$,*

$$\eta_\epsilon(\Lambda) \leq \frac{\max_{i\in[n]} \tau_i \cdot n^{1/p} \cdot \sqrt{\log(2n(1+1/\epsilon))/\pi}}{\lambda_1^{(p,\tau)}(\Lambda^*)}.$$

In particular, for any $\omega(\sqrt{\log n})$ function, there is a negligible function $\epsilon(n)$ such that

$$\eta_\epsilon(\Lambda) \leq \max_{i\in[n]} \tau_i \cdot n^{1/p} \cdot \omega(\sqrt{\log n})/\lambda_1^{(p,\tau)}(\Lambda^*).$$

Lemmas 1 and 2 will be used in Section 6.2 to derive the approximation factors in the security reductions for our generalized Ring-LWE problem aiming at estimating the NP-hardness of the (Ring)-LWE problem, in light of previous works [26,16,25]. Notice that, when $\tau = 1$, the upper bounds given in Lemmas 1 and 2 are exactly the same as presented in [22].

5 Computational Problems

In the following definitions, a lattice Λ is usually represented by a basis $\mathbf{B}$ and, in the context of algebraic lattices, Λ can be seen as a fractional ideal $\mathcal{I}$ of an arbitrary number field K via canonical embedding.

Firstly, we define the computational problems which form the foundation of the (Ring)-LWE hardness, namely the decision version of the Shortest Vector Problem

(GapSVP), the Shortest Independent Vectors Problem (SIVP), and the Discrete Gaussian Sampling (DGS) problem, which is denoted K-DGS when the underlying lattice is taken over a number field K [16].

Definition 5 (GapSVP$_\gamma$) For an approximation factor $\gamma = \gamma(n) \geq 1$, the GapSVP$_\gamma$ is: given a lattice Λ and length $d > 0$, output YES if $\lambda_1(\Lambda) \leq d$ and NO if $\lambda_1(\Lambda) > \gamma d$.

Definition 6 (SIVP$_\gamma$) For an approximation factor $\gamma = \gamma(n) \geq 1$, the SIVP$_\gamma$ is: given a lattice Λ, output n linearly independent lattice vectors of length at most $\gamma(n) \cdot \lambda_n(\Lambda)$.

For any $\mathbf{c} \in \mathbb{R}^n$, real $r > 0$, and an arbitrary lattice Λ with dimension n, normalizing the Gaussian function $\rho_{r,\mathbf{c}}(\mathbf{a})$ gives the *discrete Gaussian distribution* over Λ as

$$D_{\Lambda,r,\mathbf{c}}(\mathbf{a}) = \frac{\rho_{r,\mathbf{c}}(\mathbf{a})}{\rho_{r,\mathbf{c}}(\Lambda)},$$

for all $\mathbf{a} \in \Lambda$. Seeing a fractional ideal $\mathcal{I}$ of an arbitrary number field K as a lattice, let $D_{\mathcal{I},r}$ denote the discrete Gaussian distribution over the lattice $\mathcal{I}$ in $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_{\tau=1})$ of width r.

Definition 7 (K-DGS$_\gamma$) For a function γ that maps lattices to nonnegative reals, the K-DGS$_\gamma$ problem is: given an ideal $\mathcal{I}$ in K and a parameter $r \geq \gamma = \gamma(\mathcal{I})$, output an independent sample from a distribution that is within negligible distance of $D_{\mathcal{I},r}$.

Alternatively, for the purpose of the worst-case to average-case reduction for (Ring-)LWE, the DGS problem can be stated as follows: given an n-dimensional lattice Λ and a number $r \geq \sqrt{2n} \cdot \eta_\epsilon(\Lambda)/\alpha$, output a sample from $D_{\Lambda,r}$.

In order to define the Ring-LWE distribution and the computational problems associated with it, let K be a number field with ring of integers $R = \mathcal{O}_K$. Recall that $R^\vee$ is the (fractional) codifferent ideal of K, and let $\mathbb{T} = K_\mathbb{R}/R^\vee$. Let $q \geq 2$ be a (rational) integer modulus and, for any fractional ideal $\mathcal{I}$ of K, let $\mathcal{I}_q = \mathcal{I}/q\mathcal{I}$. In this context, we assume the inner product space $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_{\tau=1})$, which corresponds to the original definition of the Ring-LWE problem.

Definition 8 ([16] Ring-LWE distribution) For $s \in R_q^\vee$ (the "secret") and an error distribution ψ over $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_{\tau=1})$, a sample from the Ring-LWE distribution $\mathcal{A}_{s,\psi}$ over $R_q \times \mathbb{T}$ is generated by choosing $a \leftarrow R_q$ uniformly at random, choosing $e \leftarrow \psi$, and outputting $(a, b = (a \cdot s)/q + e \mod R^\vee)$.

Definition 9 ([16] Ring-LWE, search) Let Ψ be a family of distributions over $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_{\tau=1})$. The search version of the Ring-LWE problem, denoted R-LWE$_{q,\Psi}$, is defined as follows: given access to arbitrarily many independent samples from $\mathcal{A}_{s,\psi}$, for some arbitrary $s \in R_q^\vee$ and $\psi \in \Psi$, find s.

Definition 10 ([16,25] Ring-LWE, average-case decision) Let Υ be a distribution over a family of error distributions, each over $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_{\tau=1})$. The average-case Ring-LWE decision problem, denoted R-LWE$_{q,\Upsilon}$, is to distinguish (with non-negligible advantage) between independent samples from $\mathcal{A}_{s,\psi}$ for a random choice of $(s, \psi) \leftarrow U(R_q^\vee) \times \Upsilon$, and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$.

6 The Twisted Ring-LWE

In this section, we propose an extended version of the Ring-LWE problem, adopting twisted embeddings rather than the canonical embedding. We refer to this new class of problems as *Twisted Ring-LWE*, or simply Ring-LWE$^\tau$. We also prove that solving the Twisted Ring-LWE problem is at least as hard as solving the original Ring-LWE problem [16], providing a polynomial-time reduction from Ring-LWE to Twisted Ring-LWE.

In the Ring-LWE distribution, the error e is randomized by a distribution ψ over the space $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_{\tau=1})$. In this sense, an error in $K_\mathbb{R}$ can be seen as the inverse image of a sample from the distribution ψ in $H \simeq \mathbb{R}^n$ via the canonical embedding. In our general case, we consider K a number field with an involution, F its associated fixed field, $\tau \in F$ a totally positive element, and σ_τ the twisted embedding. The error e is randomized by a distribution ψ over $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$. In the following, it is assumed $q \geq 2$ is an integer number, $R := \mathcal{O}_K$, and $\mathcal{I}_q := \mathcal{I}/q\mathcal{I}$ for any fractional ideal $\mathcal{I}$ of K.

Definition 11 (Twisted Ring-LWE distribution) For a totally positive element $\tau \in F$, let ψ_τ denote an error distribution over the inner product $\langle\cdot,\cdot\rangle_\tau$ and $s \in R_q^\vee$ (the "secret") be an uniformly randomized element. The *Twisted Ring-LWE distribution* $\mathcal{A}_{s,\psi_\tau}$ produces samples of the form

$$(a,\ b = a \cdot s + e \mod qR^\vee) \in R_q \times K_\mathbb{R}/qR^\vee, \tag{7}$$

where a is uniformly randomized in R_q and the error e is randomized by ψ_τ in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$.

Analogously to Ring-LWE [16], which is defined in the space $K_\mathbb{R}$ provided with the inner product associated to the canonical embedding, we can define both search and decision problems in the space $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$ as follows. We strictly follow the search problem as defined by Lyubashevsky et al. [16] and the decision problem which was further defined by Peikert et al. [25].

Definition 12 For a positive real $\alpha > 0$, the family $\Psi_{\leq\alpha}^{(\tau)}$ is the set of all elliptical Gaussian distributions $D_\mathbf{r}$ over $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$, where each parameter $r_i \leq \alpha$.

Definition 13 (Ring-LWE$^\tau$, search) Let $\Psi^{(\tau)}$ be a family of distributions over the inner product space $(K_\mathbb{R},\langle\cdot,\cdot\rangle_\tau)$. The search version of the Ring-LWE$^\tau$ problem is defined as follows: given access to arbitrarily many independent samples from A_{s,ψ_τ} for some arbitrary $s \in R_q^\vee$ and $\psi_\tau \in \Psi^{(\tau)}$, find s.

Definition 14 Fix an arbitrary $f(n) = \omega\left(\sqrt{\log n}\right)$. For $\alpha > 0$, a distribution sampled from $\Upsilon_\alpha^{(\tau)}$ is an elliptical Gaussian $D_\mathbf{r}$ in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$, where $\mathbf{r}$ is sampled as follows: for $i \in [s_1]$, sample $x_i \leftarrow D_1$ and set $r_i^2 = \alpha^2(x_i^2 + f^2(n))/2$. For $i = s_1+1, \ldots, s_1+s_2$, sample $x_i, y_i \leftarrow D_{1/\sqrt{2}}$ and set $r_i^2 = r_{i+s}^2 = \alpha(x_i^2+y_i^2+f^2(n))/2$.

Notice that, in Definition 14, sampling $x_i \leftarrow D_1$ for $i \in [s_1]$ and $x_i, y_i \leftarrow D_{1/\sqrt{2}}$ for $i = s_1 + 1, \ldots, s_1 + s_2$ is done according to the Gaussian function given in Equation 6, using the norm induced by the corresponding twisted embedding.

Definition 15 (Ring-LWE$^\tau$, average-case decision) Let $\Upsilon^{(\tau)}$ be a distribution over a family of error distributions, each in the inner product space $(K_{\mathbb{R}}, \langle\cdot,\cdot\rangle_\tau)$. The average-case decision version of the Ring-LWE$^\tau$ problem is to distinguish, with non-negligible advantage, between arbitrarily many independent samples from $\mathcal{A}_{s,\psi_\tau}$, for a random choice of $(s, \psi_\tau) \leftarrow U(R_q^\vee) \times \Upsilon^{(\tau)}$, and the same number of uniformly random and independent samples from $R_q \times K_{\mathbb{R}}/R^\vee$.

Generally speaking, the Twisted Ring-LWE distribution and both search and decision variants of Twisted Ring-LWE collapse to their original definitions in the Ring-LWE problem when $\tau = 1$.

6.1 Hardness of Twisted Ring-LWE

In this section we provide evidence of the hardness of the Ring-LWE$^\tau$ class of problems. Firstly, we provide reductions from the Ring-LWE problem to the Ring-LWE$^\tau$ problem. By doing so, the Ring-LWE$^\tau$ problem is proven to be at least as hard as NP-hard lattice problems. It occurs that these are indeed self reductions, in the sense that they preserve the secret term $s \in R_q^\vee$, only distorting the error distribution over $K_{\mathbb{R}}$.

We recall that the reduction to the search version of Ring-LWE is defined over a set of elliptical Gaussian distributions over $K_{\mathbb{R}}$ (Definition 12).

Theorem 1 *Let K be an arbitrary number field and $\tau \in F$ be totally positive. Let (s, ψ) be randomly chosen from $(U(R_q^\vee) \times \Psi)$ in $(K_{\mathbb{R}}, \langle\cdot,\cdot\rangle_{\tau=1})$. Then there is a polynomial-time reduction from* Ring-LWE$_{q,\psi}$ *to* Ring-LWE$^\tau_{q,\psi_\tau}$.

Proof We assume the existence of an oracle for Ring-LWE$^\tau$ that, given a set of independent samples from $\mathcal{A}_{s,\psi_\tau}$, for some arbitrary $s \in R_q^\vee$ and $\psi_\tau \in \Psi^{(\tau)}$, recovers the secret term s. Given a set of independent samples from the Ring-LWE distribution $\mathcal{A}_{s,\psi}$, solving the search version of Ring-LWE amounts to finding the secret s. In order to evoke the Ring-LWE$^\tau$ oracle to solve Ring-LWE, we must ensure that the error terms from the input samples follow a Gaussian distribution $\psi_\tau \in \Psi^{(\tau)}$. Let the input samples from $\mathcal{A}_{s,\psi}$ be represented as

$$(a_i, b_i = a_i \cdot s + e_i \mod qR^\vee) \in R_q \times \mathbb{T},$$

where $e_i \xleftarrow{\psi} K_{\mathbb{R}}$. Thus, we use the fact that $e_i = \sigma^{-1}(\tilde{\mathbf{e}}_i)$, for some $\tilde{\mathbf{e}}_i$ obtained from the Gaussian distribution ψ over H. The Ring-LWE$^\tau$ samples are obtained by first computing the corresponding representatives of each pair (a_i, b_i) in H as

$$\{(\sigma(a_i), \sigma(b_i))\} = \{(\sigma(a_i), \sigma(a_i) \cdot \sigma(s) + \tilde{\mathbf{e}}_i)\}.$$

By applying the inverse transformation σ_τ^{-1}, we obtain that

$$\left\{\left(\sigma_\tau^{-1}(\sigma(a_i)), \sigma_\tau^{-1}(\sigma(b_i))\right)\right\} = \left\{\left(\sigma_\tau^{-1}(\sigma(a_i)), \sigma_\tau^{-1}(\sigma(a_i)) \cdot s + \sigma_\tau^{-1}(\tilde{\mathbf{e}}_i)\right)\right\}. \tag{8}$$

Notice that s was unchanged by the transformations, so it is a randomized element over $R_q^\vee$. Because a_i was sampled according to a uniform distribution over R_q and both σ and σ_τ^{-1} transformations are injective, $\sigma_\tau^{-1}(\sigma(a_i))$ is also uniform in R_q.

And, finally, since $e_i \xleftarrow{\psi^\tau} K_\mathbb{R}$, the set of samples in (8) follows the distribution $\mathcal{A}_{s,\psi^\tau}$. Given the set of samples (8) as input for the Ring-LWE$^\tau$ solver, it finds the secret s. Then, mapping the solution to the Ring-LWE instance of the Ring-LWE$^\tau$ solution is done by the identity transformation. Since the computation of the transformations σ and σ_τ^{-1} can be seen as vector-matrix multiplications, the reduction costs $O(n^2)$ operations. Thus, the given reduction from Ring-LWE to Ring-LWE$^\tau$ runs in polynomial time. This concludes the proof. □

Theorem 2 *Let K be an arbitrary number field and $\tau \in F$ be a totally positive element. Let (s, ψ) be randomly chosen from $(U(R_q^\vee) \times \Upsilon)$ in $(K_\mathbb{R}, \langle \cdot, \cdot \rangle_{\tau=1})$. There is a polynomial-time reduction from* Ring-LWE$_{q,\Upsilon}$ *to* Ring-LWE$^\tau_{q,\Upsilon^{(\tau)}}$.

Proof Given a set of m pairs of the form $(a_i, b_i) \in R_q \times \mathbb{T}$, each drawn either from $\mathcal{A}_{s,\psi}$ or from a uniform distribution over $R_q \times \mathbb{T}$, we prove that the (decision) Ring-LWE problem can be solved using only an oracle for (decision) Ring-LWE$^\tau$ and a polynomial-time function for mapping the input instances. As in the reduction for the search variant, we apply the transformations σ and σ_τ^{-1}, in this order, to each pair $(a_i, b_i) \in R_q \times \mathbb{T}$. As a result, those pairs drawn from $(U(R_q), U(\mathbb{T}))$ are still uniformly distributed over $R_q \times \mathbb{T}$, since both σ and σ_τ^{-1} are injective maps. On the other hand, the pairs drawn from $\mathcal{A}_{q,\psi}$ now follow the Ring-LWE$^\tau$ distribution $\mathcal{A}_{q,\psi_\tau}$. Thus, given an algorithm that solves (decision) Ring-LWE$^\tau$, it distinguishes in two different sets the $m/2$ samples drawn from $\mathcal{A}_{q,\psi_\tau}$ and those $m/2$ uniformly distributed. Since mapping Ring-LWE to Ring-LWE$^\tau$ instances preserves distributions, the solution for (decision) Ring-LWE problem is done by an identity transformation. Finally, the computation of the transformations σ and σ_τ^{-1} costs $O(n^2)$ operations; thus, the reduction runs in polynomial time. This concludes the proof. □

6.2 Computing the Approximation Factors

Throughout this section, consider an arbitrary number field K of degree n with ring of integers $R = \mathcal{O}_K$, and $\mathcal{I}$ a fractional ideal in K. Concerning the canonical embedding, a twisted embedding modifies the representatives of a fractional ideal $\mathcal{I}$ when seen as a lattice $\sigma_\tau(\mathcal{I})$ in H. Thus, since we use lattice measures such as the minimum distance and the successive minima in the security reductions, in this section we analyze the effect of redefining the inner product in the Ring-LWE security reductions.

The (search) Ring-LWE hardness consists in two reductions: *i*) a worst-case to average-case reduction from DGS to Ring-LWE (Theorem 3); and *ii*) a reduction from the Generalized Independent Vectors Problem (GIVP), which is a generalization of SIVP, to DGS (Lemma 3).

Theorem 3 ([16, Theorem 4.1]) *Let K be an arbitrary number field of degree n with ring of integers $R = \mathcal{O}_K$, and $\mathcal{I}$ a fractional ideal in K. Let $\alpha = \alpha(n) > 0$, and let $q = q(n) \geq 2$ be such that $\alpha q \geq 2 \cdot \omega(\sqrt{\log n})$. For some negligible $\epsilon = \epsilon(n)$, there is a probabilistic polynomial-time quantum reduction from K-DGS$_\gamma$ to R-LWE$_{q,\Psi_{\leq\alpha}}$, where*

$$\gamma = \max\left\{\eta_\epsilon(\mathcal{I}) \cdot (\sqrt{2}/\alpha) \cdot \omega(\sqrt{\log n}), \sqrt{2n}/\lambda_1(\mathcal{I}^\vee)\right\}.$$

Lemma 3 **([26, Lemma 3.17])** *For any $\epsilon = \epsilon(n) \leq \frac{1}{10}$ and any $\varphi(\Lambda) \geq \sqrt{2}\eta_\epsilon(\Lambda)$, there is a polynomial time reduction from GIVP$_{2\sqrt{n}\varphi}$ to DGS$_\varphi$.*

In light of Theorem 3 and Lemma 3, we use the inequalities for the smoothing parameter η_ϵ derived in Lemmas 1 and 2 (Section 4) to recompute the approximation factors, considering the parameter $\tau \in F$ induced by using twisted embeddings.

We start by computing the approximated factor γ from Theorem 3. As long as $\alpha < \sqrt{\log n/n}$, it follows that the K-DGS$_\gamma$ parameter is

$$\gamma = \eta_\epsilon(\mathcal{I}) \cdot (\sqrt{2}/\alpha) \cdot \omega(\sqrt{\log n}) = \eta_\epsilon(\mathcal{I}) \cdot \tilde{O}(1/\alpha).$$

Using the inequality $\eta_\epsilon(\mathcal{I}) \leq \lambda_n^{(p,\tau)}(\Lambda) \cdot \frac{n^{1/2-1/p}}{\min_{i\in[n]} \tau_i} \cdot \omega(\sqrt{\log n})$ from Lemma 1, we obtain that the parameter φ in Lemma 3 is

$$\varphi \leq \lambda_n^{(p,\tau)}(\Lambda) \cdot \frac{n^{1/2-1/p}}{\min_{i\in[n]} \tau_i} \cdot \omega(\sqrt{\log n}) \cdot \tilde{O}(1/\alpha).$$

Now, using the above inequality for φ, we define the upper bound for the GIVP parameter to be μ, for which

$$\mu = 2\sqrt{n}\varphi \leq 2\sqrt{n} \cdot \lambda_n^{(p,\tau)}(\Lambda) \cdot \frac{n^{1/2-1/p}}{\min_{i\in[n]} \tau_i} \cdot \omega(\sqrt{\log n}) \cdot \tilde{O}(1/\alpha).$$

Remark 1 Notice that, regardless of the ℓ_p-norm, $\mu = \tilde{O}(\sqrt{n}/\alpha)$. Since $\tilde{O}(\sqrt{n}/\alpha)$ is the approximation factor for the search version of the Ring-LWE problem [16, Section 4], we conclude that the approximation factors remain unchanged with respect to the change of embeddings due to the asymptotic notation. Moreover, since the twisting factor is constant concerning the number field degree n, the approximation factors for the decision version of the Twisted Ring-LWE problem also remain unchanged.

7 Applications of the Twisted Ring-LWE

In this section, we discuss how to extend to a more general class of number fields the results of Ducas and Durmus for sampling from a spherical Gaussian distribution [11], focusing on the algebraic realization of $\mathbb{Z}^n$-lattices.

Durmus and Ducas proved a special case when a spherical Gaussian distribution with width s in the power basis corresponds to a spherical Gaussian distribution with width $s\sqrt{m'}$ over the space H (Theorem 4) [11]. In order to sample directly over the cyclotomic ring $\mathbb{Q}[x]/(\Phi_m(x))$, leading to the correct distribution in the embedding representation, they sample the error polynomial in the ring $\mathbb{Q}[x]/(\Theta_m(x))$, where $\Theta_m(x) = x^m - 1$ if m is odd, and $\Theta_m(x) = x^{\frac{m}{2}} + 1$ if m is even. Then, the reduction modulo Φ_m leads to the correct distribution under the canonical embedding. This method avoids resorting to complex embeddings and the inverse of the Vandermonde matrix.

In the statement of Theorem 4, let $m' = m$ if m is odd and $m' = m/2$ if m is even. Also, let β represent the polynomial reduction from $\mathbb{Q}[x]/(\Theta_m(x))$ to $\mathbb{Q}[x]/(\Phi_m(x))$, and let the linear operator $\mathbf{T} : H \to H$ with matrix in the canonical basis of H be:

$$\mathbf{T} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{Id}_{\phi(m)/2} & i\,\mathbf{Id}_{\phi(m)/2} \\ \mathbf{Id}_{\phi(m)/2} & -i\,\mathbf{Id}_{\phi(m)/2} \end{pmatrix}, \quad \text{with } i = \sqrt{-1}. \tag{9}$$

Theorem 4 **([11, Theorem 5])** *Let $v \in \mathbb{Q}[x]/(\Theta_m(x))$ be a random variable distributed as $\psi_s^{m'}$ in the power basis. Then, the distribution of $(\mathbf{T}^{-1} \circ \sigma \circ \beta)(v)$, seen in the canonical basis of H, is the spherical Gaussian $\psi_{s\sqrt{m'}}^{\phi(m)}$.*

The shape of the distribution is preserved because the transformation $\mathbf{T}^{-1} \circ \sigma$ is, in fact, a scaled-orthogonal map from the power basis of $\mathbb{Q}[x]/(\Phi_m(x))$ to the space H, where $\mathbf{T}^{-1}$ is Hermitian ($\mathbf{T}^{-1} = \overline{\mathbf{T}}^t$). The proof for Theorem 4 reduces to proving that $\mathbf{M} \in \mathbb{C}^{\phi(m) \times m'}$, the matrix representing the linear map γ from the power basis of $\mathbb{Z}[x]/(\Theta_m(x))$ to the canonical basis of $\mathbb{C}^{\phi(m)}$ satisfies $\mathbf{C} = \mathbf{M}\overline{\mathbf{M}}^t = m' \, \mathbf{Id}_{\phi(m)}$. The coefficients of $\mathbf{M}$ are given by $m_{i,j} = \sigma_j(x^i) = \zeta_m^{ij}$. Then, for all $i, j \in \mathbb{Z}_m^*$, we have that

$$c_{i,j} = \sum_{k \in [m']} \zeta_m^{ik} \overline{\zeta_m^{jk}} = \sum_{k \in [m']} (\zeta_m^{i-j})^k = \begin{cases} m' & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, $\mathbf{E} = \mathbf{T}^{-1}\mathbf{M} = \overline{\mathbf{E}}$, so $\mathbf{E}\mathbf{E}^t = \mathbf{E}\overline{\mathbf{E}}^t = \mathbf{T}^{-1}\mathbf{M}\overline{\mathbf{M}}^t\mathbf{T} = m' \, \mathbf{Id}_{\phi(m)}$. This last equation implies that, if a random variable $v \in \mathbb{Q}[x]/(\Theta_m(x))$ has covariance matrix $s^2 \, \mathbf{Id}_{m'}$, then the covariance matrix of $(\mathbf{T}^{-1} \circ \gamma)(v)$ is $s^2 \mathbf{E} \, \mathbf{Id}_{m'} \, \overline{\mathbf{E}}^t = s^2 m' \, \mathbf{Id}_{\phi(m)}$, and the distribution of $(\mathbf{T}^{-1} \circ \gamma)(v)$ is the spherical Gaussian $\psi_{s\sqrt{m'}}^{\phi(m)}$.

In the following, we discuss how the shape of spherical Gaussian distributions may be preserved when seen in the space H for special algebraic constructions under twisted embeddings. Following Ducas and Durmus' approach, we are interested in lattices equivalent to $\mathbb{Z}^n$, whose Gram matrices have the form $c \, \mathbf{Id}_n$ for $c \in \mathbb{R}$. In this sense, the matrix mapping elements of $K_\mathbb{R}$ to the space H is a scaled-orthogonal map [11]. It follows that any algebraic realization of the $\mathbb{Z}^n$-lattice preserves the shape of an error distribution over $K_\mathbb{R}$ when seen as in H.

In Theorem 5, we prove that fractional ideals realizing lattices equivalent to $\mathbb{Z}^n$ in an orthonormal basis, which are the special case when the Gram matrix is simply $\mathbf{Id}_n$, preserve both format and standard deviation of spherical Gaussian distributions. We recall that ideal lattices can be obtained if and only if K is a totally real number field, or if K is a CM-field [6].

Theorem 5 *Let K be a number field with an involution and F its associated fixed field. Consider $\tau \in F$ totally positive and $\mathcal{I} \subset \mathcal{O}_K$ a fractional ideal such that $\mathcal{I}$ is an ideal lattice in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$. If $\mathcal{I}$ is a lattice equivalent to $\mathbb{Z}^n$, then both the shape and the standard deviation of a spherical Gaussian distribution in an orthonormal basis of $\mathcal{I} \subset K_\mathbb{R}$ are preserved when seen in the canonical basis of the space H (via the twisted embedding σ_τ).*

Proof Let n be the degree of K and let $v \in \mathcal{I}$ be a random variable over the spherical Gaussian distribution with covariance matrix $s^2 \, \mathbf{Id}_n$ in an orthonormal $\mathbb{Z}$-basis of $\mathcal{I}$, for some real number s. Since the twisted embedding $\sigma_\tau : K_\mathbb{R} \to H$ is a linear transformation, the covariance matrix of $\sigma_\tau(v)$ in the canonical basis of H is $\mathbf{E}s^2 \, \mathbf{Id}_n \, \mathbf{E}^t$, where $\mathbf{E} = \mathbf{T}^{-1}\mathbf{M}$, with $\mathbf{T}$ as in (9) and $\mathbf{M}$ is the generator matrix of $\sigma_\tau(\mathcal{I})$. Since $\mathbf{M}\mathbf{M}^t = \mathbf{M}^t\mathbf{M} = \mathbf{Id}_n$, and because $\mathbf{M}\mathbf{M}^t$ is the Gram matrix of the $\mathbb{Z}^n$-equivalent lattice $\mathcal{I}$ in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$, the covariance matrix of $\sigma_\tau(v)$ is

$$\mathbf{E}s^2 \, \mathbf{Id}_n \, \mathbf{E}^t = \mathbf{T}^{-1}\mathbf{M}s^2 \, \mathbf{Id}_n \, \mathbf{M}^t\mathbf{T} = s^2 \, \mathbf{Id}_n,$$

which proves that $\sigma_\tau(v)$ is randomized in the spherical Gaussian distribution over the canonical basis of H with the same standard deviation as v over $K_\mathbb{R}$ in the orthonormal basis of $\mathcal{I}$. This concludes the proof. □

Examples of ideal lattices equivalent to $\mathbb{Z}^n$ are those obtained from cyclotomic number fields $\mathbb{Q}(\zeta_{2^k})$ [6], and their maximal real subfields [3], and the maximal real subfields $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ for any prime $p \geq 5$. The case of the power-of-two cyclotomic number fields were previously addressed by Lyubashevsky et al. [16], and Ducas and Durmus [11]. In the following, we discuss the family of lattices equivalent to $\mathbb{Z}^n$ built on $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, for any $p \geq 5$ prime.

Let $p \geq 5$ be a prime number, $n = (p-1)/2$, and $\zeta = \zeta_p = \exp(-2i\pi/p)$. The cyclotomic construction of the $\mathbb{Z}^n$-lattice (Proposition 3) is on the ring of integers of the maximal real subfield of a cyclotomic number field, denoted $\mathbb{Q}(\zeta + \zeta^{-1})$, whose integral basis is $\mathcal{C} = \{e_j = \zeta^j + \zeta^{-j} \mid 1 \leq j \leq n\}$.

Proposition 3 ([21, Proposition 1]) *Let $p \geq 5$ be a prime number, and let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $\tau = \frac{1}{p}(1-\zeta_p)(1-\zeta_p^{-1})$. Then $\mathcal{O}_K$ in $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$ is a lattice equivalent to $\mathbb{Z}^n$ with basis $\mathcal{C}' = \{e'_1, \ldots, e'_n \mid e'_n = e_n$ and $e'_j = e_j + e'_{j+1}\}$, where $\mathcal{C} = \{e_1, \ldots, e_n\}$ is an integral basis of K.*

The generator matrix of the $\mathbb{Z}^n$-lattice in $H = \mathbb{R}^n$ (this is an equality because K is totally real), realized in Proposition 3, is given by

$$\mathbf{M} = \mathbf{D}\mathbf{M}'\mathbf{U}, \tag{10}$$

where $\mathbf{D} = \operatorname{diag}\left[\sqrt{\frac{\sigma_k(\tau)}{p}}\right]_{n\times n}$, $\mathbf{M}' = \left[\sigma_i(\zeta^j + \zeta^{-j})\right]_{i,j\in[n]\times[n]}$ and

$$\mathbf{U} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix}_{n\times n}.$$

As an immediate consequence of Theorem 5, in Corollary 1 we prove that the construction for the $\mathbb{Z}^n$-lattice mentioned above, in fact does not change the shape of the error distribution and, more importantly, the standard deviation is the same when the distribution is seen over H.

Corollary 1 *Let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ for $p \geq 5$ prime and let $v \in \mathcal{O}_K$ be a random variable distributed as ψ_s^n in the basis $\mathcal{C}'$. Then, the distribution of $(\mathbf{T}^{-1} \circ \sigma_\tau)(v)$ for $\tau = \frac{1}{p}(1-\zeta_p)(1-\zeta_p^{-1})$, seen in the canonical basis of H, is the spherical Gaussian ψ_s^n.*

Proof In the realization of the $\mathbb{Z}^n$-lattice (Proposition 3), the matrix representing the linear map σ_τ from the basis $\mathcal{C}'$ of $\mathcal{O}_K$ to the canonical basis of $\mathbb{R}^n$ is given by $\mathbf{M}$ (10). Since $\mathcal{O}_K$ is a lattice equivalent to $\mathbb{Z}^n$ in the basis $\mathcal{C}'$, the result follows immediately from Theorem 5. This concludes the proof. □

8 Practical Impacts

In this section, we use the fact that $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is a subfield of $\mathbb{Q}(\zeta_p)$, for p prime, to analyze the practical impacts of instantiating the Ring-LWE problem over the ring of integers of K in the compact public-key cryptosystem of Lyubashevsky, Peikert, and Regev [17, Section 8.2].

The public-key cryptosystem presented below is parameterized by an mth cyclotomic ring R and two coprime integers p and q. The message space is defined as R_p and it is required that q be coprime with every odd prime dividing m. Consider that ψ_τ is an error distribution over $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$ and $\lfloor\cdot\rceil$ denotes a valid discretization to (cosets) of $R^\vee$ or $pR^\vee$. Also, $\hat{m} = m/2$ if m is even, otherwise $\hat{m} = m$. Finally, for any $\bar{a} \in \mathbb{Z}_q$, let $[\![\bar{a}]\!]$ denote the unique representative $a \in (\bar{a} + q\mathbb{Z}) \cap [-q/2, q/2)$, which is entry-wise extended to polynomials.

- $\texttt{Gen}$: choose a uniformly random $a \in R_q$. Choose $x \leftarrow \lfloor\psi_\tau\rceil_{R^\vee}$ and $e \leftarrow \lfloor p \cdot \psi_\tau\rceil_{pR^\vee}$. Output $(a, b = \hat{m}(a \cdot x + e) \mod qR) \in R_q \times R_q$ as the public key, and x as the secret key.
- $\texttt{Enc}_{(a,b)}(\mu \in R_p)$: choose $z \leftarrow \lfloor\psi_\tau\rceil_{R^\vee}, e' \leftarrow \lfloor p \cdot \psi_\tau\rceil_{pR^\vee}$, and $e'' \leftarrow \lfloor p \cdot \psi_\tau\rceil_{t^{-1}\mu + pR^\vee}$. Let $u = \hat{m}(a \cdot z + e') \mod qR$ and $v = z \cdot b + e'' \in R_q^\vee$. Output $(u, v) \in R_q \times R_q^\vee$.
- $\texttt{Dec}_x(u, v)$: compute $v - u \cdot x \mod qR^\vee$, and decode it to $d = [\![v - u \cdot x]\!] \in R^\vee$. Output $\mu = t \cdot d \mod pR$.

In such an encryption scheme, the most computationally expensive operations are given by the error sampling and the discretization of the error terms, and the polynomial multiplication. As proved in Corollary 1, when R is the ring of integers of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, the sampling of error terms can be performed directly over $(K_\mathbb{R}, \langle\cdot,\cdot\rangle_\tau)$ in the orthonormal basis $\mathcal{C}^\perp$ while preserving the spherical format and the standard deviation with respect to the corresponding distribution in H. In this case, the error sampling is similar to that performed when K is a cyclotomic field with dimension a power of two, where the spherical format is preserved but the standard deviation increases by m'. Because of that, any algorithm for one-dimensional discrete Gaussian sampling can be used in our instantiation, including those already adopted in the power-of-two cyclotomic case. The efficiency of discrete sampling when $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is emphasized by the fact that the discretization in $\mathbb{Z}^n$-lattices is simply a coordinate-wise rounding to the nearest integer.

In Ring-LWE cryptosystems, arithmetic operations such as addition and multiplication are performed in the polynomial representation of the ring of integers. The ring of integers of the maximal real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. Thus, associating $\zeta_p + \zeta_p^{-1}$ with indeterminate x yields an isomorphism between $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ and $\mathbb{Z}[x]/(\Psi_p(x))$, where $\Psi_p(x)$ is the minimal polynomial of $\zeta_p + \zeta_p^{-1}$. This would require a change of basis from $\mathcal{C}^\perp$, the basis used for error sampling, to the power basis $\{(\zeta + \zeta^{-1})^j \mid 0 \leq j < n\}$. The coefficients of the defining polynomial $\Psi_p(x)$ vary according to the choice of p. Aranés and Arenas provided a closed formula for the coefficients of $\Psi_{p^v}(x)$ for p prime and $v \geq 1$ (Theorem 7). Consider that, for strictly positives r and k, $A_r(k)$ are the determinants of order k, defined in Theorem 6. For details, we refer the reader to [4].

Theorem 6 **([4, Theorem 1])** *For any strictly positive integers r and k, we have that*

$$A_r(k) = \binom{r+k-2}{k} + \binom{r+k-3}{k-1},$$

where $\binom{n}{k}$ denotes the binomial coefficient $\frac{n!}{k!(n-k)!}$.

Theorem 7 **([4, Theorem 2])** *The coefficients a_j of the polynomial $\Psi_{p^\upsilon}(x)$ are given by the following formulae. If p is odd,*

$$a_j = \begin{cases} 0, & \text{if } j > m - p^{\upsilon-1}; \\ \displaystyle\sum_{\substack{k=1 \\ k \equiv 1 \pmod 2}}^{\left[\frac{m-j}{p^{\upsilon-1}}\right]} (-1)^{(m-j-kp^{\upsilon-1})/2} A_{j+2}\left(\frac{m-j-kp^{\upsilon-1}}{2}\right), & \text{if } m+j \equiv 1 \pmod 2; \\ (-1)^{\frac{m-j}{2}} \displaystyle\sum_{k=0}^{\left[\frac{m-j}{2p^{\upsilon-1}}\right]} (-1)^k A_{j+2}\left(\frac{m-j}{2} - kp^{\upsilon-1}\right), & \text{if } m+j \equiv 0 \pmod 2; \end{cases}$$

and in the case $p = 2$, $\upsilon \geq 3$:

$$a_j = \begin{cases} (-1)^{\frac{m-j}{2}} A_{j+2}\left(\frac{m-j}{2}\right), & \text{if } j \text{ is even;} \\ 0, & \text{otherwise.} \end{cases}$$

Notice that, in our case, $\upsilon = 1$; thus, all coefficients are always non-zero. For example, when $p = 31$, we have that $n = 15$ and the defining polynomial $\Psi_p(x)$ is

$$\begin{aligned} \Psi_{31}(x) = x^{15} &+ x^{14} - 14x^{13} - 13x^{12} + 78x^{11} + 66x^{10} - 220x^9 - 165x^8 \\ &+ 330x^7 + 210x^6 - 252x^5 - 126x^4 + 84x^3 + 28x^2 - 8x - 1, \end{aligned}$$

which is very dense and the coefficients are not restricted to the set $\{0, 1\}$. However, depending on the choice of value for the coefficient's modulus q, the defining polynomial may have a complete factorization modulo q, which allows algorithms based on the Chinese Remainder Theorem (CRT) for efficient polynomial multiplication. For example, for $p = 31$ and $q = 61$, the defining polynomial factors in 15 distinct degree-one polynomials as follows:

$$\begin{aligned} \Psi_{31}(x) \bmod 61 = &(x+5)(x+6)(x+15)(x+16)(x+21)(x+22)(x+24)(x+27) \\ &(x+29)(x+36)(x+38)(x+41)(x+48)(x+49)(x+51). \end{aligned}$$

Thus, $f(x) = \Psi_{31}(x)$ can be factored as $f(x) = \prod_{i \in [k]} f_i(x) \pmod q$, where $f_i(x)$ are polynomials of small degree. The multiplication $a \cdot b$ modulo $f(x)$ is done by computing $a_i = a \mod f_i(x)$ and $b_i = b \mod f_i(x)$, for $i \in [k]$, computing the component-wise multiplication $(a_i b_i)$ and, finally, using the inverse operation to obtain the polynomial c such that $c \mod f_i(x) = a_i b_i \mod f_i(x)$, as discussed by Lyubashevsky and Seiler [18]. Although the asymptotic cost of an algorithm based on this technique is $O(n \log n)$, the hidden constants may be large due to the increased number of reductions modulo q in comparison with CRT-based algorithms for power-of-two cyclotomic number fields [18,10]. Another important aspect of the defining polynomial is captured by the *expansion factor*, a property introduced by Lyubashevsky and Micciancio [15]. The expansion factor of a polynomial f is

$$\mathrm{EF}(f,k) = \max_{g \in \mathbb{Z}[x], \deg(g) \le k(\deg(f)-1)} \|g\|_f / \|g\|_\infty,$$

where $\|g\|_f$ is the norm of the polynomial g after reduction modulo f. By computing the expansion factor of $\Psi_p(x)$, we can measure the increase in magnitude of the maximum coefficient of $\|g\|_{\Psi_p(x)}$. Also, the expansion factor helps us in choosing a value for q such that the coefficients do not wrap around after arithmetic operations, avoiding the occurrence of decryption errors.

In order to analyze the expansion factor of $\Psi_p(x)$, we compare it with $x^n + 1$, the defining polynomial of cyclotomic polynomial rings with dimension a power of two, which is widely adopted in practical applications. For that, we recall Lemma 4, which defines an upper bound for the magnitude of the coefficients of a polynomial $g \in \mathbb{Z}[x]$ after a reduction modulo f.

Lemma 4 *If g is a polynomial in $\mathbb{Z}[x]$ and f is a monic polynomial in $\mathbb{Z}[x]$ such that $\deg(g) \ge \deg(f)$, then $\|g\|_f \le \|g\|_\infty (2\|f\|_\infty)^{\deg(g)-\deg(f)+1}$.*

For the case $f(x) = \Psi_p(x)$, it is sufficient to analyze the value of $\|f\|_\infty$. Firstly, for $f(x) = x^n + 1$, we have that $\|f\|_\infty = 1$. On the other hand, when $f(x) = \Psi_p(x)$, $\|f\|_\infty$ assumes the maximum value of a_j according to Theorem 7. For example, for $p = 31$, $\|f\|_\infty = 330$, leading to an exponential growth of coefficients, which is roughly $330^{\deg(g)-\deg(f)+1}$ times bigger with respect to the case when $f(x) = x^{16}+1$. Such growth of coefficients require an increased value for the choice of the modulus q in order to avoid the coefficients to wrap around after polynomial operations. This also leads to an increase in the length of system parameters and memory/bandwidth requirement for transmission of public parameters.

In the positive direction, since the dimension of K does not increase as a power-of-two, one may want to find a ring instantiation that closely achieves a target security level. For example, to obtain a ring dimension between 700 and 800, the required for achieving 128-bit security [18], possible choices for the value of p ranges from the 223-th to the 252-th prime number, comprehending 29 possible choices.

In a nutshell, we have discussed some practical impacts of instantiating the Twisted Ring-LWE problem when K is the maximal real subfield of a cyclotomic number field, whose dimension is $n = (p-1)/2$ for any prime $p \ge 5$. The increased cost in arithmetic operations is inherent to this particular instantiation, but the same cannot be said about all algebraic constructions which lead to lattices equivalent to $\mathbb{Z}^n$. This is reinforced by the fact that the ring of integers of power-of-two cyclotomic number fields also leads to lattices equivalent to $\mathbb{Z}^n$ and, yet, it allows for very efficient algorithms for polynomial operations. Thus, it is an open question whether there are other number fields that realize lattices equivalent to $\mathbb{Z}^n$, having polynomial arithmetic that can be efficiently performed with tolerable or minor drawbacks.

References

1. Ajtai, M.: Generating Hard Instances of Lattice Problems (Extended Abstract). In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC

’96, pp. 99–108. ACM, New York, NY, USA (1996). DOI 10.1145/237814.237838. URL http://doi.acm.org/10.1145/237814.237838

2. Albrecht, M.R., Deo, A.: Large Modulus Ring-LWE $\geq$ Module-LWE. In: T. Takagi, T. Peyrin (eds.) Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I, *Lecture Notes in Computer Science*, vol. 10624, pp. 267–296. Springer (2017). DOI 10.1007/978-3-319-70694-8_10. URL https://doi.org/10.1007/978-3-319-70694-8_10
3. Andrade, A.A., Interlando, J.C.: Rotated $\mathbb{Z}^n$-Lattices via Real Subfields of $\mathbb{Q}(\zeta_{2^r})$. TEMA (São Carlos) **20**, 445 – 456 (2019). URL http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2179-84512019000300445&nrm=iso
4. Aranés, M., Arenas, A.: On the defining polynomials of maximal real cyclotomic extensions. Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas **101**(2), 187–203 (2008)
5. de Araujo, R.R., Jorge, G.C.: Constructions of full diversity D_n-lattices for all n. Rocky Mountain J. Math. **50**(4), 1137–1150 (2020). DOI 10.1216/rmj.2020.50.1137. URL https://doi.org/10.1216/rmj.2020.50.1137
6. Bayer-Fluckiger, E.: Lattices and Number Fields. Algebraic Geometry: Hirzebruch 70 **241** (1999)
7. Bayer-Fluckiger, E., Oggier, F., Viterbo, E.: New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel. IEEE Transactions on Information Theory **50**(4), 702–714 (2004). DOI 10.1109/TIT.2004.825045
8. Boutros, J., Viterbo, E., Rastello, C., Belfiore, J.C.: Good lattice constellations for both Rayleigh fading and Gaussian channels. IEEE Transactions on Information Theory **42**(2), 502–518 (1996). DOI 10.1109/18.485720
9. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) Fully Homomorphic Encryption without Bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ITCS ’12, p. 309–325. Association for Computing Machinery, New York, NY, USA (2012). DOI 10.1145/2090236.2090262. URL https://doi.org/10.1145/2090236.2090262
10. Chu, E., George, A.: Inside the FFT Black Box – Serial and Parallel Fast Fourier Transform Algorithms. CRC Press, Boca Raton, FL (2000)
11. Ducas, L., Durmus, A.: Ring-LWE in Polynomial Rings, pp. 34–51. Springer Berlin Heidelberg, Berlin, Heidelberg (2012). DOI 10.1007/978-3-642-30057-8_3
12. Jorge, G.C., Costa, S.I.: On rotated D_n-lattices constructed via totally real number fields. Archiv der Mathematik **100**(4), 323–332 (2013). DOI 10.1007/s00013-013-0501-8
13. Kirshanova, E., Nguyen, H., Stehlé, D., Wallet, A.: On the smoothing parameter and last minimum of random orthogonal lattices. Designs, Codes and Cryptography **88**, 931–950 (2020). DOI https://doi.org/10.1007/s10623-020-00719-w
14. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography **75**(3), 565–599 (2015). DOI 10.1007/s10623-014-9938-4. URL https://doi.org/10.1007/s10623-014-9938-4
15. Lyubashevsky, V., Micciancio, D.: Generalized Compact Knapsacks Are Collision Resistant. In: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (eds.) Automata, Languages and Programming, pp. 144–155. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
16. Lyubashevsky, V., Peikert, C., Regev, O.: On Ideal Lattices and Learning with Errors over Rings, pp. 1–23. Springer Berlin Heidelberg, Berlin, Heidelberg (2010). DOI 10.1007/978-3-642-13190-5_1
17. Lyubashevsky, V., Peikert, C., Regev, O.: A Toolkit for Ring-LWE Cryptography. Cryptology ePrint Archive, Report 2013/293 (2013). http://eprint.iacr.org/2013/293
18. Lyubashevsky, V., Seiler, G.: NTTRU: Truly Fast NTRU Using NTT. Cryptology ePrint Archive, Report 2019/040 (2019). https://eprint.iacr.org/2019/040
19. Micciancio, D., Regev, O.: Worst-Case to Average-Case Reductions Based on Gaussian Measures. SIAM J. Comput. **37**(1), 267–302 (2007). DOI 10.1137/S0097539705447360. URL https://doi.org/10.1137/S0097539705447360
20. NIST, N.: Post-Quantum Cryptography (2017). https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization
21. Oggier, F., Viterbo, E.: Algebraic Number Theory and Code Design for Rayleigh Fading Channels. Commun. Inf. Theory **1**(3), 333–416 (2004). DOI 10.1561/0100000003. URL http://dx.doi.org/10.1561/0100000003

22. Peikert, C.: Limits on the Hardness of Lattice Problems in ℓ_p Norms. Comput. Complex. **17**(2), 300–351 (2008). DOI 10.1007/s00037-008-0251-3. URL https://doi.org/10.1007/s00037-008-0251-3
23. Peikert, C.: A Decade of Lattice Cryptography. Found. Trends Theor. Comput. Sci. **10**(4), 283–424 (2016). DOI 10.1561/0400000074. URL http://dx.doi.org/10.1561/0400000074
24. Peikert, C., Pepin, Z.: Algebraically Structured LWE, Revisited. In: D. Hofheinz, A. Rosen (eds.) Theory of Cryptography, pp. 1–23. Springer International Publishing, Cham (2019)
25. Peikert, C., Regev, O., Stephens-Davidowitz, N.: Pseudorandomness of ring-LWE for Any Ring and Modulus. In: Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, pp. 461–473. ACM, New York, NY, USA (2017). DOI 10.1145/3055399.3055489
26. Regev, O.: On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In: Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing, STOC '05, pp. 84–93. ACM, New York, NY, USA (2005). DOI 10.1145/1060590.1060603
27. Ribenboim, P.: Classical Theory of Algebraic Numbers. Universitext. Springer-Verlag New York (2001). DOI 10.1007/978-0-387-21690-4
28. Samuel, P., Silberger, A.J.: Algebraic Theory of Numbers. Hermann, Paris (1970)
29. Stewart, I.N., Tall, D.O.: Algebraic Number Theory. Springer; 2nd edition (May 7, 1987) (1987)