Exploring General Cyclotomic Rings in Torus-Based Fully Homomorphic Encryption: Part I - Prime Power Instances*

P. Chartier[†], M. Koskas[‡] and M. Lemou[§]

March 14, 2025

Abstract

In the realm of fully homomorphic encryption on the torus, we investigate the algebraic manipulations essential for handling polynomials within cyclotomic rings characterized by prime power indices. This includes operations such as modulo reduction, computation of the trace operator, extraction, and the blind rotation integral to the bootstrapping procedure, all of which we reformulate within this mathematical framework.

Keywords: fully homomorphic encryption, residue number system, trace operator, extraction, bootstrapping.

1 Introduction

Non-power of two cyclotomic polynomials, which pertain to cyclotomic rings indexed by integers M that are not restricted to the form $M = 2^k$, carry significant implications for fully homomorphic encryption (FHE) systems. Non-power of two cyclotomic polynomials Φ_M are associated with a wider variety of primitive roots of unity. Generally speaking, this diversity allows for richer algebraic structures and facilitates computations on more complex data types, thus enhancing the versatility of FHE schemes. In particular, we highlight four main advantages that we believe justify the current work:

- Increased Input Space: Utilizing cyclotomic rings beyond powers of two can significantly expand the plaintext space available for bootstrapping operations. This makes it feasible to encrypt and perform homomorphic computations on a greater range of data, improving the overall utility of the encryption scheme.
- Flexibility in Parameter Choices: Non-power of two cyclotomic polynomials enables the tailoring of FHE parameters to better suit particular applications or security requirements. This adaptability is crucial for developing practical implementations that meet specific performance benchmarks or operational contexts.

*This work was partly conducted while the first and last authors were affiliated with Ravel Technologies and is protected by Ravel Technologies patents.

†INRIA-IRMAR-University of Rennes, Campus de Beaulieu, 35042 Rennes Cedex

‡Ravel Technologies, 75 rue de Richelieu, 75020 Paris

§CNRS-IRMAR-University of Rennes, Campus de Beaulieu, 35042 Rennes Cedex

- Potential for Optimized Bootstrapping: With a broader range of polynomial forms to work with, one can devise methods that enhance the efficiency and effectiveness of noise reduction techniques.

- Beginning the Transition to General Cyclotomic Polynomials: Advancing toward fully general cyclotomic polynomials presents several computational advantages, which will be examined in an upcoming paper.

The standard TFHE [13] and FHEW [18] schemes, primarily operating under the assumption that $M = 2^k$, have rarely been practically extended to more general cyclotomic rings. In fact, such extensions have typically been limited to cyclotomic polynomials of the forms $M = 2^\alpha 3^\beta$ [21, 22] or $M = t^\alpha$ as shown in [2], particularly for homomorphically testing the equality of an encrypted message with a specified plaintext message. Here, we propose an extension of both the FHEW and TFHE *comprehensive* frameworks to include the class of M-th cyclotomic polynomials with $M = t^\alpha$, where t is any prime integer greater than or equal to 3, and α is any non-zero integer. More concretely, whereas traditional TFHE systems often operate within the polynomial ciphertext space defined as:

$$\mathbb{Z}[X]/(X^{2^k}+1) \quad \text{and} \quad \mathbb{T}[X]/(X^{2^k}+1), \quad \mathbb{T} = \mathbb{Q}/\mathbb{Z},$$

we are addressing a broader scenario characterized by:

$$\mathcal{R} := \mathbb{Z}[X]/(\Phi_M(X)) \quad \text{and} \quad \mathcal{T} := \mathbb{T}[X]/(\Phi_M(X)),$$

where M adopts the aforementioned form $M = t^\alpha$. The extension to the fully general case $M = t_1^{\alpha_1} t_2^{\alpha_2} \cdots t_r^{\alpha_r}$, which introduces additional complexities as well as new possibilities, will be elaborated upon in Part II.

In the following sections, we will delve into the processes of extraction, bootstrapping, and fast homomorphic evaluation of the trace operator. Tasks such as *blind extraction* and *fast packing* will be addressed in a forthcoming publication. Our objective is to clarify the purpose of each procedure and illustrate how the original methods can be adapted and improved or simplified for the current context. Before exploring these topics, we will introduce in Section 3 the essential algebraic tools needed for constructing the various algorithms detailed. Furthermore, we will provide a brief overview of standard procedures for LWE and RLWE, including encryption, decryption, addition, and external product, as discussed in Section 5. It is important to note that throughout this text, we consider messages in $\frac{1}{p}\mathbb{Z}_p$, with applications to large integers through the Residual Number System in mind, as explored in [6, 7, 8, 9].

We will now summarize the main content of the paper: Section 6 centers on the extraction of the coefficient μ_i from the encrypted polynomial $\mu(X)$ expressed in any basis of $\mathcal{T}$. Although this process is a common practice, we propose a systematic approach to defining it within any prime-power cyclotomic field. This section also presents an opportunity to highlight the importance of the dual basis with respect to the scalar product associated to the trace and sets the stage for the situation where the index i is encrypted-an aspect that will be explored in an upcoming publication, as previously mentioned.

In Section 7, we redefine the standard functional bootstrapping procedure in terms of the trace operator and the dual basis. We will show that this formulation allows for a clear articulation of the "negacyclic" conditions that the functions to be bootstrapped must satisfy, particularly within the context of prime-power cyclotomic fields. Moreover, we will emphasize the advantages of considering polynomials that are not powers of two.

Section 8 offers a comprehensive overview of different traces. We will demonstrate how standard Galois theory is utilized within our particular algebraic framework to enhance the efficiency of computing the trace from a field to its subfield. The authors believe that the trace operator is highly beneficial for a range of applications, which is why its factored homomorphic evaluation holds a prominent position in this paper.

2 Related works

The selection of underlying algebraic structures, particularly cyclotomic polynomials, is a crucial element of Fully Homomorphic Encryption (FHE) schemes, as these choices significantly influence efficiency and functionality. Notably, several studies have investigated the adaptation of the Number Theoretic Transform (NTT) for these polynomials, which can greatly enhance the speed of polynomial multiplication, with efficiency gains being especially pronounced for specific parameter selections, as demonstrated by Bajard et al. [1] in their RNS variant of FV-like schemes. In addition to efficiency, noise growth behavior presents another critical concern, particularly as it differs from what is observed in power-of-two cyclotomic rings; this issue was examined in the recent paper by De Micheli et al. [17], underscoring the importance of understanding noise dynamics for establishing the parameters and overall effectiveness of FHE schemes. For instance, Kim et al. [23] explore how these polynomials specifically impact noise growth within the context of private query processing. When employing prime-power cyclotomic polynomials, selecting optimal parameters becomes increasingly complex due to the interplay between polynomial structure, noise growth, and security considerations. Costache and Smart [15] provide a comprehensive comparison of various ring choices, offering detailed evaluations of schemes that utilize different prime-power cyclotomic structures. Given the critical nature of security in FHE schemes based on prime-power cyclotomic polynomials, Eric Crockett and Chris Peikert [16] explore significant obstacles associated with the Ring Learning With Errors (Ring-LWE) problem. They discuss various factors that complicate the implementation and security of RLWE-based schemes, including issues related to parameter selection, the implications of error distributions, and the impact of specific polynomial structures on both security and efficiency. Finally, extension to multivariate RLWE with several cyclotomic polynomials is for instance considered in [3] while Chen et al. [11] investigate potential vulnerabilities and attack strategies that could be exploited due to the unique characteristics of Galois non-dual RLWE families.

3 Algebraic setting

In this section, we present several basic definitions essential for the foundation of the encryption protocol. While some of this material could have been introduced later in the paper, doing so would have compromised clarity, as many concepts here also possess more compact though more abstract definitions we could have relied upon. The identification of the dual sets $\mathcal{R}^\vee$ and $\mathcal{T}^\vee$ with their expressions is provided below.

3.1 Prime power cyclotomic polynomials

We begin by briefly revisiting the definition of cyclotomic polynomials, along with some of their properties and representations when M is a power of a prime.

Definition 3.1 *The M^{th} cyclotomic polynomial is defined by the formula*

$$\Phi_M(X) = \prod_{\substack{1\leq k\leq M \\ \gcd(k,M)=1}} \left(X - e^{2i\pi\frac{k}{M}}\right).$$

The cyclotomic polynomials are monic polynomials with integer coefficients that are irreducible over the field of the rational numbers. Except for $M = 1, 2$, they are palindromes of even degree. The degree of Φ_M, or in other words the number of M^{th}- primitive roots of unity, is $N = \varphi(M)$, where φ is Euler's totient function. As we consider indices of the form $M = t^\alpha$, where t is a prime number and $\alpha \geq 1$, only two relational definitions are necessary for computing the cyclotomic polynomials we need:

1. Cyclotomic Polynomial for a Prime: If t is a prime number, the t^{th} cyclotomic polynomial $\Phi_t(X)$ is defined as:

$$\Phi_t(X) = 1 + X + X^2 + \cdots + X^{t-1} = \sum_{k=0}^{t-1} X^k.$$

   This polynomial has roots that are the primitive t^{th} roots of unity, and it is irreducible over the integers.

2. Cyclotomic Polynomial for Prime Powers: If $M = t^\alpha$ with $\alpha \geq 2$, where t is prime, the M^{th} cyclotomic polynomial can be expressed as:

$$\Phi_{t^\alpha}(X) = \Phi_t(X^{t^{\alpha-1}}) = \sum_{k=0}^{t-1} X^{kt^{\alpha-1}}.$$

   This relation indicates that the cyclotomic polynomial for the prime power t^α is derived by substituting $X^{t^{\alpha-1}}$ into the t^{th} cyclotomic polynomial. The resulting polynomial captures the multiples of $t^{\alpha-1}$ in its exponents.

We end up this subsection by stating a useful (and well-known) relation on cyclotomic polynomials:

Proposition 3.2 *Let M be a positive integer and d a coprime with M. Then*

$$\Phi_M(X) | \Phi_M(X^d).$$

3.2 The cyclotomic field $\mathcal{K}$ and the ring of algebraic integers $\mathcal{R}$

All sets of polynomials examined in the following sections are embedded within the set of polynomials with rational coefficients modulo Φ_M, which we will refer to as $\mathcal{K}$. This set constitutes a Galois extension of $\mathbb{Q}$ and possesses the structure of both a field and a $\mathbb{Q}$-linear space with dimension $N = \varphi(M)$. It is thus natural to consider the action of the trace operator on $\mathcal{K}$, the associated scalar product on $\mathcal{K}^2$ and to develop the dual basis of the canonical basis from which both $\mathcal{R}^\vee$ and $\mathcal{T}^\vee$ can be described. In this paper, we will use the notation $P \bmod \Phi_M$ interchangeably to refer either to the equivalence class $P(X) + \Phi_M(X)Q(X)$, where $Q \in \mathbb{Q}[X]$, or to the representative element P of this class.

Definition 3.3 (Field of rational polynomials modulo Φ_M) *The field of polynomials with coefficients in $\mathbb{Q}$ modulo $\Phi_M(X)$ is defined as the quotient ring*

$$\mathcal{K} = \frac{\mathbb{Q}[X]}{(\Phi(X))} = \Big\{ P \text{ mod } \Phi_M,\ P \in \mathbb{Q}_{N-1}[X] \Big\}.$$

The field $\mathcal{K}$ is also a Galois extension of $\mathbb{Q}$ of dimension $N = \varphi(M)$. We denote the ring of algebraic integers of $\mathcal{K}$ as $\mathcal{R}$: it is made of the equivalence classes of $\mathcal{K}$ which have representatives in $\mathbb{Z}_{N-1}[X]$, that is to say

$$\mathcal{R} = \Big\{ P \text{ mod } \Phi_M,\ P \in \mathbb{Z}_{N-1}[X] \Big\}.$$

The trace operator in the context of Galois extensions is a linear map from a field extension (here $\mathcal{K}$) back to its base field (here $\mathbb{Q}$). Denoting the associated Galois group $\mathrm{Gal}(\mathcal{K}/\mathbb{Q})$, the trace of an element $P \in \mathcal{K}$ is given by

$$\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(P) = \sum_{\tau \in \mathrm{Gal}(\mathcal{K}/\mathbb{Q})} \tau(P) \in \mathbb{Q},$$

where the sum accounts for the action of each automorphism τ in the Galois group (that is to say here the group of substitutions $X \mapsto X^d$ for all $1 \leq d \leq M$ coprime with M) on P. As the trace plays a crucial role in studying the structure and properties of $\mathcal{K}$, we give below its definition instantiated in the context of cyclotomic rings:

Definition 3.4 (Trace operator) *The trace operator* Tr *is defined as the linear map*

$$\begin{array}{rccl} Tr: & \mathcal{K} & \longrightarrow & \mathbb{Q} \\ & P(X) & \longmapsto & \displaystyle\sum_{\substack{1 \leq d \leq M \\ \gcd(d,M)=1}} P(X^d) \text{ mod } \Phi_M \end{array} \tag{1}$$

The trace is a well-defined operator on $\mathcal{K}$, as its value does not depend on the particular representative of a class in $\mathcal{K}$: for any d such that $\gcd(d, M) = 1$, the cyclotomic polynomial $\Phi_M(X)$ indeed divides $\Phi_M(X^d)$ (Proposition 8.1), so that

$$\sum_{\substack{1 \leq d \leq M \\ \gcd(d,M)=1}} (P + k\Phi_M)(X^d) = \sum_{\substack{1 \leq d \leq M \\ \gcd(d,M)=1}} P(X^d) \text{ mod } \Phi_M.$$

We are now in position to introduce the following scalar product:

Definition 3.5 (Scalar product) *The scalar product $\langle \cdot, \cdot \rangle$ is defined on $\mathcal{K}^2$ as follows*

$$\forall (P, Q) \in \mathcal{K}^2, \quad \langle P, Q \rangle = \mathrm{Tr}\big(P(X)\bar{Q}(X)\big) \in \mathbb{Q} \tag{2}$$

with $\bar{Q}(X) = Q(X^{-1}) \text{ mod } \Phi_M = Q(X^{M-1}) \text{ mod } \Phi_M$.

Once more, this definition demonstrates consistency since the value of $\langle P, Q \rangle$ remains invariant regardless of the particular representatives selected for P mod Φ_M and Q mod Φ_M. This invariance is a consequence of the relation $\bar{\Phi}_M = 0 \text{ mod } \Phi_M$ (see Proposition 8.1). Furthermore, it is straightforward to verify that this scalar product adheres to the typical requirements found in vector spaces, such as bilinearity, symmetry, and positive definiteness. This ensures that $\langle P, Q\rangle$ is both a well-defined and fundamentally sound operation within the context of this algebraic framework.

Now, given any basis $(B_i)_{0\leq i<N}$ of $\mathcal{K}$, it possesses a dual basis that we shall denote $(B_i^*)_{0\leq i<N} \subset \mathcal{K}$ defined by

$$\forall 0 \leq i, j < N, \quad \langle B_i^*, B_j\rangle = \delta_{i,j}.$$

It is important to notice that the dual basis $(\Omega_i^*)_{0\leq i<N}$ of the canonical basis $(X^i)_{0\leq i<N}$ has the following explicit form (see Proposition 8.1)

$$\begin{aligned}\Omega_i^*(X) &= \frac{1}{M}\left(X^i - X^{N+[i]_{M/t}}\right), \quad 0 \leq i < N, \qquad (3)\\ &= \frac{1}{M}\left(\Omega_i(X) + \sum_{\substack{0\leq j\leq N-1\\ \text{s.t. } [j-i]_{\frac{M}{t}}=0}} \Omega_j(X)\right)\end{aligned}$$

where for $0 \leq i < N$, $[i]_{M/t}$ denotes the integer $0 \leq j < \frac{M}{t}$ such that $i = j \bmod \frac{M}{t}$. Conversely, the inverse formula is given by

$$\Omega_i(X) = M\Omega_i^*(X) - \frac{M}{t} \sum_{\substack{0\leq j\leq N-1\\ \text{s.t. } [j-i]_{\frac{M}{t}}=0}} \Omega_j^*(X) \qquad (4)$$

A few remarks are now in order. First of all, since $\Omega_0^*(X) = \frac{1-X^N}{M}$ and $\Phi_M(X)$ are coprime elements of the euclidean ring $\mathbb{Q}[X]$, the Bezout identity asserts that there exist U and V in $\mathbb{Q}[X]$ such that

$$\Omega_0^*(X)U(X) + \Phi_M(X)V(X) = 1$$

so that

$$U = (\Omega_0^*)^{-1} \bmod \Phi_M$$

and it can be checked that whereas $V(X) = 1 + \frac{1}{t}\left(X^N - \Phi_M(X)\right) \in \mathcal{T}$,

$$(\Omega_0^*)^{-1}(X) = \underbrace{t^{\alpha-1}\Big(1 + \sum_{k=1}^{t-2} (k+1-t)\, X^{k\frac{M}{t}}\Big)}_{\in \mathbb{Z}_{N-1}[X]} \bmod \Phi_M$$

is the representative of an element of $\mathcal{R}$. In particular, it has integer coefficients. This implies, not only that the N-dimensional $\mathbb{Q}$-linear space

$$\mathcal{K} = \Big\{ \sum_{i=0}^{N-1} \lambda_i X^i \bmod \Phi_M,\ (\lambda_0, \ldots, \lambda_{N-1}) \in \mathbb{Q}^N \Big\}$$

coincides, through the paring $\langle\cdot,\cdot\rangle$ and the usual identification of linear forms with elements of $\mathcal{K}$, with its dual space

$$\mathcal{K}^\vee = \Big\{ \sum_{i=0}^{N-1} \omega_i^*\Omega_i^* \bmod \Phi_M,\ (\omega_0^*, \ldots, \omega_{N-1}^*) \in \mathbb{Q}^N \Big\} = \Omega_0^*\mathcal{K} = \mathcal{K}$$

where the last equality stems from the fact that $\mathcal{K}$ is a field, but also that the dual $\mathcal{R}^\vee$ of $\mathcal{R}$ can be identified similarly to $\Omega_0^*\mathcal{R}$. As a matter of fact, a linear form ℓ on

$$\mathcal{R} = \left\{ \sum_{i=0}^{N-1} n_i X^i \bmod \Phi_M,\ (n_0, \dots, n_{N-1}) \in \mathbb{Z}^N \right\}$$

is the restriction to $\mathcal{R}$ of a linear form defined on $\mathcal{K}$ and is thus the action though the pairing $\langle \cdot, \cdot \rangle$ of an element $\Omega^* \bmod \Phi_M \in \mathcal{K}^\vee = \mathcal{K}$ with $\Omega^* = \sum_{i=0}^{N-1} \omega_i^* \Omega_i^*$, i.e.

$$\exists \Omega^* \bmod \Phi_M \in \mathcal{K}^\vee,\ \forall P \in \mathcal{R},\ \ell(P) = \langle \Omega^*, P \rangle \in \mathbb{Q}.$$

For the image of ℓ to be included in $\mathbb{Z}$, as is required for a linear form on the $\mathbb{Z}$-module $\mathcal{R}$, it can be seen that for all $P \bmod \Phi_M \in \mathcal{R}$ with $P(X) = \sum_{i=0}^{N-1} n_i X^i$, one must have

$$\forall n \in \mathbb{Z}^N, \ell(P) = \sum_{i=0}^{N-1} \omega_i^* n_i \in \mathbb{Z}$$

that is to say $\omega^* \in \mathbb{Z}^N$, or in other words

$$\Omega^* \bmod \Phi_M \in \mathcal{R}^\vee = \left\{ \sum_{i=0}^{N-1} \omega_i^* \Omega_i^* \bmod \Phi_M,\ (\omega_0^*, \dots, \omega_{N-1}^*) \in \mathbb{Z}^N \right\} = \Omega_0^* \mathcal{R}.$$

The last equality is derived from the fact that $(\Omega_0^* \Omega_j)_{j=0}^{N-1}$, which forms a basis for the $\mathbb{Q}$-linear space $\mathcal{K}$, also acts as a basis for $\mathcal{R}^\vee$. Specifically, we have:

$$\langle \Omega_0^* \Omega_j, \Omega_k \rangle = \langle \Omega_0^*, \Omega_{-j} \Omega_k \rangle \in \mathbb{Z}$$

owing to the fact that $\Omega_{-j}\Omega_k \in \mathcal{R}$. In particular, the change of basis

$$\begin{pmatrix} 1 \\ (\Omega_0^*)^{-1}\Omega_1^* \\ \vdots \\ (\Omega_0^*)^{-1}\Omega_{N-1}^* \end{pmatrix} = \Phi_t(J^{\frac{M}{t}}) \begin{pmatrix} 1 \\ X \\ \vdots \\ X^{N-1} \end{pmatrix} = \Phi_M(J) \begin{pmatrix} 1 \\ X \\ \vdots \\ X^{N-1} \end{pmatrix} \bmod \Phi_M$$

where

$$J = \begin{pmatrix} 0 & \dots & \dots & \dots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_N(\mathbb{Z}),$$

is cleary unimodular with inverse $(I - J^{\frac{M}{t}}) \in \mathcal{M}_N(\mathbb{Z})$. Furthermore, we observe in passing that $\mathcal{R}^\vee \subset \frac{1}{M}\mathcal{R}$.

3.3 The module $\mathcal{T}$ of polynomials with coefficients in $\mathbb{T}$ and its dual $\mathcal{T}^\vee$

We start by recalling that the torus $\mathbb{T}$ is defined as the set of rational numbers modulo 1, i.e. $\mathbb{T} = \mathbb{Q}/\mathbb{Z}$.

Definition 3.6 *The quotient of the $\mathbb{Z}[X]$-module $\mathcal{K}$ by the sub-module $\mathcal{R}$ is the quotient $\mathbb{Z}[X]$-module $\mathcal{T} = \mathcal{K}/\mathcal{R}$, that is to say the set of equivalence classes*

$$\mathcal{T} = \Big\{ \sum_{i=0}^{N-1} x_i X^i \ mod\ \mathbb{Z}[X]\ mod\ \Phi_M, (x_0, \dots, x_{N-1}) \in \mathbb{Q}^N \Big\}.$$

Definition 3.7 *The quotient of the $\mathbb{Z}[X]$-module $\mathcal{K}$ by the sub-module $\mathcal{R}^\vee$ is the quotient $\mathbb{Z}[X]$-module $\mathcal{T}^\vee = \mathcal{K}/\mathcal{R}^\vee$, that is to say the set of equivalence classes*

$$\mathcal{T}^\vee = \Big\{ \sum_{i=0}^{N-1} \omega_i^* \Omega_i^*(X)\ mod\ \Omega_0^* \mathbb{Z}[X]\ mod\ \Phi_M, (\omega_0^*, \dots, \omega_{N-1}^*) \in \mathbb{Q}^N \Big\}.$$

Remark 3.8 *The polynomial product is well-defined from $\mathcal{R}^\vee \times \mathcal{T}$ to $\mathcal{T}^\vee$, as well as from $\mathcal{R} \times \mathcal{T}^\vee$ to $\mathcal{T}^\vee$. Specifically, we have:*

$$\begin{aligned}\Big(\Omega_0^*(X)Z_1(X) + \Phi_M(X)Q_1(X)\Big) &\times \Big(P_2(X) + Z_2(X) + \Phi_M(X)Q_2(X)\Big) \\ &= \Omega_0^*(X)Z_1(X)P_2(X) + \Omega_0^*(X)Z_1(X)Z_2(X) + \Phi_M(X)Q_3(X) \\ &= \Omega_0^*(X)Z_1(X)P_2(X)\ mod\ \mathcal{R}^\vee\end{aligned}$$

And symmetrically,

$$\begin{aligned}\Big(Z_1(X) + \Phi_M(X)Q_1(X)\Big) &\times \Big(\Omega_0^*(X)P_2(X) + \Omega_0^*(X)Z_2(X) + \Phi_M(X)Q_2(X)\Big) \\ &= \Omega_0^*(X)Z_1(X)P_2(X) + \Omega_0^*(X)Z_1(X)Z_2(X) + \Phi_M(X)Q_3(X) \\ &= \Omega_0^*(X)Z_1(X)P_2(X)\ mod\ \mathcal{R}^\vee\end{aligned}$$

Here, Z_1 and Z_2 are polynomials in $\mathbb{Z}[X]$, while P_2, Q_1, Q_2, and Q_3 are polynomials in $\mathbb{Q}[X]$. Note that the multiplication of a polynomial of $\mathcal{R}$ by a a polynomial of $\mathcal{T}$ also makes sense, in contrast with the case where both are in the duals $\mathcal{R}^\vee$ and $\mathcal{T}^\vee$.

Remark 3.9 *Consider a linear form $\ell \in \mathcal{L}(K, \mathbb{Q})$ represented by*

$$\sum_{i=0}^{N-1} \omega_i^* \Omega_i^*(X) + \Phi_M(X)\tilde{Q}(X)$$

in $\mathcal{K}^\vee = \mathcal{K}$, where $\tilde{Q}$ is a polynomial in $\mathbb{Q}[X]$. The application ℓ can be consistently defined on $\mathcal{T}$ as follows:

$$\begin{array}{rcl} \ell : \mathcal{T} & \to & \mathbb{T} \\ \sum_{i=0}^{N-1} x_i X^i + Z(X) + \Phi_M(X)Q(X) & \mapsto & \Big\langle \sum_{i=0}^{N-1} \omega_i^* \Omega_i^*(X), \sum_{i=0}^{N-1} x_i X^i \Big\rangle\ mod\ 1 \end{array}$$

provided that $(\omega_0^*, \ldots, \omega_{N-1}^*) \in \mathbb{Z}^{N-1}$. *In fact, the value of*

$$\Big\langle \sum_{i=0}^{N-1} \omega_i^* \Omega_i^*(X) + \Phi_M(X)\tilde{Q}(X), \sum_{i=0}^{N-1} x_i X^i + Z(X) + \Phi_M(X)Q(X) \Big\rangle$$
$$= \sum_{i=0}^{N-1} \omega_i^* x_i + \Big\langle \sum_{i=0}^{N-1} \omega_i^* \Omega_i^*(X), Z(X) \Big\rangle \ mod\ 1$$

depends on Z *unless* $\langle \sum_{i=0}^{N-1} \omega_i^* \Omega_i^*, Z \rangle \in \mathbb{Z}$, *which necessitates that* $(\omega_0^*, \ldots, \omega_{N-1}^*) \in \mathbb{Z}^{N-1}$. *In other words,* ℓ *is defined by an element of* $\mathcal{R}^\vee$.

4 Plaintext messages in the TFHE framework

In the context of TFHE, all messages, also referred to as *plaintext messages* or simply *plaintexts*, can be classified into two types: either as elements of the torus $\mathbb{T}$, or as polynomials within a cyclotomic ring, with coefficients that belong either to $\mathbb{T}$ or $\mathbb{Z}$.

4.1 The set of torus plaintexts

Despite the fact that all elements of the torus can be encrypted, only a discretized subset can be safely decrypted. This observation leads to the following definition:

Definition 4.1 (Discretized torus for messages) *Let* $p \geq 3$ *be an odd integer. The structure of the discrete torus* $\mathbb{T}_p$ *is inherited from* $(\mathbb{Z}_p, +, \times)$, *with privileged representative*[1]

$$i \ mods\ p.$$

The discrete torus $\mathbb{T}_p \subset \mathbb{T} = [-\frac{1}{2}, \frac{1}{2}) + \mathbb{Z}$ *is defined by* $\mathbb{T}_p = \frac{1}{p}\mathbb{Z}_p$:

$$\mathbb{T}_p = \big\{ -(p-1)/(2p), ..., (p-1)/(2p) \big\} + \mathbb{Z}$$

This definition is crucial in the design of schemes such as TFHE, where ensuring the integrity of decrypted messages relies on restricting the plaintext space to a manageable and well-defined subset. The choice of this discretized subset ultimately influences the efficiency, security, and overall functionality of the homomorphic encryption system. It allows the framework to balance between operational flexibility and the necessary constraints imposed by noise growth during cryptographic operations. Note that $\mathbb{T}_p$, the p-adic torus, is a ring that is isomorphic to $(\mathbb{Z}_p, +, \times)$. Its structure can be outlined as follows:

1. Addition: The addition operation in $\mathbb{T}_p$ is inherited from the torus $\mathbb{T}$. Specifically, for any $(x, y) \in \mathbb{T}_p \times \mathbb{T}_p$:
$$x + y \equiv x + y \text{ mod } 1.$$
2. Multiplication: The multiplication in $\mathbb{T}_p$ is inherited from the integers modulo p. For any $(x, y) \in \mathbb{T}_p \times \mathbb{T}_p$:
$$x \times y = (px) \times y \text{ mod } 1.$$

[1] The symmetric modulo operation returns the remainder of a division such that the result is centered around zero. For a number i and odd modulus p, it maps i to the interval $\big\{ -(p-1)/2, ..., (p-1)/2 \big\}$, ensuring the result is balanced symmetrically around zero.

4.2 The set of polynomial plaintexts

The extension to prime power cyclotomic rings manifests itself when considering polynomial messages and all subsequent attached procedures (packing, extraction, bootstrapping...).

Definition 4.2 (Polynomial plaintext) *Let M be a non-zero integer and let Φ_M be the M^{th} cyclotomic polynomial. Polynomial plaintexts are polynomial representatives of equivalence classes, either in $\mathcal{R}$ or in*

$$\mathcal{T}_p = \left\{ P(X) \ mod \ \mathbb{Z}[X] \ mod \ \Phi_M, P \in \frac{1}{p}\mathbb{Z}[X] \right\} \subset \mathcal{T}.$$

The polynomials in $\mathcal{T}_p$ can not only be encrypted and manipulated but also decrypted exactly with a high probability under standard parameter conditions (see next Section).

5 LWE and RLWE encryptions cryptographic schemes

5.1 Encryption/decryption schemes in $\mathbb{T}$

Learning With Errors (LWE) is a cryptographic problem widely used in post-quantum cryptography due to its hardness against quantum attacks [30]. The LWE problem consists in solving systems of noisy linear equations. More specifically, given a secret vector $\mathbf{s} \in \mathbb{S}^n$, where $\mathbb{S}$ is a finite subset of $\mathbb{Z}$, if we are given a set of linear equations of the form

$$\mathbf{c} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e},$$

where $\mathbf{A}$ is randomly chosen matrix over a finite field (e.g., modulo $\mathbb{Z}_q$) and $\mathbf{e}$ is a random noise vector with small entries, recovering $\mathbf{s}$ from the equations is computationally hard. Of course, if $\mathbf{A} \in \mathcal{M}_n(\mathbb{Z}_q)$ and $\mathbf{e} \in (\mathbb{Z}_q)^n$, the actual hardness depends on how large q and n are. When it is hard enough, the LWE-problem is said to be secure.

Now, assume the LWE-problem on $\mathbb{Z}_q$ is secure and assimilate $\mathbb{T} \equiv \frac{1}{q}\mathbb{Z}_q$ for the purpose of the following definition [12, 13].

Definition 5.1 (EncryptLWE$_\mathbf{s}(\mu)$) *The* LWE*-encryption of a message $\mu \in \mathbb{T}$ with the secret key $\mathbf{s} \in \mathbb{S}^n$ is defined as*

$$\mathbf{c} = \mathrm{LWE}_\mathbf{s}(\mu) = (\mathbf{a}, b) \in \mathbb{T}^{n+1}$$

with

$$\mathbf{a} = (a_1, \ldots, a_n) \overset{\$}{\leftarrow} \mathbb{T}^n, \quad e \leftarrow \mathcal{N}(0, \sigma^2)$$

and

$$b = \mathbf{s} \cdot \mathbf{a} + \mu + e.$$

Algorithm 1 LWE Encryption of Message μ

Input: Message $\mu \in \mathcal{T}$, secret key $\mathbf{s} \in \mathbb{S}^n$.

Generate random vector: $\mathbf{a} = (a_1, \ldots, a_n) \overset{\$}{\leftarrow} \mathcal{T}^n$
Sample error term: $e \leftarrow \mathcal{N}(0, \sigma^2)$
$b \leftarrow \mathbf{s} \cdot \mathbf{a} + \mu + e$
Return $\mathbf{c} = (\mathbf{a}, b)$.

Definition 5.2 (DecryptLWE$_\mathbf{s}$ $(\mathbf{c}, p)$) *The* LWE*-decryption of a ciphertext* $(\mathbf{a}, b) \in \mathbb{T}^{n+1}$ *with secret key* $\mathbf{s} \in \mathbb{S}^n$ *is defined as*

$$\pi_p(b - \mathbf{s} \cdot \mathbf{a}) \in \mathbb{T}_p$$

where π_p *is a projection on the discrete torus* $\mathbb{T}_p$*.*

Algorithm 2 LWE Decryption

Input: Ciphertext $(\mathbf{a}, b) \in \mathcal{T}^{n+1}$, secret key $\mathbf{s} \in \mathbb{S}^n$, modulus p.

1: $\varphi \leftarrow b - \mathbf{s} \cdot \mathbf{a}$

2: **Return**

$$\frac{\lfloor p\varphi \rceil}{p} \in \mathbb{T}_p.$$

It is clear that if $\mathbf{c} = (\mathbf{a}, b)$ is the LWE-encryption of a message μ in $\mathbb{T}_p$, then

$$\pi_p(b - \mathbf{a} \cdot \mathbf{s}) = \mu$$

if $|e|$ is small enough, more precisely if $|e| < \frac{1}{2p}$. Here, the projection π_p is defined as $\pi_p(\mu) = \frac{\lfloor p\mu \rceil}{p}$ for all $\mu \in \mathbb{T}$.

5.2 Encryption/decryption schemes in $\mathcal{T}$ and $\mathcal{T}^\vee$

The security of Ring Learning With Errors (Ring-LWE) is rooted in the same principles as the standard LWE problem [31]. As mentioned earlier, the dual sets $\mathcal{T}$ and $\mathcal{T}^\vee$ respectively, while abstractly well-defined, can be represented in the following respective forms that are convenient to work with:

$$\mathcal{T} = \left\{ P \bmod \mathbb{Z}[X] \bmod \Phi_M,\ P \in \mathbb{Q}_{N-1}[X] \right\} = \mathcal{K}/\mathcal{R},$$
$$\mathcal{T}^\vee = \left\{ \Omega_0^* P \bmod \Omega_0^* \mathbb{Z}[X] \bmod \Phi_M,\ P \in \mathbb{Q}_{N-1}[X] \right\} = \mathcal{K}/\mathcal{R}^\vee.$$

The Ring-LWE problem (adapted to the torus in this context) as articulated by Regev in [31] is defined as follows:

Ring-LWE problem. For $M > 1$, consider the cyclotomic ring $\mathcal{R}$ and the cyclotomic $\mathbb{Z}[X]$-module $\mathcal{T}^\vee$. Given samples of the form

$$(a^*, b^*) \in \mathcal{T}^\vee \times \mathcal{T}^\vee,$$

with $b^* = s \cdot a^* + e^*$ and where

- a^* is chosen uniformly at random from $\mathcal{T}^\vee$;
- s is a secret element in $\mathcal{R}$ with coefficients in $\mathbb{S}$;
- e^* is a small error term sampled from a normal distribution over $\mathcal{T}^\vee$;

it is a computationally hard problem to distinguish such samples from uniformly random pairs in $\mathcal{T}^\vee \times \mathcal{T}^\vee$.

The security of Ring-LWE is built upon its reduction to hard problems on ideal lattices [31], such as the *Ideal Shortest Vector Problem (Ideal-SVP)* and the *Ideal Closest Vector Problem (Ideal-CVP)*. Once again, the effective level of security depends in particular on how large parameters M and q in $\mathbb{T} \equiv \frac{1}{q}\mathbb{Z}_q$ are.

Now, assume the RLWE-problem is secure. We may encrypt and decrypt polynomial messages as follows:

Definition 5.3 (EncryptRLWE*$_s(\mu^*)$) *The* RLWE**-encryption of a message* $\mu^*(X) \in \mathcal{T}^\vee$ *with the secret key*

$$s(X) = \sum_{i=0}^{N-1} s_i X^i \in \mathcal{R}, \qquad (s_0, \ldots, s_{N-1}) \in \mathbb{S}^N,$$

is defined as

$$c^*(X) = \mathrm{RLWE}_s^*(\mu^*(X)) = (a^*(X), b^*(X)) \in \mathcal{T}^\vee \times \mathcal{T}^\vee$$

with

$$(a_0^*, \ldots, a_{N-1}^*) \xleftarrow{\$} \mathbb{T}^N, \qquad a^*(X) = \sum_{i=0}^{N-1} a_i^* \Omega_i^*(X),$$

$$(e_0^*, \ldots, e_{N-1}^*) \xleftarrow{\mathcal{N}(0,\sigma^2)} \mathbb{T}^N, \qquad e^*(X) = \sum_{i=0}^{N-1} e_i^* \Omega_i^*(X),$$

and

$$b^* = s \cdot a^* + \mu^* + e^* \ \mathit{mod}\ \mathcal{R}^\vee.$$

In other words, the equality holds modulo $\Omega_0^*\mathbb{Z}[X]$ *and* Φ_M*, and* $b^* \in \mathcal{T}^\vee$.

Algorithm 3 RLWE* Encryption of a polynomial message in $\mathcal{T}^\vee$

Input: Message $\mu^*(X) \in \mathcal{T}^\vee$ and secret key $s(X) \in \mathcal{R}$.

1: **Generate:** $(a_0^*, \ldots, a_{N-1}^*) \xleftarrow{\$} \mathbb{T}^N$ and $(e_0^*, \ldots, e_{N-1}^*) \xleftarrow{\mathcal{N}(0,\sigma^2)} \mathbb{T}^N$
2: $a^*(X) \leftarrow \sum_{i=0}^{N-1} a_i^* \Omega_i^*(X)$ and $e^*(X) \leftarrow \sum_{i=0}^{N-1} e_i^* \Omega_i^*(X)$
3: $b^*(X) \leftarrow s(X) \cdot a^*(X) + \mu^*(X) + e^*(X) \bmod \mathcal{R}^\vee$.
4: **Return** $c^*(X) = (a^*(X), b^*(X)) \in \mathcal{T}^\vee \times \mathcal{T}^\vee$.

Definition 5.4 (EncryptRLWE$_s(\mu)$) *The* RLWE*-encryption of a message* $\mu(X) \in \mathcal{T}$ *with the secret key*

$$s(X) = \sum_{i=0}^{N-1} s_i X^i \in \mathcal{R}, \qquad (s_0, \ldots, s_{N-1}) \in \mathbb{S}^N,$$

is defined as

$$c(X) = \mathrm{RLWE}_s(\mu(X)) = (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$$

with $a = (\Omega_0^*)^{-1}a^*$ *mod* Φ_M*,* $b = (\Omega_0^*)^{-1}b^*$ *mod* Φ_M *and where*

$$(a^*(X), b^*(X)) = \mathrm{RLWE}_s^*(\Omega_0^*(X)\mu(X)).$$

Note that

$$b = s \cdot a + \mu + e \bmod \mathcal{R},$$

with $e = (\Omega_0^*)^{-1}e^*$*. The equality holds modulo* $\mathbb{Z}[X]$ *and* Φ_M*, and* $b \in \mathcal{T}$*.*

Algorithm 4 RLWE Encryption of Message μ

Input: Message $\mu(X) \in \mathcal{T}$, secret key $s(X)$.

1: **Compute the RLWE*-encryption:** $(a^*(X), b^*(X)) = \mathrm{RLWE}_s^*(\Omega_0^*(X)\mu(X))$.
2: $a \leftarrow \Big((\Omega_0^*)^{-1}a^* \bmod \Phi_M\Big) \bmod \mathcal{R}$
3: $b \leftarrow \Big((\Omega_0^*)^{-1}b^* \bmod \Phi_M\Big) \bmod \mathcal{R}$
4: **Return** $c(X) = (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$.

Definition 5.5 (DecryptRLWE$_s^*$ ($\mathbf{c}^*(\mathbf{X}), p$)) *The* RLWE**-decryption of the ciphertext* $c^*(X) = (a^*(X), b^*(X)) \in \mathcal{T}^\vee \times \mathcal{T}^\vee$ *with the secret key* $s \in \mathcal{R}$ *is defined as*

$$\pi_p\Big(b^*(X) - s(X)a^*(X)\Big) \in \mathcal{T}_p$$

where π_p *is a projection coefficient by coefficient (in the basis* $(\Omega_i^*(X))_{0\le i<N}$*) on the discrete torus* $\mathbb{T}_p$*.*

Algorithm 5 RLWE* Decryption

Input: Ciphertext $c^*(X) = (a^*(X), b^*(X)) \in \mathcal{T}^\vee \times \mathcal{T}^\vee$, secret key $s \in \mathcal{R}$, modulus p.

1: $\varphi^*(X) \leftarrow b^*(X) - s(X)a^*(X) \bmod \mathcal{R}^\vee$.
2: **Return**

$$\tilde{\varphi}(X) = \sum_{i=0}^{N-1} \frac{\lfloor p\varphi_i^* \rceil}{p}\Omega_i^*(X) \in \mathcal{T}_p^\vee.$$

Definition 5.6 (DecryptRLWE$_s$ ($\mathbf{c}(\mathbf{X}), p$)) *The* RLWE*-decryption of the ciphertext* $c(X) = (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$ *with the secret key* $s \in \mathcal{R}$ *is defined as*

$$\pi_p\Big(b(X) - s(X)a(X)\Big) \in \mathcal{T}_p$$

where π_p *is a projection coefficient by coefficient on the discrete torus* $\mathbb{T}_p$*.*

Algorithm 6 RLWE Decryption

Input: Ciphertext $c(X) = (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$, secret key $s \in \mathcal{R}$, modulus p.

1: $\varphi(X) \leftarrow b(X) - s(X)a(X) = \sum_{i=0}^{N-1} \varphi_i X^i \bmod \mathcal{R}$.
2: **Return**

$$\tilde{\varphi}(X) = \sum_{i=0}^{N-1} \frac{\lfloor p\varphi_i \rceil}{p} X^i \in \mathcal{T}_p.$$

It is clear that if $c(X) = (a(X), b(X))$ is the RLWE-encryption of a message $\mu(X)$ in $\mathcal{T}_p$, then

$$\pi_p\Big(b(X) - s(X)a(X)\Big) = \mu(X)$$

if $\|e\|_\infty$ is small enough, more precisely if $\|e\|_\infty < \frac{1}{2p}$. The norm $\|\cdot\|_\infty$ of a polynomial denotes here, as is customary, the maximum of the absolute values of its coefficients.

5.3 Encryption/decryption schemes in $\mathcal{R}$ and $\mathcal{R}^\vee$

In this subsection, we describe the encryption of elements in the dual sets $\mathcal{R}$ and $\mathcal{R}^\vee$:

$$\mathcal{R} = \Big\{P \bmod \Phi_M,\ P \in \mathbb{Z}_{N-1}[X]\Big\} \subset \mathcal{K} \text{ and } \mathcal{R}^\vee = \Big\{\Omega_0^* P \bmod \Phi_M,\ P \in \mathbb{Z}_{N-1}[X]\Big\} \subset \mathcal{K}.$$

Definition 5.7 (EncryptGRLWE*$_s(\mu^*)$) *Given two intergers $D \geq 2$ and $\ell \geq 1$, the* GRLWE**-encryption of a message*

$$\mu^*(X) = \sum_{i=0}^{N-1} \mu_i^* \Omega_i^*(X) \in \mathcal{R}^\vee$$

with the secret key

$$s(X) = \sum_{i=0}^{N-1} s_i X^i \in \mathcal{R}, \qquad (s_0, \ldots, s_{N-1}) \in \mathbb{S}^N,$$

is defined as

$$C^*(X) = \mathrm{GRLWE}_s^*(\mu^*(X)) = \begin{pmatrix} \mathrm{RLWE}_s^*\left(\frac{\mu^*(X)}{D}\right) \\ \vdots \\ \mathrm{RLWE}_s^*\left(\frac{\mu^*(X)}{D^\ell}\right) \end{pmatrix}.$$

Algorithm 7 GRLWE* Encryption of Message $\mu^* \in \mathcal{R}^\vee$

Input: Message $\mu^*(X) \in \mathcal{R}^\vee$, secret key $s(X)$, integers $D \geq 2$ and $\ell \geq 1$.

Initialize an empty vector: $C^*(X) \leftarrow \emptyset$.
for each k from 1 to ℓ **do**
  $c_k^*(X) \leftarrow \mathrm{RLWE}_s^*\left(\frac{\mu^*(X)}{D^k}\right)$.
  Append $c_k^*(X)$ to $C^*(X)$.
end for
Return

$$C^*(X) = \begin{pmatrix} c_1^* \\ \vdots \\ c_\ell^* \end{pmatrix}.$$

Definition 5.8 (EncryptGRLWE$_s(\mu)$) *Given two intergers $D \geq 2$ and $\ell \geq 1$, the* GRLWE*-encryption of a message*

$$\mu(X) = \sum_{i=0}^{N-1} \mu_i X^i \in \mathcal{R}$$

with the secret key

$$s(X) = \sum_{i=0}^{N-1} s_i X^i \in \mathcal{R}, \qquad (s_0, \ldots, s_{N-1}) \in \mathbb{S}^N,$$

is defined as

$$C(X) = \mathrm{GRLWE}_s(\mu(X)) = \begin{pmatrix} \mathrm{RLWE}_s\left(\frac{\mu(X)}{D}\right) \\ \vdots \\ \mathrm{RLWE}_s\left(\frac{\mu(X)}{D^\ell}\right) \end{pmatrix}.$$

Algorithm 8 GRLWE Encryption of Message $\mu \in \mathcal{R}$

Input: Message $\mu(X) \in \mathcal{R}$, secret key $s(X)$, integers $D \geq 2$ and $\ell \geq 1$.

Initialize an empty vector: $C(X) \leftarrow \emptyset$.
for each k from 1 to ℓ **do**
    $c_k \leftarrow \mathrm{RLWE}_s\left(\frac{\mu(X)}{D^k}\right)$.
    Append c_k to C.
end for
Return

$$C(X) = \begin{pmatrix} c_1 \\ \vdots \\ c_\ell \end{pmatrix}.$$

Definition 5.9 (EncryptRGSW*$_s(\mu^*)$) *Given two intergers $D \geq 2$ and $\ell \geq 1$, the* RGSW**-encryption of a message $\mu^*(X) \in \mathcal{T}^\vee$ with the secret key*

$$s(X) = \sum_{i=0}^{N-1} s_i X^i \in \mathcal{R}, \qquad (s_0, \ldots, s_{N-1}) \in \mathbb{S}^N,$$

is defined as

$$c^*(X) = \mathrm{RGSW}^*_s(\mu^*(X)) = \begin{pmatrix} \mathrm{GRLWE}^*_s(-s(X)\mu^*(X)) \\ \mathrm{GRLWE}^*_s(\mu^*(X)) \end{pmatrix}.$$

Algorithm 9 RGSW* Encryption of Message μ^*

Input: Message $\mu^*(X) \in \mathcal{T}^\vee$, secret key $s(X)$, integers $D \geq 2$ and $\ell \geq 1$.

1: **Compute the RGSW* encryptions:** $C_1^* = \mathrm{GRLWE}_s^*(-s(X)\mu^*(X))$ and $C_2^* = \mathrm{GRLWE}_s^*(\mu^*(X))$.

2: **Return**

$$C^*(X) = \begin{pmatrix} C_1^* \\ C_2^* \end{pmatrix}.$$

Definition 5.10 (EncryptRGSW$_s(\mu)$) *Given two intergers $D \geq 2$ and $\ell \geq 1$, the* RGSW*-encryption of a message $\mu(X) \in \mathcal{T}$ with the secret key*

$$s(X) = \sum_{i=0}^{N-1} s_i X^i \in \mathcal{R}, \qquad (s_0, \ldots, s_{N-1}) \in \mathbb{S}^N,$$

is defined as

$$C(X) = \mathrm{RGSW}_s(\mu(X)) = \left(\begin{array}{c} \mathrm{GRLWE}_s(-s(X)\mu(X)) \\ \mathrm{GRLWE}_s(\mu(X)) \end{array} \right).$$

Algorithm 10 RGSW Encryption of Message μ

Input: Message $\mu(X) \in \mathcal{T}$, secret key $s(X)$, integers $D \geq 2$ and $\ell \geq 1$.

1: $C_1 \leftarrow \mathrm{GRLWE}_s(-s(X)\mu(X))$

2: $C_2 \leftarrow \mathrm{GRLWE}_s(\mu(X))$.

3: **Return**

$$C(X) = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix}.$$

5.4 Homomorphic addition

We denote unambiguously by $\oplus$ the addition of (R)LWE-ciphertexts and RGSW-ciphertexts, as well as (R)LWE*-ciphertexts and RGSW*-ciphertexts,. We recall that, if c_1 and c_2 are two (R)LWE-ciphertexts, i.e.

$$c_1 = \mathrm{(R)LWE}_s(\mu_1) \text{ and } c_2 = \mathrm{(R)LWE}_s(\mu_2),$$

then

$$c_1 \oplus c_2 = \mathrm{(R)LWE}_s(\mu_1 + \mu_2)$$

where the equality means that

$$\mathrm{Decrypt(R)LWE}_s(c_1 \oplus c_2, p) = \mu_1 + \mu_2.$$

Similarly, if C_1 and C_2 are two RGSW-ciphertexts, i.e.

$$C_1 = \mathrm{RGSW}_s(m_1) \text{ and } C_2 = \mathrm{RGSW}_s(m_2)$$

then

$$C_1 \oplus C_2 = \mathrm{RGSW}_s(m_1 + m_2)$$

where the equality means that both sides are (possibly different) encryptions of $m_1 + m_2$. Finally, if C_1^* and C_2^* are two RGSW-ciphertexts, i.e.

$$C_1^* = \mathrm{RGSW}_s^*(m_1^*) \text{ and } C_2^* = \mathrm{RGSW}_s^*(m_2^*)$$

then

$$C_1^* \oplus C_2^* = \mathrm{RGSW}_s^*(m_1^* + m_2^*)$$

In all cases, the effective addition is component-wise (with polynomial coefficients).

5.5 Homomorphic modular product

We recall that the $\mathbb{Z}_{N,q}[X]$-module $\mathbb{T}_{N,q}[X]$ is by definition endowed with a *modular* product $\cdot$ whose counterpart on RGSW-ciphertexts is the co-called *external* product $\boxdot$. Besides, if

$$C^* = \mathrm{RGSW}_s^*(m^*) \in \mathcal{R}^\vee \text{ and } c = \mathrm{RLWE}_s(\mu) \in \mathcal{T},$$

then

$$C^* \boxdot c = \mathrm{RLWE}_s^*(m^* \cdot \mu) \in \mathcal{T}^\vee$$

in the sense that

$$C^* \boxdot c \text{ is an } \mathrm{RLWE}_s\text{-encryption of } m^* \cdot \mu. \tag{5}$$

The effective external product of C^* and c is obtained through the vector-matrix multiplication (with polynomial coefficients)

$$C^* \boxdot c = \mathrm{dec}_{B,\ell}(c)\; C^*$$

where $\mathrm{dec}_{B,\ell}(c) = (\mathrm{dec}_{B,\ell}(a(X)), \mathrm{dec}_{B,\ell}(b(X)))$ and

$$\mathrm{dec}_{B,\ell}(a(X)) = \left(\sum_{r=0}^{N-1} \mathrm{dec}_{B,\ell}(a_r)_1 X^r, \ldots, \sum_{r=0}^{N-1} \mathrm{dec}_{B,\ell}(a_r)_\ell X^r \right)$$

for some integers $B \geq 2$ and $\ell \geq 1$. To complete the definition of $\mathrm{dec}_{B,\ell}(c)$ we decompose any $x \in \mathbb{T} \equiv [-\frac{1}{2}, \frac{1}{2})$ as:

$$x = \sum_{t=1}^{\ell} \mathrm{dec}_{B,\ell}(x)_t B^{-t} + \delta(x), \quad \mathrm{dec}_{B,\ell}(x)_t \in \{-B/2, \ldots, B/2\}, \quad |\delta(x)| \leq \frac{B^{-\ell}}{2}.$$

The dual product $C \boxdot c^*$ is defined similarly.

5.6 Key switching

Key switching is a technique that changes a RLWE-ciphertext (or RLWE*-ciphertext) encrypted under one key to another RLWE-ciphertext (or RLWE*-ciphertext) encrypted under another key, without decrypting the message. This process uses a *key switching key*: the key switching key, written as $\mathrm{KSK}_{s_1 \to s_2}$, is created by encrypting the first key s_1 using the second key s_2. This is a standard method described in many research papers (see, for example, [12, 13, 18]), and for our purposes, we will just assume we have a function called

$$\mathrm{KeySwitch}_{s_1(X) \to s_2(X)}$$

that performs this operation[2].

[2] We don't need to go into the details of how it works internally, as the process is the same regardless of the specific cyclotomic polynomial used in the encryption scheme.

6 Extraction of a LWE from a RLWE

This section describes a procedure aimed at extracting an LWE-encryption $\mathrm{LWE}_{\mathbf{s}}(\mu_i)$ of the i^{th} coefficient $\mu_i \in \mathbb{T}$ from a RLWE-ciphertext $\mathrm{RLWE}_s(\mu)$, where the polynomial message is expressed as

$$\mu(X) = \sum_{i=0}^{N-1} \mu_i \Omega_i(X),$$

where $(\Omega_i(X))_{0\leq i<N} = (X^i)_{0\leq i<N}$ but which could be any basis of $\mathcal{R}$. The connection between s and $\mathbf{s}$ will be elucidated in the subsequent discussion.

The extraction operation can be articulated using the scalar product: from the polynomial message $\mu(X)$, the coefficient μ_i can be obtained as

$$\mu_i = \langle \Omega_i^*(X), \mu(X) \rangle$$

This expression is equal to μ_i by definition of Ω_i^*. Now, considering that

$$\mu(X) = b(X) - s(X) \cdot a(X) - e(X),$$

that is to say that $\mu(X)$ is given in RLWE-encrypted form $c(X) = (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$, we have the following relations:

$$\begin{aligned}
\mu_i = \langle \Omega_i^*(X), \mu(X) \rangle &= \langle \Omega_i^*(X), b(X) \rangle - \langle \Omega_i^*(X), s(X) \cdot a(X) \rangle - \langle \Omega_i^*(X), e(X) \rangle \\
&= \langle \Omega_i^*(X), b(X) \rangle - \sum_{j=0}^{N-1} s_j \langle \Omega_i^*(X), B_j(X) \cdot a(X) \rangle - \langle \Omega_i^*(X), e(X) \rangle \\
&:= b^{(i)} - \mathbf{s} \cdot \mathbf{a}^{(i)} - e^{(i)}
\end{aligned}$$

where we have assumed that $s(X)$ is written in the basis $(B_j)_{0\leq j<N}$ as

$$s(X) = \sum_{j=0}^{N-1} s_j B_j(X) \quad \text{and} \quad \mathbf{s}_j = s_{j-1} \quad \text{for} \quad j = 1, \ldots, N. \tag{6}$$

The values $b^{(i)}$, $\mathbf{a}^{(i)}$ and $e^{(i)}$ are thus defined as

$$b^{(i)} = \langle \Omega_i^*(X), b(X) \rangle, \quad \mathbf{a}_j^{(i)} = \langle \Omega_i^*(X), B_{j-1}(X) \cdot a(X) \rangle \quad \text{for} \quad j = 1, \ldots, N,$$

and $e^{(i)} = \langle \Omega_i^*(X), e(X) \rangle$. Thus, we obtain an LWE-encryption of μ_i as

$$\mathrm{LWE}_{\mathbf{s}}(\mu_i) = (\mathbf{a}^{(i)}, b^{(i)}).$$

In order to get explicit expressions, we can assume for instance, that $B_i(X) = \Omega_i(X) = X^i$ and that $a(X) = \sum_{j=0}^{N-1} a_j \Omega_j(X)$, $b(X) = \sum_{j=0}^{N-1} b_j \Omega_j(X)$. Using the expression of $s(X) \cdot a(X) \bmod \Phi_M$ furnished in Lemma 8.7, we then obtain

$$\mathbf{a}_j^{(i)} = a_{i-j+1} - a_{N-j+1+[i]_{\frac{M}{t}}} \quad \text{for} \quad j = 1, \ldots, N,$$

and a LWE-encryption of μ_i as

$$\mathrm{LWE}_{\mathbf{s}}(\mu_i) = (\mathbf{a}^{(i)}, b_i).$$

The dual version of this procedure can be derived in a similar fashion: given an RLWE*-encryption $(a^*(X), b^*(X))$ of the polynomial message

$$\mu^*(X) = \sum_{j=0}^{N-1} \mu_j^* \Omega_j^*(X),$$

the coefficient μ_i^* can be obtained as

$$\begin{aligned}\mu_i^* &= \langle \Omega^i(X), \mu^*(X) \rangle \\ &= \langle \Omega^i(X), b^*(X) \rangle - \sum_{j=0}^{N-1} s_j \langle \Omega_i(X), B_j(X) \cdot a^*(X) \rangle - \langle \Omega_i(X), e^*(X) \rangle \\ &:= b^{(i)} - \mathbf{s} \cdot \mathbf{a}^{(i)} - e^{(i)}\end{aligned}$$

where we have assumed relations (6). The values $b^{(i)}$, $\mathbf{a}^{(i)}$ and $e^{(i)}$ are thus defined as

$$b^{(i)} = \langle \Omega_i(X), b^*(X) \rangle, \quad \mathbf{a}_j^{(i)} = \langle \Omega_i(X), B_{j-1}(X) \cdot a^*(X) \rangle \quad \text{for} \quad j = 1, \ldots, N,$$

and $e^{(i)} = \langle \Omega_i(X), e^*(X) \rangle$. Thus, we obtain an LWE-encryption of μ_i as

$$\mathrm{LWE}_{\mathbf{s}}(\mu_i) = (\mathbf{a}^{(i)}, b^{(i)}).$$

Again, explicit expressions can be obtained by assuming for instance, that $B_i(X) = \Omega_i(X) = X^i$ and that $a^*(X) = \sum_{j=0}^{N-1} a_j^* \Omega_j^*(X)$, $b^*(X) = \sum_{j=0}^{N-1} b_j^* \Omega_j^*(X)$. In that case

$$\mathbf{a}_j^{(i)} = \langle X^{i-j+1}, a^*(X) \rangle$$

and using the expression of $X^{i-j+1} \bmod \Phi_M$ furnished in Lemma 8.7, we finally obtain

$$\mathbf{a}_j^{(i)} = a_{i-j+1}^* - a_{N-j+1+[i]_{\frac{M}{t}}}^* \quad \text{for} \quad j = 1, \ldots, N,$$

and a LWE-encryption of μ_i^* as

$$\mathrm{LWE}_{\mathbf{s}}(\mu_i^*) = (\mathbf{a}^{(i)}, b_i^*).$$

Proposition 6.1 *Given an encryption $(a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$ of*

$$\mu(X) = \sum_{j=0}^{N-1} \mu_j \Omega_j(X)$$

with key $s(X) = \sum_{j=0}^{N-1} s_j B_j(X)$ and an integer index $i \in \{0, \ldots, N-1\}$, a LWE-encryption with key $\mathbf{s} = (s_0, \ldots, s_{N-1})$ of μ_i is obtained as

$$\mathrm{LWE}_{\mathbf{s}}(\mu_i) = (\mathbf{a}^{(i)}, b^{(i)}),$$

where

$$b^{(i)} = \langle \Omega_i^*(X), b(X) \rangle, \quad \mathbf{a}_j^{(i)} = \langle \Omega_i^*(X), B_{j-1}(X) \cdot a(X) \rangle \quad \textit{for} \quad j = 1, \ldots, N.$$

If we furthermore assume that $\Omega_i(X) = B_i(X) = X^i$ *for* $0 \le i < N$ *and that*

$$a(X) = \sum_{j=0}^{N-1} a_j X^j \quad \textit{and} \quad b(X) = \sum_{j=0}^{N-1} b_j X^j,$$

then

$$b^{(i)} = b_i \quad \textit{and} \quad \mathbf{a}_j^{(i)} = a_{i-j+1} - a_{N-j+1+[i]_{\frac{M}{t}}} \quad \textit{for} \quad j = 1, \ldots, N.$$

Similarly, given an encryption $(a^*(X), b^*(X)) \in \mathcal{T}^\vee \times \mathcal{T}^\vee$ *of*

$$\mu^*(X) = \sum_{i=0}^{N-1} \mu_i^* \Omega_i^*(X)$$

with key $s(X) = \sum_{j=0}^{N-1} s_j B_j(X)$ *and an integer index* $i \in \{0, \ldots, N-1\}$*, a* LWE-*encryption with key* $\mathbf{s} = (s_0, \ldots, s_{N-1})$ *of* μ_i^* *is obtained as*

$$LWE_{\mathbf{s}}(\mu_i^*) = (\mathbf{a}^{(i)}, b^{(i)}),$$

where

$$b^{(i)} = \langle \Omega_i(X), b^*(X) \rangle \quad \textit{and} \quad \mathbf{a}_j^{(i)} = \langle \Omega_i(X), B_{j-1}(X) \cdot a^*(X) \rangle \quad \textit{for} \quad j = 1, \ldots, N.$$

If we furthermore assume that $\Omega_i(X) = B_i(X) = X^i$ *for* $0 \le i < N$ *and that*

$$a^*(X) = \sum_{j=0}^{N-1} a_j^* \Omega_j^*(X) \quad \textit{and} \quad b^*(X) = \sum_{j=0}^{N-1} b_j^* \Omega_j^*(X),$$

then

$$b^{(i)} = b_i^* \quad \textit{and} \quad \mathbf{a}_j^{(i)} = a_{i-j+1}^* - a_{N-j+1+[i]_{\frac{M}{t}}}^* \quad \textit{for} \quad j = 1, \ldots, N.$$

Remark 6.2 *Alternatively, we could have expressed*

$$\begin{aligned} \mu_i = \langle \Omega_i^*(X), \mu \rangle &= \langle \Omega_i^*(X), b(X) \rangle - \langle \Omega_i^*(X), s(X) \cdot a(X) \rangle - \langle \Omega_i^*(X), e(X) \rangle \\ &= b_i - \mathbf{s} \cdot \mathbf{a} - e_i \end{aligned}$$

by assuming

$$a(X) = \sum_{j=0}^{N-1} a_j \Omega_j(X) \quad \textit{and} \quad b(X) = \sum_{j=0}^{N-1} b_j \Omega_j(X),$$

and writing

$$\langle \Omega_i^*(X), s(X) \cdot a(X) \rangle = \sum_{j=0}^{N-1} a_j \langle \Omega_i^*(X), \Omega_j(X) s(X) \rangle,$$

so that

$$\mathbf{a}_j = a_{j-1} \quad \textit{and} \quad \mathbf{s}_j = \langle \Omega_i^*(X), \Omega_{j-1}(X) s(X) \rangle \quad \textit{for} \quad j = 1, \ldots, N.$$

This corresponding encryption is characterized by the use of a secret key with components drawn from a larger set than the original set $\mathbb{S}$*, which could be a disadvantage in certain implementations.*

Algorithm 11 LWE extraction of μ_i from $\mu(X) = \sum_{j=0}^{N-1} \mu_j \Omega_j(X) \in \mathcal{T}$

Input: $(a(X), b(X)) = \mathrm{RLWE}_s(\mu(X)) \in \mathcal{T} \times \mathcal{T}$, index $i \in \{0, \ldots, N-1\}$.

for each j from 1 to N **do**
  $\mathbf{a}_j \leftarrow a_{i-j+1} - a_{N-j+1+[i]_{\frac{M}{t}}}$
  $\mathbf{s}_j \leftarrow s_{j-1}$
end for
$b_i \leftarrow (b(X))_i$
Return: $\mathrm{LWE}_{\mathbf{s}}(\mu_i) = (\mathbf{a}, b_i)$

Note: $a(X)$, $b(X)$, $s(X)$ are expressed in $(\Omega_j)_{0 \leq j < N}$

Algorithm 12 LWE extraction of μ_i^* from $\mu^*(X) = \sum_{j=0}^{N-1} \mu_j^* \Omega_j^*(X) \in \mathcal{T}^\vee$

Input: $(a^*(X), b^*(X)) = \mathrm{RLWE}_s^*(\mu^*(X)) \in \mathcal{T}^\vee \times \mathcal{T}^\vee$, index $i \in \{0, \ldots, N-1\}$.

for each j from 1 to N **do**
  $\mathbf{a}_j \leftarrow \langle X^{i+M-j+1}, a^*(X) \rangle$
  $\mathbf{s}_j \leftarrow s_{j-1}$
end for
$b_i^* \leftarrow (b^*(X))_i$
Return: $\mathrm{LWE}_{\mathbf{s}}(\mu_i) = (\mathbf{a}, b_i^*)$

Note: $a^*(X)$, $b^*(X)$ expressed in $(\Omega_j^*)_{0 \leq j < N}$ and $s(X)$ in $(\Omega_j)_{0 \leq j < N}$

7 Bootstrapping in the prime power cyclotomic setting

The primary objective of bootstrapping in fully homomorphic encryption (FHE) is to reduce the noise that builds up in ciphertext during operations, as excessive noise can impede decryption. The key objectives of bootstrapping can be summarized as follows:

(i) **Noise Reduction**: Enables an unlimited number of homomorphic operations by refreshing the ciphertext and lowering the noise level;

(ii) **Function Mapping**: Facilitates the application of a function during the bootstrapping process;

(iii) **Security Maintenance**: Ensures that the original data remains secure throughout the operation.

In the context of TFHE, this goal can be articulated as follows:

Goal of bootstrapping: Given a LWE-encryption c of $\mu \in \mathbb{T}_p$ with error e and a function f that maps $\mathbb{T}_p$ to $\mathbb{T}$, produce a LWE-encryption of $f(\mu)$ with a fresh error of smaller size than e.

In summary, bootstrapping is crucial for the practical implementation of encrypted computations in HE. A significant contribution of the authors of TFHE was the improvement of the efficiency of their variant of FHEW bootstrapping, highlighting the need to preserve this efficiency in the context of prime power cyclotomic polynomials. Therefore, it becomes essential to reformulate the mathematical representation of bootstrapping in a manner that aligns with our context. The following function serves as the foundation for our formulation of the bootstrapping process:

Definition 7.1 *Given a polynomial $v^*(X) \in \mathcal{T}^\vee$, the bootstrap function Θ_{v^*} is defined as*

$$\begin{array}{rccl} \Theta_{v^*}: & \mathbb{T} & \to & \mathbb{T} \\ & \mu & \mapsto & \mathrm{Tr}\Big(X^{-\lfloor M\mu \rceil} v^*(X)\Big) = \langle X^{\lfloor M\mu \rceil}, v^*(X) \rangle \end{array}$$

It is important to highlight that this definition and its implementation retain the concepts of the bootstrapping procedure proposed by Ducas and Micciancio [18], with the distinction lying solely in its formulation. It is evident that Θ_{v^*} is fully characterized by the values

$$\Theta_{v^*}\Big(\frac{i}{M}\Big), \quad 0 \leq i \leq M-1,$$

along with the observation that

$$\forall \mu \in \mathbb{T}, \quad \Theta_{v^*}(\mu) = \Theta_{v^*}\Big(\lfloor M\mu \rceil\Big).$$

A homomorphic and efficient implementation of this function, essential for the correctness of the bootstrapping procedure, must satisfy the following:

Requirement: For all $\mu \in \mathbb{T}_p$ and for all error $e \in \mathbb{T}$ such that $|e| \leq \frac{1}{2p}$

$$\Theta_{v^*}\Big(\mu + e\Big) = f(\mu). \tag{7}$$

Note that condition (7) implies that

$$\forall \mu \in \mathbb{T}, \quad \Theta_{v^*}\Big(\mu\Big) = f\Big(\frac{\lfloor p\mu \rceil}{p}\Big).$$

In this section, we aim to establish clear and concise compatibility conditions on f that guarantee the existence of v^* and explicitly determine its form.

7.1 General formulation of the compatibility conditions

Let the function F be defined on the interval $0 \leq i \leq M-1$ by

$$F(i) = \Theta_{v^*}\Big(\frac{i}{M}\Big) = \mathrm{Tr}(X^{-i} v^*(X)), \quad 0 \leq i \leq M-1,$$

that is to say

$$F(i) = \Theta_{v^*}\Big(\frac{i}{M}\Big) = \langle X^i, v^*(X) \rangle, \quad 0 \leq i \leq M-1.$$

The coefficients of the polynomial

$$v^*(X) = \sum_{i=0}^{N-1} v_i^* \Omega_i^*(X) \in \mathcal{T}^\vee$$

are completely and uniquely determined by the relations

$$F(i) = \Theta_{v^*}\left(\frac{i}{M}\right) = \langle X^i, v^*(X)\rangle, \quad 0 \le i \le N-1,$$

which leads to

$$v_i^* = F(i), \quad 0 \le i \le N-1.$$

However, the values of $F(i)$ for $N \le i \le M-1$ are then constrained by

$$F(i) = \langle X^i, v^*(X)\rangle, \quad N \le i \le M-1.$$

For $N \le i < M$, we can express X^i as

$$X^i = \sum_{j=0}^{N-1} \beta_{ij} X^j.$$

Under this condition, we find that

$$\forall N \le i \le M-1, \quad F(i) = \sum_{j,k=0}^{N-1} \beta_{ij} v_k^* \langle X^j, \Omega_k^*\rangle = \sum_{j=0}^{N-1} \beta_{ij} F(j)$$

This results in $M-N$ compatibility conditions that may be equivalently expressed in terms of f as

$$\forall N \le i \le M-1, \quad f\left(\frac{\lfloor p\frac{i}{M}\rceil}{p}\right) = \sum_{j=0}^{N-1} \beta_{ij} \quad f\left(\frac{\lfloor p\frac{j}{M}\rceil}{p}\right).$$

7.2 Explicit formulation

It is easy to check from Lemma 8.6 that

$$\forall N \le i \le M-1, \quad X^i = -\sum_{\substack{0 \le j \le N-1, \\ [j]_{M/t} = i-N}} X^j,$$

so that

$$\beta_{ij} = -\delta_{i,N+[j]_{M/t}}$$

where, as is standard, $\delta_{i,j} = 1$ if $i = J$ and 0 otherwise. The compatibility relations thus write

$$N \le i \le M-1, \quad F(i) + \sum_{\substack{0 \le j \le N-1, \\ [j]_{M/t} = i-N}} F(j) = 0$$

or equivalently

$$\forall 0 \le r \le \frac{M}{t} - 1, \quad \sum_{k=0}^{t-1} F\left(kt^{\alpha-1} + r\right) = 0.$$

In summary, we can state the following:

Proposition 7.2 *There exists a polynomial $v^* \in \mathcal{T}^\vee$ such that*

$$\forall \mu \in \mathbb{T}_p, \quad \Theta_{v^*}\Big(\mu + e\Big) = f(\mu)$$

for all errors $e \in \mathbb{T}$ with $|e| \leq \frac{1}{2p}$ if and only if the function f satisfies the compatibility conditions

$$\forall 0 \leq r \leq \frac{M}{t} - 1, \quad \sum_{k=0}^{t-1} f\left(\frac{\lfloor (kt^{\alpha-1} + r)\frac{p}{M} \rceil}{p}\right) = 0. \tag{8}$$

The polynomial v^* are then determined by the relation

$$v^*(X) = \sum_{i=0}^{N-1} f\Big(\frac{\lfloor p\frac{i}{M} \rceil}{p}\Big)\Omega_i^*(X).$$

Remark 7.3 *In the specific case where $p = t$, the compatibility relations simplify to a single equation:*

$$\sum_{k=0}^{t-1} f\left(\frac{k}{t}\right) = 0.$$

This can be understood by noting that for any integer $\ell \in \mathbb{Z}$, it holds that

$$\sum_{k=0}^{t-1} f\left(\frac{k}{t} + \frac{\ell}{t}\right) = \sum_{k=0}^{t-1} f\left(\frac{k}{t}\right).$$

It is important to note that this condition can be easily eliminated by adding a constant to f prior to bootstrapping and subsequently removing it from the result.

7.3 Homomorphic implementation

We now convert Definition 7.1 into a practical algorithm that operates on the ciphertext $(\mathbf{a}, b)$, which encrypts $\mu \in \mathbb{T}_p$ with a secret key $\mathbf{s}$:

$$\mu = b - \mathbf{s} \cdot \mathbf{a} - e.$$

The first step, while not critical to the definition of bootstrapping, is essential for enhancing its efficiency. This step involves re-encrypting the ciphertext with a smaller key $\hat{\mathbf{s}} \in \mathbb{S}^{\hat{n}}$, such that

$$\mu = \hat{b} - \hat{\mathbf{s}} \cdot \hat{\mathbf{a}} - \hat{e}.$$

Bootstrapping fundamentally entails the homomorphic computation of an LWE-encryption of $\Theta_{v^*}(\mu)$ from an LWE-encryption of μ. Since rounding to an integer is not inherently a homomorphic operation, it is necessary to first approximate

$$\lfloor M\mu \rceil = \lfloor M(\hat{b} - \hat{\mathbf{s}} \cdot \hat{\mathbf{a}} - \hat{e}) \rceil$$

To achieve this, we employ the *collapsing* strategy from [7]. For the sake of simplicity, we suppose here that m divides $\hat{n}$. We denote, on the one hand,

$$\tilde{\mathbf{s}}_k = \big(\hat{s}_{m(k-1)+1}, \hat{s}_{m(k-1)+2}, \ldots, \hat{s}_{mk}\big) \in \mathbb{S}^m, \quad k = 1, \ldots, \hat{n}/m, \tag{9}$$

and on the other hand

$$\tilde{\mathbf{a}}_k = \left(\hat{a}_{m(k-1)+1}, \hat{a}_{m(k-1)+2}, \ldots, \hat{a}_{mk}\right) \in \mathbb{T}_q^m, \quad k = 1, \ldots, \hat{n}/m, \tag{10}$$

so that

$$\mu + e = \hat{b} - \hat{\mathbf{s}} \cdot \hat{\mathbf{a}} = \hat{b} - \sum_{k=1}^{\hat{n}/m} \tilde{\mathbf{s}}_k \cdot \tilde{\mathbf{a}}_k.$$

As explained in [7], we then round partial sums $\tilde{\mathbf{s}}_k \cdot \tilde{\mathbf{a}}_k$ and not individual products $s_k a_k$ as it is customary [12, 13, 18]. This leads to the approximation

$$\lfloor M(\mu + e) \rceil \approx -\sum_{k=1}^{\hat{n}/m} \sum_{\tilde{\mathbf{j}} \in \mathbb{S}^m} \delta_{\tilde{\mathbf{j}}, \tilde{s}_k} \bar{a}_{k, \tilde{\mathbf{j}}} = -\sum_{k=1}^{\hat{n}/m} \bar{a}_{k, \tilde{\mathbf{s}}_k} =: \imath, \tag{11}$$

where we denote $\delta_{\tilde{\mathbf{i}}, \tilde{\mathbf{j}}}$, for $(\tilde{\mathbf{i}}, \tilde{\mathbf{j}}) \in \mathbb{S}^m \times \mathbb{S}^m$, the symbol with value 1 if $\tilde{\mathbf{i}} = \tilde{\mathbf{j}}$ and 0 otherwise, and where

$$\bar{a}_{1,\tilde{\jmath}} = \lfloor M \tilde{\mathbf{a}}_1 \cdot \tilde{\mathbf{j}} - Mb \rceil, \qquad \bar{a}_{k, \tilde{\mathbf{j}}} = \lfloor M \tilde{\mathbf{a}}_k \cdot \tilde{\mathbf{j}} \rceil \;\text{ for }\; k = 2, \ldots, \hat{n}/m \;\text{ and }\; \tilde{\mathbf{j}} \in \mathbb{S}^m. \tag{12}$$

Note that the sum in (11) is valid for all m dividing $\hat{n}$, in particular for $m = 1$, where we recover the usual expression, as seen in [12], for example, or for $m = \hat{n}$, where the two sides (of the approx sign) in equation (11) become equal. We finally observe that

$$X^{-\imath} \;=\; \prod_{k=1}^{\hat{n}/m} X^{\bar{a}_{k, \tilde{\mathbf{s}}_k}} = \prod_{k=1}^{\hat{n}/m} \sum_{\tilde{\mathbf{j}} \in \mathbb{S}^m} \delta_{\tilde{\mathbf{j}}, \tilde{\mathbf{s}}_k} X^{\bar{a}_{k,\tilde{\jmath}}} = \prod_{k=1}^{\hat{n}/m} H_k(X) \tag{13}$$

with

$$H_k(X) = \sum_{\tilde{\mathbf{j}} \in \mathbb{S}^m} \delta_{\tilde{\mathbf{j}}, \tilde{\mathbf{s}}_k} X^{\bar{a}_{k,\tilde{\jmath}}} \in \mathcal{R}, \quad k = 1, \ldots, \hat{n}/m, \tag{14}$$

so that $X^{-\imath} \cdot v^*(X)$ can be computed as the result of $\hat{n}/m$ successive modular products $\mathcal{R} \times \mathcal{T}^\vee$ applied from the right to the left

$$X^{-\imath} \cdot v^*(X) = H_{n/m}(X) \ldots (H_2(X) \cdot (H_1(X) \cdot v^*(X))) \ldots) \tag{15}$$

The full bootstrapping procedure involves three steps:

1. **Keyswitch Operation:** Given $\mathbf{c} = (\mathbf{a}, b)$ a $\mathrm{LWE}_{\mathbf{s}}$-encryption of a message $\mu \in \mathbb{T}_p$, compute $\hat{\mathbf{c}} = (\hat{\mathbf{a}}, \hat{b})$ a $\mathrm{LWE}_{\hat{\mathbf{s}}}$-encryption for a reduced size key $\hat{\mathbf{s}}$;

2. **Blind Rotate Operation:** Given RGSW_s-encryptions of the $\delta_{\tilde{\mathbf{j}}, \tilde{\mathbf{s}}_k}$, computes a RLWE_s-encryption of $X^{-\imath} \cdot v^*(X)$;

3. **Extract Operation:** Compute an $\mathrm{LWE}_{\mathbf{s}}$-encryption of the constant term of $X^{-\imath} \cdot v^*(X)$, which is the final output of the bootstrap[3].

The first step is entirely standard and resembles for instance what is done in the context of powers-of-two cyclotomic polynomials; therefore, we will omit its description. Below, we will outline the two other essential steps in detail.

[3]The final LWE-key is fully specified by the polynomial key $s(X) = \sum_{j=0}^{N-1} s_j X^j \in \mathcal{R}$, and the extraction procedure we adopt guarantees that $\mathbf{s} = (s_0, s_1, \ldots, s_{N-1})$.

7.3.1 Blind rotation

Given RGSW_s-encryptions of the $\delta_{\tilde{\mathbf{j}},\tilde{\mathbf{s}}_k}$, it is straightforward to compute the homomorphic RGSW_s-encryptions of $H_k(X)$ for $k = 1, \ldots, \hat{n}/m$,as outlined in Formula (14). Specifically, we have:

$$\mathrm{RGSW}_s(H_k) = \bigoplus_{\tilde{\mathbf{j}} \in \mathbb{S}^m} \Big(X^{\bar{a}_{k,\tilde{\mathbf{j}}}} \cdot \mathrm{RGSW}_s(\delta_{\tilde{\mathbf{j}},\tilde{\mathbf{s}}_k}) \Big), \tag{16}$$

where the $\cdot$ denotes the product of the polynomial $X^{\bar{a}_{k,\tilde{\mathbf{j}}}} \in \mathcal{R}$ by each of the polynomial components of $\mathrm{RGSW}_s(\delta_{\tilde{\mathbf{j}},\tilde{\mathbf{s}}_k})$, all of which reside in $\mathcal{T}^\vee$. The RLWE^*_s-encrypted value $X^{-\imath} \cdot v^*(X)$ can now be computed homomorphically according to Formula (15) as follows:

$$\mathrm{RGSW}_s(H_{n/m}) \boxdot (\ldots(\mathrm{RGSW}_s(H_1) \boxdot \mathrm{RLWE}^*_s(v^*))\ldots). \tag{17}$$

Note that $\mathrm{RLWE}^*_s(v^*)$ is defined here as the trivial noise-free zero-mask $(0, \ldots, 0, v^*(X))$. Additionally, we assume that v^* aligns with its definition in Proposition 7.2 for the specified target function f.

Algorithm 13 Blind Rotation Algorithm

Input: $\mathbf{c} = (\mathbf{a}, b) \in \mathbb{T}^{\hat{n}+1}$ and $\mathrm{RGSW}_s(\delta_{\tilde{\mathbf{j}},\tilde{\mathbf{s}}_k})$ for $\tilde{\mathbf{j}} \in \mathbb{S}^m$, $k = 1, \ldots, \hat{n}/m$.
for $\tilde{\mathbf{j}} \in \mathbb{S}^m$ **do**
    Compute: $\bar{a}_{1,\tilde{\jmath}} = \lfloor M\tilde{\mathbf{a}}_1 \cdot \tilde{\mathbf{j}} - Mb \rceil$
    for $k = 2$ to $\hat{n}/m$ **do**
        Compute: $\bar{a}_{k,\tilde{\mathbf{j}}} = \lfloor M\tilde{\mathbf{a}}_k \cdot \tilde{\mathbf{j}} \rceil$.
    end for
end for
for $k = 1$ to $\hat{n}/m$ **do**
    Initialize: $\mathrm{RGSW}_s(H_k) = \mathrm{RGSW}_s(0)$
    for $\tilde{\mathbf{j}} \in \mathbb{S}^m$ **do**
        Compute: $\mathrm{RGSW}_s(H_k) = \mathrm{RGSW}_s(H_k) \bigoplus \Big(X^{\bar{a}_{k,\tilde{\mathbf{j}}}} \cdot \mathrm{RGSW}_s(\delta_{\tilde{\mathbf{j}},\tilde{\mathbf{s}}_k}) \Big)$
    end for
end for
Initialize: $\mathrm{ACC}^* = (0, v^*(X))$.
for $k = 1$ to $\hat{n}/m$ **do**
    Compute: $\mathrm{ACC}^* = \mathrm{RGSW}_s(H_k) \boxdot \mathrm{ACC}^*$
end for
Output: $\mathrm{ACC}^* = \mathrm{RLWE}^*_s(X^{-\imath} v^*(X))$ with $\imath = -\sum_{k=1}^{\hat{n}/m} \bar{a}_{k,\tilde{\mathbf{s}}_k}$.

7.3.2 Extraction of the trace

The final step of the bootstrapping procedure mirrors the second scenario outlined in Paragraph 6, where we have $\mu^* = v^*$ and $i = \imath$. Utilizing the output from the Blind Rotate algorithm, our objective is to derive an LWE encryption of the trace of $X^{-\imath}v^*(X)$ from its RLWE^*_s encryption with $s(X) = \sum_{j=0}^{N-1} s_j \Omega_j(X)$, denoted as $\mathrm{ACC}^*(X) = (a^*(X), b^*(X))$. Without further elaboration, we can summarize this as follows:

$$\mathrm{LWE}_{\mathbf{s}}(\mathrm{Tr}(X^{-\imath}v^*(X))) = (\mathbf{a}^*, b^*_0)$$

with $b_0^* = \mathrm{Tr}(b^*(X))$ and

$$\mathbf{a}_j^* = \langle X^{M-j+1}, a^*(X)\rangle \quad \text{and} \quad \mathbf{s}_j = s_{j-1} \quad \text{for} \quad j = 1, \ldots, N.$$

Algorithm 14 Extraction of an Encryption of the Trace

Input: $\mathrm{ACC}^*(X) = (a^*(X), b^*(X)) = \mathrm{RLWE}_s(X^{-\imath}v^*(X))$ with $s(X) = \sum_{j=0}^{N-1} s_j\Omega_j(X)$.

for $j = 1$ **to** N **do**
  $\mathbf{a}_j^* \leftarrow \langle X^{M-j+1}, a^*(X)\rangle$
  $\mathbf{s}_j \leftarrow s_{j-1}$
end for
Output: $\mathrm{LWE}_{\mathbf{s}}(X^{-\imath}v^*(X)) = (\mathbf{a}^*, b_0^*)$ with $\mathbf{s} = (s_0, \ldots, s_{N-1})$

8 Trace operators and their homomorphic evaluations

The trace operator is a crucial concept in the study of algebraic fields and structures. It fundamentally allows for the mapping of elements from a field extension back to the base field. Moreover, the trace operator is utilized to analyze and manipulate algebraic structures effectively, enhancing the security and functionality of TFHE/FHEW systems. In this section, we will demonstrate how it can be computed efficiently and highlight its significance for fast packing algorithms.

8.1 The complete trace and its encryption

We recall that if $\mathcal{K}$ is a Galois extension of a number field $\mathcal{K}_0$, then the associated Galois group $\mathrm{Gal}(\mathcal{K}/\mathcal{K}_0)$ is defined as the collection of all automorphisms of $\mathcal{K}$ that leave the subfield $\mathcal{K}_0$ unchanged. In our context, the field $\mathcal{K} = \mathbb{Q}[X]/\Phi_M(X)$ serves as a Galois extension of the field $\mathcal{K}_0 = \mathbb{Q}$. It is well-known that the Galois group in this scenario comprises the automorphisms τ_d defined by

$$\tau_d(P)(X) = P(X^d) \quad \text{for all} \quad P \in \mathcal{K},$$

where d is any integer that is co-prime to M. Notably, this group is isomorphic to $\mathbb{Z}_M^\times$ and its cardinality is precisely $N = \varphi(M)$, which also represents the degree of the extension. In what follows, we will explicitly denote the extension and base fields in the notation of the trace (refer to Definition 3.4) as follows:

$$\mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0}(P)(X) = \sum_{\substack{1 \le d \le M \\ \gcd(d, M) = 1}} P(X^d), \quad \text{for all } P \in \mathcal{K}.$$

We have the following useful identities, from which the expression of the dual basis $(\Omega_i^*)_{0 \le i < N}$ can be derived (see Formula (3)). Their proof is straightforward and therefore omitted:

Proposition 8.1 *When $M = t^\alpha$ with $\alpha \ge 1$ and t being a prime, we have the following identity in $\mathcal{K}$: For all $n, k \in \mathbb{Z}$,*

$$\mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0}(X^n) = 0 \;\; \textit{if } [n]_{M/t} \neq 0 \textit{ and } \mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0}\left(X^{kM/t}\right) = M\delta_{[k]_t, 0} - \frac{M}{t}.$$

As a result, we obtain the following:

- *For any polynomial* $\mu(X) = \sum_{n=0}^{N-1} \mu_n X^n \in \mathcal{K}$

$$\mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0}\left(\mu(X)\right) = \sum_{k=0}^{t-2} \left(M\delta_{[k]_t,0} - \frac{M}{t} \right) \mu_{kM/t} = N\mu_0 - \frac{M}{t} \sum_{k=1}^{t-2} \mu_{kM/t}.$$

- *For any index* $i \in \mathbb{Z}$ *and any polynomial* $\mu(X) = \sum_{n=0}^{N-1} \mu_n X^n \in \mathcal{K}$*, we have*

$$\mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0}\left(\bar{\Omega}_i^*(X)\mu(X)\right) = \mu_i,$$

where the definition of the coefficients μ_i *is extended to indices* i *in* $\mathbb{Z}$ *as above.*

Now, to derive an RLWE-encryption of the quantity $\mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0}(\mu(X))$ from a RLWE-encryption of $\mu(X) \in \mathcal{T}$, a well-established and intuitive strategy can be employed. Start with an encryption $c(X) = (a(X), b(X) \in \mathcal{T} \times \mathcal{T}$ of $\mu(X)$ using the key $s(X) \in \mathcal{R}$:

$$b(X) = s(X) \cdot a(X) + \mu(X) + e(X) \bmod \mathcal{R}.$$

For any integer d that is co-prime to M, we can rewrite the expression as follows:

$$b(X^d) = s(X^d) \cdot a(X^d) + \mu(X^d) + e(X^d) \bmod \mathcal{R}.$$

Since $\Phi_M(X^d)$ is a multiple of $\Phi_M(X)$ for all integers d co-prime to M (see Proposition), it follows that $(a(X^d), b(X^d))$ constitutes an encryption of $\mu(X^d)$ with the secret key $s(X^d)$. Next, a simple key switching from $s(X^d)$ to $s(X)$ transforms this encryption into one of $\mu(X^d)$ under the key $s(X)$, which is now independent of d. Finally, by summing these encryptions over all integers d that are less than M and co-prime to M, we obtain an encryption of $\mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0}(\mu(X))$ with the key $s(X)$.

Algorithm 15 RLWE Encryption of the Trace of $\mu(X) \in \mathcal{T}$

Input: RLWE encryption $c(X) = (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$ of $\mu(X)$ with key $s(X) \in \mathcal{R}$
Initialize: $(a_\Sigma(X), b_\Sigma(X)) = (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$
for $d = 2$ **to** $M - 1$ such that $\gcd(d, M) = 1$ **do**
  Compute: $(a(X^d), b(X^d)) \bmod \mathcal{R}$
  Perform key switching:

$$(a_d(X), b_d(X)) = \mathrm{KeySwitch}_{s(X^d) \to s(X)}\left((a(X^d), b(X^d)) \right)$$

  $(a_\Sigma(X), b_\Sigma(X)) \leftarrow (a_\Sigma(X), b_\Sigma(X)) + (a_d(X), b_d(X))$
end for
Output: $(a_\Sigma(X), b_\Sigma(X)) = \mathrm{RLWE}_{s(X)}(\mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0}(\mu(X)))$ with key $s(X)$

Despite its straightforward nature, we note that the algorithm necessitates

$$\varphi(M) = N = (t-1)t^{\alpha-1}$$

key-switches to obtain homomorphic encryptions of all quantities $P(X^d)$ from the encryption of $P(X)$. To mitigate this cost, we will utilize a Galois tower of field extensions

$$\mathbb{Q} = \mathcal{K}_0 \subset \mathcal{K}_1 \subset \ldots \subset \mathcal{K}_\alpha = \mathcal{K}$$

along with the associated partial traces.

8.2 Partial traces and fast evaluation of the complete trace

When dealing with a tower of field extensions $\mathbb{Q} \subseteq \mathcal{L} \subseteq \mathcal{K}$, the complete trace from $\mathcal{K}$ to $\mathbb{Q}$ can be efficiently expressed in terms of partial traces. The procedure involves first calculating the partial trace from $\mathcal{K}$ down to $\mathcal{L}$, and then from $\mathcal{L}$ to $\mathbb{Q}$. This decomposition effectively simplifies what might otherwise be a complex computation into more manageable steps. We will explore these optimization opportunities further in this section.

8.2.1 Fast evaluation of the trace: a first approach

A tower of fields can be intuitively constructed by introducing, for $1 \leq j \leq \alpha$, the extensions $\mathcal{K}_j$ over $\mathbb{Q}$, which have degree $(t-1)t^{j-1}$, defined as follows:

$$\begin{aligned}
\mathbb{Q} = \mathcal{K}_0 &:= \left\{ P(X^{M/1}) \bmod \Phi_M(X), P \in \mathbb{Q}[X] \right\}, \\
\mathcal{K}_1 &:= \left\{ P(X^{M/t}) \bmod \Phi_M(X), P \in \mathbb{Q}[X] \right\}, \\
\mathcal{K}_2 &= \left\{ P(X^{M/t^2}) \bmod \Phi_M(X), P \in \mathbb{Q}[X] \right\}, \\
&\vdots \\
\mathcal{K}_j &= \left\{ P(X^{M/t^j}) \bmod \Phi_M(X), P \in \mathbb{Q}[X] \right\}, \\
&\vdots \\
\mathcal{K}_\alpha &= \left\{ P(X^{M/t^\alpha}) \bmod \Phi_M(X), P \in \mathbb{Q}[X] \right\} = \mathcal{K}.
\end{aligned}$$

It is noteworthy that $\mathcal{K}_1$ is isomorphic to the field $\mathbb{Q}[X]/\Phi_t(X)$, while $\mathcal{K}_2$ corresponds to the field $\mathbb{Q}[X]/\Phi_{t^2}(X)$. This pattern continues until $\mathcal{K}_\alpha$ which coincides with $\mathcal{K} = \mathbb{Q}[X]/\Phi_M(X)$. We then examine the tower structure defined by the following inclusions:

$$\mathbb{Q} = \mathcal{K}_0 \subset \mathcal{K}_1 \subset \mathcal{K}_2 \subset \cdots \subset \mathcal{K}_{\alpha-1} \subset \mathcal{K}_\alpha = \mathcal{K},$$

which enables the decomposition of the trace utilizing the tower structure of the associated Galois groups as follows:

$$\mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0} = \mathrm{Tr}_{\mathcal{K}_1/\mathcal{K}_0} \circ \mathrm{Tr}_{\mathcal{K}_2/\mathcal{K}_1} \circ \cdots \circ \mathrm{Tr}_{\mathcal{K}/\mathcal{K}_{\alpha-1}}. \tag{18}$$

Lemme 8.2 *The Galois groups associated to the successive field extensions may be described as follows: for all* $1 \leq j \leq \alpha$*,*

$$\mathrm{Gal}(\mathcal{K}_j/\mathcal{K}_0) = \left\{ \tau_d \,|\, 0 \leq d \leq t^j - 1, \, \gcd(d,t) = 1 \right\},$$

and for all $0 \leq j \leq \alpha - 1$*:*

$$\mathrm{Gal}(\mathcal{K}/\mathcal{K}_j) = \left\{ \tau_d \,|\, d = kt^j + 1, \, 0 \leq k \leq t^{\alpha-j} - 1 \right\}.$$

Furthermore, we have, for all $1 \leq j \leq \alpha$*:*

$$\mathrm{Gal}(\mathcal{K}_{j+1}/\mathcal{K}_j) = \left\{ \tau_d \,|\, d = kt^j + 1, \, 0 \leq k \leq t - 1 \right\}. \tag{19}$$

Proof. To prove (19), observe that we must have

$$\forall\, \tau_d \in \mathrm{Gal}(\mathcal{K}_{j+1}/\mathcal{K}_j), \quad \tau_d\left(X^{M/t^j}\right) = X^{M/t^j}.$$

Hence, $X^{(d-1)M/t^j} = 1$, so that $(d-1)M/t^j = 0 \bmod M$. In other words, $d = kt^j + 1$ for some $k \in \mathbb{Z}$. In order to prove that we only need to consider values of k in $\{0, \ldots, t-1\}$, we decompose $k = qt + r$ with $0 \le r \le t-1$, and notice that

$$\frac{dM}{t^{j+1}} = \frac{(kt^j+1)M}{t^{j+1}} = \frac{((qt+r)t^j+1)M}{t^{j+1}} = \frac{((rt^j+1)M}{t^{j+1}} \bmod M.$$

This completes the proof of (19).

Efficiency: We now elucidate why the decomposition formula (18) facilitates a more efficient homomorphic evaluation of an encryption of $\mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0}(\mu(X))$. The costs can be assessed in terms of the number of necessary automorphisms (or key-switchings). Recall that directly computing the complete trace requires $N-1 = (t-1)t^{\alpha-1} - 1$ non-trivial automorphisms. By utilizing the decomposition (18), only $t-1$ non-trivial automorphisms are needed for each partial trace $\mathrm{Tr}_{\mathcal{K}_{j+1}/\mathcal{K}_j}$, for $1 \le j \le \alpha - 1$, and $t-2$ automorphisms for evaluating $\mathrm{Tr}_{\mathcal{K}_1/\mathcal{K}_0}$. Indeed, the order of the Galois group $\mathrm{Gal}_{\mathcal{K}_{j+1}/\mathcal{K}_j}$ is t for $1 \le j \le \alpha - 1$, and $t-1$ for $j = 0$. Consequently, the total number of required automorphisms is $(\alpha-1)(t-1) + t - 2 = \alpha(t-1) - 1$, which is significantly less than $N-1$.

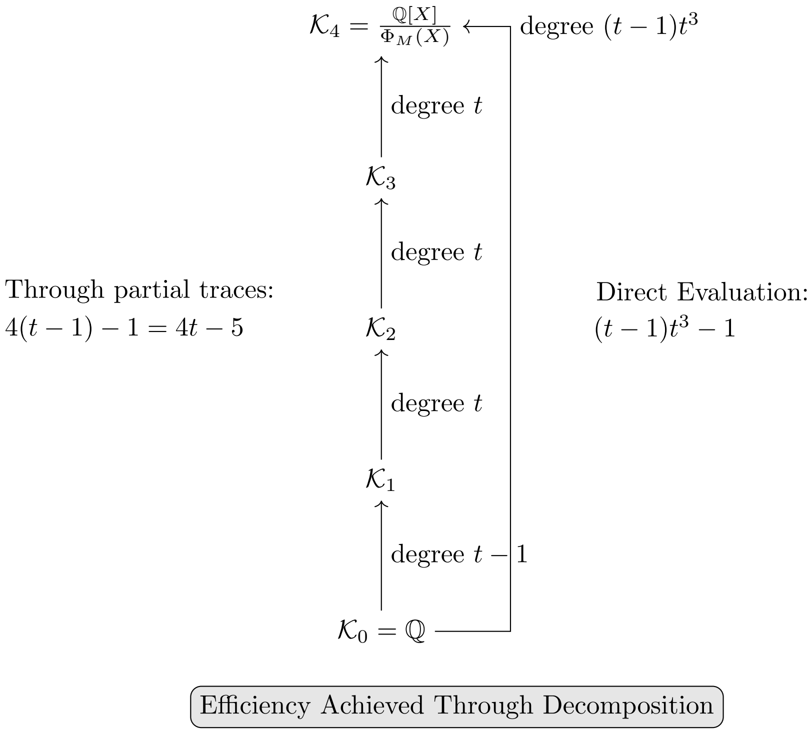


Figure 1: Illustration of the Galois tower with $\alpha = 4$ and the decomposition of the trace.

The structure of the Galois groups allows us to express the successive traces, for $1 \le j \le$

$\alpha - 1$, as

$$\forall\, P \in \mathcal{K},\ \mathrm{Tr}_j(P)(X) = \sum_{0 \le k \le t-1} P(X^{kt^j+1}), \tag{20}$$

and for the case $j = 0$:

$$\forall\, P \in \mathcal{K},\ \mathrm{Tr}_0(P)(X) = \sum_{0 \le k \le t-1} P(X^k). \tag{21}$$

Note that $\mathrm{Tr}_j(P)(X) = \mathrm{Tr}_{\mathcal{K}_{j+1}/\mathcal{K}_j}(P)(X)$ for $P \in \mathcal{K}_{j+1}$. Introducing the notation for $0 \le j \le \alpha$ (note that $\mathcal{T}_\alpha = \mathcal{T}$ and $\mathcal{T}_0 \equiv \mathbb{T}$)

$$\mathcal{T}_j = \left\{ P(X^{M/t^j}) \bmod \mathbb{Z}[X] \bmod \Phi_M(X), P \in \mathbb{Q}[X] \right\},$$

their homomorphic computation can be carried out as described in the following algorithm:

Algorithm 16 Partial Trace $\mathrm{Tr}_j(\mu)$ of $\mu(X) \in \mathcal{K}$ for $1 \le j \le \alpha - 1$

Input: RLWE encryption $c(X) = (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$ of $\mu(X)$ with key $s(X) \in \mathcal{R}$
Initialize: $(a_\Sigma(X), b_\Sigma(X)) = (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$
for $k = 1$ **to** $t - 1$ **do**
  Compute: $d = kt^j + 1$
  Compute: $(a(X^d), b(X^d)) \bmod \mathcal{R}$
  Perform key switching: $(a_d(X), b_d(X)) = \mathrm{KeySwitch}_{s(X^d) \to s(X)}\left((a(X^d), b(X^d))\right)$
  $(a_\Sigma(X), b_\Sigma(X)) \leftarrow (a_\Sigma(X), b_\Sigma(X)) + (a_d(X), b_d(X))$
end for
Output: $(a_\Sigma(X), b_\Sigma(X)) = \mathrm{RLWE}_{s(X)}(\mathrm{Tr}_{\mathcal{K}_{j+1}/\mathcal{K}_j}(\mu(X)))$ with key $s(X)$

We will temporarily defer discussion of a similar algorithm for the trace Tr_0 since it can be further decomposed and optimized. In the meantime, we can present the following:

Proposition 8.3 *Let $M = t^\alpha$ with $\alpha \ge 1$, where t is a prime. We have the following identities in $\mathcal{K}$: For all $\nu \in \mathbb{Z}$ and all $1 \le j \le \alpha - 1$, the trace is given by:*

$$\mathrm{Tr}_j\left(X^\nu\right) = \begin{cases} tX^\nu & \text{if } [\nu]_{M/t^j} = 0, \\ 0 & \text{if } [\nu]_{M/t^j} \ne 0 \quad \text{and} \quad [\nu]_{M/t^{j+1}} = 0, \\ \sum_{k=0}^{t-1} X^{\nu\left(1+kt^j\right)} & \text{if } [\nu]_{M/t^{j+1}} \ne 0. \end{cases}$$

And for $j = 0$:

$$\mathrm{Tr}_0\left(X^\nu\right) = \begin{cases} t - 1 & \text{if } [\nu]_M = 0, \\ -1 & \text{if } [\nu]_M \ne 0 \quad \text{and} \quad [\nu]_{M/t} = 0, \\ \sum_{k=1}^{t-1} X^{\nu k} & \text{if } [\nu]_{M/t} \ne 0. \end{cases}$$

In particular

$$\mathrm{Tr}_0\left((1 - X^{M/t})X^\nu\right) = \begin{cases} t & \text{if } [\nu]_M = 0, \\ 0 & \text{if } [\nu]_M \ne 0 \quad \text{and} \quad [\nu]_{M/t} = 0, \\ \sum_{k=1}^{t-1} X^{\nu k}\left(1 - X^{kM/t}\right) & \text{if } [\nu]_{M/t} \ne 0. \end{cases}$$

8.2.2 Fast evaluation of the Trace: the algebraic approach

We recall that a tower of fields can be constructed using the corresponding tower of Galois groups via the fundamental theorem of Galois theory. This theorem asserts that for every subgroup G of $\mathrm{Gal}(\mathcal{K}/\mathbb{Q})$, there exists an intermediate field $\mathcal{G}$ such that $\mathbb{Q} \subseteq \mathcal{G} \subseteq \mathcal{K}$, with $\mathcal{G}$ being the fixed field of G. Specifically, the fixed field of G comprises those elements in $\mathcal{K}$ that remain unchanged under all automorphisms in G. In our context, identifying subgroups of $\mathrm{Gal}(\mathcal{K}/\mathbb{Q})$ is particularly straightforward, as these subgroups are isomorphic to the subgroups of $\mathbb{Z}_M^\times$. To enumerate the elements of these Galois subgroups, it is customary to utilize the generators of the group $\mathbb{Z}_M^\times$. It is well-known that for a prime $t \geq 3$, the group $(\mathbb{Z}_{t^\alpha})^\times$ has a generator, unlike the situation for $t = 2$, which only possesses a generator if $\alpha = 2$ or $\alpha = 4$. Furthermore, this generator can be readily derived in one of the following ways:

- If $\tilde{g}$ is of order $t-1$ in $(\mathbb{Z}_{t^\alpha})^\times$ then $g = (t+1)\tilde{g}$ serves as a generator of $(\mathbb{Z}_{t^\alpha})^\times$;
- Alternatively, if $\tilde{g}$ is a generator of $\mathbb{Z}_t^\times$, it is known that either $g = \tilde{g}$ or $g = \tilde{g} + t$ will act as a generator of $\mathbb{Z}_{t^2}^\times$ and also a generator of $(\mathbb{Z}_{t^\beta})^\times$ for any power $\beta \geq 2$.

Thus, assuming that g is a generator of $(\mathbb{Z}_{t^\alpha})^\times$ coinciding with $\tilde{g}$ or $\tilde{g}+t$ (where $\tilde{g}$ is a generator of $\mathbb{Z}_t^\times$), we have

$$\mathrm{Gal}(\mathcal{K}/\mathbb{Q}) = \{\tau_{g^k},\ k = 0, \dots, N-1\} \cong \mathbb{Z}_M^\times \cong (\mathbb{Z}_N, +)$$

and we have the following sequence of inclusions of additive sub-groups:

$$(t-1)t^{\alpha-1}\mathbb{Z}_1 \subset (t-1)t^{\alpha-2}\mathbb{Z}_t \subset (t-1)t^{\alpha-3}\mathbb{Z}_{t^2} \subset \dots \subset (t-1)t\mathbb{Z}_{t^{\alpha-2}} \subset (t-1)\mathbb{Z}_{t^{\alpha-1}} \subset \mathbb{Z}_N,$$

to which we can associate a tower of Galois groups

$$\{\tau_1\} \subset G_1 = \{\tau_{g^k},\ k \in (t-1)t^{\alpha-2}\mathbb{Z}_t\} \subset \dots \subset G_{\alpha-1} = \{\tau_{g^k},\ k \in (t-1)\mathbb{Z}_{t^{\alpha-1}}\} \subset \mathrm{Gal}_{\mathcal{K}/\mathbb{Q}},$$

and by the Galois correspondence, a tower of Galois fields

$$\mathcal{K} \supset \mathcal{K}_{\alpha-1} \supset \dots \supset \mathcal{K}_1 \supset \mathbb{Q}. \tag{22}$$

Note that the fixed field $\mathcal{G}_j$ associated with G_j for $1 \leq j \leq \alpha - 1$ is unique and must coincide with with $\mathcal{K}_j$ due to the following relationships:

$$[\mathcal{K} : \mathcal{K}_j] = |\mathrm{Gal}(\mathcal{K}/\mathcal{K}_j)| = t^{\alpha-j} = |G_j| = [\mathcal{K} : \mathcal{G}_j].$$

In summary, we can state the following:

Lemme 8.4 *The successive Galois groups associated with the field tower described in (22) can be characterized as follows:*

$$\mathrm{Gal}(\mathcal{K}_{j+1}/\mathcal{K}_j) = \left\{\tau_d,\ d = g^{k(t-1)t^{j-1}},\ 0 \leq k \leq t-1\right\}, \quad \textit{for all } 1 \leq j \leq \alpha - 1,$$
$$\mathrm{Gal}(\mathcal{K}_j/\mathcal{K}_0) = \left\{\tau_d, d = g^k,\ 0 \leq k \leq (t-1)t^{j-1} - 1\right\}, \quad \textit{for all } 1 \leq j \leq \alpha.$$

The corresponding composition of partial traces

$$\mathrm{Tr}_{\mathcal{K}/\mathcal{K}_0} = \mathrm{Tr}_0 \circ \mathrm{Tr}_1 \circ \dots \circ \mathrm{Tr}_{\alpha-1}.$$

involves

$$(\alpha-1)(t-1) + t - 2 = \alpha(t-1) - 1$$

non-trivial automorphisms.

Another "natural" tower of Galois groups is given by the sequence

$$\{\tau_1\} \subset H_1 = \{\tau_{g^k},\ k \in t^{\alpha-1}\mathbb{Z}_{t-1}\} \subset \ldots \subset H_{\alpha-1} = \{\tau_{g^k},\ k \in t\mathbb{Z}_{(t-1)t^{\alpha-2}}\} \subset \mathrm{Gal}_{\mathcal{K}/\mathbb{Q}}$$

which is associated with the field tower

$$\mathcal{K} \supset \mathcal{H}_{\alpha-1} = \mathbb{Q}(\tau(X), \tau \in H_{\alpha-1}) \supset \ldots \supset \mathcal{H}_1 = \mathbb{Q}(\tau(X), \tau \in H_1) \supset \mathbb{Q}.$$

where $\mathbb{Q}(\tau(X), \tau \in H_j)$ represents the field generated by the elements $\tau(X), \tau \in H_j$. The associated trace decomposition differs slightly from the previous one but does not provide any computational advantage; thus, it will not be further discussed.

Remark 8.5 *In general, there are several possible configurations for towers of Galois groups. For illustration, we will comprehensively construct these towers with* $t = 7$ *and* $\alpha = 2$*. Specifically, we create the Tower of Subgroups of the Multiplicative Group* $\mathbb{Z}_{49}^{\times}$*:*

(i) The group $\mathbb{Z}_{49}^{\times}$ *consists of integers from* 1 *to* 48 *that are coprime to* 49*. There are* $|\mathbb{Z}_{49}^{\times}| = \varphi(49) = 7 \cdot 6 = 42$ *elements in* $\mathbb{Z}_{49}^{\times}$*:*

$$\mathbb{Z}_{49}^{\times} = \{1, \ldots, 6, 8, \ldots, 13, 15, \ldots, 20, 22, \ldots, 27, 29, \ldots, 34, 36, \ldots, 41, 43, \ldots, 48\}.$$

(ii) The possible orders of the subgroups must divide 42 *(the order of the group). Thus, the possible orders are:* $1, 2, 3, 6, 7, 14, 21, 42$.

(iii) The subgroups of $\mathbb{Z}_{49}^{\times}$ *are thus:*
Order 1*:* $G_0 = H_0 = \{1\}$.
Order 2*:* $H_{0,2} = \{1, 48\}$.
Order 3*:* $H_{0,3} = \{1, 18, 30\}$.
Order 6*:* $H_1 = \{1, 18, 19, 30, 31, 48\}$.
Order 7*:* $G_1 = \{1, 8, 15, 22, 29, 36, 43\}$.
Order 14*:* $G_{1,3} = \{1, 6, 8, 13, 15, 20, 22, 27, 29, 34, 36, 41, 43, 48\}$.
Order 21*:* $G_{1,2} = \{1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32, 36, 37, 39, 43, 44, 46\}$.
Order 42*:* $G_2 = H_2 = \mathbb{Z}_{49}^{\times}$.

Note that we have not represented the more elementary towers with fewer subgroups such as $G_0 \subset H_1 \subset H_2$.

Now, a last observation is in order: as can be seen on the example in Remark 8.5, the subgroups $G_{1,2}$ or $G_{1,3}$ can be introduced in the sequence

$$G_1 \subset G_{1,2} \subset G_2 \quad \text{or} \quad G_1 \subset G_{1,3} \subset G_2.$$

If ℓ divides $t-1$, it is in fact always possible to introduce a subgroup $G_{\alpha-1,\ell}$ in the sequence of inclusions

$$G_{\alpha-1} \subset G_{\alpha-1,\ell} \subset G_\alpha = \mathbb{Z}_M^{\times}$$

into strict subgroups of cardinals ℓ and $(t-1)/\ell$ as soon as $t \geq 3$. The Galois subgroup $G_{\alpha-1,\ell}$ is again characterized by the corresponding subgroup $\ell\mathbb{Z}_{\frac{N}{\ell}}$ of $\mathbb{Z}_N$

$$G_{\alpha-1,\ell} = \{\tau_{g^k}, k \in \ell\mathbb{Z}_{\frac{N}{\ell}}\}$$

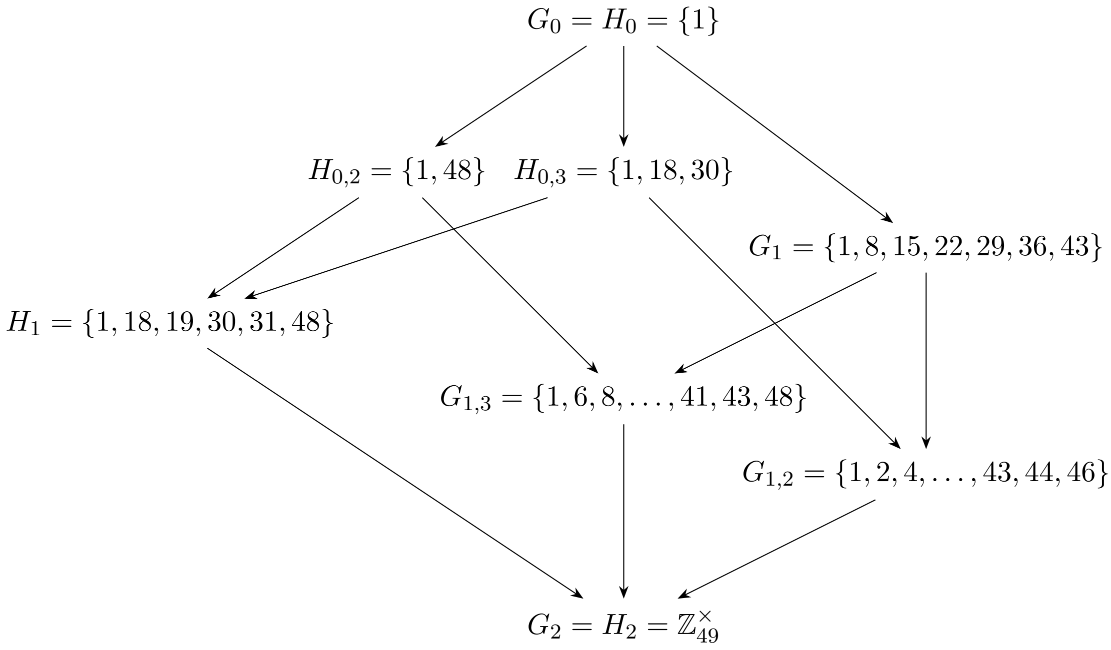


Figure 2: Tower of subgroups of the multiplicative group $\mathbb{Z}_{49}^{\times}$.

to which we can associated the field extension $\mathcal{K}_{1,\ell} := \mathbb{Q}(\tau(X), \tau \in G_{\alpha-1,\ell})$ in such a way that

$$\mathcal{K}_1 \supset \mathcal{K}_{1,\ell} \supset \mathbb{Q}.$$

More generally, if $t - 1 = \ell_1 \ell_2 \cdots \ell_r$ with $r \geq 2$, we can establish the following tower of subgroups:

$$G_{\alpha-1} \subset G_{\alpha-1,\ell_1\cdots\ell_r} \subset G_{\alpha-1,\ell_1\cdots\ell_{r-1}} \subset \ldots \subset G_{\alpha-1,\ell_1} \subset G_\alpha = \mathbb{Z}_M^{\times}$$

Let $\mathcal{K}_{1,\ell_1\cdots\ell_j}$ denote the associated fixed field such that:

$$\mathcal{K}_1 \supset \mathcal{K}_{1,\ell_1\cdots\ell_r} \supset \mathcal{K}_{1,\ell_1\cdots\ell_{r-1}} \supset \ldots \supset \mathcal{K}_{1,\ell_1} \supset \mathbb{Q}.$$

For $2 \leq j \leq r$, we have:

$$\mathrm{Gal}(\mathcal{K}/\mathcal{K}_{1,\ell_1\ell_2\cdots\ell_{j-1}}) = \{\tau_{g^k}, k \in (\ell_1 \cdots \ell_{j-1})\mathbb{Z}_{\ell_j\cdots\ell_r}\}.$$

Additionally,

$$\mathrm{Gal}(\mathcal{K}_{1,\ell_1\ell_2\cdots\ell_j}/\mathcal{K}_{1,\ell_1\ell_2\cdots\ell_{j-1}}) = \left\{\tau_{g^{k\ell_1\cdots\ell_{j-1}}},\ k \in \mathbb{Z}_{\ell_j}\right\}.$$

As an immediate consequence, the first term of the decomposition in (18) can be factored as follows:

$$\mathrm{Tr}_{\mathcal{K}_1/\mathbb{Q}} = \mathrm{Tr}_{\mathcal{K}_{1,\ell_1}/\mathbb{Q}} \circ \mathrm{Tr}_{\mathcal{K}_{1,\ell_1\ell_2}/\mathcal{K}_{1,\ell_1}} \circ \cdots \circ \mathrm{Tr}_{\mathcal{K}_{1,\ell_1\ell_2\cdots\ell_r}/\mathcal{K}_{1,\ell_1\ell_2\cdots\ell_{r-1}}}.$$

The evaluation of this trace requires:

$$\sum_{j=1}^{r}(\ell_j - 1)$$

non-trivial automorphisms instead of $t-2$. This reduction is particularly significant when $t-1=2^{\gamma}$, since

$$\sum_{j=1}^{r}(\ell_j-1)=\sum_{j=1}^{\gamma}(2-1)=\gamma=\log_2(t-1).$$

It has become quite straightforward to obtain the following algorithm for the optimized partial trace $\mathrm{Tr}_{\mathcal{K}_1/\mathbb{Q}}$:

Algorithm 17 Partial Trace $\mathrm{Tr}_0(\mu)$ of $\mu(X)\in\mathcal{K}$

Input: $c(X)=(a(X),b(X))=\mathrm{RLWE}_{s(X)}(\mu(X))$ of $\mu(X)$ with key $s(X)\in\mathcal{R}$, g a generator of $\mathbb{Z}_M^{\times}$ and $t-1$.
Initialize: $\Pi=t-1$, $\ell=2$ and $(\tilde{a}(X),\tilde{b}(X))=(a(X),b(X))\in\mathcal{T}\times\mathcal{T}$
while $\Pi>1$ **do**
  while $\ell\nmid\Pi$ **do**
    $\ell\leftarrow\mathrm{NextPrime}(\ell)$
  end while
  $\Pi\leftarrow\Pi/\ell$
  $(a_{\Sigma}(X),b_{\Sigma}(X))\leftarrow(\tilde{a}(X),\tilde{b}(X))$
  for $k=1$ **to** $\ell-1$ **do**
    Compute: $d=g^{k\Pi}$
    Compute: $(\tilde{a}(X^d),\tilde{b}(X^d))$ mod $\mathcal{R}$
    Perform key switching:

$$(\tilde{a}_d(X),\tilde{b}_d(X))=\mathrm{KeySwitch}_{s(X^d)\to s(X)}\left((\tilde{a}(X^d),\tilde{b}(X^d))\right)$$

    $(a_{\Sigma}(X),b_{\Sigma}(X))\leftarrow(a_{\Sigma}(X),b_{\Sigma}(X))+(\tilde{a}_d(X),\tilde{b}_d(X))$
  end for
  $(\tilde{a}(X),\tilde{b}(X))\leftarrow(a_{\Sigma}(X),b_{\Sigma}(X))$
end while
Output: $(\tilde{a}(X),\tilde{b}(X))=\mathrm{RLWE}_{s(X)}(\mathrm{Tr}_0(\mu(X)))$ with key $s(X)$

8.2.3 General expression of the trace for $t\geq 3$.

Assume g that is a generator of $\mathbb{Z}_M^{\times}$ and that $N=\ell_1\ell_2\cdots\ell_r$, where $(\ell_k)_{1\leq k\leq r}$ represents a sequence of prime divisors, some of which may occur more than once. We define

$$F_{\ell}=\{\tau_{g^k},k\in\ell\mathbb{Z}_{\frac{N}{\ell}}\}\subset\mathbb{Z}_M^{\times}$$

resulting in the following sequence of subgroup inclusions:

$$\{1\}=F_{\ell_1\cdots\ell_r}\subset F_{\ell_1\cdots\ell_{r-1}}\subset\ldots\subset F_{\ell_1}\subset F_1=\mathbb{Z}_M^{\times}$$

Let $\mathcal{F}_{\ell}$ denote the fixed field associated with F_{ℓ}, such that:

$$\mathcal{K}=\mathcal{F}_N=\mathcal{F}_{\ell_1\cdots\ell_r}\supset\mathcal{F}_{\ell_1\cdots\ell_{r-1}}\supset\ldots\supset\mathcal{F}_{\ell_1}\supset\mathcal{F}_1=\mathbb{Q}$$

Consequently, the trace can be expressed as:

$$\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}=\mathrm{Tr}_{\mathcal{F}_{\ell_1}/\mathbb{Q}}\circ\mathrm{Tr}_{\mathcal{F}_{\ell_1\ell_2}/\mathcal{F}_{\ell_1}}\circ\cdots\circ\mathrm{Tr}_{\mathcal{K}/\mathcal{F}_{\ell_1\ell_2\cdots\ell_{r-1}}}.$$

The corresponding Galois groups are given for $0 \le j \le r$ by

$$\mathrm{Gal}(\mathcal{F}_{\ell_1\cdots\ell_j}/\mathcal{F}_{\ell_1\cdots\ell_{j-1}}) = \{\tau_{g^k}, k \in (\ell_1\cdots\ell_{j-1})\mathbb{Z}_{\ell_j}\}$$

where we adopt the convention that $\ell_0 = 1$. We now present the corresponding algorithm:

Algorithm 18 CompleteTrace: computes an encryption of $\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\mu)$ for $\mu(X) \in \mathcal{T}$

Input: $c(X) = (a(X), b(X)) = \mathrm{RLWE}_{s(X)}(\mu(X))$ of $\mu(X)$ with key $s(X) \in \mathcal{R}$, g a generator of $\mathbb{Z}_M^\times$ and $N = \varphi(M)$.
Initialize: $\Pi \leftarrow N$, $\ell \leftarrow 2$ and $(\tilde{a}(X), \tilde{b}(X)) \leftarrow (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$
while $\Pi > 1$ **do**
  while $\ell \nmid \Pi$ **do**
    $\ell \leftarrow \mathrm{NextPrime}(\ell)$
  end while
  $\Pi \leftarrow \Pi/\ell$
  $(a_\Sigma(X), b_\Sigma(X)) \leftarrow (\tilde{a}(X), \tilde{b}(X))$
  for $k = 1$ **to** $\ell - 1$ **do**
    Compute: $d = g^{k\Pi}$
    Compute: $(\tilde{a}(X^d), \tilde{b}(X^d)) \bmod \mathcal{R}$
    Perform key switching:

$$(\tilde{a}_d(X), \tilde{b}_d(X)) = \mathrm{KeySwitch}_{s(X^d)\to s(X)}\left((\tilde{a}(X^d), \tilde{b}(X^d))\right)$$

    $(a_\Sigma(X), b_\Sigma(X)) \leftarrow (a_\Sigma(X), b_\Sigma(X)) + (\tilde{a}_d(X), \tilde{b}_d(X))$
  end for
  $(\tilde{a}(X), \tilde{b}(X)) \leftarrow (a_\Sigma(X), b_\Sigma(X))$
end while
Output: $(\tilde{a}(X), \tilde{b}(X)) = \mathrm{RLWE}_{s(X)}(\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\mu(X)))$ with key $s(X)$

We conclude this section by presenting Algorithm 19 for the partial trace $\mathrm{Tr}_{i,j}$, which maps a $\mathbb{Q}$-extension of degree i to a $\mathbb{Q}$-extension of degree $j|i$ within the field $\mathcal{K}$:

$$\mathrm{Tr}_{i,j} = \mathrm{Tr}_j \circ \ldots \circ \mathrm{Tr}_i.$$

Note that if i/j has a non-trivial divisor, say d for instance, then it is more efficient to compute $\mathrm{Tr}_{i,j}$ by applying Algorithm 19 twice, specifically as $\mathrm{Tr}_{i,dj} \circ \mathrm{Tr}_{dj,j}$.

Appendix

Elementary operations in prime power cyclotomic rings

In this section of the paper, we explore the elementary operations necessary for manipulating the polynomials in $\mathcal{K}$ when the M-th cyclotomic polynomial Φ_M is defined by

$$\Phi_M(X) = \sum_{k=0}^{t-1} X^{k\frac{M}{t}} \tag{23}$$

so that

$$\Phi_M(X)(X^{\frac{M}{t}} - 1) = X^M - 1.$$

Algorithm 19 PartialTrace$_{i\to j}$: computes an encryption of $\mathrm{Tr}_{i,j}(\mu)$ for $\mu(X) \in \mathcal{T}$

Input: $c(X) = (a(X), b(X)) = \mathrm{RLWE}_{s(X)}(\mu(X))$ of $\mu(X)$ with key $s(X) \in \mathcal{R}$, g a generator of $\mathbb{Z}_M^\times$, $j|i$, $i|N = \varphi(M)$.
Initialize: $\ell \leftarrow i/j$ and $(a_\Sigma(X), b_\Sigma(X)) \leftarrow (a(X), b(X)) \in \mathcal{T} \times \mathcal{T}$
for $k = 1$ **to** $\ell - 1$ **do**
  Compute: $d = g^{kj}$ and $(a(X^d), b(X^d)) \bmod \mathcal{R}$
  Perform key switching:

$$(a_d(X), b_d(X)) = \mathrm{KeySwitch}_{s(X^d)\to s(X)}\Big((a(X^d), b(X^d))\Big)$$

  $(a_\Sigma(X), b_\Sigma(X)) \leftarrow (a_\Sigma(X), b_\Sigma(X)) + (a_d(X), b_d(X))$
end for
Output: $(a_\Sigma(X), b_\Sigma(X)) = \mathrm{RLWE}_{s(X)}(\mathrm{Tr}_{i,j}(\mu(X)))$ with key $s(X)$

Taking the modulo Φ_M

We begin by deriving a straightforward formula that allows to take the modulo Φ_M of any polynomial of degree less than or equal to $M-1$ within the ring $\mathcal{K}$. This can always be assumed as $X^M = 1 \bmod \Phi_M$.

Lemme 8.6 *Given $M = t^\alpha$ and $N = (t-1)t^{\alpha-1}$, consider the polynomial*

$$R(X) = \sum_{i=0}^{M-1} r_i X^i \in \mathcal{K}.$$

Then its unique representative modulo Φ_M of degree less or equal to $N-1$ is given by

$$(R \mod \Phi_M)(X) = \sum_{i=0}^{N-1} \left(r_i - r_{N+(i \bmod \frac{M}{t})}\right) X^i.$$

Proof. We first split R into two sums

$$R(X) = \sum_{k=0}^{M-1} r_k X^k = \sum_{k=0}^{N-1} r_k X^k + \sum_{k=N}^{M-1} r_k X^k = \sum_{k=0}^{N-1} r_k X^k + \sum_{k=0}^{M-N-1} r_{k+N} X^{k+N}.$$

and then use the following expression of Φ_M

$$X^N = -\sum_{j=0}^{t-2} X^{j\frac{M}{t}} \mod \Phi_M,$$

to rewrite R as

$$R(X) = \sum_{k=0}^{N-1} r_k X^k - \sum_{k=0}^{M-N-1} r_{k+N} \sum_{j=0}^{t-2} X^{k+j\frac{M}{t}} \mod \Phi_M.$$

Denoting

$$i = k + j\frac{M}{t},$$

and taking into account that $0 \leq k \leq M - N - 1 = \frac{M}{t} - 1$, we have

$$0 \leq i \leq M - N - 1 + (t-2)\frac{M}{t} = N - 1 \quad \text{and} \quad k = i \bmod \frac{M}{t}.$$

Eventually,

$$R(X) = \sum_{i=0}^{N-1} \left(r_i - r_{N+i \bmod \frac{M}{t}}\right) X^i \mod \Phi_M.$$

Multiplication of polynomials

We now give the expression of the product modulo Φ_M of two polynomials.

Lemme 8.7 *Consider the following two polynomials of degrees less than $M-1$*

$$D(X) = \sum_{k=0}^{M-1} d_k X^k \in \mathcal{K} \quad \textit{and} \quad P(X) = \sum_{k=0}^{M-1} a_k X^k \in \mathcal{K}.$$

The product $D \cdot P$ results in a polynomial in $\mathcal{K}$, and its unique representative modulo Φ_M of degree less than or equal to $N-1$ can be expressed as follows:

$$(D \cdot P)(X) = \sum_{i=0}^{N-1} \left(\sum_{j=0}^{M-1} d_j \left(a_{i-j} - a_{N-j+i \textit{ mod } \frac{M}{t}}\right)\right) X^i \quad \textit{mod } \Phi_M,$$

where we adopt the convention that $a_{k+M} = a_k$ for all $k \in \mathbb{Z}$.

Proof. The product $D \cdot P$ modulo $X^M - 1$ can easily be written as

$$D(X)P(X) = \sum_{i=0}^{M-1} \left(\sum_{j=0}^{M-1} d_j a_{i-j} \right) X^i \mod X^M - 1,$$

with the convention that $a_{M+j} = a_j$ for all $j \in \mathbb{Z}$. Now, by applying Lemma 8.6 to $R = D \cdot P$, we obtain the result stated in this lemma.

Remark for $t = 2$, $M = 2N$. If either of the polynomials D or P has a degree less than or equal to $(N-1)$ –let's assume D for instance– the summation over j can be restricted to indices between 0 and $N-1$. In the case where both polynomials have degrees less than or equal to $N-1$ and $M = 2N$, the sums can be further truncated. Specifically, we have:

$$D(X)P(X) = \sum_{i=0}^{N-1} \left(\sum_{j=0}^{i} d_j a_{i-j} - \sum_{j=i+1}^{N-1} d_j a_{N+i-j} \right) X^i \mod \quad X^N + 1.$$

Now, provided that the coefficients of D and P are extended by zeros for indices between N and $M-1$, and that both the negacyclicity and M-periodicity conventions $d_{N+i} = -d_i$, $a_{N+i} = -a_i$ and $d_{M+i} = d_i$, $a_{M+i} = a_i$ for all $i \in \mathbb{Z}$ hold, then we obtain the simple (and well-known) formula

$$D(X)P(X) = \sum_{i=0}^{N-1} \left(\sum_{j=0}^{N-1} d_j a_{i-j} \right) X^i \mod X^N + 1.$$

8.3 Estimates of the error growth resulting from a polynomial product

We now turn our attention to the number of non-zero terms in the coefficients of the product modulo Φ_M of two polynomials of degree less than $N-1$. Specifically, we seek to determine the number of non-zero terms in the sums given by

$$\sum_{j=0}^{N-1} d_j \left(a_{i-j} - a_{N-j+i \bmod \frac{M}{t}}\right).$$

We will show that an accurate estimate of this quantity allows us to effectively evaluate how the noise is amplified during various encryption operations, including bootstrapping, key-switching, and packing. For instance, in the particular case where $t=2$, this number equals N (as opposed to $2N$), which elucidates the multiplicative factor of N that appears in the noise levels of nearly all encryption operations involving polynomials. More specifically, we have the following lemma:

Lemme 8.8 *Let t be a prime integer, $M = t^\alpha$, with $\alpha \geq 2$, and $N = \varphi(M) = \frac{t-1}{t}M$. Consider the polynomials*

$$D = \sum_{i=0}^{N-1} d_i X^i \in \mathcal{R}, \qquad E = \sum_{i=0}^{N-1} e_i X^i \in \mathcal{T}$$

where the coefficients d_i and e_i are independent random variables with common standard deviations $\sigma(D)$ and $\sigma(E)$, respectively. Finally, let

$$P(X) = D(X) \cdot E(X) \ mod\ \Phi_M(X) = \sum_{i=0}^{N-1} p_i X^i$$

The variance of the random variable p_i can be expressed as follows:

$$\sigma(p_i)^2 = \left(N + i - i \ mod\ \frac{M}{t} + \max\left(N - 1 - \frac{M}{t} - i, 0\right)\right) \sigma(D)^2 \sigma(E)^2, \quad 0 \leq i \leq N-1.$$

Proof. For $0 \leq i \leq N-1$, let

$$A_i = \left\{0 \leq j \leq N-1, \quad s.\ t. \quad (i-j) \bmod M \leq N-1 \ and\ \left(N - j + i \bmod \frac{M}{t}\right) \leq N-1\right\},$$

$$B_i = \left\{0 \leq j \leq N-1, \quad s.\ t. \quad (i-j) \bmod M \geq N \ and\ \left(N - j + i \bmod \frac{M}{t}\right) \leq N-1\right\},$$

$$C_i = \left\{0 \leq j \leq N-1, \quad s.\ t. \quad (i-j) \bmod M \leq N-1 \quad and\ \left(N - j + i \bmod \frac{M}{t}\right) \geq N\right\}.$$

We have from lemma 8.7 the following expression for the coefficient p_i:

$$p_i = \sum_{j \in A_i} d_j \left(e_{i-j} - e_{N-j+i \bmod \frac{M}{p}}\right) - \sum_{j \in B_i} d_j e_{N-j+i \bmod \frac{M}{t}} + \sum_{j \in C_i} d_j e_{i-j}.$$

This formulation relies on the conditions that

$$0 \leq N - j + i \bmod \frac{M}{t} \leq M-1$$

and

$$(i-j) \bmod M \geq N \quad \Longrightarrow \quad N-j+i \bmod \frac{M}{t} \leq N-1.$$

Given the mutual independence of the random variables d_i and e_i for $0 \leq i \leq N-1$, we can derive the expression for the variance of p_i:

$$\sigma(p_i)^2 = \sum_{j \in A_i} \sigma(d_j)^2 \left(\sigma(e_{i-j})^2 + \sigma(e_{N-j+i \bmod \frac{M}{p}})^2\right) + \sum_{j \in B_i} \sigma(d_j)^2 \sigma(e_{N-j+i \bmod \frac{M}{t}})^2 + \sum_{j \in C_i} \sigma(d_j)^2 \sigma(e_{i-j})^2.$$

(Note that $i-j \bmod M \neq N-j+i \bmod \frac{M}{t}) for (0 \leq j \leq N-1.)$ We can easily determine the sets:

$$A_i = \left\{ j \text{ such that } 1+i \bmod \frac{M}{t} \leq j \leq i \text{ or } M-N+i+1 \leq j \leq N-1 \right\},$$
$$B_i = \left\{ j \text{ such that } i+1 \leq j \leq \min(N-1, M-N+i) \right\},$$
$$C_i = \left\{ j \text{ such that } 0 \leq j \leq i \bmod \frac{M}{t} \right\}.$$

From this, we derive the sizes:

$$|A_i| = i - (i \bmod \frac{M}{t}) + \max(2N-M-i-1, 0),$$
$$|B_i| = \min(N-1, M-N+i) - i,$$
$$|C_i| = 1 + (i \bmod \frac{M}{t}).$$

Now, taking into account $\sigma(d_i) = \sigma(D)$ and $\sigma(e_i) = \sigma(E)$, we obtain:

$$\sigma(p_i)^2 = (2|A_i| + |B_i| + |C_i|)\, \sigma(D)^2 \sigma(E)^2.$$

Finally noting that $|A_i| + |B_i| + |C_i| = N$, we conclude with the result of the lemma.

Remark 8.9 *In the case where $t = 2$, we can verify that:*

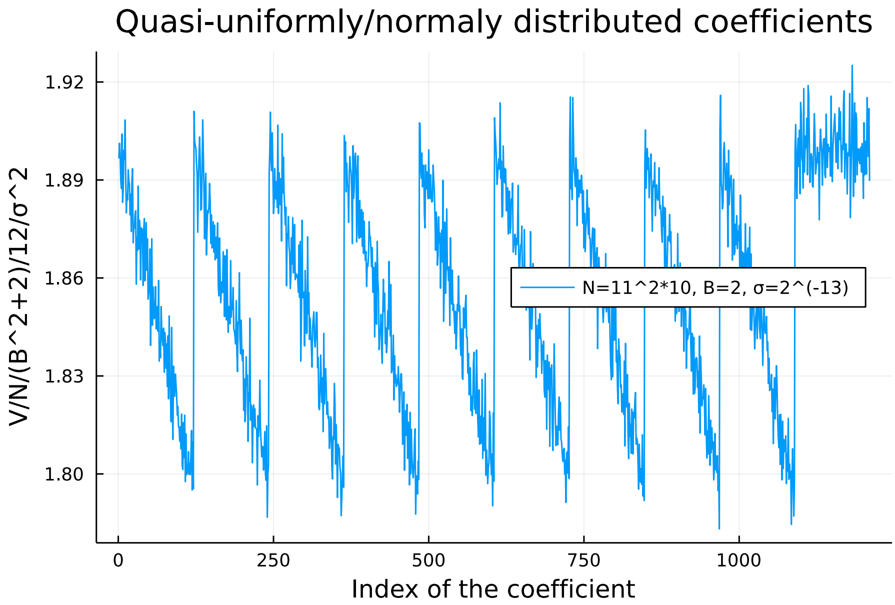
$$A_i = \emptyset, \quad |B_i| = N-1-i \quad \textit{and} \quad |C_i| = i+1.$$

This observation aligns with the expressions derived under the more standard condition $t = 2$.

Remark 8.10 *We may seek an index that exhibits minimal variance. Such an index could be particularly beneficial in extraction operations, as it would help to minimize the error associated with the extracted ciphertext. We have*

$$\sigma((DP)_i)^2 = \sigma(D)^2 \sigma(E)^2 \times \begin{cases} \frac{2t-3}{t-1} N - i \bmod \frac{M}{t} - 1, & if \quad i \leq (t-2)\frac{M}{t} - 1, \\ \dfrac{2t-3}{t-1} N, & if \quad i \geq (t-2)\dfrac{M}{t}. \end{cases}$$

The coefficient zero yields a factor $\frac{2t-3}{t-1}N - 1$ while the coefficient $i = \frac{M}{t} - 1$ yields a smaller factor $\frac{2t-4}{t-1}N$. In Figure 3, we illustrate this behavior through a numerical experiment. We *consider the product of a polynomial D with coefficients sampled from a quasi-uniform distribution over the interval $[-B/2, B/2] \cap \mathbb{Z}$, and another polynomial with Gaussian coefficients possessing a standard deviation of σ. Both polynomials are of degree $N-1$. The results clearly show in the figure that the variance exhibits a periodic pattern, with a period of M/t, up until the index $(t-2)\frac{M}{t}$, beyond which the variance remains nearly constant. For this experiment, we set $M = 11^3$ and $N = 1210$, with around 10^5 samples taken.*



[

Figure 3: Behavior of the variances after a product of two polynomials

References

[1] J.-C. Bajard, T. Gouget, B. Laigle, and M. Naya-Plasencia, *RNS Variant of FV-like Schemes*, in *Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT)*, 2017, pp. 1596–1600. IEEE.

[2] J-F. Biasse and L. Ruiz, *FHEW with efficient multibit bootstrapping.* In Progress in Cryptology - LATINCRYPT 2015 (Lecture Notes in Computer Science, Vol. 9230), K. Lauter and F. RodrÃ̃guez-HenrÃ̃quez (Eds.). Springer, 119-135. `https://doi.org/10.1007/978-3-319-22174-8_7`

[3] C. Bootland, W. Castryck, and F. Vercauteren, *On the Security of the Multivariate Ring Learning with Errors Problem*, in Proceedings of the 2020 ACM Conference on Computer and Communications Security (CCS), 2020, pp. 1237–1253. ACM.

[4] J.-P. Bossuat, A. Costache, C. Mouchet, L. Nürnberger, and J.R. Troncoso-Pastoriza, *Practical q-IND-CPA-D-Secure Approximate Homomorphic Encryption*, Cryptology ePrint Archive, Paper 2024/853, 2024.

[5] J. H. Cheon, A. Kim, and Y. Song, *A Simple, Efficient Bootstrapping Method for Fully Homomorphic Encryption over the Integers*, Cryptology ePrint Archive, 2021. https://eprint.iacr.org/2021/180

[6] P. Chartier, M. Koskas, M. Lemou, and F. Méhats, *Homomorphic Sign Evaluation with a RNS Representation of Integers*, *Advances in Cryptology-ASIACRYPT 2024*, Chung, K.M., Sasaki, Y. (eds.), Lecture Notes in Computer Science, vol. 15484, Springer, Singapore, 2025. https://doi.org/10.1007/978-981-96-0875-1_9.

[7] P. Chartier, M. Koskas, M. Lemou, and F. Méhats, *Fully Homomorphic Encryption on Large Integers*, Cryptology ePrint Archive, 2024.

[8] P. Chartier, M. Koskas, M. Lemou, and F. Méhats, *Method for Homomorphically Determining the Sign of a Message by Dilation, Associated Methods and Devices*, Patent no. WO2023242429 - 12/21/2023. Number and date of priority: FR2205957 - 06/17/2022.

[9] P. Chartier, M. Koskas, M. Lemou, and F. Méhats, *Homomorphic Encryption Method and Associated Devices and System*, Patent no. WO2022129979 - 06/23/2022. Number and date of priority: PCT/IB2020001147 - 12/18/2020.

[10] H. Chen, W. Dai, M. Kim, and Y. Song, *Efficient Homomorphic Conversion Between (Ring) LWE Ciphertexts*, In: K. Sako and N. O. Tippenhauer (eds), Applied Cryptography and Network Security, ACNS 2021, Lecture Notes in Computer Science, vol. 12726, Springer, Cham.

[11] H. Chen, K. Lauter, and K. E. Stange, *Security Considerations for Galois Non-Dual RLWE Families*, Cryptology ePrint Archive, 2021. https://eprint.iacr.org/2021/1620

[12] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, *Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds*, Advances in Cryptology – ASIACRYPT 2016, pp. 3–33. Berlin, Heidelberg, Springer, 2016.

[13] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, *TFHE: Fast Fully Homomorphic Encryption over the Torus*, Journal of Cryptology, 33(1), pp. 34–91, 2020.

[14] A. Costache, B. R. Curtis, E. Hales, S. Murphy, T. Ogilvie, and R. Player, *On the Precision Loss in Approximate Homomorphic Encryption*, Cryptology ePrint Archive, Report 2022/162, 2022.

[15] A. Costache and N. P. Smart, *Ring-LWE and its Applications to Lattice-Based Cryptography*, in *Proceedings of the 2016 IEEE International Conference on Advanced Information Networking and Applications (AINA)*, 2016, pp. 163–170.

[16] E. Crockett and C. Peikert, *Challenges for Ring-LWE*, in *Proceedings of the 2017 IEEE International Conference on the Theory and Application of Cryptography Technology (ACT)*, 2017, pp. 125–130. IEEE.

[17] G. De Micheli, D. Kim, D. Micciancio, and A. Suhl, *Faster Amortized FHEW Bootstrapping Using Ring Automorphisms*, Cryptology ePrint Archive, Paper 2023/112, 2023. https://eprint.iacr.org/2023/112

[18] L. Ducas and D. Micciancio, *FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second*, Advances in Cryptology – EUROCRYPT 2015, pp. 617–640. Berlin, Heidelberg, Springer, 2015.

[19] C. Gentry, *Fully Homomorphic Encryption Using Ideal Lattices*, 41st Annual ACM Symposium on Theory of Computing, pp. 169–178. ACM Press, 2009.

[20] R. Geelen and F. Vercauteren, *Fully Homomorphic Encryption for Cyclotomic Prime Moduli*, Cryptology ePrint Archive, Paper 2024/1587, 2024. `https://eprint.iacr.org/2024/1587`

[21] M. Joye, *SoK: Fully homomorphic encryption over the [discretized] torus PDF*, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022(4):661-692, 2022

[22] M. Joye, M. Walter, *Liberating TFHE: Programmable Bootstrapping with General Quotient Polynomials*, WAHC'22: Proceedings of the 10th Workshop on Encrypted Computing & Applied Homomorphic Cryptography Pages 1 - 11 `https://doi.org/10.1145/3560827.3563376`

[23] A. Kim, J. H. Cheon, and Y. Song, *A Simple, Efficient Bootstrapping Method for Fully Homomorphic Encryption over the Integers*, in Proceedings of the 2020 ACM Conference on Computer and Communications Security (CCS), 2020, pp. 123–145. ACM.

[24] E. Lee, J.-W. Lee, J.-S. No, and Y.-S. Kim, *Minimax Approximation of Sign Function by Composite Polynomial for Homomorphic Comparison*, IEEE Transactions on Dependable and Secure Computing, 2021.

[25] E. Lee, J.-W. Lee, Y.-S. Kim, and J.-S. No, *Optimization of Homomorphic Comparison Algorithm on RNS-CKKS Scheme*, IEEE Access, 10, pp. 26163-26176, 2022.

[26] Y. Lee, D. Micciancio, A. Kim, R. Choi, M. Deryabin, J. Eom, and D. Yoo, *Efficient FHEW Bootstrapping with Small Evaluation Keys, and Applications to Threshold Homomorphic Encryption*, Advances in Cryptology – EUROCRYPT 2023.

[27] D. Micciancio and Y. Polyakov, *Bootstrapping in FHEW-like Cryptosystems*, Association for Computing Machinery, New York, NY, USA, pp. 17–28, 2021.

[28] D. Micciancio and J. Sorrell, *Ring Packing and Amortized FHEW Bootstrapping*, Cryptology ePrint Archive, Paper 2018/532, 2018.

[29] O. Regev, "Learning with Errors," in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 84–93, 2005, ACM. DOI: 10.1145/1060590.1060608.

[30] O. Regev, "On LWE and RLWE," in *Proceedings of the 2010 5th Theory of Cryptography Conference (TCC)*, vol. 5978, pp. 1–20, 2009.

[31] O. Regev, *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography*, Journal of the ACM (JACM), 56(6), pp. 1–40, 2009.

[32] R. Schwerdt, L. Benz, W. Beskorovajnov, S. Eilebrecht, J. Müller-Quade, and A. Ottenhues, *Sender-binding Key Encapsulation*, Cryptology ePrint Archive, Paper 2023/127, 2023.

[33] M. Wang and F. Zhang, *On the Construction of Lattice-Based Fully Homomorphic Encryption Scheme with Prime Power Cyclotomic Polynomials*, International Journal of Information Security, 17(5), pp. 547–560, 2018. https://doi.org/10.1007/s10207-018-0437-1