# The Splitting Field of $Y^n - 2$, Two-Variable NTT and Lattice-Based Cryptography

**Wenzhe Yang**

wenzheyang87@gmail.com

https://orcid.org/0000-0002-2456-7453

**Abstract**

The splitting field $F$ of the polynomial $Y^n - 2$ is an extension over $\mathbb{Q}$ generated by $\zeta_n = \exp(2\pi\sqrt{-1}/n)$ and $\sqrt[n]{2}$. In this paper, we lay the foundation for applying the Order-LWE in the integral ring $\mathcal{R} = \mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ to cryptographic uses when $n$ is a power-of-two integer. We explicitly compute the Galois group $\mathrm{Gal}\,(F/\mathbb{Q})$ and the canonical embedding of $F$, based on which we study the properties of the trace pairings of the integral basis $\zeta_n^{k_0} \sqrt[n]{2}^{k_1}$. Then we discuss the security of the Order-LWE in $\mathcal{R}$, and show that it offers the same security level as the RLWE in $\mathbb{Z}[X]/\langle X^{n^2/4}+1\rangle$. Moreover, we design a Two-Variable Number Theoretic Transform (2NTT) algorithm for the quotient $\mathcal{R}_p = \mathcal{R}/p\mathcal{R}$, where $p$ is a prime number such that $Y^n \equiv 2 \bmod p$ has $n$ distinct solutions. Compared to the one-variable NTT in $\mathbb{Z}[X]/\langle X^{n^2/4} + 1\rangle$, a crucial advantage of 2NTT is that it enjoys a quadratic saving of twiddle factors. Hence, we can leverage this quadratic saving to boost the performance of 2NTT in practical implementations. At last, we also look at the applications of the Order-LWE in $\mathcal{R}$. In particular, we construct a new variant of CKKS for $\mathcal{R}$ and study its new properties.

**Keywords**: Splitting Field, Galois Group, Trace Pairing, Order-LWE, 2NTT.

# 1 Introduction

In the last three decades, lattice-based cryptography has played a crucial role in the development of cryptography. Initially, it gained interests in the communities of cryptographers because the constructions in it were often accompanied by strong security proofs based on the worst-case instances in the problems of lattice theory [1]. Later, this type of scheme was significantly improved by Regev when he introduced a new intermediate problem: Learning With Errors (LWE) [31, 33], which is flexible to use in practice, while also asymptotically being at least as hard as certain worst-case lattice problems [8, 29]. In early 2010s, a more efficient variant of LWE, the Ring Learning With Errors (RLWE) problem, was introduced by researchers [20], the public key of which has a much smaller size, thus making it more practical. The most important class of rings in RLWE is the ring of algebraic integers of a cyclotomic field [20]. The RLWE problem in these rings enjoy strong security proofs based on the worst-case instances in the computational problems of the ideal lattices of cyclotomic fields [20].

A highly crucial property of lattice-based cryptography is that it is quantum resistant, as a result it has attracted rapidly increasing interest because of the recent important advances in quantum computing [2, 14]. In 2016, the National Institute of Standards and Technology (NIST) announced to update their standards to include post-quantum digital-signature, encryption and key-establishment protocols [9]. In July 2022, NIST announced the candidate algorithms for standardization [26]. In particular, it recommended two primary algorithms to be implemented for most use cases: CRYSTALS-Kyber [6] for key-establishment and CRYSTALS-Dilithium for digital signature [15]. The constructions of both schemes are based on the RLWE (and Module-LWE) problem in the ring of algebraic integers of the 512-th cyclotomic field: $\mathbb{Z}[X]/\langle X^{256}+1\rangle$.

Lattice-based cryptography has also been highly crucial in the development of Homomorphic Encryption (HE), another important theme in cryptography in recent years. An HE scheme enables homomorphic operations to be performed on encrypted data without decryption [17]. As a result, data is encrypted throughout its entire lifecycle, which guarantees the security of sensitive data in scenarios such as cloud computing. The first Fully Homomorphic Encryption (FHE) scheme was constructed by Gentry in his thesis [17]. Following Gentry's original blueprint, researchers have come up with many new FHE schemes. Many of the currently popular schemes, e.g., BGV [7], BFV [16], CKKS [11] and TFHE [12], are based on the RLWE problem in the ring $\mathbb{Z}[X]/\langle X^{M/2}+1\rangle$, where $M$ is a power-of-two integer. The value of $M$ depends on many factors, e.g., the level of security needed in practice, which can be very large. For example, in the implementations of CKKS, $M$ could be as large as $2^{17}$, which makes it very challenging to compute the polynomial multiplications even using Number Theoretic Transform (NTT) on special hardware [19, 34, 35, 36]. This is a major reason why these FHE schemes are so slow.

The main motivation of this paper is to propose a new ring, a subring of the ring of algebraic integers of the splitting field of $Y^n - 2$, for cryptographic uses. First, the Order-LWE problem in the new ring has similar hardness results as that of $\mathbb{Z}[X]/\langle X^{M/2}+1\rangle$. More importantly, this new ring admits a crucial Two-Variable Number Theoretic Transform (2NTT) that has a different algebraic structure. In particular, it enjoys a quadratic saving of twiddle factors. As a result, the multiplications of polynomials in it can be further boosted via leveraging the new properties of 2NTT. Hence, it offers a new promising way to improve the performance of cryptographic schemes by using this new ring instead, especially when polynomials have very high degrees.

## 1.1 The Cyclotomic Fields and Related Works

Let us briefly review the appealing properties of the cyclotomic field that makes it highly important in lattice-based cryptography. The $M$-th cyclotomic field is a number field that is constructed by adjoining a complex root of unity to the field of rational numbers $\mathbb{Q}$ [20, 21, 23]. More precisely, for a positive integer $M$, $\zeta_M = \exp\left(2\pi\sqrt{-1}/M\right)$ is a primitive $M$-th root of unity. The $M$-th cyclotomic field is the extension $\mathbb{Q}(\zeta_M)$ generated by $\zeta_M$. The ring of algebraic integers of $\mathbb{Q}(\zeta_M)$ is the integral ring $\mathbb{Z}[\zeta_M]$ [21, 25].

In practice, the most important case is where $M$ is a power-of-two integer. Then via sending $\zeta_M$ to $X$, $\mathbb{Z}[\zeta_M]$ is isomorphic to $R = \mathbb{Z}[X]/\langle X^{M/2}+1\rangle$. The algebraic properties of $\mathbb{Z}[\zeta_M]$ and $\mathbb{Q}[\zeta_M]$ are very well studied by mathematicians [18]. In particular, its Galois group, canonical embedding and trace pairings are well understood [20, 23]. Based on these results, the hardness of the RLWE problem in $R$ was carefully studied in [20]. Another crucial property of $R$ is that if we choose a prime number $p$ such that $X^{M/2} + 1 = 0 \bmod p$ has a solution in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, then polynomial multiplication in $R_p = R/pR$ can be computed by using NTT, whose complexity is $O(M \log_2 M)$ [19, 27, 34]. This property is widely used in practice to boost the performance of the cryptographic schemes based on the RLWE problem in $R$. Besides, the Galois group $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_M\right)/\mathbb{Q}\right)$ is naturally isomorphic to the multiplicative group of units modulo $M$, i.e., $(\mathbb{Z}/M\mathbb{Z})^{\times}$, which is very important in FHE schemes [7, 11]. For example, the construction of the bootstrapping of CKKS crucially depends on the action of $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_M\right)/\mathbb{Q}\right)$ on the ciphertexts [10].

Since 2015, Pedrouzo-Ulloa el al. has written papers on the Multivariate Ring Learning With Errors ($m$-RLWE) based on the cyclotomic rings [28]. The idea is to study the $m$-RLWE in the ring

$$R_{n_1,n_2} = \mathbb{Z}[X,Y]/\langle \Phi_{n_1}(X), \Phi_{n_2}(Y)\rangle,$$

where $\Phi_{n_1}$ is the $n_1$-th cyclotomic polynomial, etc [23]. However, as pointed out by the paper [5], such an approach can easily lead to security issues. In particular, the security level of $m$-RLWE in $R_{n_1,n_2}$ is drastically less than the RLWE in the ring $\mathbb{Z}[X]/\langle \Phi_{n_1 n_2}(X)\rangle$ in general. For example, to be able to efficiently using NTT to boost polynomial multiplications in $R_{n_1,n_2}$, we are certainly most interested in the case where both $n_1$ and $n_2$ are power-of-two integers. But the paper [5] presents an efficient attack against the $m$-RLWE in such case. More explicitly, the authors of [5] show that even when $n_1 = n_2 = 1024$, the $m$-RLWE in $\mathbb{Z}[X,Y]/\langle X^{1024}+1, Y^{1024}+1\rangle$ offers at most 98 bits of security, which is far less than the security offered by the ring $\mathbb{Z}[X]/\langle X^{2^{20}}+1\rangle$. In conclusion, this approach has serious security issues, thus it is not a sound alternative to the RLWE in cyclotomic rings.

## 1.2 Our Contributions

Throughout this paper, $n$ ($\geq 8$) is a power-of-two integer. Recall that $\zeta_n$ is the $n$-th root of unity $\exp\left(2\pi\sqrt{-1}/n\right)$ and $\sqrt[n]{2} \in \mathbb{R}$ is the real positive $n$-th root of 2. The splitting field $F$ of $Y^n - 2$ is constructed by adjoining $\zeta_n$ and $\sqrt[n]{2}$ to $\mathbb{Q}$, namely $F = \mathbb{Q}\left(\zeta_n, \sqrt[n]{2}\right)$. The integral ring $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ is only known to be an order of $F$ [4, 23]. Via sending $\zeta_n$ to $X$ and $\sqrt[n]{2}$ to $Y$, $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ is naturally isomorphic to the quotient

$$\mathcal{R} = \mathbb{Z}[X,Y]/\langle X^{n/2}+1, Y^{n/2} - (X^{n/8} - X^{3n/8})\rangle.$$

Our major contributions in this paper include the following important results.

### 1.2.1 Number Theoretic Results

We first compute the Galois group $\mathrm{Gal}\left(F/\mathbb{Q}\right)$ of $F$ over $\mathbb{Q}$. Through studying the immediate fields $\mathbb{Q}\left(\sqrt{-1}\right)$ and $\mathbb{Q}\left(\zeta_n\right)$ of $F$ using the fundamental theorem of Galois theory, we obtain an explicit algebraic structure of $\mathrm{Gal}\left(F/\mathbb{Q}\right)$. Based on these results, we construct the canonical embedding of $F$ into $\mathbb{C}^{n^2/4}$ and give a proof that it sends the natural integral basis $\zeta_n^{k_0}\sqrt[n]{2}^{k_1}$, $0 \leq k_0, k_1 < n/2$, of $F$ to an orthogonal basis of $\mathbb{C}^{n^2/4}$.

Then, we compute the trace pairings of the integral basis $\zeta_n^{k_0}\sqrt[n]{2}^{k_1}$, from which we construct its dual that forms an integral basis for $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]^{\vee}$ [23, 37].

We also compute the absolute discriminant of the integral ring $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$, which is a power-of-two integer. Moreover, we find the first minimums of $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ and its dual $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]^\vee$, which are very crucial when analyzing the error distributions on ideal lattices.

Based on these results, we study the behaviors of the elliptic Gaussian distributions on the ideal lattices associated with $\mathcal{R}$. In particular, we analyze how $\mathrm{Gal}(F/\mathbb{Q})$ acts on these probability distributions.

### 1.2.2 Order-LWE

We formulate the Search and Average-Case Decision Order-LWE problems in $\mathcal{R}$. We study the worst-case hardness of the Search Order-LWE using the algebraic properties of $\mathcal{R}$ and the results in [20]. Then we adapt the proof in [20] to give reductions from the Search Order-LWE to Average-Case Decision Order-LWE, thereby showing that the Order-LWE distribution over $\mathcal{R}$ is pseudorandom. As in [4, 20], we give two variants of the reductions. The first reduction is to the Average-Case Decision Order-LWE problem with a nonsperical error distribution defined with respect to the canonical embedding. The second reduction is to the Average-Case Decision Order-LWE problem with a spherical error distribution with respect to the canonical embedding, but with only a bounded number of samples [20, 33].

### 1.2.3 2NTT

Perhaps the most important new feature of the ring $\mathcal{R}$ is the existence of a 2NTT. We choose a prime number $p$ such that $X^n \equiv 1 \bmod p$ has a primitive solution $\alpha \in \mathbb{F}_p$ and $Y^n \equiv 2 \bmod p$ has a solution $\beta \in \mathbb{F}_p$. Then the equations

$$X^{n/2} + 1 \equiv 0 \bmod p \text{ and } Y^{n/2} - \left(X^{n/8} - X^{3n/8}\right) \equiv 0 \bmod p \tag{1.1}$$

have $n^2/4$ solutions in total. The first equation of Eq. (1.1) has $n/2$ solutions: $\{\alpha^{2i+1} : 0 \leq i < n/2\}$. For every solution $X = \alpha^{2i+1}$, the second equation of Eq. (1.1) also has $n/2$ solutions: $\{\alpha^{2j}\beta : 0 \leq j < n/2\}$ if $i \equiv 0, 3 \bmod 4$; and $\{\alpha^{2j+1}\beta : 0 \leq j < n/2\}$ if $i \equiv 1, 2 \bmod 4$. We give a criterion about the good prime numbers that Eq. (1.1) has $n^2/4$ solutions:

$$n|(p-1) \text{ and } 2^{(p-1)/n} \equiv 1 \bmod p. \tag{1.2}$$

While the solutions $\alpha$ and $\beta$ can be efficiently found by using Tonelli-Shanks algorithm recursively as $n$ is a power-of-two integer.

Given a two-variable polynomial $\mathbf{F}(X, Y) = \sum_{k,l=0}^{n/2-1} f_{k,l} X^k Y^l$ in $\mathcal{R}_p = \mathcal{R}/p\mathcal{R}$. The idea of 2NTT is to evaluate $\mathbf{F}$ at the $n^2/4$ solutions of Eq. (1.1). The 2NTT of $\mathbf{F}$ consists of transverse and longitudinal vector butterflies:

1. Transverse vector butterfly. This phase uses a vector butterfly to evaluate $\mathbf{F}$ at the $n/2$ roots $X = \alpha^{2i+1}$, $0 \leq i < n/2$, the output of which are $n/2$ vectors $\mathbf{F}\left(\alpha^{2i+1}, Y\right)$. There are $\log_2(n/2)$ stages in this phase, and each stage consumes $O(n)$ vector operations (vector summation and scalar multiplication).

2. Transpose and longitudinal vector butterfly. The output of the transverse vector butterfly naturally falls into two groups: Group 1 with $i \equiv 0, 3 \bmod 4$ and Group 2 with $i \equiv 1, 2 \bmod 4$. Each group forms an $n/4 \times n/2$ matrix. Now we evaluate the vector-valued polynomial constructed from the $n/2$ column vectors of Group 1 at the roots $\{\alpha^{2j}\beta : 0 \leq j < n/2\}$ using a vector butterfly with a new set of twiddle factors. We also evaluate the vector-valued polynomial constructed from the $n/2$ column vectors of Group 2 at the roots $\{\alpha^{2j+1}\beta : 0 \leq j < n/2\}$ using a vector butterfly with another set of twiddle factors. Each evaluation consists of $\log_2(n/2)$ stages and each stage consumes $O(n)$ vector operations.

### 1.2.4 Comparisons with Existing Results

First, compared to the works of Pedrouzo-Ulloa el al. [28], our approach does not have any of the security issues presented in the paper [5]. More precisely, the Order-LWE in $\mathcal{R}$, whose rank is $n^2/4$, offers the same security level as the RLWE in $\mathbb{Z}[X]/\langle X^{n^2/4} + 1\rangle$, whose rank is also $n^2/4$ [20].

So, it is natural to compare the properties of the new ring $\mathcal{R}$ with that of $\mathbb{Z}[X]/\langle X^{n^2/4} + 1\rangle$. First, both the 2NTT and NTT consist of $\log_2\left(n^2/4\right)$ stages, and the computational complexity of each stage is the same. Therefore, the computational complexity of 2NTT is the same as the one-variable NTT.

The most important advantage of 2NTT is that it enjoys a quadratic saving of twiddle factors. The space of the twiddle factors of NTT in $\mathbb{Z}[X]/\langle X^{n^2/4}+1\rangle$ is $O(n^2/4)$, which essentially come from the $n^2/4$ solutions of $X^{n^2/4} + 1 \equiv 0 \bmod p'$. The space of the twiddle factors of 2NTT is only $O(n)$, which essentially come from the solutions of $X^{n/2} \equiv -1 \bmod p$ and $Y^n \equiv 2 \bmod p$ ($3n/2$ in total). Thus, there is a quadratic saving of twiddle factor space, which is especially desirable for large polynomials. This saving offers new possibilities for optimizations in practical implementations of 2NTT on platforms such as GPU and FPGA.

### 1.2.5 Applications and Generalizations

The results in this paper can have immediate applications in cryptography, namely we can construct cryptographic schemes whose security is based on the RLWE in the new ring $\mathcal{R}$. An interesting direction is to construct variants of existing schemes by replacing the ring $\mathbb{Z}[X]/\langle X^{n^2/4} + 1\rangle$ with $\mathcal{R}$. For example, we can construct variants of CRYSTALS-Kyber and CRYSTALS-Dilithium by replacing the ring $\mathbb{Z}[X]/\langle X^{256} + 1\rangle$ with $\mathcal{R}$ where $n = 32$, i.e., $R = \mathbb{Z}[X, Y]/\langle X^{16} + 1, Y^{16} - (X^4 - X^{12})\rangle$, since both rings offer the same level of security. Of course, a caveat is that one need to show such a replacement does not cause unbearable loss of security.

The quadratic saving of twiddle factors is much more significant when the degree of polynomials in use is large. In an FHE schemes such as BGV, BFV or CKKS, it frequently uses polynomial rings as large as $\mathbb{Z}[X]/\langle X^{16384} + 1\rangle$. The ring $\mathcal{R}$ with $n = 256$ offers the same level of security, while has a much smaller twiddle factor space. Hence if we instead build variants of BGV, BFV and CKKS using the ring $\mathcal{R}$, we can further boost the performances of these schemes by leveraging this quadratic saving of twiddle factors.

The constructions of the new variants of leveled BGV and BFV schemes based on the Order-LWE in the new ring $\mathcal{R}$ follow immediately from the original papers [7, 16], hence will be omitted here. In this paper, we focus on the properties of a new variant of CKKS based on $\mathcal{R}$. Our new contributions include the construction of a careful choice of encoding and decoding maps for $\mathcal{R}$ using the algebraic structure of $\mathrm{Gal}\,(F/\mathbb{Q})$, and the action of $\mathrm{Gal}\,(F/\mathbb{Q})$ on the plaintexts and ciphertexts in this new variant. We also show that this new variant of CKKS is bootstrappable.

In the appendix, we show that all the results obtained in this paper can be generalized to the ring $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$, which is an order of the splitting field of $Y^n + 2$. We also briefly touch on the splitting field $\mathbb{Q}(\zeta_n, \sqrt[n]{r})$ of $Y^n - r$, where $|r|$ $(\geq 3)$ is a prime number.

## 1.3 Outline

In Section 2, we compute the Galois group of $F$ over $\mathbb{Q}$ and study its algebraic structures using the fundamental theorem of Galois theory. In Section 3, we construct the canonical embedding of $F$ into $\mathbb{C}^{n^2/4}$ and present an important orthogonality property for it. In Section 4, we compute the trace pairings of the natural integral basis of $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ and compute its absolute discriminant. We also find the first minimums of $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ and $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]^\vee$. In Section 5, we discuss the error distributions on the ideal lattices associated with $\mathcal{R}$. We formulate the Search and Average-Case Decision Order-LWE in $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ and study their hardness. In Section 6, we introduce the 2NTT for $\mathcal{R}$ and design a vector butterfly algorithm. In Section 7, we study a new variant of CKKS based on $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$. The appendix is devoted to some technical details needed in this paper. In particular, we show that all the results obtained for $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ can be generalized to $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$.

# 2 The Splitting Field and Its Galois Group

In this section, we give a detailed description of the splitting field $F$ of $Y^n - 2$, where $n$ $(\geq 8)$ is a power-of-two integer. In particular, we explicitly construct the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ of $F$ over $\mathbb{Q}$ [13] and study its structures using the fundamental theorem of Galois theory [25].

## 2.1 The Construction of the Splitting Field

The splitting field $F$ of $Y^n - 2$ is a finite extension over $\mathbb{Q}$ generated by two numbers $\zeta_n = \exp(2\pi\sqrt{-1}/n)$ and $\sqrt[n]{2}$, i.e., $F = \mathbb{Q}\left(\zeta_n, \sqrt[n]{2}\right)$ [21, 25]. The two numbers $\zeta_n$ and $\sqrt[n]{2}$ satisfy an algebraic relation

$$\sqrt[n]{2}^{n/2} = \zeta_n^{n/8} - \zeta_n^{3n/8}, \tag{2.1}$$

which is just the equation $\sqrt{2} = \exp\left(2\pi\sqrt{-1}/8\right) - \exp\left(6\pi\sqrt{-1}/8\right)$.

**Lemma 2.1.** *For a power-of-two integer $n$ $(\geq 8)$, the degree of the field extension of $F$ over $\mathbb{Q}$, denoted by $[F : \mathbb{Q}]$, is $n^2/4$.*

The readers are referred to the webpage [38] for a detailed proof of this lemma. Thus viewed as a vector space over $\mathbb{Q}$, the dimension of $F$ is $n^2/4$, with a natural basis given by

$$\left\{\zeta_n^{k_0}\sqrt[n]{2}^{k_1} : 0 \leq k_0, k_1 < n/2\right\}. \tag{2.2}$$

## 2.2 The Galois Group of the Splitting Field

The construction of the Galois group of $F$ over $\mathbb{Q}$, denoted by $\mathrm{Gal}(F/\mathbb{Q})$, uses a method from Conrad's note [13]. The order of $\mathrm{Gal}(F/\mathbb{Q})$ is equal to the dimension of $F$ over $\mathbb{Q}$, hence $\mathrm{Gal}(F/\mathbb{Q})$ has $n^2/4$ elements. Since $F$ is generated by $\zeta_n$ and $\sqrt[n]{2}$ over $\mathbb{Q}$, any element of $\mathrm{Gal}(F/\mathbb{Q})$ is determined by its actions on them, which must be of the form

$$\sigma_{a,b}(\zeta_n) = \zeta_n^a \text{ and } \sigma_{a,b}(\sqrt[n]{2}) = \zeta_n^b\sqrt[n]{2} \text{ with } a, b \in \mathbb{Z}/n\mathbb{Z}. \tag{2.3}$$

Notice that here we have used the property that $\sigma_{a,b}$ must send a root of $X^n - 1$ (resp. $Y^n - 2$) to another root of the same equation [25]. In this paper, the notation $\mathbb{Z}/n\mathbb{Z}$ has an additional meaning that its representative is chosen to be

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}.$$

The action of $\sigma_{a,b}$ on a general basis element $\zeta_n^{k_0}\sqrt[n]{2}^{k_1}$ is $\zeta_n^{ak_0+bk_1}\sqrt[n]{2}^{k_1}$.

Since $\sigma_{a,b}(\zeta_n)$ is another primitive root of $X^n - 1$, $a$ must be an odd integer in $\mathbb{Z}/n\mathbb{Z}$. Moreover, $a$ and $b$ are not totally independent from each other, as $\sigma_{a,b}$ must preserve the algebraic relation in Eq. (2.1), which can be rewritten into

$$\sqrt[n]{2}^{n/2} = \zeta_n^{n/8} + \zeta_n^{-n/8}.$$

Under the action of $\sigma_{a,b}$, this equation becomes

$$(-1)^b\sqrt[n]{2}^{n/2} = \zeta_n^{na/8} + \zeta_n^{-na/8}.$$

For it to be valid, we must have

$$a \equiv \begin{cases} 1,\ 7 \bmod 8, & \text{if } b \text{ is even,} \\ 3,\ 5 \bmod 8, & \text{if } b \text{ is odd.} \end{cases} \tag{2.4}$$

For later convenience, we define the finite set $G$ to be

$$G = \{(a, b) \in (\mathbb{Z}/n\mathbb{Z})^2 : (a, b) \text{ satisfies the condition in Eq. (2.4)}\}, \tag{2.5}$$

which has $n^2/4$ elements. Then the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ is

$$\mathrm{Gal}(F/\mathbb{Q}) = \{\sigma_{a,b} : (a, b) \in G\}.$$

Moreover, $\sigma_{1,0}$ is the identity element of $\mathrm{Gal}(F/\mathbb{Q})$ and $\sigma_{n-1,0}$ is the complex conjugation. A quick computation shows that the composition of two elements $\sigma_{a,b}$ and $\sigma_{c,d}$ is $\sigma_{a,b} \circ \sigma_{c,d} = \sigma_{ac,ad+b}$.

## 2.3 The Algebraic Structure of the Galois Group

We need the fundamental theorem of Galois theory to study the algebraic structure of the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ [25]. In its most basic form, this theorem tells us that there is a one-to-one correspondence between the immediate fields of $F$ and the subgroups of $\mathrm{Gal}(F/\mathbb{Q})$, while the intermediate fields that are Galois extensions of $\mathbb{Q}$ correspond to the normal subgroups of $\mathrm{Gal}(F/\mathbb{Q})$. Here, an immediate field is a subfield of $F$ [25].

### 2.3.1 The Subfield of the Gaussian Rationals

The first important immediate field is $\mathbb{Q}(\zeta_n^{n/4})$, which is just $\mathbb{Q}(\sqrt{-1})$ as $(\zeta_n^{n/4})^2$ is $-1$. Since $\mathbb{Q}(\sqrt{-1})$ is a quadratic extension of $\mathbb{Q}$, the degree of $F$ over $\mathbb{Q}(\sqrt{-1})$ is $n^2/8$. The Galois group $\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right)$ is a subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ that fixes $\mathbb{Q}(\sqrt{-1})$:

$$\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right) = \{\sigma_{a,b} \in \mathrm{Gal}(F/\mathbb{Q}) : \sigma_{a,b}(x) = x,\ \forall x \in \mathbb{Q}(\sqrt{-1})\}.$$

Let $N$ be the subset of $G$ of the form

$$N = \{(a,b) \in G : a \equiv 1 \text{ or } 5 \bmod 8\}, \tag{2.6}$$

which has $n^2/8$ elements. Then $\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right)$ is the subgroup

$$\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right) = \{\sigma_{a,b} \in \mathrm{Gal}(F/\mathbb{Q}) : (a,b) \in N\}.$$

Because $\mathbb{Q}(\sqrt{-1})$ is a Galois extension of $\mathbb{Q}$, $\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right)$ is a normal subgroup of $\mathrm{Gal}(F/\mathbb{Q})$. The group $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}\right)$ is naturally identified with the subgroup $\{\sigma_{1,0}, \sigma_{n-1,0}\}$, so $\mathrm{Gal}(F/\mathbb{Q})$ is the disjoint union of cosets

$$\mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right) \cup \left(\sigma_{n-1,0} \circ \mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right)\right).$$

From the relation $\sigma_{n-1,0} \circ \sigma_{a,b} = \sigma_{(n-1)a,(n-1)b}$, we deduce that $G \setminus N$ can be expressed as

$$G \setminus N = \{((n-1)a, (n-1)b) : (a,b) \in N\}. \tag{2.7}$$

Furthermore, since the restriction of the quotient map on $\{\sigma_{1,0}, \sigma_{n-1,0}\}$ is identity, $\mathrm{Gal}\left(F/\mathbb{Q}\right)$ can be represented as a semidirect product [24]

$$\mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}\left(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}\right) \ltimes \mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right). \tag{2.8}$$

### 2.3.2 The Cyclotomic Subfield

Another important immediate field of $F$ is $\mathbb{Q}(\zeta_n)$, the $n$-th cyclotomic field [23]. The Galois group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) = \{\varsigma_a : a = 1, 3, \ldots, n-1\},$$

where $\varsigma_a$ is the automorphism of $\mathbb{Q}(\zeta_n)$ that sends $\zeta_n$ to $\zeta_n^a$. The field $\mathbb{Q}(\sqrt{-1})$ is a subfield of $\mathbb{Q}(\zeta_n)$, and the Galois group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}(\sqrt{-1})$ is

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\sqrt{-1})\right) = \langle \varsigma_5 \rangle = \{\varsigma_5^j : 0 \le j < n/4\},$$

which has $n/4$ elements since $5^{n/4} \equiv 1 \bmod n$ [10]. Moreover, $\varsigma_{n-1}$ acts on $\mathbb{Q}(\zeta_n)$ as complex conjugation and the Galois group of $\mathbb{Q}(\sqrt{-1})$ over $\mathbb{Q}$ is naturally $\{\varsigma_1, \varsigma_{n-1}\}$. In conclusion, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ can be represented as the direct product

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \langle \varsigma_5 \rangle \times \langle \varsigma_{n-1} \rangle.$$

The field $\mathbb{Q}(\zeta_n)$ is a Galois extension over $\mathbb{Q}$ with degree $n/2$. The Galois group of $F$ over $\mathbb{Q}(\zeta_n)$, $\mathrm{Gal}\,(F/\mathbb{Q}(\zeta_n))$, is the normal subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ that fixes $\mathbb{Q}(\zeta_n)$:

$$\mathrm{Gal}\,(F/\mathbb{Q}(\zeta_n)) = \{\sigma_{a,b} \in \mathrm{Gal}(F/\mathbb{Q}) : \sigma_{a,b}(x) = x,\ \forall x \in \mathbb{Q}(\zeta_n)\},$$

which is given by

$$\mathrm{Gal}\,(F/\mathbb{Q}(\zeta_n)) = \{\sigma_{1,b} \in \mathrm{Gal}(F/\mathbb{Q}) : b = 0, 2, \ldots, n-2\} = \langle \sigma_{1,2} \rangle.$$

From the inclusion $\mathbb{Q}(\sqrt{-1}) \subset \mathbb{Q}(\zeta_n) \subset F$, we obtain an isomorphism [25]

$$\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right)/\mathrm{Gal}\,(F/\mathbb{Q}(\zeta_n)) \cong \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\sqrt{-1})\right). \tag{2.9}$$

Let us look at the isomorphism in Eq. (2.9) more carefully. Since $\sigma_{5,1}^{n/4}$ lies in $\mathrm{Gal}(F/\mathbb{Q}(\zeta_n))$ and $\sigma_{5,1}^{i} \notin \mathrm{Gal}(F/\mathbb{Q}(\zeta_n))$ for $1 \le i < n/4$, $\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right)$ is the disjoint union of cosets of the form

$$\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right) = \cup_{i=0}^{n/4-1}\left(\sigma_{5,1}^{i} \circ \mathrm{Gal}\,(F/\mathbb{Q}(\zeta_n))\right).$$

Thus every element of $\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right)$ can be uniquely written as

$$\sigma_{5,1}^{i} \circ \sigma_{1,2}^{j} \text{ with } 0 \le i < n/4 \text{ and } 0 \le j < n/2.$$

To multiply two elements of $\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{-1})\right)$, we need the relation

$$\sigma_{5,1}^{-1} \circ \sigma_{1,2} \circ \sigma_{5,1} = \sigma_{1,2}^{5^{-1}}, \tag{2.10}$$

where the inverse $5^{-1}$ is computed modulo $n/2$ as $\sigma_{1,2}^{n/2} = \sigma_{1,0}$. From the semidirect product in Eq. (2.8), we deduce that every element of $\mathrm{Gal}\,(F/\mathbb{Q})$ can be uniquely written as

$$\sigma_{n-1,0}^{k} \circ \sigma_{5,1}^{i} \circ \sigma_{1,2}^{j}, \text{ where } 0 \le i < n/4,\ 0 \le j < n/2 \text{ and } k = 0, 1.$$

To multiply two elements of $\mathrm{Gal}\,(F/\mathbb{Q})$, we further need the relations

$$\sigma_{n-1,0} \circ \sigma_{5,1} \circ \sigma_{n-1,0} = \sigma_{5,1} \circ \sigma_{1,2}^{-5^{-1}} \text{ and } \sigma_{n-1,0} \circ \sigma_{1,2} \circ \sigma_{n-1,0} = \sigma_{1,2}^{-1}. \tag{2.11}$$

These results will be crucial when we study the error distributions over the ideal lattices associated with the ring $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ and a new variant of CKKS in $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ in Section 7.

# 3 The Canonical Embedding

In this section, we construct the canonical embedding of $F$ into $\mathbb{C}^{n^2/4}$ and study its properties [21, 23]. We prove that this canonical embedding sends the natural integral basis in Eq. (2.2) to an orthogonal basis of $\mathbb{C}^{n^2/4}$, a property that will become important when we discuss the error distributions over the ideal lattices associated with $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$.

Since the degree of $F$ over $\mathbb{Q}$ is $n^2/4$, there exist $n^2/4$ distinct embeddings of $F$ into $\mathbb{C}$ [21, 23, 25]. The inclusion $F \hookrightarrow \mathbb{C}$ is naturally an embedding. Furthermore, for every $\sigma_{a,b} \in \mathrm{Gal}\,(F/\mathbb{Q})$, there is an embedding of the form

$$\sigma_{a,b} : F \xrightarrow{\sigma_{a,b}} F \hookrightarrow \mathbb{C},$$

which gives us all the embeddings of $F$ into $\mathbb{C}$. Similar to the cyclotomic fields, $F$ does not admit any real embedding [20]. In this paper, a vector in $\mathbb{C}^{n^2/4}$ is denoted by $\mathbf{z} = (z_{a,b})_{(a,b)\in G}$, namely its coordinate is indexed by the elements of $G$. Given two vectors $\mathbf{z} = (z_{a,b})$ and $\mathbf{z}' = (z'_{a,b})$, their standard inner product is given by $\langle \mathbf{z}, \mathbf{z}' \rangle = \sum_{(a,b)\in G} z_{a,b} \cdot \overline{z'}_{a,b}$, which is positive definite, linear in the first argument and antilinear in the second argument. Hence the canonical embedding of $F$ into $\mathbb{C}^{n^2/4}$ is given by

$$\sigma : x \in F \mapsto (\sigma_{a,b}(x))_{(a,b)\in G} \in \mathbb{C}^{n^2/4}. \tag{3.1}$$

In fact, $\sigma$ induces an injective real linear map from $F_{\mathbb{R}} = F \otimes_{\mathbb{Q}} \mathbb{R}$ to $\mathbb{C}^{n^2/4}$:

$$\sigma : x \otimes r \mapsto (\sigma_{a,b}(x) \cdot r)_{(a,b)\in G}\,, \text{ where } x \in F \text{ and } r \in \mathbb{R}. \tag{3.2}$$

The complex conjugation of $\sigma_{a,b}(x)$, denoted by $\overline{\sigma_{a,b}(x)}$, is $\sigma_{(n-1)a,(n-1)b}(x)$ for every $x \in F$ and $(a,b) \in G$. Therefore, the image of $F_{\mathbb{R}}$ under $\sigma$ is the following real subspace of $\mathbb{C}^{n^2/4}$

$$H = \left\{ (z_{a,b})_{(a,b)\in G} \in \mathbb{C}^{n^2/4} : z_{(n-1)a,(n-1)b} = \overline{z_{a,b}} \right\},$$

which is isomorphic to $F_{\mathbb{R}}$. In this paper, we often implicitly identify $H$ with $F_{\mathbb{R}}$ via the canonical embedding. The homomorphism in Eq. (3.2) can also be written as

$$\sigma : x \otimes r \mapsto \left(\sigma_{a,b}(x) \cdot r, \sigma_{(n-1)a,(n-1)b}(x) \cdot r\right)_{(a,b)\in N}.$$

An automorphism $\sigma_{c,d} \in \mathrm{Gal}(F/\mathbb{Q})$ of $F$ induces an automorphism of $H$ by making the following diagram commute

$$\begin{tikzcd}
x \otimes r \arrow[r, "\sigma"] \arrow[d, "\sigma_{c,d}"] & \left(\sigma_{a,b}(x) \cdot r, \sigma_{(n-1)a,(n-1)b}(x) \cdot r\right)_{(a,b)\in N} \arrow[d, "\sigma_{c,d}"] \\
\sigma_{c,d}(x) \otimes r \arrow[r, "\sigma"] & \left(\sigma_{a,b}(\sigma_{c,d}(x)) \cdot r, \sigma_{(n-1)a,(n-1)b}(\sigma_{c,d}(x)) \cdot r\right)_{(a,b)\in N}
\end{tikzcd} \quad . \tag{3.3}$$

Therefore, the effect of the automorphism $\sigma_{c,d}$ is to permute the components of a vector in $H$. Let $\mathbf{e}_{a,b} \in \mathbb{C}^{n^2/4}$ be the vector with 1 in its $(a,b)$-th component and 0 elsewhere, which is a natural basis of $\mathbb{C}^{n^2/4}$. For every $(a,b) \in N$, we define

$$\begin{aligned} \mathbf{h}_{(a,b)} &= \frac{1}{\sqrt{2}}\left(\mathbf{e}_{a,b} + \mathbf{e}_{(n-1)a,(n-1)b}\right), \\ \mathbf{h}_{((n-1)a,(n-1)b)} &= \frac{\sqrt{-1}}{\sqrt{2}}\left(\mathbf{e}_{a,b} - \mathbf{e}_{(n-1)a,(n-1)b}\right), \end{aligned} \tag{3.4}$$

which form a real basis of $H$. The inner product $\langle\cdot,\cdot\rangle$ on $\mathbb{C}^{n^2/4}$ induces a real positive definite inner product on $H$, with respect to which $\{\mathbf{h}_{a,b} : (a,b) \in G\}$ is an orthonormal basis.

**Proposition 3.1.** *Under the canonical embedding, the natural basis of $F$ in Eq. (2.2) is sent to an orthogonal basis of $\mathbb{C}^{n^2/4}$. More precisely,*

$$\left\langle \sigma\left(\zeta_n^{k_0}\sqrt[n]{2}^{k_1}\right), \sigma\left(\zeta_n^{l_0}\sqrt[n]{2}^{l_1}\right)\right\rangle = \begin{cases} \left(\sqrt[n]{2}\right)^{2k_1}\cdot n^2/4, & \textit{if } k_0 = l_0 \textit{ and } k_1 = l_1. \\ 0, & \textit{otherwise.} \end{cases}$$

The proof of Proposition 3.1 is given in Appendix A. It is very illustrating to compare this orthogonality property of the canonical embedding of $F$ to that of the cyclotomic fields. For the $M$-th cyclotomic field, the integral basis $\{\zeta_M^{2i+1} : 0 \le i < M/2\}$, where $M$ is a power-of-two integer, is sent to an orthogonal basis of $\mathbb{C}^{M/2}$ under the canonical embedding of $\mathbb{Q}(\zeta_M)$. But the norm of the image of $\zeta_M^i$ under canonical embedding is always $\sqrt{M/2}$. Hence up to the overall constant $\sqrt{M/2}$, the canonical embedding of $\mathbb{Q}(\zeta_M)$ is an isometry [20]. However for the splitting field $F$, the norm of $\sigma(\zeta_n^{k_0}\sqrt[n]{2}^{k_1})$ is $2^{k_1/n}\cdot n/2$, which depends on the value of $k_1$, so certain basis vectors are elongated. But since $k_1 < n/2$, the ratio between the longest vector and shortest vector is smaller than $\sqrt{2}$.

# 4 The Trace Pairings and the First Minimums

In this section, we compute the trace pairings of the natural integral basis $\zeta_n^{k_0}\sqrt[n]{2}^{k_1}$ of $\mathcal{R} = \mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ and construct a dual basis for

$$\mathcal{R}^\vee = \{x \in F : \mathrm{Tr}(x\mathcal{R}) \subset \mathbb{Z}\}.$$

We will also compute the absolute discriminant of $\mathcal{R}$, from which we find the first minimums of $\mathcal{R} = \mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ and its dual $\mathcal{R}^\vee$ [23, 37].

## 4.1 The Computations of the Trace Pairings and the Absolute Discriminant

Recall that given an element $x \in F$, its trace $\mathrm{Tr}(x)$ can be computed by $\sum_{(a,b)\in G}\sigma_{a,b}(x)$ [20, 23]. The trace-pairing matrix is given by $\mathrm{Tr}(\zeta_n^{k_0}\sqrt[n]{2}^{k_1}\cdot\zeta_n^{l_0}\sqrt[n]{2}^{l_1})$ for every pair $(\zeta_n^{k_0}\sqrt[n]{2}^{k_1}, \zeta_n^{l_0}\sqrt[n]{2}^{l_1})$ with $0 \le k_0, k_1, l_0, l_1 < n/2$. We have the following important theorem, whose proof is given in Appendix A.

**Theorem 4.1.** *$Tr(\zeta_n^{k_0+l_0}\sqrt[n]{2}^{k_1+l_1})$ is always 0 unless $k_1 = l_1 = 0$ or $k_1 + l_1 = n/2$. When $k_1 = l_1 = 0$, we have*

$$Tr(\zeta_n^{k_0+l_0}) = \begin{cases} n^2/4, & \text{if } k_0 = l_0 = 0; \\ -n^2/4, & \text{if } k_0 + l_0 = n/2. \end{cases}$$

*when $k_1 + l_1 = n/2$, we have*

$$Tr(\zeta_n^{k_0+l_0}\sqrt[n]{2}^{n/2}) = \begin{cases} n^2/4, & \text{if } k_0 + l_0 = n/8 \text{ or } 7n/8; \\ -n^2/4, & \text{if } k_0 + l_0 = 3n/8 \text{ or } 5n/8. \end{cases}$$

From Theorem 4.1, if we choose a special order of the indices $k_0$, $k_1$, $l_0$ and $l_1$, the $n^2/4 \times n^2/4$ trace-pairing matrix $\mathrm{Tr}(\zeta_n^{k_0}\sqrt[n]{2}^{k_1} \cdot \zeta_n^{l_0}\sqrt[n]{2}^{l_1})$ becomes a block diagonal matrix, which consists of $n/2$ blocks of size $1 \times 1$ and $n(n-2)/8$ blocks of size $2 \times 2$. The $1 \times 1$ block is either $n^2/4$ or $-n^2/4$, and the $2 \times 2$ block can be chosen to be

$$\begin{pmatrix} n^2/4 & -n^2/4 \\ -n^2/4 & -n^2/4 \end{pmatrix}.$$

Now, recall that a lattice is a discrete subgroup of a real vector space $\mathbb{R}^m$, $m \in \mathbb{N}_+$ [32]. In this paper, we are only concerned with the full-rank lattices, i.e., the lattices generated by a basis of $\mathbb{R}^m$: $\mathcal{L} = \{\sum_{i=1}^m x_i\mathbf{v}_i : (x_i)_{1\le i\le m} \in \mathbb{Z}^m\}$, where $\{\mathbf{v}_i : 1 \le i \le m\}$ forms a basis of $\mathbb{R}^m$. The dual lattice of $\mathcal{L}$ is defined as $\mathcal{L}^* = \{\mathbf{x} \in \mathbb{R}^m : \langle \mathcal{L}, \mathbf{x}\rangle \subset \mathbb{Z}\}$, where $\langle \cdot, \cdot \rangle$ is the natural inner product on $\mathbb{R}^m$. From the definition, we immediately deduce that $(\mathcal{L}^*)^* = \mathcal{L}$. The absolute discriminant $\mathrm{disc}(\mathcal{L})$ of a lattice $\mathcal{L}$ is the square of the fundamental volume of $\mathcal{L}$ [20, 23, 37].

The absolute discriminant of $\mathcal{R}$, $\mathrm{disc}(\sigma(\mathcal{R})/\mathbb{Z})$, is also written as $\mathrm{disc}(\mathcal{R}/\mathbb{Z})$ [23]. Equivalently, it is the absolute value of the determinant of the trace-pairing matrix [20]:

$$\mathrm{disc}(\mathcal{R}/\mathbb{Z}) = \left|\det\left(\mathrm{Tr}\left(\zeta_n^{k_0}\sqrt[n]{2}^{k_1} \cdot \zeta_n^{l_0}\sqrt[n]{2}^{l_1}\right)\right)\right|.$$

Therefore, it is equal to

$$\mathrm{disc}(\mathcal{R}/\mathbb{Z}) = 2^{n(n-2)/8} \cdot \left(n^2/4\right)^{n^2/4},$$

which is a power of 2.

By definition, the dual of the integral basis of $\mathcal{R}$ is a set of elements of $F$

$$\{e_{l_0,l_1} \in F : 0 \le l_0, l_1 < n/2\}$$

such that $\mathrm{Tr}(e_{l_0,l_1} \cdot \zeta_n^{k_0}\sqrt[n]{2}^{k_1})$ equals 1 if $l_0 = k_0$, $l_1 = k_1$, and 0 otherwise. As a result, $e_{l_0,l_1}$ forms an integral basis for $\mathcal{R}^\vee$. The construction of $e_{l_0,l_1}$ follows immediately from Theorem 4.1.

**Proposition 4.2.** *When $l_1 = 0$, $e_{l_0,0}$ is given by*

$$e_{0,0} = \frac{4}{n^2} \text{ and } e_{l_0,0} = -\frac{4}{n^2} \cdot \zeta_n^{n/2-l_0} \text{ if } l_0 > 0.$$

*When $0 < l_1 < n/2$, $e_{l_0,l_1}$ is given by*

$$e_{l_0,l_1} = \begin{cases} \frac{2}{n^2}\zeta_n^{n/8-l_0}\sqrt[n]{2}^{n/2-l_1} - \frac{2}{n^2}\zeta_n^{3n/8-l_0}\sqrt[n]{2}^{n/2-l_1}, & \text{if } 0 \le l_0 \le \frac{n}{8}; \\ -\frac{2}{n^2}\zeta_n^{3n/8-l_0}\sqrt[n]{2}^{n/2-l_1} - \frac{2}{n^2}\zeta_n^{5n/8-l_0}\sqrt[n]{2}^{n/2-l_1}, & \text{if } \frac{n}{8} < l_0 \le \frac{3n}{8}; \\ -\frac{2}{n^2}\zeta_n^{5n/8-l_0}\sqrt[n]{2}^{n/2-l_1} + \frac{2}{n^2}\zeta_n^{7n/8-l_0}\sqrt[n]{2}^{n/2-l_1}, & \text{if } \frac{3n}{8} < l_0 < \frac{n}{2}. \end{cases}$$

## 4.2 The First Mininums of Ideal Lattices

The $i$-th minimum $\lambda_i(\mathcal{L})$ of a lattice $\mathcal{L}$ is defined as the minimum of $\max_{1\leq j\leq i}\|\mathbf{x}_j\|$ over all choices of $i$ linearly independent vectors $\mathbf{x}_1,\ldots,\mathbf{x}_i \in \mathcal{L}$ [20]. In particular, $\lambda_1(\mathcal{L})$ is the shortest nonzero vector of $\mathcal{L}$.

In this paper, we are mostly interested in the lattices of $H$ that come from the fractional ideals associated with $\mathcal{R}$ [21, 23]. Recall that a fractional ideal $\mathcal{I}$ associated with $\mathcal{R}$ is an $\mathcal{R}$-submodule that lies in $F$ such that there exists a nonzero element $r \in \mathcal{R}$ such that $r\mathcal{I} \subset \mathcal{R}$ [23]. A priori, an ideal of $\mathcal{R}$ is a fractional ideal. Because the degree of $F$ over $\mathbb{Q}$ is $n^2/4$, a fractional ideal $\mathcal{I}$ always has an integral basis consisting of $n^2/4$ elements: $\{u_i \in \mathcal{I} : 1 \leq i \leq n^2/4\}$ [23]. Then, under the canonical embedding, the image of $\mathcal{I}$, denoted by $\sigma(\mathcal{I})$, is a full-rank lattice in $H$ with a basis $\{\sigma(u_i) : 1 \leq i \leq n^2/4\}$. In particular, $\sigma(\mathcal{R})$ is a full-rank lattice of $H$ with a basis $\{\sigma(\zeta_n^{k_0}\sqrt[n]{2}^{k_1}) : 0 \leq k_0, k_1 < n/2\}$. In this paper, when we say the lattice $\mathcal{I}$ what we really mean is the lattice $\sigma(\mathcal{I})$ in $H$. Furthermore, the norm of an element $x \in F$ is the norm of the vector $\sigma(x)$ in $\mathbb{C}^{n^2/4}$, i.e., $\|x\| = \|\sigma(x)\|$.

If $\mathcal{I}$ is an ideal in $\mathcal{R}$, then the quotient ring $\mathcal{R}/\mathcal{I}$ only has finitely many elements, whose order by definition is the norm of $\mathcal{I}$, i.e., $\mathrm{Nm}(\mathcal{I}) = |\mathcal{R}/\mathcal{I}|$. To define the norm of a fractional ideal, we first choose an $r \in \mathcal{R}$ such that $r\mathcal{I} \subset \mathcal{R}$, then $\mathrm{Nm}(\mathcal{I})$ is defined to be $\mathrm{Nm}(r\mathcal{I})/\mathrm{Nm}(\langle r\rangle)$, where $\langle r\rangle$ is the principal ideal generated by $r$. This definition is independent of the choice of $r$ [21, 23]. Given a fractional ideal $\mathcal{I} \subset F$, its inverse $\mathcal{I}^{-1}$ and dual $\mathcal{I}^\vee$ are defined to be

$$\mathcal{I}^{-1} = \{x \in F : x\mathcal{I} \subset \mathcal{R}\},\ \mathcal{I}^\vee = \{x \in F : \mathrm{Tr}(x\mathcal{I}) \subset \mathbb{Z}\},$$

where the trace $\mathrm{Tr}(x)$ of $x \in F$ can be computed by $\sum_{(a,b)\in G}\sigma_{a,b}(x)$ [20, 23]. Notice that $\mathcal{I}^\vee$ is also a fractional ideal and $(\mathcal{I}^\vee)^\vee = \mathcal{I}$ [23]. However, $\sigma(\mathcal{I}^\vee)$ is the complex conjugate of the dual lattice of $\sigma(\mathcal{I})$ in $H$ [20]. Let $\Delta_{\mathcal{R}}$ be the absolute discriminant of $\mathcal{R}$ [23]. From Lemma 2.9 of [20], we obtain the upper and lower bounds on the first minimums of the ideal lattices associated with $\mathcal{R}$.

**Lemma 4.3.** *The first minimum of any fractional ideal $\mathcal{I}$ associated with $\mathcal{R}$ satisfies*

$$\frac{n}{2}\cdot \mathrm{Nm}(\mathcal{I})^{4/n^2} \leq \lambda_1(\mathcal{I}) \leq \frac{n}{2}\cdot \mathrm{Nm}(\mathcal{I})^{4/n^2}\cdot\sqrt{\Delta_{\mathcal{R}}^{4/n^2}}.$$

From this lemma, we immediately have $\lambda_1(\mathcal{R}) \geq n/2$. But the norm of $\zeta_n^{k_0} \in \mathcal{R}$, $0 \leq k_0 < n/2$, is $n/2$, hence we deduce that $\lambda_1(\mathcal{R}) = n/2$. Since the norm of $\zeta_n^{k_0}\sqrt[n]{2}^{k_1}$ is $2^{k_1/n}\cdot n/2$, we learn that $\lambda_{n^2/4}(\mathcal{R}) \leq \left(\sqrt{2}\right)^{1-2/n}\lambda_1(\mathcal{R})$. From this lemma, we also have $\lambda_1(\mathcal{R}^\vee) \geq \frac{n}{2}\cdot\mathrm{Nm}(\mathcal{R}^\vee)^{4/n^2}$. The norm of $\mathcal{R}^\vee$ can be computed directly from the dual basis $e_{l_0,l_1}$ (Proposition 4.2) [23, 37]. More precisely, since $(n^2/2)\cdot\mathcal{R}^\vee \subset \mathcal{R}$, the norm of $\mathcal{R}^\vee$ can be computed by [20]

$$\mathrm{Nm}\left(\mathcal{R}^\vee\right) = \mathrm{Nm}\left(\frac{n^2}{2}\cdot\mathcal{R}^\vee\right)/\mathrm{Nm}\left(\frac{n^2}{2}\right).$$

The norm $\mathrm{Nm}(n^2/2)$ of $n^2/2$ is just $(n^2/2)^{n^2/4}$ [23, 37]. The norm of $(n^2/2)\cdot\mathcal{R}^\vee$ is the number of elements of the finite group $\mathcal{R}/\left((n^2/2)\cdot\mathcal{R}^\vee\right)$, which can be directly computed from the integral basis $e_{l_0,l_1}$ of $\mathcal{R}^\vee$:

$$\left|\mathcal{R}/\left((n^2/2)\cdot\mathcal{R}^\vee\right)\right| = 2^{n/2}\cdot 2^{n(n-2)/8}.$$

Hence the norm $\mathrm{Nm}(\mathcal{R}^\vee)$ of $\mathcal{R}^\vee$ is $2^{-n(n-2)/8} \cdot (n^2/4)^{-n^2/4}$, i.e., $\Delta_{\mathcal{R}}^{-1}$, from which we immediately deduce that $\lambda_1(\mathcal{R}^\vee) \geq 2^{\frac{1}{2}+\frac{1}{n}}/n$. As the norm of $e_{l_0,n/2-1} \in \mathcal{R}^\vee$ is $2^{\frac{1}{2}+\frac{1}{n}}/n$, we must have $\lambda_1(\mathcal{R}^\vee) = 2^{\frac{1}{2}+\frac{1}{n}}/n$. Namely, $\mathcal{R}^\vee$ achieves its first minimum at the element $e_{l_0,n/2-1}$. Moreover, since the norm of $e_{l_0,0}$ is $2/n$, we have $\lambda_{n^2/4}(\mathcal{R}^\vee) \leq 2/n$.

For a general fractional ideal $\mathcal{I}$ associated with $\mathcal{R}$, suppose $v \in \mathcal{I}$ is a nonzero element at which $\mathcal{I}$ achieves its first minimum, i.e., $\|v\| = \lambda_1(\mathcal{I})$. Then the elements $(\zeta_n^{k_0} \sqrt[n]{2}^{k_1}) \cdot v$ with $0 \leq k_0, k_1 < n/2$ will be $n^2/4$ linearly independent elements of $\mathcal{I}$. From Section 3, the norm of the element $(\zeta_n^{k_0} \sqrt[n]{2}^{k_1}) \cdot v$ is $(\sqrt[n]{2})^{k_1} \cdot \|v\|$, from which we deduce

$$\lambda_1(\mathcal{I}) = \cdots = \lambda_{n/2}(\mathcal{I}) \text{ and } \lambda_{n^2/4}(\mathcal{I}) \leq \left(\sqrt{2}\right)^{1-2/n} \lambda_1(\mathcal{I}). \tag{4.1}$$

# 5 Order Learning With Errors

In this section, we first study the error distributions on the ideal lattices associated with $\mathcal{R}$. Then we formulate the Search and Average-Case Decision Order-LWE problem in $\mathcal{R}$ and study their hardness using available results in literature [4, 20].

## 5.1 Computational Problems in Lattice Theory

In lattice theory, there are several important computational problems, among which are the shortest vector problem ($\mathsf{SVP}$), the shortest independent vectors problem ($\mathsf{SIVP}$), the bounded distance decoding ($\mathsf{BDD}$) problem and the discrete Gaussian sampling ($\mathsf{DGS}$) problem. Suppose $\gamma(m) \geq 1$ is a function of $m$. The goal of $\mathsf{SVP}_\gamma$ is to find a nonzero vector with length at most $\gamma(m) \cdot \lambda_1(\mathcal{L})$. The goal of $\mathsf{SIVP}_\gamma$ is to find $m$ linearly independent lattice vectors with length at most $\gamma(m) \cdot \lambda_m(\mathcal{L})$. Given a number $0 < d < \lambda_1(\mathcal{L})/2$ and assume $\mathbf{y} \in \mathbb{R}^m$ is of the form $\mathbf{y} = \mathbf{x} + \mathbf{e}$ for some $\mathbf{x} \in \mathcal{L}$ and $||\mathbf{e}|| \leq d$, then the goal of $\mathsf{BDD}_d$ is to find $\mathbf{x}$ [20, 32].

The spherical Gaussian distribution $D_r$ with width $r$ on $\mathbb{R}^m$ is a distribution whose probability density function is proportional to $\rho_r(\mathbf{x}) = \exp\left(-\pi\|\mathbf{x}\|^2/r^2\right)$. A discrete Gaussian distribution over $\mathcal{L}$ with width $r$, denoted by $D_{\mathcal{L},r}$, is a distribution in which the probability of the event $\mathbf{x} \in \mathcal{L}$ is proportional to $\rho_r(\mathbf{x})$. Suppose $\varphi$ is a positive real-valued function defined on the set of all lattices. Given a lattice $\mathcal{L}$ and a real number $r > \varphi(\mathcal{L})$, the goal of $\mathsf{DGS}_\varphi$ is to output a sample from $D_{\mathcal{L},r}$ [20, 32].

The smoothing parameter is an important concept in lattice theory [22]. Intuitively speaking, it is the smallest positive real number $r$ starting from which the distribution $D_{\mathcal{L},r}$ behaves like a continuous Gaussian distribution [20].

**Definition 5.1.** *Given a lattice $\mathcal{L}$ and a real number $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\mathcal{L})$ is the smallest number $r > 0$ such that $\rho_{1/r}(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \epsilon$.*

From Lemmas 3.2 and 3.3 of [22], we have the following lemma [20].

**Lemma 5.2.** *For any $m$-dimensional lattice $\mathcal{L}$, we have*

$$\eta_{2^{-2m}}(\mathcal{L}) \leq \sqrt{m}/\lambda_1(\mathcal{L}^*) \text{ and } \eta_\epsilon(\mathcal{L}) \leq \sqrt{\log(m/\epsilon)}\lambda_n(\mathcal{L}) \text{ for all } 0 \leq \epsilon \leq 1.$$

The computational problems in lattice theory introduced in Section 5.1 are also defined over the special lattices that come from the fractional ideals associated with $\mathcal{R}$. For a real number $\gamma \geq 1$, the $\mathcal{R}$-$\mathsf{SVP}_\gamma$ problem is: given a fractional ideal $\mathcal{I}$, find a nonzero element $x \in \mathcal{I}$ such that $\|x\| \leq \gamma \cdot \lambda_1(\mathcal{I})$. The $\mathcal{R}$-$\mathsf{SIVP}_\gamma$ problem is: given a fractional ideal $\mathcal{I}$, find $n^2/4$ linearly independent elements in $\mathcal{I}$ with norms at most $\gamma \cdot \lambda_{n^2/4}(\mathcal{I})$. The $\mathcal{R}$-$\mathsf{BDD}_\gamma$ problem is: given a fractional ideal $\mathcal{I}$, a positive real number $d < \lambda_1(\mathcal{I})/2$ and an element $y$ of the form $y = x + e$ with $x \in \mathcal{I}$ and $\|e\| \leq d$, find $x$.

## 5.2 The Error Distributions over Ideal Lattices

An error distribution $\psi$ over the ideal lattices associated with $\mathcal{R}$ (or over $F_\mathbb{R}$) is not directly defined with respect to the naive coefficient embedding, i.e., the coefficients of an element of $F_\mathbb{R}$ with respect to the integral basis $\{\zeta_n^{k_0} \sqrt[n]{2}^{k_1} : 0 \leq k_0, k_1 < n/2\}$. Instead, $\psi$ is first defined on $H$, which then pulls back to a probability distribution on the ideal lattices under the canonical embedding $\sigma$. The readers are referred to the paper [20] for an explanation about the motivations behind this definition.

One way to define the elliptical Gaussian distributions on $H$ is through the orthonormal basis $\{\mathbf{h}_{a,b}\}_{(a,b)\in G}$ (Eq. (3.4)). Let $\mathbf{r} = (r_{a,b})_{(a,b)\in G} \in (\mathbb{R}^+)^{n^2/4}$ be a vector of positive real numbers such that $r_{a,b} = r_{((n-1)a,(n-1)b)}$ for every pair $(a,b) \in N$. Then a sample from the elliptical Gaussian distribution $D_\mathbf{r}$ is a vector $\sum_{(a,b)\in G} x_{a,b}\mathbf{h}_{a,b}$, where each $x_{a,b}$ is sampled independently from the one-dimensional Gaussian distribution $D_{r_{a,b}}$ [20].

Recall that Proposition 3.1 tells us that the canonical embedding $\sigma$ sends the integral basis $\{\zeta_n^{k_0} \sqrt[n]{2}^{k_1} : 0 \leq k_0, k_1 < n/2\}$ to an orthogonal basis of $\mathbb{C}^{n^2/4}$. Hence an elliptical Gaussian distribution on $H$ pulls back to an elliptical Gaussian distribution for the coefficient embedding. However, the norm of the basis element $\sigma\left(\zeta_n^{k_0} \sqrt[n]{2}^{k_1}\right)$ is $2^{k_1/n} \cdot n/2$, which depends on the value of $k_1$. But since $k_1 < n/2$, the ratio between the longest vector and shortest vector is smaller than $\sqrt{2}$. Therefore, there are small distortions of the elliptical Gaussian distributions under this pull-back. In particular, the pull-back of a spherical Gaussian distribution is only elliptical. This is different from the canonical embedding of the cyclotomic field case, which is an isometry up to an overall constant [20].

**Definition 5.3.** *Given a positive real number $\varrho$, let $\Psi_{\leq\varrho}$ be the set of all elliptical Gaussian distribution $D_\mathbf{r}$ over $H$ ($\cong F_\mathbb{R}$) where for every $(a,b) \in N$ we have $r_{a,b} = r_{((n-1)a,(n-1)b)}$ and $r_{a,b} \leq \varrho$.*

**Lemma 5.4.** *For any positive real number $\varrho$, the family of distributions $\Psi_{\leq\varrho}$ is closed under the action of any element of Gal$(F/\mathbb{Q})$.*

*Proof.* The action of $\sigma_{c,d} \in \mathrm{Gal}(F/\mathbb{Q})$ on $\Psi_{\leq\varrho}$ is induced by the action of $\sigma_{c,d}$ on $H$. For any distribution $D_\mathbf{r} \in \Psi_{\leq\varrho}$, let $\sigma_{c,d}(D_\mathbf{r})$ be $D_{\mathbf{r}'}$. From the commutative diagram in Eq. (3.3), $\sigma_{c,d}$ permutes the coordinates of the canonical embedding. Moreover, $\sigma_{c,d}$ preserves the complex conjugation pairs in the canonical embedding. Therefore, $r'_{a,b} = r'_{((n-1)a,(n-1)b)}$ and $(r'_{a,b})_{(a,b)\in N}$ is a permutation of $(r_{a,b})_{(a,b)\in N}$, which implies $r'_{a,b}$ is also at most $\varrho$. Hence we learn that $D_{\mathbf{r}'} \in \Psi_{\leq\varrho}$. □

The discrete Gaussian sampling problem can also be defined over $\mathcal{R}$ [33]. The $\mathcal{R}$-$\mathsf{DGS}_\gamma$ problem is: given a fractional ideal $\mathcal{I}$ associated with $\mathcal{R}$ and a number $s \geq \gamma = \gamma(\mathcal{I})$, output a sample from the distribution $D_{\mathcal{I},s}$.

**Definition 5.5.** *Given a positive real number $\delta$, $\Upsilon_\delta$ is a distribution over distributions: a sample from $\Upsilon_\delta$ is an elliptical Gaussian distribution $D_{\mathbf{r}}$ on $H$ with parameters*

$$r_{a,b}^2 = r_{(n-1)a,(n-1)b}^2 = \delta^2 \left(1 + nx_{a,b}/2\right), \ (a,b) \in N,$$

*where $x_{a,b}$ is sampled independently from the distribution $\Gamma(2,1)$.*

Recall that the probability density function for the Gamma distribution $\Gamma(2,1)$ is $x \exp(-x)$ for $x \geq 0$. The mean of $\Gamma(2,1)$ is 2, thus the noises sampled from $\Upsilon_\delta$ are of size roughly $O(\delta \cdot n^{1/2})$ when $n$ is large [20, 33].

## 5.3 The Order-LWE Problem

Given a probability distribution $\psi$, the notation $\mathbf{x} \leftarrow \psi$ means we draw a sample $\mathbf{x}$ according to $\psi$. For a finite set $\mathcal{S}$, $\mathbf{x} \leftarrow \mathcal{U}(\mathcal{S})$ means we draw a sample $\mathbf{x}$ uniformly randomly from $\mathcal{S}$. Given a positive integer $q \geq 2$, let $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$, $\mathcal{R}_q^\vee = \mathcal{R}^\vee/q\mathcal{R}^\vee$, and $\mathbb{T} = F_{\mathbb{R}}/\mathcal{R}^\vee$.

**Definition 5.6** (Order-LWE **Distribution**)**.** *Suppose we are given an element $\mathbf{s} \in \mathcal{R}_q^\vee$ (the secret key) and a noise distribution $\psi$ defined over $F_{\mathbb{R}}$. The* Order-LWE *distribution $A_{\mathbf{s},\psi}$ is defined over $\mathcal{R}_q \times \mathbb{T}$, a sample of which is generated by choosing $\mathbf{a} \leftarrow \mathcal{R}_q$ uniformly randomly and $\mathbf{e} \leftarrow \psi$ according to $\psi$, and then outputting $(\mathbf{a}, \mathbf{b} = \mathbf{a} \cdot \mathbf{s}/q + \mathbf{e} \bmod \mathcal{R}^\vee)$.*

Notice that since $\mathbf{a} \cdot \mathbf{s}/q$ is in the abelian group $q^{-1}\mathcal{R}^\vee/\mathcal{R}^\vee$, the reduction mod $\mathcal{R}^\vee$ in the second entry of the sample is well-defined.

**Definition 5.7** (Order-LWE, **Search**)**.** *Let $\Psi$ be a family of probability distributions over $F_{\mathbb{R}}$. Suppose we are given access to arbitrarily many independent samples from $A_{\mathbf{s},\psi}$ for arbitrary $\mathbf{s} \in \mathcal{R}_q^\vee$ and $\psi \in \Psi$, then the goal of the Search Order Learning With Errors problem, denoted by $\mathsf{OLWE}_{q,\Psi}$, is to find $\mathbf{s}$.*

**Definition 5.8** (Order-LWE, **Average-Case Decision**)**.** *Suppose $\Upsilon$ is a distribution over a family of error distributions over $F_{\mathbb{R}}$. The Average-Case Decision Order Learning With Errors problem, denoted by $\mathsf{DOLWE}_{q,\Upsilon}$, is to distinguish with non-negligible advantage between the following two cases*

1. *arbitrarily many independent samples from $A_{\mathbf{s},\psi}$ for a random choice of $(\mathbf{s},\psi) \leftarrow \mathcal{U}(\mathcal{R}_q^\vee) \times \Upsilon$,*

2. *the same number of uniformly random and independent samples from $\mathcal{R}_q \times \mathbb{T}$.*

As the error distribution is added modulo $\mathcal{R}^\vee$, the error must not exceed the smoothing parameter of $\mathcal{R}$. Otherwise the Order-LWE distribution is statistically indistinguishable from the uniform distribution, thus making the Order-LWE problem impossible to solve. Since $\lambda_{n^2/4}(\mathcal{R}^\vee) \leq 2/n$, Lemma 5.2 gives us an upper bound of the smoothing parameter: $O(2\sqrt{\log(n^2/4)}/n)$ [20].

On the other hand, as $\zeta_n^{n/8}+\zeta_n^{-n/8}=\sqrt{2}$ and $\zeta_n^{n/8}-\zeta_n^{-n/8}=\zeta_n^{n/4}\sqrt{2}$, from Proposition 4.2, we immediately deduce $(\sqrt{2}n^2/4)\cdot\mathcal{R}^\vee\subset\mathcal{R}$. In fact, $\sqrt{2}n^2/4$ is the smallest real number of $\mathbb{Z}[\zeta_n,\sqrt[n]{2}]$ that satisfies this property. If we instead work with the non-dual form of Order-LWE in practice, this property is helpful for choosing error distributions over $F_{\mathbb{R}}/\mathcal{R}$ [30].

## 5.4 The Reductions for Order-LWE Problem

The worst-case hardness of $\mathsf{OLWE}_{q,\Psi}$ comes from the proof of Theorem 4.1 in [20] and the paper [4].

**Proposition 5.9.** *Let $\varrho=\varrho(n^2/4)$ $(>0)$ and $q=q(n^2/4)$ be such that $\varrho q\geq 2\cdot\omega\left(\sqrt{\log(n^2/4)}\right)$. For some negligible function $\epsilon=\epsilon\left(n^2/4\right)$, there exists a probabilistic polynomial-time reduction from $\mathcal{R}$-$\mathsf{DGS}_\gamma$ to the problem $\mathsf{OLWE}_{q,\Psi_{\leq\varrho}}$, where $\gamma$ is*

$$\gamma=\max\left\{\eta_\epsilon(\mathcal{I})\cdot\left(\sqrt{2}/\varrho\right)\cdot\omega\left(\sqrt{\log(n^2/4)}\right),\sqrt{n^2/2}/\lambda_1(\mathcal{I}^\vee)\right\}.$$

Here $\omega(\sqrt{\log(n^2/4)})$ denotes a fixed but arbitrary function that grows asymptotically faster than $\sqrt{\log(n^2/4)}$. There exist reductions from the standard lattice problems to $\mathcal{R}$-$\mathsf{DGS}_\gamma$ using lattice theory [20, 33]. In particular, an oracle for $\mathcal{R}$-$\mathsf{DGS}_\gamma$ with $\gamma=\eta_\epsilon(\mathcal{I})\cdot\widetilde{O}(1/\varrho)$ implies the existence of an oracle for $\widetilde{O}(n/(2\varrho))$-approximate $\mathsf{SIVP}$ on the ideal lattices associated with $\mathcal{R}$. Moreover, from Eq. (4.1) this oracle also implies the existence of an oracle for $\widetilde{O}(n/(2\varrho))$-approximate $\mathsf{SVP}$ on the ideal lattices associated with $\mathcal{R}$. The main theorem concerning the hardness of $\mathsf{DOLWE}_{q,\Upsilon}$ is Theorem 5.10, which follows from [4, 20]. A detailed proof of this theorem is given in Appendix B.

**Theorem 5.10.** *Let $\delta<2\sqrt{\log(n^2/4)}/n$ and let $q=q(n^2)\geq 3$ be a poly$(n)$-bounded prime number such that both $X^{n/2}\equiv -1 \bmod q$ and $Y^n\equiv 2 \bmod q$ have solutions. Then there exists a polynomial-time reduction from $\widetilde{O}(n/(2\delta))$-approximate* $\mathsf{SIVP}$ *(or* $\mathsf{SVP}$*) on the ideal lattices associated with $\mathcal{R}$ to $\mathsf{DOLWE}_{q,\Upsilon_\delta}$. Moreover, for any integer $\ell\geq 1$, we can replace the target problem in the reduction with the problem of solving $\mathsf{DOLWE}_{q,D_\xi}$ given only $\ell$ samples, where $\xi=\delta\cdot\left(n^2\ell/(4\log(n^2\ell/4))\right)^{1/4}$.*

# 6 The Two-Variable Number Theoretic Transform

In this section, we design a Two-Variable Number Theoretic Transform (2NTT) for the ring

$$\mathcal{R}_p=\mathcal{R}/p\mathcal{R}=\mathbb{F}_p[X,Y]/\langle X^{n/2}+1,Y^{n/2}-(X^{n/8}-X^{3n/8})\rangle, \tag{6.1}$$

where $p$ is a prime number such that $Y^n\equiv 2 \bmod p$ has $n$ distinct solutions. The 2NTT consumes $O(n\log_2 n)$ vector operations (vector summation and scalar multiplication), thus it has an intrinsic parallel algebraic structure [19, 34]. While its twiddle factor space enjoys a quadratic saving compared to the one-variable NTT, which is perhaps the most important new feature of $\mathcal{R}$.

## 6.1 The Factorization of Polynomials over a Finite Field

We first choose a prime number $p$ such that $X^n \equiv 1 \bmod p$ has a primitive solution $\alpha \in \mathbb{F}_p$ and $Y^n \equiv 2 \bmod p$ has a solution $\beta \in \mathbb{F}_p$. Since $\alpha$ is a primitive root, we must have $\alpha^{n/2} \equiv -1 \bmod p$, thus $X^n \equiv 1 \bmod p$ has $n$ distinct solutions in $\mathbb{F}_p$: $\{\alpha^i : 0 \le i < n\}$. The $n$ distinct solutions of $Y^n \equiv 2 \bmod p$ are $\{\alpha^i \beta : 0 \le i < n\}$. Replace $\beta$ with $\alpha\beta$ if necessary, we can always assume $\beta^{n/2} \equiv \alpha^{n/8} - \alpha^{3n/8} \bmod p$. Therefore, the polynomial equations

$$X^{n/2} \equiv -1 \bmod p \text{ and } Y^{n/2} \equiv X^{n/8} - X^{3n/8} \bmod p \tag{6.2}$$

have $n^2/4$ solutions. More precisely, the first equation has $n/2$ solutions $\{\alpha^{2i+1} : 0 \le i < n/2\}$. For every solution $X = \alpha^{2i+1}$, the second equation also has $n/2$ solutions for $Y$:

$$Y = \begin{cases} \alpha^{2j}\beta, \ 0 \le j < n/2, \ \text{if } i \equiv 0, 3 \bmod 4, \\ \alpha^{2j+1}\beta, \ 0 \le j < n/2, \ \text{if } i \equiv 1, 2 \bmod 4. \end{cases}$$

## 6.2 Selecting Good Prime Numbers

We now show how to select good prime numbers such that Eq. (6.2) has $n^2/4$ solutions. For the first equation to have a solution, we must have $n|(p-1)$ [19, 34]. Then we have the following lemma.

**Lemma 6.1.** *Given a prime number $p$ that satisfies $p - 1 = n \cdot q'$, the equation $Y^n \equiv 2 \bmod p$ has a solution if $2^{q'} \equiv 1 \bmod p$.*

*Proof.* Suppose the order of 2 in $\mathbb{F}_p^\times$ is $\ell$, i.e., $\ell$ is the smallest positive integer such that

$$2^\ell \equiv 1 \bmod p.$$

Moreover, we have $\ell|(p-1)$, so let us define an integer $l' = (p-1)/\ell$. Suppose $a$ is a primitive root of the multiplicative group $\mathbb{F}_p^\times$, which always exists from elementary number theory. Then there exists a positive integer $i$ such that

$$a^i \equiv 2 \bmod p.$$

As the order of 2 is $\ell$, so we must have $(p-1)|\ell \cdot i$, i.e., $\ell'|i$. If $n|\ell'$, then $n|i$, so there exists an $n$-th root of 2 in $\mathbb{F}_p$. If $n|\ell'$, we must have $\ell|q'$, which implies $2^{q'} \equiv 1 \bmod p$. □

Moreover, to find the solutions $\alpha$ and $\beta$, we just need to use the Tonelli-Shanks algorithm recursively since $n$ is a power-of-two integer. Using this criterion, we can easily find the good prime numbers that are over 64 bits and the corresponding solutions of (6.2).

## 6.3 The One-Variable Negacyclic NTT

Let us now review the negacyclic NTT for the ring $\mathbb{F}_p[X]/\langle X^{n/2}+1 \rangle$, where $p$ is a prime number such that $X^{n/2}+1 \equiv 0 \bmod p$ has $n/2$ solutions: $\{\alpha^{2i+1} : 0 \le i < n/2\}$. Given a polynomial $\mathbf{f}(X) = \sum_{k=0}^{n/2-1} f_k X^k$ with $f_k \in \mathbb{F}_p$, the NTT of $\mathbf{f}$, denoted by $\widetilde{\mathbf{f}}$, is the evaluations of $\mathbf{f}$ at the $n/2$ solutions of $X^{n/2}+1 \equiv 0 \bmod p$:

$$\tilde{\mathbf{f}} = \big(\mathbf{f}(\alpha), \mathbf{f}(\alpha^3), \ldots, \mathbf{f}(\alpha^{n-1})\big) \in \mathbb{F}_p^{n/2}. \tag{6.3}$$

Hence we deduce that for any two polynomials $\mathbf{f}$ and $\mathbf{f}'$, $\widetilde{\mathbf{f}\cdot\mathbf{f}'} = \widetilde{\mathbf{f}} \odot \widetilde{\mathbf{f}'}$, where $\odot$ is the Hadamard product (entrywise product) of vectors.

If we naively evaluate $\mathbf{f}$ at the $n/2$ roots, then the complexity is $O(n^2)$. Luckily, there is an efficient algorithm to compute NTT with complexity $O(n\log_2 n)$: the Cooley-Tukey butterfly, which is based on the Chinese Remainder Theorem (CRT) [3, 27]. In $\mathbb{F}_p$, $X^{n/2}+1$ has a factorization $\prod_{i=0}^{n/2-1}\left(X-\alpha^{2i+1}\right)$, which induces an isomorphism [3]

$$\mathbb{F}_p[X]/\langle X^{n/2}+1\rangle \cong \prod_{i=0}^{n/2-1} \mathbb{F}_p[X]/\langle X-\alpha^{2i+1}\rangle.$$

Notice that the right hand side is isomorphic to $\mathbb{F}_p^{n/2}$. Under the CRT, a polynomial $\mathbf{f}(X)$ is sent to the vector

$$\mathbf{f}(X) \mapsto \left(\mathbf{f}(X) \bmod \left(X-\alpha^{2i+1}\right)\right)_{0\le i<n/2} = \left(\mathbf{f}(\alpha^{2i+1})\right)_{0\le i<n/2},$$

which is just the NTT of $\mathbf{f}$. The idea of the Cooley-Tukey butterfly is that CRT can be computed using a sequence of polynomial mods [27].

The butterfly consists of $\log_2(n/2)$ stages, and let us look at each stage in detail. The first stage depends on the factorization

$$X^{n/2}+1 = \left(X^{n/4}-\alpha^{n/4}\right)\left(X^{n/4}+\alpha^{n/4}\right) \bmod p,$$

from which we obtain an isomorphism

$$\mathbb{F}_p[X]/\langle X^{n/2}+1\rangle \cong \mathbb{F}_p[X]/\langle X^{n/4}-\alpha^{n/4}\rangle \times \mathbb{F}_p[X]/\langle X^{n/4}+\alpha^{n/4}\rangle.$$

The image of $\mathbf{f}$ under this isomorphism is

$$\begin{aligned} \mathbf{f}_0 = \mathbf{f} \bmod \left(X^{n/4}-\alpha^{n/4}\right) &= \sum_{k=0}^{n/4-1}\left(f_k+\alpha^{n/4}f_{k+n/4}\right)X^k,\\ \mathbf{f}_1 = \mathbf{f} \bmod \left(X^{n/4}+\alpha^{n/4}\right) &= \sum_{k=0}^{n/4-1}\left(f_k-\alpha^{n/4}f_{k+n/4}\right)X^k; \end{aligned}$$

the computation of which consumes $O(n)$ (integer) operations. In the second stage, we need the factorizations

$$\begin{aligned} X^{n/4}-\alpha^{n/4} &= \left(X^{n/8}-\alpha^{n/8}\right)\left(X^{n/8}-\alpha^{5n/8}\right) \bmod p,\\ X^{n/4}+\alpha^{n/4} &= \left(X^{n/8}-\alpha^{3n/8}\right)\left(X^{n/8}-\alpha^{7n/8}\right) \bmod p; \end{aligned}$$

which gives us isomorphisms

$$\begin{aligned} \mathbb{F}_p[X]/\langle X^{n/4}-\alpha^{n/4}\rangle &\cong \mathbb{F}_p[X]/\langle X^{n/8}-\alpha^{n/8}\rangle \times \mathbb{F}_p[X]/\langle X^{n/8}-\alpha^{5n/8}\rangle,\\ \mathbb{F}_p[X]/\langle X^{n/4}+\alpha^{n/4}\rangle &\cong \mathbb{F}_p[X]/\langle X^{n/8}-\alpha^{3n/8}\rangle \times \mathbb{F}_p[X]/\langle X^{n/8}-\alpha^{7n/8}\rangle. \end{aligned}$$

We can compute the polynomial mods from the output of the first stage:

$$\begin{aligned}
\mathbf{f}_{00} = &\quad \mathbf{f}_0 \bmod \left(X^{n/8} - \alpha^{n/8}\right) &= \quad \mathbf{f} \bmod \left(X^{n/8} - \alpha^{n/8}\right), \\
\mathbf{f}_{01} = &\quad \mathbf{f}_0 \bmod \left(X^{n/8} - \alpha^{5n/8}\right) &= \quad \mathbf{f} \bmod \left(X^{n/8} - \alpha^{5n/8}\right), \\
\mathbf{f}_{10} = &\quad \mathbf{f}_1 \bmod \left(X^{n/8} - \alpha^{3n/8}\right) &= \quad \mathbf{f} \bmod \left(X^{n/8} - \alpha^{3n/8}\right), \\
\mathbf{f}_{11} = &\quad \mathbf{f}_1 \bmod \left(X^{n/8} - \alpha^{7n/8}\right) &= \quad \mathbf{f} \bmod \left(X^{n/8} - \alpha^{7n/8}\right);
\end{aligned}$$

which also consumes $O(n)$ operations.

Continue in this way, and suppose the output of the $m$-th stage is

$$\mathbf{f} \bmod \left(X^{n/2^{m+1}} - \alpha^{(2i+1)\cdot n/2^{m+1}}\right) \text{ with } 0 \le i < 2^m.$$

For every $0 \le i < 2^m$, the polynomial $X^{n/2^{m+1}} - \alpha^{(2i+1)\cdot n/2^{m+1}}$ has a factorization

$$\left(X^{n/2^{m+2}} - \alpha^{(2i+1)\cdot n/2^{m+2}}\right) \cdot \left(X^{n/2^{m+2}} - \alpha^{(2i+1+2^{m+1})\cdot n/2^{m+2}}\right). \tag{6.4}$$

Then in the $(m+1)$-th stage we compute

$$\mathbf{f} \bmod \left(X^{n/2^{m+2}} - \alpha^{(2i+1)\cdot n/2^{m+2}}\right) \text{ with } 0 \le i < 2^{m+1}$$

using the output of the $m$-th stage, which consumes $O(n)$ operations.

The butterfly comes to an end in the $\log_2(n/2)$-th stage, the output of which is Eq. (6.3). It is important to notice that the order of the components of the output vector depends on the implementation, and in general it will not be in the order shown in Eq. (6.3). Since the complexity of each stage is $O(n)$, the total complexity of the butterfly is $O(n \log_2 n)$. Moreover, each stage of the butterfly is an invertible linear transformation. Hence if we take the inverse of each stage, we obtain INTT, whose complexity is also $O(n \log_2 n)$ [19, 34].

## 6.4 A Generalization of the One-Variable NTT

Given a prime number $p$ that satisfies the conditions in Section 6.1, we can generalize the butterfly in Section 6.3 to the ring $\mathbb{F}_p[Y]/\langle Y^{n/2} + \beta^{n/2}\rangle$. A polynomial in this ring is of the form $\mathbf{g}(Y) = \sum_{l=0}^{n/2-1} g_l Y^l$, $g_l \in \mathbb{F}_p$. In $\mathbb{F}_p$, $Y^{n/2} + \beta^n$ has a factorization

$$Y^{n/2} + \beta^{n/2} = \prod_{j=0}^{n/2-1} (Y - \alpha^{2j+1}\beta) \bmod p.$$

From the CRT [3], we have an isomorphism

$$\mathbb{F}_p[Y]/\langle Y^{n/2} + \beta^{n/2}\rangle \cong \prod_{j=0}^{n/2-1} \mathbb{F}_p[Y]/\langle Y - \alpha^{2j+1}\beta\rangle,$$

the right hand side of which is isomorphic to $\mathbb{F}_p^{n/2}$. Under the CRT, the image of $\mathbf{g}(Y)$ is

$$\mathbf{g}(Y) \mapsto \left(\mathbf{g}(Y) \bmod \left(Y - \alpha^{2j+1}\beta\right)\right)_{0 \le j < n/2} = \left(\mathbf{g}(\alpha^{2j+1}\beta)\right)_{0 \le j < n/2},$$

which is defined to be the NTT of $\mathbf{g}(Y)$. From the definition, we deduce

$$\widetilde{\mathbf{g}\cdot\mathbf{g}'} = \widetilde{\mathbf{g}} \odot \widetilde{\mathbf{g}'}.$$

The butterfly for computing the new NTT also consists of $\log_2(n/2)$ stages of polynomial mods. In the first stage, we need the factorization

$$Y^{n/2} + \beta^{n/2} = \left(Y^{n/4} - \alpha^{n/4}\beta^{n/4}\right)\left(Y^{n/4} - \alpha^{3n/4}\beta^{n/4}\right) \bmod p.$$

The output of the first stage is

$$\begin{aligned} \mathbf{g}_0 = \mathbf{g} \bmod \left(Y^{n/4} - \alpha^{n/4}\beta^{n/4}\right) &= \sum_{l=0}^{n/4-1}\left(g_l + \alpha^{n/4}\beta^{n/4}\cdot g_{l+n/4}\right)Y^l, \\ \mathbf{g}_1 = \mathbf{g} \bmod \left(Y^{n/4} - \alpha^{3n/4}\beta^{n/4}\right) &= \sum_{l=0}^{n/4-1}\left(g_l + \alpha^{3n/4}\beta^{n/4}\cdot g_{l+n/4}\right)Y^l. \end{aligned} \tag{6.5}$$

Notice that $O(n)$ operations are needed for the first stage. Suppose the output of the $m$-th stage is

$$\mathbf{g} \bmod \left(Y^{n/2^{m+1}} - \alpha^{(2j+1)\cdot n/2^{m+1}}\beta^{n/2^{m+1}}\right) \text{ with } 0 \le j < 2^m.$$

In the $(m+1)$-th stage, for every $0 \le j < 2^m$, we have a factorization

$$\begin{aligned} Y^{n/2^{m+1}} - \alpha^{(2j+1)\cdot n/2^{m+1}}\beta^{n/2^{m+1}} &= \left(Y^{n/2^{m+2}} - \alpha^{(2j+1)\cdot n/2^{m+2}}\beta^{n/2^{m+2}}\right) \\ &\cdot \left(Y^{n/2^{m+2}} - \alpha^{(2j+1+2^{m+1})\cdot n/2^{m+2}}\beta^{n/2^{m+2}}\right). \end{aligned}$$

Then we compute

$$\mathbf{g} \bmod \left(Y^{n/2^{m+2}} - \alpha^{(2j+1)\cdot n/2^{m+2}}\beta^{n/2^{m+2}}\right) \text{ with } 0 \le j < 2^{m+1}$$

using the output of the $m$-th stage, which consumes $O(n)$ operations. The algorithm comes to an end in the $\log_2(n/2)$-th stage. From an algorithmic point of view, the butterfly for this generalization is almost the same as that in Section 6.3, while the only difference is that the twiddle factors in the $m$-th stage are multiplied by an overall factor $\beta^{n/2^{m+1}}$.

At the same time, the polynomial $Y^{n/2} - \beta^{n/2}$ has a factorization

$$Y^{n/2} - \beta^{n/2} = \prod_{j=0}^{n/2-1}(Y - \alpha^{2j}\beta) \bmod p,$$

which implies

$$\mathbb{F}_p[Y]/\langle Y^{n/2} - \beta^{n/2}\rangle \cong \prod_{j=0}^{n/2-1}\mathbb{F}_p[Y]/\langle Y - \alpha^{2j}\beta\rangle.$$

Under this isomorphism, $\mathbf{h}(Y) = \sum_{l=0}^{n/2-1} h_l Y^l$ in $\mathbb{F}_p[Y]/\langle Y^{n/2} - \beta^{n/2}\rangle$ is sent to

$$\mathbf{h}(Y) \mapsto \left(\mathbf{h}(Y) \bmod \left(Y - \alpha^{2j}\beta\right)\right)_{0\le j<n/2} = \left(\mathbf{h}(\alpha^{2j}\beta)\right)_{0\le j<n/2},$$

which is defined to be the NTT of $\mathbf{h}(Y)$. From the definition, we have

$$\widetilde{\mathbf{h}\cdot\mathbf{h}'} = \widetilde{\mathbf{h}} \odot \widetilde{\mathbf{h}'}.$$

Similarly, the butterfly for computing the NTT of $\mathbf{h}(Y)$ also consists of $\log_2(n/2)$ stages. The output of the $m$-th stage is

$$\mathbf{h} \bmod \left(Y^{n/2^{m+1}} - \alpha^{j\cdot n/2^m}\beta^{n/2^{m+1}}\right) \text{ with } 0 \le j < 2^m.$$

In the $(m+1)$-th stage, for every $0 \le j < 2^m$, we have a factorization

$$\begin{aligned} Y^{n/2^{m+1}} - \alpha^{j\cdot n/2^m}\beta^{n/2^{m+1}} &= \left(Y^{n/2^{m+2}} - \alpha^{j\cdot n/2^{m+1}}\beta^{n/2^{m+2}}\right) \\ &\quad \cdot \left(Y^{n/2^{m+2}} - \alpha^{(j+2^m)\cdot n/2^{m+1}}\beta^{n/2^{m+2}}\right). \end{aligned}$$

Then we compute

$$\mathbf{h} \bmod \left(Y^{n/2^{m+2}} - \alpha^{j\cdot n/2^{m+1}}\beta^{n/2^{m+2}}\right) \text{ with } 0 \le j < 2^{m+1}$$

using the output of the $m$-th stage. Compared to the butterfly in Section 6.3, the twiddle factors in the $m$-th stage is multiplied by an overall factor $(\alpha^{-1}\beta)^{n/2^{m+1}}$.

## 6.5 The 2NTT

Now we are ready to introduce the 2NTT for the ring $\mathcal{R}_p$, where the prime number $p$ satisfies the conditions in Section 6.1. We design an efficient algorithm (vector butterfly) to compute the 2NTT (and its inverse). An element of $\mathcal{R}_p$ is of the form

$$\mathbf{F}(X,Y) = \sum_{k=0}^{n/2-1}\sum_{l=0}^{n/2-1} f_{k,l}X^kY^l \text{ with } f_{k,l} \in \mathbb{F}_p.$$

For later convenience, the $n/2\times n/2$ coefficient matrix of $\mathbf{F}(X,Y)$ is also denoted by $\mathbf{F}$:

$$\mathbf{F} = (f_{k,l})_{0\le k,l<n/2}\,.$$

**Definition 6.2.** *The 2NTT of $\mathbf{F} \in \mathcal{R}_p$, denoted by $\widetilde{\mathbf{F}}$, is the evaluation of $\mathbf{F}$ at the $n^2/4$ solutions of the two polynomial equations in Eq.* (6.2)*.*

Thus $\widetilde{\mathbf{F}}$ is an $n/2 \times n/2$ matrix with entries in $\mathbb{F}_p$. From the definition, we immediately deduce that $\widetilde{\mathbf{F}\cdot\mathbf{F}'} = \widetilde{\mathbf{F}} \odot \widetilde{\mathbf{F}'}$ for any two polynomials $\mathbf{F}$ and $\mathbf{F}'$ in $\mathcal{R}_p$, where $\odot$ is the Hadamard product (entrywise product) of two matrices. We now give an efficient butterfly algorithm to compute 2NTT, which consists of three phases: the transverse vector butterfly, transpose and the longitudinal vector butterfly.

### 6.5.1 The Transverse Vector Butterfly

Let $\mathbf{F}_{k,-}$ be the $k$-th row of the matrix $\mathbf{F}$, i.e., $\mathbf{F}_{k,-} = \left(f_{k,0},\ldots,f_{k,n/2-1}\right)$. Let $\mathbf{G}$ be a polynomial with vector-valued coefficients:

$$\mathbf{G}(X) = \sum_{k=0}^{n/2-1} X^k \cdot \mathbf{F}_{k,-}.$$

We generalize the butterfly in Section 6.3 to evaluate $\mathbf{G}$ at $X = \alpha^{2i+1}$ for $0 \le i < n/2$, which is called the transverse vector butterfly. It consists of $\log_2(n/2)$ stages and the first stage is given by

$$\begin{aligned}
\mathbf{G}_0 = \mathbf{G} \bmod \left(X^{n/4} - \alpha^{n/4}\right) &= \sum_{k=0}^{n/4-1} X^k \cdot \left(\mathbf{F}_{k,-} + \alpha^{n/4} \cdot \mathbf{F}_{k+n/4,-}\right), \\
\mathbf{G}_1 = \mathbf{G} \bmod \left(X^{n/4} + \alpha^{n/4}\right) &= \sum_{k=0}^{n/4-1} X^k \cdot \left(\mathbf{F}_{k,-} - \alpha^{n/4} \cdot \mathbf{F}_{k+n/4,-}\right).
\end{aligned}$$

Notice that the integer summation and multiplication in the negacyclic NTT in Sections 6.3 are replaced with vector summation and scalar multiplication in the transverse vector butterfly. Thus the first stage costs $O(n)$ vector operations. Similarly, the output of the second stage is

$$\begin{aligned}
\mathbf{G}_{00} &= \mathbf{G}_0 \bmod X^{n/8} - \alpha^{n/8}, & \mathbf{G}_{01} &= \mathbf{G}_0 \bmod X^{n/8} - \alpha^{5n/8}, \\
\mathbf{G}_{10} &= \mathbf{G}_1 \bmod X^{n/8} - \alpha^{3n/8}, & \mathbf{G}_{11} &= \mathbf{G}_1 \bmod X^{n/8} - \alpha^{7n/8},
\end{aligned} \tag{6.6}$$

the computation of which also costs $O(n)$ vector operations. We can continue in the same way as the negacyclic NTT in Section 6.3. Suppose the output of the $m$-th stage is

$$\mathbf{G}(X) \bmod \left(X^{n/2^{m+1}} - \alpha^{(2i+1)\cdot n/2^{m+1}}\right) \text{ with } 0 \le i < 2^m.$$

Then in the $(m+1)$-th stage we compute

$$\mathbf{G}(X) \bmod \left(X^{n/2^{m+2}} - \alpha^{(2i+1)\cdot n/2^{m+2}}\right) \text{ with } 0 \le i < 2^{m+1}$$

using the factorization in Eq. (6.4) and the output of the $m$-th stage, which consumes $O(n)$ vector operations. The transverse vector butterfly comes to an end in the $\log_2(n/2)$-th stage, the output of which are $n/2$ vectors of length $n/2$:

$$\mathbf{G}(X) \bmod \left(X - \alpha^{2i+1}\right) = \mathbf{G}(\alpha^{2i+1}) \in \mathbb{F}_p^{n/2} \text{ with } 0 \le i < n/2.$$

The order of the $n/2$ output vectors depends on the implementation of the algorithm, which is similar to the negacyclic NTT in Section 6.3. Each stage costs $O(n)$ vector operations, so in total the transverse vector butterfly costs $O\left(n \log_2 n\right)$ vector operations.

### 6.5.2 The Transpose

The output vectors of the transverse vector butterfly fall into four groups:

1. $\mathbf{B}_{00}$, whose rows are vectors of the form $\mathbf{G}(\alpha^{2i+1})$ with $i = 0 \bmod 4$. It comes from the branch $\mathbf{G}_{00}$ in Eq. (6.6).
2. $\mathbf{B}_{01}$, whose rows are vectors of the form $\mathbf{G}(\alpha^{2i+1})$ with $i = 2 \bmod 4$. It comes from the branch $\mathbf{G}_{01}$ in Eq. (6.6).
3. $\mathbf{B}_{10}$, whose rows are vectors of the form $\mathbf{G}(\alpha^{2i+1})$ with $i = 1 \bmod 4$. It comes from the branch $\mathbf{G}_{10}$ in Eq. (6.6).

4. $\mathbf{B}_{11}$, whose rows are vectors of the form $\mathbf{G}(\alpha^{2i+1})$ with $i = 3 \bmod 4$. It comes from the branch $\mathbf{G}_{11}$ in Eq. (6.6).

Notice that each of $\mathbf{B}_{00}$, $\mathbf{B}_{01}$, $\mathbf{B}_{10}$ and $\mathbf{B}_{11}$ is an $n/8 \times n/2$ matrix. The concatenations of these four matrices give us two $n/4 \times n/2$ matrices:

$$\mathbf{C}' = \begin{pmatrix} \mathbf{B}_{00} \\ \mathbf{B}_{11} \end{pmatrix}, \quad \mathbf{C}'' = \begin{pmatrix} \mathbf{B}_{01} \\ \mathbf{B}_{10} \end{pmatrix}.$$

The $l$-th column of $\mathbf{C}'$ (resp. $\mathbf{C}''$) is denoted by $\mathbf{C}'_{-,l}$ (resp. $\mathbf{C}''_{-,l}$), which is a column vector of length $n/4$. Define polynomials (with vector-valued coefficients) $\mathbf{H}'$ and $\mathbf{H}''$ to be

$$\mathbf{H}'(Y) = \sum_{l=0}^{n/2-1} \mathbf{C}'_{-,l} Y^l \text{ and } \mathbf{H}''(Y) = \sum_{l=0}^{n/2-1} \mathbf{C}''_{-,l} Y^l.$$

### 6.5.3 The Longitudinal Vector Butterfly

Now comes the longitudinal vector butterfly. For the polynomial $\mathbf{H}'(Y)$, we need to evaluate it at the roots $Y = \alpha^{2j}\beta$ with $0 \le j < n/2$. The vector butterfly for this evaluation is a vector version of the butterfly in Section 6.4, which costs $O(n \log_2 n)$ vector operations. The output are $n/2$ vectors with length $n/4$, which form an $n/4 \times n/2$ matrix $\widetilde{\mathbf{F}}_{\text{even}}$.

For the polynomial $\mathbf{H}''(Y)$, we need to evaluate it at the roots $Y = \alpha^{2j+1}\beta$ with $0 \le j < n/2$. The vector butterfly for this evaluation is also a vector version of butterfly in Section 6.4, which costs $O(n \log_2 n)$ vector operations. The output are also $n/2$ vectors with length $n/4$, which form another $n/4 \times n/2$ matrix $\widetilde{\mathbf{F}}_{\text{odd}}$.

The output of the 2NTT of $\mathbf{F}$ is the concatenation

$$\widetilde{\mathbf{F}} = \begin{pmatrix} \widetilde{\mathbf{F}}_{\text{even}} \\ \widetilde{\mathbf{F}}_{\text{odd}} \end{pmatrix},$$

which is an $n/2 \times n/2$ matrix with entries in $\mathbb{F}_p$. The vector butterfly algorithm costs $O(n \log_2 n)$ vector operations (plus transposes). Each stage in the transverse and longitudinal vector butterflies is invertible, hence the inverse of 2NTT, denoted by 2INTT, can be constructed by inverting each stage of the 2NTT, whose complexity is the same as 2NTT.

## 6.6 The Advantages of 2NTT

From the analysis in Section 5, the Order-LWE in $\mathcal{R}$ offers the same security level as the RLWE in $\mathbb{Z}[X]/\langle X^{n^2/4} + 1\rangle$ [20]. Therefore, a natural comparison is between the new ring $\mathcal{R}$ and $\mathbb{Z}[X]/\langle X^{n^2/4} + 1\rangle$. Perhaps the most important comparison now is between the performances of the 2NTT of $\mathcal{R}$ and the NTT of $\mathbb{Z}[X]/\langle X^{n^2/4} + 1\rangle$. Both the 2NTT and NTT consist of $\log_2\left(n^2/4\right)$ stages, and the computational complexity of each stage is the same. Therefore, the computational complexity of 2NTT is the same as the one-variable NTT.

Let us now briefly discuss the differences and advantages of 2NTT. First, for negacyclic NTT, we need prime numbers such that

$$X^{n^2/4} + 1 \equiv 0 \bmod p' \tag{6.7}$$

has $n^2/4$ solutions. While for 2NTT, we need prime numbers such that $Y^n \equiv 2 \bmod p$ has $n$ solutions, which are (generally) different from the negacyclic NTT case. As a result, $\mathcal{R}$ provides a new set of prime numbers to practitioners when designing cryptographic schemes.

The most important advantage of 2NTT is that it enjoys a quadratic saving of twiddle factors. The space of the twiddle factors of the negacyclic NTT is $O(n^2/4)$, which essentially come from the $n^2/4$ solutions of Eq. (6.7). The space of the twiddle factors of 2NTT is only $O(n)$, which essentially come from the solutions of $X^{n/2} \equiv -1 \bmod p$ and $Y^n \equiv 2 \bmod p$ ($3n/2$ in total). Thus, there is a quadratic saving of twiddle factor space, which is especially desirable for large polynomials. This saving offers new possibilities for optimizations in practical implementations of 2NTT on platforms such as GPU and FPGA.

# 7 A New Variant of CKKS

As an important application of the Order-LWE in $\mathcal{R}$ that we have developed so far, we show how to construct a new variant of CKKS [10, 11]. In particular, we give the constructions of a new decoding and encoding map for $\mathcal{R}$, based on which we study the actions of the Galois group $\mathrm{Gal}\,(F/\mathbb{Q})$ in this variant. At last, we show that this new variant is bootstrappable by adapting the method in the paper [10]. As a result, this new variant is in fact a Fully Homomorphic Encryption (FHE) scheme.

## 7.1 The Decoding and Encoding Maps

The plaintext space of this new variant is the ring $\mathcal{R}$, thus a plaintext is a two-variable polynomial of the form

$$\mathbf{M}(X,Y) = \sum_{i=0}^{n/2-1} \sum_{i=0}^{n/2-1} m_{i,j} X^i Y^j \text{ where } m_{ij} \in \mathbb{Z}.$$

The coefficients of $\mathbf{M}(X,Y)$ naturally form an $n/2 \times n/2$ matrix that is also denoted by $\mathbf{M}$, i.e., $\mathbf{M} = (m_{i,j})_{0 \le i,j < n/2-1} \in \mathbb{Z}^{n/2 \times n/2}$.

Under the canonical embedding $\sigma$ in Eq. (3.1), a polynomial $\mathbf{M}$ is sent to its evaluations at all the root-pairs $\left(X = \zeta_n^a,\ Y = \zeta_n^b \sqrt[n]{2}\right)$ where $(a,b) \in G$. The decoding map is essentially the canonical embedding, except that since the coefficients of $\mathbf{M}$ are integers, we only need to consider the evaluation of $\mathbf{M}$ at $\left(X = \zeta_n^a,\ Y = \zeta_n^b \sqrt[n]{2}\right)$ where $(a,b) \in N$. Namely, the evaluation of $\mathbf{M}$ at the half of root-pairs that come from $N$, while the evaluation of $\mathbf{M}$ at the other half is determined by the complex conjugation of the first half, which is similar to CKKS [11].

From Section 2.3, any element of $\{\sigma_{a,b} : (a,b) \in N\}$ can be uniquely written as $\sigma_{5,1}^i \circ \sigma_{1,2}^j$ with $0 \le i < n/4$ and $0 \le j < n/2$. Therefore, we let the decoding of $\mathbf{M}$ to be the matrix $\mathbf{z} = (z_{i,j}) \in \mathbb{C}^{n/4 \times n/2}$ where $z_{i,j}$ is the evaluation $\mathbf{M}$ at

$$X = \sigma_{5,1}^i \circ \sigma_{1,2}^j(\zeta_n) = \zeta_n^{5^i} \text{ and } Y = \sigma_{5,1}^i \circ \sigma_{1,2}^j(\sqrt[n]{2}) = \zeta_n^{2j\cdot 5^i + (5^i-1)/4} \sqrt[n]{2}.$$

More explicitly, $z_{i,j}$ is given by

$$z_{i,j} = \mathbf{M}(\zeta_n^{5^i}, \zeta_n^{2j\cdot 5^i + (5^i-1)/4} \sqrt[n]{2}) \text{ where } 0 \le i < n/4 \text{ and } 0 \le j < n/2.$$

By abuse of notations, we will also use $\sigma$ to denote this decoding map:

$$\sigma : \mathbf{M} \in \mathcal{R} \mapsto \mathbf{z} = (z_{i,j}) \in \mathbb{C}^{n/4 \times n/2}. \tag{7.1}$$

Moreover, we will also follow CKKS and introduce a scale $\Delta$ to control the errors of the encoding and decoding process [11]. Therefore, the decoding map is modified to

$$\mathbf{z} = \mathbf{Dcd}(\mathbf{M}, \Delta) = \Delta^{-1} \cdot \sigma(\mathbf{M}).$$

The encoding map is given by the inverse of $\sigma$:

$$\mathbf{M} = \mathbf{Ecd}(\mathbf{z}, \Delta) = \lfloor \sigma^{-1}(\Delta \cdot \mathbf{z}) \rceil,$$

which can be directly computed by using linear algebra. Here $\lfloor \cdot \rceil$ denotes the rounding of a number to the nearest integer, and rounds upward in case of a tie.

## 7.2 The Actions of the Galois Group

From Section 2.3, there exists an action of the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ on $\mathcal{R}$ via

$$\sigma_{a,b}(X) = X^a \text{ and } \sigma_{a,b}(Y) = X^b \cdot Y, \ \forall \sigma_{a,b} \in \mathrm{Gal}(F/\mathbb{Q}).$$

For a polynomial $\mathbf{M} \in \mathcal{R}$, we immediately deduce that

$$\begin{gathered} \sigma_{a,b} \circ \sigma_{c,d} (\mathbf{M}) = \sigma_{a,b}(\sigma_{c,d}(\mathbf{M})), \\ \sigma_{c,d}(\mathbf{M})(\sigma_{a,b}(\zeta_n), \sigma_{a,b}(\sqrt[n]{2})) = \mathbf{M}(\sigma_{a,b} \circ \sigma_{c,d}(\zeta_n), \sigma_{a,b} \circ \sigma_{c,d}(\sqrt[n]{2})). \end{gathered}$$

Let us now explicitly look at the "geometric" meaning of the action of $\mathrm{Gal}(F/\mathbb{Q})$. Suppose $\mathbf{M}$ is the encoding of a matrix $\mathbf{z} = (z_{i,j}) \in \mathbb{C}^{n/4 \times n/2}$, then the decoding of $\sigma_{a,b}(\mathbf{M})$ is given by

$$\begin{aligned} &\sigma_{a,b}(\mathbf{M}) \left( \sigma_{5,1}^i \circ \sigma_{1,2}^j(\zeta_n), \sigma_{5,1}^i \circ \sigma_{1,2}^j(\sqrt[n]{2}) \right) \\ &\qquad = \mathbf{M} \left( \sigma_{5,1}^i \circ \sigma_{1,2}^j \circ \sigma_{a,b}(\zeta_n), \sigma_{5,1}^i \circ \sigma_{1,2}^j \circ \sigma_{a,b}(\sqrt[n]{2}) \right). \end{aligned} \tag{7.2}$$

From Section 2.3, $\mathrm{Gal}(F/\mathbb{Q})$ can be generated by three elements: $\sigma_{1,2}$, $\sigma_{5,1}$ and $\sigma_{n-1,0}$, thus we only need to understand the geometric meanings of the actions of these three elements. The action of $\sigma_{1,2}$ is straightforward. From Eq. (7.2), the evaluation of $\sigma_{1,2}(\mathbf{M})$ at $X = \sigma_{5,1}^i \circ \sigma_{1,2}^j(\zeta_n)$ and $Y = \sigma_{5,1}^i \circ \sigma_{1,2}^j(\sqrt[n]{2})$ is

$$\mathbf{M} \left( \sigma_{5,1}^i \circ \sigma_{1,2}^{j+1}(\zeta_n), \sigma_{5,1}^i \circ \sigma_{1,2}^{j+1}(\sqrt[n]{2}) \right).$$

So the decoding of $\sigma_{1,2}(\mathbf{M})$ is $\mathbf{z}' = \left( z'_{i,j} \right) \in \mathbb{C}^{n/2 \times n/4}$ with $z'_{i,j} = z_{i,j+1}$. Therefore, $\sigma_{1,2}$ induces a rotation of the columns of the matrix $\mathbf{z}$.

To understand the action of $\sigma_{5,1}$ on $\mathbf{z}$, we will need the relations $\sigma_{5,1}^{n/4} = \sigma_{1,2}^{3n/8}$ and $\sigma_{1,2}^{n/2} = \sigma_{1,0}$. So we immediately learn that the action of $\sigma_{5,1}^{n/4}$ is the same as that of $\sigma_{1,2}^{3n/8}$, i.e., the effect of $\sigma_{5,1}$ repeatedly acting on a data point $\mathbf{z}$ $n/4$ times is the same as $3n/8$ rotations of columns. To proceed, we also need Eq. (2.10), which implies

$$\sigma_{5,1}^i \circ \sigma_{1,2}^j \circ \sigma_{5,1} = \sigma_{5,1}^{i+1} \circ \sigma_{1,2}^{j/5}.$$

Hence together with Eq. (7.2), we learn that the evaluation of $\sigma_{5,1}(\mathbf{M})$ at $X = \sigma_{5,1}^{i} \circ \sigma_{1,2}^{j}(\zeta_n)$ and $Y = \sigma_{5,1}^{i} \circ \sigma_{1,2}^{j}(\sqrt[n]{2})$ is given by

$$\mathbf{M}\left(\sigma_{5,1}^{i+1} \circ \sigma_{1,2}^{j/5}(\zeta_n), \sigma_{5,1}^{i+1} \circ \sigma_{1,2}^{j/5}(\sqrt[n]{2})\right).$$

Thus $\sigma_{5,1}(\mathbf{M})$ decodes to a matrix $\mathbf{z}'' = \left(z''_{i,j}\right) \in \mathbb{C}^{n/4 \times n/2}$ such that

$$z''_{i,j} = \begin{cases} z_{i+1,j/5}, & \text{if } i < n/4 - 1, \\ z_{0,j/5+3n/8}, & \text{if } i = n/4 - 1. \end{cases}$$

Besides rotating the rows, $\sigma_{5,1}$ also permutes the entries of each row at the same time.

To understand the effect of $\sigma_{n-1,0}$, we will need Eq. (2.11), from which we deduce that

$$\sigma_{5,1}^{i} \circ \sigma_{1,2}^{j} \circ \sigma_{n-1,0} = \sigma_{n-1,0} \circ \sigma_{5,1}^{i} \circ \sigma_{1,2}^{-j-(1-1/5^i)/4}.$$

Notice that here an inverse is computed modulo $n/2$, the order of $\sigma_{1,2}$. Together with Eq. (7.2), we learn that the evaluation of $\sigma_{n-1,0}(\mathbf{M})$ at $X = \sigma_{5,1}^{i} \circ \sigma_{1,2}^{j}(\zeta_n)$ and $Y = \sigma_{5,1}^{i} \circ \sigma_{1,2}^{j}(\sqrt[n]{2})$ is the complex conjugation of

$$\mathbf{M}\left(\sigma_{5,1}^{i} \circ \sigma_{1,2}^{-j-(1-1/5^i)/4}(\zeta_n), \sigma_{5,1}^{i} \circ \sigma_{1,2}^{-j-(1-1/5^i)/4}(\sqrt[n]{2})\right),$$

where we have used the property that $\sigma_{n-1,0}$ is the complex conjugation. Thus $\sigma_{n-1,0}(\mathbf{M})$ decodes to $\mathbf{z}^c = \left(z^c_{i,j}\right)$ where $z^c_{i,j} = \overline{z}_{i,-j-(1-1/5^i)/4}$.

## 7.3 The New Variant is Bootstrappable

We now show that this new variant of CKKS is bootstrappable using the method in [10]. The process consists of five steps: 1, Modulus Raising; 2, Putting polynomial coefficients into plaintext slots; 3, Evaluation of the complex exponential function; 4, Extraction of the imaginary part ; 5, Switching back to the coefficient representation. The steps 1, 3 and 4 are exactly the same as in [10], hence will not be discussed here. So we only need to show how to construct a new Coefficients-to-Slots map, whose inverse gives us step 5. Let us first introduce a linear algebra trick.

Suppose $m$ is a positive integer, $\mathbf{A} = (a_{i,j})_{0 \le i,j < m}$ is an $m \times m$ matrix, and $\mathbf{x} = (x_i)_{0 \le i < m}$ is a column vector. Suppose we have $m$ distinct permutations $\sigma_i$, $0 \le i < m$, of $\{0, 1, \ldots, m-1\}$, where $\sigma_0$ is the identity. We further assume that for every $0 \le j < m$, $(\sigma_0(j), \sigma_1(j), \ldots, \sigma_{m-1}(j))$ is also a permutation of $\{0, 1, \cdots, m-1\}$. Let $\sigma_i(\mathbf{x})$ be the column vector $\left(x_{\sigma_i(0)}, x_{\sigma_i(1)}, \ldots, x_{\sigma_i(m-1)}\right)$ and let $\mathbf{u}_i$ be the column vector $\left(a_{0,\sigma_i(0)}, a_{1,\sigma_i(1)}, \ldots, a_{m-1,\sigma_i(m-1)}\right)$. Then a quick computation shows $\mathbf{A} \cdot \mathbf{x} = \sum_{i=0}^{m-1} \mathbf{u}_i \odot \sigma_i(\mathbf{x})$.

On the other hand, a real linear map from $\mathbb{C}^m$ to $\mathbb{R}^m$ is always of the form $\mathbf{A} \cdot \mathbf{x} + \overline{\mathbf{A}} \cdot \overline{\mathbf{x}}$, where $\mathbf{A}$ is a complex matrix and $\mathbf{x} \in \mathbb{C}^m$ [10]. To be relevant to this paper, we look at the case where there is a further permutation of the coordinates of $\overline{\mathbf{x}}$ represented by a matrix $\mathbf{S}$. Now, the linear transformation becomes $\mathbf{A} \cdot \mathbf{x} + \overline{\mathbf{A}} \cdot \mathbf{S}^{-1} \cdot (\mathbf{S}\overline{\mathbf{x}})$, which can always be written into

$$\mathbf{A} \cdot \mathbf{x} + \overline{\mathbf{A}} \cdot \mathbf{S}^{-1} \cdot (\mathbf{S}\overline{\mathbf{x}}) = \sum_{i=0}^{m-1} \mathbf{u}_i \odot \sigma_i(\mathbf{x}) + \sum_{i=0}^{m-1} \mathbf{u}'_i \odot \sigma_i(\mathbf{S}\overline{\mathbf{x}}),$$

where the new vector $\mathbf{u}'_i$ depends on $\overline{\mathbf{A}}$, $\mathbf{S}$ and $\sigma_i$.

Now, we are ready to construct the Coefficients-to-Slots map in Step 2 for the ring $\mathcal{R}$. Notice that the encoding map is a real linear map $\sigma^{-1} : \mathbb{C}^{n/4\times n/2} \to \mathbb{R}^{n/2\times n/2}$, i.e., it linearly maps a complex matrix $(z_{i,j}) \in \mathbb{C}^{n/4\times n/2}$ to a real coefficient matrix $\mathbf{M} \in \mathbb{R}^{n/2\times n/2}$. Let us now define two projection maps $\mathbf{P}_0, \mathbf{P}_1$ from $\mathbb{R}^{n/2\times n/2}$ to $\mathbb{R}^{n/4\times n/2}$ such that $\mathbf{P}_0$ (resp. $\mathbf{P}_1$) projects $\mathbf{M}$ to its upper half (resp. lower half). Then both $\mathbf{P}_0 \circ \sigma^{-1}$ and $\mathbf{P}_1 \circ \sigma^{-1}$ are real linear maps from $\mathbb{C}^{n/4\times n/2}$ to $\mathbb{R}^{n/4\times n/2}$.

Suppose $\mathbf{M}$ decodes to $\mathbf{z} = (z_{i,j}) \in \mathbb{C}^{n/4\times n/2}$, then we define $\sigma_{a,b}(\mathbf{z})$ to be the decoding of $\sigma_{a,b}(\mathbf{M})$. From the properties of $\mathrm{Gal}(F/\mathbb{Q})$, we learn that $\{\sigma_{a,b} : (a,b) \in N\}$ give us permutations of $\mathbf{z} = (z_{i,j})$ that satisfy the condition in the previous paragraphs. (Of course, we first need to flatten $(z_{i,j})$ to a column vector.) We immediately deduce that for every pair $(a,b) \in N$, there exist $n/4 \times n/2$ complex matrices $\mathbf{U}^0_{a,b}$, $\mathbf{U}'^0_{a,b}$, $\mathbf{U}^1_{a,b}$, $\mathbf{U}'^1_{a,b}$ such that

$$\mathbf{M}_0 = \mathbf{P}_0 \circ \sigma^{-1}(\mathbf{z}) = \sum_{(a,b)\in N} \left(\mathbf{U}^0_{a,b} \odot \sigma_{a,b}(\mathbf{z}) + \mathbf{U}'^0_{a,b} \odot \sigma_{a,b}(\sigma_{n-1,0}(\mathbf{z}))\right),$$

$$\mathbf{M}_1 = \mathbf{P}_1 \circ \sigma^{-1}(\mathbf{z}) = \sum_{(a,b)\in N} \left(\mathbf{U}^1_{a,b} \odot \sigma_{a,b}(\mathbf{z}) + \mathbf{U}'^1_{a,b} \odot \sigma_{a,b}(\sigma_{n-1,0}(\mathbf{z}))\right).$$

These matrices can be computed by brute force. The encoding of these two equations give us

$$\sigma^{-1}(\mathbf{M}_0) = \sum_{(a,b)\in N} \left(\sigma^{-1}\left(\mathbf{U}^0_{a,b}\right) \cdot \sigma_{a,b}(\mathbf{M}) + \sigma^{-1}\left(\mathbf{U}'^0_{a,b}\right) \cdot \sigma_{a,b} \circ \sigma_{n-1,0}(\mathbf{M})\right),$$

$$\sigma^{-1}(\mathbf{M}_1) = \sum_{(a,b)\in N} \left(\sigma^{-1}\left(\mathbf{U}^1_{a,b}\right) \cdot \sigma_{a,b}(\mathbf{M}) + \sigma^{-1}\left(\mathbf{U}'^1_{a,b}\right) \cdot \sigma_{a,b} \circ \sigma_{n-1,0}(\mathbf{M})\right),$$

which gives us the Coefficients-to-Slots map for the new ring $\mathcal{R}$. In conclusion, the new variant is bootstrappable.

# A The Proofs of Number Theoretic Results

In this section, we present the proofs of Proposition 3.1 and Theorem 4.1. The proof of Proposition 3.1 is as follows.

*Proof.* From the construction of $\sigma$, we immediately have

$$\left\langle \sigma\left(\zeta_n^{k_0}\sqrt[n]{2}^{k_1}\right), \sigma\left(\zeta_n^{l_0}\sqrt[n]{2}^{l_1}\right)\right\rangle = \left(\sqrt[n]{2}\right)^{k_1+l_1} \cdot \sum_{(a,b)\in G} \zeta_n^{a(k_0-l_0)+b(k_1-l_1)}. \tag{A.1}$$

If $a \equiv 1, 7 \bmod 8$, then $b$ is even, i.e., $b = 2i$ with $0 \le i < n/2$. In this case, keep the value of $a$ fixed and let us look at the partial sum

$$\sum_{i=0}^{n/2-1} \zeta_n^{a(k_0-l_0)+2i(k_1-l_1)} = \zeta_n^{a(k_0-l_0)} \sum_{i=0}^{n/2-1} \zeta_n^{2i(k_1-l_1)}, \tag{A.2}$$

which is 0 unless $\zeta_n^{2(k_1-l_1)} = 1$. Since both $0 \le k_1 < n/2$ and $0 \le l_1 < n/2$, we have $-n/2 < k_1 - l_1 < n/2$, from which we deduce that $\zeta_n^{2(k_1-l_1)} = 1$ if and only if $k_1 = l_1$. Therefore, Eq. (A.2) is equal to 0 unless $k_1 = l_1$. Similarly, if $a \equiv 3, 5 \bmod 8$, then $b = 2i + 1$ with $0 \le i < n/2$. In this case, keep the value of $a$ fixed and let us look at the partial sum

$$\sum_{i=0}^{n/2-1} \zeta_n^{a(k_0-l_0)+(2i+1)(k_1-l_1)} = \zeta_n^{a(k_0-l_0)+(k_1-l_1)} \sum_{i=0}^{n/2-1} \zeta_n^{2i(k_1-l_1)},$$

which again is equal to 0 unless $k_1 = l_1$. Therefore, Eq. (A.1) is always equal to 0 unless $k_1 = l_1$. Now assume $k_1 = l_1$, then Eq. (A.1) becomes

$$\left(\sqrt[n]{2}\right)^{2k_1} \cdot \sum_{(a,b)\in G} \zeta_n^{a(k_0-l_0)} = \frac{n}{2} \cdot \left(\sqrt[n]{2}\right)^{2k_1} \sum_{i=0}^{n/2-1} \zeta_n^{(2i+1)(k_0-l_0)}. \qquad (A.3)$$

Similarly, since $-n/2 < k_0 - l_0 < n/2$, Eq. (A.3) is equal to 0 unless $k_0 = l_0$. When both $k_0 = l_0$ and $k_1 = l_1$, Eq. (A.1) is equal to $\left(\sqrt[n]{2}\right)^{2k_1} \cdot n^2/4$. □

The proof of Theorem 4.1 is divided into the following three lemmas.

**Lemma A.1.** *If $k_1 + l_1 \neq 0$ or $n/2$, then $Tr(\zeta_n^{k_0+l_0} \sqrt[n]{2}^{k_1+l_1}) = 0$.*

*Proof.* The finite set $G$ can be expressed as a disjoint union

$$G = H_1 \cup H_3 \cup H_5 \cup \cdots \cup H_{n-1},$$

where each subset $H_a$ is

$$H_a = \begin{cases} \{(a,0),(a,2),(a,4),\ldots,(a,n-2)\}, & \text{if } a \equiv 1,7 \bmod 8, \\ \{(a,1),(a,3),(a,5),\ldots,(a,n-1)\}, & \text{if } a \equiv 3,5 \bmod 8. \end{cases}$$

The trace $\mathrm{Tr}(\zeta_n^{k_0+l_0} \sqrt[n]{2}^{k_1+l_1})$ can be computed by

$$\mathrm{Tr}(\zeta_n^{k_0+l_0} \sqrt[n]{2}^{k_1+l_1}) = \sum_{a \text{ odd}} \sum_{(a,b)\in H_a} \sigma_{a,b}(\zeta_n^{k_0+l_0} \sqrt[n]{2}^{k_1+l_1}). \qquad (A.4)$$

If $a = 1, 7 \bmod 8$, the inner layer of the sum in Eq. (A.4) becomes

$$\sum_{(a,b)\in H_a} \sigma_{a,b}(\zeta_n^{k_0+l_0} \sqrt[n]{2}^{k_1+l_1}) = \zeta_n^{a(k_0+l_0)} (\sqrt[n]{2})^{k_1+l_1} \sum_{i=0}^{n/2-1} \zeta_n^{2i(k_1+l_1)}.$$

Hence this sum must be 0 unless $\zeta_n^{2(k_1+l_1)} = 1$, i.e., $k_1 + l_1 = 0, n/2$. Similarly, if $a = 3, 5 \bmod 8$, the inner layer of the sum in Eq. (A.4) becomes

$$\sum_{(a,b)\in H_a} \sigma_{a,b}(\zeta_n^{k_0+l_0} \sqrt[n]{2}^{k_1+l_1}) = \zeta_n^{a(k_0+l_0)} (\sqrt[n]{2})^{k_1+l_1} \sum_{i=0}^{n/2-1} \zeta_n^{(2i+1)(k_1+l_1)}.$$

Again it must be 0 unless $\zeta_n^{2(k_1+l_1)} = 1$, i.e., $k_1 + l_1 = 0,\ n/2$. Combine the two cases we proves this lemma. □

**Lemma A.2.** *$Tr(\zeta_n^{k_0+l_0}) = 0$ unless $k_0 = l_0 = 0$ or $k_0 + l_0 = n/2$. If so, we trivially have $Tr(1) = n^2/4$ and $Tr(-1) = -n^2/4$.*

*Proof.* From the proof of Lemma A.1, we obtain

$$\sum_{(a,b)\in H_a} \sigma_{a,b}(\zeta_n^{k_0+l_0}) = \frac{n}{2}\zeta_n^{a(k_0+l_0)}.$$

Therefore, the trace $\mathrm{Tr}(\zeta_n^{k_0+l_0})$ becomes

$$\mathrm{Tr}(\zeta_n^{k_0+l_0}) = \sum_{a \text{ odd}} \frac{n}{2}\zeta_n^{a(k_0+l_0)} = \frac{n}{2}\cdot \sum_{i=0}^{n/2-1} \zeta_n^{(2i+1)(k_0+l_0)},$$

which is 0 unless $k_0+l_0=0$ (i.e., $k_0=l_0=0$) or $k_0+l_0=n/2$. If $k_0=l_0=0$, $\mathrm{Tr}(1)$ is just the order of $G$, i.e., $n^2/4$. If $k_0+l_0=n/2$, then $\mathrm{Tr}(\zeta_n^{k_0+l_0})$ is just $\mathrm{Tr}(-1)=-n^2/4$. □

**Lemma A.3.**

$$Tr(\zeta_n^{k_0+l_0}\sqrt[n]{2}^{n/2}) = \begin{cases} n^2/4, & \textit{if } k_0+l_0=n/8 \textit{ or } 7n/8, \\ -n^2/4, & \textit{if } k_0+l_0=3n/8 \textit{ or } 5n/8, \\ 0, & \textit{otherwise.} \end{cases}$$

*Proof.* For each $b \in \mathbb{Z}_n$, let the subset $H'_b$ of $G$ be defined as

$$H'_b = \begin{cases} \{(a,b) : a \equiv 1,7 \bmod 8\}, & \text{if } b \text{ is even;} \\ \{(a,b) : a \equiv 3,5 \bmod 8\}, & \text{if } b \text{ is odd.} \end{cases}$$

Therefore $G$ is equal to the disjoint union $\cup_{b=0}^{n-1} H'_b$, so the trace can be computed via

$$\mathrm{Tr}(\zeta_n^{k_0+l_0}\sqrt[n]{2}^{n/2}) = \sum_{b=0}^{n-1}\sum_{(a,b)\in H'_b} \sigma_{a,b}(\zeta_n^{k_0+l_0}\sqrt[n]{2}^{n/2}). \tag{A.5}$$

When $b$ is even, we have

$$\sum_{(a,b)\in H'_b} \sigma_{a,b}(\zeta_n^{k_0+l_0}\sqrt[n]{2}^{n/2}) = \sqrt{2}\cdot\left(\zeta_n^{k_0+l_0} + \zeta_n^{7(k_0+l_0)}\right)\sum_{i=0}^{n/8-1}\zeta_n^{8i(k_0+l_0)}.$$

Similarly, when $b$ is odd, we have

$$\sum_{(a,b)\in H'_b} \sigma_{a,b}(\zeta_n^{k_0+l_0}\sqrt[n]{2}^{n/2}) = -\sqrt{2}\cdot\left(\zeta_n^{3(k_0+l_0)} + \zeta_n^{5(k_0+l_0)}\right)\sum_{i=0}^{n/8-1}\zeta_n^{8i(k_0+l_0)}.$$

Both equations are 0 unless $\zeta_n^{8(k_0+l_0)} = 1$, i.e., $k_0+l_0 = jn/8$ with $j = 0,1,2,\ldots,7$. In these cases, we have

$$\mathrm{Tr}(\zeta_n^{jn/8}\sqrt[n]{2}^{n/2}) = \frac{\sqrt{2}n^2}{16}\left(\zeta_n^{jn/8} - \zeta_n^{3jn/8} - \zeta_n^{5jn/8} + \zeta_n^{7jn/8}\right),$$

whose value can be easily computed for different $j$:

$$\mathrm{Tr}(\zeta_n^{jn/8}\sqrt[n]{2}^{n/2}) = \begin{cases} n^2/4, & \text{if } j=1,7; \\ -n^2/4, & \text{if } j=3,5. \end{cases}$$

Thus completes the proof of this lemma.

□

# B The Order-LWE Distribution is Pseudorandom

In this section, we give a reduction from the Search Order-LWE to the Average-Case Decision Order-LWE by adapting the methods in [20] to the new ring $\mathcal{R}$, thereby showing that the Order-LWE distribution over $\mathcal{R}$ is pseudorandom.

## B.1 The Factorization of Primes in $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$

Suppose we have a prime number $q$ such that $X^{n/2}+1 \equiv 0 \bmod q$ has a solution $\alpha \in \mathbb{F}_q$ and $Y^n - 2 \equiv 0 \bmod q$ has a solution $\beta \in \mathbb{F}_q$. Through replacing $\beta$ by $\alpha\beta$ if necessary, we can always assume $\beta^{n/2} = \alpha^{n/8} - \alpha^{3n/8} \bmod q$. Such a prime number $q$ splits completely in $\mathbb{Z}[\zeta_n]$ into a product of prime ideals $\prod_{i=0}^{n/2-1} \mathfrak{p}_{2i+1}$, where $\mathfrak{p}_{2i+1} \subset \mathbb{Z}[\zeta_n]$ is [20, 23]

$$\mathfrak{p}_{2i+1} = \langle q, \zeta_n - \alpha^{2i+1} \rangle = q\mathbb{Z}[\zeta_n] + (\zeta_n - \alpha^{2i+1})\mathbb{Z}[\zeta_n]. \tag{B.1}$$

The automorphism $\varsigma_j : \zeta_n \to \zeta_n^j$, $j \in (\mathbb{Z}/n\mathbb{Z})^\times$, of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ acts transitively on the $n/2$ prime ideals via $\varsigma_j : \mathfrak{p}_{2i+1} \to \mathfrak{p}_{(2i+1)/j}$, where the quotient $(2i+1)/j$ is computed in $(\mathbb{Z}/n\mathbb{Z})^\times$ [20]. The residue class degree of $\mathfrak{p}_{2i+1}$ is 1 for every $i$, i.e., $f(\mathfrak{p}_{2i+1}/q) = 1$, hence we have an isomorphism $\mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}[\zeta_n]/\mathfrak{p}_{2i+1}$ [23, 37]. By definition, the norm $\mathrm{Nm}(\mathfrak{p}_{2i+1})$ of $\mathfrak{p}_{2i+1}$ is $q$ [23].

Let us now look at the factorization of the prime ideal $\mathfrak{p}_{2i+1}$ in $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$. If $i \equiv 0, 3 \bmod 4$, we have a factorization

$$Y^{n/2} - \left(\zeta_n^{n/8} - \zeta_n^{3n/8}\right) = \prod_{j=0}^{n/2-1} (Y - \alpha^{2j}\beta) \bmod \mathfrak{p}_{2i+1}.$$

In this case, let the prime ideal $\mathfrak{P}_{2i+1,2j}$ be

$$\mathfrak{P}_{2i+1,2j} = q\mathbb{Z}[\zeta_n, \sqrt[n]{2}] + (\zeta_n - \alpha^{2i+1})\mathbb{Z}[\zeta_n, \sqrt[n]{2}] + (\sqrt[n]{2} - \alpha^{2j}\beta)\mathbb{Z}[\zeta_n, \sqrt[n]{2}].$$

Because $\mathfrak{P}_{2i+1,2j} \cap \mathbb{Z}[\zeta_n] = \mathfrak{p}_{2i+1}$ for every $j$, so $\mathfrak{p}_{2i+1}$ splits completely into $\prod_{j=0}^{n/2-1} \mathfrak{P}_{2i+1,2j}$ in $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$. If $i \equiv 1, 2 \bmod 4$, we have a factorization of the form

$$Y^{n/2} - \left(\zeta_n^{n/8} - \zeta_n^{3n/8}\right) = \prod_{j=0}^{n/2-1} (Y - \alpha^{2j+1}\beta) \bmod \mathfrak{p}_{2i+1}.$$

In this case, let the prime ideal $\mathfrak{P}_{2i+1,2j+1}$ be

$$\mathfrak{P}_{2i+1,2j+1} = q\mathbb{Z}[\zeta_n, \sqrt[n]{2}] + (\zeta_n - \alpha^{2i+1})\mathbb{Z}[\zeta_n, \sqrt[n]{2}] + (\sqrt[n]{2} - \alpha^{2j+1}\beta)\mathbb{Z}[\zeta_n, \sqrt[n]{2}].$$

Similarly, $\mathfrak{p}_{2i+1}$ splits completely into $\prod_{j=0}^{n/2-1} \mathfrak{P}_{2i+1,2j+1}$ in $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$. In conclusion, the prime number $q$ splits completely in $\mathbb{Z}[\zeta_n, \sqrt[n]{2}]$ into

$$q\mathbb{Z}[\zeta_n, \sqrt[n]{2}] = \prod_{(a,b)\in G} \mathfrak{P}_{a,b}. \tag{B.2}$$

The action of the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ on $\mathfrak{P}_{a,b}$ can be obtained immediately: $\sigma_{a,b}(\mathfrak{P}_{c,d}) = \mathfrak{P}_{c/a,d-b}$. Moreover, since $q$ splits completely, we have an isomorphism $\mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}[\zeta_n, \sqrt[n]{2}]/\mathfrak{P}_{a,b}$ for every $(a,b) \in G$, from which we deduce that the norm $\mathrm{Nm}(\mathfrak{P}_{a,b})$ of $\mathfrak{P}_{a,b}$ is $q$ [23].

## B.2 The Main Reduction Theorems

We now prove the main reduction theorems using the lemmas that will be proved later in Sections B.3 and B.4.

**Theorem B.1.** *Suppose $\delta$ and $q$ satisfy $\delta q \geq \eta_\epsilon(\mathcal{R}^\vee)$ for some negligible function $\epsilon = \epsilon(n^2/4)$. Then there exists a randomized polynomial-time reduction from $\mathsf{OLWE}_{q,\Psi_{\leq\delta}}$ to $\mathsf{DOLWE}_{q,\Upsilon_\delta}$.*

*Proof.* The proof comes from a sequence of reductions given in Sections B.3 and B.4. From Lemma B.5, we have a deterministic polynomial-time reduction from $\mathsf{OLWE}_{q,\Psi_{\leq\delta}}$ to $\mathfrak{P}_{a,b}$-$\mathsf{OLWE}_{q,\Psi_{\leq\delta}}$. From Lemma B.8, there exists a probabilistic polynomial-time reduction from $\mathfrak{P}_{a,b}$-$\mathsf{OLWE}_{q,\Psi_{\leq\delta}}$ to $\mathsf{WDOLWE}^{(a,b)}_{q,\Psi_{\leq\delta}}$. From Lemma B.10, there exists a randomized polynomial-time reduction from $\mathsf{WDOLWE}^{(a,b)}_{q,\Psi_{\leq\delta}}$ to $\mathsf{DOLWE}^{(a,b)}_{q,\Upsilon_\delta}$. Then using Lemma B.12, we obtain a reduction to $\mathsf{DOLWE}_{q,\Upsilon_\delta}$. □

From Lemma 5.2, we have $\eta_{2^{-n^2/2}}(\mathcal{R}^\vee) \leq n/(2\lambda_1(\mathcal{R})) = 1$, where we have used $\lambda_1(\mathcal{R}) = n/2$. So in Theorem B.1, it suffices to require $\delta q \geq 1$.

**Theorem B.2.** *Suppose $\delta$ and $q$ are as in Theorem B.1, and let $\ell \geq 1$. Then there exists a randomized polynomial time reduction from solving $\mathsf{OLWE}_{q,\Psi_{\leq\delta}}$ to solving $\mathsf{DOLWE}_{q,D_\xi}$ given only $\ell$ samples, where $\xi = \delta \cdot \left(n^2\ell/(4\log(n^2\ell/4))\right)^{1/4}$.*

*Proof.* The proof also comes from a similar sequence of reductions as in the proof of Theorem B.1. From Lemma B.5, we have a deterministic polynomial-time reduction from $\mathsf{OLWE}_{q,\Psi_{\leq\delta}}$ to $\mathfrak{P}_{a,b}$-$\mathsf{OLWE}_{q,\Psi_{\leq\delta}}$. From Lemma B.8, there exists a probabilistic polynomial-time reduction from $\mathfrak{P}_{a,b}$-$\mathsf{OLWE}_{q,\Psi_{\leq\delta}}$ to $\mathsf{WDOLWE}^{(a,b)}_{q,\Psi_{\leq\delta}}$. From Lemma B.13, there exists a randomized polynomial-time reduction from $\mathsf{WDOLWE}^{(a,b)}_{q,\Psi_{\leq\delta}}$ to $\mathsf{DOLWE}^{(a,b)}_{q,D_\xi}$ given only $\ell$ samples. Then using Lemma B.12, we obtain a reduction to $\mathsf{DOLWE}_{q,D_\xi}$. □

**Theorem B.3.** *Suppose $\delta$ and $q$ are as in Theorem B.1, then there exists a randomized polynomial time reduction from solving $\mathsf{OLWE}_{q,D_\delta}$ to solving $\mathsf{DOLWE}_{q,D_\delta}$.*

*Proof.* Use the same sequence of reductions as in the proof of Theorem B.1, except that Lemma B.10 must be modified so that the error distribution is not randomized but only the secret $\mathbf{s}$ is randomized. □

## B.3 The Reduction from Search to Worst-Case Decision

Let $q$ be a prime number that satisfies the conditions in Section B.1, i.e., $q$ splits completely into the product of $n^2/4$ prime ideals in $\mathcal{R}$. From the Chinese Remainder Theorem, there is an efficiently computable $\mathcal{R}$-module isomorphism [3, 20]

$$\mathcal{R}_q^\vee \cong \prod_{(a,b)\in G} (\mathcal{R}^\vee/\mathfrak{P}_{a,b}\mathcal{R}^\vee)\,. \tag{B.3}$$

**Definition B.4** ($\mathsf{OLWE}$ over $\mathfrak{P}_{a,b}$)**.** *The $\mathfrak{P}_{a,b}$-$\mathsf{OLWE}_{q,\Psi}$ problem is to find* $\mathbf{s} \bmod \mathfrak{P}_{a,b}\mathcal{R}^\vee$ *given access to samples from $A_{\mathbf{s},\psi}$ for arbitrary $\mathbf{s} \in \mathcal{R}_q^\vee$ and $\psi \in \Psi$.*

**Lemma B.5** (OLWE **to** $\mathfrak{P}_{a,b}$-OLWE)**.** *Suppose the family of distributions $\Psi$ over $F_{\mathbb{R}}$ is closed under the actions of Gal$(F/\mathbb{Q})$: $\sigma_{a,b}(\psi) \in \Psi$ for every $\psi \in \Psi$ and $\sigma_{a,b} \in$ Gal$(F/\mathbb{Q})$. Then for every $(a, b) \in G$, there exists a deterministic polynomial-time reduction from* $\mathsf{OLWE}_{q,\Psi}$ *to* $\mathfrak{P}_{a,b}$-$\mathsf{OLWE}_{q,\Psi}$.

*Proof.* Suppose we are given an oracle for $\mathfrak{P}_{a,b}$-$\mathsf{OLWE}_{q,\Psi}$ for an arbitrary $(a, b) \in G$, then using it we can recover the value $\mathbf{s} \bmod \mathfrak{P}_{a,b}\mathcal{R}^\vee$ given access to samples from $A_{\mathbf{s},\psi}$ for any $\psi \in \Psi$. If we can recover $\mathbf{s} \bmod \mathfrak{P}_{c,d}\mathcal{R}^\vee$ for every $(c, d) \in G$, then we can efficiently reconstruct $\mathbf{s} \in \mathcal{R}^\vee$ using the Chinese Remainder Theorem, i.e., Eq. (B.3), thus completes the proof.

We now show how to recover $\mathbf{s} \bmod \mathfrak{P}_{c,d}\mathcal{R}^\vee$ from $\mathbf{s} \bmod \mathfrak{P}_{a,b}\mathcal{R}^\vee$ using Galois action. Let $\sigma_{a',b'}$ be an element of Gal$(F/\mathbb{Q})$ such that $\sigma_{a',b'}(\mathfrak{P}_{c,d}) = \mathfrak{P}_{a,b}$. Notice that such an element always exists [23]. Suppose we are given an arbitrary sample $(\mathbf{a}, \mathbf{b}) \leftarrow A_{\mathbf{s},\psi}$, where $\mathbf{b} = (\mathbf{a}\cdot\mathbf{s})/q + \mathbf{e} \bmod \mathcal{R}^\vee$. We transform this sample to $(\sigma_{a',b'}(\mathbf{a}), \sigma_{a',b'}(\mathbf{b}))$, which satisfies

$$\sigma_{a',b'}(\mathbf{b}) = \left(\sigma_{a',b'}(\mathbf{a}) \cdot \sigma_{a',b'}(\mathbf{s})\right)/q + \sigma_{a',b'}(\mathbf{e}) \bmod \mathcal{R}^\vee.$$

Notice that $\sigma_{a',b'}(\mathbf{a})$ is a uniformly random element of $\mathcal{R}_q$ since $\sigma_{a',b'}$ fixes $\mathcal{R}_q$. Thus $(\sigma_{a',b'}(\mathbf{a}), \sigma_{a',b'}(\mathbf{b}))$ is distributed according to $A_{\sigma_{a',b'}(\mathbf{s}),\psi'}$ where $\psi'$ is $\sigma_{a',b'}(\psi) \in \Psi$. If we feed the transformed samples to the oracle, it returns an answer $\mathbf{t} \in \mathcal{R}^\vee/\mathfrak{P}_{a,b}\mathcal{R}^\vee$. Then we efficiently obtain $\mathbf{s} \equiv \sigma^{-1}_{a',b'}(\mathbf{t}) \bmod \mathfrak{P}_{c,d}\mathcal{R}^\vee$. □

Let us define a lexicographic order on $G$. Recall from Section 2.3 that an element of $G$ is chosen to be of the form $(a, b)$ with $a, b \in \{0, 1, \cdots, n-1\}$. Define $(a, b) < (c, d)$ if $a < c$ or $a = c$ and $b < d$. The smallest element is $(1, 0)$ and the largest element is $(n-1, n-2)$. Given $(a, b) \in G$, let $(a, b)-$ be the largest element in $G$ that is smaller than $(a, b)$, while let $(1, 0)-$ be $(0, 0)$ [20].

**Definition B.6** (**Hybrid** RLWE **Distribution**)**.** *Given $(a, b) \in G$, $\mathbf{s} \in \mathcal{R}_q^\vee$, and a distribution $\psi$ over $F_{\mathbb{R}}$, the distribution $A^{(a,b)}_{\mathbf{s},\psi}$ over $\mathcal{R}_q \times \mathbb{T}$ is defined as follows. If $(a, b) = (0, 0)$, define $A^{(0,0)}_{\mathbf{s},\psi}$ to be $A_{\mathbf{s},\psi}$. Otherwise, sample $(\mathbf{a}, \mathbf{b}) \leftarrow A_{\mathbf{s},\psi}$ and output $(\mathbf{a}, \mathbf{b} + \mathbf{h}/q)$, where $\mathbf{h} \in \mathcal{R}_q^\vee$ is uniformly random and independent* $\bmod \mathfrak{P}_{(c,d)}\mathcal{R}^\vee$ *for all $(c, d) \leq (a, b)$, and is 0 mod all the remaining $\mathfrak{P}_{(c,d)}\mathcal{R}^\vee$.*

**Definition B.7** (**Worst-Case Decision** Order-LWE **Relative to** $\mathfrak{P}_{a,b}$)**.** *Given $(a, b) \in G$ and a family of distributions $\Psi$, the Worst-Case Decision* Order-LWE *relative to $\mathfrak{P}_{a,b}$, denoted by* $\mathsf{WDOLWE}^{(a,b)}_{q,\Psi}$, *is defined as follows: given access to samples from $A^{(c,d)}_{\mathbf{s},\psi}$ for arbitrary $\mathbf{s} \in \mathcal{R}_q^\vee$, $\psi \in \Psi$ and $(c, d) \in \{(a, b)-, (a, b)\}$, find $(c, d)$.*

**Lemma B.8** (**Search to Decision**)**.** *For any $(a, b) \in G$, there exists a probabilistic polynomial-time reduction from* $\mathfrak{P}_{a,b}$-$\mathsf{OLWE}_{q,\Psi}$ *to* $\mathsf{WDOLWE}^{(a,b)}_{q,\Psi}$.

*Proof.* Let $\mathbf{v} \in \mathcal{R}_q$ be uniformly random $\bmod \mathfrak{P}_{a,b}$, but equals 0 mod all the other $\mathfrak{P}_{c,d}$. Let $\mathbf{h} \in \mathcal{R}_q^\vee$ be uniformly random and independent $\bmod \mathfrak{P}_{c,d}\mathcal{R}^\vee$ for all $(c, d) < (a, b)$, but is 0 mod all the remaining $\mathfrak{P}_{c,d}\mathcal{R}^\vee$. Suppose we have an element $\mathbf{g} \in \mathcal{R}_q^\vee$ and we are given a sample $(\mathbf{a}, \mathbf{b}) \leftarrow A_{\mathbf{s},\psi}$, we transform it to

$$(\mathbf{a}', \mathbf{b}') = (\mathbf{a} + \mathbf{v}, \mathbf{b} + (\mathbf{h} + \mathbf{v}\mathbf{g})/q) \in \mathcal{R}_q \times \mathbb{T}.$$

Since $\mathbf{a}$ is uniformly random in $\mathcal{R}_q$, whence $\mathbf{a}'$ is also uniformly random in $\mathcal{R}_q$. In terms of $\mathbf{a}'$, $\mathbf{b}'$ can also be written as

$$\mathbf{b}' = (\mathbf{a}' \cdot \mathbf{s} + \mathbf{h} + \mathbf{v}(\mathbf{g} - \mathbf{s}))\, /q + \mathbf{e},$$

where $\mathbf{e}$ is sampled according to $\psi$. Depending on the value of $\mathbf{g}$, there are two different cases:

1. $\mathbf{g} \equiv \mathbf{s} \bmod \mathfrak{P}_{a,b}\mathcal{R}^\vee$. If so, the Chinese Remainder Theorem, i.e., Eq. (B.3) tells us that $\mathbf{v}(\mathbf{g} - \mathbf{s}) = 0$. Hence the distribution of $(\mathbf{a}', \mathbf{b}')$ is $A_{\mathbf{s},\psi}^{(a,b)-}$.
2. $\mathbf{g} \not\equiv \mathbf{s} \bmod \mathfrak{P}_{a,b}\mathcal{R}^\vee$. As $\mathcal{R}/\mathfrak{P}_{a,b}$ is a field, $\mathbf{v}(\mathbf{g} - \mathbf{s}) \in \mathcal{R}_q^\vee$ is distributed uniformly mod $\mathfrak{P}_{a,b}\mathcal{R}^\vee$ and is 0 mod all other $\mathfrak{P}_{c,d}\mathcal{R}^\vee$. Therefore, $\mathbf{v}(\mathbf{g} - \mathbf{s}) + \mathbf{h}$ is uniformly random and independent mod $\mathfrak{P}_{c,d}\mathcal{R}^\vee$ for all $(c, d) \leq (a, b)$, and is 0 mod all the remaining $\mathfrak{P}_{c,d}\mathcal{R}^\vee$. Hence the distribution of $(\mathbf{a}', \mathbf{b}')$ is $A_{\mathbf{s},\psi}^{(a,b)}$.

If we are given an oracle for $\mathsf{WDOLWE}_{q,\Psi}^{(a,b)}$, then we can distinguish the above two cases for $\mathbf{g}$. Now, we randomly take some $\mathbf{g} \in \mathcal{R}^\vee$ and use the oracle to determine whether $\mathbf{g} \equiv \mathbf{s} \bmod \mathfrak{P}_{a,b}\mathcal{R}^\vee$ or not. If not, we change to a different $\mathbf{g}$ and repeat the process. Since there are only $\mathrm{Nm}(\mathfrak{P}_{a,b}) = q = \mathrm{poly}(n)$ possible values for $\mathbf{s} \bmod \mathfrak{P}_{a,b}\mathcal{R}^\vee$, we certainly can enumerate over all the values and efficiently discover the correct one.

□

## B.4 Worst-Case Decision to Average-Case Decision

We now give a reduction from the worst-case problem $\mathsf{WDOLWE}_{q,\Psi}^{(a,b)}$ to an average-case problem, which distinguishes $A_{\mathbf{s},\psi}$ from the uniform distribution for a random choice of $\mathbf{s}$ and $\psi$. But the error distribution $\psi$ must be drawn randomly from a certain distribution $\Upsilon$ and is kept secret.

**Definition B.9** (**Average-Case Decision** Order-LWE **Relative to** $\mathfrak{P}_{a,b}$)**.** *For $(a, b) \in G$ and a distribution $\Upsilon$ defined over the error distributions $\Psi$, an algorithm is said to solve the problem $\mathsf{DOLWE}_{q,\Upsilon}^{(a,b)}$ with a non-negligible probability over the choice of a random $(\mathbf{s}, \psi) \leftarrow \mathcal{U}(\mathcal{R}_q^\vee) \times \Upsilon$ if there is a non-negligible difference in acceptance probability between inputs from $A_{\mathbf{s},\psi}^{(a,b)}$ and inputs from $A_{\mathbf{s},\psi}^{(a,b)-}$.*

Recall that Claim 5.11 of the paper [20] tells us that for $P = \Gamma(2, 1)^{n^2/4}$ and

$$Q(z_1, \ldots, z_{n^2/4}) = (\Gamma(2, 1) - z_1) \times \cdots \times \left(\Gamma(2, 1) - z_{n^2/4}\right),$$

where $0 \leq z_1, \ldots, z_{n^2/4} \leq 2/n$, any set $S \subset \mathbb{R}^n$ with non-negligible measure under $P$ also has non-negligible measure under $Q$.

**Lemma B.10** (**Worst-Case to Average-Case**)**.** *For any $\delta > 0$ and $(a, b) \in G$, there exists a randomized polynomial-time reduction from $\mathsf{WDOLWE}_{q,\Psi_{\leq\delta}}^{(a,b)}$ to $\mathsf{DOLWE}_{q,\Upsilon_\delta}^{(a,b)}$.*

*Proof.* Suppose we are given $\mathbf{s}' \in \mathcal{R}_q^\vee$, $\mathbf{r}' \in (\mathbb{R}^+)^{n^2/4}$ and $(c,d) \in G$. Let $\mathbf{h} \in \mathcal{R}_q^\vee$ be uniformly random and independent mod $\mathfrak{P}_{e,f}\mathcal{R}^\vee$ for all $(e,f) \le (c,d)$, and is 0 mod all the remaining $\mathfrak{P}_{e,f}\mathcal{R}^\vee$. Now consider the transformation

$$(\mathbf{a}, \mathbf{b}) \to (\mathbf{a}, \mathbf{b} + (\mathbf{a} \cdot \mathbf{s}' + \mathbf{h})/q + \mathbf{e}')\,,$$

where $\mathbf{e}'$ is sampled from $D_{\mathbf{r}'}$. For all $\mathbf{s} \in \mathcal{R}_q^\vee$ and $(a,b) \in G$, this transformation maps $A_{\mathbf{s},\psi}^{(a,b)}$ to $A_{\mathbf{s}+\mathbf{s}',\psi+D_{\mathbf{r}'}}^{\max\{(a,b),(c,d)\}}$.

The reduction repeats the following procedure a polynomial number of times. Choose a uniform $\mathbf{s}' \in \mathcal{R}_q^\vee$ and a real positive $x_{e,f}$, $(e,f) \in N$, independently from $\Gamma(2,1)$. Let $\mathbf{r}' \in (\mathbb{R}^+)^{n^2/4}$ be

$$r_{e,f}'^2 = r_{(n-1)e,(n-1)f}'^2 = n\delta^2 x_{e,f}/2, \ \forall\,(e,f) \in N.$$

Then estimate the acceptance probability of the oracle for $\mathsf{DOLWE}_{q,\Upsilon_\epsilon}^{(a,b)}$ on the following two input distributions:

1. apply the transformation with $\mathbf{s}'$, $\mathbf{r}'$ and $(a,b)-$ to input samples.

2. apply the transformation with $\mathbf{s}'$, $\mathbf{r}'$ and $(a,b)$ to input samples.

If in any of these polynomial numbers of attempts a non-negligible difference is observed between the two acceptance probabilities, output $(a,b)-$. Otherwise, output $(a,b)$. If our input samples are from $A_{\mathbf{s},\psi}^{(a,b)}$, then both transformations map $A_{\mathbf{s},\psi}^{(a,b)}$ to $A_{\mathbf{s}+\mathbf{s}',\psi+D_{\mathbf{r}'}}^{(a,b)}$. Then the oracle's acceptance probability will be exactly the same, thus we output $(a,b)$ with overwhelming probability.

If our input samples are from $A_{\mathbf{s},D_\mathbf{r}}^{(a,b)-}$ for some $\mathbf{r}$ such that all $r_{e,f}$ are in $[0,\delta]$. Then the transformation with parameters $\mathbf{s}'$, $\mathbf{r}'$ and $(a,b)-$ transforms $A_{\mathbf{s},D_\mathbf{r}}^{(a,b)-}$ to $A_{\mathbf{s}+\mathbf{s}',D_\mathbf{r}+D_{\mathbf{r}'}}^{(a,b)-}$. The transformation with parameters $\mathbf{s}'$, $\mathbf{r}'$ and $(a,b)$ transforms $A_{\mathbf{s},D_\mathbf{r}}^{(a,b)-}$ to $A_{\mathbf{s}+\mathbf{s}',D_\mathbf{r}+D_{\mathbf{r}'}}^{(a,b)}$. Moreover, we have

$$D_\mathbf{r} + D_{\mathbf{r}'} = D_{\mathbf{r}''} \text{ with } r_{e,f}''^2 = r_{e,f}^2 + r_{e,f}'^2, \ \forall\,(e,f) \in N.$$

Let $S$ be the set of all pairs $(\mathbf{s},\psi)$ such that the oracle has a non-negligible difference in acceptance probability on $A_{\mathbf{s},\psi}^{(a,b)-}$ and $A_{\mathbf{s},\psi}^{(a,b)}$. Here "non-negligible" means the measure of $S$ under the distribution $\mathcal{U}(\mathcal{R}_q^\vee) \times \Upsilon_\delta$ is non-negligible. By Claim 5.11 of [20], the probability of $(\mathbf{s}+\mathbf{s}', D_\mathbf{r}+D_{\mathbf{r}'}) \in S$ is also non-negligible, hence we will output $(a,b)-$. Thus proves the lemma.

□

**Lemma B.11.** *Suppose $\delta \ge \eta_\epsilon(\mathcal{R}^\vee)/q$ for some $\epsilon > 0$, then for any $\psi$ in the support of $\Upsilon_\delta$ and $\mathbf{s} \in \mathcal{R}_q^\vee$, the distribution $A_{\mathbf{s},\psi}^{(n-1,n-2)}$ is within statistical distance $\epsilon/2$ from the uniform distribution over $\mathcal{R}_q \times \mathbb{T}$.*

*Proof.* From its definition, a sample from the distribution $A_{\mathbf{s},\psi}^{(n-1,n-2)}$ is of the form $(\mathbf{a}, (\mathbf{a} \cdot \mathbf{s} + \mathbf{h})/q + \mathbf{e})$, where $\mathbf{a} \leftarrow \mathcal{U}(\mathcal{R}_q)$, $\mathbf{h} \leftarrow \mathcal{U}(\mathcal{R}_q^\vee)$ and $\mathbf{e} \leftarrow \psi$. Thus it suffices to prove that conditioned on an arbitrary value of $\mathbf{a}$, the second component of the pair is within statistical distance $\epsilon$ of the uniform distribution over $\mathbb{T}$. Now, take an $\mathbf{a}$ and keep its valued fixed, then $(\mathbf{a} \cdot \mathbf{s} + \mathbf{h})/q$ is distributed like a uniformly random element of $(q^{-1}\mathcal{R}^\vee)/\mathcal{R}^\vee$. Moreover, any noise distribution $\psi$ in the support of $\Upsilon_\delta$ can be written as the sum of two independent Gaussian distributions $D_{\mathbf{r}} + D_{\mathbf{r}'}$, where the first is with parameters $r_{e,f} = \delta$ and the second is with parameters $r'^2_{e,f} = x_{e,f} \geq 0$. From Lemma 2.3 of [20] and our assumption on $\delta$, the sum of a uniform element of $(q^{-1}\mathcal{R}^\vee)/\mathcal{R}^\vee$ and a noise sampled from $D_{\mathbf{r}}$ is within statistical distance $\epsilon/2$ from the uniform distribution on $\mathbb{T}$, while this remains the case even after adding the independent noise $D_{\mathbf{r}'}$. □

**Lemma B.12** (**Hybrid**). *Suppose $\Upsilon$ is a distribution over error distributions such that for any $\psi$ in the support of $\Upsilon$ and any $\mathbf{s} \in \mathcal{R}_q^\vee$, the distribution $A_{\mathbf{s},\psi}^{(n-1,n-2)}$ is within negligible statistical distance from uniform. Then for any oracle that solve $\mathsf{DOLWE}_{q,\Upsilon}$, there exists an $(a,b) \in G$ and an efficient algorithm that solves $\mathsf{DOLWE}_{q,\Upsilon}^{(a,b)}$ using the oracle.*

*Proof.* Let $(\mathbf{s},\psi)$ be any pair for which the oracle distinguishes between $A_{\mathbf{s},\psi}$ and the uniform inputs with a non-negligible advantage. From Markov's inequality, the probability measure of such pairs is non-negligible. Since $A_{\mathbf{s},\psi}^{(0,0)} = A_{\mathbf{s},\psi}$ and $A_{\mathbf{s},\psi}^{(n-1,n-2)}$ is far from the uniform distribution, there exists an element $(a,b) \in G$ such that the oracle distinguishes between $A_{\mathbf{s},\psi}^{(a,b)}$ and $A_{\mathbf{s},\psi}^{(a,b)-}$ with a non-negligible advantage. The lemma follows immediately by choosing the $(a,b)$ associated with the set of pairs $(\mathbf{s},\psi)$ with highest probability. □

Suppose $r_1, \ldots, r_{n^2/4} \in \mathbb{R}^+$ and $s_1, \ldots, s_{n^2/4} \in \mathbb{R}^+$ satisfy $|s_i/r_i - 1| < 2\sqrt{\log(n^2/4)}/n$ for all $i$. Then Claim 5.15 of [20] says that any set $S$ with non-negligible measure under the Gaussian distribution $D_{r_1} \times \cdots D_{r_{n^2/4}}$ also has non-negligible measure under $D_{s_1} \times \cdots \times D_{s_{n^2/4}}$.

**Lemma B.13** (**Worst-case to average-case with spherical noise**). *For any $\delta > 0$, $\ell \geq 1$, and every $(a,b) \in G$, there exists a randomized polynomial-time reduction from solving $\mathsf{WDOLWE}_{q,\Psi_{\leq\delta}}^{(a,b)}$ to solving $\mathsf{DOLWE}_{q,D_\xi}^{(a,b)}$ given only $\ell$ samples, where $\xi = \delta \cdot \left(n^2\ell/(4\log(n^2\ell/4))\right)^{1/4}$.*

*Proof.* For some $\mathbf{s}' \in \mathcal{R}_q^\vee$, $(c,d) \in G$ and $\mathbf{e}_1, \ldots, \mathbf{e}_\ell \in \mathbb{T}$, consider the transformation

$$(\mathbf{a}_i, \mathbf{b}_i) \to (\mathbf{a}_i, \mathbf{b}_i + (\mathbf{a}_i \cdot \mathbf{s}' + \mathbf{h}_i)/q + \mathbf{e}_i)\,,\ 1 \leq i \leq \ell, \tag{B.4}$$

where for every $i$, $\mathbf{h}_i \in \mathcal{R}_q^\vee$ is chosen independently to be uniformly random $\bmod \mathfrak{P}_{e,f}\mathcal{R}^\vee$ for all $(e,f) \leq (c,d)$ and be 0 mod all the remaining $\mathfrak{P}_{e,f}\mathcal{R}^\vee$. Then for any $\mathbf{s} \in \mathcal{R}_q^\vee$, $\psi$, $\mathbf{r}'$, and $(a,b) \in G$, if we sample from $(A_{\mathbf{s},\psi}^{(a,b)})^\ell$, i.e., $\ell$ independent samples from $A_{\mathbf{s},\psi}^{(a,b)}$, and apply this transformation with $\mathbf{e}_1, \ldots, \mathbf{e}_\ell$ sampled independently from $D_{\mathbf{r}'}$, then averaged over the choice of $\mathbf{e}_i$ the output is distributed according to $\left(A_{\mathbf{s}+\mathbf{s}',\psi+D_{\mathbf{r}'}}^{\max\{(a,b),(c,d)\}}\right)^\ell$.

The reduction repeats the following process a polynomial number of times. Choose $\mathbf{s}' \in \mathcal{R}_q^\vee$ uniformly randomly, and sample $\mathbf{e}_1, \ldots, \mathbf{e}_\ell$ independently from $D_\xi$. Now let us estimate the acceptance probability of the oracle on the following two different input distributions:

1. apply the transformation with parameters $\mathbf{s}'$, $\mathbf{e}_1, \ldots, \mathbf{e}_\ell$ and $(a,b)-$.

2. apply the transformation with parameters $\mathbf{s}'$, $\mathbf{e}_1, \ldots, \mathbf{e}_\ell$ and $(a, b)$

If during any of the polynomial number of attempts a non-negligible difference is observed between the two acceptance probabilities, output $(a, b)-$; otherwise output $(a, b)$.

If the input distribution is $A^{(a,b)}_{\mathbf{s},\psi}$, then in each of the two attempts, the two distributions on which we estimate the oracle's acceptance probability are the same, hence we output $(a, b)$ with overwhelming probability. If the input distribution is $A^{(a,b)-}_{\mathbf{s},D_\mathbf{r}}$ for a vector $\mathbf{r}$ with all $r_{c,d}$ in $[0, \epsilon]$. Let the distributions $B^{(a,b)-}(\mathbf{s}', \mathbf{e}_1, \ldots, \mathbf{e}_\ell)$ and $B^{(a,b)}(\mathbf{s}', \mathbf{e}_1, \ldots, \mathbf{e}_\ell)$ be on $\ell$ pairs which our reduction uses as input to the oracle. Let the vector $\mathbf{r}'$ be given by $r'^2_{c,d} = \xi - r^2_{c,d}$ so that $D_\mathbf{r} + D_{\mathbf{r}'} = D_\xi$. From our analysis above, the average of $B^{(a,b)-}(\mathbf{s}', \mathbf{e}_1, \ldots, \mathbf{e}_\ell)$ over $\mathbf{e}_1, \ldots, \mathbf{e}_\ell$ sampled independently from $D_{\mathbf{r}'}$ is $(A^{(a,b)-}_{\mathbf{s}+\mathbf{s}',D_\xi})^\ell$, and similarly with $B^{(a,b)}$ and $A^{(a,b)}$. Let $S$ be the set of all $(\mathbf{s}, \mathbf{e}_1, \ldots, \mathbf{e}_\ell)$ for which the oracle has a non-negligible difference in acceptance probability on $B^{(a,b)-}(\mathbf{s}', \mathbf{e}_1, \ldots, \mathbf{e}_\ell)$ and $B^{(a,b)}(\mathbf{s}', \mathbf{e}_1, \ldots, \mathbf{e}_\ell)$. From our assumption and a Markov argument, the measure of $S$ under $\mathcal{U}(\mathcal{R}^\vee_q) \times (D_{\mathbf{r}'})^\ell$ is non-negligible [20]. From the inequalities

$$1 \leq \frac{\xi}{\sqrt{\xi^2 - r^2_{c,d}}} \leq \frac{\xi}{\sqrt{\xi^2 - \epsilon^2}} \leq 1 + \sqrt{\frac{\log(n^2\ell/4)}{n^2\ell/4}},$$

we deduce that the measure of $S$ under $\mathcal{U}(\mathcal{R}^\vee_q) \times (D_\xi)^\ell$ is also non-negligible, thus proves the lemma.

□

# C The Twin: the Splitting Field of $Y^n + 2$

In this section, we study the splitting field $\widehat{F}$ of $Y^n+2$, where $n$ ($\geq 8$) is a power-of-two integer. We show that all the results we have obtained for $F = \mathbb{Q}(\zeta_n, \sqrt[n]{2})$ can be directly generalized to $\widehat{F} = \mathbb{Q}(\zeta_n, \sqrt[n]{-2})$.

## C.1 The Splitting Field of $Y^n + 2$

The splitting field $\widehat{F}$ of $Y^n + 2$ is generated by $\zeta_n$ and $\sqrt[n]{-2}$ over $\mathbb{Q}$: $\widehat{F} = \mathbb{Q}(\zeta_n, \sqrt[n]{-2})$. The two numbers satisfy the algebraic relations

$$\zeta_n^{n/2} = -1 \text{ and } \sqrt{-2} = \zeta_n^{n/8} + \zeta_n^{3n/8}. \tag{C.1}$$

The proof in the webpage [38] can be immediately adapted to prove that the degree of $\widehat{F}$ over $\mathbb{Q}$ is also $n^2/4$. An element of the Galois group $\mathrm{Gal}(\widehat{F}/\mathbb{Q})$ is determined by the actions

$$\widehat{\sigma}_{a,b}(\zeta_n) = \zeta_n^a \text{ and } \widehat{\sigma}_{a,b}(\sqrt[n]{-2}) = \zeta_n^b \sqrt[n]{-2}.$$

To preserve the relations in Eq. (C.1), $a$ and $b$ must satisfy

$$a \equiv \begin{cases} 1,\ 3 \bmod 8, & \text{if } b \text{ is even,} \\ 5,\ 7 \bmod 8, & \text{if } b \text{ is odd.} \end{cases} \tag{C.2}$$

For later convenience, we define the finite set $\widehat{G}$ to be

$$\widehat{G} = \left\{(a,b) \in (\mathbb{Z}/n\mathbb{Z})^2 : (a,b) \text{ satisfies the condition in Eq. (C.2)}\right\},$$

then $\mathrm{Gal}(\widehat{F}/\mathbb{Q})$ is given by $\{\widehat{\sigma}_{a,b} : (a,b) \in \widehat{G}\}$. The identity of $\mathrm{Gal}(\widehat{F}/\mathbb{Q})$ is $\widehat{\sigma}_{1,0}$ and the complex conjugation is $\widehat{\sigma}_{n-1,n-1}$. Let $\widehat{N}$ be the subset

$$\widehat{N} = \left\{(a,b) \in \widehat{G} : a \equiv 1 \text{ or } 5 \bmod 8\right\}.$$

Then the Galois group $\mathrm{Gal}(\widehat{F}/\mathbb{Q}(\sqrt{-1}))$ is the subgroup

$$\mathrm{Gal}\left(\widehat{F}/\mathbb{Q}(\sqrt{-1})\right) = \left\{\widehat{\sigma}_{a,b} \in \mathrm{Gal}(\widehat{F}/\mathbb{Q}) : (a,b) \in \widehat{N}\right\}.$$

Moreover, the Galois group $\mathrm{Gal}(\widehat{F}/\mathbb{Q}(\zeta_n))$ is the subgroup generated by $\widehat{\sigma}_{1,2}$, whose order is $n/2$. Through studying the subfields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\zeta_n)$ using the fundamental theorem of Galois theory, we can obtain an explicit algebraic structure of $\mathrm{Gal}(\widehat{F}/\mathbb{Q})$ in the same way as in Section 2, which is omitted here.

## C.2 The Canonical Embedding

The canonical embedding of $\widehat{F}$ into $\mathbb{C}^{n^2/4}$ is given by

$$\widehat{\sigma} : x \in \widehat{F} \mapsto (\widehat{\sigma}_{a,b}(x))_{(a,b)\in\widehat{G}} \in \mathbb{C}^{n^2/4},$$

which induces an injective real linear map from $\widehat{F}_{\mathbb{R}} = \widehat{F} \otimes_{\mathbb{Q}} \mathbb{R}$ to $\mathbb{C}^{n^2/4}$ via

$$\widehat{\sigma} : x \otimes r \mapsto (\widehat{\sigma}_{a,b}(x) \cdot r)_{(a,b)\in\widehat{G}}, \text{ where } x \in \widehat{F} \text{ and } r \in \mathbb{R}. \tag{C.3}$$

The complex conjugation of $\widehat{\sigma}_{a,b}(x)$, denoted by $\overline{\widehat{\sigma}_{a,b}(x)}$, satisfies

$$\overline{\widehat{\sigma}_{a,b}(x)} = \widehat{\sigma}_{(n-1)a,(n-1)b+(n-1)}(x) \tag{C.4}$$

for every $x \in \widehat{F}$ and $(a,b) \in \widehat{G}$. Therefore, the image of $\widehat{F}_{\mathbb{R}}$ under $\widehat{\sigma}$ is the real subspace

$$\widehat{H} = \left\{(z_{a,b})_{(a,b)\in\widehat{G}} \in \mathbb{C}^{n^2/4} : z_{(n-1)a,(n-1)b+(n-1)} = \overline{z_{a,b}}\right\},$$

which is isomorphic to $\widehat{F}_{\mathbb{R}}$. As a result, we often implicitly identify $\widehat{H}$ with $\widehat{F}_{\mathbb{R}}$. The homomorphism in Eq. (C.3) can also be written as

$$\widehat{\sigma} : x \otimes r \mapsto (\widehat{\sigma}_{a,b}(x) \cdot r, \widehat{\sigma}_{(n-1)a,(n-1)b+(n-1)}(x) \cdot r)_{(a,b)\in\widehat{N}}.$$

An automorphism $\widehat{\sigma}_{c,d} \in \mathrm{Gal}(\widehat{F}/\mathbb{Q})$ of $\widehat{F}$ induces an automorphism of $\widehat{H}$ by making the following diagram commute

$$\begin{tikzcd}
x \otimes r \arrow[r, "\widehat{\sigma}"] \arrow[d, "\widehat{\sigma}_{c,d}"] & (\widehat{\sigma}_{a,b}(x) \cdot r, \widehat{\sigma}_{(n-1)a,(n-1)b+(n-1)}(x) \cdot r)_{(a,b)\in\widehat{N}} \arrow[d, "\widehat{\sigma}_{c,d}"] \\
\widehat{\sigma}_{c,d}(x) \otimes r \arrow[r, "\widehat{\sigma}"] & (\widehat{\sigma}_{a,b}(\widehat{\sigma}_{c,d}(x)) \cdot r, \widehat{\sigma}_{(n-1)a,(n-1)b+(n-1)}(\widehat{\sigma}_{c,d}(x)) \cdot r)_{(a,b)\in\widehat{N}}
\end{tikzcd}.$$

Therefore, the effect of the automorphism $\widehat{\sigma}_{c,d}$ is to permute the components of vectors in $\widehat{H}$.

Let $\widehat{\mathbf{e}}_{a,b} \in \mathbb{C}^{n^2/4}$ be the vector with 1 in its $(a,b)$-th coordinate and 0 elsewhere, which forms a natural basis of $\mathbb{C}^{n^2/4}$. For every $(a,b) \in \widehat{N}$, we define

$$\begin{aligned}\widehat{\mathbf{h}}_{(a,b)} &= \frac{1}{\sqrt{2}}\left(\widehat{\mathbf{e}}_{a,b} + \widehat{\mathbf{e}}_{(n-1)a,(n-1)b+(n-1)}\right), \\ \widehat{\mathbf{h}}_{((n-1)a,(n-1)b+(n-1))} &= \frac{\sqrt{-1}}{\sqrt{2}}\left(\widehat{\mathbf{e}}_{a,b} - \widehat{\mathbf{e}}_{(n-1)a,(n-1)b+(n-1)}\right),\end{aligned}$$

which forms a real basis for $\widehat{H}$. The restriction of the inner product $\langle\cdot,\cdot\rangle$ of $\mathbb{C}^{n^2/4}$ on $\widehat{H}$ is a real positive definite inner product, with respect to which $\{\widehat{\mathbf{h}}_{a,b} : (a,b) \in \widehat{G}\}$ forms an orthonormal basis.

**Proposition C.1.** *Under the canonical embedding, the basis $\zeta_n^{k_0}\sqrt[n]{-2}^{k_1}$, $0 \le k_0, k_1 < n/2$, of $\widehat{F}$ is sent to an orthogonal basis of $\mathbb{C}^{n^2/4}$:*

$$\langle \widehat{\sigma}(\zeta_n^{k_0}\sqrt[n]{-2}^{k_1}), \widehat{\sigma}(\zeta_n^{l_0}\sqrt[n]{-2}^{l_1})\rangle = \begin{cases} \sqrt[n]{2}^{2k_1}\cdot n^2/4, & \textit{if } k_0 = l_0 \textit{ and } k_1 = l_1; \\ 0, & \textit{otherwise.}\end{cases}$$

*Proof.* Same as the proof of Proposition 3.1. □

**Theorem C.2.** *$Tr(\zeta_n^{k_0+l_0}\sqrt[n]{-2}^{k_1+l_1})$ is always 0 unless $k_1 = l_1 = 0$ or $k_1 + l_1 = n/2$. When $k_1 = l_1 = 0$, we have*

$$Tr(\zeta_n^{k_0+l_0}) = \begin{cases} n^2/4, & \textit{if } k_0 = l_0 = 0; \\ -n^2/4, & \textit{if } k_0 + l_0 = n/2.\end{cases}$$

*when $k_1 + l_1 = n/2$, we have*

$$Tr(\zeta_n^{k_0+l_0}\sqrt[n]{-2}^{n/2}) = \begin{cases} -n^2/4, & \textit{if } k_0 + l_0 = n/8 \textit{ or } 3n/8; \\ n^2/4, & \textit{if } k_0 + l_0 = 5n/8 \textit{ or } 7n/8.\end{cases}$$

*Proof.* Same as the proof of Theorem 4.1. □

From this theorem, we can compute the absolute discriminant of $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$ using the method given in Section 4.1, which is also equal to $2^{n(n-2)/8}(n^2/4)^{n^2/4}$, a power-of-two integer. The dual of the natural integral basis $\zeta_n^{k_0}\sqrt[n]{-2}^{k_1}$ of $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$ is a set of elements $\{\widehat{e}_{l_0,l_1} \in \widehat{F} : 0 \le l_0, l_1 < n/2\}$ such that $\mathrm{Tr}(\widehat{e}_{l_0,l_1}\cdot \zeta_n^{k_0}\sqrt[n]{-2}^{k_1})$ is equal to 1 if $l_0 = k_0$ and $l_1 = k_1$, and 0 otherwise.

**Proposition C.3.** *When $l_1 = 0$, $\widehat{e}_{l_0,0}$ is given by*

$$\widehat{e}_{0,0} = \frac{4}{n^2} \textit{ and } \widehat{e}_{l_0,0} = -\frac{4}{n^2}\cdot\zeta_n^{n/2-l_0} \textit{ if } l_0 > 0.$$

*When $0 < l_1 < n/2$, $\widehat{e}_{l_0,l_1}$ is given by*

$$\widehat{e}_{l_0,l_1} = \begin{cases} -\frac{2}{n^2}\zeta_n^{n/8-l_0}\sqrt[n]{-2}^{n/2-l_1} - \frac{2}{n^2}\zeta_n^{3n/8-l_0}\sqrt[n]{-2}^{n/2-l_1}, & \textit{if } 0 \le l_0 \le \frac{n}{8}, \\ -\frac{2}{n^2}\zeta_n^{3n/8-l_0}\sqrt[n]{-2}^{n/2-l_1} + \frac{2}{n^2}\zeta_n^{5n/8-l_0}\sqrt[n]{-2}^{n/2-l_1}, & \textit{if } \frac{n}{8} < l_0 \le \frac{3n}{8}, \\ \frac{2}{n^2}\zeta_n^{5n/8-l_0}\sqrt[n]{-2}^{n/2-l_1} + \frac{2}{n^2}\zeta_n^{7n/8-l_0}\sqrt[n]{-2}^{n/2-l_1}, & \textit{if } \frac{3n}{8} < l_0 < \frac{n}{2}.\end{cases}$$

## C.3 The Error Distributions on the Ideal Lattices

Let $\widehat{\mathbf{r}} = (\widehat{r}_{a,b})_{(a,b)\in\widehat{G}} \in (\mathbb{R}^+)^{n^2/4}$ be a vector of positive real numbers such that $\widehat{r}_{a,b} = \widehat{r}_{((n-1)a,(n-1)b+(n-1))}$ for every pair $(a,b) \in \widehat{N}$. Then a sample from the elliptical Gaussian distribution $D_{\widehat{\mathbf{r}}}$ is a vector $\sum_{(a,b)\in\widehat{G}} \widehat{x}_{a,b}\widehat{\mathbf{h}}_{a,b}$, where each $\widehat{x}_{a,b}$ is sampled independently from the one-dimensional Gaussian distribution $D_{\widehat{r}_{a,b}}$.

**Definition C.4.** *Given a positive real number $\widehat{\varrho}$, let $\widehat{\Psi}_{\leq\widehat{\varrho}}$ be the set of all elliptic Gaussian distribution $D_{\widehat{\mathbf{r}}}$ over $\widehat{H}$ ($\cong \widehat{F}_{\mathbb{R}}$) where for every $(a,b) \in \widehat{N}$ we have $\widehat{r}_{a,b} = \widehat{r}_{((n-1)a,(n-1)b+(n-1))}$ and $\widehat{r}_{a,b} \leq \widehat{\varrho}$.*

**Lemma C.5.** *For any $\widehat{\varrho}$, the family of distributions $\widehat{\Psi}_{\leq\widehat{\varrho}}$ is closed under the action of any element of Gal$(\widehat{F}/\mathbb{Q})$.*

*Proof.* Same as the proof of Lemma 5.4. □

The $\widehat{\mathcal{R}}$-$\mathsf{DGS}_\gamma$ problem is: given a fractional ideal $\widehat{\mathcal{I}}$ associated with $\widehat{\mathcal{R}}$ and a number $\widehat{s} \geq \widehat{\gamma} = \widehat{\gamma}(\widehat{\mathcal{I}})$, output a sample from the distribution $D_{\widehat{\mathcal{I}},\widehat{s}}$.

**Definition C.6.** *Given a positive real number $\widehat{\delta}$, $\widehat{\Upsilon}_{\widehat{\delta}}$ is a distribution over distributions: a sample from $\widehat{\Upsilon}_{\widehat{\delta}}$ is an elliptical Gaussian distribution $D_{\widehat{\mathbf{r}}}$ on $\widehat{H}$ with parameters*

$$\widehat{r}^2_{a,b} = \widehat{r}^2_{(n-1)a,(n-1)b+(n-1)} = \widehat{\delta}^2\left(1 + n\widehat{x}_{a,b}/2\right),\ (a,b) \in \widehat{N},$$

*where $\widehat{x}_{a,b}$ is sampled independently from $\Gamma(2,1)$.*

## C.4 Reduction Theorems for Order-LWE

Recall that via sending $\zeta_n$ to $X$ and $\sqrt[n]{-2}$ to $Y$, the integral ring $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$ is isomorphic to a quotient polynomial ring

$$\widehat{\mathcal{R}} = \mathbb{Z}[X,Y]/\langle X^{n/2}+1, Y^{n/2} - (X^{n/8} + X^{3n/8})\rangle.$$

The results in Section 4.2 can be extended to $\widehat{F}$. In particular, we have

$$\begin{aligned} \lambda_1(\widehat{\mathcal{R}}) &= n/2, & \lambda_{n^2/4}(\widehat{\mathcal{R}}) &\leq 2^{-\frac{1}{2}-\frac{1}{n}}n, \\ \lambda_1(\widehat{\mathcal{R}}^\vee) &= 2^{\frac{1}{2}+\frac{1}{n}}/n, & \lambda_{n^2/4}(\widehat{\mathcal{R}}^\vee) &\leq 2/n. \end{aligned}$$

The worst-case hardness of the Search Order-LWE in $\widehat{\mathcal{R}}$ comes from Theorem 4.1 of [20].

**Proposition C.7.** *Let $\widehat{\varrho} = \widehat{\varrho}(n^2/4)$ ($> 0$) and let $\widehat{q} = \widehat{q}(n^2/4)$ be such that $\widehat{\varrho}\widehat{q} \geq 2 \cdot \widehat{\omega}\left(\sqrt{\log{(n^2/4)}}\right)$. For some negligible function $\widehat{\epsilon} = \widehat{\epsilon}\left(n^2/4\right)$, there exists a probabilistic polynomial-time reduction from $\widehat{\mathcal{R}}$-$\mathsf{DGS}_{\widehat{\gamma}}$ to $\mathsf{OLWE}_{\widehat{q},\widehat{\Psi}_{\leq\widehat{\varrho}}}$, where $\widehat{\gamma}$ is*

$$\widehat{\gamma} = \max\left\{\eta_{\widehat{\epsilon}}\left(\widehat{\mathcal{I}}\right) \cdot \left(\sqrt{2}/\widehat{\varrho}\right) \cdot \widehat{\omega}\left(\sqrt{\log{(n^2/4)}}\right), \sqrt{n^2/2}/\lambda_1\left(\widehat{\mathcal{I}}^\vee\right)\right\}.$$

Here $\widehat{\omega}(\sqrt{\log(n^2/4)})$ denotes a fixed but arbitrary function that grows asymptotically faster than $\sqrt{\log(n^2/4)}$. The proof of the following theorem is almost exactly the same as that of Theorem 5.10. Here we also need a lexicographic order on $\widehat{G}$: $(a,b) < (c,d)$ if $a < c$ or $a = c$ and $b < d$.

**Theorem C.8.** *Let $\widehat{\delta} < 2\sqrt{\log(n^2/4)}/n$ and let $\widehat{q} = \widehat{q}(n^2) \geq 3$ be a poly($n$)-bounded prime number such that both $X^{n/2} \equiv -1 \bmod \widehat{q}$ and $Y^n \equiv -2 \bmod \widehat{q}$ have solutions. Then there exists a polynomial-time reduction from $\widetilde{O}(n/(2\widehat{\delta}))$-approximate* SIVP *(or* SVP*) in the ideal lattices associated with $\widehat{\mathcal{R}}$ to* $\mathsf{DOLWE}_{\widehat{q},\Upsilon_{\widehat{\delta}}}$. *Moreover, for any $\widehat{\ell} \geq 1$, we can replace the target problem in the reduction with the problem of solving* $\mathsf{DOLWE}_{\widehat{q},D_{\widehat{\xi}}}$ *given only $\widehat{\ell}$ samples, where $\widehat{\xi} = \widehat{\delta} \cdot \left(n^2\widehat{\ell}/(4\log(n^2\widehat{\ell}/4))\right)^{1/4}$.*

## C.5 The 2NTT

Via sending $\zeta_n$ to $X$ and $\sqrt[n]{-2}$ to $Y$, the integral ring $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$ is isomorphic to a quotient polynomial ring

$$\widehat{\mathcal{R}} = \mathbb{Z}[X,Y]/\langle X^{n/2}+1, Y^{n/2} - (X^{n/8} + X^{3n/8})\rangle.$$

We now choose a prime number $\widehat{p}$ such that $X^{n/2} + 1 \equiv 0 \bmod \widehat{p}$ has a solution $\widehat{\alpha}$ and $Y^n + 2 \equiv 0 \bmod \widehat{p}$ has a solution $\widehat{\beta}$. By replacing $\widehat{\beta}$ with $\widehat{\alpha}\widehat{\beta}$ if necessary, we can always assume $\widehat{\beta}^{n/2} = \widehat{\alpha}^{n/8} + \widehat{\alpha}^{3n/8} \bmod \widehat{p}$. For such a prime number $\widehat{p}$, the polynomial equations

$$X^{n/2} \equiv -1 \bmod \widehat{p} \text{ and } Y^{n/2} \equiv X^{n/8} + X^{3n/8} \bmod \widehat{p} \tag{C.5}$$

have $n^2/4$ solutions in $\mathbb{F}_{\widehat{p}}$. The first equation has $n/2$ solutions $\{\widehat{\alpha}^{2i+1} : 0 \leq i < n/2\}$. For every solution $X = \widehat{\alpha}^{2i+1}$, the second equation also has $n/2$ solutions for $Y$:

$$Y = \begin{cases} \widehat{\alpha}^{2j}\widehat{\beta}, \ 0 \leq j < n/2, \ \text{if } i \equiv 0, 1 \bmod 4; \\ \widehat{\alpha}^{2j+1}\widehat{\beta}, \ 0 \leq j < n/2, \ \text{if } i \equiv 2, 3 \bmod 4. \end{cases}$$

An element of $\widehat{\mathcal{R}}_{\widehat{p}} = \widehat{\mathcal{R}}/\widehat{p}\widehat{\mathcal{R}}$ is of the form $\widehat{\mathbf{F}}(X,Y) = \sum_{k,l=0}^{n/2-1} \widehat{f}_{k,l}X^kY^l$ with $\widehat{f}_{k,l} \in \mathbb{F}_{\widehat{p}}$.

**Definition C.9.** *The 2NTT of a polynomial $\widehat{\mathbf{F}} \in \widehat{\mathcal{R}}_{\widehat{p}}$ is the evaluation of $\widehat{\mathbf{F}}$ at the $n^2/4$ solutions of the two polynomial equations in Eq.* (C.5).

The vector butterflies for the 2NTT of $\widehat{\mathbf{F}}$ follows immediately from Section 6:

1. Transverse vector butterfly. We use generalized one-variable NTT to evaluate $\widehat{\mathbf{F}}$ at the $n/2$ roots $X = \widehat{\alpha}^{2i+1}$ with $0 \leq i < n/2$, the output of which are $n/2$ vectors $\widehat{\mathbf{F}}(\widehat{\alpha}^{2i+1}, Y)$. There are $\log_2(n/2)$ stages in this phase, and each stage consumes $O(n)$ vector operations.

2. Transpose and longitudinal vector butterfly. The output of the transverse vector butterfly naturally falls into two groups: Group 1 with $i \equiv 0, 1 \bmod 4$ and Group 2 with $i \equiv 2, 3 \bmod 4$. Each group forms an $n/4 \times n/2$ matrix. Now we evaluate the polynomial (with column vector coefficients)

constructed from the column vectors of Group 1 at the roots $\{\widehat{\alpha}^{2j}\widehat{\beta} : 0 \leq j < n/2\}$ using a vector butterfly with a new set of twiddle factors. Then we evaluate the polynomial constructed from the column vectors of Group 2 at the roots $\{\widehat{\alpha}^{2j+1}\widehat{\beta} : 0 \leq j < n/2\}$ using a vector butterfly with another new set of twiddle factors. Each evaluation consists of $\log_2(n/2)$ stages and each stage consumes $O(n)$ vector operations with the length of the vectors now being $n/4$.

## C.6 The Factorization of Primes in $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$

Suppose now we have a prime number $\widehat{q}$ such that $X^{n/2} + 1 \equiv 0 \bmod \widehat{q}$ has a solution $\widehat{\alpha} \in \mathbb{F}_{\widehat{q}}$ and $Y^n + 2 \equiv 0 \bmod \widehat{q}$ has a solution $\widehat{\beta} \in \mathbb{F}_{\widehat{q}}$. Through replacing $\widehat{\beta}$ by $\widehat{\alpha}\widehat{\beta}$ if necessary, we can always assume $\widehat{\beta}^{n/2} = \widehat{\alpha}^{n/8} + \widehat{\alpha}^{3n/8} \bmod \widehat{q}$. Such a prime number $\widehat{q}$ splits completely in $\mathbb{Z}[\zeta_n]$ into a product of prime ideals $\prod_{i=0}^{n/2-1} \widehat{\mathfrak{p}}_{2i+1}$, where $\widehat{\mathfrak{p}}_{2i+1} \subset \mathbb{Z}[\zeta_n]$ is given by [20, 23]

$$\widehat{\mathfrak{p}}_{2i+1} = \langle \widehat{q}, \zeta_n - \widehat{\alpha}^{2i+1} \rangle = \widehat{q}\mathbb{Z}[\zeta_n] + (\zeta_n - \widehat{\alpha}^{2i+1})\mathbb{Z}[\zeta_n]. \tag{C.6}$$

The automorphism $\varsigma_j$ acts transitively on the $n/2$ prime ideals in the factorization via $\varsigma_j : \widehat{\mathfrak{p}}_{2i+1} \to \widehat{\mathfrak{p}}_{(2i+1)/j}$, where the quotient $(2i+1)/j$ is computed in $(\mathbb{Z}/n\mathbb{Z})^\times$ [20]. The residue class degree of $\widehat{\mathfrak{p}}_{2i+1}$ is 1, i.e., $f(\widehat{\mathfrak{p}}_{2i+1}/\widehat{q}) = 1$, for every $i$, hence we have a field isomorphism $\mathbb{Z}/\widehat{q}\mathbb{Z} \cong \mathbb{Z}[\zeta_n]/\widehat{\mathfrak{p}}_{2i+1}$ [23, 37]. By definition, the norm $\mathrm{Nm}(\widehat{\mathfrak{p}}_{2i+1})$ of $\widehat{\mathfrak{p}}_{2i+1}$ is $\widehat{q}$ [23].

The prime ideal $\widehat{\mathfrak{p}}_{2i+1}$ splits completely in $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$. If $i \equiv 0, 1 \bmod 4$, we have a factorization

$$Y^{n/2} - \left(\zeta_n^{n/8} + \zeta_n^{3n/8}\right) = \prod_{j=0}^{n/2-1} (Y - \widehat{\alpha}^{2j}\widehat{\beta}) \bmod \widehat{\mathfrak{p}}_{2i+1}.$$

In this case, let the prime ideal $\widehat{\mathfrak{P}}_{2i+1,2j}$ be

$$\widehat{\mathfrak{P}}_{2i+1,2j} = \langle \widehat{q}, \zeta_n - \widehat{\alpha}^{2i+1}, \sqrt[n]{-2} - \widehat{\alpha}^{2j}\widehat{\beta} \rangle.$$

Because $\widehat{\mathfrak{P}}_{2i+1,2j} \cap \mathbb{Z}[\zeta_n] = \widehat{\mathfrak{p}}_{2i+1}$ for every $j$, so $\widehat{\mathfrak{p}}_{2i+1}$ splits completely into $\prod_{j=0}^{n/2-1} \widehat{\mathfrak{P}}_{2i+1,2j}$ in $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$. If $i \equiv 2, 3 \bmod 4$, we have a factorization

$$Y^{n/2} - \left(X^{n/8} + X^{3n/8}\right) = \prod_{j=0}^{n/2-1} (Y - \widehat{\alpha}^{2j+1}\widehat{\beta}) \bmod \widehat{\mathfrak{p}}_{2i+1}.$$

In this case, let the prime ideal $\widehat{\mathfrak{P}}_{2i+1,2j+1}$ be

$$\widehat{\mathfrak{P}}_{2i+1,2j+1} = \langle \widehat{q}, \zeta_n - \widehat{\alpha}^{2i+1}, \sqrt[n]{-2} - \widehat{\alpha}^{2j+1}\widehat{\beta} \rangle,$$

and similarly $\widehat{\mathfrak{p}}_{2i+1}$ splits completely into $\prod_{j=0}^{n/2-1} \widehat{\mathfrak{P}}_{2i+1,2j+1}$ in $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$. In conclusion, the prime number $\widehat{q}$ splits completely in $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$ into

$$\widehat{q}\mathbb{Z}[\zeta_n, \sqrt[n]{-2}] = \prod_{(a,b) \in \widehat{G}} \widehat{\mathfrak{P}}_{a,b}. \tag{C.7}$$

The action of the Galois group $\mathrm{Gal}(\widehat{F}/\mathbb{Q})$ on $\widehat{\mathfrak{P}}_{a,b}$, $(a,b) \in \widehat{G}$, can be obtained straightforwardly: $\widehat{\sigma}_{a,b}(\widehat{\mathfrak{P}}_{c,d}) = \widehat{\mathfrak{P}}_{c/a,d-b}$. Moreover, since $\widehat{q}$ splits completely in $\mathbb{Z}[\zeta_n, \sqrt[n]{-2}]$, we have an isomorphism $\mathbb{Z}/\widehat{q}\mathbb{Z} \cong \mathbb{Z}[\zeta_n, \sqrt[n]{-2}]/\widehat{\mathfrak{P}}_{a,b}$ for all $(a,b) \in \widehat{G}$, from which we deduce that $\mathrm{Nm}(\widehat{\mathfrak{P}}_{a,b}) = \widehat{q}$ [23].

# D The Splitting Field of $Y^n - r$

In this section, we look at the splitting field $F_r$ of $Y^n - r$, where $n$ $(\geq 8)$ is a power-of-two integer and $|r|$ $(\geq 3)$ is a prime number. We compute the Galois group $\mathrm{Gal}(F_r/\mathbb{Q})$ and introduce a 2NTT for $\mathbb{Z}[\zeta_n, \sqrt[n]{r}]$.

## D.1 The Computation of the Galois Group

The splitting field $F_r$ of $Y^n - r$ is generated by $\zeta_n$ and $\sqrt[n]{r}$: $F_r = \mathbb{Q}(\zeta_n, \sqrt[n]{r})$. In order to compute the degree of $F_r$ over $\mathbb{Q}$, we first need to find all the quadratic subfields of $\mathbb{Q}(\zeta_n)$.

**Lemma D.1.** *Given a power-of-two integer $n$ $(\geq 8)$, the only quadratic subfields of $\mathbb{Q}(\zeta_n)$ are $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$.*

*Proof.* From the fundamental theorem of Galois theory [25], the quadratic subfields of $\mathbb{Q}(\zeta_n)$ correspond to the subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with index being 2. From Section 2.3.2, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is $\langle\varsigma_5\rangle \times \langle\varsigma_{n-1}\rangle$, where the order of $\varsigma_5$ is $n/4$ and the order of $\varsigma_{n-1}$ is 2. Define pr to be the natural projection map

$$\mathrm{pr} : \langle\varsigma_5\rangle \times \langle\varsigma_{n-1}\rangle \to \langle\varsigma_5\rangle,$$

the kernel of which is the subgroup $\langle\varsigma_{n-1}\rangle$ of order 2.

Suppose $H$ is a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of index 2. If $\langle\varsigma_{n-1}\rangle$ is a subgroup of $H$, then $\mathrm{pr}(H)$ is a subgroup of $\langle\varsigma_5\rangle$ of index 2, namely the order of $\mathrm{pr}(H)$ is $n/8$. Since $\langle\varsigma_5\rangle$ is a cyclic group of order $n/4$, we immediately deduce that $\mathrm{pr}(H)$ is $\langle\varsigma_5^2\rangle$, hence $H$ is $\langle\varsigma_5^2\rangle \times \langle\varsigma_{n-1}\rangle$. The subfield of $\mathbb{Q}(\zeta_n)$ fixed by $H$ is $\mathbb{Q}(\zeta_n^{n/8} + \zeta_n^{7n/8})$, i.e., $\mathbb{Q}(\sqrt{2})$.

If $\langle\varsigma_{n-1}\rangle$ is not a subgroup of $H$, then pr must be surjective since the order of $H$ is $n/4$, which is equal to the order of $\langle\varsigma_5\rangle$. Therefore, we deduce $H = \langle\varsigma_5\rangle$ or $H = \langle\varsigma_5 \circ \varsigma_{n-1}\rangle$. If $H = \langle\varsigma_5\rangle$, then the subfield of $\mathbb{Q}(\zeta_n)$ fixed by it is $\mathbb{Q}(\sqrt{-1})$. If $H = \langle\varsigma_5 \circ \varsigma_{n-1}\rangle$, then the subfield of $\mathbb{Q}(\zeta_n)$ fixed by it is $\mathbb{Q}(\sqrt{-2})$. □

We now adapt the proof in [38] to prove the following proposition.

**Proposition D.2.** *The degree of $F_r$ over $\mathbb{Q}$ is $n^2/2$.*

*Proof.* As the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $n/2$ and the degree of $\mathbb{Q}(\sqrt[n]{r})$ over $\mathbb{Q}$ is $n$, so the degree of $F_r$ over $\mathbb{Q}$ satisfies [25]

$$[F_r : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt[n]{r}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\sqrt[n]{r}) : \mathbb{Q}]} = \frac{n^2/2}{[\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\sqrt[n]{r}) : \mathbb{Q}]}.$$

Let $[\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\sqrt[n]{r}) : \mathbb{Q}]$ be $m$, which is also a power-of-two integer and $m \leq n/2$. Let $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\sqrt[n]{r})$ be denoted by $K$, we now show $K = \mathbb{Q}(\sqrt[m]{r})$. The norm of $\sqrt[n]{r}$ over $K$, denoted by $\mathrm{Nm}_{\mathbb{Q}(\sqrt[n]{r})/K}(\sqrt[n]{r})$, is given by the product of $n/m$ conjugates of $\sqrt[n]{r}$ over $K$. But each of these conjugates is of the form $\zeta_n^i \cdot \sqrt[n]{r}$, hence the norm of $\sqrt[n]{r}$ must be of the form

$$\mathrm{Nm}_{\mathbb{Q}(\sqrt[n]{r})/K}(\sqrt[n]{r}) = \zeta_n^j \cdot \sqrt[n]{r}^{n/m} = \zeta_n^j \cdot \sqrt[m]{r} \in K.$$

But $K$ also lies in $\mathbb{Q}(\zeta_n)$, thus $\zeta_n^j \cdot \sqrt[m]{r}$ is in $\mathbb{Q}(\zeta_n)$, hence $\sqrt[m]{r}$ is also in $\mathbb{Q}(\zeta_n)$. The upshot is that $\sqrt[m]{r} \in K$. But $[\mathbb{Q}(\sqrt[m]{r}) : \mathbb{Q}]$ is also $m$, so $K = \mathbb{Q}(\sqrt[m]{r})$.

The Galois group of $\mathbb{Q}(\zeta_n)$ is abelian, therefore every subfield is a Galois extension of $\mathbb{Q}$, which tells us $K$ is a Galois extension of $\mathbb{Q}$ [25]. As a result, $K$ contains all the conjugates of $\sqrt[m]{r}$. In particular, $K$ contains $\zeta_m \cdot \sqrt[m]{r}$, which implies $\zeta_m \in K$. So $K$ is a real subfield of $\mathbb{Q}(\zeta_n)$, whence $m \leq 2$. From Lemma D.1, $\mathbb{Q}(\sqrt[2]{r})$ cannot be in $\mathbb{Q}(\zeta_n)$ if $|r| \geq 3$, hence $m = 1$ and $K = \mathbb{Q}$. Thus completes the proof. □

The Galois group of $F_r$ over $\mathbb{Q}$, $\text{Gal}(F_r/\mathbb{Q})$, can be computed similarly. An element of $\text{Gal}(F_r/\mathbb{Q})$ is determined by its actions on $\zeta_n$ and $\sqrt[n]{r}$:

$$\sigma_{a,b}(\zeta_n) = \zeta_n^a \text{ and } \sigma_{a,b}(\sqrt[n]{r}) = \zeta_n^b \cdot \sqrt[n]{r},$$

where $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/n\mathbb{Z}$. From Proposition D.2, there is no further restriction on the values of $a$ and $b$. Let $G_r$ be the finite set

$$G_r = \left\{(a,b) : a \in (\mathbb{Z}/n\mathbb{Z})^\times \text{ and } b \in \mathbb{Z}/n\mathbb{Z}\right\},$$

then $\text{Gal}(F_r/\mathbb{Q})$ is given by $\{\sigma_{a,b} : (a,b) \in G_r\}$. The canonical embedding of $F_r$ into $\mathbb{C}^{n^2/2}$ can be constructed similarly:

$$\sigma : x \in F_r \mapsto (\sigma_{a,b}(x))_{(a,b)\in G_r} \in \mathbb{C}^{n^2/2}. \tag{D.1}$$

**Proposition D.3.** *Under the canonical embedding of $F_r$ into $\mathbb{C}^{n^2/2}$, we have:*

$$\langle \sigma(\zeta_n^{k_0} \sqrt[n]{r}^{k_1}), \sigma(\zeta_n^{l_0} \sqrt[n]{r}^{l_1}) \rangle = \begin{cases} \sqrt[n]{|r|}^{2k_1} \cdot n^2/2, & \textit{if } k_0 = l_0 \textit{ and } k_1 = l_1; \\ 0, & \textit{otherwise.} \end{cases}$$

*Proof.* The proof uses similar method as in the proof of Proposition 3.1. □

However, we only know $\mathbb{Z}[\zeta_n, \sqrt[n]{r}]$ is an order of $F_r$ [4, 23]. The hardness of Order-LWE in $\mathbb{Z}[\zeta_n, \sqrt[n]{r}]$ can be analysed similarly. A mild issue is that under the canonical embedding, the length of the shortest vector $\sigma(\zeta_n^{k_0})$ is $n/\sqrt{2}$, while the length of the longest vector $\sigma(\zeta_n^{k_0} \sqrt[n]{r}^{n-1})$ is $|r|^{1-1/n} n/\sqrt{2}$, which is almost $|r|$ times larger than the shortest ones. This could potentially lead to some technical issues when choosing the error distributions for Order-LWE in $\mathbb{Z}[\zeta_n, \sqrt[n]{r}]$, which deserves further studies [4, 20].

## D.2 The 2NTT

Via sending $\zeta_n$ to $X$ and $\sqrt[n]{r}$ to $Y$, $\mathbb{Z}[\zeta_n, \sqrt[n]{r}]$ is isomorphic to the ring

$$\mathcal{R}' = \mathbb{Z}[X,Y]/\langle X^{n/2}+1, Y^n - r\rangle.$$

The 2NTT for the ring $\mathcal{R}'$ can be defined similarly as in Section 6. Suppose $p$ is a prime number such that there exist $\alpha, \beta \in \mathbb{F}_p$ that satisfy $\alpha^{n/2} + 1 \equiv 0 \bmod p$ and $\beta^n - r \equiv 0 \bmod p$. Then the roots of $X^{n/2} + 1 \equiv 0 \bmod p$ are $\{\alpha^{2i+1} : 0 \leq i < n/2\}$ and the roots of $Y^n - r \equiv 0 \bmod p$ are $\{\alpha^j \beta : 0 \leq j < n\}$. The 2NTT of a polynomial $\mathbf{F}(X,Y) \in \mathcal{R}'_p$ is to evaluate it at the $n^2/2$ root-pairs

$$\left\{(\alpha^{2i+1}, \alpha^j\beta) : 0 \leq i < n/2,\ 0 \leq j < n\right\}.$$

The vector butterfly for 2NTT follows immediately from Section 6:

1. Transverse vector butterfly, which is the evaluation of $\mathbf{F}(X, Y)$ at the roots $X = \alpha^{2i+1}$, $0 \leq i < n/2$. It consists of $\log_2(n/2)$ stages, and each stage costs $O(n)$ vector operations. The output is an $n/2 \times n$ matrix, with each row the coefficient vector of the one-variable polynomial $\mathbf{F}(\alpha^{2i+1}, Y)$ for some $0 \leq i < n/2$.

2. Transpose and longitudinal vector butterfly, which is the evaluation of a vector-valued polynomial constructed from the column vectors of the output of the first phase at the roots $Y = \alpha^j \beta$, $0 \leq j < n$. It consists of $\log_2 n$ stages and each stage costs $O(n)$ vector operations. The output is an $n/2 \times n$ matrix.

Hence, the total complexity of 2NTT is $O(n \log_2 n)$ vector operations.

# References

[1] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. *Electron. Colloquium Comput. Complex.*, TR96, 1997.

[2] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando Brandao, David Buell, Brian Burkett, Yu Chen, Jimmy Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Michael Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew Harrigan, Michael Hartmann, Alan Ho, Markus Rudolf Hoffmann, Trent Huang, Travis Humble, Sergei Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, Dave Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod Ryan McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin Jeffery Sung, Matt Trevithick, Amit Vainsencher, Benjamin Villalonga, Ted White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John Martinis. Quantum supremacy using a programmable superconducting processor. *Nature*, 574:505–510, 2019.

[3] Michael Francis Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley-Longman, 1969.

[4] Madalina Bolboceanu, Zvika Brakerski, and Devika Sharma. On algebraic embedding for unstructured lattices. Cryptology ePrint Archive, Paper 2021/053, 2021. `https://eprint.iacr.org/2021/053`.

[5] Carl Bootland, Wouter Castryck, and Frederik Vercauteren. On the Security of the Multivariate Ring Learning with Errors Problem. Cryptology ePrint Archive, Paper 2018/966, 2018. `https://eprint.iacr.org/2018/966`.

[6] Joppe Bos, Ducas Léo, Eike Kiltz, Tancréde Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS–Kyber: a CCA-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367. IEEE, 2018.

[7] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3):1–36, 2014.

[8] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *Proceedings of the forty-fifth annual ACM symposium on Theory of Computing*, pages 575–584, 2013.

[9] Lidong Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. Report on post-quantum cryptography, 2016-04-28 2016.

[10] Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, and Yongsoo Song. Bootstrapping for Approximate Homomorphic Encryption. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 360–384, Cham, 2018. Springer International Publishing.

[11] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song. Homomorphic encryption for arithmetic of approximate numbers. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 409–437. Springer, 2017.

[12] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. TFHE: Fast Fully Homomorphic Encryption Over the Torus. *Journal of Cryptology*, 33(1):34–91, 2020.

[13] Keith Conrad. GALOIS THEORY AT WORK: CONCRETE EXAMPLES. `https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisappn.pdf`.

[14] Michel H. Devoret and Robert J. Schoelkopf. Superconducting circuits for quantum information: An outlook. *Science*, 339:1169 – 1174, 2013.

[15] Leo Ducas, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehle. Crystals – dilithium: Digital signatures from module lattices. Cryptology ePrint Archive, Paper 2017/633, 2017. `https://eprint.iacr.org/2017/633`.

[16] Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. *IACR Cryptol. ePrint Arch.*, 2012:144, 2012.

[17] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 169–178, 2009.

[18] Serge Lang. *Cyclotomic fields I and II*, volume 121. Springer Science & Business Media, 2012.

[19] Haohao Liao, Mahmoud A. Elmohr, Xuan Dong, Yanjun Qian, Wenzhe Yang, Zhiwei Shang, and Yin Tan. Turbohe: Accelerating fully homomorphic encryption using fpga clusters. In *2023 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, pages 788–797, 2023.

[20] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *Journal of the ACM*, 60(6):1–35, 2013.

[21] Daniel A. Marcus. *Number Fields.* Springer, 2018.

[22] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. In *45th Annual IEEE Symposium on Foundations of Computer Science*, pages 372–381, 2004.

[23] James S. Milne. Algebraic Number Theory (v3.08), 2020. Available at www.jmilne.org/math/.

[24] James S. Milne. Group Theory (v4.00), 2021. Available at www.jmilne.org/math/.

[25] James S. Milne. Fields and Galois Theory (v5.10), 2022. Available at www.jmilne.org/math/.

[26] NIST. PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates. `https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4`.

[27] Henry J. Nussbaumer. *Fast Fourier Transform and Convolution Algorithms.* Springer series in information sciences. Springer, 1990.

[28] Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, Nicolas Gama, Mariya Georgieva, and Fernando Pérez-González. Revisiting multivariate ring learning with errors and its applications on lattice-based cryptography. Cryptology ePrint Archive, Paper 2019/1109, 2019. `https://eprint.iacr.org/2019/1109`.

[29] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 333–342, 2009.

[30] Chris Peikert. How (Not) to Instantiate Ring-LWE. In Vassilis Zikas and Roberto De Prisco, editors, *Security and Cryptography for Networks*, pages 411–430, Cham, 2016. Springer International Publishing.

[31] Oded Regev. New lattice-based cryptographic constructions. *Journal of the ACM (JACM)*, 51(6):899–942, 2004.

[32] Oded Regev. Lattice-based cryptography. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006*, pages 131–141, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[33] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[34] M Sadegh Riazi, Kim Laine, Blake Pelton, and Wei Dai. HEAX: An Architecture for Computing on Encrypted Data. In *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems*, pages 1295–1309, 2020.

[35] Nikola Samardzic, Axel Feldmann, Aleksandar Krastev, Srinivas Devadas, Ronald Dreslinski, Christopher Peikert, and Daniel Sanchez. F1: A fast and programmable accelerator for fully homomorphic encryption. In *MICRO-54: 54th Annual IEEE/ACM International Symposium on Microarchitecture*, pages 238–252, 2021.

[36] Nikola Samardzic, Axel Feldmann, Aleksandar Krastev, Nathan Manohar, Nicholas Genise, Srinivas Devadas, Karim Eldefrawy, Chris Peikert, and Daniel Sanchez. Craterlake: a hardware accelerator for efficient unbounded computation on encrypted data. In *ISCA'22: Proceedings of the 49th Annual International Symposium on Computer Architecture*, pages 173–187, 2022.

[37] William Stein. Algebraic Number Theory, a Computational Approach, 2012. Available at https://wstein.org/books/ant/ant.pdf.

[38] Michael Zieve. Galois Group of $x^n - 2$. `https://mathoverflow.net/questions/143739/galois-group-of-xn-2`, October 2013.