An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem

Zhiyong Zheng[1], Fengxia Liu[2]*, Kun Tian[1]*

[1]Engineering Research Center of Ministry of Education for Financial Computing and Digital Engineering, Henan Academy of Sciences, Renmin University of China, Beijing, China
[2]Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing, Institute of Artificial Intelligence, Beijing, China
Email: *shunliliu@buaa.edu.cn, *tkun19891208@ruc.edu.cn

Abstract

We propose an unbounded fully homomorphic encryption scheme, *i.e.* a scheme that allows one to compute on encrypted data for any desired functions without needing to decrypt the data or knowing the decryption keys. This is a rational solution to an old problem proposed by Rivest, Adleman, and Dertouzos [1] in 1978, and to some new problems that appeared in Peikert [2] as open questions 10 and open questions 11 a few years ago. Our scheme is completely different from the breakthrough work [3] of Gentry in 2009. Gentry's bootstrapping technique constructs a fully homomorphic encryption (FHE) scheme from a somewhat homomorphic one that is powerful enough to evaluate its own decryption function. To date, it remains the only known way of obtaining unbounded FHE. Our construction of an unbounded FHE scheme is straightforward and can handle unbounded homomorphic computation on any refreshed ciphertexts without bootstrapping transformation technique.

Keywords

Fully Homomorphic Encryption, Ideal Lattices, Chinese Remainder Theorem, General Compact Knapsacks Problem

1. Introduction

In 1978, Rivest, Adleman, and Dertouzos [1] proposed a concept which has come to be known as fully homomorphic encryption (FHE), at the time they called it a privacy homomorphism. In brief, we write a cryptosystem by $\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$, where

$\mathcal{P}$ is the plaintexts space, and $\mathcal{C}$ is the ciphertexts space, f is the encryption function depends on public keys, and f^{-1} is the decryption function depends on secret keys. Suppose that $\mathcal{P}$ and $\mathcal{C}$ are two commutative rings, and

$$f^{-1}(c_1 + c_2) = f^{-1}(c_1) + f^{-1}(c_2), \ f^{-1}(c_1 c_2) = f^{-1}(c_1) f^{-1}(c_2), \forall c_1, c_2 \in \mathcal{C},$$

then f is called a fully homomorphic encryption, or FHE. Under a FHE f, for any polynomials $p(x) \in \mathcal{C}[x]$, it is easy to see that

$$f^{-1}(p(c)) = p^*(f^{-1}(c)), \quad \forall c \in \mathcal{C},$$

where $p^*(x) \in \mathcal{P}[x]$ is the corresponding polynomial over $\mathcal{P}$. Since all elementary functions can be approximated by polynomials, we can do any desired computation on ciphertexts without the decryption of data.

1.1. Unbounded FHE Schemes

Fully homomorphic encryption was known to have abundant applications in cryptography, but for more than three decades no plausibly secure scheme was known. This changed in 2009 when Gentry [3] [4] proposed a candidate FHE scheme based on ideal lattices. The candidate FHE scheme means a somewhat homomorphic scheme that supports only a bounded amount of homomorphic computation on fresh ciphertexts, then, one applies the bootstrapping transformation to convert the scheme into one that can handle unbounded homomorphic computation. Gentry's breakthrough seminal work generated tremendous excitement and was quickly followed by many works [5]-[16]. Despite significant advances, bootstrapping is computationally quite expensive, because it involves homomorphically evaluating the entire decryption function. In addition, bootstrapping for unbounded FHE requires one to make a "circular security" assumption, *i.e.*, it is secure to reveal an encryption of the secret key under itself. So far, such assumptions are poorly understood, and we have little theoretical evidence to support them, in particular, no worst-case hardness. Because of this, Peikert [2] put out two open problems relating to unbounded FHE as follows.

- **Open Question 10:** Is there an unbounded FHE scheme that does not rely on bootstrapping? Is there a version of bootstrapping that uses a lighter-weight computation than full decryption?
- **Open Question 11:** Is there an unbounded FHE scheme that can be proved secure solely under a worst-case complexity assumption?

1.2. The FHE Schemes from LWE Distribution

To date, all known full homomorphic encryption schemes follow the same basic template from Gentry's initial work [3]. In a sequence of work, Brakerski and Vaikuntanathan [7] [8] gave a "second generation" of FHE constructions based on LWE distribution [17] [18]. In 2013, Gentry, Sahai, and Waters [19] proposed another interesting LWE-based FHE scheme that has some unique and advantageous properties. For example, the GSW Scheme can be used to bootstrap with

only a small polynomial-factor growth in the error rate. We describe these schemes in detail here.

- **BV FHE Scheme** Let $1 < t < q$ be two positive integers such that $(t, q) = 1$. In the BV system, a secret key s is an LWE secret and encrypts a plaintext $u \in \mathbb{Z}_t$ using an LWE sample for modulus q. We use the most significant bit encoding to obtain a ciphertext c by

$$\langle c, s \rangle \equiv_\chi \lfloor \frac{qu}{t} \rceil (\bmod\, q),$$

where χ is a discrete Gauss distribution over $\mathbb{Z}_q$, and $\lfloor x \rceil$ is the rounding of a real number x to the nearest integer. We use secret key s to decrypt the ciphertext c by

$$f^{-1}(c) \equiv_\chi \lfloor \frac{t}{q} \cdot \langle c, s \rangle \rceil (\bmod\, t).$$

Obviously, one has $f^{-1}(c) = u$ (see [20]). To explain this scheme is a somewhat FHE scheme, we may use the least significant bit encoding of the message (The equivalence of two encodings is referred to in **Appendix A** of [21]). In fact, the ciphertext c satisfies

$$\langle s, c \rangle \equiv_\chi m (\bmod\, q), \text{ and } m \in \{nt + u \mid n \in \mathbb{Z}\} \cap \left(-\frac{q}{2}, \frac{q}{2} \right).$$

To decrypt c, one just compute $\langle s, c \rangle \in \mathbb{Z}_q$, lifts the result to its unique representative m in $\mathbb{Z} \cap \left[-\frac{q}{2}, \frac{q}{2} \right)$, and the outputs $u \equiv m (\bmod\, t)$. It is easily seen that the homomorphic computation on ciphertext c induces some noises, which, if too large, will destroy the plaintext. Therefore, the bootstrapping technique that re-encrypts a ciphertext and reduces the noise level remains the only known way of building the unbounded FHE schemes.

- **GSW FHE Scheme** The GSW FHE scheme is presented most simply in terms of the gadget-based trapdoor described in [22] [23] [24] [25] [26]. The heart of the GSW scheme is the following additive and multiplicative homomorphisms for tags and trapdoors. Let $\bar{A} \in \mathbb{Z}_q^{n \times \bar{m}}$ be LWE samples with a secret key $\bar{s} \in \mathbb{Z}_q^{n-1}$, and for $i = 1, 2$, let

$$A_i = x_i G - \bar{A} R_i,$$

where $x_i \in \mathbb{Z}_q$, G is the block-diagonal gadget matrix of dimension $n \times nl$, $R_i \in \mathbb{Z}_q^{\bar{m} \times n}$ are random Gauss matrices over $\mathbb{Z}_q$, and $\bar{m} = n + nl$ (see p.50 of [2]). Since $\begin{pmatrix} R_i \\ I_n \end{pmatrix}$ is a trapdoor with a tag $x_i I_n$ for matrix $[\bar{A}, A_i]$, it is easy to verify that

$$A_1 + A_2 = (x_1 + x_2) G - \bar{A}(R_1 + R_2)$$

and

$$A_1 G^{-1}(A_2) = x_1 x_2 G - \bar{A} \underbrace{(R_1 G^{-1}(A_2) + x_1 R_2)}_{R}.$$

In other words, $\begin{pmatrix} R_1 + R_2 \\ I_n \end{pmatrix}$ is a trapdoor with a tag $(x_1 + x_2)I_n$ for matrix $\left[\bar{A}, A_1 + A_2 \right]$, and $\begin{pmatrix} R \\ I_n \end{pmatrix}$ is a trapdoor with a tag $x_1 x_2 I_n$ for matrix $\left[\bar{A}, A_1 G^{-1}(A_2) \right]$. Even with all of the above techniques, homomorphic operations always increase the error rate of a ciphertext, by as much as a polynomial factor per operation. Therefore, the schemes described here can only homomorghically evaluate circuits of an a-priori bounded depth.

1.3. The FHE Schemes from Ring-LWE

Several constructions based on Ring-LWE are today among the most promising FHE candidates. There are three most popular FHE schemes from Ring-LWE: (1) TFHE [27] [28] particularly suitable for combinatorial operations on individual slots and tolerating large noise and thus, large multiplicative depth; (2) B/FV [5] [29] [30] allowing to perform large vectorial arithmetic operations as long as the multiplicative depth of the evaluated circuit remains small; (3) HEAAN [31] [32]—a mixed encryption scheme shown to be very efficient for floating-point computations. We introduce these schemes slightly in detail as follows.

- **TFHE Scheme** TFHE consists of three major encryption/decryption schemes, each represented by a different plaintext space. First, the scheme TLWE encrypts messages over the entire torus $\mathbb{T}$ and produces ciphertexts in $\mathbb{T}^{N+1}$. The other two schemes are:

  - TRGSW encrypts elements of the ring $\mathcal{R}_{\mathbb{Z}}$ (integer polynomials) with bounded l^{∞}-norms (of the corresponding vectors in $\mathbb{Z}^N$ under the natural identification $\mathcal{R} \simeq \mathbb{Z}^N$).
  - TRLWE encrypts elements μ of the $\mathcal{R}_{\mathbb{Z}}$-module $\mathbb{T}_{\mathcal{R}}$ that can also be viewed as elements of $\mathbb{T}^N$ via the natural bijection $\mathbb{T}_{\mathcal{R}} \simeq \mathbb{T}^N$.

  There is an external product $\boxdot_\alpha$ depending on a noise parameter α (see Corollary 3.14 [28]) which yields a FHE module structure on the schemes TRGSW and TRLWE.

  In TFHE, TLWE ciphertexts of a message $\mu \in \mathbb{T}$ have the form $(a, b = \langle s, a \rangle + \mu + e) \in \mathbb{T}^{N+1}$ where $s \in \{0,1\}^N$ is the secret key, $a \in \mathbb{T}^N$ is uniformly random and $e \in \mathbb{T}$ is sampled according to a noise distribution centered at zero. Similarly, for TRLWE, ciphertexts of $\mu \in \mathbb{T}_{\mathcal{R}}$ are of the form $(a, b = s \cdot a + \mu + e) \in \mathbb{T}_{\mathcal{R}}^2$ where $s \in \mathcal{B}$, $a \in \mathbb{T}_{\mathcal{R}}$ is uniformly random and $e \in \mathbb{T}_{\mathcal{R}}$.

  The decryption in TLWE (resp. TRLWE) uses a secret κ-Lipschitz function (here, $\kappa > 0$ is small and we mean "with respect to the l^{∞}-norm on the torus") $\varphi_s : \mathbb{T}^N \times \mathbb{T} \to \mathbb{T}$ (resp. $\varphi_s : \mathbb{T}_{\mathcal{R}} \times \mathbb{T}_{\mathcal{R}} \to \mathbb{T}_{\mathcal{R}}$) called phase parametrized by a small (often binary) secret key $s \in \{0,1\}^N$ (resp. $s \in \mathcal{B}$) and defined by $(a, b) \in \mathbb{T}^N \times \mathbb{T} \to b - \langle s, a \rangle$ (resp. $(a, b) \to b - s \cdot a$). The fact that the phrase is a κ-Lipschitz function for small $\kappa \leq N + 1$ makes the decryption tolerant to errors and allows working with approximated numbers.

Ciphertexts are either fresh (*i.e.*, generated by directly encrypting a plaintext) or they are produced by a sequence of homomorphic operations. In both cases, one views the ciphertext as a random variable depending on the random coins used to generate a and e as well as all random coins used in all these homomorphic operations.

Since $\varphi_s(a,b) = b - s \cdot a = \mu + e$, the decryption μ and the noise parameter α are the mean and the standard deviation of the phase function $\varphi_s(a,b)$, respectively (here, the mean and standard deviation are computed over the random coins in the encryption algorithm).

- **B/FV Scheme** In this scheme, the message space is the finite ring $\mathcal{R}_p = \mathbb{Z}_p[x] / \langle x^N + 1 \rangle$ for some integer p (typically a power of 2 or a prime number). A message $\mu \in \mathcal{R}_p$ is encrypted on a quotient ring $\mathcal{R}_q$ (for a larger modulus q) as a ciphertext $(a,b) \in \mathcal{R}_q^2$ where $a \in \mathcal{R}_q$ is chosen uniformly at random and b is sampled from $\mathcal{D}_{\mathcal{R}_q, \sigma, s \cdot a + \frac{p}{q}\mu}$. Here, $\mathcal{D}_{\mathcal{R}_q, \sigma, \mu}$ is the discrete Gaussian distribution over $\mathcal{R}_q$ centered at μ with standard deviation σ (discrete means that the values are integers only). In addition, $s \in \mathcal{B}$ is the secret key.

Homomorphic addition of two ciphertexts (a_1, b_1) and (a_2, b_2) is achieved by component-wise addition. The idea behind the homomorphic multiplication of two ciphertexts (a_1, b_1) and (a_2, b_2) is a technique referred to as relinearization: one first lifts $(a_i, b_i) \in \mathcal{R}_q^2$ to $(\tilde{a}_i, \tilde{b}_i) \in \mathcal{R}^2$ where each coefficient is lifted to $[-q/2, q/2)$ and then views of μ_i as being expressed as a linear polynomial on s (*i.e.*, $\mu_i \sim \frac{p}{q}(b_i + s \cdot a_i)$). One then computes the quadratic polynomial corresponding to the product, namely $\frac{p}{q}(b_1 + s \cdot a_1) \cdot \frac{p}{q}(b_2 + s \cdot a_2)$, and uses the relinearization described in [30] to write this product as $\frac{p}{q}(b + s \cdot a)$ and determine the coefficients $(a,b) \in \mathcal{R}_q$.

The noise amplitude grows by a small factor $O(N)$ on average after each multiplication, so it is a common practice to perform a modulus-rescaling step, that divides and rounds each coefficient as well as the modulus q by the same scalar in order to bring the noise amplitude back to $O(1)$ so that the subsequent operations continue on smaller ciphertexts.

- **HEAAN Scheme** In this scheme, the message space is the subset of $\mathcal{R}_q$ containing all elements of norm $\leq B$ for some bound B, where the norm of an element $x \in \mathcal{R}_q$ is defined as $\|\tilde{x}\|_\infty$. Here $\tilde{x} \in \mathcal{R}_\mathbb{R}$ is the minimal lift of x, *i.e.*, coefficients lifted to $[-q/2, q/2)$. The message is decrypted up to a constant number of the least significant bits which are considered as noise.

A HEAAN ciphertext is also a Ring-LWE pair $(a,b) \in \mathcal{R}_q^2$ where $a \in \mathcal{R}_q$ is uniformly random and b is equal to $s \cdot a + \mu$ up to a Gaussian error of small standard deviation. This time, plaintexts and ciphertexts share the same space,

so no rescaling factor p/q is used. Multiplication of two messages uses the same formula as in B/FV including relinearization: if both input messages are bounded by B with $O(1)$ noise, the product is a message bounded by B^2 with noise $O(B)$, so it is a common practice at this point to perform a modulusrescaling step that divides everything by B to bring the noise back to $O(1)$ (see [32]). Unlike B/FV, this division in the modulus switching scales not only the ciphertext but also the plaintext by B. This can be fixed by adding a (public) tag to the ciphertext to track the number of divisions by B performed.

Recently, Boura, Gama, Georgieva, and Jetchev [33] proposed a practical hybrid solution for combining and switching between the above three Ring-LWE-based FHE schemes. They achieved it by first mapping the different plaintext spaces to a common algebra structure and then by applying efficient switching algorithms. This approach has many practical applications, for example, it becomes an integral tool for the recent standardization initiatives of homomorphic schemes and common APIs.

1.4. Other Related Works

At Eurocrypt 2010, van Dijk, Gentry, Halevi, and Vaikuntanathan [34] described a fully homomorphic encryption scheme over the integers (see also [9] [10] [11]). As in Gentry's scheme, the authors first describe a somewhat homomorphic scheme supporting a limited number of additions and multiplications over encrypted bits. Then they apply Gentry's squash decryption technique to get a bootstrappable scheme and then Gentry's ciphertext refresh procedure to get a full homomorphic scheme. The main appeal of the scheme (compared to the original Gentry's scheme) is its conceptual simplicity, namely, all operations are done over those integers instead of ideal lattices. However, the public key was too large for any practical system. In [10] and [11], the authors reduced the public key site from $\tilde{\mathcal{O}}(\lambda^{10})$ to $\tilde{\mathcal{O}}(\lambda^7)$ by encrypting with a quadratic form in the public key elements, instead of a linear form.

It is the latest scheme, without using noise reduction techniques (see [35]). In 2015, Yagisawa proposed a non-associative octonion ring over a finite field fully homomorphic encryption scheme [36]. This scheme's cryptographic robustness is based on the complexity of multivariate algebraic equations with high degree. In his next paper, he developed some improvements to the scheme [37]. Liu presented a symmetric fully homomorphic encryption scheme based on non-commutative rings [38]. Liu's scheme provides an arbitrary number of additions and multiplications, and the correct decryption in contempt of the amount of noise reduction mechanisms and based on the approximating-GCD complexity. Noise-free symmetric fully homomorphic encryption scheme was proposed by Li and Wang [39] that used matrices over non-commutative rings. Needless to say, those noise-free schemes are not the solutions to problems of the FHE scheme, because of using non-associative and non-commutative rings for the plaintexts and ciphertexts.

1.5. Our Contribution

Our contribution to the unbounded FHE scheme is straightforward, which is completely different from Gentry's initial construction. More precisely, our FHE scheme can handle unbounded homomorphic computation on any refreshed ciphertexts without bootstrapping transformation. This is a rational solution to open problems on fully homomorphic encryption.

Our solution comes in three steps. First, we provide a general noise-free construction based on ideal lattices and the Chinese Remainder Theorem, which includes three efficient algorithms for generating secret key, public key and decryption. The plaintext space is the direct sum of rings $\mathbb{Z}_{t_i}$, where t_i is the one-dimensional modulus of each ideal lattice I_i ($1 \leq i \leq m$). The ciphertext space $\mathbb{Z}^n$ is a commutative ring with the addition and convolutional product $\otimes$ of vectors, needless to say, the algebraic structures for homomorphic computation are simplest. The main ideal is to set up a multiplicative operation for $\mathbb{Z}^n$, such that $\mathbb{Z}^n$ becomes a commutative ring, therefore, one views $I \subset \mathbb{Z}^n$ both as an ideal and as a lattice in $\mathbb{Z}^n$, in particular, $\mathbb{Z}^n/I$ becomes a quotient ring. Working with the ring $(\mathbb{Z}^n, +, \otimes)$, we can efficiently utilize the Chinese Remainder Theorem for generating of public key. Next, we provide a probabilistic algorithm for public keys, so that the encryption algorithms are secure against indistinguishable under chosen-plaintext attacks, namely, our scheme is IND-CPA secure. Finally, we discuss the IND-CCA security of our scheme based on the general compact knapsacks problem for arbitrary rings, we show that the security is solely under the worst-case complexity assumption. This is also a solution to open question 11 of Peikert [2]. In the last section of this paper, we provide a practical system based on some basic results from cyclotomic fields [40]. The novelty of this practical system is to establish a connection between a cryptosystem and the ancient hard problem in mathematics: how to find a solution to an algebraic equation with a high degree. By the famous Galois theory, there is no general method to find a solution when the degree of an algebraic equation is bigger than 5.

The generalization of compact knapsack problem for arbitrary ring may be described as follows: given m ring elements $a_1, a_2, \cdots, a_m \in R$ and a target value $b \in R$, find coefficients $x_1, x_2, \cdots, x_m \in X \subset R$ such that $\sum_{i=1}^{m} a_i x_i = b$. The computational complexity of this problem depends on the choice of ring R and the size of X. This problem is known to be solvable in quasi polynomial time when R is the ring of integers and X is the set of small integers $\{0, 1, \cdots, 2^{m-1}\}$ (see [41] and [42]). Micciancio [42] studied the knapsack problem when R is an appropriately chosen ring of modulo polynomials and X is the subset of polynomials with small coefficients, he has shown that the complexity is as hard to solve on the average as the worst-case instance of approximating the covering radius of any cyclic lattice within a polynomial factor.

We generalize this result to any ideal lattices, such that our FHE scheme is as hard to solve on the average as the worst case of approximating the covering

radius of any ideal lattices.

2. The General Construction without Disturbance

Let $\mathbb{Z}[x]$ be the ring of integer coefficients polynomials with variable *x*, $\phi(x) \in \mathbb{Z}[x]$, and $\phi(x) = x^n - \phi_{n-1}x^{n-1} - \cdots - \phi_1 x - \phi_0$ with $\phi_0 \neq 0$ be a given polynomial, $\langle \phi(x) \rangle$ be the principal ideal generated by $\phi(x)$ in $\mathbb{Z}[x]$, $R = \mathbb{Z}[x]/\langle \phi(x) \rangle$ be the quotient ring. Let $\mathbb{R}^n$ be the *n* dimensional Euclidean space, and $\mathbb{Z}^n \subset \mathbb{R}^n$ be all of integer vectors in $\mathbb{R}^n$. We use column notation for vectors in $\mathbb{R}^n$.

There is a one to one correspondence between the quotient ring $\mathbb{Z}[x]/\langle \phi(x) \rangle$ and all the integer vectors $\mathbb{Z}^n$:

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{Z}[x]/\langle \phi(x) \rangle \xrightarrow{\tau} a = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \in \mathbb{Z}^n, \qquad (2.1)$$

we write $\tau(a(x)) = a$, or $\tau^{-1}(a) = a(x)$. Since $\tau(a(x) + b(x)) = \tau(a(x)) + \tau(b(x))$, τ is an isomorphism of additive groups in fact. To regard τ as an isomorphism of rings, we need to define a multiplicative operator in $\mathbb{Z}^n$. To do this, let the rotation matrix $H = H_\phi$ be given by

$$H = \begin{pmatrix} 0 & \cdots & 0 & \phi_0 \\ & & & \phi_1 \\ & I_{n-1} & & \vdots \\ & & & \phi_{n-1} \end{pmatrix}$$

where I_{n-1} is the unit matrix of $n-1$ dimension.

DEFINITION 2.1 For any $\alpha \in \mathbb{R}^n$, the ideal matrix generated by α is defined by

$$H^*(\alpha) = \left[\alpha, H\alpha, \cdots, H^{n-1}\alpha \right] \in \mathbb{R}^{n \times n}.$$

Some basic properties about ideal matrix may be described as the following lemma, its proof is referred to Lemma 2.5 of [43], or Lemma 5.2.4 of [44].

Lemma 2.1 Let $\alpha = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix}$ and $\beta = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix}$ be any two vectors in $\mathbb{R}^n$, then

one has

(i) $H^*(\alpha) = \alpha_0 I_n + \alpha_1 H + \cdots + \alpha_{n-1}H^{n-1}$;

(ii) $H^*(\alpha)H^*(\beta) = H^*(\beta)H^*(\alpha)$;

(iii) $H^*(\alpha)H^*(\beta) = H^*\left(H^*(\alpha)\beta\right)$;

(iv) $\det\left(H^*(\alpha)\right) = \prod_{i=1}^{n} \alpha(\omega_i)$;

where $\det\left(H^*(\alpha)\right)$ is the determinant of $H^*(\alpha)$, $\alpha(x) = \tau^{-1}(\alpha)$, and $\omega_1, \omega_2, \cdots, \omega_n$ are *n* roots of $\phi(x)$.

By (iv) of Lemma 2.1, $H^*(\alpha)$ is an invertible matrix if and only if $\alpha(x)$ and $\phi(x)$ have no common roots in complex numbers field. Now, we may define a multiplicative operator in $\mathbb{Z}^n$ in terms of the ideal matrix.

DEFINITION 2.2 Let $\alpha, \beta \in \mathbb{Z}^n$ be two integer vectors, we define the convolutional product $\alpha \otimes \beta$ by

$$\alpha \otimes \beta = H^*(\alpha)\beta.$$

Obviously, under the convolutional product $\alpha \otimes \beta$, $\mathbb{Z}^n$ becomes a commutative ring with the unit element $e = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{Z}^n$, since $\alpha \otimes \beta = \beta \otimes \alpha$ and

$$\alpha \otimes e = e \otimes \alpha = \alpha, \quad \forall \alpha \in \mathbb{Z}^n.$$

Sometimes, we write this ring by $(\mathbb{Z}^n, +, \otimes) = \mathbb{Z}^n$.

Lemma 2.2 The correspondence τ given by (2.1) is a ring isomorphism between $\mathbb{Z}^n / \langle \phi(x) \rangle$ and $\mathbb{Z}^n$, namely, we have

$$\mathbb{Z}[x] / \langle \phi(x) \rangle \cong (\mathbb{Z}^n, +, \otimes).$$

Proof. By Lemma 2.4 of [43] or Lemma 5.2.5 of [44], it is easy to see that

$$\tau(\alpha(x) + \beta(x)) = \alpha + \beta = \tau(\alpha(x)) + \tau(\beta(x)),$$
$$\tau(\alpha(x)\beta(x)) = \alpha \otimes \beta = \tau(\alpha(x)) \otimes \tau(\beta(x)).$$

The conclusion follows immediately.

According to the definition of ideal lattices [2] [42] [45] [46] [47] [48], an ideal lattice $I \subset \mathbb{Z}^n$, just is an ideal of $(\mathbb{Z}^n, +, \otimes)$, we view $I \subset \mathbb{Z}^n$ both as an ideal of $\mathbb{Z}^n$ and as a lattice in $\mathbb{Z}^n$, in particular, $\mathbb{Z}^n / I$ is a quotient ring.

A lattice $I \subset \mathbb{R}^n$ is a discrete additive group of $\mathbb{R}^n$ [46] [49] [50], we write $I = \mathcal{L}(B)$ as usual, where $B = [\beta_1, \beta_2, \cdots, \beta_n] \in \mathbb{R}^{n \times n}$ is the generated matrix or a basis of *I*. All lattices we discuss here are the full rank lattice, it means that $\det(B) \neq 0$. If $I \subset \mathbb{Z}^n$, then *I* is called an integer lattice. The Hermite Normal Form base B [40] [51] for an integer lattice is an upper triangular matrix $B = (b_{ij})_{n \times n} \in \mathbb{Z}^{n \times n}$ satisfying $b_{ii} \geq 1$ ($1 \leq i \leq n$) and

$$b_{ij} = 0, \text{ if } 0 \leq j < i \leq n, \text{ and } 0 \leq b_{ij} < b_{ii}, \text{ if } 0 \leq i < j \leq n.$$

It is known that there is a unique HNF basis for an integer lattice and its Gram-Schmidt orthogonal basis is a diagonal matrix, more precisely, if $B = [\beta_1, \beta_2, \cdots, \beta_n]$ is the HNF basis of an integer lattice, $B^* = \left[\beta_1^*, \beta_2^*, \cdots, \beta_n^* \right]$ is the corresponding orthogonal basis obtained by Gram-Schmidt orthogonal method, then $B^* = \text{diag}\{b_{11}, b_{22}, \cdots, b_{nn}\}$ is a diagonal matrix (see Lemma 7.26 of [40]).

DEFINITION 2.3 b_{11} is called the one dimensional modulus of an ideal lattice $I = \mathcal{L}(\beta_1, \beta_2, \cdots, \beta_n)$, and denoted by $t(I) = b_{11}$.

Let $I \subset (\mathbb{Z}^n, +, \otimes)$ be an ideal lattice, to obtain a set of representative elements for the quotient ring $\mathbb{Z}^n / I$, we use the notation of orthogonal parallelepiped due

to Micciancio [51]. The following lemma is referred to as Lemma 7.45 and (7.131) of [40], or §4.1 of [51], and a proof will be appeared in Lemma 2.6 below.

Lemma 2.3 Suppose that $I = \mathcal{L}(B)$ is a full rank ideal of $\mathbb{Z}^n$, B is the HNF basis of I, and $B^* = \mathrm{diag}\{b_{11}, b_{22}, \cdots, b_{nn}\}$ is the corresponding orthogonal basis, then a set of representative elements of the quotient ring $\mathbb{Z}^n / I$ is

$$\mathcal{F}(I) = \left\{ x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Z}^n \mid 0 \le x_i < b_{ii}, 1 \le i \le n \right\},$$

and $\mathcal{F}(I)$ is called the orthogonal parallelepiped of I.

Next, we turn to discuss the ideal lattices and the ring $(\mathbb{Z}^n, +, \otimes)$. Let $\alpha \in \mathbb{Z}^n$ be a given vector, the principal ideal lattice $\langle \alpha \rangle$ is a principal ideal generated by α in $\mathbb{Z}^n$. It is easily verified that

$$\langle \alpha \rangle = \left\{ \alpha \otimes x \mid x \in \mathbb{Z}^n \right\} = \mathcal{L}\left(H^*(\alpha) \right).$$

Thus, the generated matrix of a principle ideal lattice $\langle \alpha \rangle$ just is the ideal matrix generated by α.

The operations among the ideal lattices in $(\mathbb{Z}^n, +, \otimes)$ are defined as usual, in particular, the addition and multiplication for two ideals, I and J are defined by

$$I + J = \left\{ \alpha + \beta \mid \alpha \in I, \beta \in J \right\},$$

$$IJ = \left\{ \sum_{i < \infty} \alpha_i \otimes \beta_i \mid \alpha_i \in I, \beta_i \in J \right\},$$

and

$$I \cap J = \left\{ \gamma \mid \gamma \in I, \text{ and } \gamma \in J \right\}.$$

Since $I + J$, IJ and $I \cap J$ are also the ideals of $\mathbb{Z}^n$, therefore, all of them are ideal lattices.

DEFINITION 2.4 Let $I \subset \mathbb{Z}^n$, $J \subset \mathbb{Z}^n$ be two ideal lattices. If $I + J = \mathbb{Z}^n$, we call I and J to be relatively prime, and denoted by $(I, J) = 1$.

It is easy to see that two ideal lattices I and J are relatively prime, if and only if there are $\alpha \in I$ and $\beta \in J$ such that $\alpha + \beta = e$, where e is the unit element of $(\mathbb{Z}^n, +, \otimes)$.

To construct a FHE scheme, we utilize the Chinese Remainder Theorem in the ring $(\mathbb{Z}^n, +, \otimes)$, which is a well-known theorem in Number Theory.

THEOREM 1 (Chinese Remainder Theorem) Let $I_1, I_2, \cdots, I_m$ be pairwise relatively prime ideal lattices in $\mathbb{Z}^n$, and $\alpha_1, \alpha_2, \cdots, \alpha_m \in \mathbb{Z}^n$ be m target vectors in $\mathbb{Z}^n$, then there exists a common solution of the following congruences:

$$x \equiv \alpha_i \pmod{I_i}, 1 \le i \le m,$$

and the solution of $x \in \mathbb{Z}^n$ is a unique modulo-ideal lattice $I_1 \cap I_2 \cdots \cap I_m$.

For arbitrary pairwise relatively prime lattices $I_1, I_2, \cdots, I_m$, it is known that

$$I_1 \cap I_2 \cdots \cap I_m = I_1 I_2 \cdots I_m.$$

By the above Chinese Remainder Theorem, one has the following consequence immediately.

Corollary 2.1 Suppose that $I_1, I_2, \cdots, I_m$ are pairwise relatively prime ideal lattices in $\mathbb{Z}^n$, then we have the following ring isomorphism

$$\mathbb{Z}^n / I_1 I_2 \cdots I_m \cong \mathbb{Z}^n / I_1 \oplus \mathbb{Z}^n / I_2 \oplus \cdots \oplus \mathbb{Z}^n / I_m. \qquad (2.2)$$

The right-hand side of (2.2) is the direct sum of m quotient ring $\mathbb{Z}^n / I_i$ ($1 \le i \le m$), and the addition and multiplication of $\bigoplus_{i=1}^{m} \mathbb{Z}^n / I_i$ are given by

$$(a_1, a_2, \cdots, a_m) + (b_1, b_2, \cdots, b_m) = (a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m)$$

and

$$(a_1, a_2, \cdots, a_m) \otimes (b_1, b_2, \cdots, b_m) = (a_1 \otimes b_1, a_2 \otimes b_2, \cdots, a_m \otimes b_m).$$

Proof. Since $I_1, I_2, \cdots, I_m$ are pairwise prime, by Theorem 1, there are m vectors A_i ($1 \le i \le m$) in $\mathbb{Z}^n$ such that

$$A_i \equiv e \pmod{I_i}, \text{ and } A_i \equiv 0 \pmod{I_j}, \text{ if } j \ne i.$$

For any $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_m) \in \mathbb{Z}^n / I_1 \oplus \mathbb{Z}^n / I_2 \oplus \cdots \oplus \mathbb{Z}^n / I_m$, by Theorem 1 again, there is a unique solution $x \in \mathbb{Z}^n / I_1 I_2 \cdots I_m$ such that

$$\begin{cases} x \equiv \alpha_1 \pmod{I_1} \\ \quad \vdots \\ x \equiv \alpha_m \pmod{I_m} \end{cases}$$

We define $f(\alpha) = x$, which is the ring isomorphism from $\mathbb{Z}^n / I_1 \oplus \mathbb{Z}^n / I_2 \oplus \cdots \oplus \mathbb{Z}^n / I_m$ to $\mathbb{Z}^n / I_1 I_2 \cdots I_m$ as we desired. Using $A_1, A_2, \cdots, A_m$, one may clearly write down f by

$$f(\alpha) = f((\alpha_1, \alpha_2, \cdots, \alpha_m)) = \alpha_1 \otimes A_1 + \cdots + \alpha_m \otimes A_m.$$

Let $\beta = (\beta_1, \beta_2, \cdots, \beta_m)$ be another element of $\bigoplus_{i=1}^{m} \mathbb{Z}^n / I_i$, it is easy to see that

$$\begin{aligned} f(\alpha + \beta) &= f((\alpha_1 + \beta_1, \alpha_2 + \beta_2, \cdots, \alpha_m + \beta_m)) \\ &= \alpha_1 \otimes A_1 + \cdots + \alpha_m \otimes A_m + \beta_1 \otimes A_1 + \cdots + \beta_m \otimes A_m \\ &= f(\alpha) + f(\beta). \end{aligned}$$

To verify $f(\alpha \otimes \beta) = f(\alpha) \otimes f(\beta)$, since

$$f(\alpha) \equiv \alpha_i \pmod{I_i}, \text{ and } f(\beta) \equiv \beta_i \pmod{I_i}, 1 \le i \le m.$$

It follows that

$$f(\alpha) \otimes f(\beta) \equiv \alpha_i \otimes \beta_i \pmod{I_i}, 1 \le i \le m.$$

By the definition of f, we have

$$f(\alpha \otimes \beta) = f((\alpha_1 \otimes \beta_1, \alpha_2 \otimes \beta_2, \cdots, \alpha_m \otimes \beta_m)) = f(\alpha) \otimes f(\beta).$$

This proves that f is a ring isomorphism.

We extend the inverse isomorphism f^{-1} to the whole space $\mathbb{Z}^n$ by

$f^* = f \circ \pi :$

$$f^* : \mathbb{Z}^n \xrightarrow{\pi} \mathbb{Z}^n / I_1 I_2 \cdots I_m \xrightarrow{f^{-1}} \bigoplus_{i=1}^{m} \mathbb{Z}^n / I_i,$$

where π is the natural homomorphism from $\mathbb{Z}^n$ to its quotient ring $\mathbb{Z}^n / I_1 I_2 \cdots I_m$. It is easy to see that f^* is a homomorphism from $\mathbb{Z}^n$ to $\bigoplus_{i=1}^{m} \mathbb{Z}^n / I_i$, and

$$f^*\big(f(u)\big) = f^{-1}\big(f(u)\big) = u, \; \forall u \in \bigoplus_{i=1}^{m} \mathbb{Z}^n / I_i, \tag{2.3}$$

f^* will play the role of decryption in our scheme, and always write down f^* by f^{-1} in the following discussion.

Since $\mathbb{Z}$ is a ring, we wish to embed this ring into $\big(\mathbb{Z}^n, +, \otimes\big)$. To do this, we define an embedding mapping from $\mathbb{Z}$ to $\mathbb{Z}^n$ by

$$\forall a \in \mathbb{Z}, a \to \overline{a} = \begin{pmatrix} a \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{Z}^n. \tag{2.4}$$

Lemma 2.4 Under the embedding mapping $a \to \overline{a}$, $\mathbb{Z}$ becomes a subring of $\big(\mathbb{Z}^n, +, \otimes\big)$, namely, for any $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, one has $\overline{a+b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a} \otimes \overline{b}$.

Proof. By (2.4), we have

$$\overline{a+b} = \begin{pmatrix} a+b \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} b \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \overline{a} + \overline{b}$$

and

$$\overline{a} \otimes \overline{b} = \begin{pmatrix} ab \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \overline{a \cdot b},$$

the lemma follows at once.

Lemma 2.5 Let $I \subset \mathbb{Z}^n$ be an ideal lattice, and $t = t(I)$ be its one dimensional modulus given by DEFINATION 2.3. Then, for any $a, b \in \mathbb{Z}$, we have

$$a \equiv b \,(\mathrm{mod}\, t) \Leftrightarrow \overline{a} \equiv \overline{b} \,(\mathrm{mod}\, I).$$

Proof. By assumption, *I* is a full rank lattice and its HNF basis may be written by

$$B = \begin{pmatrix} b_{11} & * & * & * \\ & b_{22} & * & * \\ & 0 & \ddots & * \\ & & & b_{nn} \end{pmatrix}.$$

If $\overline{a} \equiv \overline{b} \pmod I$, then there is a vector $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Z}^n$ such that

$$\overline{a} - \overline{b} = Bx = \begin{pmatrix} a-b \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since $b_{nn}x_n = 0$, and $b_{nn} \geq 1$, we have $x_n = 0$, similarly, since $b_{n-1,n-1}x_{n-1} + b_{n-1,n}x_n = 0$, it follows that $x_{n-1} = 0$. Therefore, we have $x_n = x_{n-1} = \cdots = x_2 = 0$, and $a - b = x_1 b_{11} = x_1 t \Rightarrow a \equiv b \pmod t$. Conversely, if $a \equiv b \pmod t$, then $a - b = qt$, and

$$\overline{a} - \overline{b} = B \begin{pmatrix} q \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in I \Rightarrow \overline{a} \equiv \overline{b} \pmod I.$$

The assertion is true.

For arbitrary given pairwise relatively prime ideal lattices $I_1, I_2, \cdots, I_m$, one uses the Chinese Remainder Theorem to generate the public key $A_1, A_2, \cdots, A_m$, where $A_i \in \mathbb{Z}^n (1 \leq i \leq m)$ such that

$$A_i \equiv e \pmod{I_i}, \text{ and } A_i \equiv 0 \pmod{I_j}, \text{ if } j \neq i, \tag{2.5}$$

where $e = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{Z}^n$ is the unit element of $(\mathbb{Z}^n, +, \otimes)$.

Now, we describe a scheme for unbounded fully homomorphic encryption as follows.

Algorithm 1: The General Unbounded FHE Scheme without Noises

- **Secret Key:** One selects m pairwise relatively prime ideal lattices $I_1, I_2, \cdots, I_m$ in $\mathbb{Z}^n$ as the decryption key.

- **Public Key:** Let $t_i = t(I_i)$ be the one dimensional modulus of $I_i (1 \leq i \leq m)$. The plaintexts space is the direct sum of ring $\mathcal{P} = \bigoplus_{i=1}^{m} \mathbb{Z}_{t_i}$, the addition and multiplication in $\mathcal{P}$ are given by

  $$(a_1, a_2, \cdots, a_m) + (b_1, b_2, \cdots, b_m) = (a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m),$$

  $$(a_1, a_2, \cdots, a_m) \cdot (b_1, b_2, \cdots, b_m) = (a_1 b_1, a_2 b_2, \cdots, a_m b_m).$$

  The public key for encryption is $\{A_1, A_2, \cdots, A_m\} \subset \mathbb{Z}^n$, and each A_i is given by (2.5).

Continued

- **Encryption:** For any plaintext $u = (u_1, u_2, \cdots, u_m) \in \mathcal{P} = \bigoplus\limits_{i=1}^{m} \mathbb{Z}_{t_i}$, the encryption function f is given by

$$c = f(u) = \overline{u_1} \otimes A_1 + \overline{u_2} \otimes A_2 + \cdots + \overline{u_m} \otimes A_m, \qquad (2.6)$$

  where $\overline{u_i}$ is the embedding of u_i.

- **Decryption:** For any ciphertext $c \in \mathbb{Z}^n$, we use the secret key $I_1, I_2, \cdots, I_m$ to decrypt c. Since for every i, $1 \le i \le m$, we have $c \equiv \overline{u_i} \pmod{I_i}$, and c mod I_i is a unique vector in the orthogonal parallelepiped $\mathcal{F}(I_i)$ of I_i, thus one has $c \bmod I_i = \overline{u_i}$, and by (2.3), we have

$$f^{-1}(c) = (u_1, u_2, \cdots, u_m) = u.$$

To verify the homomorphic addition and multiplication for the above scheme, by Lemma 2.4, $\mathbb{Z}$ is a subring of $(\mathbb{Z}^n, +, \otimes)$. By Lemma 2.5, we can embed the direct sum $\bigoplus\limits_{i=1}^{m} \mathbb{Z}_{t_i}$ into $\bigoplus\limits_{i=1}^{m} \mathbb{Z}^n / I_i$, so that $\bigoplus\limits_{i=1}^{m} \mathbb{Z}_{t_i}$ also is a subring of $\bigoplus\limits_{i=1}^{m} \mathbb{Z}^n / I_i$. Therefore, the property of fully homomorphism directly follows by f^* (or f^{-1}) a ring homomorphism:

$$\bigoplus\limits_{i=1}^{m} \mathbb{Z}_{t_i} \hookrightarrow \bigoplus\limits_{i=1}^{m} \mathbb{Z}^n / I_i \xrightarrow{f} \mathbb{Z}^n / I_1 I_2 \cdots I_m \xleftarrow{f^*} \mathbb{Z}^n.$$

More precisely, let $c_1 = f(u)$, and $c_2 = f(v)$ be arbitrary two ciphertexts, where $u = (u_1, u_2, \cdots, u_m) \in \bigoplus\limits_{i=1}^{m} \mathbb{Z}_{t_i}$, and $v = (v_1, v_2, \cdots, v_m) \in \bigoplus\limits_{i=1}^{m} \mathbb{Z}_{t_i}$, we note that for all i, $1 \le i \le m$,

$$c_1 + c_2 \equiv \overline{u_i} + \overline{v_i} \pmod{I_i}, \text{ and } c_1 \otimes c_2 \equiv \overline{u_i} \otimes \overline{v_i} \pmod{I_i}.$$

By Lemma 2.4, it follows that

$$c_1 + c_2 \equiv \overline{u_i + v_i} \pmod{I_i}, \text{ and } c_1 \otimes c_2 \equiv \overline{u_i v_i} \pmod{I_i}.$$

Therefore, by Lemma 2.5, we have

$$\begin{aligned}
f^{-1}(c_1 + c_2) &= (u_1 + v_1, u_2 + v_2, \cdots, u_m + v_m) \\
&= (u_1, u_2, \cdots, u_m) + (v_1, v_2, \cdots, v_m) \\
&= f^{-1}(c_1) + f^{-1}(c_2),
\end{aligned}$$

and

$$\begin{aligned}
f^{-1}(c_1 \otimes c_2) &= (u_1 v_1, u_2 v_2, \cdots, u_m v_m) \\
&= (u_1, u_2, \cdots, u_m)(v_1, v_2, \cdots, v_m) \\
&= f^{-1}(c_1) \cdot f^{-1}(c_2).
\end{aligned}$$

This is an unbounded fully homomorphic encryption as we desired.

How to decrypt the ciphertext $c \in \mathbb{Z}^n$ using the secret key $I_1, I_2, \cdots, I_m$ in our algorithm for the general unbounded FHE scheme? Here we give a lemma to show that there is only one vector $\overline{u_i} \in \mathbb{Z}^n$ in the orthogonal parallelepiped

$\mathcal{F}(I_i)$ of I_i such that $c \equiv \overline{u_i}(\bmod I_i)$, and give an algorithm to calculate $\overline{u_i}$ in detail.

Lemma 2.6 Given an ideal lattice I, for any vector $c \in \mathbb{Z}^n$, there is only one vector $w \in \mathcal{F}(I)$ such that $c \equiv w(\bmod I)$.

Proof. Assume $B = [\beta_1, \beta_2, \cdots, \beta_n]$ is the HNF basis of I, and $B^* = [\beta_1^*, \beta_2^*, \cdots, \beta_n^*]$ is the corresponding orthogonal basis of B. Write c as the linear combination of $[\beta_1^*, \beta_2^*, \cdots, \beta_n^*]$, *i.e.*

$$c = \sum_{i=1}^{n} c_i \beta_i^*, \ c_i = \frac{\langle c, \beta_i^* \rangle}{\langle \beta_i^*, \beta_i^* \rangle}.$$

Let $w = \sum_{i=1}^{n} c_i \beta_i^* - \sum_{i=1}^{n} k_i \beta_i$, $k_1, k_2, \cdots, k_n \in \mathbb{Z}$, then $c - w = \sum_{i=1}^{n} k_i \beta_i \in I$. Next, we prove that there is only one group of integers $k_1, k_2, \cdots, k_n$ such that $w \in \mathcal{F}(I)$, *i.e.*

$$w_i = \frac{\langle w, \beta_i^* \rangle}{\langle \beta_i^*, \beta_i^* \rangle} \in [0,1), \forall 1 \le i \le n.$$

Firstly, we determine the value of k_n. Since

$$w_n = \frac{\langle w, \beta_n^* \rangle}{\langle \beta_n^*, \beta_n^* \rangle} = c_n - k_n \frac{\langle \beta_n, \beta_n^* \rangle}{\langle \beta_n^*, \beta_n^* \rangle} = c_n - k_n,$$

therefore, when $k_n = [c_n]$, here $[x]$ means the largest integer no more than real number x, we have $w_n \in [0,1)$. Secondly, we determine k_{n-1}. Note that

$$w_{n-1} = \frac{\langle w, \beta_{n-1}^* \rangle}{\langle \beta_{n-1}^*, \beta_{n-1}^* \rangle} = c_{n-1} - k_{n-1} - k_n \frac{\langle \beta_n, \beta_{n-1}^* \rangle}{\langle \beta_{n-1}^*, \beta_{n-1}^* \rangle},$$

so there is only one integer

$$k_{n-1} = \left[c_{n-1} - [c_n] \frac{\langle \beta_n, \beta_{n-1}^* \rangle}{\langle \beta_{n-1}^*, \beta_{n-1}^* \rangle} \right]$$

such that $w_{n-1} \in [0,1)$. Similarly, we could determine any k_i, $\forall 1 \le i \le n-1$,

$$w_i = \frac{\langle w, \beta_i^* \rangle}{\langle \beta_i^*, \beta_i^* \rangle} = c_i - k_i - \frac{\left\langle \sum_{j=i+1}^{n} k_j \beta_j, \beta_i^* \right\rangle}{\langle \beta_i^*, \beta_i^* \rangle},$$

hence, there is only one integer

$$k_i = \left[c_i - \frac{\left\langle \sum_{j=i+1}^{n} k_j \beta_j, \beta_i^* \right\rangle}{\langle \beta_i^*, \beta_i^* \rangle} \right]$$

such that $w_i \in [0,1)$, $\forall 1 \le i \le n-1$. Above all, there is only one vector

$$w = \sum_{i=1}^{n} c_i \beta_i^* - \sum_{i=1}^{n} k_i \beta_i \in \mathcal{F}(I) \text{ such that } c \equiv w(\bmod I).$$

Based on Lemma 2.6, we give an algorithm for the decryption of our general FHE scheme.

Algorithm 2: Decryption Algorithm for FHE Scheme

- For any ciphertext $c \in \mathbb{Z}^n$, given a full rank ideal lattice I_i with HNF basis $B = [\beta_1, \beta_2, \cdots, \beta_n]$ and the corresponding orthogonal basis $B^* = [\beta_1^*, \beta_2^*, \cdots, \beta_n^*]$, we can find only one vector $\overline{u}_i = c - \sum_{i=1}^{n} k_i \beta_i \in \mathcal{F}(I)$ such that $c \equiv \overline{u}_i \pmod{I_i}$, where

$$k_n = \left[\frac{\langle c, \beta_n^* \rangle}{\langle \beta_n^*, \beta_n^* \rangle} \right], k_i = \left[\frac{\langle c, \beta_i^* \rangle}{\langle \beta_i^*, \beta_i^* \rangle} - \frac{\left\langle \sum_{j=i+1}^{n} k_j \beta_j, \beta_i^* \right\rangle}{\langle \beta_i^*, \beta_i^* \rangle} \right], i = n-1, n-2, \cdots, 1.$$

To create an efficient algorithm for generating the secret key of the above unbounded FHE scheme, we assume that $\phi(x)$ is an irreducible polynomial, so that the principal ideal $\langle \phi(x) \rangle$ is a prime ideal in $\mathbb{Z}[x]$, and the quotient ring $\mathbb{Z}[x]/\langle \phi(x) \rangle$ is a domain, equivalently, $(\mathbb{Z}^n, +, \otimes)$ becomes a domain. Under this assumption, we see that arbitrary many pairwise relatively prime ideals in $\mathbb{Z}^n$ almost come in automatically, we describe the process as follows.

Algorithm 3: Generating Algorithm for Secret Key

- **First Step.** Randomly select an non-zero vector $\alpha \in \mathbb{Z}^n$ as input, and the output is the following relatively prime two ideal I_1 and I_2, where

$$I_1 = \langle \alpha \rangle, \text{ and } I_2 = \langle e - \alpha \rangle.$$

- **Second Step.** Randomly select two non-zero vectors $\alpha_1 \in I_1$ and $\alpha_2 \in I_2$ as input, and the output is the following ideal I_3, where

$$I_3 = \langle e - \alpha_1 \otimes \alpha_2 \rangle.$$

  It is easy to see that I_1, I_2, I_3 are pairwise relatively prime ideals.

- **Last Step.** Suppose that $m-1$ pairwise relatively prime ideals $I_1, I_2, \cdots, I_{m-1}$ are selected, then one randomly finds $\alpha_1 \in I_1$, $\alpha_2 \in I_2$, $\cdots$, $\alpha_{m-1} \in I_{m-1}$, $\alpha_i \neq 0$, and the output ideal I_m given by

$$I_m = \langle e - \alpha_1 \otimes \alpha_2 \otimes \cdots \otimes \alpha_{m-1} \rangle.$$

  Obviously, $I_1, I_2, \cdots, I_m$ are pairwise relatively prime ideals in $\mathbb{Z}^n$.

To construct an efficient algorithm for finding public key, we first show that

Lemma 2.7 Suppose that $I_1, I_2, \cdots, I_m$ are pairwise relatively ideals in $\mathbb{Z}^n$, and each I_i is a principal ideal generated by α_i, namely, $I_i = \langle \alpha_i \rangle$. Let

$$d_i = \bigotimes_{j=1, j \neq i}^{m} \alpha_j, 1 \leq i \leq m.$$

Then for every d_i, there is a vector $\mathcal{D}_i \in \mathbb{Z}^n$ such that

$$d_i \otimes \mathcal{D}_i \equiv e \pmod{I_i}, 1 \le i \le m.$$

Proof. Since $I_1, I_2, \cdots, I_m$ are pairwise relatively prime by assumption, we have

$$(I_i, I_1 I_2 \cdots I_{i-1} I_{i+1} \cdots I_m) = 1, 1 \le i \le m.$$

In other words, we have $(I_i, \langle d_i \rangle) = 1$, or

$$\langle \alpha_i \rangle + \langle d_i \rangle = \mathbb{Z}^n.$$

Therefore, there is a vector $\mathcal{D}_i \in \mathbb{Z}^n$ such that $d_i \otimes \mathcal{D}_i \equiv e \pmod{I_i}$, and we have Lemma 2.7 immediately.

How to find the vector $\mathcal{D}_i$ defined by Lemma 2.7? We introduce a polynomial algorithm to obtain $\mathcal{D}_i$ ($1 \le i \le m$), and generate the public key $\{A_1, A_2, \cdots, A_m\}$ by taking $A_i = d_i \otimes \mathcal{D}_i$ ($1 \le i \le m$).

Algorithm 4: Generating Algorithm for Public Key without Noises

- Let $I_i = \langle \alpha_i \rangle$ ($1 \le i \le m$) be pairwise relatively prime, and

$$d_i(x) = \prod_{j=1, j \ne i}^{m} \tau^{-1}(\alpha_i), 1 \le i \le m,$$

where the secret key $I_i = \langle \alpha_i \rangle$ ($1 \le i \le m$), and τ^{-1} is the inverse mapping of τ given by (2.1).

Since $d_i(x)$ and $\tau^{-1}(\alpha_i)$ are relatively prime polynomial in quotient ring $\mathbb{Z}[x]/\langle \phi(x) \rangle$, it follows that

$$\langle d_i(x) \rangle + \langle \tau^{-1}(\alpha_i) \rangle = \mathbb{Z}[x]/\langle \phi(x) \rangle.$$

Therefore, there is a polynomial $\mathcal{D}_i(x)$ such that

$$d_i(x)\mathcal{D}_i(x) \equiv 1 \pmod{\tau^{-1}(\alpha_i)}.$$

We put $\mathcal{D}_i = \tau(\mathcal{D}_i(x))$, and $A_i = d_i \otimes \mathcal{D}_i$, $1 \le i \le m$.

---

3. A Probabilistic Algorithm for Encryption

In our general construction for unbounded FHE, the encryption formula (2.6) is deterministic, so it is not IND-CPA secure, *i.e.* it is not secure against indistinguishable under chosen-plaintexts attack. To improve the encryption algorithm, we require to add some noises to the generating algorithm for public keys.

Let $\chi = (\chi_1, \chi_2, \cdots, \chi_m)$ be an arbitrary multiple discrete probability distributions over $\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \cdots \times \mathbb{Z}_{t_m}$, where χ_i be any discrete distribution over $\mathbb{Z}_{t_i}$ ($1 \le i \le m$). Let $a_i \leftarrow \chi_i$ and $a_i \in \mathbb{Z}_{t_i}$ ($1 \le i \le m$), so that $a = (a_1, a_2, \cdots, a_m) \in \mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \cdots \times \mathbb{Z}_{t_m}$ are the samples drawn from the distribution χ. By Theorem 1, we have *m* vectors E_i ($1 \le i \le m$) in $\mathbb{Z}^n$ such that

$$E_i \equiv e \pmod{I_i}, \text{ and } E_i \equiv \overline{a_j} \pmod{I_j}, \text{if } j \ne i, \tag{3.1}$$

where e is the unit element of $\mathbb{Z}^n$ and $\overline{a_j}$ is the embedding of a_j given by (2.4). According to the probabilistic distribution χ, we generate the public keys $A_\chi = \{A_1', A_2', \cdots, A_m'\}$ with noises by

$$A_i' = A_i \otimes E_i, 1 \le i \le m, \tag{3.2}$$

where A_i given by (2.5), and E_i given by (3.1). Therefore, the encryption algorithm (2.6) in our general construction (see algorithm 1) becomes the following formula for any $u = (u_1, u_2, \cdots, u_m) \in \mathbb{Z}_{t_1} \oplus \cdots \oplus \mathbb{Z}_{t_m}$,

$$f_\chi(u) = \overline{u_1} \otimes A_1' + \overline{u_2} \otimes A_2' + \cdots + \overline{u_m} \otimes A_m'. \tag{3.3}$$

Lemma 3.1 For arbitrary samples $a = (a_1, a_2, \cdots, a_m)$ drawn from the distribution χ, we have ($1 \le i \le m$)

$$A_i' \equiv e \pmod{I_i}, \text{ and } A_i' \equiv 0 \pmod{I_j}, \text{ if } j \ne i.$$

Proof. By (2.5), for every $i (1 \le i \le m)$ we have $A_i \equiv e \pmod{I_i}$, and $A_i \equiv 0 \pmod{I_j}$ when $j \ne i$, it follows that

$$A_i' \equiv A_i \otimes E_i \equiv e \pmod{I_i}, \text{ and } A_i' \equiv 0 \pmod{I_j}, \text{ if } j \ne i.$$

The dramatic effect of the above lemma is that the probabilistic encryption function f_χ shares the same decryption formula (see Algorithm 2) with the deterministic encryption algorithm f given by (2.6). In other words, there are no noises occurred in the decryption procedure, although the encryption algorithms with disturbance. It explains why we may obtain an unbounded FHE scheme without Gentry's bootstrapping transformation technique.

Next, we discuss how to randomly find the public keys $A_\chi = \{A_1', A_2', \cdots, A_m'\}$ according to the probabilistic distribution χ, the following lemma tells us how to obtain the error term E_i.

Lemma 3.2 Let $a = (a_1, a_2, \cdots, a_m) \leftarrow \chi$, and $A = \{A_1, A_2, \cdots, A_m\}$ be given by Algorithm 4, then we have

$$E_i = \overline{a_1} \otimes A_1 + \cdots + \overline{a_{i-1}} \otimes A_{i-1} + A_i + \overline{a_{i+1}} \otimes A_{i+1} + \cdots + \overline{a_m} \otimes A_m, \tag{3.4}$$
$$1 \le i \le m,$$

where $\overline{a_j}$ is the embedding of a_j.

Proof. Since $A_i \equiv e \pmod{I_i}$, and $A_i \equiv 0 \pmod{I_j}$ for $j \ne i$, it follows that

$$E_i \equiv e \pmod{I_i}, \text{ and } E_i \equiv \overline{a_j} \pmod{I_j}, \text{ if } j \ne i.$$

We have the lemma immediately.

Now, we give the final algorithm for the unbounded FHE scheme as follows.

Algorithm 5: The General Unbounded FHE Scheme

- **Secret Key:** One randomly selects m pairwise relatively prime principal ideal lattices $I_1, I_2, \cdots, I_m$ in $\mathbb{Z}^n$ as the decryption key according to Algorithm 3.

Continued

- **Public Key:** Let $t_i = t(I_i)$ be the one dimensional modulus of I_i $(1 \le i \le m)$. The plaintexts space is the direct sum of ring $\mathcal{P} = \bigoplus_{i=1}^{m} \mathbb{Z}_{t_i}$, the addition and multiplication in $\mathcal{P}$ are given by

$$(a_1, a_2, \cdots, a_m) + (b_1, b_2, \cdots, b_m) = (a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m),$$

$$(a_1, a_2, \cdots, a_m) \cdot (b_1, b_2, \cdots, b_m) = (a_1 b_1, a_2 b_2, \cdots, a_m b_m).$$

  Let $\chi = (\chi_1, \chi_2, \cdots, \chi_m)$ be a probabilistic distribution over $\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \cdots \times \mathbb{Z}_{t_m}$. The public key for encryption is $A_\chi = \{A'_1, A'_2, \cdots, A'_m\} \subset \mathbb{Z}^n$, and each $A'_i = A_i \otimes E_i$, where A_i given by Algorithm 4 and E_i given by (3.4).

- **Encryption:** For any plaintext $u = (u_1, u_2, \cdots, u_m) \in \mathcal{P} = \bigoplus_{i=1}^{m} \mathbb{Z}_{t_i}$, the encryption function f_χ is given by

$$c = f_\chi(u) = \overline{u_1} \otimes A'_1 + \overline{u_2} \otimes A'_2 + \cdots + \overline{u_m} \otimes A'_m, \tag{3.5}$$

  where $\overline{u_i}$ is the embedding of u_i.

- **Decryption:** For any ciphertext $c \in \mathbb{Z}^n$, we use the secret key $I_1, I_2, \cdots, I_m$ to decrypt c. Since for every i, $1 \le i \le m$, we have $c \equiv \overline{u_i} \pmod{I_i}$, and c mod I_i is a unique vector in the orthogonal parallelepiped $\mathcal{F}(I_i)$ of I_i, thus one has $c \bmod I_i = \overline{u_i}$, and by Lemma 3.1 and (2.3), we have

$$f_\chi^{-1}(c) = f^{-1}(c) = (u_1, u_2, \cdots, u_m) = u.$$

Because of the decryption procedure without noises, and the homomorphic computation on ciphertexts, we claim that the above Algorithm 5 is the unbounded FHE scheme as we desired.

Remark Since the probabilistic distribution χ is arbitrary, an alternative method to add noises to public key $A = \{A_1, A_2, \cdots, A_m\}$ may be described as follows: Randomly find m vectors $\gamma_1, \gamma_2, \cdots, \gamma_m$ in $\mathbb{Z}^n$, and put

$$\Gamma_i = \gamma_1 \otimes A_1 + \cdots + \gamma_{i-1} \otimes A_{i-1} + A_i + \gamma_{i+1} \otimes A_{i+1} + \cdots + \gamma_m \otimes A_m, 1 \le i \le m, \tag{3.6}$$

and then let $A''_i = A_i \otimes \Gamma_i$. Thus, we obtain the public key $A_{p_k} = \{A''_1, A''_2, \cdots, A''_m\}$ with noises, which guarantees the encryption formula (2.6) is not deterministic.

To discuss the security of this scheme, we observe that all risks come from the encryption algorithm (3.5). This algorithm contains some noises for public keys and guarantees the scheme could resist CPA attack. We describe the other risk as a generalized compact knapsack problem over the ring $(\mathbb{Z}^n, +, \otimes)$ as follows:

$$\sum_{i=1}^{m} a_i \otimes x_i = u, \quad |x_i| \le \beta, \tag{3.7}$$

where $a_1, a_2, \cdots, a_m$ are given m vectors in $\mathbb{Z}^n$, $u \in \mathbb{Z}^n$ is a target vector, and

$\beta = \max\limits_{1 \le i \le m} t_i$. Next section, we will show that the security of our scheme is solely under a worst-case complexity assumption, this is also a solution to open question 11 of [2].

4. The Generalized Compact Knapsack Problem over $\mathbb{Z}^n$

In this section, we discuss the security of our scheme based on the general compact knapsack problem over the ring $(\mathbb{Z}^n, +, \otimes)$. In [42], Micciancio has proved that if we can solve the knapsack problem over $\mathbb{Z}_q^n$ for some sufficiently large positive integer number q, then there is a probabilistic polynomial algorithm solving the covering radius problem for any n dimensional full rank cyclic lattice. First we generalize Micciancio's result to arbitrary ideal lattices based on our precious work [48], and then solving the knapsack problem from $\mathbb{Z}_q^n$ to $(\mathbb{Z}^n, +, \otimes)$. We give an entire proof for the reason of completeness, although the method we present here is quite similar to Micciancio's original proof.

DEFINITION 4.1 Let L be a full rank lattice, $\gamma(n)$ is a parameter of n, $\gamma(n) \ge 1$, CDP_γ problem is to find an r such that

$$\rho(L) \le r \le \gamma(n)\rho(L),$$

where $\rho(L) = \max\limits_{x \in \mathbb{R}^n} \text{dist}(x, L)$ and $\text{dist}(x, L) = \min\limits_{\alpha \in L} |x - \alpha|$.

DEFINITION 4.2 Let L be a full rank lattice, $S = \{s_1, s_2, \cdots, s_n\} \subset L$ be n linearly independent lattice vectors. $S^* = \{s_1^*, s_2^*, \cdots, s_n^*\}$ is the orthogonal basis corresponding to S by the Gram-Schmidt method. We define

$$\sigma(S) = \left(\sum_{i=1}^{n} |s_i^*|^2 \right)^{\frac{1}{2}}.$$

Here we give our main result to show that the generalized knapsack problem over $\mathbb{Z}^n$ is at least as hard as the covering radius problem for any n dimensional full rank ideal lattice.

THEOREM 2 Let $m = O(\log n)$, $k = \tilde{O}(\log n)$, $|\phi|^2 = \phi_0^2 + \phi_1^2 + \cdots + \phi_{n-1}^2$, $M = \sqrt{2 + 2|\phi|^2}$, $W = \dfrac{M^n - 1}{M - 1}$, $\gamma \ge 16mkn^3W$, if we can solve the knapsack problem (3.7), then there is a positive probabilistic polynomial algorithm solving the covering radius problem CDP_γ for any n dimensional full rank ideal lattice L.

Remark In the original work of Micciancio [42], the parameter γ is bigger than $16mkn^3$, we require $\gamma \ge 16mkn^3W$, where W is given by $\dfrac{M^n - 1}{M - 1}$. The main difference is to estimate the length of convolutional product $\alpha \otimes \beta$ for any two vectors α and β. It is clearly that $|\alpha \otimes \beta| \le \sqrt{n}|\alpha||\beta|$ in the case of circulant lattice, but it is non-trivial in the case of ideal lattices.

Lemma 4.1 For any $\alpha, \beta \in \mathbb{Z}^n$, we have

$$|\alpha \otimes \beta| \le W|\alpha| \cdot |\beta|,$$

where W is defined in Theorem 2.

Proof. We first prove $|H\alpha| \le M|\alpha|$. Let $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{n-1})^{\mathrm{T}}$, then

$$
\begin{aligned}
|H\alpha|^2 &= \phi_0^2 \alpha_{n-1}^2 + (\alpha_0 + \phi_1 \alpha_{n-1})^2 + \cdots + (\alpha_{n-2} + \phi_{n-1}\alpha_{n-1})^2 \\
&\le \phi_0^2 \alpha_{n-1}^2 + 2(\alpha_0^2 + \phi_1^2 \alpha_{n-1}^2) + \cdots + 2(\alpha_{n-2}^2 + \phi_{n-1}^2 \alpha_{n-1}^2) \\
&\le 2(\alpha_0^2 + \cdots + \alpha_{n-2}^2) + 2|\phi|^2 (\alpha_0^2 + \alpha_1^2 + \cdots + \alpha_{n-1}^2) \\
&\le (2 + 2|\phi|^2)|\alpha|^2.
\end{aligned}
$$

So $|H\alpha| \le M|\alpha|$. Similarly,

$$
|H^2 \alpha| \le M|H\alpha| \le M^2 |\alpha|.
$$

In the same way, we can get $|H^k \alpha| \le M^k |\alpha|$, $\forall 1 \le k \le n-1$. Let $\beta = (\beta_0, \beta_1, \cdots, \beta_{n-1})^{\mathrm{T}}$, it follows that

$$
\begin{aligned}
|\alpha \otimes \beta| &= |H^*(\alpha)\beta| = |\beta_0 \alpha + \beta_1 H\alpha + \cdots + \beta_{n-1}H^{n-1}\alpha| \\
&\le \sum_{i=0}^{n-1} |\beta_i H^i \alpha| \le \sum_{i=0}^{n-1} M^i |\alpha||\beta| = \frac{M^n - 1}{M - 1}|\alpha| \cdot |\beta|.
\end{aligned}
$$

We complete this proof.

Let $L = \mathcal{L}(B) \subset \mathbb{R}^n$ be a full rank ideal lattice, $q \ge 4mkn^2 W^2$, $\{e_0, e_1, \cdots, e_{n-1}\} \subset \mathbb{Z}_q^n$ is a standard orthogonal basis, $S = \{s_1, s_2, \cdots, s_n\} \subset L$ is a set of n linearly independent vectors. We define the parameter

$$
\mu = \left(\frac{4nq}{\gamma} + \frac{W}{2}\right)\sigma(S). \tag{4.1}
$$

According to Lemma 1.6 in Chapter 3 in [44], there is a lattice vector $c \in L$ such that $|c - \mu e_0| \le \frac{1}{2}\sigma(S)$, let $B' = q(H^*(c))^{-1} B$. It follows that the lattice $\mathcal{L}(B')$ generated by B' satisfies $q\mathbb{Z}^n \subset \mathcal{L}(B')$ according to Lemma 2.1 in Chapter 3 in [44]. Therefore, $q\mathbb{Z}^n$ is an additive subgroup in $\mathcal{L}(B')$. Randomly choose mk elements $x'_{ij} (1 \le i \le m, 1 \le j \le k)$ in the quotient group $G = \mathcal{L}(B')/q\mathbb{Z}^n$, the integral vectors w'_{ij} of x'_{ij} is defined by

$$
w'_{ij} = \lfloor x'_{ij} \rceil \in \mathbb{Z}^n, 1 \le i \le m, 1 \le j \le k.
$$

Let

$$
a_{ij} \equiv w'_{ij} (\mathrm{mod}\, q), \quad a_i \equiv \sum_{j=1}^{k} w'_{ij} (\mathrm{mod}\, q),
$$

Assume $A = (a_1, a_2, \cdots, a_m) \in \mathbb{Z}_q^{n \times m}$. Since the knapsack problem (3.7) is solvable on $\mathbb{Z}^n$, it could also be solved on $\mathbb{Z}_q^n$. Let $y = (y_1, y_2, \cdots, y_m) \in \mathbb{Z}_q^{n \times m}$ and $\hat{y} = (\hat{y}_1, \hat{y}_2, \cdots, \hat{y}_m) \in \mathbb{Z}_q^{n \times m}$ be two different integer matrices such that $\sum_{i=1}^{m} a_i \otimes (y_i - \hat{y}_i) = 0$, $|y_i| \le \sqrt{n}$, $|\hat{y}_i| \le \sqrt{n}$, $\forall 1 \le i \le m$. We define

$$
x_{ij} = \frac{1}{q}H^*(c)x'_{ij}, w_{ij} = \frac{1}{q}H^*(c)w'_{ij}, 1 \le i \le m, 1 \le j \le k,
$$

and

$$s' = \sum_{i=1}^{m}\sum_{j=1}^{k}\left(x_{ij} - w_{ij}\right) \otimes \left(y_i - \hat{y}_i\right). \tag{4.2}$$

Then x_{ij} is a lattice vector in the given ideal lattice $L = \mathcal{L}(B)$ ($1 \le i \le m$, $1 \le j \le k$), and s' is also a lattice vector in $L = \mathcal{L}(B)$ based on Lemma 2.2 in Chapter 3 in [44].

The next lemma gives an estimation of the length of s', which has some differences from the proof of Micciancio's.

Lemma 4.2 Let $S = \{s_1, s_2, \cdots, s_n\} \subset L$ be a set of n linearly independent vectors in the full rank ideal lattice *L*. Denote $|S| = \max_{1 \le i \le n}|s_i|$, s' is the lattice vector defined in (4.2), then

$$|s'| \le \frac{1}{2}|S|.$$

Proof. This proof is similar to that of Lemma 2.3 in Chapter 3 in [44] except some computations about the parameters. We prove $|s'| \le \frac{1}{2\sqrt{n}}\sigma(S)$ first. Based on the definition of s' in (4.2),

$$|s'| \le \sum_{i=1}^{m}\sum_{j=1}^{k}\left|\left(x_{ij} - w_{ij}\right) \otimes \left(y_i - \hat{y}_i\right)\right|. \tag{4.3}$$

$$x_{ij} - w_{ij} = \frac{1}{q}H^*(c)\left(x'_{ij} - w'_{ij}\right) = \frac{1}{q}c \otimes \left(x'_{ij} - w'_{ij}\right).$$

Let $\alpha = c - \mu e_0$, where μ is defined in (4.1). Then $|\alpha| \le \frac{1}{2}\sigma(S)$, and

$$\begin{aligned}
x_{ij} - w_{ij} &= \frac{1}{q}(\alpha + \mu e_0) \otimes \left(x'_{ij} - w'_{ij}\right) = \frac{1}{q}H^*(\alpha + \mu e_0)\left(x'_{ij} - w'_{ij}\right) \\
&= \frac{1}{q}\mu H^*(e_0)\left(x'_{ij} - w'_{ij}\right) + \frac{1}{q}H^*(\alpha)\left(x'_{ij} - w'_{ij}\right) \\
&= \frac{\mu}{q}\left(x'_{ij} - w'_{ij}\right) + \frac{1}{q}H^*(\alpha)\left(x'_{ij} - w'_{ij}\right).
\end{aligned}$$

Since $w'_{ij} = \lfloor x'_{ij} \rceil \in \mathbb{Z}^n$, we have

$$\left|x'_{ij} - w'_{ij}\right| \le \frac{1}{2}\sqrt{n},$$

combine with Lemma 4.1, we get

$$\begin{aligned}
\left|x_{ij} - w_{ij}\right| &\le \frac{\mu}{q}\left|x'_{ij} - w'_{ij}\right| + \frac{1}{q}\left|\alpha \otimes \left(x'_{ij} - w'_{ij}\right)\right| \le \frac{\mu}{q} \cdot \frac{1}{2}\sqrt{n} + \frac{1}{q} \cdot W \cdot \frac{1}{2}\sigma(S) \cdot \frac{\sqrt{n}}{2} \\
&= \frac{\sqrt{n}}{2q}\left(\frac{4nq}{\gamma} + \frac{W}{2}\right)\sigma(S) + \frac{\sqrt{n}W}{4q}\sigma(S) = \sigma(S)\left(\frac{2n^{\frac{3}{2}}}{\gamma} + \frac{\sqrt{n}W}{2q}\right) \\
&\le \sigma(S)\left(\frac{1}{8} \cdot \frac{1}{mkn^{\frac{3}{2}}W} + \frac{1}{8} \cdot \frac{1}{mkn^{\frac{3}{2}}W}\right) = \sigma(S)\frac{1}{4mkn^{\frac{3}{2}}W}.
\end{aligned}$$

Based on (4.3), we know

$$\left| s' \right| \le mkW \max_{i,j} \left| x_{ij} - w_{ij} \right| \cdot \max_i \left| y_i - \hat{y}_i \right|$$

$$\le mkW \cdot \frac{\sigma(S)}{4mkn^{\frac{3}{2}}W} \cdot 2\sqrt{n} = \frac{\sigma(S)}{2\sqrt{n}}.$$

Since

$$\sigma(S) \le \left(\sum_{i=1}^{n} \left| s_i \right|^2 \right)^{\frac{1}{2}} \le \sqrt{n} \left| S \right|$$

We can get

$$\left| s' \right| \le \frac{\sigma(S)}{2\sqrt{n}} \le \frac{\sqrt{n} \left| S \right|}{2\sqrt{n}} = \frac{1}{2} \left| S \right|.$$

So we complete the proof of Lemma 4.2.

Based on the above lemmas, Theorem 2 follows directly from Micciancio's method [42]. From Theorem 2, we can see that the general compact knapsack problem over $\mathbb{Z}^n$ is at least as hard as the covering radius problem CDP_γ of any ideal lattice. Therefore, the security of our unbounded FHE scheme is solely under the worst-case complexity assumption, as a result, it is a reasonable solution to **Open Question 11** of [2].

5. A Practical System

As an example, we introduce a practical system for FHE using some basic results about the cyclotomic field [50]. Suppose that p is an odd prime number and $Q(\xi_p)$ is the cyclotomic field, where $\xi_p = \mathrm{e}^{\frac{2\pi i}{p}}$ is a primitive p-th root of the unit.

Let

$$\mathbb{Z}[\xi_p] = \left\{ \sum_{i=0}^{p-1} a_i \xi_p^i \mid a_i \in \mathbb{Z} \right\}.$$

It is known that $\mathbb{Z}[\xi_p]$ is the ring of algebraic integers of field $Q(\xi_p)$. Therefore $\mathbb{Z}[\xi_p]$ is a Dedekind domain (so we have unique factorization into prime ideals, etc. see Proposition 1.2 of [50]).

To construct a commutative ring for $\mathbb{Z}^n$, we select $\phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$. Obviously, $\phi(x)$ is the minimal polynomial of ξ_p. Let $n = p-1$, then we obtain a ring $(\mathbb{Z}^n, +, \otimes)$ in terms of $\phi(x)$ and the rotation matrix H_ϕ, it is easy to see that (see (3.2) of [43])

$$(\mathbb{Z}^n, +, \otimes) \cong \mathbb{Z}[x] / \langle \phi(x) \rangle \cong \mathbb{Z}[\xi_p].$$

Thus, $\mathbb{Z}^n$ becomes a Dedekind domain.

For any integer $q \in \mathbb{Z}$, we define an integer vector $\alpha_q \in \mathbb{Z}^n$ by

$$\alpha_q = \begin{pmatrix} q \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \in \mathbb{Z}^n.$$

The principal ideal $\langle \alpha_q \rangle$ generated by α_q is denoted by

$$I_q = \langle \alpha_q \rangle = \mathcal{L}\left(H^*\left(\alpha_q\right)\right).$$

Lemma 5.1 If q_1 and q_2 are two different prime numbers, then I_{q_1} and I_{q_2} are relatively prime ideal lattices in $\mathbb{Z}^n$.

Proof. Suppose that q is a prime number. Since $\left(\mathbb{Z}^n, +, \otimes\right) \cong \mathbb{Z}[x]/\langle \phi(x) \rangle$, we see the polynomial $\tau^{-1}\left(\alpha_q\right) = \alpha_q(x) = x^{n-1} + q \in \mathbb{Z}[x]$, which is the type polynomial of Eisenstein, thus it is an irreducible polynomial over $\mathbb{Z}[x]$. Regarding $\alpha_q(x)$ as the polynomial of $\mathbb{Z}[x]/\langle \phi(x) \rangle$, clearly, it is also an irreducible polynomial in $\mathbb{Z}[x]/\langle \phi(x) \rangle$. By assumption, q_1 and q_2 are different prime numbers, we show that the principal ideals $\langle \alpha_{q_1}(x) \rangle$, and $\langle \alpha_{q_2}(x) \rangle$ are relatively prime ideals in $\mathbb{Z}[x]/\langle \phi(x) \rangle$. Since $\mathbb{Z}[x]/\langle \phi(x) \rangle$ is a Dedekind domain, if $\langle \alpha_{q_1}(x) \rangle$ and $\langle \alpha_{q_2}(x) \rangle$ are not relatively prime, then, there exists a prime ideal P in $\mathbb{Z}[x]/\langle \phi(x) \rangle$ such that

$$\langle \alpha_{q_1}(x) \rangle \subset P, \text{ and } \langle \alpha_{q_2}(x) \rangle \subset P.$$

It follows for any positive integer $k \geq 1$ that

$$\langle \alpha_{q_1}^k(x) \rangle \subset P^k, \text{ and } \langle \alpha_{q_2}^k(x) \rangle \subset P^k.$$

It is known that three exists a positive integer $k \geq 1$, such that $P^k = \langle d(x) \rangle$ is a principal ideal, we thus have

$$\langle \alpha_{q_1}^k(x) \rangle \subset \langle d(x) \rangle, \text{ and } \langle \alpha_{q_2}^k(x) \rangle \subset \langle d(x) \rangle.$$

In other words, we have $d(x) | \alpha_{q_1}^k(x)$, and $d(x) | \alpha_{q_2}^k(x)$. However, this is impossible, since $\alpha_{q_1}(x)$ and $\alpha_{q_2}(x)$ are two irreducible polynomials in $\mathbb{Z}[x]/\langle \phi(x) \rangle$, and $\alpha_{q_1}(x) \neq \alpha_{q_2}(x)$.

This proves that $\langle \alpha_{q_1}(x) \rangle$ and $\langle \alpha_{q_2}(x) \rangle$ are relatively prime ideals in $\mathbb{Z}[x]/\langle \phi(x) \rangle$. Equivalently, I_{q_1} and I_{q_2} are two relatively prime ideal lattices in $\mathbb{Z}^n$.

Lemma 5.2 The one dimensional modulus of the principal ideal I_q is

$$t_q = t\left(I_q\right) = q^n - q^{n-1} + \cdots - q + 1.$$

Proof. It is not hard to compute that $\det\left(H^*\left(\alpha_q\right)\right) = q^n - q^{n-1} + \cdots - q + 1$. Since the polynomial $x^n - x^{n-1} + \cdots - x + 1$ is an irreducible polynomial over $\mathbb{Z}$, we have the assertion of lemma immediately.

According to Lemma 5.1 and Lemma 5.2, we obtain a generating algorithm for the secret key as follows:

Algorithm 6: Generating Algorithm for Secret Key

- Randomly select m different prime numbers $q_1, q_2, \cdots, q_m$ such that $q_i \neq p$. The principal ideal lattices

$$I_{q_i} = \langle \alpha_{q_i} \rangle, \ 1 \leq i \leq m$$

are the secret key, and the corresponding one dimensional modulus t_{q_i} given by

$$t_{q_i} = t\left(I_{q_i}\right) = q_i^n - q_i^{n-1} + \cdots - q_i + 1. \tag{5.1}$$

To get an attainable algorithm for public key, we define m vectors $d_i \, (1 \le i \le m)$ by

$$d_i = \alpha_{q_1} \otimes \alpha_{q_2} \otimes \cdots \otimes \alpha_{q_{i-1}} \otimes \alpha_{q_{i+1}} \otimes \cdots \otimes \alpha_{q_m} = \otimes_{\substack{j=1 \\ j \ne i}}^m \alpha_{q_j}, \quad 1 \le i \le m.$$

Lemma 5.3 For every vector $d_i \, (1 \le i \le m)$, there is a vector $\mathcal{D}_i \in \mathbb{Z}^n$ such that

$$d_i \otimes \mathcal{D}_i \equiv e \left(\bmod I_{q_i} \right),$$

where $e = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ is the unit element of rimg $\left(\mathbb{Z}^n, +, \otimes \right)$.

Proof. By lemma 5.1, $I_{q_1}, I_{q_2}, \cdots, I_{q_m}$ are pairwise relatively prime ideals, hence we have $\left(I_{q_i}, I_{q_1} I_{q_2} \cdots I_{q_{i-1}} I_{q_{i+1}} \cdots I_{q_m} \right) = 1$. In other words, we have $\left(\langle \alpha_{q_i} \rangle, \langle d_i \rangle \right) = 1$, or

$$\langle \alpha_{q_i} \rangle + \langle d_i \rangle = \mathbb{Z}^n.$$

Therefore, there is a vector $\mathcal{D}_i \in \mathbb{Z}^n$ such that $\mathcal{D}_i \otimes d_i \equiv e \left(\bmod I_{q_i} \right)$. We have Lemma 5.3.

We propose a polynomial algorithm to find the vector $\mathcal{D}_i$ appeared in Lemma 5.3, and then put $A_i = d_i \otimes \mathcal{D}_i$ getting the public key $A_1, A_2, \cdots, A_m$. The polynomial algorithm for finding vector $\mathcal{D}_i$ like follows.

Algorithm 7: Generating Algorithm for Public Key without Noises

- Let

$$d_i(x) = \prod_{\substack{j=1 \\ j \ne i}}^m \left(x^{n-1} + q_j \right), 1 \le i \le m.$$

Since polynomial $x^{n-1} + q_i$ and $x^{n-1} + q_j \, (j \ne i)$ are relatively prime in $\mathbb{Z}[x] / \langle \phi(x) \rangle$, it follows that $\left(x^{n-1} + q_i, d_i(x) \right) = 1$. Therefore, there is a polynomial $\mathcal{D}_i(x)$ such that

$$d_i(x) \mathcal{D}_i(x) \equiv 1 \left(\bmod \left(x^{n-1} + q_i \right) \right).$$

We obtain $\mathcal{D}_i = \tau \left(\mathcal{D}_i(x) \right)$ under the mapping τ given in section 2.

Now, we describe an attainable algorithm for our FHE Scheme based on cyclotomic field as follows.

Algorithm 8: A Practical Scheme for Unbounded FHE

- **Secret key:** Let $q_1, q_2, \cdots, q_m$ be m different prime numbers such that $q_i \ne p$. The m pairwise relatively prime principal ideal lattices $I_{q_1}, I_{q_2}, \cdots, I_{q_m}$ are the secret keys for decryption.

Continued

- **Public Key:** Let $A_i = d_i \otimes \mathcal{D}_i \ (1 \le i \le m)$, then $A_\chi = \{A_1', A_2', \cdots, A_m'\}$ are the public key for encryption, where $A_i' = A_i \otimes E_i$ and E_i is given by (3.4) according to the probabilistic distribution χ. The plaintext space is

$$\mathcal{P} = \mathbb{Z}_{t_1} \oplus \mathbb{Z}_{t_2} \oplus \cdots \oplus \mathbb{Z}_{t_m},$$

where t_i is the one dimensional modulus of I_{q_i} given by (5.1).

- **Encryption:** For any plaintext $u = (u_1, u_2, \cdots, u_m) \in \bigoplus\limits_{i=1}^{m} \mathbb{Z}_{t_i}$, then

$$c = f_\chi(u) = \overline{u_1} \otimes A_1' + \overline{u_2} \otimes A_2' + \cdots + \overline{u_m} \otimes A_m',$$

where $\overline{u_i}$ is the embedding of u_i into $\mathbb{Z}^n$.

- **Decryption:** For given ciphertext $c \in \mathbb{Z}^n$, there is an unique vector $\overline{u_i}$ in the orthogonal parallelepiped $\mathcal{F}(I_{q_i})$, such that $c \equiv \overline{u_i} \pmod{I_{q_i}}$, $1 \le i \le m$. Thus, one has

$$f_\chi^{-1}(c) = f^{-1}(c) = (u_1, u_2, \cdots, u_m) = u.$$

The property of FHE follows immediately from the general construction. We mainly discuss the security of this practical system for FHE. Obviously, an additional risk comes from the messages of one-dimensional modulus $t_i \ (1 \le i \le m)$. It is equivalent to find a solution to the algebraic equation with a high degree of

$$x^n - x^{n-1} + \cdots - x + 1 = t$$

For a given target value $t \in \mathbb{Z}$. This is an ancient hard problem in mathematics, there is no general method to find the solution according to the famous Galois theory. Therefore, we conclude that there are no special risks coming from the one-dimensional modulus t_i of I_{q_i}.

6. Conclusions

In this work, we construct the first unbounded fully homomorphic encryption scheme without the bootstrapping transformation technique. In the encryption algorithm (3.5), we see that $H^*(\overline{a}) = aI_n$ for any $a \in \mathbb{Z}$. Therefore, the problem of security may transfer to the standard Ring-SIS problem: suppose that $A_\chi = [A_1', A_2', \cdots, A_m'] \in \mathbb{Z}^{n \times m}$, where A_i' is given by (3.2), $u \in \mathbb{Z}^n$ is a target vector, find $x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in \mathbb{Z}^m$ such that $Ax = u$, and $0 < |x| \le \beta$. Let q be a sufficiently large positive integer, if one can show that every column A_i' of A_χ is uniformly random vectors in $\mathbb{Z}_q^n$, then this problem can be changed to an inhomogeneous version of the SIS problem, which is to find a short integer solution to $Ax \equiv u \pmod{q}$. It is not hard to show that the homogeneous and inhomogeneous problems are essentially equivalent to typical parameters.

According to Ajtai's seminal work [23] [41], the hardness of the SIS problem

is relative to the worst-case lattice problem. More precisely, for any $m = \text{poly}(n)$, any $\beta > 0$, and any sufficiently large $q \geq \beta \cdot \text{poly}(n)$, solving $\text{SIS}_{n,q,\beta,m}$ with non-negligible probability is at least as hard as solving the decisional approximate shortest vector problem GapSVP_γ for some $\gamma = \beta \cdot \text{poly}(n)$ (also see [52] and Theorem 4.1.2 of [2]). Perhaps, we may find another proof that the security of our FHE scheme is solely under a worst-case complexity assumption.

On the other hand, the fully homomorphic signature is the dual question of the fully homomorphic encryption, we will develop a scheme for a fully homomorphic signature in another article.

Acknowledgements

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Rivest, R.L., Adleman, L. and Dertouzos, M.L. (1978) On Data Banks and Privacy Homomorphisms. *Foundations of Secure Computation*, **4**, 169-180.

[2] Peikert, C. (2016) A Decade of Lattice Cryptography. Now Foundations and Trends, Boston, 1-90. https://doi.org/10.1561/9781680831139

[3] Gentry, C. (2009) A Fully Homomorphic Encryption Scheme. Ph.D. Thesis, Stanford University, Stanford.

[4] Gentry, C. (2009) Fully Homomorphic Encryption Using Ideal Lattices. *Proceedings of the* 41*st Annual ACM Symposium on Theory of Computing*, Bethesda, 31 May-2 June 2009, 169-178. https://doi.org/10.1145/1536414.1536440

[5] Brakerski, Z. (2012) Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. *Advances in Cryptology-CRYPTO* 2012, Santa Barbara, 19-23 August 2012, 868-886. https://doi.org/10.1007/978-3-642-32009-5_50

[6] Brakerski, Z., Gentry, C. and Vaikuntanathan, V. (2014) (Leveled) Fully Homomorphic Encryption without Bootstrapping. *Proceedings of the* 3*rd Innovations in Theoretical Computer Science Conference*, Cambridge, 8-10 January 2012, 309-325. https://doi.org/10.1145/2090236.2090262

[7] Brakerski, Z. and Vaikuntanathan, V. (2011) Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. *Advances in Cryptology-CRYPTO* 2011, Santa Barbara, 14-18 August 2011, 505-524. https://doi.org/10.1007/978-3-642-22792-9_29

[8] Brakerski, Z. and Vaikuntanathan, V. (2014) Efficient Fully Homomorphic Encryption from (Standard) LWE. *SIAM Journal on Computing*, **43**, 831-871. https://doi.org/10.1137/120868669

[9] Cheon, J.H., Coron, J.-S., Kim, J., Lee, M.S., Lepoint, T., Tibouchi, M. and Yun, A. (2013) Batch Fully Homomorphic Encryption over the Integers. *Advances in Cryp-*

tology-EUROCRYPT 2013, Athens, 26-30 May 2013, 315-335.
https://doi.org/10.1007/978-3-642-38348-9_20

[10] Coron, J.-S., Mandal, A., Naccache, D. and Tibouchi, M. (2011) Fully Homomorphic Encryption over the Integers with Shorter Public Keys. *Advances in Cryptology-CRYPTO* 2011, Santa Barbara, 14-18 August 2011, 487-504.
https://doi.org/10.1007/978-3-642-22792-9_28

[11] Coron, J.-S., Naccache, D. and Tibouchi, M. (2012) Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers. *Advances in Cryptology-EUROCRYPT* 2012, Cambridge, 15-19 April 2012, 446-464.
https://doi.org/10.1007/978-3-642-29011-4_27

[12] Gentry, C. (2010) Computing Arbitrary Functions of Encrypted Data. *Communications of the ACM*, **53**, 97-105. https://doi.org/10.1145/1666420.1666444

[13] Gentry, C. (2010) Toward Basing Fully Homomorphic Encryption on Worst-Case Hardness. *Advances in Cryptology-CRYPTO* 2010, Santa Barbara, 15-19 August 2010, 116-137. https://doi.org/10.1007/978-3-642-14623-7_7

[14] Gentry, C., Halevi, S., Peikert, C. and Smart, N.P. (2012) Field Switching in BGV-Style Homomorphic Encryption. *Journal of Computer Security*, **21**, 663-684.
https://doi.org/10.3233/JCS-130480

[15] Gentry, C., Halevi, S. and Smart, N.P. (2012) Fully Homomorphic Encryption with Polylog Overhead. *Advances in Cryptology-EUROCRYPT* 2012, Cambridge, 15-19 April 2012. 465-482. https://doi.org/10.1007/978-3-642-29011-4_28

[16] Smart, N.P. and Vercauteren, F. (2014) Fully Homomorphic SIMD Operations. *Designs, Codes and Cryptography*, **71**, 57-81.
https://doi.org/10.1007/s10623-012-9720-4

[17] Regev, O. (2009) On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *JOURNAL OF THE ACM*, **56**, Article No. 34.
https://doi.org/10.1145/1568318.1568324

[18] Regev, O. (2010) The Learning with Errors Problem. *IEEE Conference on Computational Complexity*, Cambridge, 9-11 June 2010, 191-204.
https://doi.org/10.1109/CCC.2010.26

[19] Gentry, C., Sahai, A. and Waters, B. (2013) Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. *Advances in Cryptology-CRYPTO* 2013, Santa Barbara, 18-22 August 2013, 75-92.
https://doi.org/10.1007/978-3-642-40041-4_5

[20] Zheng, Z. and Tian, K. (2022) On the LWE Cryptosystem with More General Disturbance. *Journal of Information Security*, **13**, 127-139.
https://doi.org/10.4236/jis.2022.133008

[21] Alperin-Sheriff, J. and Peikert, C. (2013) Practical Bootstrapping in Quasilinear Time. *Advances in Cryptology-CRYPTO* 2013, Santa Barbara, 18-22 August 2013, 1-20.
https://doi.org/10.1007/978-3-642-40041-4_1

[22] Agrawal, S., Boneh, D. and Boyen, X. (2010) Efficient Lattice (H)IBE in the Standard Model. *EUROCRYPT*, Monaco, 30 May-3 June 2010, 553-572.
https://doi.org/10.1007/978-3-642-13190-5_28

[23] Ajtai, M. (1999) Generating Hard Instances of the Short Basis Problem. In: Wiedermann, J., Boas, P.E. and Nielsen, M., Eds., *Automata, Languages and Programming*, Springer, Berlin, 1-9. https://doi.org/10.1007/3-540-48523-6_1

[24] Alwen, J. and Peikert, C. (2009) Generating Shorter Bases for Hard Random Lattices. *Theory of Computing Systems*, **48**, 535-553.

https://doi.org/10.1007/s00224-010-9278-3

[25] Micciancio, D. and Peikert, C. (2012) Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. *Advances in Cryptology-EUROCRYPT* 2012, Cambridge, 15-19 April 2012, 700-718. https://doi.org/10.1007/978-3-642-29011-4_41

[26] Peikert, C. and Waters, B. (2011) Lossy Trapdoor Functions and Their Applications. *SIAM Journal on Computing*, **40**, 1803-1844. https://doi.org/10.1137/080733954

[27] Chillotti, I., Gama, N., Georgieva, M. and Izabachene, M. (2016) Faster Fully Homomorphic Encryption: Bootstrapping in Less than 0.1 Seconds. *Advances in Cryptology-ASIACRYPT* 2016, Hanoi, 4-8 December 2016, 3-33. https://doi.org/10.1007/978-3-662-53887-6_1

[28] Chillotti, I., Gama, N., Georgieva, M. and Izabachene, M. (2018) TFHE: Fast Fully Homomorphic Encryption over the Torus. *Journal of Cryptology*, **33**, 34-91. https://doi.org/10.1007/s00145-019-09319-x

[29] Chen, H., Laine, K. and Player, R. (2017) Simple Encrypted Arithmetic Library-SEAL v2.1. *FC* 2017 *International Workshops*, *WAHC, BITCOIN, VOTING, WTSC, and TA*, Sliema, 7 April 2017, 3-18. https://doi.org/10.1007/978-3-319-70278-0_1

[30] Fan, J. and Vercauteren, F. (2012) Somewhat Practical Fully Homomorphic Encryption. IACR Cryptology ePrint Archive.

[31] Cheon, J.H., Han, K., Kim, A., Kim, M. and Song, Y. (2018) Bootstrapping for Approximate Homomorphic Encryption. *Advances in Cryptology-EUROCRYPT* 2018, Tel Aviv, 29 April-3 May 2018, 360-384. https://doi.org/10.1007/978-3-319-78381-9_14

[32] Cheon, J.H., Kim, A., Kim, M. and Song, Y.S. (2017) Homomorphic Encryption for Arithmetic of Approximate Numbers. *Advances in Cryptology-ASIACRYPT* 2017, Hong Kong, 3-7 December 2017, 409-437. https://doi.org/10.1007/978-3-319-70694-8_15

[33] Boura, C., Gama, N., Georgieva, M. and Jetchev, D. (2020) CHIMERA: Combining Ring-LWE-Based Fully Homomorphic Encryption Schemes. *Journal of Mathematical Cryptology*, **14**, 316-338. https://doi.org/10.1515/jmc-2019-0026

[34] van Dijk, M., Gentry, C., Halevi, S. and Vaikuntanathan, V. (2010) Fully Homomorphic Encryption over the Integers. *Advances in Cryptology-EUROCRYPT* 2010, French Riviera, 30 May-3 June 2010, 24-43. https://doi.org/10.1007/978-3-642-13190-5_2

[35] Kogos, K.G., Filippova, K.S. and Epishkina, A.V. (2017) Fully Homomorphic Encryption Schemes: The State of the Art. 2017 *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, St. Petersburg, 1-3 February 2017, 463-466. https://doi.org/10.1109/EIConRus.2017.7910591

[36] Yagisawa, M. (2015) Fully Homomorphic Encryption without Bootstrapping. Cryptology ePrint Archive.

[37] Yagisawa, M. (2015) Fully Homomorphic Encryption on Octonion Ring. Cryptology ePrint Archive.

[38] Liu, D. (2015) Practical Fully Homomorphic Encryption without Noise Reduction. Cryptology ePrint Archive.

[39] Li, J. and Wang, L. (2015) Noise-Free Symmetric Fully Homomorphic Encryption Based on Non-Commutative Rings. Cryptology ePrint Archive.

[40] Zheng, Z. (2022) Modern Cryptography Volume 1—A Classical Introduction to Informational and Mathematical Principle. Springer, Berlin. https://doi.org/10.1007/978-981-19-0920-7

[41] Ajtai, M. (1996) Generating Hard Instances of Lattice Problems. *Quaderni di Matematica*, **13**, 99-108. https://doi.org/10.1145/237814.237838

[42] Micciancio, D. (2002) Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions from Worst-Case Complexity Assumptions. *The 43rd Annual IEEE Symposium on Foundations of Computer Science*, Vancouver, 16-19 November 2002, 356-365.

[43] Zheng, Z., Liu, F. and Chen, M. (2022) On the High Dimensional RSA Algorithm—A Public Key Cryptosystem Based on Lattice and Algebraic Number Theory. *International Journal of Latest Research in Engineering and Technology*, **8**, 1-16.

[44] Zheng, , Z., Tian, K. and Liu, F. (2022) Modern Cryptography Volume 2—A Classical Introduction to Informational and Mathematical Principle. Springer, Berlin. https://doi.org/10.1007/978-981-19-7644-5

[45] Lyubashevsky, V., Peikert, C. and Regev, O. (2010) On Ideal Lattices and Learning with Errors over Rings. *Advances in Cryptology-EUROCRYPT* 2010, French Riviera, 30 May-3 June 2010, 1-23. https://doi.org/10.1007/978-3-642-13190-5_1

[46] Micciancio, D. and Regev, O. (2009) Lattice-Based Cryptography. In: Bernstein, D.J., Buchmann, J. and Dahmen, E., Eds., *Post-Quantum Cryptography*, Springer, Berlin, 147-191. https://doi.org/10.1007/978-3-540-88702-7_5

[47] Zheng, Z., Liu, F., Huang, W., Xu, J. and Tian, K. (2022) A Generalization of NTRU-Encrypt—Cryptosystem Based on Ideal Lattice. *Journal of Information Security*, **13**, 165-180. https://doi.org/10.4236/jis.2022.133010

[48] Zheng, Z., Liu, F., Lu, Y. and Tian, K. (2022) Cyclic Lattices, Ideal Lattices and Bounds for the Smoothing Parameter. *Journal of Information Security*, **13**, 272-293. https://doi.org/10.4236/jis.2022.134015

[49] Micciancio, D. and Regev, O. (2007) Worst-Case to Average-Case Reductions Based on Gaussian Measures. *SIAM Journal on Computing*, **37**, 267-302. https://doi.org/10.1137/S0097539705447360

[50] Washington, L.C. (1980) Graduate Texts in Mathematics—Introduction to Cyclotomic Fields. Springer-Verlag, New York.

[51] Micciancio, D. (2001) Improving Lattice Based Cryptosystems Using the Hermite Normal Form. In: Silverman, J.H., Ed., *Cryptography and Lattices*, Springer, Berlin, 126-145. https://doi.org/10.1007/3-540-44670-2_11

[52] Micciancio, D. and Peikert, C. (2013) Hardness of SIS and LWE with Small Parameters. *Advances in Cryptology-CRYPTO* 2013, Santa Barbara, 18-22 August 2013, 21-39. https://doi.org/10.1007/978-3-642-40041-4_2