Subring Homomorphic Encryption

Seiko Arita and Sari Handa

Graduate School of Information Security,
Institute of Information Security, Japan
arita@iisec.ac.jp, dgs158101@iisec.ac.jp

Abstract. In this paper, we construct *subring homomorphic encryption* scheme that is a homomorphic encryption scheme built on the decomposition ring, which is a subring of cyclotomic ring. In the scheme, each plaintext slot contains an integer in $\mathbb{Z}_{p^l}$, rather than an element of $\mathrm{GF}(p^d)$ as in conventional homomorphic encryption schemes on cyclotomic rings. Our benchmark results indicate that the subring homomorphic encryption scheme is several times faster than HElib *for mod-p^l integer plaintexts*, due to its high parallelism of mod-p^l integer slot structure. We believe in that such plaintext structure composed of mod-p^l integer slots will be more natural, easy to handle, and significantly more efficient for many applications such as outsourced data mining, than conventional $\mathrm{GF}(p^d)$ slots.
Keywords: Fully homomorphic encryption, Ring-LWE, Cyclotomic ring, Decomposition ring, Plaintext slots.

1 Introduction

Background. Homomorphic encryption (HE) scheme enables us computation on encrypted data. One can add or multiply (or more generally "evaluate") given ciphertexts and generate a new ciphertext that encrypts the sum or product (or "evaluation") of underlying data of the input ciphertexts. Such computation (called *homomorphic* addition or multiplication or evaluation) can be done without using the secret key and one will never know anything about the processed or generated data.

Since the breakthrough construction given by Gentry [7], many efforts are dedicated to make such homomorphic encryption scheme more secure and more efficient. Especially, HE schemes based on the Ring-LWE problem [15, 4, 6, 16] have obtained theoretically-sound proof of security and well-established implementations such as HElib [10] and SEAL v2.0 [14]. Nowadays many researchers apply HE schemes to privacy-preserving tasks for mining of outsourced data such as genomic data, medical data, financial data and so on [9, 12, 5, 11, 13].

Our perspective: $\mathrm{GF}(p^d)$ *versus* $\mathbb{Z}_{p^l}$ *slots.* The HE schemes based on the Ring-LWE problem (*Ring-HE schemes* in short), depend on arithmetic of cyclotomic integers [15]. Cyclotomic integers a are algebraic integers generated by some primitive m-th root of unity ζ and have the form like $a = a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1}$ where a_i are ordinary integers in $\mathbb{Z}$ and $n = \phi(m)$.

Generally, plaintexts in the Ring-HE schemes are encoded by cyclotomic integers modulo some *small prime* p. (Here, taking modulo p of cyclotomic integers a means taking modulo p of each coefficient a_i.) Then, what type of algebraic structure will a cyclotomic integer a mod p have? Its structure is known to be a tuple of elements of Galois field $\mathrm{GF}(p^d)$ of some degree d. For small primes p, this degree $d\,(> \log_p(m))$ will be large. Thus, in the Ring-HE schemes, a plaintext is a tuple of *plaintext slots* and each plaintext slot represents an element of Galois field $\mathrm{GF}(p^d)$ of large degree d [17]. Addition or multiplication of plaintexts actually means addition or multiplication of each plaintext slots as elements of Galois field $\mathrm{GF}(p^d)$.

Such plaintext structure is good for applications that use data represented by elements of Galois field $\mathrm{GF}(p^d)$, such as error correcting codes or AES ciphers. However, many applications will use integers modulo p^l (i.e., elements in $\mathbb{Z}_{p^l}$) for some positive integer l (and especially for $p = 2$), rather than elements of Galois field $\mathrm{GF}(p^d)$. By using the Hensel lifting technique, Ring-HE schemes can have plaintext slots of integers modulo p^l (as some applications do in fact) but with expense of efficiency. If we want to encrypt mod-p^l integer plaintexts on slots using Ring-HE schemes, actually we can use only 1-dimensional constant polynomials in each d-dimensional slots for homomorphic evaluation. As stated earlier, the dimension d would not be small [1].

In this paper, we propose a novel HE scheme in which plaintext structure is inherently a tuple of integers modulo p^l (for some positive integer l), that is, each plaintext slot contains an integer in $\mathbb{Z}_{p^l}$, rather than an element of $\mathrm{GF}(p^d)$. We believe in that such plaintext structure will be more natural, easy to handle, and significantly efficient for many applications such as outsourced data mining.

Method. To realize plaintext structure composed of slots of mod-p^l integers, we use decomposition ring R_Z with respect to the prime p, instead of cyclotomic ring R.

Let ζ be a primitive m-th root of unity. The m-th cyclotomic ring $R = \{a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} \mid a_i \in \mathbb{Z}\}$ is a ring of all cyclotomic integers generated by ζ, where $n = \phi(m)$ is the value of Euler function at m. Plaintext space of Ring-HE schemes will be the space of mod-p cyclotomic integers, i.e., $R_p = R/pR$ for some small prime p. It is known that in the cyclotomic ring R, the prime number p is not prime any more (in general) and it factors into a product of g prime ideals $\mathfrak{P}_i$ (with some divisor g of n): $pR = \mathfrak{P}_0\mathfrak{P}_1\cdots\mathfrak{P}_{g-1}$. The residual fields $R/\mathfrak{P}_i$ of each factor $\mathfrak{P}_i$ are nothing but the space of plaintext slots of Ring-HE schemes, which are isomorphic to $\mathrm{GF}(p^d)$ with $d = n/g$. Thus, the

[1] For instance, Lu, Kawasaki and Sakuma [13] uses the HElib with parameters $n = m - 1 = 27892$ and $p \approx 2^{36}$ to perform homomorphic computation needed for their statistical analysis on encrypted data in 110-bit security, that results in the plaintext space composed of $l \approx 70$ tuples of the Galois field $\mathrm{GF}(p^d)$ of the degree $d = n/l \approx 398$. They are enforced to use only constant polynomials in those Galois fields.

plaintext space is

$$R_p \;\simeq\; R/\mathfrak{P}_0 \oplus \cdots \oplus R/\mathfrak{P}_{g-1} \;\simeq\; \mathrm{GF}(p^d) \oplus \cdots \oplus \mathrm{GF}(p^d).$$

As stated before, we can use only 1-dimensional subspace $\mathrm{GF}(p) = \mathbb{Z}_p$ in each d-dimensional slot $\mathrm{GF}(p^d)$ for homomorphic evaluation as mod-p integers.

The decomposition ring R_Z with respect to prime p is the minimum subring of R in which the prime p has the same form of prime ideal factorization as in R , that is,

$$pR_Z = \mathfrak{p}_0\mathfrak{p}_1 \cdots \mathfrak{p}_{g-1} \tag{1}$$

with the same number g of factors. By the minimality of R_Z, the residual fields $R_Z/\mathfrak{p}_i$ of each factor $\mathfrak{p}_i$ must be one-dimensional, that is, isomorphic to $\mathbb{Z}_p$. So the plaintext space on R_Z will be

$$(R_Z)_p \;\simeq\; R_Z/\mathfrak{p}_0 \oplus \cdots \oplus R_Z/\mathfrak{p}_{g-1} \;\simeq\; \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p.$$

Applying the Hensel lifting l times, we get $(R_Z)_q \;\simeq\; \mathbb{Z}_q \oplus \cdots \oplus \mathbb{Z}_q$ for $q = p^l$. Thus, the decomposition ring R_Z realizes plaintext slots of integers modulo $q = p^l$, as desired. Note that now we can use *all of the dimensions* of R_Z as its plaintext slots for mod-p^l integer plaintexts. This high parallelism of slot structure will bring us significantly more efficient SIMD operations for mod-p^l integer plaintexts.

Two bases. The cyclotomic ring R has attractive features that enable efficient implementation of addition/multiplication of and noise handling on their elements. Can we do the similar thing even if we use the decomposition ring R_Z instead of cyclotomic ring R?

The cyclotomic ring R's nice properties are consolidated to the existence of two types of bases [16]:

- The power(ful) basis: Composed of short and nearly orthogonal vectors to each other. Used when rounding rational cyclotomic numbers to their nearest cyclotomic integers.
- The CRT basis: Related to the FFT transformation and multiplication. Vectors of coefficients of given two cyclotomic integers w.r.t. the CRT basis can be multiplied component-wise, resulting a new vector corresponding to the multiplied cyclotomic integer.

We investigate structure of the decomposition ring R_Z, following the way in cyclotomic cases given by Lyubashevsky, Peikert, and Regev [16]. Then, we will give two types of bases of R_Z, called η-basis and ξ-basis in this paper, which can substitute for the power(ful) and CRT bases in cyclotomic cases, respectively. The trace map from R to R_Z enables us to observe structure of R_Z as an image of the cyclotomic ring R, along with some particular phenomenon emerging from flatness of the decomposition ring (the degree $d = 1$). We also study noise growth occurred by algebraic manipulations (especially, by multiplication) of elements in R_Z, following [16].

Construction. Based on the above investigation, we construct our *subring homomorphic encryption scheme* that is an HE scheme over the decomposition ring R_Z, or a realization of the FV scheme [6] over R_Z. The construction is described concretely using the η-basis and ξ-basis above. We show several bounds on the noise growth occurred among homomorphic computations on its ciphertexts and prove that our HE scheme is fully homomorphic using ciphertext modulus of the magnitude $q = O(\lambda^{\log \lambda})$ with security parameter λ, as the FV scheme is so.

For security we will need hardness of a variant of the decisional Ring-LWE problem over the decomposition ring. Recall the search version of Ring-LWE problem is already proved to have a quantum polynomial time reduction from the approximate shortest vector problem of ideal lattices in *any number field* by Lyubashevsky, Peikert, and Regev [15]. They proved equivalence between the search and decisional versions of the Ring-LWE problems only for cyclotomic rings. However, it is not difficult to see that the equivalence holds also over the decomposition rings, since they are subrings of cyclotomic rings and inherit good properties from them.

Implementation and benchmark. We implemented our subring homomorphic encryption scheme using the C++ language and performed several experiments with different parameters. Our benchmark results show that the η-basis and ξ-basis can substitute well for the power(ful) and CRT bases of cyclotomic rings, and indicate that our subring homomorphic encryption scheme is several times faster than HElib *for mod-p^l integer plaintexts*, due to its high parallelism of mod-p^l slot structure.

Organization. In Section 2 we prepare notions and tools needed for our work, especially about cyclotomic rings. Section 3 investigates structure and properties of the decomposition ring, and gives its η-basis and ξ-basis as well as quasi-linear time conversion between them. In Section 4 we state a variant of the Ring-LWE problem over the decomposition ring and construct our subring homomorphic encryption scheme over the decomposition ring. Finally, Section 5 shows our benchmark results, comparing efficiency of our implementation of subring homomorphic encryption scheme and HElib. Proofs of lemmas or theorems are collected in the appendices.

2 Preliminaries

Notation. For a positive integer m, $\mathbb{Z}_m$ denotes the ring of congruent integers mod m, and $\mathbb{Z}_m^*$ denotes its multiplicative subgroup. For an integer a (that is prime to m), $\mathrm{ord}_m^{\times}(a)$ denotes the order of $a \in \mathbb{Z}_m^*$. Basically vectors are supposed to represent column vectors. The symbol $\mathbf{1}$ denotes a column vector with all entries equal to 1. I_n denotes the $n \times n$ identity matrix. The symbol $\mathrm{Diag}(\alpha_1, \cdots, \alpha_n)$ means a diagonal matrix with diagonals $\alpha_1, \ldots, \alpha_n$. For vectors $\boldsymbol{x}, \boldsymbol{y}$ $(\in \mathbb{C}^n)$, $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{i=1}^{n} x_i \overline{y}_i$ denotes the inner product of $\boldsymbol{x}$ and $\boldsymbol{y}$. $\|\boldsymbol{x}\|_2 = \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}$ denotes the l_2-norm of vector $\boldsymbol{x}$ and $\|\boldsymbol{x}\|_\infty = \max_{i=1}^{n}\{|x_i|\}$ denotes the infinity norm of $\boldsymbol{x}$. For vectors $\boldsymbol{a}$ and $\boldsymbol{b}$, $\boldsymbol{a} \odot \boldsymbol{b} = (a_i b_i)_i$ denotes the component-wise product of $\boldsymbol{a}$ and $\boldsymbol{b}$. For a square matrix M over $\mathbb{R}$, $s_1(M)$ denotes the largest singular value of M. For a matrix A over $\mathbb{C}$, $A^* = \overline{A}^T$ denotes the transpose of complex conjugate of A.

2.1 Homomorphic encryption scheme

A homomorphic encryption scheme is a quadruple HE=(Gen, Encrypt, Decrypt, Evaluate) of probabilistic polynomial time algorithms. Gen generates a public key pk, a secret key sk and an evaluation key evk: $(\mathsf{pk}, \mathsf{sk}, \mathsf{evk}) \leftarrow \mathsf{Gen}(1^\lambda)$. Encrypt encrypts a plaintext $x \in \mathsf{X}$ to a ciphertext c under a public key pk: $c \leftarrow \mathsf{Encrypt}(\mathsf{pk}, x)$. Decrypt decrypts a ciphertext c to a plaintext x using the secret key sk: $x \leftarrow \mathsf{Decrypt}(\mathsf{sk}, c)$. Evaluate applies a function $f : \mathsf{X}^l \to \mathsf{X}$ (given as an arithmetic circuit) to ciphertexts $c_1, \dots, c_l$ and outputs a new ciphertext c_f using the evaluation key $\mathsf{evk} : c_f \leftarrow \mathsf{Evaluate}(\mathsf{evk}, f, c_1, \dots, c_l)$.

A homomorphic encryption scheme HE is *L-homomorphic* for $L = L(\lambda)$ if for any function $f : \mathsf{X}^l \to \mathsf{X}$ given as an arithmetic circuit of depth L and for any l plaintexts $x_1, \dots, x_l \in \mathsf{X}$, it holds that

$$\mathsf{Decrypt}_{\mathsf{sk}}(\mathsf{Evaluate}_{\mathsf{evk}}(f, c_1, \dots, c_l)) \;=\; f(x_1, \dots, x_l)$$

for $c_i \leftarrow \mathsf{Encrypt}_{\mathsf{pk}}(x_i)$ $(i = 1, \dots, l)$ except with a negligible probability (i.e., $\mathsf{Decrypt}_{\mathsf{sk}}$ is ring homomorphic). A homomorphic encryption scheme is called *fully homomorphic* if it is L-homomorphic for any polynomial function $L = poly(\lambda)$.

2.2 Gaussian distributions and subgaussian random variables

For a positive real $s > 0$, the n-dimensional (spherical) Gaussian function $\rho_s : \mathbb{R}^n \to (0, 1]$ is defined as

$$\rho_s(x) = \exp(-\pi \|x\|_2 / s^2).$$

It defines the continuous Gaussian distribution D_s with density $s^{-n}\rho_s(x)$.

A random variable X over $\mathbb{R}$ is called *subgaussian with parameter s* (> 0) if $\mathbb{E}[\exp(2\pi t X)] \le \exp(\pi s^2 t^2) \quad (\forall t \in \mathbb{R})$. A random variable X over $\mathbb{R}^n$ is called subgaussian with parameter s if $\langle X, u \rangle$ is subgaussian with parameter s for any unit vector $u \in \mathbb{R}^n$. A random variable X according to Gaussian distribution D_s is subgaussian with parameter s. A bounded random variable X (as $|X| \le B$) with $\mathbb{E}[X] = 0$ is subgaussian with parameter $B\sqrt{2\pi}$.

A subgaussian random variable with parameter s satisfies the tail inequality:

$$\Pr[|X| \ge t] \;\le\; 2\exp\Big(-\pi \frac{t^2}{s^2}\Big) \quad (\forall t \ge 0). \tag{2}$$

2.3 Lattices

For n linearly independent vectors $B = \{b_j\}_{j=1}^n \subset \mathbb{R}^n$, $\Lambda = \mathcal{L}(B) = \left\{\sum_{j=1}^n z_j b_j \mid z_j \in \mathbb{Z}\ (\forall j)\right\}$ is called an n-dimensional *lattice*. For a lattice $\Lambda \subset \mathbb{R}^n$, its *dual lattice* is defined by $\Lambda^\vee = \left\{y \in \mathbb{R}^n \mid \langle x, y\rangle \in \mathbb{Z}\ (\forall x \in \Lambda)\right\}$. The dual lattice is itself a lattice. The dual of dual lattice is the same as the original lattice: $(\Lambda^\vee)^\vee = \Lambda$. For a countable subset $A \subset \mathbb{R}^n$, the sum $D_s(A) \stackrel{\text{def}}{=} \sum_{x\in A} D_s(x)$ is well-defined. The discrete Gaussian distribution $D_{\Lambda+c,s}$ on a (coset of) lattice Λ is defined by restricting the continuous Gaussian distribution D_s on the (coset of) lattice Λ:

$$D_{\Lambda+c,s}(x) \stackrel{\text{def}}{=} \frac{D_s(x)}{D_s(\Lambda+c)} \quad (x \in \Lambda + c).$$

2.4 Number Fields

A complex number $\alpha \in \mathbb{C}$ is called an *algebraic number* if it satisfies $f(\alpha) = 0$ for some nonzero polynomial $f(X) \in \mathbb{Q}[X]$ over $\mathbb{Q}$. For an algebraic number α, the monic and irreducible polynomial $f(X)$ satisfying $f(\alpha) = 0$ is uniquely determined and called the *minimum polynomial* of α. An algebraic number α generates a *number field* $K = \mathbb{Q}(\alpha)$ over $\mathbb{Q}$, which is isomorphic to $\mathbb{Q}[X]/(f(X))$, via $g(\alpha) \mapsto g(X)$. The dimension of K as a $\mathbb{Q}$-vector space is called the *degree* of K and denoted as $[K : \mathbb{Q}]$. By the isomorphism, $[K : \mathbb{Q}] = \deg f$.

An algebraic number α is called an *algebraic integer* if its minimum polynomial belongs to $\mathbb{Z}[X]$. All algebraic integers belonging to a number field $K = \mathbb{Q}(\alpha)$ constitutes a ring R, called an *integer ring* of K.

A number field $K = \mathbb{Q}(\alpha)$ has $n\,(= [K : \mathbb{Q}])$ isomorphisms ρ_i $(i = 1, \ldots, n)$ into the complex number field $\mathbb{C}$. The trace map $\mathrm{Tr}_{K|\mathbb{Q}} : K \to \mathbb{Q}$ is defined by $\mathrm{Tr}_{K|\mathbb{Q}}(a) = \sum_{i=1}^n \rho_i(a)$ $(\in \mathbb{Q})$. If all of the isomorphisms ρ_i induce automorphisms of K (i.e., $\rho_i(K) = K$ for any i), the field K is called a *Galois extension* of $\mathbb{Q}$ and the set of isomorphisms $\mathrm{Gal}(K|\mathbb{Q}) \stackrel{\text{def}}{=} \{\rho_1, \ldots, \rho_n\}$ constitutes a group, called the *Galois group* of K over $\mathbb{Q}$. By the Galois theory, all subfields L of K and all subgroups H of $G = \mathrm{Gal}(K|\mathbb{Q})$ corresponds to each other one-to-one:

$$\begin{aligned} L &\mapsto H = G_L = \{\rho \in G \mid \rho(a) = a \text{ for any } a \in L\} \\ &\qquad : \text{the stabilizer group of } L \\ H &\mapsto L = K^H = \{a \in K \mid \rho(a) = a \text{ for any } \rho \in H\} \\ &\qquad : \text{the fixed field by } H. \end{aligned}$$

Here, K is also a Galois extension of L with Galois group $\mathrm{Gal}(K|L) = H$ (since any isomorphism (of K into $\mathbb{C}$) that fixes L sends K to K). Especially, $[K : L] = |H|$. The trace map of K over L is defined by $\mathrm{Tr}_{K|L}(a) = \sum_{\rho\in H} \rho(a)$ $(\in L)$ for $a \in K$.

2.5 Cyclotomic Fields and Rings

Let m be a positive integer. A primitive m-th root of unity $\zeta = \exp(2\pi\sqrt{-1}/m)$ has the minimum polynomial $\Phi_m(X) \in \mathbb{Z}[X]$ of degree $n = \phi(m)$ that belongs to $\mathbb{Z}[X]$, called the *cyclotomic polynomial*. Especially, ζ is an algebraic integer. A number field $K = \mathbb{Q}(\zeta)$ generated by ζ is called the m-th *cyclotomic field* and its elements are called *cyclotomic numbers*. The integer ring R of the cyclotomic field $K = \mathbb{Q}(\zeta)$ is known to be $R = \mathbb{Z}[\zeta] = \mathbb{Z}[X]/\Phi_m(X)$. In particular, as a $\mathbb{Z}$-module, R has a basis (called *power basis*) $\{1, \zeta, \ldots, \zeta^{n-1}\}$, i.e., $R = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \zeta + \cdots + \mathbb{Z} \cdot \zeta^{n-1}$. The integer ring R is called the m-th *cyclotomic ring* and its elements are called *cyclotomic integers*. For a positive integer q, $R_q = R/qR = \mathbb{Z}_q[X]/\Phi_m(X)$ is a ring of *cyclotomic integers mod* q.

The cyclotomic field $K = \mathbb{Q}(\zeta)$ is a Galois extension over $\mathbb{Q}$ since it has $n = [K : Q]$ automorphisms ρ_i defined by $\rho_i(\zeta) = \zeta^i$ for $i \in \mathbb{Z}_m^*$. Its Galois group $G = \mathrm{Gal}(K|\mathbb{Q})$ is isomorphic to $\mathbb{Z}_m^*$ by corresponding ρ_i to i. Note that $\rho_i(\overline{b}) = \overline{\rho_i(b)}$, since $\overline{a} = \rho_{-1}(a)$.

The trace of ζ for the prime index m is simple:

Lemma 1. *If the index m is prime, we have*

$$\mathrm{Tr}_{K|\mathbb{Q}}(\zeta^i) = \begin{cases} m-1 & (i \equiv 0 \pmod{m}) \\ -1 & (i \not\equiv 0 \pmod{m}). \end{cases}$$

Structure of R_p Let p be a prime that does not divide m. Although the cyclotomic polynomial $\Phi_m(X)$ is irreducible over $\mathbb{Z}$, by taking mod p, it will be factored into a product of several polynomials $F_i(X)$'s:

$$\Phi_m(X) \equiv F_0(X) \cdots F_{g-1}(X) \pmod{p}, \tag{3}$$

where all of $F_i(X)$ are irreducible mod p, and have the same degree $d = \mathrm{ord}_m^{\times}(p)$ which is a divisor of n. The number of factors is equal to $g = n/d$.

It is known that there are g prime ideals $\mathfrak{P}_0, \ldots, \mathfrak{P}_{g-1}$ of R lying over p : $\mathfrak{P}_i \cap \mathbb{Z} = p\mathbb{Z}$ $(i = 0, \ldots, g-1)$ and p decomposes into a product of those prime ideals in R:

$$pR = \mathfrak{P}_0 \cdots \mathfrak{P}_{g-1}. \tag{4}$$

This decomposition of the prime p reflects the factorization of $\Phi_m(X)$ mod p (Eq (3)). In fact, each prime factor $\mathfrak{P}_i$ is generated by p and $F_i(\zeta)$ as ideals of R, $\mathfrak{P}_i = (p, F_i(\zeta))$ for $i = 0, \ldots, g-1$. The corresponding residual fields are given by

$$R/\mathfrak{P}_i \;\simeq\; \mathbb{Z}_p[X]/F_i(X) \;\simeq\; \mathrm{GF}(p^d)$$

for $i = 0, \ldots, g-1$. Thus, we have

$$R_p \;\simeq\; R/\mathfrak{P}_0 \oplus \cdots \oplus R/\mathfrak{P}_{g-1} \;\simeq\; \mathrm{GF}(p^d) \oplus \cdots \oplus \mathrm{GF}(p^d).$$

In the Ring-HE schemes such as [3, 4, 6], plaintexts are encoded by cyclotomic integers $x \in R_p$ modulo some *small prime* $p\,(\nmid m)$. By the factorization of R_p above, g plaintexts $x_0, \ldots, x_{g-1}$ belonging to $\mathrm{GF}(p^d)$ are encoded into a single cyclotomic integer $x \in R_p$. The place of each plaintext $x_i \in \mathrm{GF}(p^d)$ is called a *plaintext slot*. Thus, in the Ring-HE schemes, one can encrypt g plaintexts into a single ciphertext by setting them on corresponding plaintext slots and can evaluate or decrypt the g encrypted plaintexts at the same time using arithmetic of cyclotomic integers [17]. Gentry, Halevi, and Smart [8] homomorphically evaluates AES circuit on HE-encrypted AES-ciphertexts in the SIMD manner, using such plaintext slot structure for $p = 2$, which fits to the underlying $\mathrm{GF}(2^d)$-arithmetic of the AES cipher.

Geometry of numbers Using the n automorphisms $\rho_i\,(i \in \mathbb{Z}_m^*)$, the cyclotomic field K is embedded into an n-dimensional complex vector space $\mathbb{C}^{\mathbb{Z}_m^*}$, called the *canonical embedding* $\sigma : K \to H\,(\subset \mathbb{C}^{\mathbb{Z}_m^*})$: $\sigma(a) = (\rho_i(a))_{i \in \mathbb{Z}_m^*}$. Its image $\sigma(K)$ is contained in the space H defined as

$$H \overset{\mathrm{def}}{=} \{x \in \mathbb{C}^{\mathbb{Z}_m^*} : x_i = \overline{x}_{m-i} \quad (\forall i \in \mathbb{Z}_m^*)\}.$$

Since $H = B\mathbb{R}^n$ with the unitary matrix $B = \frac{1}{\sqrt{2}}\begin{pmatrix} I & \sqrt{-1}J \\ J & -\sqrt{-1}I \end{pmatrix}$, the space H is isomorphic to $\mathbb{R}^n$ as an inner product $\mathbb{R}$-space (where J is the reversal matrix of the identity matrix I).

By the canonical embedding σ, one can regard R (or its (fractional) ideals of R) as lattices in the n-dimensional real vector space H, called *ideal lattices*. Inner products or norms of elements $a \in K$ are defined through the embedding σ:

$$\langle a, b\rangle \overset{\mathrm{def}}{=} \langle \sigma(a), \sigma(b)\rangle = \mathrm{Tr}_{K|\mathbb{Q}}(a\bar{b}), \quad \|a\|_2 \overset{\mathrm{def}}{=} \|\sigma(a)\|_2, \ \|a\|_\infty \overset{\mathrm{def}}{=} \|\sigma(a)\|_\infty.$$

3 Decomposition Rings and Their Properties

To realize plaintext structure composed of slots of mod-p^l integers for some small prime p, we use decomposition rings R_Z w.r.t. p instead of cyclotomic rings R.

3.1 Decomposition Field

Let $G = \mathrm{Gal}(K|\mathbb{Q})$ be the Galois group of the m-th cyclotomic field $K = \mathbb{Q}(\zeta)$ over $\mathbb{Q}$. Let p be a prime that does not divide m. Recall such p has the prime ideal decomposition of Eq (4). The *decomposition group* G_Z of K w.r.t. p is the subgroup of G defined as

$$G_Z \overset{\mathrm{def}}{=} \{\rho \in G \mid \mathfrak{P}_i^\rho = \mathfrak{P}_i \ \ (i = 0, \ldots, g-1)\}.$$

That is, G_Z is the subgroup of automorphisms ρ of K that stabilize each prime ideal $\mathfrak{P}_i$ lying over p. Recall the Galois group $G = \mathrm{Gal}(K|\mathbb{Q})$ is isomorphic to $\mathbb{Z}_m^*$

via ρ^{-1}. Since p does not divide m, $p \in \mathbb{Z}_m^*$. It is known that the decomposition group G_Z is generated by the automorphism ρ_p corresponding to the prime p, called the Frobenius map w.r.t. p: $G_Z = \langle \rho_p \rangle \simeq \langle p \rangle \subseteq \mathbb{Z}_m^*$. The order of G_Z is equal to $d = \mathrm{ord}_m^{\times}(p)$. The fixed field $Z = K^{G_Z}$ by G_Z is called the *decomposition field* of K (w.r.t. p). The decomposition field Z can be characterized as the smallest subfield Z of K such that $\mathfrak{P}_i \cap Z$ does not split in K, so that the prime p factorizes into prime ideals in Z in much the same way as in K. By the Galois theory, $G_Z = \mathrm{Gal}(K|Z)$. For degrees, we have $[K : Z] = |G_Z| = d$, $[Z : \mathbb{Q}] = n/d = g$. The decomposition field Z is itself the Galois extension of $\mathbb{Q}$ and its Galois group $\mathrm{Gal}(Z|\mathbb{Q}) = G/G_Z$ is given by $\mathrm{Gal}(Z|\mathbb{Q}) \simeq \mathbb{Z}_m^*/\langle p \rangle$.

3.2 Decomposition Ring

The integer ring $R_Z = R \cap Z$ of the decomposition field Z is called the *decomposition ring*. Primes ideals over p in the decomposition ring R_Z are given by $\mathfrak{p}_i = \mathfrak{P}_i \cap Z$ for $i = 0, \ldots, g-1$, and the prime p factors into the product of those prime ideals in much the same way as in K:

$$pR_Z = \mathfrak{p}_0 \cdots \mathfrak{p}_{g-1}. \tag{5}$$

This leads to the decomposition of $(R_Z)_p$: $(R_Z)_p \simeq R_Z/\mathfrak{p}_0 \oplus \cdots \oplus R_Z/\mathfrak{p}_{g-1}$.

For each prime ideal $\mathfrak{P}_i$ (of R) lying over $\mathfrak{p}_i$, the Frobenius map ρ_p acts as the p-th power automorphism $\mathrm{pow}_p(x) = x^p$ on $R/\mathfrak{P}_i$:

$$\begin{array}{ccc} R & \longrightarrow & R/\mathfrak{P}_i \\ {\scriptstyle \rho_p}\big\downarrow & & {\scriptstyle \mathrm{pow}_p}\big\downarrow \\ R & \longrightarrow & R/\mathfrak{P}_i \end{array}$$

Then, by definition of $R_Z = R^{\langle \rho_p \rangle}$, any element in $R_Z/\mathfrak{p}_i$ must be fixed by pow_p, which means:

$$R_Z/\mathfrak{p}_i = (R/\mathfrak{P}_i)^{\langle \mathrm{pow}_p \rangle} = \mathbb{Z}_p.$$

Thus, we see that all slots of $(R_Z)_p$ must be one-dimensional: $(R_Z)_p \simeq \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$.

By applying the Hensel lifting (w.r.t. p) l times to the situation, we get

$$qR_Z = \mathfrak{q}_0 \cdots \mathfrak{q}_{g-1} \tag{6}$$

$$(R_Z)_q \simeq \mathbb{Z}_q \oplus \cdots \oplus \mathbb{Z}_q \tag{7}$$

for $q = p^l$ with any positive integer l. This structure of the decomposition ring $(R_Z)_q$ brings us the plaintext structure of our subring homomorphic encryption scheme, being composed of g mod-q integer slots.

3.3 Bases of the decomposition ring R_Z

To construct homomorphic encryption schemes using some ring R, we will need two types of bases of the ring R over $\mathbb{Z}$, one for decoding elements in $R \otimes \mathbb{R}$ into its nearest element in R, and another one that enables FFT-like fast computations among elements in R. In addition, we also need some quasi-linear time transformations among vector representations with respect to the two types of bases. Here, *assuming the index m of cyclotomic ring R is prime*, we construct such two types of bases for the decomposition ring R_Z, following the cyclotomic ring case given by Lyubashevsky, Peikert and Regev [16].

The $\boldsymbol{\eta}$-basis Let m be a prime and $K = \mathbb{Q}(\zeta)$ be the m-th cyclotomic field. For a prime $p\,(\neq m)$, let Z be the decomposition field of K with respect to p.

Fix any set of representatives $\{t_0, \ldots, t_{g-1}\}$ of $\mathbb{Z}_m^*/\langle p\rangle \simeq \mathrm{Gal}(Z|\mathbb{Q})$. For $i = 0, \ldots, g-1$, define

$$\eta_i \stackrel{\mathrm{def}}{=} \mathrm{Tr}_{K|Z}(\zeta^{t_i}) = \sum_{a\in\langle p\rangle} \zeta^{t_i a} \ \ (\in R_Z).$$

Lemma 2. *For $i = 0, \ldots, g-1$, we have* $\mathrm{Tr}_{Z|\mathbb{Q}}(\eta_i) = \sum_{i=0}^{g-1} \eta_i = -1$, $\mathrm{Tr}_{Z|\mathbb{Q}}(\overline{\eta}_i) = \sum_{i=0}^{g-1} \overline{\eta}_i = -1$.

Lemma 3. *For the prime index m, the set $\{\eta_0, \ldots, \eta_{g-1}\}$ is a basis of the decomposition ring R_Z (w.r.t. $p\,(\neq m)$) over $\mathbb{Z}$, i.e., $R_Z = \mathbb{Z}\eta_0 + \cdots + \mathbb{Z}\eta_{g-1}$.*

Definition 1. *We call the basis $\boldsymbol{\eta} := (\eta_0, \ldots, \eta_{g-1})$* η-basis *of R_Z. For any $a \in R_Z$, there exists unique $\boldsymbol{a} \in \mathbb{Z}^g$ satisfying $a = \boldsymbol{\eta}^T \boldsymbol{a}$. We call such $\boldsymbol{a} \in \mathbb{Z}^g$* η-vector *of $a \in R_Z$.*

The $\boldsymbol{\xi}$-basis By the choice of t_i's, the Galois group $\mathrm{Gal}(Z|\mathbb{Q})$ of Z is given by

$$\mathrm{Gal}(Z|\mathbb{Q}) = \{\rho_{t_0}, \ldots, \rho_{t_{g-1}}\}.$$

Elements $a \in Z$ in the decomposition field are regarded as g-dimensional $\mathbb{R}$-vectors through the canonical embedding $\sigma_Z : Z \to H_Z \,(\subset \mathbb{C}^{\mathbb{Z}_m^*/\langle p\rangle})$ defined as $\sigma_Z(a) = (\rho_i(a))_{i\in\mathbb{Z}_m^*/\langle p\rangle}$. The g-dimensional $\mathbb{R}$-subspace H_Z is as

$$H_Z \stackrel{\mathrm{def}}{=} \{x \in \mathbb{C}^{\mathbb{Z}_m^*/\langle p\rangle} \ : \ x_i = \overline{x}_{m-i} \quad (\forall i \in \mathbb{Z}_m^*/\langle p\rangle)\}.$$

Define a $g \times g$ matrix Ω_Z over R_Z as

$$\Omega_Z = \Big(\rho_{t_i}(\eta_j)\Big)_{0\le i,j<g} \quad (\in R_Z^{g\times g}).$$

Note that each column of Ω_Z is the canonical embedding $\sigma_Z(\eta_j)$ of η_j. Since the index m is prime, the Galois group $\mathrm{Gal}(Z|\mathbb{Q})$ is cyclic and we can take the representatives $\{t_0, \dots, t_{g-1}\}$ so that $t_j \equiv t^j \pmod{\langle p \rangle}$ with some $t \in \mathbb{Z}_m^*$ for $j = 0, \dots, g-1$. Setting $\eta = \mathrm{Tr}_{K|Z}(\zeta)$, for any i and j,

$$\rho_{t_i}(\eta_j) = \rho_{t_i}(\rho_{t_j}(\eta)) = \rho_{t_i \cdot t_j}(\eta) = \rho_{t_{i+j}}(\eta) = \eta_{i+j}.$$

In particular, Ω_Z is symmetric. We can show that:

Lemma 4. $\Omega_Z^* \Omega_Z \;=\; (\mathrm{Tr}_{Z|\mathbb{Q}}(\overline{\eta}_i \eta_j))_{0 \le i,j < g} \;=\; m I_g - d \mathbf{1} \cdot \mathbf{1}^T \;(\in \mathbb{Z}^{g \times g})$.

Corollary 1. *The set* $\{m^{-1}(\eta_0 - d), \cdots, m^{-1}(\eta_{g-1} - d)\}$ *is the dual basis of conjugate* η*-basis* $\{\overline{\eta_0}, \cdots, \overline{\eta_{g-1}}\}$*, i.e. for any* $0 \le i, j < g$*,*

$$\mathrm{Tr}_{Z|\mathbb{Q}}\Big(\frac{\eta_i - d}{m} \cdot \overline{\eta_j}\Big) = \delta_{ij}.$$

In particular, $R_Z^\vee = \mathbb{Z}\frac{\eta_0 - d}{m} + \cdots + \mathbb{Z}\frac{\eta_{g-1} - d}{m}$.

Define a $g \times g$ matrix Γ_Z over Z as

$$\Gamma_Z \stackrel{\text{def}}{=} \Big(\rho_{t_i}\big(\frac{\overline{\eta_j} - d}{m}\big)\Big)_{0 \le i,j < g} \quad (\in Z^{g \times g}).$$

Corollary 1 means that $\overline{\Gamma}_Z^T \overline{\Omega}_Z = I$. Since Ω_Z is symmetric,

$$\Gamma_Z \Omega_Z = \Omega_Z \Gamma_Z = I. \tag{8}$$

Lemma 5. *For any* $\boldsymbol{b} = \Omega_Z \boldsymbol{a}$*, we have*

$$\boldsymbol{a} \;=\; \Gamma_Z \boldsymbol{b} \;=\; \frac{1}{m}\Big(\overline{\Omega}_Z \boldsymbol{b} - d\big(\sum_j b_j\big) \cdot \mathbf{1}\Big).$$

Let r be a positive integer and $q = p^r$. Let $\mathfrak{q} = \mathfrak{q}_0$ be the first ideal that appears in the factorization of qR_Z (Eq (6)). Recall that $R_Z/\mathfrak{q} \;\simeq\; \mathbb{Z}_q$.

Let

$$\Omega_Z^{(q)} \stackrel{\text{def}}{=} \Omega_Z \bmod \mathfrak{q} \;\; (\in (R_Z)_{\mathfrak{q}}^{g \times g} \simeq \mathbb{Z}_q^{g \times g})$$

Since $p \nmid m$, $\Gamma_Z \bmod \mathfrak{q}$ is well-defined and by Eq (8), $\Omega_Z^{(q)}$ is invertible mod $\mathfrak{q}$.

Definition 2. *Define* $\boldsymbol{\xi} = (\xi_0, \dots, \xi_{g-1}) \in (R_Z)_{\mathfrak{q}}^g$ *by* $\boldsymbol{\eta}^T \equiv \boldsymbol{\xi}^T \Omega_Z^{(q)} \pmod{\mathfrak{q}}$*. We call the basis* $\boldsymbol{\xi}$ *of* $(R_Z)_{\mathfrak{q}}$ *over* $\mathbb{Z}_q$ ξ-basis *of* R_Z *(with respect to* $\mathfrak{q}$*). For any* $a \in (R_Z)_{\mathfrak{q}}$*, there exists unique* $\boldsymbol{b} \in \mathbb{Z}_q^g$ *satisfying that* $a = \boldsymbol{\xi}^T \boldsymbol{b}$*. We call such* $\boldsymbol{b} \in \mathbb{Z}_q^g$ *as* ξ-vector *of* $a \in (R_Z)_{\mathfrak{q}}$*.*

Lemma 6. *For any* $a \in R_Z$ *it holds that*

$$a \equiv \boldsymbol{\eta}^T \cdot \boldsymbol{a} \;\Leftrightarrow\; a \equiv \boldsymbol{\xi}^T \cdot (\Omega_Z^{(q)} \cdot \boldsymbol{a}) \pmod{\mathfrak{q}}$$
$$a = \boldsymbol{\eta}^T \cdot \boldsymbol{a} \;\Leftrightarrow\; \sigma_Z(a) = \Omega_Z \boldsymbol{a}$$
$$a \equiv \boldsymbol{\xi}^T \cdot \boldsymbol{b} \pmod{\mathfrak{q}} \;\Leftrightarrow\; \sigma_Z(a) \equiv \boldsymbol{b} \pmod{\mathfrak{q}}$$

Lemma 7. *If* $a_1 = \boldsymbol{\xi}^T \cdot \boldsymbol{b}_1$ *and* $a_2 = \boldsymbol{\xi}^T \cdot \boldsymbol{b}_2$*, then* $a_1 a_2 = \boldsymbol{\xi}^T \cdot (\boldsymbol{b}_1 \odot \boldsymbol{b}_2)$*.*

3.4 Conversion between η- and ξ-vectors

Resolution of unity in R_Z mod $\mathfrak{q}$ By Hensel-lifting the factorization of $\Phi_m(X) \bmod p$ (Eq (3)) to modulus $q = p^r$, we get factorization of $\Phi_m(X) \bmod q$: $\Phi_m(X) \equiv \overline{F}_0(X) \cdots \overline{F}_{g-1}(X) \pmod q$. Here, note that the number g of irreducible factors and the degree d of each factors remain unchanged in the lifting. According to this factorization, the ideal qR of R is factored as $qR = \mathfrak{Q}_0 \cdots \mathfrak{Q}_{g-1}$ with ideals $\mathfrak{Q}_i = (q, \overline{F}_i(\zeta))$ of R.

For each $i = 0, \dots, g-1$, let $G_i(X) \stackrel{\text{def}}{=} \prod_{j \neq i} \overline{F}_j(X) \pmod q$ and $P_i(X) \stackrel{\text{def}}{=} (G_i(X)^{-1} \bmod (q, \overline{F}_i(X))) \cdot G_i(X) \pmod q$. It is verified that the set $\{\tau_i = P_i(\zeta)\}_{i=0}^{g-1}$ constitutes a *resolution of unity* in $R \bmod q$, i.e.

$$\tau_i \equiv \begin{cases} 1 & \pmod{\mathfrak{Q}_i}\ (i = 0, \dots, g-1) \\ 0 & \pmod{\mathfrak{Q}_j}\ (j \neq i) \end{cases}$$

and it satisfies that

$$\sum_{i=0}^{g-1} \tau_i \equiv 1,\ \tau_i^2 \equiv \tau_i,\ \tau_i \tau_j \equiv 0 \pmod q\ (j \neq i).$$

By the Chinese remainder theorem, the resolution of unity $\{\tau_i\}_{i=0}^{g-1}$ is uniquely determined mod qR. In the following we take coefficients of each τ_i from $[-q/2, q/2)$ over the basis $B' = \{\zeta, \zeta^2, \dots, \zeta^{m-1}\}$ of R.

Lemma 8. *For any $0 \le i < g$ it is that $\tau_i \in R_Z$, and $\{\tau_i\}_{i=0}^{g-1}$ is also a resolution of unity in R_Z mod q.*

Using the resolution of unity $\{\tau_i\}_{i=0}^{g-1}$ in R_Z, we can compute $a_i \in \mathbb{Z}_q$ satisfying $a \equiv a_i \pmod{\mathfrak{q}_i}$ given $a \in R_Z$, as follows:

$$a \bmod \mathfrak{q}_i = a\tau_i \bmod q \ = \ a_i \tau_i \bmod q \overset{\text{dividing by } \tau_i}{\mapsto} a_i.$$

Computation of $\boldsymbol{\Omega_Z^{(q)}}$ Now we can compute the matrix $\Omega_Z^{(q)} = \Big(\eta_{i+j} \bmod \mathfrak{q}\Big)_{0 \le i,j < g}$ $(\in \mathbb{Z}_q^{g \times g})$ by computing the entities η_{i+j} in Ω_Z as cyclotomic integers and reducing them modulo $\mathfrak{q}\ (= \mathfrak{q}_0)$ using the resolution of unity $\{\tau_i\}_{i=0}^{g-1}$. Since the matrix $\Omega_Z^{(q)}$ has cyclic structure (the $(i+1)$-th row is a left shift of the i-th row), it is sufficient to compute its first row. Here, we remark that once we have computed the matrix $\Omega_Z^{(q)}$, we can totally forget the original structure of cyclotomic ring R, and all we need is doing various computations among η- and ξ-vectors (of elements in R_Z) with necessary conversion between them using the matrix $\Omega_Z^{(q)}$.

Computation of $\boldsymbol{b} = \boldsymbol{\Omega}_{\boldsymbol{Z}}^{(q)} \cdot \boldsymbol{a}$ To convert η-vector $\boldsymbol{a}$ of an element $a = \boldsymbol{\eta}^T \cdot \boldsymbol{a} \in R_Z$ to its corresponding ξ-vector $\boldsymbol{b}$ (satisfying $a = \boldsymbol{\xi}^T \cdot \boldsymbol{b}$), by Lemma 6, we need to compute a matrix-vector product $\boldsymbol{b} = \Omega_Z^{(q)} \cdot \boldsymbol{a}$. By Lemma 5, the inverse conversion from ξ-vector $\boldsymbol{b}$ to its corresponding η-vector $\boldsymbol{a} = \Gamma_Z \cdot \boldsymbol{b}$ also can be computed using a similar matrix-vector product $\overline{\Omega}_Z^{(q)} \cdot \boldsymbol{b}$. Here, $\overline{\Omega}_Z^{(q)} \stackrel{\text{def}}{=} \overline{\Omega_Z} \bmod \mathsf{q}$.

By definition of $\Omega_Z^{(q)}$, the j-th component b_j of the product $\boldsymbol{b} = \Omega_Z^{(q)} \cdot \boldsymbol{a}$ is $b_j = \sum_{i=0}^{g-1} a_i \eta_{i+j}$ (where indexes are mod g and we omit mod$\mathsf{q}$). This means that $\boldsymbol{b}$ is the convolution product of vector $\boldsymbol{\eta}$ and the reversal vector $(a_0, a_{g-1}, a_{g-2}, \cdots, a_1)$ of $\boldsymbol{a}$, where $\boldsymbol{\eta} = (\eta_i)_{i=0}^{g-1}$ is the first row of $\Omega_Z^{(q)}$.

Define two polynomials $f(X) = \sum_{i=0}^{g-1} \eta_i X^i$ and $g(X) = a_0 + \sum_{i=1}^{g-1} a_{g-i} X^i$ over $\mathbb{Z}_q$. Since $\boldsymbol{b}$ is the convolution product of $\boldsymbol{\eta}$ and the reversal vector of $\boldsymbol{a}$, it holds that $f(X)g(X) = \sum_{i=0}^{g-1} b_i X^i \pmod{X^g - 1}$. The polynomial product $f(X)g(X) \pmod{X^g - 1}$ can be computed in quasi-linear time $\tilde{O}(g)$ using the FFT multiplication. Thus, we know that conversions between η-vectors $\boldsymbol{a}$ and ξ-vectors $\boldsymbol{b}$ can be done in quasi-linear time $\tilde{O}(g)$.

4 Subring Homomorphic Encryption

Now we construct an HE scheme using the decomposition ring R_Z, *subring homomorphic encryption* scheme.

4.1 The Ring-LWE problem on the decomposition ring

For security of our subring homomorphic encryption scheme, we will need hardness of a variant of the decisional Ring-LWE problem over the decomposition ring. Let m be a prime. Let R_Z be the decomposition ring of the m-th cyclotomic ring R with respect to some prime $p\,(\neq m)$. Let q be a positive integer. For an element $s \in R_Z$ and a distribution χ over R_Z, define a distribution $A_{s,\chi}$ on $(R_Z)_q \times (R_Z)_q$ as follows: First choose an element a uniformly from $(R_Z)_q$ and sample an element e according to the distribution χ. Then return the pair $(a, b = as + e \bmod q)$.

Definition 3 (The decisional Ring-LWE problem on the decomposition ring). *Let q, χ be as above.* The R-DLWE$_{q,\chi}$ problem on the decomposition ring R_Z *asks to distinguish samples from $A_{s,\chi}$ with $s \stackrel{\text{u}}{\leftarrow} \mathbb{Z}_q$ and (the same number of) samples uniformly chosen from $(R_Z)_q \times (R_Z)_q$.*

Recall the search version of Ring-LWE problem is already proved to have a quantum polynomial time reduction from the approximate shortest vector problem of ideal lattices in *any number field* by Lyubashevsky, Peikert, and Regev [15]. They proved equivalence between the search and the decisional versions of the Ring-LWE problems only for cyclotomic rings. The key of their proof of equivalence is the existence of prime modulus q for Ring-LWE problem which totally decomposes into n prime ideal factors: $qR = \mathfrak{Q}_0 \cdots \mathfrak{Q}_{n-1}$. (Their residual fields $R/\mathfrak{Q}_i$ have polynomial order q and we can guess the solution of the

Ring-LWE problem modulo ideal $\mathfrak{Q}_i$, and then we can verify validity of the guess using the assumed oracle for the decisional Ring-LWE problem.) Since the decomposition ring R_Z is a subring of the cyclotomic ring R, such modulus q totally decomposes into g prime ideals also in the decomposition ring R_Z: $qR_Z = \mathfrak{q}_0 \cdots \mathfrak{q}_{g-1}$. Using this decomposition, the proof of equivalence by [15] holds also over the decomposition rings R_Z, essentially as it is.

4.2 Parameters

Let m be a prime index of cyclotomic ring R. Choose a (small) prime p, distinct from m. Let $d = \mathrm{ord}_m^\times(p)$ be the multiplicative order of p mod m, and $g = (m-1)/d$ be the degree of the decomposition ring R_Z of R with respect to p. Take two powers of p, $q = p^r$ and $t = p^l$ $(r > l)$ as ciphertext and plaintext modulus, respectively. Set the quotient as $\Delta = q/t = p^{r-l}$. Choose two distributions $\boldsymbol{\chi}_{key}$ and $\boldsymbol{\chi}_{err}$ over $\mathbb{Z}^g$.

4.3 Encoding methods and basic operations of elements in R_Z

Basically, we use η-vectors $\boldsymbol{a} \in \mathbb{Z}^g$ to encode elements $a = \boldsymbol{\eta}^T \cdot \boldsymbol{a}$ in R_Z. To multiply two elements encoded by η-vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ modulo $q = p^r$, first we convert those η-vectors to corresponding ξ-vectors modulo q. We can multiply resulting ξ-vectors component-wise, and then re-convert the result into its corresponding η-vector modulo q. The functions eta_to_xi and xi_to_eta use the matrix $\Omega_Z^{(q)}$ computed in advance. $(\eta_i)_{i=0}^{g-1}$ denotes the first row of $\Omega_Z^{(q)}$.

mult_eta $(\boldsymbol{a}, \boldsymbol{b}, q)$:
- $\boldsymbol{\alpha} = \text{eta\_to\_xi}(\boldsymbol{a}, q)$
- $\boldsymbol{\beta} = \text{eta\_to\_xi}(\boldsymbol{b}, q)$
- $\gamma_i = \alpha_i \beta_i \bmod q \ (i = 0, \ldots, g-1)$
- return $\boldsymbol{c} = \text{xi\_to\_eta}(\boldsymbol{\gamma}, q)$

eta_to_xi $(\boldsymbol{a}, q)$:
- $a(X) = a_0 + \sum_{i=1}^{g-1} a_{g-i} X^i$
- $c(X) = \sum_{i=0}^{g-1} \eta_i X^i$
- $b(X) = a(X)c(X) \bmod (q, X^g - 1)$
- return $\boldsymbol{b} = (b_0, \ldots, b_{g-1})$

xi_to_eta $(\boldsymbol{b}, q)$:
- $b(X) = b_0 + \sum_{i=1}^{g-1} b_{g-i} X^i$
- $c(X) = \sum_{i=0}^{g-1} \overline{\eta}_i X^i$
- $a(X) = b(X)c(X) \bmod (q, X^g - 1)$
- $t = b_0 + \cdots + b_{g-1} \bmod q$
- return $\boldsymbol{a} = (m^{-1}(a_i - dt) \bmod q)_{i=0}^{g-1}$

We regard plaintext vectors $\boldsymbol{m} \in \mathbb{Z}_t^g$ as ξ-vectors of corresponding elements $m_\xi = \boldsymbol{\xi}^T \boldsymbol{m} \in (R_Z)_t$. By Lemma 7 their products $m_\xi m'_\xi \in (R_Z)_t$ encodes the plaintext vector $\boldsymbol{m} \odot \boldsymbol{m'} \in \mathbb{Z}_t^g$. For a fixed integer base w, let $l_w = \lfloor \log_w(q) \rfloor + 1$. Any vector $\boldsymbol{a} \in \mathbb{Z}_q^g$ can be written as $\boldsymbol{a} = \sum_{k=0}^{l_w-1} w^k \boldsymbol{a}_k$ with vectors $\boldsymbol{a}_k \in \mathbb{Z}_w^g$ of small entries. Define $\mathsf{WD}(\boldsymbol{a}) \stackrel{\text{def}}{=} \left(\boldsymbol{a}_k\right)_{k=0}^{l_w-1} \left(\in (\mathbb{Z}_w^g)^{l_w}\right)$.

4.4 Scheme Description

Our subring homomorphic encryption scheme is a realization of the FV scheme by Fan and Vercauteren [6], using the decomposition ring R_Z. Here we describe its symmetric key version. The public key version is easily derived as like in the FV and other HE schemes.

SecretKeyGen () :
  $\boldsymbol{s} \leftarrow \chi_{key}$
  return $\mathsf{sk} = \boldsymbol{s} \in \mathbb{Z}^g$

Encrypt ($\mathsf{sk} = \boldsymbol{s} \in \mathbb{Z}^g, \boldsymbol{m} \in \mathbb{Z}_t^g$) :
  $\boldsymbol{a} \overset{\mathsf{u}}{\leftarrow} \mathbb{Z}_q^g$, $\boldsymbol{e} \leftarrow \chi_{err}$, $\boldsymbol{n} = \mathsf{xi\_to\_eta}(\boldsymbol{m}, t)$
  $\boldsymbol{b} = \mathsf{mult\_eta}(\boldsymbol{a}, \boldsymbol{s}, q) + \Delta \boldsymbol{n} + \boldsymbol{e} \bmod q$
  return $ct = (\boldsymbol{a}, \boldsymbol{b})$

Decrypt ($\mathsf{sk} = \boldsymbol{s} \in \mathbb{Z}^g, ct = (\boldsymbol{a}, \boldsymbol{b})$):
  $\boldsymbol{n} = \left\lfloor \frac{1}{\Delta}(\boldsymbol{b} - \mathsf{mult\_eta}(\boldsymbol{a}, \boldsymbol{s}, q) \bmod q) \right\rceil$
  $\boldsymbol{m} = \mathsf{eta\_to\_xi}(\boldsymbol{n}, t)$
  return $\boldsymbol{m}$

Add ($ct_1 = (\boldsymbol{a}_1, \boldsymbol{b}_1), ct_2 = (\boldsymbol{a}_2, \boldsymbol{b}_2)$):
  $\boldsymbol{a} = \boldsymbol{a}_1 + \boldsymbol{a}_2 \bmod q$,
  $\boldsymbol{b} = \boldsymbol{b}_1 + \boldsymbol{b}_2 \bmod q$
  return $ct = (\boldsymbol{a}, \boldsymbol{b})$

EvaluateKeyGen ($\boldsymbol{s}$) :
  $\boldsymbol{\gamma} = \mathsf{mult\_eta}(\boldsymbol{s}, \boldsymbol{s}, q)$
  For $k = 0$ to $l_w - 1$:
    $\boldsymbol{\alpha}_k \overset{\mathsf{u}}{\leftarrow} \mathbb{Z}_q^g$, $\boldsymbol{x}_k \leftarrow \chi_{err}$, $\boldsymbol{\beta}_k = \mathsf{mult\_eta}(\boldsymbol{\alpha}_k, \boldsymbol{s}, q) + w^k \boldsymbol{\gamma} + \boldsymbol{x}_k \bmod q$
  return $\mathsf{ev} = \big((\boldsymbol{\alpha}_k, \boldsymbol{\beta}_k)\big)_{k=0}^{l_w-1}$

Mult ($ct_1 = (\boldsymbol{a}_1, \boldsymbol{b}_1), ct_2 = (\boldsymbol{a}_2, \boldsymbol{b}_2), \mathsf{ev} = \big((\boldsymbol{\alpha}_k, \boldsymbol{\beta}_k)\big)_k$) :
  $\boldsymbol{e} = \left\lfloor \frac{1}{\Delta} \cdot \mathsf{mult\_eta}(\boldsymbol{b}_1, \boldsymbol{b}_2, q^2/t) \right\rceil$,
  $\boldsymbol{c} = \left\lfloor \frac{1}{\Delta} \cdot \big(\mathsf{mult\_eta}(\boldsymbol{a}_1, \boldsymbol{b}_2, q^2/t) + \mathsf{mult\_eta}(\boldsymbol{a}_2, \boldsymbol{b}_1, q^2/t)\big) \right\rceil$,
  $\boldsymbol{d} = \left\lfloor \frac{1}{\Delta} \cdot \mathsf{mult\_eta}(\boldsymbol{a}_1, \boldsymbol{a}_2, q^2/t) \right\rceil$, $(\boldsymbol{d}_0, \cdots, \boldsymbol{d}_{l_w-1}) = \mathsf{WD}(\boldsymbol{d})$
  $\boldsymbol{a} = \boldsymbol{c} + \sum_{k=0}^{l_w-1} \mathsf{mult\_eta}(\boldsymbol{d}_k, \boldsymbol{\alpha}_k, q) \bmod q$,
  $\boldsymbol{b} = \boldsymbol{e} + \sum_{k=0}^{l_w-1} \mathsf{mult\_eta}(\boldsymbol{d}_k, \boldsymbol{\beta}_k, q) \bmod q$
  return $ct = (\boldsymbol{a}, \boldsymbol{b})$

It is straightforward to see:

Theorem 1. *The subring homomorphic encryption scheme is indistinguishably secure under the chosen plaintext attack if the* R-DLWE$_{q,\chi_{key},\chi_{err}}$ *problem on the decomposition ring R_Z is hard.*

For correctness we have the following theorem. (The proof is in Section A.3)

Theorem 2. *The subring homomorphic encryption scheme will be fully homomorphic under circular security assumption (i.e., an encryption of secret key $\boldsymbol{s}$ does not leak any information about $\boldsymbol{s}$) by taking ciphertext modulus $q = O(\lambda^{\log \lambda})$.*

5 Benchmark Results

We implemented our subring homomorphic encryption scheme (SR-HE in short) using the C++ language and performed several experiments using different parameters, comparing efficiency of our implementation of SR-HE and homomorphic encryption library HElib by Halevi and Shoup [10], which is based on the BGV scheme [4]. For notation of parameters, see Section 4.2.

As common parameters, we choose four values of prime m so that the m-th cyclotomic ring R will have as many number of plaintext slots (i.e., large g and small d values) as possible. The plaintext modulus $t = 2^l$ is fixed as $l = 8$. The noise parameter $s_{err} = \sqrt{2\pi}\sigma_{err}$ is fixed as $\sigma_{err} = 3.2$. The ciphertext modulus $q = 2^r$ is chosen as small as possible so that it enables homomorphic evaluation of exponentiation by 2^8 (i.e., $\mathsf{Enc}(\boldsymbol{s}, \boldsymbol{m})^{2^8}$) with respect to each implementation. Table 1 summarizes the chosen parameters.

	m	g	d	l	r (SR-HE)	r (HElib)
par-127	127	18	7	8	162	135
par-8191	8191	630	13	8	210	250
par-43691	43691	1285	34	8	234	256
par-131071	131071	7710	17	8	242	-

Table 1. Chosen parameters.

Assuming that there is no special attack utilizing the particular algebraic structure of involving rings, corresponding security parameters λ are estimated using the lwe-estimator-9302d4204b4f by [2, 1].

Table 2 shows timing results for HElib in milliseconds on Intel Celeron(R) CPU G1840 @ 2.80GHz × 2. (We could not perform the test for par-131071 due to shortage of memory.) The secret key is chosen uniformly random among binary vectors of Hamming weight 64 over the power basis (default of HElib) and we encrypt g number of mod-2^l integer plaintexts into a single HElib ciphertext using plaintext slots. As seen in Section 2.5, HElib (based on the BGV scheme) basically realizes $GF(2^d)$ arithmetic in each of g slots. If we want to encrypt mod-2^l integer plaintexts on slots and to homomorphically evaluate on them, we can use only 1-dimensional constant polynomials in each $d(= m/g)$-dimensional slots. This should cause certain waste in time and space. In fact, for example, timings for par-43691 ($g = 1285$) is much larger than two times of those for par-8191 ($g = 630$). This indicates that the HElib scheme cannot handle many mod-2^l integer slots with high parallelism. So, to encrypt large number of mod-2^l integer plaintexts using HElib, we have no choice but to prepare many ciphertexts, each of which encrypts a divided set of small number of plaintexts on their slots. On the other hand, Table 3 shows timing results (also in milliseconds on Intel Celeron(R) CPU G1840 @ 2.80GHz × 2) for our SR-HE scheme. The secret key is chosen uniformly random among binary vectors of Hamming weight 64 over η-basis and we encrypt g number of mod-2^l integer plaintexts into a single SR-HE ciphertext. As seen, timings are approximately linear with respect to the numbers of slots g. This shows that our SR-HE scheme can handle many mod-2^l slots with high parallelism, as expected. We can encrypt large number of mod-2^l integer plaintexts into a single SR-HE ciphertext using mod-2^l slots without waste, and can homomorphically compute on them with high parallelism.

Then, which is faster to encrypt many number of mod-2^l integer plaintexts between the following two cases?

	λ	Enc	Dec	Add	Mult	Exp-by-2^8
par-127	26	0.23	0.18	0.00	0.66	4.78
par-8191	92	30.45	210.77	0.84	107.53	512.64
par-43691	237	268.00	5158.44	4.74	634.69	4187.81
par-131071	-	-	-	-	-	-

Table 2. Timing results of HElib on mod-2^l integer plaintexts.

	λ	Enc	Dec	Add	Mult	Exp-by-2^8
par-127	-	0.14	0.12	0.00	0.57	4.47
par-8191	29	7.39	7.37	0.03	39.43	318.65
par-43691	32	17.38	17.19	0.11	92.14	741.42
par-131071	91	104.33	103.93	0.97	574.44	4620.22

Table 3. Timing results of SR-HE on mod-2^l integer plaintexts.

(1) A single SR-HE ciphertext with many plaintext slots.
(2) Many HElib ciphertexts with small number of plaintext slots.

The result for par-131071 of Table 3 shows we can encrypt 7710 mod-2^l integer slots in a single SR-HE ciphertext with security parameter $\lambda = 91$ with timing:

$$(104.33, 103.93, 0.97, 574.44, 4620.22)$$

On a while, the result for par-8191 of Table 2 shows we can encrypt the same number of 7710 mod-2^l integer slots using $\lceil 7710/630 \rceil = 13$ ciphertexts with security parameter $\lambda = 92$. The 13 times of the line par-8191 of Table 2 is

$$(395.85, 2740.01, 10.92, 1397.89, 6664.32).$$

Thus, our benchmark results indicate that Case (1) (a single SR-HE ciphertext with many slots) is significantly faster than Case (2) (many HElib ciphertexts with small number of plaintext slots) under equivalent security parameters.

Acknowledgments. This work was supported by JST CREST Grant Number JPMJCR1503. This work is further supported by the JSPS KAKENHI Grant Number 17K05353.

References

1. Martin R. Albrecht, On Dual Lattice Attacks Against Small-Secret LWE and Parameter Choices in HElib and SEAL, EUROCRYPT 2017: Advances in Cryptology - EUROCRYPT 2017 pp 103-129, 2017.
2. Martin R. Albrecht, Rachel Player and Sam Scott, On the concrete hardness of Learning with Errors. Journal of Mathematical Cryptology. Volume 9, Issue 3, Pages 169203, 2015.

3. Zvika Brakerski, Fully homomorphic encryption without modulus switching from classical GapSVP. Crypto 2012, LNCS 7417, pages 868-886. Springer, 2012.
4. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan, (Leveled) fully homomorphic encryption without bootstrapping. ITCS, pages 309-325. ACM, 2012.
5. Jung Hee Cheon, Miran Kim, Kristin Lauter, Homomorphic Computation of Edit Distance. Financial Cryptography and Data Security 2015, LNCS 8976, pp 194-212, 2015.
6. Junfeng Fan and Frederik Vercauteren, Somewhat practical fully homomorphic encryption. IACR Cryptology ePrint Archive, 2012-144, 2012.
7. Craig Gentry, Fully homomorphic encryption using ideal lattices. STOC, pages 169-178. ACM, 2009.
8. Craig Gentry, Shai Halevi, Nigel P. Smart, Homomorphic Evaluation of the AES Circuit. Crypto 2012, LNCS 7417, pages 850-867. Springer, 2012.
9. Thore Graepel, Kristin Lauter, Michael Naehrig, ML Confidential: Machine Learning on Encrypted Data. ICISC 2012, LNCS 7839, Springer-Verlag (2013), pp 1-21.
10. Shai Halevi, Victor Shoup, Algorithms in HElib. CRYPTO 2014, LNCS 8616, pp 554-571.
11. J. Liu, J. Li, S. Xu, and B. C.M. Fung, Secure Outsourced Frequent Pattern Mining by Fully Homomorphic Encryption. DaWaK 2015, LNCS 9263, pp 70-81, 2015.
12. K. Lauter, A. Lpez-Alt, M. Naehrig, Private Computation on Encrypted Genomic Data. LATINCRYPT 2014, LNCS 8895, Springer-Verlag, pp 3-27.
13. Wen-jie Lu, Shohei Kawasaki, Jun Sakuma, Using Fully Homomorphic Encryption for Statistical Analysis of Categorical, Ordinal and Numerical Data. Network and Distributed System Security Symposium (NDSS) in February, 2017.
14. Kim Laine and Rachel Player, Simple Encrypted Arithmetic Library - SEAL(v2.0). Technical report, Microsoft Research, September 2016. MSR-TR-2016-52.
15. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On Ideal Lattices and Learning with Errors over Rings. EUROCRYPT 2010, LNCS 6110, pp 1-23, 2010.
16. Vadim Lyubashevsky, Chris Peikert, Oded Regev, A Toolkit for Ring-LWE Cryptography. EUROCRYPT 2013, LNCS 7881, pp 35-54, Springer, 2013.
17. N. P. Smart, F. Vercauteren, Fully homomorphic SIMD operations. Designs, Codes and Cryptography, April 2014, Volume 71, Issue 1, pp 57-81.

A Appendices

A.1 Proofs of Lemma

Proof of Lemma 2. $\mathrm{Tr}_{Z|\mathbb{Q}}(\eta_i) = \mathrm{Tr}_{Z|\mathbb{Q}}(\mathrm{Tr}_{K|Z}(\zeta^{t_i})) = \mathrm{Tr}_{K|\mathbb{Q}}(\zeta^{t_i})$. So, by Lemma 1, $\mathrm{Tr}_{Z|\mathbb{Q}}(\eta_i) = -1$ for any i. Similarly, $\mathrm{Tr}_{Z|\mathbb{Q}}(\overline{\eta}_i) = \mathrm{Tr}_{Z|\mathbb{Q}}(\mathrm{Tr}_{K|Z}(\zeta^{-t_i})) = \mathrm{Tr}_{K|\mathbb{Q}}(\zeta^{-t_i}) = -1$. □

Proof of Lemma 3 Since the index m is prime, the cyclotomic ring R has a basis $B = \{1, \zeta, \dots, \zeta^{m-2}\}$ over $\mathbb{Z}$. Since ζ is a unit of R, $B' := \zeta B = \{\zeta, \zeta^2, \dots, \zeta^{m-1}\}$ is also a basis of R over $\mathbb{Z}$. The fixing group $G_Z = \langle \rho_p \rangle$ of Z acts on B' and decomposes it into g orbits $\zeta^{t_i\langle p\rangle} = \{\zeta^{t_i}, \zeta^{t_i p}, \dots, \zeta^{t_i p^{d-1}}\}$ $(i = 0, \dots, g-1)$. An element $z = \sum_{i=1}^{m-1} z_i \zeta^i \in R_Z$ that is stable under the action of G_Z must have constant integer coefficients over the each orbits $\zeta^{t_i\langle p\rangle}$. Hence, z is a $\mathbb{Z}$-linear combination of $\{\eta_1, \dots, \eta_g\}$ □

Proof of Lemma 4 For $0 \le i, j < g$,

$$\overline{\eta}_i \eta_j = \Big(\sum_{a\in\langle p\rangle} \zeta^{-at_i}\Big)\Big(\sum_{b\in\langle p\rangle} \zeta^{bt_j}\Big) = \sum_{a,b\in\langle p\rangle} \zeta^{-at_i+bt_j} = \sum_{a\in\langle p\rangle}\sum_{b\in\langle p\rangle} \rho_a(\zeta^{-t_i+ba^{-1}t_j})$$
$$= \sum_{a\in\langle p\rangle}\sum_{b\in\langle p\rangle} \rho_a(\zeta^{-t_i+bt_j}) = \sum_{b\in\langle p\rangle} \mathrm{Tr}_{K|Z}(\zeta^{-t_i+bt_j}).$$

Here, Suppose $i \ne j$. Then, $-t_i + bt_j \not\equiv 0 \pmod{m}$ for any $b \in \langle p\rangle$. Hence, by Lemma 1,

$$\mathrm{Tr}_{Z|\mathbb{Q}}(\overline{\eta}_i\eta_j) = \sum_{b\in\langle p\rangle} \mathrm{Tr}_{K|\mathbb{Q}}(\zeta^{-t_i+bt_j}) = |\langle p\rangle| \cdot (-1) = -d.$$

If $i = j$, since $\mathrm{Tr}_{K|\mathbb{Q}}(\zeta^{-t_i+bt_i}) = m-1$ only if $b = 1$ and -1 otherwise by Lemma 1,

$$\mathrm{Tr}_{Z|\mathbb{Q}}(\overline{\eta}_i\eta_i) = \sum_{b\in\langle p\rangle} \mathrm{Tr}_{K|\mathbb{Q}}(\zeta^{-t_i+bt_i}) = m - 1 + (d-1)\cdot(-1) = m - d \quad \square$$

Proof of Corollary 1 For any i, by Lemma 2 and 4 we have

$$\mathrm{Tr}_{Z|\mathbb{Q}}\Big(\frac{\eta_i - d}{m} \cdot \overline{\eta_i}\Big) = \frac{1}{m}(m-d) - \frac{d}{m}\cdot(-1) = 1.$$

Similarly, for any $i \ne j$ we have

$$\mathrm{Tr}_{Z|\mathbb{Q}}\Big(\frac{\eta_i - d}{m} \cdot \overline{\eta_j}\Big) = \frac{-d}{m} - \frac{d}{m}\cdot(-1) = 0 \quad \square$$

Proof of Lemma 5

$$\boldsymbol{a} \;=\; \mathit{\Gamma}_Z\boldsymbol{b} \;=\; \Big(\rho_{t_i}\big(\frac{\overline{\eta}_j - d}{m}\big)\Big)_{ij}\boldsymbol{b} \;=\; \Big(\frac{1}{m}\sum_j \rho_{t_i}(\overline{\eta}_j - d)b_j\Big)_i$$
$$=\; \frac{1}{m}\Big(\sum_j \rho_{t_i}(\overline{\eta}_j)b_j - d\sum_j b_j\Big)_i \;=\; \frac{1}{m}\Big(\overline{\mathit{\Omega}}_Z\boldsymbol{b} - d\big(\sum_j b_j\big)\cdot\boldsymbol{1}\Big) \quad \square$$

Proof of Lemma 6 The first claim is the definition of $\boldsymbol{\xi}$.

Since $\mathit{\Omega}_Z = \Big(\sigma_Z(\eta_j)\Big)_{0\le j<g}$, $a = \boldsymbol{\eta}^T \cdot \boldsymbol{a}$ if and only if $\sigma_Z(a) = \mathit{\Omega}_Z\boldsymbol{a}$.

Next,

$$a = \boldsymbol{\xi}^T \cdot \boldsymbol{b} \;\Leftrightarrow\; a \equiv \boldsymbol{\eta}^T(\mathit{\Omega}_Z^{(q)})^{-1}\cdot\boldsymbol{b} \pmod{\mathfrak{q}}$$
$$\Leftrightarrow\; \sigma_Z(a) \equiv \mathit{\Omega}_Z(\mathit{\Omega}_Z^{(q)})^{-1}\cdot\boldsymbol{b} \equiv \boldsymbol{b} \pmod{\mathfrak{q}} \quad \square$$

Proof of Lemma 7 $\sigma_Z(a_1a_2) = \sigma_Z(a_1)\odot\sigma_Z(a_2) = \boldsymbol{b}_1 \odot \boldsymbol{b}_2$ $\square$

Proof of Lemma 8 The ideal qR_Z factors in R_Z as

$$qR_Z = \mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_{g-1}$$

where $\mathfrak{q}_i = \mathfrak{Q}_i \cap R_Z$ for any i.

Let $\{\tau_i'\}_{i=0}^{g-1}$ be a resolution of unity in R_Z mod q. Here, we take the coefficients of each τ_i' from $[-q/2, q/2)$ over the η-basis $\{\eta_0, \dots, \eta_{g-1}\}$ of R_Z.

Then,

$$\tau_i' \equiv \begin{cases} 1 & (\text{mod } \mathfrak{q}_i)\ (i = 0, \dots, g-1) \\ 0 & (\text{mod } \mathfrak{q}_j)\ (j \neq i). \end{cases}$$

Since $\mathfrak{q}_i \subset \mathfrak{Q}_i$ for any i, $\{\tau_i'\}_{i=0}^{g-1}$ is also a resolution of unity in R mod q. Since the coefficients of each τ_i' over the η-basis are in $[-q/2, q/2)$, by definition of $\eta_i = \sum_{a\in\langle p\rangle} \zeta^{t_i a}$, their coefficients over the basis B' are trivially also in $[-q/2, q/2)$. Hence, by the uniqueness of resolution, it must be that $\tau_i' = \tau_i$ for all i □

A.2 Norms on the decomposition ring

Norms of $a \in Z$ are defined by

$$\|a\|_2 \overset{\text{def}}{=} \|\sigma_Z(a)\|_2,\ \|a\|_\infty \overset{\text{def}}{=} \|\sigma_Z(a)\|_\infty.$$

Lemma 9. *For any $a, b \in Z$, we have*

$$\|ab\|_\infty \leq \|a\|_\infty \cdot \|b\|_\infty.$$

Proof. $\|ab\|_\infty = \|\sigma_Z(ab)\|_\infty = \|\sigma_Z(a) \odot \sigma_Z(b)\|_\infty \leq \|\sigma_Z(a)\|_\infty \cdot \|\sigma_Z(b)\|_\infty = \|a\|_\infty \cdot \|b\|_\infty$. □

In the following, $\boldsymbol{a}$ means the η-vector of given $a = \boldsymbol{\eta}^T \cdot \boldsymbol{a} \in R_Z$.

Lemma 10. *(1) For any $a \in Z$, $\|a\|_2 \leq \sqrt{m}\|\boldsymbol{a}\|_2$.*
(2) For any $\boldsymbol{a} \in \mathbb{R}^g$, $\|\boldsymbol{a}\|_2 \leq \|a\|_2$.
(3) If $\boldsymbol{a} \in \mathbb{R}^g$ is far from being proportional to vector **1** *(*far from constants *in short), we have $\|\boldsymbol{a}\|_2 \approx \frac{1}{\sqrt{m}}\|a\|_2$.*

Proof. (1) By Lemma 6, $\sigma_Z(a) = \Omega_Z\boldsymbol{a}$ and by Lemma 4

$$\Omega_Z^*\Omega_Z = mI_g - d\mathbf{1} \cdot \mathbf{1}^T.$$

The right-hand side matrix has eigenvalues $g-1$ times of m and 1 with corresponding eigenvectors $(1, -1, 0, \cdots, 0)$, $(1, 0, -1, 0, \cdots, 0)$, …, $(1, 0, \cdots, 0, -1)$, $(1, 1, \cdots, 1)$. So, the symmetric matrix $\Omega_Z^*\Omega_Z$ can be diagonalized to $\text{Diag}(m, \cdots, m, 1)$ by an orthogonal transformation, and we have $s_1(\Omega_Z) = \sqrt{m}$. This means $\|a\|_2 \leq \sqrt{m}\|\boldsymbol{a}\|_2$.
(2), (3) Conversely, $\boldsymbol{a} = (\Omega_Z)^{-1}\sigma_Z(a) = \Gamma_Z\sigma_Z(a)$. Similarly as above, the matrix $\Gamma_Z^*\Gamma_Z$ can be diagonalized to $\text{Diag}(1/m, \cdots, 1/m, 1)$ by the orthogonal transformation. Hence, $s_1(\Gamma_Z) = 1$ and $\|\boldsymbol{a}\|_2 \leq \|a\|_2$. Since almost all of the eigenvalues of $\Gamma_Z^*\Gamma_Z$ are $1/m$, except 1 for eigenvector $(1, 1, \cdots, 1)$, if $\boldsymbol{a}$ is far from being proportional to the eigenvector $(1, 1, \cdots, 1)$, $\|\boldsymbol{a}\|_2 \approx \frac{1}{\sqrt{m}}\|a\|_2$ □

Lemma 11. *(1) For any $a \in Z$, $\|a\|_\infty \leq \sqrt{mg}\|\boldsymbol{a}\|_\infty$.*
(2) For any $\boldsymbol{a} \in \mathbb{R}^g$, $\|\boldsymbol{a}\|_\infty \leq \sqrt{g}\|a\|_\infty$.
(3) If a is far from constants, we have $\|\boldsymbol{a}\|_\infty \lessapprox \sqrt{g/m}\|a\|_\infty$.

Proof. (1) By Lemma 10-(1), $\|a\|_\infty \leq \|a\|_2 \leq \sqrt{m}\|\boldsymbol{a}\|_2 \leq \sqrt{mg}\|\boldsymbol{a}\|_\infty$.
(2) By Lemma 10-(2), $\|\boldsymbol{a}\|_\infty \leq \|\boldsymbol{a}\|_2 \leq \|a\|_2 \leq \sqrt{g}\|a\|_\infty$.
(3) By Lemma 10-(3), $\|\boldsymbol{a}\|_\infty \leq \|\boldsymbol{a}\|_2 \approx \frac{1}{\sqrt{m}}\|a\|_2 \leq \sqrt{g/m}\|a\|_\infty$. □

Subgaussian elements We call a random variable $a \in Z$ *subgaussian with parameter s* if corresponding random variable $\sigma_Z(a)$ on H_Z is subgaussian with parameter s.

Lemma 12 (Claim 2.1, Claim 2.4 [16]). *Let a_i be independent subgaussian random variables over Z with parameter s_i $(i = 1, 2)$. Then,*

1. *The sum $a_1 + a_2$ is subgaussian with parameter $\sqrt{s_1^2 + s_2^2}$.*
2. *For any a_2 fixed, the product $a_1 \cdot a_2$ is subgaussian with parameter $\|a_2\|_\infty s_1$.*

Lemma 13. *Let $\boldsymbol{a}$ be a subgaussian random variable over $\mathbb{R}^g$ of parameter s. Then, $a = \boldsymbol{\eta}^T \cdot \boldsymbol{a}$ is subgaussian over Z of parameter $\sqrt{m}s$.*

Proof. By Lemma 6 $\sigma_Z(a) = \Omega_Z \boldsymbol{a}$. As seen in the proof of Lemma 10, $s_1(\Omega_Z) = \sqrt{m}$. Hence, $\sigma_Z(a)$ is subgaussian of parameter $\sqrt{m}s$ □

A.3 Correctness of our subring homomorphic encryption scheme

Let $\boldsymbol{\chi}_{key}$ and $\boldsymbol{\chi}_{err}$ be discrete Gaussian distributions over $\mathbb{Z}^g$ of parameters s_{key} and s_{err}, respectively. In the following, vectors $\boldsymbol{a}$, $\boldsymbol{b}$, $\cdots$ mean corresponding η-vectors of elements $a = \boldsymbol{\eta}^T \cdot \boldsymbol{a}$, $b = \boldsymbol{\eta}^T \cdot \boldsymbol{b}$, $\cdots$ in the decomposition ring R_Z, respectively.

Definition 4. *The* inherent noise term *e of ciphertext $ct = (\boldsymbol{a}, \boldsymbol{b})$* designed for *$\boldsymbol{m} \in \mathbb{Z}_t^g$ is an element $e \in R_Z$ with the smallest norm $\|e\|_\infty$ satisfying that*

$$b - as = \Delta m_\xi + e + q\alpha$$

for some $\alpha \in R_Z$, secret key $\mathsf{sk} = \boldsymbol{s}$, and $m_\xi = \boldsymbol{\xi}^T \cdot \boldsymbol{m} \in R_Z$.

By definition, a ciphertext $ct = (\boldsymbol{a}, \boldsymbol{b}) \leftarrow \mathsf{Encrypt}(\boldsymbol{s}, \boldsymbol{m})$ has $e = \boldsymbol{\eta}^T \cdot \boldsymbol{e}$ as an inherent noise term designed for $\boldsymbol{m}$ with $\boldsymbol{e} \leftarrow \boldsymbol{\chi}_{err}$. By Lemma 13, e is subgaussian of parameter $\sqrt{m}s_{err}$ and by the tail inequality (Eq. 2), $\|e\|_\infty \leq \omega(\sqrt{\log \lambda})\sqrt{m}s_{err}$ with an overwhelming probability.

Define $B_{correct} \stackrel{\text{def}}{=} \frac{\sqrt{m}}{2\sqrt{g}}\Delta$.

Lemma 14 (Noise bound for correctness). *Let e be the inherent noise term of ciphertext $ct = (\boldsymbol{a}, \boldsymbol{b})$ designed for $\boldsymbol{m} \in \mathbb{Z}_t^g$. If $\|e\|_\infty < B_{correct}$ (i.e. if $\frac{\sqrt{g}}{\sqrt{m}}\|e\|_\infty < \frac{1}{2}\Delta$), then decryption works correctly, i.e. $\mathsf{Decrypt}(\boldsymbol{s}, ct) = \boldsymbol{m}$.*

Proof. By definition of the inherent noise term, $\boldsymbol{a}$ and $\boldsymbol{b}$ satisfy that

$$\frac{1}{\Delta}(b - as - \alpha q) \;=\; m_\xi + \frac{e}{\Delta}. \tag{9}$$

By Lemma 11-(3),

$$\|\frac{\boldsymbol{e}}{\Delta}\|_\infty < \sqrt{g/m} \cdot \|\frac{e}{\Delta}\|_\infty \leq \sqrt{g/m} \cdot \frac{\sqrt{m}}{2\sqrt{g}} = \frac{1}{2}.$$

Hence, the η-vector of the left-hand side of Eq.(9) rounds to $\boldsymbol{n}$ satisfying that $\boldsymbol{\eta}^T \cdot \boldsymbol{n} = m_\xi = \boldsymbol{\xi}^T \cdot \boldsymbol{m}$ □

Lemma 15 (Noise bound for Add). *Let e_1 and e_2 be inherent noise terms of ciphertexts $ct_1 = (\boldsymbol{a}_1, \boldsymbol{b}_1)$ and $ct_2 = (\boldsymbol{a}_2, \boldsymbol{b}_2)$ designed for $\boldsymbol{m}_1$ and $\boldsymbol{m}_2 \in \mathbb{Z}_t^g$, respectively. Let e be the inherent noise term of $ct = \mathsf{Add}(ct_1, ct_2)$ designed for $\boldsymbol{m}_1 + \boldsymbol{m}_2 \in \mathbb{Z}_t^g$. Then,*

$$\|e\|_\infty \leq \|e_1\|_\infty + \|e_2\|_\infty.$$

Lemma 16 (Noise bound for linearization). *Let $\mathsf{ev} = \big((\boldsymbol{\alpha}_k, \boldsymbol{\beta}_k)\big)_{k=0}^{l_w-1} \leftarrow$ $\mathsf{EvaluateKeyGen}(\boldsymbol{s})$ be an evaluation key for a secret key $\mathsf{sk} = \boldsymbol{s}$. Suppose that a triple of elements e, c, d in R_Z satisfies*

$$e - cs + ds^2 \equiv \Delta m_\xi + x \pmod q$$

with $m_\xi = \boldsymbol{\xi}^T \cdot \boldsymbol{m}$ and some $x \in R_Z$ bounded as $\|x\|_\infty \leq B$. Let $(\boldsymbol{d}_0, \cdots, \boldsymbol{d}_{l_w-1}) = \mathsf{WD}(\boldsymbol{d})$. Then, for $a = c + \sum_{k=0}^{l_w-1} d_k\alpha_k$ and $b = e + \sum_{k=0}^{l_w-1} d_k\beta_k$, the pair $ct = (\boldsymbol{a}, \boldsymbol{b})$ constitutes a ciphertext that has an inherent noise term y designed for $\boldsymbol{m}$ bounded as

$$\|y\|_\infty \leq B + \omega(\sqrt{\log\lambda})\sqrt{l_w mgw} s_{err}.$$

Proof. By definition of $\mathsf{EvaluateKeyGen}$, the k-th pair $(\boldsymbol{\alpha}_k, \boldsymbol{\beta}_k)$ of ev has an inherent noise term x_k designed for $w^k s^2$, which is subgaussian of parameter $\sqrt{m}s_{err}$. Then,

$$\begin{aligned} b - as &\equiv \Big(e + \sum_{k=0}^{l_w-1} d_k\beta_k\Big) - \Big(c + \sum_{k=0}^{l_w-1} d_k\alpha_k\Big)s \;\equiv\; e - cs + \sum_{k=0}^{l_w-1} d_k(\beta_k - \alpha_k s) \\ &\equiv\; e - cs + \sum_{k=0}^{l_w-1} d_k(w^k s^2 + x_k) \;\equiv\; e - cs + ds^2 + \sum_{k=0}^{l_w-1} d_k x_k \\ &\equiv\; \Delta m_\xi + x + \sum_{k=0}^{l_w-1} d_k x_k \pmod q. \end{aligned}$$

We estimate $\|y\|_\infty$ for $y := x + \sum_{k=0}^{l_w-1} d_k x_k$. First by Lemma 11 (1), $\|d_k\|_\infty \leq \sqrt{mg}\|\boldsymbol{d}_k\|_\infty \leq \sqrt{mg}w$. Then, by Lemma 12, $d_k x_k$ are independently subgaussian of parameter $\|d_k\|_\infty s_{err} \leq \sqrt{mg}ws_{err}$, and $\sum_{k=0}^{l_w-1} d_k x_k$ is subgaussian of parameter $\sqrt{l_w}\sqrt{mg}ws_{err}$. Hence,

$$\|y\|_\infty \le \|x\|_\infty + \Big\|\sum_{k=0}^{l_w-1} d_k x_k\Big\| \le B + \omega(\sqrt{\log\lambda})\sqrt{l_w}\sqrt{mg}ws_{err}. \quad \square$$

Lemma 17 (Noise bound for Mult**).** *Let e_1 and e_2 be inherent noise terms of ciphertexts $ct_1 = (\boldsymbol{a}_1, \boldsymbol{b}_1)$ and $ct_2 = (\boldsymbol{a}_2, \boldsymbol{b}_2)$ designed for $\boldsymbol{m}_1$ and $\boldsymbol{m}_2 \in \mathbb{Z}_t^g$, respectively. Suppose $\|e_i\|_\infty \le B\,(< B_{correct})$ for $i = 1, 2$. Let f be the inherent noise term of $ct = \mathsf{Mult}(ct_1, ct_2)$ designed for $\boldsymbol{m}_1 \odot \boldsymbol{m}_2 \in \mathbb{Z}_t^g$. Then,*

$$\|f\|_\infty \le t\omega(\sqrt{\log\lambda})\sqrt{mg}s_{key}\cdot B + \omega(\sqrt{\log\lambda})\sqrt{l_w mg}ws_{err}.$$

Proof. We prepare two claims.

Claim. Let $e_0 = \frac{1}{\Delta}b_1b_2$, $c_0 = \frac{1}{\Delta}(a_1b_2 + a_2b_1)$, $d_0 = \frac{1}{\Delta}a_1a_2$. Then,

$$e_0 - c_0 s + d_0 s^2 \equiv \Delta m_\xi + x \pmod q$$

with $m_\xi = (m_1)_\xi (m_2)_\xi$ and some $x \in R_Z$ bounded as

$$\|x\|_\infty \le t\omega(\sqrt{\log\lambda})\sqrt{mg}s_{key}\cdot B.$$

Proof. By assumption,

$$b_i - a_i s = \Delta(m_i)_\xi + x_i + \alpha_i q \quad (i = 1, 2) \tag{10}$$

with $\|x_i\|_\infty < B$. By Lemma 12 the product $a_i s$ is subgaussian of parameter $\|a_i\|_\infty s_{key} \le \sqrt{mg}\|\boldsymbol{a}_i\|_\infty s_{key} \le \sqrt{mg}qs_{key}$. So, $\alpha_i = \lfloor (b_i - a_i s)/q \rceil$ is bounded as

$$\|\alpha_i\|_\infty \le \omega(\sqrt{\log\lambda})\sqrt{mg}s_{key}.$$

By taking product of the two equations (10), we get

$$\begin{aligned} e_0 - c_0 s + d_0 s^2 &= \frac{1}{\Delta}\Big(b_1b_2 - (a_1b_2 + a_2b_1)s + a_1a_2s^2\Big) \\ &= \Delta(m_1)_\xi(m_2)_\xi + x + qv \end{aligned}$$

with some $v \in R_Z$, where

$$x = (m_1)_\xi x_2 + (m_2)_\xi x_1 + \frac{1}{\Delta}x_1x_2 + t(x_1\alpha_2 + x_2\alpha_1).$$

By Lemma 9, 11,

$$\begin{aligned} \|(m_i)_\xi x_j\|_\infty &\le \|(m_i)_\xi\|_\infty \|x_j\|_\infty = \sqrt{mg}\|\boldsymbol{n}_i\|_\infty\|x_j\|_\infty \le \sqrt{mg}tB \\ \Big\|\frac{1}{\Delta}x_1x_2\Big\|_\infty &\le \frac{1}{\Delta}\|x_1\|_\infty\|x_2\|_\infty \le \frac{1}{\Delta}B_{correct}\cdot\|x_2\|_\infty \le \frac{\sqrt{m}}{2\sqrt{g}}\cdot B \\ \|tx_i\alpha_j\|_\infty &\le t\|x_i\|_\infty\|\alpha_j\|_\infty \le tB\omega(\sqrt{\log\lambda})\sqrt{mg}s_{key}. \end{aligned}$$

Hence, x is bounded as

$$\begin{aligned}\|x\|_\infty &\le 2\sqrt{mg}tB + \frac{\sqrt{m}}{2\sqrt{g}}\cdot B + 2\sqrt{mg}tB\omega(\sqrt{\log\lambda})\sqrt{mg}s_{key}\\ &= (2\sqrt{mg}t + \frac{\sqrt{m}}{2\sqrt{g}} + 2t\omega(\sqrt{\log\lambda})\sqrt{mg}s_{key})B\\ &= t\omega(\sqrt{\log\lambda})\sqrt{mg}s_{key}\cdot B \quad \square\end{aligned}$$

Claim. Let $\boldsymbol{e} = \lfloor \boldsymbol{e_0} \rceil$, $\boldsymbol{c} = \lfloor \boldsymbol{c_0} \rceil$, $\boldsymbol{d} = \lfloor \boldsymbol{d_0} \rceil$. Then,

$$e - cs + ds^2 \equiv e_0 - c_0 s + d_0 s^2 + y \pmod q$$

with some $y \in R_Z$ bounded as

$$\|y\|_\infty \le \omega(\log\lambda)\sqrt{mg}s_{key}^2.$$

Proof. Let $y = (e - e_0) - (c - c_0)s + (d - d_0)s^2 \pmod q$.

Using Lemma 11 (1), $\|e - e_0\|_\infty \le \sqrt{mg}\|\boldsymbol{e} - \boldsymbol{e}_0\|_\infty \le \sqrt{mg}/2$.

Similarly, $\|c - c_0\|_\infty \le \sqrt{mg}/2$ and by Lemma 9, $\|(c - c_0)s\|_\infty \le \|c - c_0\|_\infty\|s\|_\infty \le \sqrt{mg}/2\cdot\omega(\sqrt{\log\lambda})s_{key} = \omega(\sqrt{\log\lambda})\sqrt{mg}s_{key}$. Similarly, $\|(d - d_0)s^2\|_\infty \le \omega(\log\lambda)\sqrt{mg}s_{key}^2$.

Thus,

$$\begin{aligned}\|y\|_\infty &\le \|e - e_0\|_\infty + \|(c - c_0)s\|_\infty + \|(d - d_0)s^2\|_\infty\\ &\le \sqrt{mg}/2 + \omega(\sqrt{\log\lambda})\sqrt{mg}s_{key} + \omega(\log\lambda)\sqrt{mg}s_{key}^2\\ &\le \omega(\log\lambda)\sqrt{mg}s_{key}^2 \quad \square\end{aligned}$$

By the two claims we know that

$$e - cs + ds^2 \equiv \Delta m_\xi + z \pmod q$$

with $z = x + y$ bounded as

$$\begin{aligned}\|z\|_\infty &\le \|x\|_\infty + \|y\|_\infty \le t\omega(\sqrt{\log\lambda})\sqrt{mg}s_{key}\cdot B + \omega(\log\lambda)\sqrt{mg}s_{key}^2\\ &\le t\omega(\sqrt{\log\lambda})\sqrt{mg}s_{key}\cdot B.\end{aligned}$$

Finally, applying Lemma 16 to our situation, we know that Mult will output a ciphertext $ct = (\boldsymbol{a}, \boldsymbol{b})$ that has an inherent noise term f designed for $m_\xi = (m_1)_\xi(m_2)_\xi$, satisfying that

$$\begin{aligned}\|f\|_\infty &\le \|z\|_\infty + \omega(\sqrt{\log\lambda})\sqrt{l_w mgw}s_{err}\\ &\le t\omega(\sqrt{\log\lambda})\sqrt{mg}s_{key}\cdot B + \omega(\sqrt{\log\lambda})\sqrt{l_w mgw}s_{err} \quad \square\end{aligned}$$

Proof of Theorem 2 By Lemma 14, a ciphertext ct that encrypts plaintext $\boldsymbol{m}$ can be correctly decrypted if its inherent noise term e designed for $\boldsymbol{m}$ satisfies that

$$\frac{\sqrt{g}}{\sqrt{m}}\|e\|_\infty < \frac{1}{2}\Delta = \frac{q}{2t}.$$

By Lemma 17, by one multiplication, $\frac{\sqrt{g}}{\sqrt{m}}$ times of infinity norm of noises under input ciphertexts increases $\log_2(t\omega(\sqrt{\log\lambda})gs_{key}) = O(\log\lambda)$ bits. Hence, to correctly evaluate an arithmetic circuit over $\mathbb{Z}_t^g$ with L levels of multiplications, it suffices that

$$\log q > L\log\lambda.$$

By Lemma 4 of [3], we can implement Decrypt algorithm by some circuit of level $L_{dec} = O(\log\lambda)$. Hence by taking $q = O(\lambda^{\log\lambda})$, the subring homomorphic encryption scheme can homomorphically evaluate its own Decrypt circuit and will be fully homomorphic under circular security assumption □