






## Article

# The Ring-LWE Problem in Lattice-Based Cryptography: The Case of Twisted Embeddings

Jheyne N. Ortiz <sup>1,\*</sup>, Robson R. de Araujo <sup>2</sup>, Diego F. Aranha <sup>3</sup>, Sueli I. R. Costa <sup>4</sup> and Ricardo Dahab <sup>1</sup><sup>1</sup> Institute of Computing, University of Campinas, Campinas 13083-852, Brazil; rdahab@ic.unicamp.br<sup>2</sup> Federal Institute of São Paulo, Cubatão 11533-160, Brazil; robson.ricardo@ifsp.edu.br<sup>3</sup> Department of Computer Science, Aarhus University, N 8200 Aarhus, Denmark; dfaranha@cs.au.dk<sup>4</sup> Institute of Mathematics, Statistics and Computing Science, University of Campinas,

Campinas 13083-859, Brazil; sueli@ime.unicamp.br

\* Correspondence: jheyne.ortiz@ic.unicamp.br

**Abstract:** Several works have characterized weak instances of the Ring-LWE problem by exploring vulnerabilities arising from the use of algebraic structures. Although these weak instances are not addressed by worst-case hardness theorems, enabling other ring instantiations enlarges the scope of possible applications and favors the diversification of security assumptions. In this work, we extend 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. By doing so, we allow the Ring-LWE problem to be used over maximal real subfields of cyclotomic number fields. We prove that Twisted 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 twist factor 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. As a result, sampling from a spherical Gaussian distribution can be done directly in the respective number field while maintaining its format and standard deviation when seen in  $\mathbb{R}^n$  via twisted embeddings.

**Keywords:** lattice-based cryptography; twisted embeddings; ring learning with errors; spherical Gaussian sampling;  $\mathbb{Z}^n$ -equivalent lattices



**Citation:** Ortiz, J.N.; de Araujo, R.R.; Aranha, D.F.; Costa, S.I.R.; Dahab, R. The Ring-LWE Problem in Lattice-Based Cryptography: The Case of Twisted Embeddings. *Entropy* **2021**, *23*, 1108. <https://doi.org/10.3390/e23091108>

Academic Editor: Amin Sakzad and Khoa Nguyen

Received: 30 July 2021

Accepted: 21 August 2021

Published: 26 August 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 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) [1,2]. The main computational problem in the foundation of most modern lattice-based cryptosystems is Learning with Errors (LWE) [3]. Since its introduction in the cryptographic realm in 2005, algebraically structured variants have been proposed, such as Learning with Errors over Rings [4], denoted Ring-LWE, and Module-LWE [5–7], among others [8].

Although the Ring-LWE hardness results hold for any number field [4,9], its most used instantiation 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 [10]. This choice of a 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 [4].

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. 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, 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 [4,12].

There are several works in the literature exploring properties of number fields used in the foundation of some cryptosystems based on ideal lattices. An example is a quantum polynomial-time algorithm to find a small generator of a principal ideal in the ring of algebraic integers of cyclotomic rings [13], which applies to a few schemes including the fully-homomorphic encryption scheme of Smart and Vercauteren [14]. Moreover, a sequence of works has characterized weak instances of Ring-LWE and Poly-LWE problems and proposed attacks using special properties for specific parameters [15–24]. Another motivation for searching for alternative number fields is the inflexibility of system parameters that grow as a power-of-two. In such cryptosystems, when it is required to increase the security level, it may be necessary to increase the lattice dimension which implies doubling its size. However, a more suitable dimension could be a value much smaller than the next power of two. In fact, a ring dimension ranging from 700 to 800 suffices for 128-bit security [25].

Although these weak instances are not addressed by worst-case hardness theorems [26], new proposals adopting non-conventional rings have emerged as alternatives, thus favoring the diversification of security assumptions. For NTRU-based schemes, examples are the NTTTRU [27], the third-round NTRU submission [28] in the NIST Post-Quantum Cryptography contest [10], and NTRU Prime [29]. For Ring-LWE, the instantiations have been restricted to cyclotomic number fields. Lyubashevsky, Peikert, and Regev introduced a toolkit with techniques for secure implementation of Ring-LWE primitives over any cyclotomic number field [12], allowing applications to work on cyclotomic rings with non-power-of-two dimension. Later on, this toolkit was implemented in software in two distinct libraries [30,31]. An alternative instantiation could be the adoption of the polynomial ring  $\mathbb{Z}[x]/(x^p - x - 1)$  for  $p$  prime, which was proposed for NTRU Prime [29], and suggested for the Ring-LWE setting [32]. In this sense, we conjecture whether the Ring-LWE problem could be parameterized by number fields other than the cyclotomic for cryptographic applications.

### 1.1. Contributions

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*. Since the canonical embedding is a special case of twisted embeddings, this replacement maintains the consolidated results for Ring-LWE. 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 [33–35].

We extend the Ring-LWE problem by replacing the canonical embedding with twisted embeddings on both the search and decision variants. As a result, we obtain the *Twisted Ring-LWE* problem, in which the error terms are sampled in the space  $H$  isomorphic to  $\mathbb{R}^n$  under the inner product induced by a twisted embedding. We show that Twisted Ring-LWE is at least as secure as Ring-LWE through a security reduction from

Ring-LWE to Twisted Ring-LWE. We also recomputed the approximation factors in the worst-case to average-case reductions from hard lattice problems taking into account the new twist factor.

As a result, algebraic constructions from coding theory via twisted embeddings can also be used in cryptographic applications based on the Ring-LWE problem. In this work, we focused our attention on the algebraic construction of rotated  $\mathbb{Z}^n$ -lattices via twisted embeddings. Ducas and Durmus [11] showed that a spherical Gaussian distribution 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, corresponds to a distribution with the same format in the space  $H$ , but linearly wider in the ring dimension. This occurs because the lattice obtained from the ring  $\mathbb{Q}[x]/(\Theta_m(x))$  is a rotated  $\mathbb{Z}^n$ -lattice in the canonical embedding. The same holds for the ring of integers of a power-of-two cyclotomic number field. Thus, we generalize this result of Ducas and Durmus by showing that if the parameter ring leads to a rotated  $\mathbb{Z}^n$ -lattice under twisted embeddings, then both the format and the standard deviation of a spherical Gaussian distribution in  $K_{\mathbb{R}}$  is preserved when seen in  $H$ . Examples of ideal lattices equivalent to  $\mathbb{Z}^n$  are those obtained from power-of-two cyclotomic number fields [36], and their maximal real subfields [37], and the maximal real subfields of  $p$ -th cyclotomic number fields. Since power-of-two cyclotomic rings have been widely used in cryptographic applications, we consider parameterizing the Ring-LWE problem with the ring of integers of the maximal real subfield of a cyclotomic number field. We discuss the limitations of using maximal real subfields in a public-key encryption scheme [12] using the polynomial representation in terms of the arithmetic operations and the expansion factor of the defining polynomial. However, we argue that these limitations could be circumvented by using the coefficient vector representation, as done in [12]. Finally, we also argue that twisted embeddings can be used as a tool to connect Ring-LWE instances over distinct rings, which may lead to a response to the open question left by Peikert, Regev, and Stephens-Davidowitz [9]. In fact, if the parameter rings generate the same algebraic lattice in the space  $H$ , their Ring-LWE instances can be efficiently converted between themselves.

## 1.2. Organization

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. In particular, Section 2.4 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 3 introduces the twisted embeddings and 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 4 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. Section 4.1 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 [12], and also the format of the ring's defining polynomial in terms of the expansion factor. Finally, Section 5 discuss our results and highlight future research directions on the practical aspects of the Twisted Ring-LWE problem.

## 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  $\{1, 2, \dots, m\}$ . For  $1 \leq p < \infty$ , the  $\ell_p$ -norm of a vector  $\mathbf{a}$  in  $\mathbb{R}^n$  or  $\mathbb{C}^n$  is  $\|\mathbf{a}\|_p = (\sum_{i=1}^n |a_i|^p)^{1/p}$ , and the  $\ell_\infty$ -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 [4,9], 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

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

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

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

The norm (usually  $\ell_2$ -norm) of  $\mathbf{a} = (a_1, a_2, \dots, a_n) \in H$  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  $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n\}$  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  $\mathcal{B} = \{\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_n\}$  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  $\mathbf{a} = (a_1, a_2, \dots, a_n) \in H \subseteq \mathbb{C}^n$  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 ( $\ell_2$ -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  $\mathcal{B}(E) = \{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n\}$  of  $E$ .

A set  $\Lambda \subset E$  is said to be a *full-rank lattice* (or simply *lattice*), if  $\Lambda$  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  $\mathbf{B} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} \subset E$  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  $\Lambda$ . 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 *minimum distance* of a lattice  $\Lambda$  in the  $\ell_p$ -norm, denoted  $\lambda_1^{(p)}(\Lambda)$ , is the length of a shortest nonzero lattice vector, that is,  $\lambda_1^{(p)}(\Lambda) = \min_{\mathbf{0} \neq \mathbf{x} \in \Lambda} \|\mathbf{x}\|_p$ . Similarly, for any  $k \leq n$ , the  $k$ -th *successive minimum* of a lattice  $\Lambda$ , denoted  $\lambda_k^{(p)}(\Lambda)$ , is the smallest  $\hat{r} > 0$  such that  $\Lambda$  contains at least  $k$  linearly independent vectors of norm at most  $\hat{r}$ .

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  $\Lambda$ . Two basis generate the same lattice if and only if the associated generator matrices  $\mathbf{M}$  and  $\mathbf{M}'$  are related as  $\mathbf{M}' = \mathbf{M}\mathbf{U}$ , 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  $\Lambda$  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  $\Lambda$  and is denoted by  $\det(\Lambda)$ . Clearly,  $\det(\Lambda) = \det(\mathbf{M})^2$  does not depend of a particular basis of  $\Lambda$ .

The *dual lattice* of  $\Lambda$  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  $\Lambda$  has generator matrix  $\mathbf{M}$ , then  $(\mathbf{M}^t)^{-1}$  is a generator matrix for  $\Lambda^*$  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,  $\Lambda$  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  $\Lambda$  and  $\Lambda'$  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  $\Lambda$  and  $\Lambda'$ , 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  $\Lambda$  in  $(E, \langle \cdot, \cdot \rangle_E)$  is *orthogonal* if it has a basis  $\mathbf{B} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$  such that  $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0$  if  $i \neq j$ , for all  $i, j \in [n]$ . This means that  $\Lambda$  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  $\Lambda$  is equivalent to the  $\mathbb{Z}^n$ -lattice. In this case,  $\Lambda$  has a Gram matrix  $\mathbf{G} = c \mathbf{I}_n$ . In particular, when  $c = 1$ , we say that  $\Lambda$  is an *orthonormal* lattice.

### Gaussian Measures

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

$$\rho_{r,c}(\mathbf{a}) = \exp(-\pi \|\mathbf{a} - \mathbf{c}\|^2 / r^2). \tag{1}$$

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  $\mathbf{r} = (r_1, \dots, r_n) \in (\mathbb{R}^+)^n$  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  $\mathbb{R}$ .

The smoothing parameter is a lattice parameter defining the width beyond which a discrete Gaussian starts to behave similarly to a continuous distribution [38]. It is related to the minimum distance and the successive minimum of a lattice and it will be

used to derive the approximation factors in the worst-case to average-case reduction for the Twisted Ring-LWE problem. 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 3** (Smoothing parameter). For an  $n$ -dimensional lattice  $\Lambda$  and positive real  $\epsilon > 0$ , the smoothing parameter  $\eta_\epsilon(\Lambda)$  is the smallest  $r$  such that  $\rho_{1/r}(\Lambda^* \setminus \{\mathbf{0}\}) \leq \epsilon$ .

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

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

for all  $\mathbf{a} \in \Lambda$ .

### 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 [39,40].

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  $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ , with  $n = [K : \mathbb{Q}]$ , is a power basis of  $K$  over  $\mathbb{Q}$ . Also, if  $p(x)$  is the minimal polynomial of  $\theta$  over  $\mathbb{Q}$ , then  $K$  is isomorphic to  $\mathbb{Q}[x]/(p(x))$  and  $K = \mathbb{Q}(\theta')$  for some root  $\theta'$  of  $p(x)$ . The roots of  $p(x)$  are called the conjugates of  $\theta$ .

**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  $\zeta_m$ , 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). For  $m \not\equiv 2 \pmod{4}$ ,  $m > 1$ , 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  $\varphi(m)/2$ .

Let  $K$  be a number field. A map  $\bar{\cdot} : K \rightarrow K$  is called an involution of  $K$  if  $\overline{\overline{a+b}} = a+b$ ,  $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$ , and  $\overline{\overline{a}} = a$ , for all  $a, b \in K$ . If  $K = \mathbb{C}$ , the complex conjugation is an example of involution. If  $K = \mathbb{Q}(\zeta_m)$  is a cyclotomic number field, then  $\overline{\zeta_m} = \zeta_m^{-1}$  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  $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ , we consider the involution given by the identity map.

The subfield  $F = \{a \in K \mid \overline{a} = a\}$ , called the fixed field by 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  $K = \mathbb{Q}(\zeta_m)$ , the fixed field by the involution  $\overline{\zeta_m} = \zeta_m^{-1}$  of  $K$  is its maximal real subfield [36].

#### 2.3.1. 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  $\theta$ , these monomorphisms can be defined as  $\sigma_i(\theta) = \theta_i$  for  $i \in [n]$ , where  $\theta_i$  are all the distinct roots of  $p(x)$ .

A monomorphism  $\sigma_i : K \rightarrow \mathbb{C}$  is said to be *real* if  $\sigma_i(K) \subset \mathbb{R}$ . Otherwise, it is said to be *complex*. If  $\sigma_i$  is a complex monomorphism, then  $\bar{\sigma}_i$  is another complex monomorphism defined by  $\bar{\sigma}_i(a) = \overline{\sigma_i(a)}$ . 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 *canonical embedding* from  $K$  into the subspace  $H$  is the homomorphism

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

Its image is a lattice, used in the Ring-LWE problem [4,9].

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  $F$  [36].

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

The number field  $K$  is said to be a *Galois* number field if, for every  $x \in K$ , the minimal polynomial of  $x$  over  $\mathbb{Q}$  has all its roots in  $K$ . In this case, the set of automorphisms  $\sigma : K \rightarrow K$ , 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  $\text{Gal}(K/\mathbb{Q})$ . If  $K \subset \mathbb{C}$  is a Galois number field, then the monomorphisms from  $K$  to  $\mathbb{C}$  are exactly the elements of  $\text{Gal}(K/\mathbb{Q})$ . 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  $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$  is isomorphic to  $\mathbb{Z}_m^*$  and  $\text{Gal}(\mathbb{Q}(\zeta_m + \zeta_m^{-1})/\mathbb{Q})$  is isomorphic to  $\mathbb{Z}_m^*/\{\pm 1\}$ .

### 2.3.2. Ring of Integers and Its Ideals

Let  $K$  be a Galois number field. For every  $a \in K$ , the *trace* and *norm* of any element  $a \in K$  can be defined, respectively, as

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

For all  $a \in K$ ,  $\text{Tr}_K(a)$  and  $\text{N}_K(a)$  are elements of  $\mathbb{Q}$ .

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  $\text{Tr}_K(a)$  and  $\text{N}_K(a)$  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  $\zeta_m$ . 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  $\mathcal{D}_K^{-1} = \{a \in K : \text{Tr}_K(a\mathcal{O}_K) \subset \mathbb{Z}\}$  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  $\theta$  [41] (Section 13.2, J). The inverse ideal

of the codifferent, 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

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

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  $N(\mathcal{I}) = |N_K(a)|$ .

#### 2.4. The Ring-LWE Problem

In the following definitions, a lattice  $\Lambda$  is usually represented by a basis  $\mathbf{B}$  and, in the context of algebraic lattices,  $\Lambda$  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  $K$  [4].

**Definition 4** (GapSVP $_\gamma$ ). For an approximation factor  $\gamma = \gamma(n) \geq 1$ , the GapSVP $_\gamma$  is: given a lattice  $\Lambda$  and length  $d > 0$ , output YES if  $\lambda_1(\Lambda) \leq d$  and NO if  $\lambda_1(\Lambda) > \gamma d$ .

**Definition 5** (SIVP $_\gamma$ ). For an approximation factor  $\gamma = \gamma(n) \geq 1$ , the SIVP $_\gamma$  is: given a lattice  $\Lambda$ , output  $n$  linearly independent lattice vectors of length at most  $\gamma(n) \cdot \lambda_n(\Lambda)$ .

By seeing a fractional ideal  $\mathcal{I}$  of an arbitrary number field  $K$  as a lattice using the canonical embedding, let  $D_{\mathcal{I},r}$  denote the discrete Gaussian distribution of width  $r$  over  $\mathcal{I}$  in the field tensor product  $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ , which is isomorphic to the space  $H$ .

**Definition 6** ( $K$ -DGS $_\gamma$ ). For a function  $\gamma$  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  $\Lambda$  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  $\mathcal{I}_q = \mathcal{I} / q\mathcal{I}$ .

**Definition 7** ([4] Ring-LWE distribution). For  $s \in R_q^\vee$  (the “secret”) and an error distribution  $\psi$  over  $K_{\mathbb{R}}$ , 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  $(a, b = (a \cdot s) / q + e \pmod{R^\vee})$ .

**Definition 8** ([4] Ring-LWE, search). Let  $\Psi$  be a family of distributions over  $K_{\mathbb{R}}$ . 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 9** ([4,9] Ring-LWE, average-case decision). Let  $\mathcal{Y}$  be a distribution over a family of error distributions, each over  $K_{\mathbb{R}}$ . The average-case Ring-LWE decision problem, denoted  $R$ -LWE $_{q,\mathcal{Y}}$ , is to distinguish (with non-negligible advantage) between independent samples from  $\mathcal{A}_{s,\psi}$



for a random choice of  $(s, \psi) \leftarrow U(R_q^V) \times Y$ , and the same number of uniformly random and independent samples from  $R_q \times \mathbb{T}$ .

### 3. The Twisted Ring-LWE

Firstly, we collect important results on algebraic lattices obtained through twisted embeddings. Then, we present the class of problems Twisted Ring-LWE, which is the main contribution of this work. The hardness of Twisted Ring-LWE is demonstrated by security reductions from the original Ring-LWE problem. Also, we recompute the approximation factors in the worst-case to average reduction from the SIVP problem, considering the twist factor defining the twisted embedding.

#### 3.1. Twisted Embeddings

In this section consider the following setting. Let  $K$  be an algebraic number field with degree  $n$ , signature  $(s_1, s_2)$ , and  $\bar{\cdot}$  a fixed involution. Consider  $F$  to be the fixed field by the involution of  $K$ . Let  $\sigma_i$  be the real monomorphisms for  $i \in [s_1]$ , and  $\sigma_{i+s_1}$  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  $i \in [s_2]$ . The twisted embeddings defined next are a generalization of the canonical embedding [36]. 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 10** (Twisted embeddings). *For any totally positive  $\tau \in F$ , the  $\tau$ -twisted embedding (or simply twisted embedding) is the homomorphism  $\sigma_\tau : K \rightarrow H$ , defined as*

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

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 [36].

**Proposition 1** ([36]). *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  $H$ .*

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  $\text{Tr}_K : K \rightarrow \mathbb{Q}$  to  $\text{Tr}_K : K_{\mathbb{R}} \rightarrow \mathbb{R}$ . For any totally positive  $\tau \in F$ , we can define an inner product in  $K_{\mathbb{R}}$  as

$$\langle a, b \rangle_\tau := \langle \sigma_\tau(a), \sigma_\tau(b) \rangle_H = \text{Tr}_K(\tau a \bar{b}), \quad a, b \in K_{\mathbb{R}}. \tag{2}$$

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  $\ell_p$ -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  $\ell_p$ -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  $\ell_\infty$ -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

$$\|a \cdot b\|_{p,\tau} \leq \|a\|_\infty \|b\|_{p,\tau} \quad \text{and} \quad \|a \cdot b\|_{p,\tau} \leq \|a\|_p \|b\|_{\infty,\tau}. \tag{3}$$

Notice that, 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  $a \cdot D_\tau$  is  $D_{r'}$ , 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  $\sigma_\tau$  [11].

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  $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$  of the free  $\mathbb{Z}$ -module  $M$  of rank  $n$  in  $K$ , the matrix  $[(v_i, v_j)_\tau]_{n \times n}$  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  $\{\sigma_\tau(v_1), \sigma_\tau(v_2), \dots, \sigma_\tau(v_n)\}$ . 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 two. 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  $M_\tau$  and the Gram matrix of the lattice  $M_\tau$  is given by

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

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  $\pm 1$ , 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  $\langle a, b \rangle_\tau = \text{Tr}_K(\tau a \bar{b})$ , 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  $\tau\overline{\mathcal{I}} = \mathcal{D}_K^{-1}$ .

**Proof.** By definition,  $a \in \mathcal{I}^*$  if and only if  $\text{Tr}_K(\tau a \overline{\mathcal{I}}) \subset \mathbb{Z}$ , 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  $\tau\overline{\mathcal{I}}^{-1} \subset \mathcal{D}_K^{-1}$ . 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  $\tau\overline{\mathcal{I}} = \mathcal{D}_K^{-1}$ . Therefore,  $\mathcal{I}$  is unimodular if and only if  $\tau\overline{\mathcal{I}} = \mathcal{D}_K^{-1}$ .  $\square$

### 3.2. The Twisted Ring-LWE Problem

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  $\text{Ring-LWE}^\tau$ . We also prove that solving the Twisted Ring-LWE problem is at least as hard as solving the original Ring-LWE problem [4], 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  $\psi$  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  $\psi$  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  $\sigma_\tau$  the twisted embedding. The error  $e$  is randomized by a distribution  $\psi$  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  $\psi_\tau$  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*

$$(a, b = a \cdot s + e \pmod{qR^\vee}) \in R_q \times K_{\mathbb{R}}/qR^\vee, \tag{6}$$

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

Analogously to Ring-LWE [4], 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. [4] and the decision problem which was further defined by Peikert et al. [9].

**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  $\mathcal{A}_{s, \psi_\tau}$  for some arbitrary  $s \in R_q^\vee$  and  $\psi_\tau \in \Psi^{(\tau)}$ , find  $s$ .*

**Definition 14.** Fix an arbitrary  $f(n) = \omega(\sqrt{\log n})$ . For  $\alpha > 0$ , a distribution sampled from  $Y_\alpha^{(\tau)}$  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  $i = s_1 + 1, \dots, s_1 + s_2$ , 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  $i = s_1 + 1, \dots, s_1 + s_2$  is done according to the Gaussian function given in Equation (1), using the norm induced by the corresponding twisted embedding.

**Definition 15 (Ring-LWE $^\tau$ , average-case decision).** Let  $Y^{(\tau)}$  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  $(s, \psi_\tau) \leftarrow U(R_q^\vee) \times Y^{(\tau)}$ , and the same number of uniformly random and independent samples from  $R_q \times K_{\mathbb{R}}/R_q^\vee$ .

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  $\tau = 1$ .

### 3.3. 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  $(s, \psi)$  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 $_{q, \psi_\tau}^\tau$ .

**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

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

where  $e_i \stackrel{\psi}{\leftarrow} K_{\mathbb{R}}$ . Thus, we use the fact that  $e_i = \sigma^{-1}(\tilde{e}_i)$ , for some  $\tilde{e}_i$  obtained from the Gaussian distribution  $\psi$  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

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

By applying the inverse transformation  $\sigma_\tau^{-1}$ , we obtain that

$$\left\{ \left( \sigma_\tau^{-1}(\sigma(a_i)), \sigma_\tau^{-1}(\sigma(b_i)) \right) \right\} = \left\{ \left( \sigma_\tau^{-1}(\sigma(a_i)), \sigma_\tau^{-1}(\sigma(a_i)) \cdot s + \sigma_\tau^{-1}(\tilde{e}_i) \right) \right\}. \tag{7}$$

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  $\sigma$  and  $\sigma_\tau^{-1}$  transformations are injective,  $\sigma_\tau^{-1}(\sigma(a_i))$  is also uniform in  $R_q$ . And, finally, since

$e'_i = \sigma_\tau^{-1}(\tilde{e}_i)$  is randomized by  $\psi_\tau$  in  $(K_{\mathbb{R}}, \langle \cdot, \cdot \rangle_\tau)$ , the set of samples in (7) follows the distribution  $\mathcal{A}_{s, \psi_\tau}$ . Given the set of samples (7) 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  $\sigma$  and  $\sigma_\tau^{-1}$  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.  $\square$

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

**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  $\sigma$  and  $\sigma_\tau^{-1}$ , 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  $\sigma$  and  $\sigma_\tau^{-1}$  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  $\sigma$  and  $\sigma_\tau^{-1}$  costs  $O(n^2)$  operations; thus, the reduction runs in polynomial time. This concludes the proof.  $\square$

### 3.4. 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, we analyze the effect of redefining the inner product in the Ring-LWE security reductions.

By strictly following the setting of Lyubashevsky et al. [4], we start by deriving upper bounds for the smoothing parameter concerning the  $\ell_p$ -norm under twisted embeddings. From the inequalities in (3), we are able to relate the  $\ell_p$ -norm 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  $\ell_p$ -norms under both embeddings in  $H$  as

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

Using the above inequalities, 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 [42]. Notice that, when  $\tau = 1$ , these upper bounds are exactly the same as presented in [42]. Consider that  $\lambda_n^{(p, \tau)}(\Lambda)$  and  $\lambda_1^{(p, \tau)}(\Lambda)$  denotes the  $k$ -th successive minimum and the minimum distance of a lattice  $\Lambda$  in the  $\ell_p$ -norm, respectively, under a  $\tau$ -twisted embedding.

**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  $\Lambda$  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  $\Lambda$  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

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

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** ([4] (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** ([3] (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  $DGS_{\varphi}$ .

Thus, we use the inequalities for the smoothing parameter  $\eta_{\epsilon}$  derived in Lemmas 1 and 2 to recompute the approximation factors in Theorem 3 and Lemma 3. We start by computing the approximated factor  $\gamma$  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  $\varphi$  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  $\varphi$ , we define the upper bound for the GIVP parameter to be  $\mu$ , 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  $\ell_p$ -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 [4] (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.

#### 4. 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  $\Phi_m$  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  $\beta$  represent the polynomial reduction from  $\mathbb{Q}[x]/(\Theta_m(x))$  to  $\mathbb{Q}[x]/(\Phi_m(x))$ , and let the linear operator  $\mathbf{T} : H \rightarrow H$  with matrix in the canonical basis of  $H$  be:

$$\mathbf{T} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{Id}_{\phi(m)/2} & i \mathbf{Id}_{\phi(m)/2} \\ \mathbf{Id}_{\phi(m)/2} & -i \mathbf{Id}_{\phi(m)/2} \end{pmatrix}, \quad \text{with } i = \sqrt{-1}. \tag{8}$$

**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  $\gamma$  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 [36].

**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  $\sigma_{\tau}$ ).*

**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  $\sigma_{\tau} : K_{\mathbb{R}} \rightarrow H$  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 (8) 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.  $\square$

Examples of ideal lattices equivalent to  $\mathbb{Z}^n$  are those obtained from cyclotomic number fields  $\mathbb{Q}(\zeta_{2^k})$  [36], and their maximal real subfields [37], and the maximal real subfields  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$  for any prime  $p \geq 5$  [43]. The case of the power-of-two cyclotomic number fields were previously addressed by Lyubashevsky et al. [4], 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** ([44] (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  $\mathcal{C}' = \{e'_1, \dots, e'_n \mid e'_n = e_n \text{ and } e'_j = e_j + e'_{j+1}\}$ , where  $\mathcal{C} = \{e_1, \dots, e_n\}$  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

$$\mathbf{M} = \mathbf{D} \mathbf{M}' \mathbf{U}, \tag{9}$$



where  $\mathbf{D} = \text{diag} \left[ \sqrt{\frac{\sigma_K(\tau)}{p}} \right]_{n \times n}$ ,  $\mathbf{M}' = [\sigma_i(\zeta^j + \zeta^{-j})]_{i,j \in [n] \times [n]}$  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  $\psi_s^n$  in the basis  $C'$ . 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  $\psi_s^n$ .*

**Proof.** In the realization of the  $\mathbb{Z}^n$ -lattice (Proposition 3), the matrix representing the linear map  $\sigma_\tau$  from the basis  $C'$  of  $\mathcal{O}_K$  to the canonical basis of  $\mathbb{R}^n$  is given by  $\mathbf{M}$  (9). Since  $\mathcal{O}_K$  is a lattice equivalent to  $\mathbb{Z}^n$  in the basis  $C'$ , the result follows immediately from Theorem 5. This concludes the proof.  $\square$

#### 4.1. Practical Impacts on a Public-Key Cryptosystem

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 [12] (Section 8.2).

The public-key cryptosystem presented below is parameterized by an  $m$ -th 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  $\psi_\tau$  is an error distribution over  $(K_{\mathbb{R}}, \langle \cdot, \cdot \rangle_\tau)$  and  $\lfloor \cdot \rfloor$  denotes a valid discretization to (cosets) of  $R^\vee$  or  $p'R^\vee$ . Also,  $\hat{m} = m/2$  if  $m$  is even, otherwise  $\hat{m} = m$ . Finally, for any  $\bar{a} \in \mathbb{Z}_q$ , let  $\llbracket \bar{a} \rrbracket$  denote the unique representative  $a \in (\bar{a} + q\mathbb{Z}) \cap [-q/2, q/2)$ , which is entry-wise extended to polynomials.

- **Gen:** choose a uniformly random  $a \in R_q$ . Choose  $x \leftarrow \lfloor \psi_\tau \rfloor_{R^\vee}$  and  $e \leftarrow \lfloor p' \cdot \psi_\tau \rfloor_{p'R^\vee}$ . Output  $(a, b = \hat{m}(a \cdot x + e) \bmod qR) \in R_q \times R_q$  as the public key, and  $x$  as the secret key.
- **Enc<sub>(a,b)</sub>**( $\mu \in R_{p'}$ ): choose  $z \leftarrow \lfloor \psi_\tau \rfloor_{R^\vee}$ ,  $e' \leftarrow \lfloor p' \cdot \psi_\tau \rfloor_{p'R^\vee}$ , and  $e'' \leftarrow \lfloor p' \cdot \psi_\tau \rfloor_{t^{-1}\mu + p'R^\vee}$ . Let  $u = \hat{m}(a \cdot z + e') \bmod qR$  and  $v = z \cdot b + e'' \in R_q^\vee$ . Output  $(u, v) \in R_q \times R_q^\vee$ .
- **Dec<sub>x</sub>**( $u, v$ ): compute  $v - u \cdot x \bmod qR^\vee$ , and decode it to  $d = \llbracket v - u \cdot x \rrbracket \in R^\vee$ . Output  $\mu = t \cdot d \bmod p'R$ .

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  $C'$  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  $\mathcal{C}'$ , the basis used for error sampling, to the power basis  $\{(\zeta_p + \zeta_p^{-1})^j \mid 0 \leq j < n\}$ . 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 [45].

**Theorem 6** ([45] (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** ([45] (Theorem 2)). *The coefficients  $a_j$  of the polynomial  $\Psi_{p^v}(x)$  are given by the following formulae. If  $p$  is odd,*

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

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

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

Notice that, in our case,  $v = 1$ ; 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:

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

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  $a_i = a \pmod{f_i(x)}$  and  $b_i = b \pmod{f_i(x)}$ , 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  $c \pmod{f_i(x)} = a_i b_i \pmod{f_i(x)}$ , as discussed by Lyubashevsky and Seiler [27]. 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 [27,46]. Another important aspect of the defining polynomial is captured by the *expansion factor*, a property introduced by Lyubashevsky and Micciancio [47]. The expansion factor of a polynomial  $f$  is

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

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  $\deg(g) \geq \deg(f)$ , then  $\|g\|_f \leq \|g\|_\infty (2\|f\|_\infty)^{\deg(g) - \deg(f) + 1}$ .*

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 [27], 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  $p \geq 5$ . The increased cost in arithmetic operations is inherent to this particular instantiation and field representation, 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 arithmetic operations in the power basis representation. Thus, in Section 5, we briefly discuss on an alternative field representation when  $K$  is the maximal real subfield of a cyclotomic number field. Moreover, we present future research possibilities related to the Twisted Ring-LWE problem.

## 5. Discussion

In this paper, we introduce an extension to the Ring-LWE class of problems, namely The Twisted Ring-LWE Problem [4,9]. The Ring-LWE problem uses the canonical embedding to map some underlying ring to a lattice in  $\mathbb{R}^n$ . By doing so, we can define geometric norms and error distributions on the tensor field  $K_{\mathbb{R}}$ , which is isomorphic to  $\mathbb{R}^n$ . The Twisted Ring-LWE problem is obtained by adopting twisted embeddings [36] rather than the canonical embedding, which is a specialization of twisted embeddings. We prove that the Twisted Ring-LWE Problem is as secure as the original Ring-LWE Problem by providing a security reduction from both variants of Ring-LWE to their twisted forms.

As a result, we broaden the scope of number of algebraic lattices that can be used for lattice-based cryptosystems, including those algebraic constructions of lattices that allow additional factors on the embedding coordinates. This type of construction has 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 [33–35]. Notice that these constructions cannot be obtained via canonical embedding. We took as an example the construction of rotated  $\mathbb{Z}^n$ -lattices. We prove that we can perform efficient and secure sampling from spherical Gaussian distributions in  $K_{\mathbb{R}}$ , if the parameter ring leads to a rotated  $\mathbb{Z}^n$ -lattice in the space  $H$  via twisted embeddings. This generalizes the results of Ducas and Durmus in Theorem 5 [11] and the power-of-two cyclotomic case.

An example of a construction of the  $\mathbb{Z}^n$ -lattice via twisted embeddings is from maximal real subfields of both power-of-two and  $p$ -th cyclotomic number fields. We analyze instantiating the Ring-LWE problem using maximal real subfields of  $p$ -th cyclotomic number fields in a public-key encryption scheme [12]. By doing so, we can instantiate the Ring-LWE problem in a dimension close to 700 to achieve 128-bit security [25] and provide variability of security assumptions, avoiding the use of the widely adopted power-of-two cyclotomic number field. However, representing the field elements as residue polynomials modulo the defining polynomial is of limited interest, since the coefficients' modulus may become very large to avoid the occurrence of decryption errors. This occurs because the expansion factor of the defining polynomial of maximal real subfields of  $p$ -th cyclotomic number fields grows exponentially.

### *Future Work*

Lyubashevsky, Peikert, and Regev [12] suggested representing the field elements as coefficient vectors in an integral basis apart from the power basis. By taking the underlying ring as the ring of integers of the maximal real subfield of a cyclotomic number field on an orthonormal basis, we can perform efficient Gaussian sampling with hardness guarantee, as discussed in Section 4. Moreover, we can perform efficient ring arithmetic by taking the ring representatives under the twisted embedding, in which both addition and multiplication are taken component-wise. Although the change of representation may need floating-point arithmetic, one may explore lattice basis symmetries to accelerate the computation of the twisted embedding or find a basis more suitable for arithmetic operations. In addition to that, all algorithmic tasks can be performed directly in the space  $H$ , without resorting to change of representation from  $K_{\mathbb{R}}$ . We leave as future work a full analysis and the software implementation of the instantiation of the Twisted Ring-LWE Problem in a cryptosystem adopting the coefficient vector representation.

We also leave as future work detailing how to connect Twisted Ring-LWE instantiations over different number fields, if the ring of integers of both number fields leads to equivalent lattices under twisted embeddings. By doing so, we can connect an instance on a power-of-two cyclotomic number field to an instance of a maximal real subfield as both rings of integers lead to a construction of the  $\mathbb{Z}^n$ -lattice. This may lead to a response to the open question left by Peikert, Regev, and Stephens-Davidowitz [9]. As a consequence, we may be able to explore algebraic properties inherent to maximal real subfields helping to assert the concrete hardness of power-of-two cyclotomic number fields.

**Author Contributions:** All authors contributed to the study conception and design. The first draft of the manuscript was written by J.N.O. and R.R.d.A. and all authors contributed to all versions of the manuscript. All authors have read and agreed to the published version of the manuscript.

**Funding:** The authors were supported in part by the Brazilian Coordination for the Improvement of Higher Education Personnel Foundation (CAPES) grant numbers 1591123 and 1540410, the Brazilian National Council for Scientific and Technological Development (CNPq) grant numbers 164489/2018-5 and 313326/2017-7, and the São Paulo Research Foundation (FAPESP) grant number 2013/25977-7. The authors acknowledge the support from the DIGIT Centre for Digitalisation, Big Data and Data Analytics; and the Concordium Blockchain Research Center at Aarhus University.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Ajtai, M. Generating Hard Instances of Lattice Problems (Extended Abstract). In Proceedings of the STOC '96, Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; ACM: New York, NY, USA, 1996; pp. 99–108. [CrossRef]
2. Peikert, C. A Decade of Lattice Cryptography. *Found. Trends Theor. Comput. Sci.* **2016**, *10*, 283–424. [CrossRef]
3. Regev, O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In Proceedings of the STOC '05, Thirty-Seventh Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, 22–24 May 2005; ACM: New York, NY, USA, 2005; pp. 84–93. [CrossRef]
4. Lyubashevsky, V.; Peikert, C.; Regev, O. On Ideal Lattices and Learning with Errors over Rings. In *Advances in Cryptology—Proceedings of the EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, 30 May–3 June 2010*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 1–23. [CrossRef]
5. Brakerski, Z.; Gentry, C.; Vaikuntanathan, V. (Leveled) Fully Homomorphic Encryption without Bootstrapping. In Proceedings of the ITCSC '12, 3rd Innovations in Theoretical Computer Science Conference, Cambridge, MA, USA, 8–10 January 2012; Association for Computing Machinery: New York, NY, USA, 2012; pp. 309–325. [CrossRef]
6. Langlois, A.; Stehlé, D. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.* **2015**, *75*, 565–599. [CrossRef]
7. Albrecht, M.R.; Deo, A. Large Modulus Ring-LWE  $\geq$  Module-LWE. In *Advances in Cryptology—ASIACRYPT 2017—23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017*; Takagi, T., Peyrin, T., Eds.; Proceedings Part I Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10624, pp. 267–296. [CrossRef]
8. Peikert, C.; Pepin, Z. Algebraically Structured LWE, Revisited. In *Theory of Cryptography*; Hofheinz, D., Rosen, A., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 1–23.
9. Peikert, C.; Regev, O.; Stephens-Davidowitz, N. Pseudorandomness of ring-LWE for Any Ring and Modulus. In Proceedings of the STOC 2017, 49th Annual ACM SIGACT Symposium on Theory of Computing, Montreal, QC, Canada, 19–23 June 2017; ACM: New York, NY, USA, 2017; pp. 461–473. [CrossRef]
10. National Institute of Standards and Technology. Post-Quantum Cryptography. 2017. Available online: <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization> (accessed on 30 July 2021).
11. Ducas, L.; Durmus, A., Ring-LWE in Polynomial Rings. In *Public Key Cryptography, Proceedings of the PKC 2012: 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, 21–23 May 2012*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 34–51. [CrossRef]
12. Lyubashevsky, V.; Peikert, C.; Regev, O. A Toolkit for Ring-LWE Cryptography. Cryptology ePrint Archive, Report 2013/293. 2013. Available online: <http://eprint.iacr.org/2013/293> (accessed on 30 July 2021).
13. Campbell, P.; Groves, M.; Shepherd, D. SOLILOQUY: A Cautionary Tale. *ETSI 2nd Quantum-Safe Crypto Workshop*. 2014; pp. 1–9. Available online: [http://docbox.etsi.org/Workshop/2014/201410\\_CRYPTOS07\\_Systems\\_and\\_Attacks/S07\\_Groves\\_Annex.pdf](http://docbox.etsi.org/Workshop/2014/201410_CRYPTOS07_Systems_and_Attacks/S07_Groves_Annex.pdf) (accessed on 30 July 2021).
14. Smart, N.P.; Vercauteren, F. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In *Public Key Cryptography, Proceedings of the PKC 2010: 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, 26–28 May 2010*; Nguyen, P.Q., Pointcheval, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 420–443. [CrossRef]
15. Eisenträger, K.; Hallgren, S.; Lauter, K. Weak Instances of PLWE. In *Selected Areas in Cryptography, Proceedings of the SAC 2014: 21st International Conference, Montreal, QC, Canada, 14–15 August 2014*; Joux, A., Youssef, A., Eds.; Revised Selected Papers; Springer International Publishing: Cham, Switzerland, 2014; pp. 183–194.
16. Elias, Y.; Lauter, K.E.; Ozman, E.; Stange, K.E. Provably Weak Instances of Ring-LWE. In *Advances in Cryptology, Proceedings of the CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015*; Gennaro, R., Robshaw, M., Eds.; Proceedings, Part I; Springer: Berlin/Heidelberg, Germany, 2015; pp. 63–92. [CrossRef]

17. Chen, H.; Lauter, K.E.; Stange, K.E. Attacks on the Search-RLWE Problem with Small Error. Cryptology ePrint Archive, Report 2015/971. 2015. Available online: <https://eprint.iacr.org/2015/971> (accessed on 30 July 2021).
18. Castryck, W.; Iliashenko, I.; Vercauteren, F. Provably Weak Instances of Ring-LWE Revisited. In Proceedings of the 35th Annual International Conference on Advances in Cryptology—EUROCRYPT 2016, Vienna, Austria, 8–12 May 2016; Springer: New York, NY, USA, 2016; Volume 9665; pp. 147–167. [CrossRef]
19. Castryck, W.; Iliashenko, I.; Vercauteren, F. On error distributions in ring-based LWE. *LMS J. Comput. Math.* **2016**, *19*, 130–145. [CrossRef]
20. Chen, H.; Lauter, K.; Stange, K.E. Security Considerations for Galois Non-dual RLWE Families. In *Selected Areas in Cryptography, Proceedings of the SAC 2016, Pisa, Italy, 4–8 April 2016*; Avanzi, R., Heys, H., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 443–462.
21. Chen, H. Solving Ring-LWE over Algebraic Integer Rings. Cryptology ePrint Archive, Report 2019/791. 2019. Available online: <https://ia.cr/2019/791> (accessed on 30 July 2021).
22. Chen, H. Subset Attacks on Ring-LWE with Wide Error Distributions I. Cryptology ePrint Archive, Report 2020/440. 2020. Available online: <https://ia.cr/2020/440> (accessed on 30 July 2021).
23. Chen, H. Ring-LWE over Two-to-Power Cyclotomics Is Not Hard. Cryptology ePrint Archive, Report 2021/418. 2021. Available online: <https://ia.cr/2021/418> (accessed on 30 July 2021).
24. Stange, K.E. Algebraic Aspects of Solving Ring-LWE, including Ring-Based Improvements in the Blum-Kalai-Wasserman algorithm. Cryptology ePrint Archive, Report 2019/183. 2019. Available online: <https://ia.cr/2019/183> (accessed on 30 July 2021).
25. Albrecht, M.R.; Curtis, B.R.; Deo, A.; Davidson, A.; Player, R.; Postlethwaite, E.W.; Virdia, F.; Wunderer, T. Estimate all the LWE, NTRU Schemes! Cryptology ePrint Archive, Report 2018/331. 2018. Available online: <https://eprint.iacr.org/2018/331> (accessed on 30 July 2021).
26. Peikert, C. How (Not) to Instantiate Ring-LWE. In *Security and Cryptography for Networks: 10th International Conference, SCN 2016, Amalfi, Italy, 31 August–2 September 2016*; Zikas, V., De Prisco, R., Eds.; Springer International Publishing: Cham, Switzerland, 2016; pp. 411–430. [CrossRef]
27. Lyubashevsky, V.; Seiler, G. NTTRU: Truly Fast NTRU Using NTT. Cryptology ePrint Archive, Report 2019/040. 2019. Available online: <https://eprint.iacr.org/2019/040> (accessed on 30 July 2021).
28. Chen, C.; Danba, O.; Hoffstein, J.; Hülsing, A.; Rijneveld, J.; Schanck, J.M.; Saito, T.; Schwabe, P.; Whyte, W.; Xagawa, K.; et al NTRU Algorithm Specifications And Supporting Documentation. Submission to the NIST Post-Quantum Cryptography Standardization Project. 2020. Available online: <https://ntru.org/resources.shtml> (accessed on 30 July 2021).
29. Bernstein, D.J.; Chuengsatiansup, C.; Lange, T.; van Vredendaal, C. NTRU Prime: Reducing Attack Surface at Low Cost. Cryptology ePrint Archive, Report 2016/461. 2016. Available online: <http://eprint.iacr.org/2016/461> (accessed on 30 July 2021).
30. Mayer, C.M. Implementing a Toolkit for Ring-LWE Based Cryptography in Arbitrary Cyclotomic Number Fields. Cryptology ePrint Archive, Report 2016/049, 2016. Available online: <http://eprint.iacr.org/2016/049> (accessed on 30 July 2021).
31. Crockett, E.; Peikert, C.  $\Lambda\sigma\lambda$ : Functional Lattice Cryptography. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; Weippl, E.R., Katzenbeisser, S., Kruegel, C., Myers, A.C., Halevi, S., Eds.; ACM: New York, NY, USA, 2016; pp. 993–1005. [CrossRef]
32. Peikert, C.; Regev, O.; Stephens-Davidowitz, N. Pseudorandomness of Ring-LWE for Any Ring and Modulus (Slides), 2017. Available online: <https://web.eecs.umich.edu/~cpeikert/pubs/slides-anyring.pdf> (accessed on 30 July 2021).
33. Boutros, J.; Viterbo, E.; Rastello, C.; Belfiore, J.C. Good lattice constellations for both Rayleigh fading and Gaussian channels. *IEEE Trans. Inf. Theory* **1996**, *42*, 502–518. [CrossRef]
34. Jorge, G.C.; Costa, S.I. On rotated  $D_n$ -lattices constructed via totally real number fields. *Arch. Der Math.* **2013**, *100*, 323–332. [CrossRef]
35. de Araujo, R.R.; Jorge, G.C. Constructions of full diversity  $D_n$ -lattices for all  $n$ . *Rocky Mt. J. Math.* **2020**, *50*, 1137–1150. [CrossRef]
36. Bayer-Fluckiger, E. Lattices and Number Fields. In *Contemporary Mathematics*; American Mathematical Society: Providence, RI, USA, 1999; Volume 241.
37. Andrade, A.A.; Interlando, J.C. Rotated  $\mathbb{Z}^n$ -Lattices via Real Subfields of  $\mathbb{Q}(\zeta_{2^r})$ . *TEMA (São Carlos)* **2019**, *20*, 445–456. [CrossRef]
38. Micciancio, D.; Regev, O. Worst-Case to Average-Case Reductions Based on Gaussian Measures. *SIAM J. Comput.* **2007**, *37*, 267–302. [CrossRef]
39. Samuel, P.; Silberberger, A.J. *Algebraic Theory of Numbers*; Hermann: Paris, France, 1970.
40. Stewart, I.N.; Tall, D.O. *Algebraic Number Theory and Fermat's Last Theorem: Third Edition*, 3rd ed.; A K Peters/CRC Press: New York, NY, USA, 2001. [CrossRef]
41. Ribenboim, P. *Classical Theory of Algebraic Numbers*; Universitext, Springer: New York, NY, USA, 2001. [CrossRef]
42. Peikert, C. Limits on the Hardness of Lattice Problems in  $\ell_p$  Norms. *Comput. Complex.* **2008**, *17*, 300–351. [CrossRef]
43. Bayer-Fluckiger, E.; Oggier, F.; Viterbo, E. New algebraic constructions of rotated  $\mathbb{Z}^n$ -lattice constellations for the Rayleigh fading channel. *IEEE Trans. Inf. Theory* **2004**, *50*, 702–714. [CrossRef]
44. Oggier, F.; Viterbo, E. Algebraic Number Theory and Code Design for Rayleigh Fading Channels. *Commun. Inf. Theory* **2004**, *1*, 333–416. [CrossRef]

- 
45. Aranés, M.; Arenas, A. On the defining polynomials of maximal real cyclotomic extensions. *Rev. Real Acad. Cienc. Exactas Físicas y Nat. Ser. A. Mat.* **2008**, *101*, 187–203. [[CrossRef](#)]
  46. Chu, E.; George, A. *Inside the FFT Black Box—Serial and Parallel Fast Fourier Transform Algorithms*; CRC Press: Boca Raton, FL, USA, 2000.
  47. Lyubashevsky, V.; Micciancio, D. Generalized Compact Knapsacks Are Collision Resistant. In *Automata, Languages and Programming*; Bugliesi, M., Preneel, B., Sassone, V., Wegener, I., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 144–155.