Revisiting an Extension of Kannan's Embedding for Ring-LWE

Satoshi Uesugi, Shinya Okumura, and Atsuko Miyaji

Osaka University, Japan
{uesugi, okumura, miyaji}@comm.eng.osaka-u.ac.jp

Abstract

Lattice-based cryptography has garnered significant attention in conjunction with the standardization of post-quantum cryptography by National Institute of Standards and Technology (NIST). The Learning With Errors (LWE) problem is a mathematical issue ensuring the security of lattice cryptography. However, cryptographic structures based on the LWE problem are noted for their inefficiency due to their large key sizes. As a result, the Ring-LWE problem was devised to reduce key sizes. While 2^k-th cyclotomic fields are typically used as the defining fields for the Ring-LWE problem, other algebraic number fields are also considered, including subfields of 2^k-th cyclotomic fields, 3^k-th cyclotomic fields and p-th cyclotomic fields for prime numbers p. Common attack methods for Ring-LWE include finding a shortest vector on a lattice using Kannan's embedding method and an extended version of Kannan's embedding method that finds the shortest vector with higher probability. In this paper, we propose an application of the extended version of Kannan's embedding method, which assumes only 2^k-th cyclotomic fields, to various number fields and demonstrate its effectiveness through experiments.

Keywords: Lattice based cryptography, Ring-LWE, Kannan's Embedding

1 Introduction

Lattice-based cryptography has garnered significant attention in conjunction with the standardization of post-quantum cryptography by National Institute of Standards and Technology (NIST). The Nist decided the standardization of post-quantum cryptography. Among these, CRYSTALS-KYBER [1], CRYSTALS-Dilithium [2] and FALCON [3] are lattice based cryptography. Furthermore, CRYSTALS-KYBER, CRYSTALS-Dilithium are based on the Module-LWE [4], which is a generalization of the Ring-LWE [5]. The Learning With Errors (LWE) problem [6] is a mathematical issue ensuring the security of lattice cryptography. It can be represented as :

$$\mathbf{t} \equiv \mathbf{sA} + \mathbf{e} \pmod{q}$$

where q is an odd prime number, $\mathbf{A}$ is an $m \times n$ matrix $(m > n)$, $\mathbf{s} \in^m$ is a secret and $\mathbf{e} \in^n$ is an error whose entries are small in $_q$. We call the pair$(\mathbf{A}, \mathbf{t})$ an LWE instance. However, cryptographic schemes based on the LWE problem are noted for their inefficiency due to their large key sizes. As a result, the Ring-LWE problem was devised to reduce key sizes and it may be useful for transmitting the public key. The key sizes, performance and security of Ring-LWE based schemes depend on its underlying number fields. More concretely, the extension degrees

The 7th International Conference on Mobile Internet Security (MobiSec'23), December 19-21, 2023, Okinawa, JAPAN, Article No.67

over Q and algebraic structure of its underlying number fields directly affect those of Ring-LWE based schemes. For example, some 2^k-th cyclotomic fields are often used for Ring-LWE, and their extension degrees over are 2^{k-1}. However, these values are not very flexible although smaller extension degrees are sufficient to achieve desired security. Moreover, as extension degrees become larger, key sizes of Ring-LWE based schemes also become larger, and thus the perfomance becomes worse. In order to set more flexible with secret/public keys and other parameters, we need to show that various number fields can be used for Ring-LWE. Thus the security analysis of Ring-LWE over various number fields are very important task. The Ring-LWE is a variant of LWE that utilizes the properties of rings and can be expressed over a ring $R_q = R/qR$, which R is the ring of integers of a number field:

$$t \equiv sa + e \in R_q,$$

where a, s and e are in R_q. Especially, for the Ring-LWE, 2^k-th cyclotomic fields are often used because of the effective calculation over 2^k-th cyclotomic fields. Let R be $[x]/(x^n+1)$, the Ring-LWE instance can be written as a LWE instance:

$$\begin{aligned} t &\equiv sa + e \\ &= \mathbf{s} \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \cdots & a_0 \end{pmatrix} \cdot \mathbf{x}^T + \mathbf{e} \cdot \mathbf{x}^T. \end{aligned}$$

where $\mathbf{s}$ and $\mathbf{e} \in_q^n$ are the coefficient vector of the elements $s, e \in R_q$, respectively. And $\mathbf{x}$ is a basis vector whose elements are $(1, x, \cdots, x^{n-1})$.Thus, we can solve the Ring-LWE over 2^k-th cyclotomic fields by transforming a Ring-LWE to a LWE instance. Any LWE instance $(\mathbf{A}, \mathbf{t})$ can be regarded as an instance of the bounded distance decoding, which is a kind of the closest vector problem and is called BDD. For the LWE, we can generate a q-aray lattice $\Lambda_q(A)$ by using $\mathbf{A}$ with $\mathbf{t}$. Kannan's embedding [7] is a method to transform any BDD instances to an instance of unique-SVP and the lattice constructed by Kannan's embedding can include $\pm\mathbf{e}$. Furthermore, we can recover the error by using reduction algorithms such as LLL algorithm [8], BKZ algorithm [9] for the lattice which has an error vector. As a particular approach to solve the Ring-LWE, we often use Kannan's embedding and the extension by using the rotation is has been considered. The rotation is the operation in some number fields where components of a vector may be moved, their signs changed, or calculations conducted between the components and the operation has been used for Sieve algorithm [10] [11]. Thus, the rotation in various number fields have been considered to be formulated because we can comprehend the structure of the lattice and the norm of the basis vector. For example, over 2^k-th cyclotomic fields, for the vector $\mathbf{v} = (v_0, \cdots v_{n-1}) \in_q^n$ which is the coefficient vector, the rotation is as follows:

$$\mathrm{rot}(\mathbf{v}) = (-v_{n-1}, v_0, \cdots, v_{n-2}).$$

Furthermore, for the Ring-LWE instance $(a, t \equiv sa + e)$, let $\mathbf{a}$, $\mathbf{s}$ and $\mathbf{e}$ be the coefficient vectors of a, s and e, and the conversion from the Ring-LWE instance to the LWE instance can be rewritten as follows:

$$\begin{aligned} t &\equiv sa + e \\ &= \mathbf{s} \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \cdots & a_0 \end{pmatrix} \cdot \mathbf{x}^T + \mathbf{e} \cdot \mathbf{x}^T \\ &= \mathbf{s} \begin{pmatrix} \mathbf{a} \\ \mathrm{rot}(\mathbf{a}) \\ \vdots \\ \mathrm{rot}^{\mathrm{n}-1}(\mathbf{a}) \end{pmatrix} \cdot \mathbf{x}^T + \mathbf{e} \cdot \mathbf{x}^T. \end{aligned}$$

This rotation is used for an extension of Kannan's Embedding, which is proposed by Nakamura et al [12]. The extension is effective for the Ring-LWE over 2^k-th cyclotomic fields. However, the extension is only for the Ring-LWE over 2^k-th cyclotomic fields. Therefore, we should demonstrate the effectiveness to the Ring-LWE over the number fields except for 2^k-th cyclotomic fields. In this work, we demonstrate the effectiveness of the extension for the Ring-LWE over 2^k-th cyclotomic fields, p-th cyclotomic fields for prime number p, 3^k-th cyclotomic fields, the maximal real subfields of 2^k-th cyclotomic fields. Section **??** provides mathematical properties and problems for lattices. Section **??** introduces an extension of Kannan's embedding and the rotation of cyclic lattices, anti-cyclic lattice, prime cyclotomic lattices and trinomial lattices. Section 4 gives our proposal for the rotation of the maximal real subfields of 2^k-th cyclotomic fields. Section **??** shows experimental results of attacks on the Ring-LWE over 2^k-th cyclotomic fields, p-th cyclotomic fields for prime number p, 3^k-th cyclotomic fields, the maximal real subfields of 2^k-th cyclotomic fields by using the extension to each number fields and BKZ algorithm. Section **??** concludes this work and refer to future works.

2 Preliminary

2.1 Lattice

[Lattice] For any linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in^m$, we define a lattice of dimension m as

$$L = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \coloneqq \left\{ \sum_{i=1}^{n} a_i \mathbf{b}_i | a_i \in \right\}.$$

The lattice L is generated by the set of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$, which is called a basis of L. The basis can construct the matrix $\mathbf{B} = (\mathbf{b}_1, \cdots, \mathbf{b}_n) \in^{m \times n}$ whose i-th column is $\mathbf{b}_i$ and n is called the rank of the lattice.

[Gram-Schmidt Orthogonalization] For a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ of a lattice $L \subset^m$, the basis $\mathbf{B}^* = \{\mathbf{b}_1^*, \cdots \mathbf{b}_n^*\}$ obtained by Gram-Schmidt orthogonalization on B is as follows:

$$\begin{aligned} \mathbf{b}_1^* &\coloneqq \mathbf{b}_1, \\ \mathbf{b}_i^* &\coloneqq \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^* \ (i \geq 2), \end{aligned}$$

where $\mu_{i,j} \coloneqq \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2}$ $(1 \leq j < i \leq n)$ and $\mu_{i,j}$ is called GSO coefficients.

[Successive Minima] For a lattice $L = \mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{b_1}, \cdots, \mathbf{b_n})$, we define successive minima as

$$\lambda_i(L) \coloneqq \min_{\mathbf{v_1}, \cdots, \mathbf{v_i} \in L} \max\{\|\mathbf{v_1}\|, \cdots, \|\mathbf{v_i}\|\|\}.$$

where the lattice vectors $\mathbf{v_1}, \cdots, \mathbf{v_i} \in L$ are linearly dependent.

[Orthogonal Projection] For $1 \leq l \leq n$, we define the orthogonal projection π_l as

$$\pi_l \colon {}^n \to \mathbf{B}_{[1:l-1]}^{\perp}, \ \pi_l(\mathbf{v}) = \sum_{i=l}^{n} \frac{\langle \mathbf{v}, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2} \mathbf{b}_i^*.$$

where $\mathbf{B}_{[1:l-1]}^{\perp}$ is a vector space orthogonal to a basis $\mathbf{B}_{[1:l-1]} = \{\mathbf{b_1}, \cdots, \mathbf{b_{l-1}}\}$.

[Volume] Let $\mathbf{b_1}, \cdots, \mathbf{b_n}$ and L be as above. The volume of the lattice L is defined as follows:

$$\mathrm{vol(L)} = \sqrt{\det(\mathbf{B}\mathbf{B}^{\mathrm{T}})}.$$

Note that the volume of the lattice is independent of the choice of basis. Specifically, when $m = n$, for any basis matrix $\mathbf{B}$ of the lattice L, it holds $\mathrm{vol(L)} = |\det(\mathbf{B})|$.

2.1.1 Lattice Problems

The Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP) are most famous mathematical problems related to lattices.

[Shortest Vector Problem] Given a basis $\{\mathbf{b}_1, \cdots \mathbf{b}_n\}$ of a lattice L, the Shortest Vector Problem (SVP) is to find a non-zero shortest vector $\mathbf{s} \in L$.

[Unique Shortest Vector Problem] Given a basis $\{\mathbf{b}_1, \cdots \mathbf{b}_n\}$ of a lattice L, the Unique Shortest Vector Problem (uSVP) is to find the shortest nonzero vector which satisfies $\lambda_1(L) << \lambda_2(L)$ in the lattice L.

[Closest Vector Problem] Given a basis $\{\mathbf{b}_1, \cdots \mathbf{b}_n\}$ of the lattice $L \subseteq^m$ and a target vector $\mathbf{t} \in^m$, the Closest Vector Problem (CVP) is to find a vector $\mathbf{w} \in L$ that minimizes $\|\mathbf{w} - \mathbf{t}\|$.

[Bounded Distance Decoding] Given a lattice L and a target vector $\mathbf{t} \in L$ which is very close to the lattice L, the Bounded Distance Decoding(BDD) is to find a vector $\mathbf{u} \in L$ such that $\|\mathbf{u} - \mathbf{t}\| \leq \gamma \lambda_1(L)$, where m is the dimension of the lattice L, for $\gamma > 0$.

2.2 Approach to Solve Lattice Problems

Lattice basis reduction algorithms are proposed to solve lattice problems by transforming given basis of a lattice as input into a basis which consists short vectors. LLL algorithm [8] and BKZ algorithm [9] are the most familiar algorithms.

[LLL: Lenstra-Lenstra-Lovász] We say a basis $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ of a lattice L to be δ-LLL reduced for a parameter $\frac{1}{4} < \delta < 1$ if it satisfies the following conditions:

- The basis $\mathbf{B}$ is size-reduced : the GSO coefficients μ_{ij} satisfy $\|\mu_{ij}\| \leq \frac{1}{2}$ for all $i > j$.
- If $\mathbf{B}$ satisfies the Lov$\acute{a}$sz condition: For $2 \leq k \leq n$, it satisfies $\delta \|\mathbf{b}_{k-1}^*\| \leq \|\pi_{k-1}(\mathbf{b}_k)\|^2$.

[BKZ: Blockwise Korkine-Zolotarev] For a basis $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ of the lattice $L = \mathcal{L}(\mathbf{B})$, let $\mathbf{B}_{[j,l]}$ be the lattice with a basis $\{\pi_j(\mathbf{b}_j), \cdots, \pi_j(\mathbf{b}_l)\}$ $(j < l)$. For a blocksize $\beta \geq 2$, a basis $\mathbf{B}$ is said β-BKZ reduced if it satisfies the following conditions:

- The basis $\mathbf{B}$ is size-reduced.
- For $1 \leq j \leq n$ and $l = \min(j+\beta-1, n)$, it satisfies $\|\mathbf{b}_j^*\| = \lambda_1(L_{[j,l]})$.

[Kannan's Embedding] Kannan's embedding method [7] is an approach to solve the CVP by reducing it to the uSVP. For an n-dimensional lattice $L \subseteq^n$ with a basis $B = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ and a target vector $\mathbf{w} \in^n$, let $\mathbf{v} = \sum_{i=1}^n v_i \mathbf{b}_i \ \in L (\exists v_i \in)$ be a solution vector for the CVP and consider the lattice $\bar{L}$ which has $(n+1)$ linearly independent vectors with a positive constant $M \in$:

$$(\mathbf{b}_1, 0), \cdots, (\mathbf{b}_n, 0), (\mathbf{w}, M) \in^{n+1} .$$

Then, the different vector $\mathbf{e}$ is represented as

$$\begin{aligned}(\mathbf{e}, M) &= \left(\mathbf{w} - \sum_{i=1}^n v_i \mathbf{b}_i,\ M\right) \\ &= -v_1(\mathbf{b}_1, 0) - \cdots - v_n(\mathbf{b}_n, 0) + (\mathbf{w}, M).\end{aligned}$$

Therefore, a vector $(\mathbf{e}, M)$ consists in the lattice $\bar{L}$. If $(\mathbf{e}, M)$ is a shortest nonzero vector in $\bar{L}$, then we can get $\mathbf{e}$. In practical, we consider the $(n+1) \times (n+1)$ matrix $\mathbf{B'}$:

$$\mathbf{B'} = \begin{pmatrix} \mathbf{B} & \mathbf{0} \\ \mathbf{w} & M \end{pmatrix}.$$

2.3 Number Fields Background

In this section, we summarize concepts from algebraic number theory.

[Cyclotomic Field] For r $m > 0$, the m-th cyclotomic number field is (ζ_m), where ζ_m is a primitive m-th root of 1. The degree of (ζ_m) is $\phi(m)$, where $\phi(\cdot)$ denotes Euler's totient function. In addition, the m-th cyclotomic polynomial is $\Phi_m(X) = \prod_{i \in_m^*}(X - \zeta_m^i)$.

[Galois Number Field] Let K be a number field. For every $x \in K$, if the minimal polynomial of x over has all its roots in K, then we call K is a Galois number field. If a number field K is a Galois number field, the set of automorphisms $\sigma\colon K \to K$, where $\sigma(a) = a$, for all $a \in$ is called the Galois group of K over and denoted by $\mathrm{Gal}(K/)$.

[Fundamental Theorem of Galois Theory] Let L and K be fields, and let $\mathcal{M}$ the set of all intermediate fields of L/K. When L/K is a Galois number field, let $\mathcal{H}$ be the set of all subgroups of $\mathrm{Gal}(L/K)$. Consider the following mappings:

$$\begin{tikzcd} \Phi\colon & \mathcal{M} \arrow[r] & \mathcal{H} \\ & \rotatebox{90}{$\in$} & \rotatebox{90}{$\in$} \\ & M \arrow[r, mapsto] & \mathrm{Gal}(L/M) \end{tikzcd}$$

$$\begin{tikzcd} \Psi\colon & \mathcal{H} \arrow[r] & \mathcal{M} \\ & \rotatebox{90}{$\in$} & \rotatebox{90}{$\in$} \\ & H \arrow[r, mapsto] & L^H \end{tikzcd}$$

where $L^H = \{a \in L | \forall \sigma \in H, \sigma(a) = a\}$. Then the following holds:

1. The mappings Φ and Ψ are bijective and $\Phi = \Psi^{-1}$, establishing a one-to-one correspondence between $\mathcal{M}$ and $\mathcal{H}$.

2. The necessary and sufficient condition for $M \in \mathcal{M}$ to be a Galois extension of K is that $\mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$.

3. When $\mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$, there exists an isomorphism between the groups: $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \cong \mathrm{Gal}(M/K)$.

[Trace] Let K be a Galois number field. For every $a \in K$,

$$\mathrm{Tr}_K(a) = \sum_{\sigma \in \mathrm{Gal}(K/)} \sigma(a).$$

[Dual Ideal] Let K be a Galois number field. For a fractional ideal $\mathcal{I}$, its dual ideal is defined as follows:

$$\mathcal{I}^\vee = \{x \in K \mid \mathrm{Tr}(x\mathcal{I}) \subset\}.$$

We use the notation $U(X)$ for the uniform distribution over a set X. Let $q \geq 2$ be an integer modulus and R be a ring. We use the notation $R_q = R/qR$. Let K be a number field, $R = \mathcal{O}_K$ its ring of integers, $R^\vee$ its dual ideal, and $R_q^\vee = R^\vee/qR^\vee$. All elements of $_q$ is represented by the integers in $[-q/2, q/2)$. For any n-dimensional vector $\mathbf{v}$, we set the Euclidean norm $\|\mathbf{v}\| = \sqrt{\sum_{1\leq i\leq n} |v_i|^2}$ and ℓ_∞- norm $\|\mathbf{v}\|_\infty := \max_{i \leq n} |v_i|$. Further, we denote the Gaussian distribution with mean 0 and standard deviation σ as D_σ.

2.4 The Ring-LWE Problem

In this section, we recall the Ring-Based Learning With Errors (Ring-LWE) problem [5].

[Ring-LWE Distribution] For a secret $s \in R_q$ and a distribution ψ over R_q, the distribution $A_{s,\psi}$ over $R_q \times R_q$ is generated by choosing $a \leftarrow U(R_q)$, choosing $e \leftarrow \psi$, and outputting $(a, b = (a \cdot s) + e) \in R_q \times R_q$.

[Search Ring-LWE] Let Ψ be a family of distributions over R_q. The Search Ring-LWE problem over $R = \mathcal{O}_K$, denoted by $\text{R-LWE}_{q,\psi}$, is defined as follows: given access to arbitrarily many independent samples from $A_{s,\psi}$ for some arbitrary $s \in R_q$ and $\psi \in \Psi$, find s.

[Average-Case Decision Ring-LWE] For a distribution γ over a family of noise distributions over R_q, the average-case Ring-LWE decision problem, denoted $\mathrm{Ring} - \mathrm{LWE}_{\mathrm{q},\gamma}$, is to distinguish between independent samples from $A_{s,\psi}$ for a random choice of $(s, \psi) \leftarrow U(R_q) \times \gamma$, and the same number of uniformly random and independent samples from $R_q \times R_q$.

[Rotation] Let n be a 2-power integer. For every $f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \in [x]/(x^n+1)$, we write its coefficient vector as $\mathbf{f} = (f_0, f_1, \cdots, f_{n-1}) \in^n$. The rotation operation for (f) is as follows:

$$\mathrm{rot}(\mathbf{f}) = (-\mathrm{f}_{\mathrm{n}-1}, \mathrm{f}_0, \mathrm{f}_1, \cdots, \mathrm{f}_{\mathrm{n}-2}).$$

This is just the coefficient vector of the element $xf(x) \in [x]/(x^n+1)$. Similarly, for each $1 \leq i \leq n$, the i times rotated vector $\mathrm{rot}^{\mathrm{i}}((\mathrm{f}))$ is the coefficient vector of $x^i f(x) \in [x]/(x^n+1)$.

Given a Ring LWE sample $(a, b = a \cdot s + e)$ from the Ring-LWE distribution $A_{s,\psi}$, let $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1})$ be a coefficient vector of a. We set the $n \times n$ matrix

$$\mathbf{A} = \begin{pmatrix} \mathbf{a} \\ \mathrm{rot}(\mathbf{a}) \\ \vdots \\ \mathrm{rot}^{\mathrm{n}-1}(\mathbf{a}) \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \cdots & a_0 \end{pmatrix}.$$

Let $\mathbf{t}, \mathbf{s}, \mathbf{e}$ be coefficient vectors of three elements $t, s, e \in [x]/(x^n+1)$ for a 2-power integer n , the equation $t = a \cdot s + e$ can be written as

$$\begin{aligned} \mathbf{t}\mathbf{x}^T = t &= s \cdot a + e \\ &= \mathbf{s} \begin{pmatrix} a \\ x \cdot a \\ \vdots \\ x^{n-1} \cdot a \end{pmatrix} + \mathbf{e}\mathbf{x}^T = \mathbf{s} \begin{pmatrix} \mathbf{a} \\ \mathrm{rot}(\mathbf{a}) \\ \vdots \\ \mathrm{rot^{n-1}}(\mathbf{a}) \end{pmatrix} + \mathbf{e}\mathbf{x}^T \\ &= (\mathbf{s}\mathbf{A} + \mathbf{e})\mathbf{x}^T. \end{aligned}$$

where $\mathbf{x} = (1, x, \cdots, x^{n-1})$ gives a basis of the ring $[x]/(x^n+1)$. For an integer $m \geq 1$, we take m independent Ring-LWE samples
$((a_1(x), t_1(x)), \cdots, (a_m(x), t_m(x))$ from $A_{q,\psi}$, where $a_i(x)$ is constituted on the basis of $\{1, x, \cdots, x^{n-1}\}$ for $1 \leq i \leq m$. Let the $n \times n$ matrix corresponding to $a_i(x)$ denoted by A_i for $1 \leq i \leq m$. Then we have m relations $\mathbf{t}_i \equiv \mathbf{s}\mathbf{A}_i + \mathbf{e}_i \pmod q$ for $1 \leq i \leq m$. We can concatenate the m relations to obtain an LWE instances of size $n \times mn$ as

$$(\tilde{A}, \tilde{t}), \tilde{t} \equiv s\tilde{A} + \tilde{e} \pmod q$$

where $\tilde{A} = (A_1|\cdots|A_m)$, $\tilde{t} = (t_1|\cdots|t_m)$, $\tilde{e} = (e_1|\cdots|e_m)$. Therefore, we can apply multiple Ring-LWE samples to LWE instances.

3 Previous Work

In [12], by applying an extension of Kannan's embedding to q-aray lattices of Ring-LWE over powers-of-two cyclotomic fields, they demonstrated increasing the success possibility of the extension. In [13], they proposed three types of ideal lattices generated by specific polynomials, which are cyclic lattices, anti-cyclic lattices, and prime cyclic lattices and applied Gauss Sieve Algorithm to them to improve the processing speed. Then, they consider the rotations of the Ring-LWE over 2^k-th cyclotomic fields, the Ring-LWE over p-th cyclotomic fields for prime number p, and the Ring-LWE over $[x]/(x^n-1)$. Furthermore, in [14], they proposed new types of an ideal lattice 'Trinomial lattice', which is generated by the trinomials in the cyclotomic polynomials and then, they propose the rotation of the Ring-LWE over 3^k-th cyclotomic fields. They also use it to speed up for solving the SVP Challenge in Ideal lattice Challenge [15].

3.1 An Extension of Kannan's Embedding

An extension of Kannan's Embedding is for solving the search Ring-LWE problem. Given Ring-LWE instances $(a_i(x), t_i(x)) \in R_q \times R_q$, where R_q is ${}_q[x]/(x^n+1)$, let $\mathbf{A_i}$ be the $n \times n$ matrix corresponding to $a_i(x)$ for each $1 \leq i \leq m$ and $\tilde{\mathbf{t}} = (\mathbf{t_1}|\cdots|\mathbf{t_m})$ is formed by each coefficient vector of $t_i(x)$. We can concatenate the m relations to obtain an LWE instance of size $n \times nm$ as

$$(\tilde{\mathbf{A}}, \tilde{t}),\ \tilde{\mathbf{t}} \equiv \mathbf{s}\tilde{\mathbf{A}} + \tilde{\mathbf{e}} \pmod q.$$

Furthermore, let $\mathbf{C}$ be a basis of the q-array lattice $\begin{pmatrix} \tilde{\mathbf{A}} \\ q\mathbf{I_n} \end{pmatrix}$ is reducted by reduction algorithms as in [8], [9]. Then an extension of Kannan's embedding is

$$\mathbf{B} = \begin{pmatrix} \mathbf{C} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \tilde{\mathbf{t}} & \eta & 0 & \cdots & 0 \\ \mathrm{rot}(\tilde{\mathbf{t}}) & 0 & \eta & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathrm{rot}^{\mathrm{k-1}}(\tilde{\mathbf{t}}) & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

m relations $x^i t_j(x) = x^i s(x) \cdot a_j(x) + x^i e_j(x) \in R_q$ multiplied by x^i can be written as

$$\mathrm{rot}^{\mathrm{i}}(\tilde{\mathbf{t}}) \equiv \mathrm{rot}^{\mathrm{i}}(\mathbf{s}) \cdot \tilde{\mathbf{A}} + \mathrm{rot}^{\mathrm{i}}(\tilde{\mathbf{t}}) \pmod q$$

in ^d_q for $i \leq i < k$, where $\mathrm{rot}^{\mathrm{i}}(\tilde{\mathbf{e}})$ denotes the rotated vector of $\tilde{\mathbf{e}}$. By the rotation and the construction of $\mathbf{B}$ (note that $\mathcal{L}(\mathbf{C}) = \Lambda_q(\tilde{\mathbf{A}})$)), the extended lattice $\tilde{\Lambda_k}$, which is the lattice of dimension $nm + k$ generated by the rows of $\mathbf{B}$ includes k short lattice vectors

$$\begin{cases} \tilde{\mathbf{e}} & = (\tilde{\mathbf{e}} \mid \eta, 0, \cdots, 0), \\ \mathrm{rot}(\tilde{\mathbf{e}}) & = (\mathrm{rot}(\tilde{\mathbf{e}}) \mid 0, \eta, \cdots, 0), \\ & \vdots \\ \mathrm{rot}^{\mathrm{k-1}}(\tilde{\mathbf{e}}) & = (\mathrm{rot}^{\mathrm{k-1}}(\tilde{\mathbf{e}}) \mid 0, 0, \cdots, \eta). \end{cases}$$

where η is a constant ($\eta > 0$). These lattice vectors have the same length since the rotation operation dose not change the length of a vector.

3.2 Three Types of Ideal Lattices

Three types of ideal lattices, which are cyclic lattices, anti-cyclic lattices, and prime cyclotomic lattices are used for solving the SVP challenge in ideal lattices and they have the rotation to transform the polynomials to the vectors. Here, we show them as follows:

1. Cyclic lattices : For an integer n, let $f_1(x) = x^n - 1$, i.e., $\bar{f} = (-1, 0, \cdots, 0)$ which is the coefficient vector of $f_1(x)$, then we call the ideal lattices of the ring $R_1 = [x]/(f_1(x))$ cyclic lattices. The rotation of a vector $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1}) \in^n$ is $\mathrm{rot}(\mathbf{v}) = (v_{n-1}, v_0, \cdots, v_{n-2})$.

2. Anti-cyclic lattices : For a 2-power integer n, let $f_2(x) = x^n + 1$, i.e., $\bar{f} = (1, 0, \cdots, 0)$ which is the coefficient vector of $f_2(x)$, then we call the ideal lattices of the ring $R_2 = [x]/(f_2(x))$ anti-cyclic lattices. The rotation of a vector $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1}) \in^n$ is $\mathrm{rot}(\mathbf{v}) = (-v_{n-1}, v_0, \cdots, v_{n-2})$.

3. Prime cyclotomic lattices : For a prime number $n+1$, let $f_3(x) = x^n + x^{n-1} + \cdots + 1$, i.e., $\bar{f} = (1, 1, \cdots, 1)$ which is the coefficient vector of $f_3(x)$, then we call the ideal lattices of the ring $R_3 = [x]/(f_3(x))$ prime cyclotomic lattices. The rotation of a vector $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1}) \in^n$ is $\mathrm{rot}(\mathbf{v}) = (-v_{n-1}, v_0 - v_{n-1}, \cdots, v_{n-2} - v_{n-1})$.

From the above, the Ring-LWE over 2^k-th cyclotomic fields is based on anti-cyclic lattices and the Ring-LWE over p-th cyclotomic fields for prime number p is based on prime cyclotomic lattices.

3.3 Trinomial lattices

A Trinomial lattice is generated by the trinomials in the cyclotomic polynomials. It is used for speeding up for solving the SVP Challenge in Ideal lattice Challenge. To constitute a Trinomial lattice, there are two conditions as follows:

- Condition 1
  Let n be an even dimension of a lattice. If $n/2$ is a power of three, an ideal lattice generated by a cyclotomic polynomial $g(x) = x^n + x^{n/2} + 1$ and a basis B is called a Trinomial lattice. In this type, the rotation of a coefficient vector $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1}) \in [x]/(g(x))$ is $\mathrm{rot}(\mathbf{v}) = (-v_{n-1}, v_0, \cdots, v_{\frac{n}{2}-2}, v_{\frac{n}{2}-1} - v_{n-1}, v_{\frac{n}{2}}, \cdots, v_{n-2})$.

- Condition 2
  Let n be an even dimension of a lattice. If n is the product of both a power of two and a power of three, an ideal lattice generated by a cyclotomic polynomial $g(x) = x^n - x^{n/2} + 1$ and a basis B is called a Trinomial lattice. In this type, the rotation of a coefficient vector $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1}) \in [x]/(g(x))$ is $\mathrm{rot}(\mathbf{v}) = (-v_{n-1}, v_0, \cdots, v_{\frac{n}{2}-2}, v_{\frac{n}{2}-1} + v_{n-1}, v_{\frac{n}{2}}, \cdots, v_{n-2})$.

From the above, in condition 1, the Ring-LWE over 3^k-th cyclotomic fields is based on the lattices. The rotate operation $\mathrm{rot}(\mathbf{v})$ using the Trinomial lattice is less computational cost than using the Anti-cyclic lattice.

4 Extension Kannan's Embedding to Various Number Fields

In this section, we consider the Ring-LWE problem over various number fields which are p-th cyclotomic fields for prime number p, maximal real subfields of 2^k-th cyclotomic fields, and 3^k-th cyclotomic fields. For maximal real subfields of 2^k-th cyclotomic fields, we suppose a new ideal lattice to use an extension of Kannan's embedding. The extension is considered under the basic Ring $R = [x]/(x^n + 1)$ for a 2-power integer n. However, there are some lattices such as [14]. Therefore, we demonstrate the effectiveness of the extension for the Ring-LWE problem over various number fields. Except for maximal real subfields of 2^k-th cyclotomic fields, we can construct lattices by using the rotation and apply an extension of Kannan's embedding to them. In the following, we propose an approach to construct lattice and the rotation for maximal real subfields of 2^k-th cyclotomic fields. Let R'_q be the ring of integers of maximal real subfields of 2^k-th cyclotomic fields, then an element $a \in R'_q$ is as folllows:

$$a = a_0 + a_1(x + x^{-1}) + \cdots + a_{m-1}(x^{m-1} + x^{-(m-1)}) \in R'_q.$$

We regard the set of -basis of the ring R', $\{1, x + x^{-1}, \cdots, x^{m-1} + x^{-(m-1)}\}$ as a basis vector ζ and let s be a secret and e be an error

$$s = s_0 + s_1(x + x^{-1}) + \cdots + s_{m-1}(x^{m-1} + x^{-(m-1)}) \in R'_q,$$
$$e = e_0 + e_1(x + x^{-1}) + \cdots + e_{m-1}(x^{m-1} + x^{-(m-1)}) \in R'_q.$$

Then we consider the Ring-LWE sample $(a, b \equiv a \cdot s + e \ (\ mod\ q))$ and it can be written as

$$\begin{aligned}
\mathbf{b} \cdot \zeta^T &= b = as + e \\
&= \mathbf{s} \cdot \zeta^T \cdot a + \mathbf{e} \cdot \zeta^T \\
&= \mathbf{s} \cdot \begin{pmatrix} a \\ a \cdot (x + x^{-1}) \\ \vdots \\ a \cdot (x^{m-1} + x^{-(m-1)}) \end{pmatrix} + \mathbf{e} \cdot \zeta^T.
\end{aligned}$$

To transform the vector $a \cdot \zeta^T$, we consider the multiplication $(x^i + x^{-i})$ for $1 \leq i < m$ by using the property of powers-of-two cyclotomic field which is $x^n = -1$. Then, we have

$$\begin{aligned}
(x^i + x^{-i}) \cdot a &= (x^i + x^{-i}) \cdot \{a_0 + a_1(x + x^{-1}) + \cdots + a_{m-1}(x^{m-1} + x^{-(m-1)})\} \\
&= (x^i + x^{-i}) \cdot \{a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + 0 \cdot x^m + a_1 x^{-1} + \\
&\cdots + a_{m-1}x^{-(m-1)}\} \\
&= (x^i + x^{-i}) \cdot (a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + 0 \cdot x^m - a_1 x^{n-1} + \\
&\cdots - a_{m-1}x^{m+1}) \\
&= (x^i + x^{-i}) \cdot \{(a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}) + 0 \cdot x^m + (-a_1 x^{n-1} - \\
&\cdots - a_{m-1}x^{m+1})\}.
\end{aligned}$$

In this case, we consider the rotation for $x + x^{-1}$ and the map φ:

$$\varphi\colon {}^m \to {}^n, \ \varphi(\mathbf{a}) = (a_0, a_1, \cdots, a_{m-1}, 0, -a_{m-1}, \cdots, -a_1),$$

where $\mathbf{a}$ is the coefficient vector of an element $a \in R'_q$. Note that $\varphi(\mathbf{a})$ is the coefficient vector of a over R_q. By using the defined map φ, we can replace $a \cdot (x^i + x^{-i})$ as

$$\begin{aligned}
(x^i + x^{-i}) \cdot a &= (x^i + x^{-i}) \cdot \{(a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}) + 0 \cdot x^m + (-a_1 x^{n-1} \\
&- \cdots - a_{m-1}x^{m+1})\} \\
&= x^i \cdot \{(a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}) + 0 \cdot x^m + (-a_1 x^{n-1} - \\
&\cdots - a_{m-1}x^{m+1})\} \\
&+ x^{-i} \cdot \{(a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}) + 0 \cdot x^m + (-a_1 x^{n-1} - \\
&\cdots - a_{m-1}x^{m+1})\} \\
&= \mathrm{rot^i}(\varphi(\mathbf{a})) + \mathrm{rot^{-i}}(\varphi(\mathbf{a})),
\end{aligned}$$

where $\mathrm{rot^{-i}}(\cdot)$ is just the inverse of rotation

$$\mathrm{rot}^{-1}(\mathbf{f}) = (\mathrm{f_1}, \mathrm{f_2}, \cdots, \mathrm{f_{n-2}}, \mathrm{f_{n-1}}, -\mathrm{f_0}),$$

Note that the coefficients of an element a from 1-th to $m-1$-th is the same as the coefficients of an element a from $n-1$ -th to $\frac{m}{2}+1$-th over ${}_q$. We consider the inverse map φ^{-1}:

$$\begin{aligned}
\mathbf{b} \cdot \zeta^T &= b = as + e \\
&= \mathbf{s} \cdot \zeta^T \cdot a + \mathbf{e} \cdot \zeta^T \\
&= \mathbf{s} \cdot \begin{pmatrix} a \\ a \cdot (x + x^{-1}) \\ \vdots \\ a \cdot (x^{m-1} + x^{-(m-1)}) \end{pmatrix} + \mathbf{e} \cdot \zeta^T \\
&= \mathbf{s} \cdot \begin{pmatrix} \mathbf{a} \\ \varphi^{-1}(\mathrm{rot}(\varphi(\mathbf{a})) + \mathrm{rot}^{-1}(\varphi(\mathbf{a}))) \\ \vdots \\ \varphi^{-1}(\mathrm{rot}^{\mathrm{m}-1}(\varphi(\mathbf{a})) + \mathrm{rot}^{-(\mathrm{m}-1)}(\varphi(\mathbf{a}))) \end{pmatrix} \cdot \zeta^T + \mathbf{e} \cdot \zeta^T \\
&= (\mathbf{s} \cdot \hat{\mathbf{A}} + \mathbf{e}) \cdot \zeta^T.
\end{aligned}$$

Therefore, we can get

$$\mathbf{b} = \mathbf{s} \cdot \hat{\mathbf{A}} + \mathbf{e}.$$

From the above, we represent the operation $\varphi^{-1}(\mathrm{rot}^{\mathrm{i}}(\varphi(\cdot)) + \mathrm{rot}^{-\mathrm{i}}(\varphi(\cdot)))$ as mrs-rot$(\cdot)$ for $1 \leq i < m$ and consider the extension of Kannan's embedding over the maximal real subfield of powers-of-two cyclotomic field:

$$\mathbf{B} = \begin{pmatrix} \mathbf{C} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \text{mrs-rot}(\tilde{\mathbf{t}}) & \eta & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \text{mrs-rot}^{k-1}(\tilde{\mathbf{t}}) & 0 & 0 & \cdots & \eta \end{pmatrix},$$

where $\mathbf{C}$ is a basis of q-array lattice and k ranges from 1 to $m-1$.

5 Experiment

In this section, we solve the Ring-LWE problem over various number fields by using the extension of Kannan's embedding and BKZ algorithm.

5.1 Approach to Solve the Ring-LWE Problem

For the Ring-LWE instance $(a, b = a \cdot s + e) \in R_q \times R_q$, we assume that a is sampled uniformly and s, e are sampled from the discrete Gaussian distribution with mean 0 and standard deviation σ. In our experiments, we attack 100 pairs of instances for the same secret s by transforming them to 100 pairs of LWE instances. Let d be the dimension of the LWE instance, we construct the q-aray lattice $\Lambda_k = \begin{pmatrix} \tilde{\mathbf{A}}_{\mathbf{i}} \\ q\mathbf{I}_{\mathbf{n}} \end{pmatrix}$ for $1 \leq i \leq 100$. Then, we reduce the q-aray lattice Λ_k to the matrix C of the size $2d \times 2d$ by LLL algorithm and construct a basis $\mathbf{B}$ of the dimension $2d + k$ by an extension of Kannan's embedding. After constructing, we reduce the basis $\mathbf{B}$ by BKZ algorithm and recover a short vector. It is successful that the norm of a short vector is smaller than $1.2\sigma\sqrt{d}$ and all the entries less than 4σ in absolute. This approach is in

detail [12].
The experimental environment is Intel(R) Xeon(R) CPU E7-4830 v4 @ 2.00GHz. We use SageMath version 9.3 [16] for generating the Ring-LWE instances and C++ with the NTL library version 11.5.1 [17] for solving the Ring-LWE problem. For generating the Ring-LWE instances, we set prime number $q = 1021$ and the standard deviation of the discrete Gaussian distribution $\sigma = 8/\sqrt{2\pi}$. For solving the Ring-LWE over various number fields, we set parameters of the extension, which are embedding constant η and the rotation parameter r ($r = 1$ is the original Kannan's embedding). Furthermore, we set the block size β, which is significant for BKZ algorithm to solve the Ring-LWE problem for observing the change of the difficulty of the Ring-LWE problem.

5.2 Experimental Results

We show results of solving the Ring-LWE problem over the 128-th cyclotomic field (ζ_{128}) in Table 1, the Ring-LWE problem over the 67-th cyclotomic field (ζ_{67}) in Table 2, the Ring-LWE problem over the 81-th cyclotomic field (ζ_{81}) in Table 3 and the Ring-LWE problem over the maximal real subfield of 128-th cyclotomic field ($\zeta_{256} + \zeta_{256}^{-1}$) in Table 4. In Table 1 and Table 3, we can see the success probability increases by the extension. Particularly, when the rotation constant r is 2, the success probability is the highest. In Table 1, the embedding constant $\eta = 1$ is appropriate, and in Table 3, $\eta = 2$ is appropriate. However, in Table 2 and Table 4, the success probability is higher when not using the rotation. In Table 2, the success probability is higher when the embedding constant η is 1, while in Table 4, using embedding constants $\eta = 2, \lfloor \sigma \rceil$ yields better results. From these results, we observe that the embedding using rotation is effective in Table 1 and Table 3. However, it is not effective in Table 2 and Table 4. One potential reason for this discrepancy could be the norm of the vector to which rotation is applied during the embedding process. For example, when we use the rotation to the norm of the vector of the Ring-LEW over the maximal real subfields of 2^k-th cyclotomic fields, the all entries of the rotated vector is changed. Thus, the norm can sometimes be larger than the norm before rotated. Also, from the sight of RHF, average RHF is decreasing when using the rotation or changing the embedding constant η. In other words, we can find the short vector.

Table 1: Result on the success probability of solving the Ring-LWE over (ζ_{128})

2*n	2*dim(L)	2*η	2*r	β	success probability	average runtime [s]	average RHF
27*128	27*64	9*1	3*1	10	0/100	28.2012	1.01307
				15	2/100	35.9549	1.01191
				20	28/100	71.6206	1.00821
4-12			3*2	10	0/100	28.7374	1.01290
				15	9/100	36.9008	1.01086
				20	52/100	76.7666	1.00532
4-12			3*3	10	0/100	29.4001	1.01265
				15	1/100	37.5975	1.01164
				20	36/100	75.3515	1.00696
		9*2	3*1	10	0/100	28.7507	1.01321
				15	5/100	36.8798	1.01158
				20	35/100	72.8721	1.00742
4-12			3*2	10	0/100	29.3034	1.01291
				15	8/100	38.3813	1.01107
				20	46/100	74.4904	1.00652
4-12			3*3	10	0/100	29.6899	1.01280
				15	6/100	38.5954	1.01117
				20	41/100	75.0901	1.00652
		9*$\lfloor\sigma\rceil$	3*1	10	0/100	28.9424	1.01315
				15	5/100	37.5599	1.01165
				20	42/100	71.5523	1.00664
4-12			3*2	10	0/100	29.6163	1.01306
				15	12/100	39.5411	1.01062
				20	47/100	73.9216	1.00596
4-12			3*3	10	1/100	29.6331	1.01266
				15	3/100	40.1286	1.01162
				20	38/100	78.2503	1.00687

Table 2: Result on the success probability of solving the Ring-LWE over (ζ_{67})

2*n	2*dim(L)	2*η	2*r	β	success probability	average runtime [s]	average RHF
27*67	27*66	9*1	3*1	10	0/100	32.2250	1.01307
				15	5/100	41.2779	1.01157
				20	25/100	69.6289	1.00848
4-12			3*2	10	0/100	32.8831	1.01292
				15	0/100	41.6514	1.01204
				20	21/100	72.6897	1.00885
4-12			3*3	10	0/100	33.4276	1.01265
				15	1/100	42.6877	1.01175
				20	12/100	74.9125	1.00971
		9*2	3*1	10	0/100	32.8557	1.01312
				15	7/100	41.4086	1.01142
				20	26/100	70.0850	1.00834
4-12			3*2	10	0/100	33.0295	1.01301
				15	0/100	42.1867	1.01208
				20	16/100	72.6963	1.00943
4-12			3*3	10	0/100	33.3357	1.01288
				15	3/100	42.9323	1.01150
				20	15/100	73.3669	1.00945
		9*$\lfloor\sigma\rceil$	3*1	10	0/100	32.5904	1.01315
				15	3/100	40.9812	1.01191
				20	23/100	69.0079	1.00880
4-12			3*2	10	0/100	32.2464	1.01309
				15	3/100	41.6757	1.01170
				20	24/100	73.3994	1.00847
4-12			3*3	10	0/100	33.2352	1.01291
				15	0/100	42.0928	1.01198
				20	15/100	72.0338	1.00953

Table 3: Result on the success probability of solving the Ring-LWE over (ζ_{81})

2*n	2*dim(L)	2*η	2*r	β	success probability	average runtime [s]	average RHF
27*81	27*54	9*1	3*1	10	32/100	21.6873	1.00912
				15	72/100	25.0095	1.00348
				20	97/100	36.2099	1.00035
4-12			3*2	10	35/100	20.4281	1.00864
				15	76/100	25.4513	1.00285
				20	98/100	35.6181	1.00022
4-12			3*3	10	38/100	19.5336	1.00805
				15	68/100	25.8174	1.00378
				20	99/100	39.0410	1.00010
		9*2	3*1	10	23/100	19.9991	1.01049
				15	70/100	25.7547	1.00373
				20	97/100	34.3704	1.00035
4-12			3*2	10	38/100	19.8861	1.00820
				15	78/100	25.5721	1.00267
				20	98/100	35.7179	1.00023
4-12			3*3	10	43/100	22.7902	1.00743
				15	72/100	23.9291	1.00336
				20	100/100	37.7671	0.99996
		9*$\lfloor\sigma\rceil$	3*1	10	32/100	19.4488	1.00926
				15	75/100	23.2080	1.00315
				20	95/100	34.0210	1.00056
4-12			3*2	10	37/100	20.4731	1.00849
				15	85/100	22.6911	1.00182
				20	99/100	33.9639	1.00011
4-12			3*3	10	39/100	20.1548	1.00798
				15	83/100	24.5066	1.00202
				20	99/100	37.4611	1.00010

Table 4: Result on the success probability of solving the Ring-LWE over $(\zeta_{128} + \zeta_{128}^{-1})$

2*n	2*dim(L)	2*η	2*r	β	success probability	average runtime [s]	average RHF
27*256	27*64	9*1	3*1	10	0/100	35.9106	1.01301
				15	4/100	44.2290	1.01156
				20	23/100	71.5068	1.00871
4-12			3*2	10	0/100	38.1171	1.01274
				15	1/100	45.7817	1.01177
				20	14/100	72.4960	1.00953
4-12			3*3	10	0/100	38.7443	1.01258
				15	2/100	45.0618	1.01144
				20	7/100	73.6846	1.01010
		9*2	3*1	10	0/100	34.8269	1.01311
				15	1/100	44.8616	1.01196
				20	26/100	71.6424	1.00841
4-12			3*2	10	1/100	36.8600	1.01277
				15	2/100	44.9364	1.01176
				20	18/100	72.0038	1.00922
4-12			3*3	10	0/100	36.3868	1.01274
				15	0/100	44.1778	1.01188
				20	8/100	71.4290	1.01023
		9*$\lfloor\sigma\rceil$	3*1	10	0/100	35.4077	1.01306
				15	2/100	43.7948	1.01195
				20	31/100	69.7193	1.00786
4-12			3*2	10	0/100	37.5812	1.01299
				15	5/100	44.6137	1.01145
				20	18/100	72.9397	1.00922
4-12			3*3	10	0/100	37.4798	1.01286
				15	1/100	46.2803	1.01182
				20	14/100	73.5979	1.00961

In Table 1 and Table 3, we can see the success probability increases by the extension. Particularly, when the rotation constant r is 2, the success probability is highest. In Table 1, the embedding constant $\eta = 1$ is appropriate, and in Table 3, $\eta = 2$ is appropriate. However, in Table 2 and Table 4, the success probability is higher when not using the rotation. In Table 2, the success probability is higher when the embedding constant η is 1, while in Table 4, using embedding constants $\eta = 2, \lfloor\sigma\rceil$ yields better results. From these results, we observe that the embedding using rotation is effective in Table 1 and Table 3. However, it is not effective in Table 2 and Table 4. One potential reason for this discrepancy could be the norm of the vector to which rotation is applied during the embedding process. In [12], the extension of the Ring-LWE over 2^k-th cyclotomic fields is to find easier by adding the target vector and the rotated vectors, which have the same norm, to the q-aray lattice than the original embedding. For example, when we use the rotation to the norm of the vector of the Ring-LEW over the maximal real subfields of 2^k-th cyclotomic fields, the all entries of the rotated vector is changed. Thus, the norm can sometimes be larger than the norm before rotated. However, when we use the rotation to the norm of the vector of the Ring-LEW over 3^k-th cyclotomic fields, the all entries of the rotated vector is not much changed. Also, from the view of root hermite factor which is an indicator that the closer it is to 1, the easier it is to find a short vector, average root hermite factor is decreasing when using the rotation or changing the embedding constant η. In other words, we can find the short vector.

6 Conclusion

In this work, we demonstrate the effectiveness of an extension of Kannan's embedding. According to our results, it is found that for the Ring-LWE over some number fields, where the norm is changed a little, and it is expected that the extension with the rotation is effective. However, for the Ring-LWE over the number fields such as p-th cyclotomic fields and the maximal real subfields of 2^k-th cyclotomic fields, where the norm of them changes significantly, the extension with the rotation is not effective. From the view of root hermite factor, the average root hermite factor of the Ring-LWE over 2^k-th cyclotomic fields, 3^k-th cyclotomic fields, p-th cyclotomic fields and subfields of 2^k-th cyclotomic fields may be decreasing by using the extension or changing the embedding constant. Thus, we conclude that we may find the short vector by using the extension or changing the embedding constant. For the future works, we need to improve the extension with the rotation for the number fields, which are not effective, by new technique which is effective to the Ring-LWE over all number fields.

Acknowledgement

This work is partially supported by JSPS KAKENHI Grant Number JP21H03443 and SECOM Science and Technology Foundation.

References

[1] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS - kyber: A cca-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018*, pages 353–367. IEEE, 2018.

[2] Léo Ducas, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS - dilithium: Digital signatures from module lattices. *IACR Cryptol. ePrint Arch.*, page 633, 2017.

[3] Thomas Pornin and Thomas Prest. More Efficient Algorithms for the NTRU Key Generation Using the Field Norm. In Dongdai Lin and Kazue Sako, editors, *Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography*, volume 11443 of *Lecture Notes in Computer Science*, pages 504–533. Springer, 2019.

[4] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3):565–599, 2015.

[5] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On Ideal Lattices and Learning with Errors over Rings. *Journal of the ACM (JACM)*, 60(6):1–35, 2013.

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

[7] Ravi Kannan. Minkowski's Convex Body Theorem and Integer Programming. *Mathematics of operations research*, 12(3):415–440, 1987.

[8] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE):515–534, 1982.

[9] Claus-Peter Schnorr and Martin Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Mathematical programming*, 66(1):181–199, 1994.

[10] Daniele Micciancio and Panagiotis Voulgaris. Faster exponential time algorithms for the shortest vector problem. In *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms*, pages 1468–1480. SIAM, 2010.

[11] Panagiotis Voulgaris. Gauss sieve alpha v. 0.1 (2010).

[12] Satoshi Nakamura and Masaya Yasuda. An extension of kannan's embedding for solving ring-based lwe problems. In *Cryptography and Coding: 18th IMA International Conference, IMACC 2021, Virtual Event, December 14–15, 2021, Proceedings 18*, pages 201–219. Springer, 2021.

[13] Michael Schneider. Sieving for shortest vectors in ideal lattices. In *Progress in Cryptology–AFRICACRYPT 2013: 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22-24, 2013. Proceedings 6*, pages 375–391. Springer, 2013.

[14] Tsukasa Ishiguro, Shinsaku Kiyomoto, Yutaka Miyake, and Tsuyoshi Takagi. Parallel gauss sieve algorithm: Solving the svp challenge over a 128-dimensional ideal lattice. In *Public-Key Cryptography–PKC 2014: 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings 17*, pages 411–428. Springer, 2014.

[15] M.Schneider. T.Plantard. *Ideal Lattice Challenge.*

[16] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020.

[17] The NTL Developers. *NTL: A Library for doing Number Theory (Version 11.5.1)*, 2021.