Approximate Homomorphic Encryption over the Conjugate-invariant Ring

Duhyeong Kim[1] and Yongsoo Song[2]

[1] Seoul National University, Seoul, Republic of Korea
[2] University of California, San Diego, United States

Abstract. The Ring Learning with Errors (RLWE) problem over a cyclotomic ring has been the most widely used hardness assumption for the construction of practical homomorphic encryption schemes. However, this restricted choice of a base ring may cause a waste in terms of plaintext space usage. For example, the approximate homomorphic encryption scheme of Cheon et al. (ASIACRYPT'17) is able to store a complex number in each of the plaintext slots since its canonical embedding of a cyclotomic field has a complex image. The imaginary part of a plaintext is not underutilized at all when the computation is performed over the real numbers, which is required in most of the real-world applications such as machine learning. In this paper, we propose a new approximate homomorphic encryption scheme which is optimized in the computation over real numbers. Our scheme is based on RLWE over a special subring of a cyclotomic ring, which is no easier than a standard lattice problem over ideal lattices by the reduction of Peikert et al. (STOC'17). Our scheme allows real numbers to be packed in a ciphertext without any waste of a plaintext space and consequently we can encrypt twice as many plaintext slots as the previous scheme while maintaining the same security level, storage, and computational costs.

Keywords: ring learning with errors, homomorphic encryption, real number arithmetic.

1 Introduction

Learning with Errors (LWE) is a computational problem which asks to distinguish a system of linear equations with small errors from a uniformly random one. After Regev [27] firstly introduced the LWE problem, it has been one of the standard assumptions for the construction of cryptographic primitives due to its security and versatility. Lyubashevsky, Peikert, and Regev [24] proposed a variant of LWE called the Ring Learning with Errors (RLWE) problem. They also showed that the (decisional) RLWE problem over a cyclotomic ring can be reduced from the Shortest Independent Vectors Problem (SIVP) over ideal lattices.

Homomorphic Encryption (HE) is a cryptographic scheme which enables arithmetic operations on encrypted data without decryption. This technology is a promising solution which can prevent leakage of sensitive personal information such as financial, medical and genomic data. A number of HE schemes [13, 5, 18, 4, 16, 3, 19, 14, 12, 11, 10] have been suggested following Gentry's blueprint [17]. Currently, security of the most of the practical HE schemes [18, 16, 11, 10] relies on the hardness of RLWE over a cyclotomic ring. For several years, the choice of base ring was restricted because nothing was known about the hardness of (decisional) RLWE over non-cyclotomic rings.

Cheon et al. [10] proposed a HE scheme (HEAAN) that supports the arithmetic of approximate numbers contrary to the exact computation on discrete plaintext spaces of the previous HE schemes. In addition to homomorphic addition and multiplication, the HEAAN scheme can compute the rounding operation (extraction of the most significant bits) efficiently which has traditionally been considered a challenging subject on HE system. Because of this, the HEAAN scheme showed

a remarkable performance in many of the applications [22, 21], requiring computations of real numbers.

Motivation. The HEAAN scheme uses the canonical embedding of a cyclotomic field to pack a number of plaintext values in a single ciphertext. A cyclotomic field is a totally imaginary number field, so each of the plaintext slots can store a complex number. We point out that this complex encoding method has an inefficiency in terms of the utilization of a plaintext space. Since most of the real-world applications (e.g. machine learning) require computations over purely real numbers, the imaginary part of a plaintext of HEAAN is underutilized. It can be viewed as a waste of a plaintext space.

Peikert et al. [26] recently showed that the RLWE problem over the ring of integers of an arbitrary number field is no easier than SIVP over ideal lattices in the same number field. So we aimed to find a new number field and construct a HE scheme over its ring of integers, which utilizes a fully packed plaintext space over real numbers to overcome the existing problem.

Our Contribution. We consider the maximal real subfield of a cyclotomic field as a base number field and define the RLWE problem over its ring of integers which is called the *conjugate-invariant* ring. We first show that the conjugate-invariant ring is the set of real numbers in the ring of integers of a cyclotomic field and adapt the reduction of [26] to guarantee the hardness of RLWE problem over the conjugate-invariant ring.

Based on this problem, we construct a new HE scheme that supports approximate arithmetic of real numbers. Our scheme can store a real number in each of the plaintext slots since the image of conjugate-invariant ring with respect to the canonical embedding belongs to the set of real vectors. We also propose a specialized Fast Fourier Transformation (FFT) algorithm over the residue ring of conjugate-invariant ring to minimize the complexity of arithmetic operations.

As a result, our HE scheme can encrypt *twice* as many plaintext slots as the original HEAAN scheme while maintaining the same security level and computational costs, i.e., the amortized timing (complexity) per slot is reduced by half.

Technical Details. Let m be a power-of-two integer so that $n := \phi(m) = m/2$ and $\Phi_m(X) = X^n + 1$. Let $\zeta = \exp(2\pi i/m)$ be an m-th primitive root of unity and let $F = \mathbb{Q}(\xi)$ be the maximal real subfield of the cyclotomic field $K = \mathbb{Q}(\zeta)$ for $\xi = \zeta + \zeta^{-1}$. Then the ring of integers of $F = \mathbb{Q}(\xi)$ is $R = \mathbb{Z}[\xi]$, and we call this ring the conjugate-invariant ring. By adapting the reduction in [26], we can show that RLWE over the ring R is no easier than SIVP over ideal lattices in K. This hardness proof reasonably motivates us to exploit R as a base ring for the construction of a HE scheme. We also give a cryptanalysis of RLWE over the conjugate-invariant ring $R = \{a(X) \in \mathbb{Z}[X]/(X^n + 1) : a(X) = a(X^{-1})\}$ to study the concrete security level. We consider all known attacks on RLWE and conclude that this problem requires the same attack complexity as the ordinary $(n/2)$-dimensional LWE problem.

The plaintext encoding technique of HEAAN utilizes the canonical embedding map for the packing of plaintexts in a single ciphertext. Similarly, we consider the canonical embedding map $\tau : F \to \mathbb{C}^{n/2}$ of the number field F. Since ξ and its conjugations are real, the image of F with respect to its canonical embedding actually lies in $\mathbb{R}^{n/2}$. Therefore, we can successfully define a ring homomorphism from F into the vector of purely real numbers, and make the use of plaintext encoding/decoding algorithms between R and $\mathbb{R}^{n/2}$ based on this canonical embedding.

We construct a new HE scheme whose security relies on the hardness of RLWE over R. We first propose a vector representation for the elements F, which is efficient for the rounding operation into R and the modulo operation of the residue ring $R_q = R/qR$. Then, we describe a HE scheme over the real numbers, which provides approximate arithmetic operations and an approximate rounding operation.

We also explain how to represent the elements of R_q and perform the arithmetic operations between them. We present a specialized Fast Fourier Transform (FFT) algorithm for an efficient

Number Theoretic Transform (NTT) on the residue ring R_q and fast multiplication between ring elements. This optimization technique constructs a simply computable ring isomorphism from R_q to $\mathbb{Z}_q[X]/(X^{n/2}-1)$, so the ordinary NTT conversion on $\mathbb{Z}_q[X]/(X^{n/2}-1)$ can be applied to R_q whose dimension is one quarter of that of a naive method.

In conclusion, our approximate HE scheme over R can encrypt $(n/2)$ plaintext slots in a single ciphertext, twice as many plaintext slots compared to $(n/4)$ of the ordinary HEAAN scheme over $\mathbb{Z}_q[X]/(X^{n/2}+1)$, while keeping the same concrete security level, storage, and computational costs.

Related Works. Arita and Handa [2] proposed a HE scheme based on RLWE over the decomposition ring, which is a subring of cyclotomic ring. Their subring technique is applied to HElib [20]: they consider the plaintext space as $\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$, which is a subring of the plaintext space $\mathrm{GF}(p^d) \oplus \cdots \oplus \mathrm{GF}(p^d)$ of HElib for some integers p and d, where $\mathrm{GF}(p^d)$ denotes the Galois field of the cardinality p^d. They claimed that RLWE over the decomposition ring is at least as hard as its search version. However, there is no known reduction from lattice problems over ideal lattices to the search version, since the decomposition ring is not known to be a ring of integers of some number field so far. In contrary, RLWE over the conjugate-invariant ring which we desired in this paper has a reduction from SIVP over ideal lattices.

Road-map. In section 2, we present notations of our paper and some backgrounds for RLWE. In section 3, we define RLWE over the conjugate-invariant ring and discuss about its hardness. In section 4, we present our new approximate HE scheme constructed over the conjugate-invariant ring, describe encoding/decoding algorithms for real numbers, and propose a specialized FFT algorithm for the desired ring. In last section, we give a summary on our approximate HE scheme compared to original HEAAN.

2 Background

2.1 Notation

All logarithms are base 2 unless otherwise indicated. For an integer $m \geq 2$, $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$, and $\mathbb{Z}_m^\times$ is the multiplicative group of units in $\mathbb{Z}_m$. For a ring R, its residue ring R/qR modular an integer q is denoted by R_q. For a real number r, $\lfloor r \rceil$ denotes the nearest integer to r, rounding upwards in case of a tie. For a vector $\boldsymbol{u}$ of (complex) numbers, $\|\boldsymbol{u}\|_2$ (resp. $\|\boldsymbol{u}\|_\infty$) denotes the ℓ_2-norm (resp. ℓ_∞-norm) of $\boldsymbol{u}$. For an element a of a number field K, $\|a\|_2^{\mathsf{can}}$ (resp. $\|a\|_\infty^{\mathsf{can}}$) denotes the ℓ_2-norm (resp. ℓ_∞-norm) of the image vector of a via the canonical embedding map. For vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ of the same dimension, $\boldsymbol{a} \odot \boldsymbol{b}$ denotes the component-wise multiplication of $\boldsymbol{a}$ and $\boldsymbol{b}$. We denote by $\phi(\cdot)$ the Euler's totient function and $\Phi_m(X)$ the m-th cyclotomic polynomial. For a complex number $z \in \mathbb{C}$, $\overline{z}$ denotes the complex conjugation of z. For a random variable X, $\mathsf{E}(X)$ denotes the expectation value of X.

2.2 Number Fields and Ideal Lattices

An (algebraic) number field is a finite extension field of $\mathbb{Q}$. For any number field K, there exists an element ζ of K such that $K = \mathbb{Q}(\zeta)$ since every number field is a simple extension. Hence K is isomorphic to $\mathbb{Q}[X]/(f(X))$ for the minimal polynomial $f(X)$ of ζ over $\mathbb{Q}$. The degree n of $f(X)$ equals to the extension degree $[K : \mathbb{Q}]$.

There exists exactly n injective ring homomorphisms $\sigma_j : K \to \mathbb{C}$ for $1 \leq j \leq n$. We call the n-tuple of these embeddings the canonical embedding of K into $\mathbb{C}^n$. The canonical embedding map is defined as

$$\begin{aligned} \sigma : K &\to \mathbb{C}^n \\ a &\mapsto (\sigma_j(a))_{1 \leq j \leq n}. \end{aligned}$$

Let s_1 be the number of real embeddings of K, then $n = s_1 + 2s_2$ for some non-negative integer s_2. Without loss of generality, let $\sigma_1, \ldots, \sigma_{s_1}$ be real embeddings of K. Then the image of σ actually lies in the space $\mathbb{H} := \{(x_1, ..., x_n) \in \mathbb{C}^n : x_{s_1+s_2+j} = \overline{x_{s_1+j}}, 1 \leq j \leq s_2\}$. Let $\{\boldsymbol{e}_j\}_{1 \leq j \leq n}$ be a canonical basis of $\mathbb{C}^n$. Let $\boldsymbol{h}_j = \boldsymbol{e}_j$ for $1 \leq j \leq s_1$, $\boldsymbol{h}_{s_1+j} = (\boldsymbol{e}_{s_1+j} + \boldsymbol{e}_{s_1+s_2+j})/\sqrt{2}$ and $\boldsymbol{h}_{s_1+s_2+j} = (\boldsymbol{e}_{s_1+j} - \boldsymbol{e}_{s_1+s_2+j})/\sqrt{-2}$ for $1 < j \leq s_2$. Then, $\{\boldsymbol{h}_j\}_{1 \leq j \leq n}$ forms an orthogonal $\mathbb{R}$-basis of H.

An element of K is called an algebraic integer if its minimal polynomial over $\mathbb{Q}$ has integral coefficients. The set of all algebraic integers, denoted by $\mathcal{O}_K$, is called the ring of integers of K. A fractional ideal I of K is $\mathcal{O}_K$-submodule of K such that there exists a non-zero element $r \in \mathcal{O}_K$ which satisfies $rI \subseteq \mathcal{O}_K$. If $I \subseteq \mathcal{O}_K$, then we call I an (integral) ideal. The image $\sigma(I)$ of a fractional ideal I via the canonical embedding σ forms a lattice in $\mathbb{C}^n$, and we call it an ideal lattice generated by I. The dual of I in K is a fractional ideal in K defined as $I^\vee := \{a \in K : \mathrm{Tr}(aI) \subseteq \mathbb{Z}\}$.

For $1 \leq k \leq n$, the k-th successive minima of the lattice $\mathcal{L}$, denoted by $\lambda_i(\mathcal{L})$, is the minimum value of $r > 0$ such that $\mathcal{L}$ has k linearly independent vectors of length at most r. If $\mathcal{L}$ is an ideal lattice $\sigma(I)$ for a fractional ideal $I \in K$, we simply denote by $\lambda_k(I)$. The SIVP over ideal lattices in K is defined as follow.

Definition 1. *(SIVP over ideal lattices) For a number field K of degree n and an approximation factor $\gamma \geq 1$, the K-SIVP_γ problem is: given a fractional ideal I of K, output n linearly independently vectors in the ideal lattice $\sigma(I)$ of length at most $\gamma \cdot \lambda_n(I)$.*

2.3 Ring Learning with Errors

For positive integers n and q, let R be the ring of integers of a number field K, $R_q = R/qR$ and $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$. Let χ_{key} and χ_{err} be distributions over $R^\vee$ and $K_\mathbb{R}$, respectively. For $s \in R_q^\vee$, $A_{q,\chi_{err}}^{R\text{-}\mathsf{LWE}}(s)$ is a distribution which draws $a \leftarrow R_q$ and $e \leftarrow \chi_{err}$, and output the pair $(a, a \cdot s + e)$ in $R_q \times K_\mathbb{R}/qR^\vee$. The (decisional) RLWE problem is defined as follows.

Definition 2 (Ring Learning with Errors). *Let n, q be positive integers, and χ_{key} (resp. χ_{err}) be a distribution over $R_q^\vee$ (resp. $K_\mathbb{R}$). The RLWE problem, denoted by R-$\mathsf{LWE}_{q,\chi_{err}}(\chi_{key})$, is to distinguish between the uniform distribution over $R_q \times K_\mathbb{R}/qR^\vee$ and $A_{q,\chi_{err}}^{R\text{-}\mathsf{LWE}}(s)$ where $s \leftarrow \chi_{key}$.*

Since $K_\mathbb{R}$ is isomorphic to the vector space H, a distribution over H can be identified as a distribution over $K_\mathbb{R}$. If χ_{err} is a (spherical) Gaussian distribution $D_{\alpha q}$ over H with respect to the basis $\{\boldsymbol{h}_i\}_{1 \leq i \leq n}$ and χ_{key} is the uniform distribution over $R_q^\vee$, we simply denote by R-$\mathsf{LWE}_{q,\alpha}$.

Lyubashevsky et al. [24] proposed a polynomial-time quantum reduction from lattice problems over ideal lattices to the RLWE problem, which holds only for the cyclotomic fields with some special conditions on the modulus q. Peikert et al. [26] gave a new reduction from the same problem which can be applied to an arbitrary number field and modulus.

Theorem 1. *[26, Corollary 7.3] Let n, q be positive integers, $0 < \alpha < 1$ be a real number such that $\alpha q = \omega(1)$, K be an arbitrary number field of degree n and $R = \mathcal{O}_K$. Then there exists a polynomial-time quantum reduction from K-SIVP_γ to R-$\mathsf{LWE}_{q,\alpha}$ given ℓ samples for $\gamma = \max\{\omega(\sqrt{n \log n}/\alpha) \cdot (n\ell/\log(n\ell))^{1/4}, \sqrt{2}n\}$.*

Recently, it was shown by Rosca et al. [28] that the non-dual RLWE problem, i.e., RLWE with the distribution of the secret over R_q rather than $R_q^\vee$, is at least as hard as the original RLWE problem. In addition, the rounding technique of Peikert [25] allows us to sample errors from a discrete Gaussian distribution rather than a continuous Gaussian distribution. With these settings, an RLWE sample lies in $R_q \times R_q$ rather than $R_q \times K_\mathbb{R}/qR^\vee$.

3 RLWE over the Conjugate-invariant Ring

The cyclotomic rings have been the most commonly used as base rings for RLWE for two main reasons. The ring of integers of the m-th cyclotomic field is isomorphic to $\mathbb{Z}[X]/(\Phi_m(X))$, and its structure was particularly well suitable in the construction of cryptographic schemes with the perspective of efficiency and some functionalities. In addition, there have been no known reduction to the RLWE over a non-cyclotomic ring for years until Peikert et al. [26] proposed a reduction from SIVP over ideal lattices to (decisional) RLWE for arbitrary number fields recently.

In this section, we introduce a new number field which has not been exploited in the lattice-based cryptography so far, and compute the ring of integers of the number field. Then we study on the hardness of RLWE problem over a new ring in two ways: we give a reduction from a standard lattice problem and study the concrete security level by considering all known attacks.

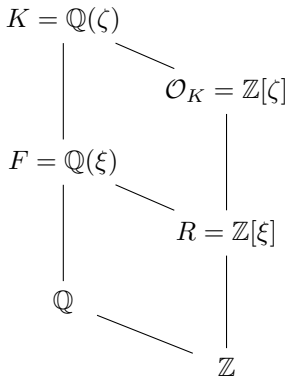
Let $m \geq 2$ be an integer and $n = \phi(m)$ for Euler's totient function $\phi(\cdot)$. For the m-th primitive root of unity $\zeta = \exp(2\pi i/m)$, the m-th cyclotomic field is defined by $K = \mathbb{Q}(\zeta)$. Let σ_{-1} be the element of $\mathrm{Gal}(K/\mathbb{Q})$ defined by $\sigma_{-1} : \zeta \mapsto \zeta^{-1}$, and $G = \{id, \sigma_{-1}\}$ be the cyclic subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ generated by σ_{-1}. We denote by $F = K^G$ the G-invariant subfield of K which is defined as $F = \{a \in K : \tau(a) = a, \forall \tau \in G\}$. We first remark that $F = \mathbb{Q}(\xi)$ for $\xi = \zeta + \zeta^{-1}$. It is clear that $\mathbb{Q}(\xi) \subseteq F \subseteq \mathbb{Q}(\zeta)$ and $[\mathbb{Q}(\zeta) : F] = |G| = 2$. Since ζ is a root of $X^2 + \xi \cdot X + 1 \in \mathbb{Q}(\xi)[X]$, the inequality $[\mathbb{Q}(\zeta) : \mathbb{Q}(\xi)] \leq 2$ holds and it implies $F = \mathbb{Q}(\xi)$. In particular, we are interested in the set of integer coefficient elements in $\mathbb{Q}(\xi)$ with respect to the $\mathbb{Q}$-basis $\{1, \xi, \xi^2, ..., \xi^{\frac{n}{2}-1}\}$. We will call this set $\mathbb{Z}[\xi]$ as the conjugate-invariant ring.

3.1 Reduction from SIVP

Some well-known reductions [24, 26] from standard problems over ideal lattices to RLWE requires a condition that the base ring exploited in RLWE should be a ring of integers of a number field. Therefore, it is crucial to study the ring of integers of a number field to define and show the hardness of RLWE problem.

We consider the subfield $F = \mathbb{Q}(\xi)$ of $K = \mathbb{Q}(\zeta)$ as a base number field, and compute its ring of integers $R := \mathcal{O}_F$ in this section. Fortunately, the structure of a cyclotomic field derives a quite simple and nice result on the conjugate-invariant ring as follows.

Fig. 1. Diagram of the cyclotomic ring and the conjugate-invariant ring



Lemma 1. *$\mathbb{Z}[\xi]$ is the ring of integers of $F = \mathbb{Q}(\xi)$.*

Proof. It is clear that $\mathbb{Z}[\xi] \subseteq \mathcal{O}_F$. Since $\mathcal{O}_F \subseteq \mathcal{O}_K = \mathbb{Z}[\zeta]$, every element $a \in \mathcal{O}_F$ is uniquely expressed as $a = \sum_{-\frac{n}{2} \le j < \frac{n}{2}} a_j \cdot \zeta^j$ for some integers $a_{-\frac{n}{2}}, \ldots, a_{\frac{n}{2}-1}$. From the definition of F, we obtain $\sigma_{-1}(a) = a$, i.e., $\sum_{-\frac{n}{2} \le j < \frac{n}{2}} a_j \zeta^j = \sum_{-\frac{n}{2} < j \le \frac{n}{2}} a_{-j} \zeta^j$ which implies $a_j = a_{-j}$ for $0 \le i < \frac{n}{2}$ and $a_{-\frac{n}{2}} = 0$. Then, $a = a_0 + \sum_{j=1}^{\frac{n}{2}-1} a_i(\zeta^j + \zeta^{-j}) \in \mathbb{Z}[\xi]$, since $\zeta^j + \zeta^{-j} \in \mathbb{Z}[\xi]$ for $1 \le j < \frac{n}{2}$. Therefore, $\mathcal{O}_F \subseteq \mathbb{Z}[\xi]$, which directly implies $\mathbb{Z}[\xi] = \mathcal{O}_F$. □

From Lemma 1, we can derive a conclusion that the RLWE problem over $R = \mathbb{Z}[\xi]$, simply denoted by R-$\mathsf{LWE}_{q,\alpha}$, is at least as hard as F-SIVP from Theorem 1.

We can naturally identify R with the ring of polynomials $\mathbb{Z}[Y]/(g(Y))$ for the minimal polynomial $g(Y) \in \mathbb{Z}[Y]$ of ξ over $\mathbb{Q}$ via mapping $a(Y) \mapsto a(\xi)$. However, it is more convenient to consider R as the subring

$$R = \{a(X) \in \mathbb{Z}[X]/(\Phi_m(X)) : a(X) = a(X^{-1})\}$$

of $\mathcal{O}_K = \mathbb{Z}[X]/(\Phi_m(X))$, where $X^{-1} \in Z[X]/(\Phi_m(X))$ denotes the inverse of X modulo $\Phi_m(X)$. Note that the condition $a(X) = a(X^{-1})$ corresponds to the conjugation-invariant property. We will follow this subring perspective in the rest of paper.

3.2 Cryptanalysis

In this section, we discuss the attack complexity of RLWE over the conjugate-invariant ring. In general, the RLWE problem does not guarantee the same security level as LWE with the same parameter. For example, there have been several attempts to attack the RLWE (or Poly-LWE) problem over a ring $\mathbb{Z}[X]/(f(X))$ by exploiting its ring structure [15, 6, 8]. One common limitation of these attacks is that $f(X)$ should have a root modulo q satisfying some strong conditions.

The RLWE assumption can be viewed as a specific case of LWE $(A, \boldsymbol{b} = A\boldsymbol{s} + \boldsymbol{e})$ where the random matrix A has a special algebraic structure. In the case of RLWE over a power-of-two cyclotomic ring, an RLWE sample can be understood as a variant of n-dimensional LWE instance where A is a random anti-circulant matrix. However, there has been no known attack achieving a lower complexity by exploiting this property. As a result, the current best known attacks are standard lattice attacks on the ordinary LWE problem such as dual attack and primal attack, which are well described in [7].

Now we explain how to understand an R-LWE instance as an LWE instance with a special structure. Let m be a power-of-two integer so that $n = m/2$ and $\Phi_m(X) = X^n + 1$. An element of $R = \{a(X) \in \mathbb{Z}[X]/(X^n + 1) : a(X) = a(X^{-1})\}$ can be uniquely expressed as $a(X) = a_0 + \sum_{j=1}^{\frac{n}{2}-1} a_j \cdot (X^j + X^{-j})$ for some integers $a_0, \ldots, a_{\frac{n}{2}-1}$. Therefore, $a(X)$ can be identified with the vector $\boldsymbol{a} = (a_0, a_1, ..., a_{\frac{n}{2}-1})$ of length $(n/2)$. Based on this identification, an RLWE sample over the conjugate-invariant ring $(a(X), b(X) = a(X) \cdot s(X) + e(X)) \in R_q^2$ with secret $s(X)$ can be transformed to

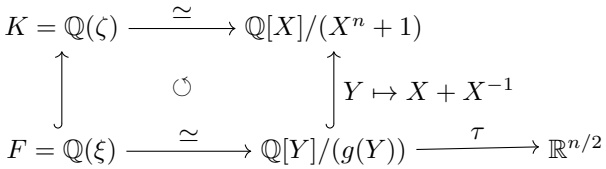
$$(A, \boldsymbol{b} = A\boldsymbol{s} + \boldsymbol{e}) \in \mathbb{Z}_q^{\frac{n}{2} \times \frac{n}{2}} \times \mathbb{Z}_q^{\frac{n}{2}}$$

where A is a square matrix of size $(n/2)$ whose (i, j)-th component is given by

$$A_{ij} = \begin{cases} a_{|i-j|} & j = 0, \text{ or } i + j = \frac{n}{2} \\ a_{|i-j|} + a_{i+j} & j > 0, \text{ and } i + j < \frac{n}{2} \\ a_{|i-j|} - a_{n-(i+j)} & j > 0, \text{ and } i + j > \frac{n}{2} \end{cases}$$

for $0 \le i, j < n/2$. This transformation shows that R-LWE can be viewed as a variant of the $(n/2)$-dimensional LWE problem where the random matrix A has this special form. We consider all known attacks on RLWE and claim that they do not achieve a lower complexity than the

Fig. 2. Polynomial representation of number fields and canonical embedding



standard lattice attacks on LWE, i.e., currently there is no special attack on R-LWE which exploits the ring structure of R corresponding to this special structural distribution of A, similar to the case of RLWE over a power-of-two cyclotomic ring. Therefore, we conclude that the current best attacks on R-$\mathsf{LWE}_{q,\alpha}$ are the standard lattice attacks, which require the same attack complexity as the lattice attacks on the $(n/2)$-dimensional LWE problem.

4 Approximate Homomorphic Encryption over the Real Numbers

The HEAAN scheme of Cheon et al. [10, 9] is the first HE system which supports an efficient rounding operation for approximate arithmetic. It allows us to encrypt a number of complex numbers in a single ciphertext and perform an approximate arithmetic between encrypted vectors in a SIMD manner. However, there remained one significant problem about the plaintext space.

Most of the real-world applications require computations over the purely real numbers, but the original HEAAN scheme could encrypt a complex number in each of plaintext slots. The previous researches [22, 21] used the set of real numbers as a subring of complex numbers, but this approach cannot be a fundamental solution for the following reason. Every algorithm of the original HEAAN scheme, such as homomorphic arithmetic and rounding operation, adds a small complex error to the plaintext vector. The imaginary part of an encrypted plaintext can gradually increase as the computation progressed, and finally the desired result (real part) can no longer be recovered after its imaginary part becomes larger than the ciphertext modulus. Consequently, every circuit in previous applications had a limited depth to bound the size of imaginary parts during its evaluation.

In this section, we describe a HE scheme which is optimized in the approximate computation over the *real* numbers compared to the original HEAAN scheme with complex plaintext slots. The security of our scheme relies on the RLWE assumption over the ring $R = \mathbb{Z}[\xi]$ introduced in the previous section. For simplicity, the integer m will be chosen as a power of two so that $n = m/2$ and $\Phi_m(X) = X^n + 1$.

4.1 Canonical Embedding and Packing Technique

In this subsection, we describe the canonical embedding map of the conjugate-invariant field and explain how to represent its elements. As mentioned in the previous section, the conjugate-invariant field $F = \mathbb{Q}(\xi)$ can be identified with the polynomial ring $\mathbb{Q}[Y]/(g(Y))$ for the minimal polynomial $g(Y) \in \mathbb{Z}[Y]$ of ξ over $\mathbb{Q}$. Note that $g(Y)$ is the polynomial of degree $(n/2)$ that satisfies $g(X + X^{-1}) = X^{n/2} + X^{-n/2}$. Let $\xi_j = \zeta^{4j+1} + \zeta^{-(4j+1)}$ for $0 \le j < n/2$. Then $\{\xi_0, \ldots, \xi_{\frac{n}{2}-1}\}$ forms the set of distinct roots of $g(Y)$ since $X^n + 1 = (X - \zeta)(X - \zeta^3) \ldots (X - \zeta^{m-1}) = \prod_{j=0}^{\frac{n}{2}-1} (X^2 - \xi_j \cdot X + 1)$. Therefore, we have a commute diagram (Fig. 2) for a polynomial representation of number fields by identifying $Y \mapsto X + X^{-1}$.

Let us denote by τ the canonical embedding of $F = \mathbb{Q}[Y]/(g(Y))$ into $\mathbb{C}^{n/2}$. It sends an element $a(Y)$ to the vector of its evaluations $\tau(a) = (a(\xi_j))_{0 \le j < \frac{n}{2}}$ at the roots of $g(Y)$. Since all roots of $g(Y)$ are real, F is a totally real number field and the image of τ is a subring of $\mathbb{R}^{n/2}$. The canonical embedding norm of an element of a number field is defined by the norm of its canonical embedding. For example, we write $\|a\|_\infty^{\mathsf{can}} := \|\tau(a)\|_\infty$ and $\|a\|_2^{\mathsf{can}} := \|\tau(a)\|_2$ for $a \in F$.

The packing technique of HE system allows us to encrypt a multiple number of messages in a single ciphertext and supports the parallel computation in a SIMD manner. It has been one of the most important techniques to improve the performance of HE schemes in the sense of expansion rate and amortized computational cost. Cheon et al. [10, 9] first suggested a packing method for the approximate HE scheme based on the canonical embedding over the complex numbers.

We present a new packing method over the real numbers, by modifying the previous solution over the complex plane. The core idea is to restrict the domain of canonical embedding τ to the ring of integers $R = \mathbb{Z}[Y]/(g(Y))$. In other words, the decoding algorithm transforms an element $a(Y)$ of R into the vector $\tau(a) = (a(\xi_j))_{0 \le j < n/2}$ of dimension $(n/2)$. This vector is real as noted above. Conversely, the encoding map takes a real vector $\boldsymbol{x} = (x_j)_{0 \le j < n/2} \in \mathbb{R}^{n/2}$ as an input. It first computes the rounding $\boldsymbol{x}' = \lfloor \boldsymbol{x} \rceil_{\tau(R)} \in \mathbb{R}^{n/2}$, which is an element of $\tau(R)$ with a small rounding error $\|\boldsymbol{x} - \boldsymbol{x}'\|_2^{\mathsf{can}}$. The output is obtained by computing the inverse of $\boldsymbol{x}'$ which is an integral polynomial in $R = \mathbb{Z}[Y]/(g(Y))$. Our packing method is explicitly described as follows.

- $\mathtt{Ecd}(\boldsymbol{x})$. For given $\boldsymbol{x} = (x_j)_{0 \le j < n/2} \in \mathbb{R}^{n/2}$, discretize $\boldsymbol{x}$ into $\tau(R)$. Output the corresponding polynomial $\mathfrak{m}(Y) = \tau^{-1}\left(\lfloor \boldsymbol{x} \rceil_{\tau(R)}\right) \in R$.
- $\mathtt{Dcd}(\mathfrak{m})$. For given $\mathfrak{m} \in R$, output the vector $\boldsymbol{x} = (x_j = \mathfrak{m}(\xi_j))_{0 \le j < n/2} \in \mathbb{R}^{n/2}$.

The $\mathtt{Ecd}$ algorithm can be viewed as an approximate inverse of the decoding function with a small rounding error. One can multiply a scale factor to an input vector before the rounding operation to reduce the relative size of rounding error and preserve the precision of plaintexts.

As a toy example, let $n = m/2 = 4$. In this case, $\zeta_8 = \exp(\pi i/4) = (1+i)/\sqrt{2}$ is an m-th primitive root of unity, and we have $\{\xi_0, \xi_1\} = \{\sqrt{2}, -\sqrt{2}\}$. For a real vector $\boldsymbol{x} = (1.1, 2.3)$, its encoding polynomial with the scaling factor $\Delta = 64$ is obtained by $\mathfrak{m}(Y) = \tau^{-1}\left(\lfloor \Delta \cdot \boldsymbol{x} \rceil_{\tau(R)}\right) = 109 - 27Y$. Conversely, the decoded vector of $109 - 27Y$ is computed by $\Delta^{-1} \cdot \mathtt{Dcd}(\mathfrak{m}) = \frac{1}{64}(109 - 27\sqrt{2}, 109 + 27\sqrt{2}) \approx (1.1065, 2.2997)$, which is a good approximation of the original vector $\boldsymbol{x}$.

4.2 Scheme Description

This subsection gives a explicit description of our HE scheme over the real numbers. Our scheme is very similar to the original HEAAN scheme, but it exploits a different ring structure $R = \mathbb{Z}[\xi]$. We first propose a method to represent the elements of the conjugate-invariant field F.

The number field F can be identified with $\mathbb{Q}^{n/2}$ as a $\mathbb{Q}$-module. For example, an arbitrary element of $F = \mathbb{Q}[Y]/(g(Y))$ can be uniquely expressed as the sum $\sum_{j=0}^{\frac{n}{2}-1} a_j \cdot Y^j$ for some $a_j \in \mathbb{Q}$, which corresponds to the isomorphism $a \mapsto (a_0, \ldots, a_{\frac{n}{2}-1})$ between two modules. However, this representation is not the best choice for the construction of HE system. One major reason is that the image $\{\tau(1), \tau(Y), \ldots, \tau(Y^{\frac{n}{2}-1})\}$ of the basis $\{1, Y, \ldots, Y^{\frac{n}{2}-1}\}$ does not form an orthogonal set in the space $\mathbb{R}^{n/2}$.

The conjugate-invariant field $F = \mathbb{Q}[Y]/(g(Y))$ can be understood as a subfield of $K = \mathbb{Q}[X]/(X^n + 1)$ by identifying $Y = X + X^{-1}$ as noted in the previous subsection. Every element $a(X)$ of $F \le K$ can be uniquely expressed as a Laurent polynomial $a(X) = a_0 + \sum_{i=1}^{\frac{n}{2}-1} a_i(X^i + X^{-i})$ of degree and order strictly less then $(n/2)$ for some $a_0, \ldots, a_{\frac{n}{2}-1} \in \mathbb{Q}$. In the following, an arbitrary element $a(X)$ of F will be identified with its vector of coefficients $(a_0, \ldots, a_{\frac{n}{2}-1}) \in \mathbb{Q}^{n/2}$. Note that the set $\{1, X + X^{-1}, \ldots, X^{n/2-1} + X^{1-n/2}\}$ is a basis of F (resp. R) as a module over

$\mathbb{Q}$ (resp. $\mathbb{Z}$). In addition, the image of this basis with respect to the canonical embedding map τ forms an orthogonal basis in $\mathbb{R}^{n/2}$.

This orthogonal property allows us to use an efficient rounding operation on F as well as a modulo operation over R. We define the rounding operation $\lfloor \cdot \rceil : F \to R$ by sending each of coefficients $a_i \in \mathbb{Q}$ to the closest integer $\lfloor a_i \rceil \in \mathbb{Z}$. Note that $\lfloor a \rceil$ is an element of R which minimizes the rounding error $\|a - \lfloor a \rceil\|_2^{\mathsf{can}}$ with respect to the ℓ_2 canonical embedding norm. Similar to the rounding operation, the modulo q operation is simply defined by the coefficient-wise modular reduction, i.e., $[a]_q$ is the element of $a + qR$ which minimizes the size $\|[a]_q\|_2^{\mathsf{can}}$.

- $\underline{\mathtt{Setup}(p, 1^\lambda, L)}$.
  - The base integer p, the number of levels L and the security parameter λ are given as input. Set moduli $q_1, q_2, ..., q_L$, which are usually chosen as $q_i = p^i$.
  - Choose integers m and P, and small distributions χ_{key}, χ_{enc}, and χ_{err} over the ring R.
  - Return the parameter set $\mathsf{params} \leftarrow (m, P, \chi_{key}, \chi_{enc}, \chi_{err})$.

The setup step should generate a HE parameter set that achieves λ-bit of security level against the best known attacks on RLWE. A security proof will be given at the end of this subsection.

- $\underline{\mathtt{KeyGen}(\mathsf{params})}$.
  - Sample $s \leftarrow \chi_{key}$. Set the secret key as $\mathsf{sk} \leftarrow (1, s)$.
  - Sample $a \leftarrow U(R_{q_L})$ and $e \leftarrow \chi_{err}$. Set the public key as $\mathsf{pk} \leftarrow (b, a) \in R_{q_L}^2$ where $b \leftarrow -as + e \pmod{q_L}$.
- $\underline{\mathtt{KSGen}(s_1, s_2)}$. For $s_1, s_2 \in R$, sample $a' \leftarrow U(R_{P \cdot q_L})$ and $e' \leftarrow \chi_{err}$. Output the switching key as $\mathsf{swk} \leftarrow (b', a') \in R_{P \cdot q_L}^2$ where $b' \leftarrow -a's_2 + e' + P \cdot s_1 \pmod{P \cdot q_L}$.
  - Set the evaluation key as $\mathsf{evk} \leftarrow \mathtt{KSGen}(s^2, s)$.
- $\underline{\mathtt{Enc}_{\mathsf{pk}}(\mathtt{m})}$. For $\mathtt{m} \in R$, sample $v \leftarrow \chi_{enc}$ and $e_0, e_1 \leftarrow \chi_{err}$. Output $v \cdot \mathsf{pk} + (\mathtt{m} + e_0, e_1) \pmod{q_L}$.
- $\underline{\mathtt{Dec}_{\mathsf{sk}}(\mathsf{ct})}$. For $\mathsf{ct} = (c_0, c_1) \in R_{q_\ell}^2$, output $\mathtt{m}' = c_0 + c_1 \cdot s \pmod{q_\ell}$.

The decryption algorithm can be simply written by $\mathtt{m}' \leftarrow [\langle \mathsf{ct}, \mathsf{sk} \rangle]_{q_\ell}$. The encryption procedure returns a level L ciphertext ct which satisfies $[\langle \mathsf{ct}, \mathsf{sk} \rangle]_{q_L} \approx \mathtt{m}$, i.e., we can only recover an approximate value of $\mathtt{m}$ from its encryption. We use the canonical embedding norm to measure the size of polynomials in R.

- $\underline{\mathtt{Add}(\mathsf{ct}, \mathsf{ct}')}$. For $\mathsf{ct}, \mathsf{ct}' \in R_{q_\ell}^2$, output $\mathsf{ct}_{add} \leftarrow \mathsf{ct} + \mathsf{ct}' \pmod{q_\ell}$.
- $\underline{\mathtt{Mult}_{\mathsf{evk}}(\mathsf{ct}, \mathsf{ct}')}$. For $\mathsf{ct} = (c_0, c_1), \mathsf{ct}' = (c_0', c_1') \in \mathcal{R}_{q_\ell}^2$, let $(d_0, d_1, d_2) = (c_0c_0', c_0c_1' + c_1c_0', c_1c_1') \pmod{q_\ell}$. Output $\mathsf{ct}_{mult} \leftarrow (d_0, d_1) + \lfloor P^{-1} \cdot d_2 \cdot \mathsf{evk} \rceil \pmod{q_\ell}$.
- $\underline{\mathtt{RS}_{\ell \to \ell'}(\mathsf{ct})}$. For a ciphertext $\mathsf{ct} \in R_{q_\ell}^2$ at level ℓ, output $\mathsf{ct}' \leftarrow \lfloor (q_{\ell'}/q_\ell) \cdot \mathsf{ct} \rceil \pmod{q_{\ell'}}$. We will omit the subscript $(\ell \to \ell')$ when $\ell' = \ell - 1$.

The algorithms $\mathtt{Add}$ and $\mathtt{Mult}_{\mathsf{evk}}$ perform the arithmetic operations over encrypted plaintexts. The *rescaling* procedure $\mathtt{RS}_{\ell \to \ell'}(\cdot)$ transforms a level ℓ encryption of $\mathtt{m}$ into an encryption of $(q_{\ell'}/q_\ell) \cdot \mathtt{m}$ of level ℓ' securely. We show the correctness of our scheme and estimate the size of noise in Appendix.

Security. We claim that our HE scheme is IND-CPA secure under the hardness of RLWE problems over the ring R. It can be shown by considering the following three distributions:

$$\mathcal{D}_1 = \{(\mathsf{pk}, \mathsf{ct}) : \mathsf{pk} \leftarrow \mathtt{KeyGen}(\mathsf{params}), \mathsf{ct} \leftarrow \mathtt{Enc}_{\mathsf{pk}}(0)\},$$
$$\mathcal{D}_2 = \{(\mathsf{pk}, \mathsf{ct}) : \mathsf{pk} \leftarrow U(\mathcal{R}_q^2), \mathsf{ct} \leftarrow \mathtt{Enc}_{\mathsf{pk}}(0)\},$$
$$\mathcal{D}_3 = \{(\mathsf{pk}, \mathsf{ct}) : \mathsf{pk} \leftarrow U(\mathcal{R}_q^2), \mathsf{ct} \leftarrow U(\mathcal{R}_q^2)\}.$$

First, the distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ are computationally indistinguishable under the assumption of R-$\mathsf{LWE}_{q_L, \chi_{err}}(\chi_{key})$ since the key generation step samples s from χ_{key} and generates an RLWE

sample pk of parameter (q_L, χ_{err}). The second and third distributions are computationally indistinguishable as long as $R\text{-}\mathsf{LWE}_{q_L,\chi_{err}}(\chi_{enc})$ since a sample from $\mathcal{D}_2$ forms two independent RLWE samples of parameter (q_L, χ_{err}) with a secret $v \leftarrow \chi_{enc}$. Finally, the evaluation key $\mathsf{evk} \leftarrow \mathtt{KSGen}(s^2, s)$ can be viewed as an encryption of s^2 encrypted by the secret s. The distribution of evk can be indistinguishable from the uniform distribution on $\mathcal{R}^2_{P \cdot q_L}$ under the assumption of circular security when the $R\text{-}\mathsf{LWE}_{P \cdot q_L,\chi_{err}}(\chi_{key})$ problem is hard.

4.3 Implications of the Conjugate-Invariant Ring

This section compares our approximate HE scheme over the real numbers with the original HEAAN scheme from a variety of perspectives. We claim that our scheme can have twice as many plaintext slots as HEAAN while guaranteeing the same security level and performance. Furthermore, the utilization of the conjugate-invariant ring fundamentally blocks the complex explosion problem of HEAAN which possibly effect on the most significant bits of real messages.

Representation of ring elements. Our HE scheme is constructed over the residue ring $R_q = \{a(X) \in \mathbb{Z}_q[X]/(X^n+1) : a(X) = a(X^{-1})\}$ for an integer q. We introduce two methods to represent the ring elements of R_q, both of which have their own pros and cons.

Basically we use the coefficient representation $(a_0, \ldots, a_{n-1}) \in \mathbb{Z}_q^{n/2}$ for an element $a(X) \in R_q$ as described in the previous subsection. The coefficient representation is useful to perform the non-arithmetic operations such as the rounding operation in rescaling procedure. However, we have to consider the following representation for an efficient multiplication between polynomials in R_q.

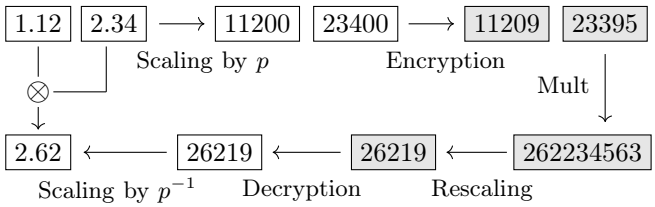
Suppose that q is an integer such that there exists an m-th primitive root ω_m of unity in the modulo space $\mathbb{Z}_q$. Note that $\omega_n := \omega_m^2$ (resp. $\omega_{\frac{n}{2}} := \omega_m^4$) is an n-th (resp. $(n/2)$-th) primitive root of unity in $\mathbb{Z}_q$. The map $Z_q[X]/(X^n+1) \to \mathbb{Z}_q^n$, $a \mapsto (a(\omega_m), a(\omega_m^3), \ldots, a(\omega_m^{m-1}))$ is a ring isomorphism since the m-th cyclotomic polynomial is expressed as a product $X^n + 1 = (X-\omega_m)(X-\omega_m^3)\ldots(X-\omega_m^{2n-1})$ modulo q. We point out that an element $a \in \mathbb{Z}_q[X]/(X^n+1)$ is contained in the subring R_q if and only if $a(\omega_m^j) = a(\omega_m^{2n-j})$ for all $j = 1, 3, \ldots, n-1$. Therefore, we can deduce an ring isomorphism from R_q to $\mathbb{Z}_q^{n/2}$ defined by $a \mapsto \hat{a} = (a(\omega_m), a(\omega_m^5), \ldots, a(\omega_m^{m-3}))$, i.e., it is satisfied that $\widehat{a \cdot b} = \hat{a} \odot \hat{b}$ for any $a, b \in R_q$ where $\odot$ denotes the Hadamard (component-wise) multiplication between vectors. It enables us to perform an arithmetic operation of R_q in $O(n)$ modulo q operations, but the rescaling procedure cannot be done under this representation.

Complexity of ring operations. The conversion between two representations $a \mapsto \hat{a}$ is one of the most important parts to improve the efficiency of the HE system on R_q. It can be viewed as a linear transformation on $\mathbb{Z}_q^{n/2}$ by identifying the elements of R_q with their coefficient vectors.

The NTT is a discrete Fourier transform over a finite field. Specifically, the NTT over the finite field $\mathbb{Z}_q$ with an m-th primitive root ω_m of unity modulo q, denoted by $\mathtt{NTT}_m(\cdot)$, converts a polynomial in $\mathbb{Z}_q[X]/(X^m-1)$ into a vector in $\mathbb{Z}_q^m$ by $a \mapsto (a(\omega_m^j))_{0 \le j < m}$. The NTT is a ring isomorphism between $\mathbb{Z}_q[X]/(X^m-1)$ and $\mathbb{Z}_q^m$, and its inverse is denoted by $\mathtt{INTT}_m(\cdot)$. The NTT conversion can be understood as a linear map from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q^n$ whose matrix representation is the $m \times m$ Vandermonde matrix generated by $\{1, \omega_m, \ldots, \omega_m^{m-1}\}$. The FFT algorithm can compute $\mathtt{NTT}_m(\cdot)$ in $O(m \cdot \log m)$ operations in $\mathbb{Z}_q$.

There have been suggested several methods to modify the NTT conversion to perform some operations used in cryptographic schemes. For example, Alkim et al. [1] and Longa-Naehrig [23] exploit a variant of NTT to make an efficient conversion between distinct representations of a ring element in $\mathbb{Z}_q[X]/(X^n+1)$. In the following, we propose a specialized FFT algorithm to perform the linear transformation $a \mapsto \hat{a}$ on R_q efficiently.

Fig. 3. An example of fixed-point operation



The main idea is to express the linear transformation $a \mapsto \hat{a}$ by a composition of $(n/2)$-dimensional NTT conversion and a few simple arithmetic operations. To be precise, the equality

$$\begin{aligned} a(\omega_m^{4j+1}) = a(\omega_m \cdot \omega_{\frac{n}{2}}^{j}) &= a_0 + \sum_{i=1}^{\frac{n}{2}-1} a_i \left(\omega_m^i \cdot \omega_{\frac{n}{2}}^{ij} + \omega_m^{-i} \cdot \omega_{\frac{n}{2}}^{-ij}\right) \\ &= a_0 + \sum_{i=1}^{\frac{n}{2}-1} a_i \cdot \omega_m^i \cdot \omega_{\frac{n}{2}}^{ij} + \sum_{i=1}^{\frac{n}{2}-1} a_{\frac{n}{2}-i} \cdot \omega_m^{-(\frac{n}{2}-i)} \cdot \omega_{\frac{n}{2}}^{ij} \\ &= a_0 + \sum_{i=1}^{\frac{n}{2}-1} \left(a_i \cdot \omega_m^i + a_{\frac{n}{2}-i} \cdot \omega_m^{-(\frac{n}{2}-i)}\right) \omega_{\frac{n}{2}}^{ij} = \tilde{a}(\omega_{\frac{n}{2}}^{j}) \end{aligned}$$

holds for any $0 \le j < \frac{n}{2}$ where

$$\tilde{a}(X) = a_0 + \left(a_1 \cdot \omega_m + a_{\frac{n}{2}-1} \cdot \omega_m^{1-\frac{n}{2}}\right) X + \cdots + \left(a_{\frac{n}{2}-1} \cdot \omega_m^{\frac{n}{2}-1} + a_1 \cdot \omega_m^{-1}\right) X^{\frac{n}{2}-1}.$$

Therefore, the linear transformation $a \mapsto \hat{a}$ can be written by the composition of $\mathtt{NTT}_{n/2}$ and a simple arithmetic operation

$$(a_0, \ldots, a_{\frac{n}{2}-1}) \mapsto (a_0, a_1 \cdot \omega_m + a_{\frac{n}{2}-1} \cdot \omega_m^{1-\frac{n}{2}}, \ldots, a_{\frac{n}{2}-1} \cdot \omega_m^{\frac{n}{2}-1} + a_1 \cdot \omega_m^{-1}),$$

and we can compute its inverse by

$$a = (\tilde{a}_0,\ 2^{-1} \cdot (\tilde{a}_1 \cdot \omega_m^{-1} + \tilde{a}_{\frac{n}{2}-1} \cdot \omega_m), \ldots,\ 2^{-1} \cdot (\tilde{a}_{\frac{n}{2}-1} \cdot \omega_m^{1-\frac{n}{2}} + \tilde{a}_1 \cdot \omega_m^{\frac{n}{2}-1}))$$

for $\tilde{a} = (\tilde{a}_0, \ldots, \tilde{a}_{\frac{n}{2}-1}) \leftarrow \mathtt{INTT}_{n/2}(\hat{a})$.

Now let us consider the multiplication of polynomials in the conjugate-invariant ring R. For given polynomials $a, b \in R_q$ with coefficient representation, we compute their product $c = a \cdot b$ by computing $\hat{c} = \widehat{a \cdot b} = \hat{a} \odot \hat{b}$ and recovering c from $\hat{c}$. It consists of three Hadamard multiplications on $\mathbb{Z}_q^{\frac{n}{2}}$, two $\mathtt{NTT}_{n/2}$ conversions, and a single $\mathtt{INTT}_{n/2}$. Since the Hadamard multiplication takes only $O(n)$, the complexity of a multiplication over the special ring R_q can be estimated by three NTT conversions of dimension $(n/2)$, while a multiplication over the ring $\mathbb{Z}_q[X]/(X^n+1)$ includes three NTT conversions of dimension n. As a result, the computational cost of an arithmetic operation on R_q is almost half that of the m-th cyclotomic ring.

4.4 Application to Fixed-Point Operation

The HEAAN scheme is able to evaluate a circuit approximately, and specifically our variant is optimized in an arithmetic over the real numbers. We explain how to use our scheme to perform the fixed-point operation with a finite precision.

As described in Section 4.1, a real-valued vector can be identified with a polynomial in the conjugate-invariant ring R via the canonical embedding τ. For the use of our scheme in fixed-point operation, the base p in scheme description will be chosen as a scaling factor. So an arbitrary real vector $\boldsymbol{x} \in \mathbb{R}^{n/2}$ is encoded to a polynomial $\mathtt{m} \in R$ such that $\mathtt{m} \approx p \cdot \tau^{-1}(\boldsymbol{x})$ with a small rounding error. An encryption procedure induces an additional error so that an encryption of $\mathtt{m}$ is a pair $\mathtt{ct} = (c_0, c_1) \in R_{q_L}^2$ satisfying $[c_0 + c_1 \cdot s]_{q_L} = \mathtt{m} + e \approx p \cdot \tau^{-1}(\boldsymbol{x})$ for some small error e. We estimate rounding and encryption errors in Appendix, and the precision of encrypted plaintext is decided by a scaling factor p and the size of errors, i.e., a larger scaling factor allows us to keep more significant bits.

Let $\mathtt{ct}_i$ be an encryption of $\mathtt{m}_i \approx p \cdot \tau^{-1}(\boldsymbol{x}_i)$ for $i = 1, 2$. Then their homomorphic multiplication returns a ciphertext $\mathtt{ct}_{mult}$ encrypting

$$\mathtt{m}_1 \cdot \mathtt{m}_2 \approx p^2 \cdot \tau^{-1}(\boldsymbol{x}_1) \cdot \tau^{-1}(\boldsymbol{x}_2) = p^2 \cdot \tau^{-1}(\boldsymbol{x}_1 \odot \boldsymbol{x}_2)$$

which is an encoding of the slot-wise product $\boldsymbol{x}_1 \odot \boldsymbol{x}_2$ with scaling factor p^2. Then, we can use the rescaling procedure $\mathtt{RS}(\cdot)$ to obtain an encryption of $p \cdot \tau^{-1}(\boldsymbol{x}_1 \odot \boldsymbol{x}_2)$ and recover the initial scaling factor p. Fig. 3 describes an example of a fixed-point multiplication between 1.12 and 2.34 with scaling factor $p = 10^4$. Numbers in gray boxes represent the encrypted values in plaintext slots.

The scaling factor stays the same and the rescaling procedure reduces a ciphertext level by one. Therefore, for the evaluation of a circuit with depth L, the bitsize of largest ciphertext modulus should be $O(L \cdot \log p)$ which grows linearly on the depth and bit precision of plaintext, compared to the exponential growth based on the HE schemes for exact computations without rounding operation [5, 16].

5 Discussions

The security of our scheme relies on the hardness of R-LWE problem. From the cryptanalysis on RLWE over the conjugate-invariant ring in Section 3.2, our approximate HE scheme over $R = \{a(X) \in \mathbb{Z}[X]/(X^{2n}+1) : a(X) = a(X^{-1})\}$ has (approximately) the same security level as the original HEAAN over $\mathbb{Z}[X]/(X^n+1)$ for a power-of-two integer n, while the other parameters are set equal. In this setting, the maximum number of plaintexts packed in a single ciphertext in our scheme is n, while that of HEAAN is $(n/2)$. This implies our approximate HE scheme supports twice more parallel computations than HEAAN in a SIMD manner.

Since it requires $n \log q$ bits to express an element of the form $a_0 + \sum_{i=1}^{n-1} a_i(X^i + X^{-i}) \in R_q$, both schemes essentially have the same key size and ciphertext size. Furthermore, both schemes exploit the NTT of dimension n for a ring multiplication, so they have almost same arithmetic complexity. As a result, our scheme over the dimension $2n$ actually performs as well as HEAAN over the dimension n while carrying a definite advantage in the number of plaintext slots.

Table 1. Comparison of our scheme and HEAAN

Approximate HE	$\mathtt{OurScheme}(2n, q)$	HEAAN(n, q)
Number of plaintext slots	n	$n/2$
NTT dimension	n	n
Bit size of ciphertexts	$2n \log q$	$2n \log q$

References

1. Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange—a new hope. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 327–343, Austin, TX, 2016. USENIX Association.
2. Seiko Arita and Sari Handa. Subring Homomorphic Encryption. In *International Conference on Information Security and Cryptology*, pages 112—-136. Springer, 2018.
3. Joppe W Bos, Kristin Lauter, Jake Loftus, and Michael Naehrig. Improved security for a ring-based fully homomorphic encryption scheme. In *Cryptography and Coding*, pages 45–64. Springer, 2013.
4. Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In *Advances in Cryptology–CRYPTO 2012*, pages 868–886. Springer, 2012.
5. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In *Proc. of ITCS*, pages 309–325. ACM, 2012.
6. Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. Provably weak instances of ring-lwe revisited. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 147–167. Springer, 2016.
7. Melissa Chase, Hao Chen, Jintai Ding, Shafi Goldwasser, Sergey Gorbunov, Jeffrey Hoffstein, Kristin Lauter, Satya Lokam, Dustin Moody, Travis Morrison, Amit Sahai, and Vinod Vaikuntanathan. Security of homomorphic encryption. Technical report, HomomorphicEncryption.org, Redmond WA, July 2017.
8. Hao Chen, Kristin E Lauter, and Katherine E Stange. Attacks on search rlwe. *IACR Cryptology ePrint Archive*, 2015:971, 2015.
9. Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, and Yongsoo Song. Bootstrapping for approximate homomorphic encryption. In *EUROCRYPT 2018*, Lecture Notes in Computer Science. Springer, 2018.
10. Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song. Homomorphic encryption for arithmetic of approximate numbers. In *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Application of Cryptology and Information Security*, pages 409–437. Springer, 2017.
11. Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In *Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–33. Springer, 2016.
12. Ana Costache and Nigel P Smart. Which ring based somewhat homomorphic encryption scheme is best? In *Cryptographers' Track at the RSA Conference*, pages 325–340. Springer, 2016.
13. Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In *Advances in Cryptology–EUROCRYPT 2010*, pages 24–43. Springer, 2010.
14. Léo Ducas and Daniele Micciancio. FHEW: Bootstrapping homomorphic encryption in less than a second. In *Advances in Cryptology–EUROCRYPT 2015*, pages 617–640. Springer, 2015.
15. Yara Elias, Kristin E Lauter, Ekin Ozman, and Katherine E Stange. Provably weak instances of ring-lwe. In *Annual Cryptology Conference*, pages 63–92. Springer, 2015.
16. Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. *IACR Cryptology ePrint Archive*, 2012:144, 2012.
17. Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009. `http://crypto.stanford.edu/craig`.
18. Craig Gentry, Shai Halevi, and Nigel P Smart. Homomorphic evaluation of the AES circuit. In *Advances in Cryptology–CRYPTO 2012*, pages 850–867. Springer, 2012.
19. Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Advances in Cryptology–CRYPTO 2013*, pages 75–92. Springer, 2013.
20. Shai Halevi and Victor Shoup. Design and implementation of a homomorphic-encryption library. *IBM Research (Manuscript)*, 2013.
21. Andrey Kim, Yongsoo Song, Miran Kim, Keewoo Lee, and Jung Hee Cheon. Logistic regression model training based on the approximate homomorphic encryption. Cryptology ePrint Archive, Report 2018/254, 2018. `https://eprint.iacr.org/2018/254`.

22. Miran Kim, Yongsoo Song, Shuang Wang, Yuhou Xia, and Xiaoqian Jiang. Secure logistic regression based on homomorphic encryption: Design and evaluation. *JMIR medical informatics*, 6(2), 2018.
23. Patrick Longa and Michael Naehrig. Speeding up the number theoretic transform for faster ideal lattice-based cryptography. In *International Conference on Cryptology and Network Security*, pages 124–139. Springer, 2016.
24. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology–EUROCRYPT 2010*, pages 1–23, 2010.
25. Chris Peikert. An efficient and parallel Gaussian sampler for lattices. In *Annual Cryptology Conference*, pages 80–97. Springer, 2010.
26. Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 461–473, New York, NY, USA, 2017. ACM.
27. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 84–93, New York, NY, USA, 2005. ACM.
28. Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the Ring-LWE and Polynomial-LWE problems. Cryptology ePrint Archive, Report 2018/170, 2018. `https://eprint.iacr.org/2018/170`.

A Noise Analysis

We show the correctness of our scheme and analyze the noise from homomorphic operations. If we identify an element of $a \in F$ with its coefficient vector $(a_0, \ldots, a_{\frac{n}{2}-1})$ such that $a = a_0 + \sum_{j=1}^{\frac{n}{2}-1} a_j \cdot (X^j + X^{-j})$, then its canonical embedding can be represented by

$$\begin{aligned}\tau(a) &= \left(a_0 + \sum_{i=1}^{\frac{n}{2}-1} a_i \cdot (\zeta^{(4i+1)j} + \zeta^{-(4i+1)j}) \right)_{0 \le j < \frac{n}{2}} \\ &= a_0 \cdot \boldsymbol{u}_0 + \sum_{j=1}^{\frac{n}{2}-1} a_j \cdot \boldsymbol{u}_j\end{aligned}$$

for the orthogonal vectors $\boldsymbol{u}_0 = (1, \ldots, 1)$ and $\boldsymbol{u}_i = (\zeta^{(4i+1)j} + \zeta^{-(4i+1)j})_{0 \le j < \frac{n}{2}}$ in $\mathbb{R}^{n/2}$. Note that $\|\boldsymbol{u}_0\|_2^2 = \frac{n}{2}$ and $\|\boldsymbol{u}_j\|_2^2 = n$.

We follow a heuristic approach of Halevi and Shoup [20] which estimates the *noise variance* of its canonical embedding. Namely, we consider a as a random variable over F, then the expected squared ℓ_2 canonical norm of a is given by

$$\mathsf{E}\left[(\|a\|_2^{\mathsf{can}})^2\right] = n \cdot \mathsf{E}\left[\frac{1}{2} \cdot a_0^2 + \sum_{i=1}^{\frac{n}{2}-1} a_i^2\right] \le n \cdot \mathsf{E}\left[\|a\|_2^2\right].$$

Therefore, each entry of $\tau(a)$ has a variance $V \approx 2 \cdot \mathsf{E}\left[\|a\|_2^2\right]$, and we call V the noise variance of a.

We choose the distributions χ_{err}, χ_{key}, and χ_{enc} on R as follows. For an error parameter $\sigma > 0$, the error distribution χ_{err} draws each coefficient independently from the discrete Gaussian distribution of a variance σ^2. For an integer $h > 0$, the secret distribution χ_{key} uniformly at random from the set $\{0, \pm 1\}^{\frac{n}{2}}$ of signed binary vectors that have exactly h nonzero coefficients. The encryption key distribution χ_{enc} draws each of coefficients independently from $\{0, \pm 1\}$, with probability $1/4$ for each of -1 and $+1$, and probability being zero $1/2$.

When $a \in R$ is sampled from $U(R_q)$, then each of its coefficient has the variance $(q^2 - 1)/12 < q^2/12$, so we get the noise variance $V_q \approx n \cdot q^2/12$. When $a \leftarrow \chi_{key}$, we get a noise variance of $V_{key} = 2h$. When $a \leftarrow \chi_{err}$ (resp. χ_{enc}), we get $V_{err} = n \cdot \sigma^2$ (resp. $V_{enc} = n/2$).

Encoding. For a given $\boldsymbol{x} \in \mathbb{R}^{\frac{n}{2}}$, there exists $a_0, \ldots, a_{\frac{n}{2}-1} \in \mathbb{R}$ such that $\boldsymbol{x} = \sum_{i=0}^{\frac{n}{2}-1} a_i \cdot \boldsymbol{u}_i$. its rounding $\boldsymbol{x}'$ to $\tau(R)$ is obtained by rounding the numbers a_i's to the closest integers. Therefore, the rounding error is bounded by $\|\boldsymbol{x} - \boldsymbol{x}'\|_2^2 \leq (1/4) \cdot (n/2) \cdot n = n^2/8$.

Rescaling. For a level ℓ ciphertext $\mathsf{ct} = (c_0, c_1) \in R_{q_\ell}^2$, let $\mathsf{ct}' = \lfloor q^{-k} \cdot \mathsf{ct} \rceil \pmod{q_{\ell-k}}$. Then it is satisfied that $[\langle \mathsf{ct}', \mathsf{sk} \rangle]_{q_{\ell-k}} = q^{-k} \cdot [\langle \mathsf{ct}, \mathsf{sk} \rangle]_{q_\ell} - q^{-k} \cdot \langle [\mathsf{ct}]_{q^k}, \mathsf{sk} \rangle$. We can (heuristically) assume that $[c_0]_{q^k}$ and $[c_1]_{q^k}$ behave as uniform random variables on R_{q^k}. Therefore, the noise variance of rescaling error $q^{-k} \cdot ([c_0]_{q^k} + [c_1]_{q^k} \cdot s)$ has a variance of $V_{rs} = (n/12) \cdot (1 + 2h)$.

Encryption. Let $\mathsf{pk} = (b = -as + e, a) \in R_{q_L}^2$ be the public key and $\mathsf{ct} \leftarrow \mathtt{Enc}_{\mathsf{pk}}(\mathtt{m})$ be an encryption of $\mathtt{m} \in R$ generated by $v \leftarrow \chi_{enc}$ and $e_0, e_1 \leftarrow \chi_{err}$. Then we have $[\langle \mathsf{ct}, \mathsf{sk} \rangle]_{q_L} = \mathtt{m} + e_{enc}$ for $e_{enc} = v \cdot e + e_0 + e_1 \cdot s$. Therefore, the noise variance of encryption error is obtained by $V_{enc} \cdot V_{err} + V_{err} + V_{err} \cdot V_{key} = n \cdot \sigma^2 \cdot (1 + 2h + n/2)$.

Addition. This operation has no additional error since $\langle \mathsf{ct}_{add}, \mathsf{sk} \rangle = \langle \mathsf{ct}, \mathsf{sk} \rangle + \langle \mathsf{ct}', \mathsf{sk} \rangle \pmod{q_\ell}$.

Multiplication. For ciphertexts $\mathsf{ct} = (c_0, c_1)$ and $\mathsf{ct}' = (c_0', c_1')$ of level ℓ, let $(d_0, d_1, d_2) = (c_0 c_0', c_0 c_1' + c_1 c_0' + c_1 c_1') \pmod{q_\ell}$. It is direct from the definition that $d_0 + d_1 s + d_2 s^2 = \langle \mathsf{ct}, \mathsf{sk} \rangle \cdot \langle \mathsf{ct}', \mathsf{sk} \rangle \pmod{q_\ell}$. We can assume that d_2 looks a uniform random variable on R_{q_ℓ} as above.

Let $\mathsf{evk} = (b' = -a's + e', a') \in R_{P \cdot q_\ell}^2$ be the evaluation key. The multiplication error comes from the key-switching procedure $d_2 \mapsto \lfloor P^{-1} \cdot d_2 \cdot \mathsf{evk} \rceil \pmod{q_\ell}$. Note that $[\langle \lfloor P^{-1} \cdot d_2 \cdot \mathsf{evk} \rceil, \mathsf{sk} \rangle]_{q_\ell} = P^{-1} \cdot d_2 \cdot [\langle \mathsf{evk}, \mathsf{sk} \rangle]_{P \cdot q_\ell} + e_{rs} = d_2 \cdot s^2 + e_{rs} + P^{-1} \cdot d_2 \cdot e'$ where e_{rs} is a rescaling error. Therefore, the output ciphertext satisfies $\langle \mathsf{ct}_{mult}, \mathsf{sk} \rangle = \langle \mathsf{ct}, \mathsf{sk} \rangle \cdot \langle \mathsf{ct}', \mathsf{sk} \rangle + e_{mult} \pmod{q_\ell}$ for a multiplication error $e_{mult} = P^{-1} \cdot d_2 \cdot e' + e_{rs}$, and its noise variance is obtained by $V_{mult} = V_{rs} + P^{-2} \cdot V_{q_\ell} \cdot V_{err} = (n/12) \cdot (1 + 2h + P^{-2} \cdot q_\ell^2 \cdot n \cdot \sigma^2)$ which is approximately equal to $V_{rs} = (n/12) \cdot (1 + 2h)$ when $P \gg q_\ell$.