

Security Impact Analysis of Degree of Field Extension in Lattice Attacks on Ring-LWE Problem

1st Yuri Lucas Direbieski
Grad. Sch. of Sci. and Tech. for Innov.
Tokushima University
Tokushima, Japan
c612235001@tokushima-u.ac.jp

2nd Hiroki Tanioka
Center for Adm. of Info. Tech.
Tokushima University
Tokushima, Japan
<https://orcid.org/0000-0003-3404-0855>

3rd Kenji Matsuura
Center for Adm. of Info. Tech.
Tokushima University
Tokushima, Japan
ma2@tokushima-u.ac.jp

4th Hironori Takeuchi
Center for Adm. of Info. Tech.
Tokushima University
Tokushima, Japan
takeuchi.hironori@tokushima-u.ac.jp

5th Masahiko Sano
Center for Adm. of Info. Tech.
Tokushima University
Tokushima, Japan
sano@tokushima-u.ac.jp

6th Tetsushi Ueta
Center for Adm. of Info. Tech.
Tokushima University
Tokushima, Japan
<https://orcid.org/0000-0001-5810-437X>

Abstract—Modern information communications use cryptography to keep the contents of communications confidential. RSA (Rivest–Shamir–Adleman) cryptography and elliptic curve cryptography, which are public-key cryptosystems, are widely used cryptographic schemes. However, it is known that these cryptographic schemes can be deciphered in a very short time by Shor’s algorithm when a quantum computer is put into practical use. Therefore, several methods have been proposed for quantum computer-resistant cryptosystems that cannot be cracked even by a quantum computer. A simple implementation of LWE-based lattice cryptography based on the LWE (Learning With Errors) problem requires a key length of $O(n^2)$ to ensure the same level of security as existing public-key cryptography schemes such as RSA and elliptic curve cryptography. In this paper, we attacked the Ring-LWE (RLWE) scheme, which can be implemented with a short key length, with a modified LLL (Lenstra-Lenstra-Lovász) basis reduction algorithm and investigated the trend in the degree of field extension required to generate a secure and small key. Results showed that the lattice-based cryptography may be strengthened by employing Cullen or Mersenne prime numbers as the degree of field extension.

Index Terms—lattice cipher, ring-LWE, LLL basis reduction

I. INTRODUCTION

Modern information communications use cryptography to keep the contents of communications confidential. The widely used cryptographic schemes include RSA (Rivest–Shamir–Adleman) and elliptic curve cryptography, which are public-key cryptographic schemes. These cryptographic schemes are based on the fact that current computers cannot solve prime factorization and discrete logarithm problems in a realistic amount of time. However, these cryptographic schemes are not secure against quantum computer attacks. It is known that these cryptographic schemes can be cracked in a very short time by Shor’s algorithm when quantum computers are put into practical use. If quantum computers are put into practical use, the security of the public key cryptography currently in use will not be guaranteed. Therefore, it is desirable to develop and implement post-

quantum cryptography that cannot be deciphered even by a quantum computer. Several methods have been proposed for post-quantum cryptography. Multivariate polynomial cryptosystems, code-based cryptosystems, lattice cryptosystems, and homomorphic mapping cryptosystems have been widely studied as promising quantum computer cryptosystems.

In this study, we focus on lattice cryptography. Lattice cryptography is a public-key cryptographic scheme that uses a mathematical problem called the lattice point search problem. Several implementations have been proposed, most of which are based on the CVP (Closest Vector Problem), SVP (Shortest Vector Problem), and LWE (Learning With Errors). Our experiments were conducted on lattice ciphers based on LWE in particular, which are described in the following flow. Sec. II explains related researches on lattice cryptography based on the LWE and Ring-LWE (RLWE) problem. Sec. III describes the concepts and definitions of lattice basis reduction and the RLWE problem, as well as the attack methods, Kannan’s embedding method [1] and the LLL (Lenstra-Lenstra-Lovász) basis reduction algorithm [2]. Sec. IV explains the structure of RLWE problem used in the experiment, and also describe our proposed method and experimental results. Finally, section V provides a summary of the study.

II. RELATED WORKS

In this section, we first introduce related works on lattice cryptography for the RLWE problem. Next, a study of an attack on the RLWE problem using Kannan’s embedding method and another study of an attack on the RLWE problem using Babai’s nearest-neighbor plane algorithm [3] are described.

A. Ring-LWE problem

Lyubashevsky et al. pointed out that the conventional LWE lattice cryptography incur an overhead of $O(n^2)$ in key sharing; therefore, they proposed more efficient LWE-based

cryptography, RLWE, by introducing an algebraic structure for the LWE problem [4]. In the RLWE problem under attack, two RLWE samples are generated with a common secret key, and are used as input for the basis reduction algorithm utilized in the lattice attack.

B. Safety Analysis of Ring-LWE

Uesugi et al. experimentally analyze the safety of RLWE by performing a lattice attack using the Progressive-BKZ algorithm on the RLWE problem on a subfield of the cyclotomic field [5] [6]. Here, Kannan’s embedding method is used in a lattice attack to extract errors by attributing the CVP to a unique SVP, and the attack is successful if the errors are found correctly. Their experimental results showed that the squared cyclotomic field is the safest, and that the success rate of lattice attacks decreases and execution time increases when the squared cyclotomic field and basis geometry are different.

C. Lattice attacks on Ring-LWE field

Terada et al. [7] experimentally analyzed the RLWE problem in the decomposition field proposed by Arita et al. [8] and performed a lattice attack on the RLWE problem of some prime cyclotomic fields, comparing execution time, success rate, and root Hermite factor. Experimental results show that Kannan’s embedding method is much faster than Babai’s nearest plane algorithm. In addition, The behavior of the basis reduction algorithm is highly dependent on the structure of the input lattice. As a lattice attack using machine learning, SALSA [9] was proposed as a method using transformers to perform modular arithmetic and combine half-trained models with statistical cryptanalysis techniques. Then, it is now clear that SALSA can break LWE problem of medium dimension (up to $n = 128$) with sparse binary secrets.

D. Summary of related works

A lattice-based cryptography on the LWE problem was proposed as an implementation of a lattice-based cryptography, however, it is inefficient because it requires the sharing of $O(n^2)$ sized matrix for parameter pre-sharing. The more efficient lattice-based cryptography, the RLWE, was proposed by restricting the LWE problem to polynomial rings, where the shared elements are vectors of polynomial coefficients. For those RLWE problem-based lattice cryptography security has not been completely proven and there may be instances that provide weak RLWE problem. This study focuses on the degree of field extension, which is the dimension of the lattice of the RLWE problem, and conducts a study on the security against lattice attacks using Kannan’s embedding method. Generally, a value of a power of two is chosen for the degree of field extension, and a value of about a power of two is considered effective against lattice attacks. However, a related study that conducted safety analysis using the Progressive-BKZ algorithm for the RLWE problem on real and imaginary segments reported that the success rate tends to be low when the dimension is prime number, and the analysis on the number of dimensions is not sufficient. Therefore, the objective of this

study is to examine the effect of the order of the field extension on the lattice attack by constructing an RLWE problem where the order is chosen to the power of two.

III. IMPLEMENTATION OF A SAFETY ANALYSIS OF THE RING-LWE PROBLEM

This section explains the lattice basis reduction algorithm and the concept of the RLWE problem, followed by a description of the attack methods, Kannan’s embedding method and the LLL basis reduction algorithm.

A. Lattice basis reduction algorithm

We explain the CVP as a basic computationally hard problem in lattice. CVP is the problem of finding a vector \mathbf{x} such that, given a lattice \mathcal{L} and target vector \mathbf{t} , $\|\mathbf{t} - \mathbf{x}\| \leq \|\mathbf{t} - \mathbf{y}\|$ for all vectors $\mathbf{y} \in \mathcal{L}$ in $\text{CVP}(\mathcal{L}, \mathbf{t})$. Furthermore, there exists an approximate CVP $\text{CVP}(\mathcal{L}, \mathbf{t}, \gamma)$ that introduces a real number $\gamma > 1$. Approximate CVP is the problem of finding a vector \mathbf{x} such that $\|\mathbf{t} - \mathbf{x}\| \leq \gamma \|\mathbf{t} - \mathbf{y}\|$ for all vectors $\mathbf{y} \in \mathcal{L}$. The Babai’s nearest plane algorithm [3] and Kannan’s embedding method [1], both of which are general-purpose methods for solving LWE problem, are algorithms for solving approximate CVPs [10]. The analysis of lattice cryptography comes down to the problem of computing lattices, including approximate CVPs. Since many of the lattice point search problems that make up lattice cryptography become more difficult as the rank of the lattice basis increases, the quality of the aforementioned algorithms depends on the rank of the input lattice. In solving lattice problems such as those described above, a lattice basis reduction algorithm is usually used that makes the lattice basis nearly orthogonal, and in practice, a LLL basis reduction is used as input for Kannan’s embedding method. The root Hermite coefficient [11] used to evaluate the quality of the basis reduction algorithm is used as a measure of how well the lattice reduction algorithm shortens the lattice elements.

B. Ring learning with errors problem

We analyze the security for the RLWE problem on a subfield on a cyclotomic field and a splitting field using the method explained in [5]. Let K the degree of a field extension and O_K be an algebraic number field. Let χ_{secret} be a secret key probability distribution on O_K , and χ_{error} be an error key probability distribution on O_K . Additionally, let p be an integer as polynomial ring, and a field extension O_K/pO_K be denoted as $O_{K,p}$. For a probability distribution χ on a set X , write $a \leftarrow \chi$ if $a \in X$ is chosen according to χ , and $U(X)$ is a uniform distribution on X . The RLWE probability distribution such that $O_{K,p} \times O_{K,p}$ is denoted by $R_{K,p,\chi_{secret},\chi_{error}}$. Various parameters $(a, as+e)$ are defined according to these probability distributions, where $a \leftarrow U(O_{K,p})$, $s \leftarrow \chi_{secret}$, $e \leftarrow \chi_{error}$ respectively. The RLWE problem has two variant. One is the problem of distinguishing $R_{K,p,\chi_{secret},\chi_{error}}$ from $U(O_{K,p} \times O_{K,p})$, which is called the decision RLWE problem. The other problem is to find $s \in O_{K,p}$ for any given number of samples $(a_i, a_i s + e_i) \in O_{K,p} \times O_{K,p}$ which chosen from $R_{K,p,\chi_{secret},\chi_{error}}$. This problem is called the search RLWE

problem. In public-key cryptography, the problem of finding the secret key corresponds to the search RLWE problem [12], [13].

C. Formalization of Ring-LWE problem

The RLWE problem used in our study is described in more detail below. The various parameters of the RLWE problem for safety analysis [12] are as follows.

- Prime number q ... a law of each coefficient.
- Number of terms in the polynomial n ... the dimension K of the RLWE problem.
- Cyclotomic integers a ... coefficients chosen from χ .
- Secret cyclotomic integer s ... coefficients take 0 or 1.
- Error cyclotomic integer e ... coefficients sufficiently smaller than modulo q .
- Public key parameter b ... defined for a , s and e .

Consider an algebraic number field O_K with respect to the degree of the field extension K and define a prime number q . In this case, a prime number p is provided for the polynomial ring $O_{K,q}$. The parameter a is chosen in the range $(-\frac{q}{2}, \frac{q}{2}]$ and according to a probability distribution χ . In addition, the parameter s takes the values 0 or 1, which is chosen from the probability distribution χ_{secret} . For an additional error e , define a normal distribution with mean 0 and variance σ^2 for $\sigma > 0$, and sample real numbers from $\chi_{error} = N(0, \sigma^2)$ to obtain the error distribution. Moreover, rounded to the nearest integer, each coefficient of the error cyclotomic integer e .

$$a \leftarrow \chi, \quad s \leftarrow \chi_{secret}, \quad e \leftarrow \chi_{error} \quad (1)$$

From the definition of the RLWE problem, the parameter b is defined for these parameters as

$$b = as + e. \quad (2)$$

To implement Kannan's embedding method, a matrix A is constructed using several cyclotomic polynomials a . Where a integral basis of $O_{K,q}$ is $\{x_0, x_1, \dots, x_{n-1}\}$, the parameters a, s, e can be expressed as

$$a = \sum_{i=0}^{n-1} a_i x_i, (a_i \in \mathbb{Z}_q), \quad (3)$$

$$s = \sum_{i=0}^{n-1} s_i x_i, (s_i \in \mathbb{Z}_q), \quad (4)$$

$$e = \sum_{i=0}^{n-1} e_i x_i, (e_i \in \mathbb{Z}_q). \quad (5)$$

However, \mathbb{Z}_q is an Abelian group. Additionally, there exists $a_{i,j}$ such that

$$ax_j = \sum_{i=0}^{n-1} a_{i,j} x_i, (a_{i,j} \in \mathbb{Z}_q) \quad (6)$$

holds for $0 \leq j \leq n-1$. Using ax_j , it can be written as

$$\begin{aligned} as &= \sum_{j=0}^{n-1} s_j (ax_j), \\ &= \sum_{j=0}^{n-1} s_j \left(\sum_{i=0}^{n-1} a_{i,j} x_i \right), \\ &= \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} a_{i,j} s_j \right) x_i. \end{aligned} \quad (7)$$

Here, by setting

$$\mathbf{b} = (b_0, \dots, b_{n-1})^T, \quad (8)$$

$$\mathbf{s} = (s_0, \dots, s_{n-1})^T, \quad (9)$$

$$\mathbf{e} = (e_0, \dots, e_{n-1})^T, \quad (10)$$

and then we obtain the following equation,

$$\mathbf{b} = A\mathbf{s} + \mathbf{e} \pmod{q}, \quad (11)$$

where A is

$$A = \begin{pmatrix} a_{0,0} & \dots & a_{0,n-1} \\ \vdots & \ddots & \vdots \\ a_{n-1,0} & \dots & a_{n-1,n-1} \end{pmatrix}. \quad (12)$$

Similarly, given that another RLWE sample (A', \mathbf{b}') is generated using the common \mathbf{s} , there is $A' \in (\mathbb{Z}/q\mathbb{Z})^{n \times n}$, $\mathbf{b}' \in (\mathbb{Z}^n)$, $\mathbf{e}' \in (\mathbb{Z})^n$ satisfying

$$\mathbf{b}' = A'\mathbf{s} + \mathbf{e}' \pmod{q}. \quad (13)$$

Therefore, it can be expressed as

$$\begin{pmatrix} \mathbf{b} \\ \mathbf{b}' \end{pmatrix} = \begin{pmatrix} A \\ A' \end{pmatrix} \cdot \mathbf{s} + \begin{pmatrix} \mathbf{e} \\ \mathbf{e}' \end{pmatrix} \pmod{q}. \quad (14)$$

This corresponds to the RLWE problem with dimension n and number of samples $2n$. Consider the case where an attack is made on the RLWE problem such that the equation is satisfied.

D. Kannan's embedding

Apply Kannan's embedding method to the RLWE sample matrix A obtained for the RLWE problem described in Sec. III-B. Kannan's embedding method [1] that is a generic solution for CVP, extracts errors as a difference vector by attributing the CVP to a unique SVP [10]. Consider the basis of the n -dimensional lattice $\mathcal{L} \subseteq \mathbb{Z}^n$ and the solution vector $\mathbf{v} = \sum_{i=1}^n v_i \mathbf{b}_i \in \mathcal{L}$, $(\exists v_i \in \mathbb{Z})$ of the CVP for the target vector \mathbf{w} . In this case, assuming that the norm $\|\mathbf{e}\|$ of the difference vector $\mathbf{e} = \mathbf{w} - \mathbf{v}$ between the target vector and of the solution vector are sufficiently small. Kannan's embedding method constructs a new lattice $\tilde{\mathcal{L}}$ containing this difference vector as the shortest vector. The lattice $\tilde{\mathcal{L}} \in \mathbb{Z}^{n+1}$ consists of a $(n+1)$ -dimensional lattice generated by a linearly independent vector $(n+1)$ of vectors $(\mathbf{b}_1, 0), \dots, (\mathbf{b}_n, 0), (\mathbf{w}_1, M) \in \mathbb{Z}^{n+1}$ for a fixed positive constant $M \in \mathbb{Z}$. Furthermore,

$$\begin{aligned} (e, M) &= \left(\mathbf{w} - \sum_{i=1}^n v_i \mathbf{b}_i, M \right) \\ &= -v_1 (\mathbf{b}_1, 0) \dots - v_n (\mathbf{b}_n, 0) + (\mathbf{w}, M) \end{aligned} \quad (15)$$

Algorithm 1 Kannan's embedding technique

Require: Basis $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ of n -dimensional lattice $\mathcal{L} \subseteq \mathbb{Z}^n$, target vector \mathbf{w}

Ensure: The lattice vector $\mathbf{v} \in \mathcal{L}$, or *false* closest to \mathbf{w}

- 1: Lattice $\tilde{\mathcal{L}} \leftarrow \begin{pmatrix} B & \mathbf{w} \\ 0 & 1 \end{pmatrix}$ generated from $Bandw$
 - 2: Simplify $\tilde{\mathcal{L}}$.
 - 3: **if** $\mathbf{v} \leftarrow \pm(\mathbf{v}_1, \dots, \mathbf{v}_n, 1)$ **then**
 - 4: return \mathbf{v}
 - 5: **else**
 - 6: return *false*
 - 7: **end if**
-

where the vector (e, M) is contained in the lattice $\tilde{\mathcal{L}}$.

In particular, when vector (e, M) is the shortest vector on lattice $\tilde{\mathcal{L}}$, by solving for the SVP on the lattice $\tilde{\mathcal{L}}$, the difference vector $\|e\|$ can be obtained.

As a result, the solution $\mathbf{v} = \mathbf{w} - e$ of CVP can be obtained. Consider applying Kannan's embedding method to the sample RLWE problem described in Sec. III-C. Using the elements of (11), construct the matrix A_c, \mathbf{b}_c as

$$A_c = \begin{pmatrix} A & A' \\ qI_n & O \\ O & qI_n \end{pmatrix}, \mathbf{b}_c = (\mathbf{b} \quad \mathbf{b}'). \quad (16)$$

Finding the errors e, e' is equivalent to solving for the CVP on the lattice, which is generated by the row vectors of A_c with \mathbf{b}_c as the target vector. By solving CVP to find the vector which closest to the target vector, the error can be extracted by difference. Algorithm 1 shows the algorithm of Kannan's embedding technique. The operation of converting the basis to a basis of the same lattice \mathcal{L} , where each basis vectors are short and nearly orthogonal to each other, when given a basis $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ of the lattice \mathcal{L} . It is called lattice basis reduction algorithm.

E. LLL lattice basis reduction algorithm

In the experiment, the LLL lattice basis reduction algorithm [2] is used as the algorithm to generate the reduced basis with Kannan's embedding method. LLL lattice basis reduction algorithm is a well-known and representative algorithm, which is an efficient algorithm to approximate SVP on an n -dimensional lattice. For basis reduction on 2-dimensional lattices, Lagrange's basis reduction algorithm can be used to reduced a 2-dimensional lattice in polynomial time and obtain an exact solution. However, in the general dimension case, the LLL basis reduction algorithm is used to approximate the reduction basis.

In particular, it is called the LLL basis reduction when the following two conditions are satisfied.

- 1) $|\mu_{i,j}| \leq \frac{1}{2}$ for natural numbers $1 \leq j < i \leq n$ (Size reduction)
- 2) $(\delta - \mu_{i+1,i}^2)|b_i^*|^2 \leq |b_{i+1}^*|^2$ for natural numbers $1 \leq j < n$ (Lovász's condition)

The LLL basis reduction algorithm reduces the lattice by repeating two operations: first, the basis is reduced to size, and then the Lovász condition is checked if it is satisfied; if

Algorithm 2 LLL basis reduction algorithm

Require: Basis $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ of n -dimensional lattice $\mathcal{L} \subseteq \mathbb{Z}^n$, parameter $0 \leq \sigma < 1$

Ensure: Simplified basis $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ for n -dimensional lattice $\mathcal{L} \subseteq \mathbb{Z}^n$ with respect to σ

- 1: Basis $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ GSO coefficient $(\mu_{i,j})_{1 \leq j < i \leq n} \leftarrow GSO(\mathbf{b}_1, \dots, \mathbf{b}_n)$
 - 2: Compute $\|b_i^*\|^2, (1 \leq i \leq n)$
 - 3: $k = 2$
 - 4: **while** $k \leq n$ **do**
 - 5: **for** $j = k - 1$ **downto** 1 **do**
 - 6: **if** $|\mu_{k,j}| > \frac{1}{2}$ **then**
 - 7: $b_k = b_k - \lfloor \mu_{k,j} \rfloor b_j$
 - 8: $b_1^*, \dots, b_n^*, (\mu_{i,j})_{1 \leq j < i \leq n} = GSO(b_1, \dots, b_n)$
 - 9: **end if**
 - 10: **end for**
 - 11: **if** $(\delta - \mu_{i+1,i}^2)|b_i^*|^2 \leq |b_{i+1}^*|^2$ **then**
 - 12: $k = k + 1$
 - 13: **else**
 - 14: $swap(b_k, b_{k-1})$
 - 15: $b_1^*, \dots, b_n^*, (\mu_{i,j})_{1 \leq j < i \leq n} = GSO(b_1, \dots, b_n)$
 - 16: Compute $\|b_i^*\|^2, (1 \leq i \leq n)$
 - 17: $k = \max\{2, k - 1\}$
 - 18: **end if**
 - 19: **end while**
 - 20: **return** $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$
-

not, the process starts over. Algorithm 2 shows the LLL basis simplification algorithm.

To apply Kannan's embedding method, first find the reduced lattice basis of the input. Therefore, the LLL basis reduction algorithm is performed on matrix A_c to obtain the reduced matrix A_{LLL} . Applying Kannan's embedding method to this matrix A_{LLL} yields a matrix $W \in (O_{K,q})^{(2n+1) \times (2n+1)}$ such that

$$W = \begin{pmatrix} A_{LLL} & 0^T \\ \mathbf{b}_c & 1 \end{pmatrix}. \quad (17)$$

Simplifying the matrix W again using the LLL basis reduction algorithm yields the error vector $(e, e', 1)$ from the reduced matrix. In our experiments, the LLL lattice basis reduction algorithm is used as the algorithm used to generate the reduced basis by Kannan's embedding method.

IV. PROPOSED METHOD AND EXPERIMENT

To analyze the impact of the degree of field extension which is the dimension of the lattice of the RLWE problem on lattice cryptography, this section describes the RLWE problem used in the lattice attack experiments, followed by a description of the experiments and the environment. For various parameters of the RLWE problem, let the prime number $q = 1997$ and the Gaussian distribution parameter $\sigma = \frac{4}{\sqrt{2\pi}}$ [14]. The values of the cyclotomic integers a, s, e follow the definition of Sect. III-C. In this experiment, three integers of powers of 2, $n = \{32, 64, 128\}$, are chosen as reference integers, two integers which are ± 1 and the two larger and smaller primes closest to each reference integer are chosen, and 100 times decoding experiments are performed for 21 integers as degree of field extension d to investigate its effect on the lattice attack. The integers representing the degree of field

extension to be handled are $d = \{23, 29, 31, 32, 33, 37, 41\}$ for $n = 32$, $d = \{59, 61, 63, 64, 65, 67, 71\}$ for $n = 64$, and $d = \{109, 113, 127, 128, 129, 131, 137\}$ for $n = 128$. For the RLWE problem described above, the equations mentioned in Sec. III-C are constructed, Kannan's embedding method mentioned in Sec. III-D is performed, and the error e_{sought} is extracted. Equation (11) is deformed to obtain the secret-key s_{sought} using (19) after extracting the error e_{sought} .

$$\mathbf{b} = A\mathbf{s} + \mathbf{e} \pmod{q} \quad (18)$$

$$\mathbf{s} = (\mathbf{b} - \mathbf{e}) \cdot A^{-1} \pmod{q} \quad (19)$$

Finally, the plaintext is decoded using the secret-key s_{sought} . If the plaintext is equal to the original plaintext, the attack is successful.

A. Experimental procedure

The following flow of experiments will be conducted.

- 1) Generating two RLWE samples including (A, \mathbf{b}) , specifically \mathbf{b} is conducted by \mathbf{e} which is based on a secret key \mathbf{s}
- 2) Encoding a plaintext \mathbf{m} with (A, \mathbf{b}) to a ciphertext C
- 3) Obtaining a error e_{sought} from (A, \mathbf{b}) using Kannan's embedding
- 4) Finding a secret key s_{sought} with e_{sought}
- 5) Decoding C to a plaintext \mathbf{m}_{sought} with s_{sought}
- 6) Comparing \mathbf{m}_{sought} with \mathbf{m}

First, convert the plaintext m from a sequence of n random numbers consisting of 0 or 1 values to a cyclotomic integer $\mathbf{m} = \sum_{i=0}^{n-1} m_i x_i (m_i \in \mathbb{Z}_q)$ and prepare 100 plaintext sentences m .

Second, consider the RLWE problem satisfying (14) and the generated plaintext is encrypted using the public-key (A, \mathbf{b}) . Specifically, a small random number $\mathbf{v} = \sum_{i=0}^{n-1} v_i x_i (v_i \in \mathbb{Z}_q)$, noise $e_0, e_1 \leftarrow (0, \sigma)$ is generated and $\mathbf{c}_0, \mathbf{c}_1$ defined by

$$\mathbf{c}_0 = \mathbf{b}\mathbf{v} + 2e_0 + \mathbf{m} \quad (20)$$

$$\mathbf{c}_1 = A\mathbf{v} + 2e_1. \quad (21)$$

Thus, ciphertext $C = (\mathbf{c}_0, \mathbf{c}_1)$ is obtained. To decrypt ciphertext C , the plaintext \mathbf{m} is decrypted according to (22) using secret key \mathbf{s} [15].

$$\begin{aligned} \mathbf{c}_0 - \mathbf{s}\mathbf{c}_1 &\equiv \mathbf{b}\mathbf{v} + 2e_0 + \mathbf{m} - \mathbf{s}(A\mathbf{v} + 2e_1) \\ &\equiv \mathbf{m} + 2(\mathbf{e}\mathbf{v} + e_0 - \mathbf{s}\mathbf{e}_1) \pmod{q} \end{aligned} \quad (22)$$

Hence, Kannan's embedding method is applied to the matrix A, AA' and target vectors \mathbf{b}, \mathbf{b}' , and the error e_{sought} is extracted according to Sec. III-D.

The secret key s_{sought} is obtained according to (19), and the plaintext \mathbf{m}_{sought} can be decrypted according to (22) with error e_{sought} and the attack is successful if the decrypted plaintext \mathbf{m}_{sought} is equal to the original plaintext \mathbf{m} . The decryption time is defined as the time from the start of the execution of Kannan's embedding method to the time when the secret key s_{sought} is obtained. The above experiment is performed 100 times for each degree of a field extension n , and the number of successful attacks and the average execution time are measured.

TABLE I
RESULTS OF ATTACK TO FIELD EXTENSION AROUND M_{32}

Field extension	Success rate	Average time [s]
23	0.61	4.38
29	0.61	4.32
31	0.55	4.65
32	0.59	4.81
33	0.64	4.93
37	0.56	4.73
41	0.68	4.26

TABLE II
RESULTS OF ATTACK TO FIELD EXTENSION AROUND M_{64}

Field extension	Success rate	Average time [s]
59	0.62	28.83
61	0.61	28.41
63	0.64	29.17
64	0.63	29.54
65	0.66	30.20
67	0.57	29.25
71	0.61	30.61

TABLE III
RESULTS OF ATTACK TO FIELD EXTENSION AROUND M_{128}

Field extension	Success rate	Average time [s]
109	0.59	152.04
113	0.65	145.59
127	0.55	169.13
128	0.68	166.51
129	0.55	165.55
131	0.59	150.45
137	0.59	157.05

B. Experimental conditions

The experiment was implemented with CPU: Intel® Core™ i5-3230M, 2.60GHz \times 4, Memory: 8GB, DDR3, 1600MHz, OS: Ubuntu 20.04.5 LTS, and Libraries: Python 3.8.10, SageMath version 9.0.

C. Results and discussion

The results of the experiment are presented and a discussion of the experimental results is provided. The results are shown in Table I, II, and III for M_{32} , M_{64} , and M_{128} , respectively. Fig. 1 compares the success rates. Fig. 2 compares processing times. The experimental results showed that the success rate of prime numbers for field extension tended to be lower than that of integers to the power of two for field extension, and that their strength as a cipher tended to be higher. The success rates for the prime numbers before and after the reference integers (32, 64 and 128) and the other integers are compared by Mann-Whitney's U-test ($p > 0.05$), resulting in $p = 9.06 \times 10^{-3}$, $r = 0.57$ to be significant differences. On the other hand, the analysis time tended to be longer for integers around the power of two, including integers to the power of two for field extension. For M_{32} , M_{64} , and M_{128} , respectively, $p = 2.21 \times 10^{-29}$, 4.08×10^{-5} , and 1.60×10^{-5} with the Shapiro-Wilk test ($p > 0.05$), and the Kruskal-Wallis test ($p > 0.05$, $n = 6$) with 5.32×10^{-25} , 2.55×10^{-7} , and 1.29×10^{-61} . Hence, between reference integers (32, 64 and 128) and the prime numbers before and after the reference integers are confirmed by the Steel-Dwass test ($p > 0.05$): $p_{31} = 0.90$, $p_{37} = 0.88$,

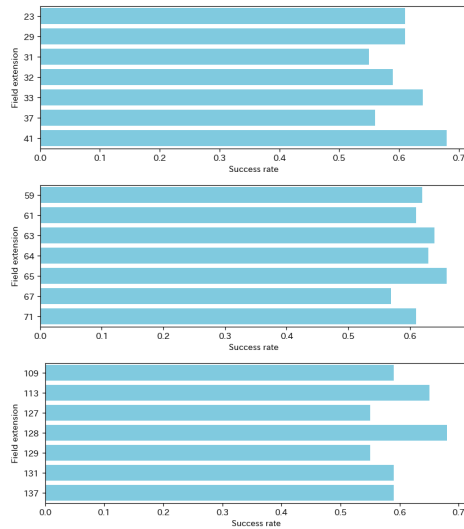


Fig. 1. Success rate to field extension around M_{32} , M_{64} and M_{128} .

$p_{61} = 0.51$, $p_{67} = 0.90$, $p_{127} = 0.49$, $p_{129} = 0.90$ to be no difference.

V. CONCLUSION

In this paper, we performed the lattice reduction algorithm as the RLWE problem with various integers to a field extension and performed a lattice attack by solving a unique SVP using Kannan’s embedding method. Results showed that the attack success rate was lower when prime numbers were used as the degree of field extension, and that the processing time tended to be longer for integers close to powers of two as the degree of field extension, suggesting that the lattice-based cryptography may be strengthened by employing Cullen or Mersenne prime numbers as the degree of field extension. Future work should include comparisons with attacks using other algorithms, such as the BKZ lattice reduction algorithm and machine learning-based algorithms.

ACKNOWLEDGMENT

I would like to thank my colleagues for their help in creating and discussing the experimental environment. This work was supported by JSPS KAKENHI Grant Number JP22K12293 and JP18K11572.

REFERENCES

- [1] R. Kannan, “Minkowski’s convex body theorem and integer programming,” *Math. Oper. Res.*, vol. 12, no. 3, pp. 415–440, aug 1987.
- [2] A. K. Lenstra, H. W. Lenstra, and L. Lovász László, “Factoring polynomials with rational coefficients,” *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, 12 1982, [published in Japanese].
- [3] L. Babai, “On lovász’ lattice reduction and the nearest lattice point problem,” in *STACS 85*, K. Mehlhorn, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 13–20.
- [4] V. Lyubashevsky, C. Peikert, and O. Regev, “On ideal lattices and learning with errors over rings,” in *Advances in Cryptology – EUROCRYPT 2010*, H. Gilbert, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 1–23.

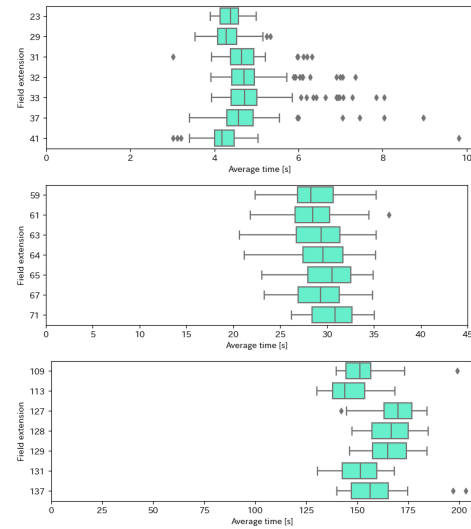


Fig. 2. Average time to field extension around M_{32} , M_{64} and M_{128} .

- [5] S. Uesugi, S. Okumura, and A. Miyaji, “Crypto analysis for ring-lwe problem on subfield in cyclotomic field,” in *IEICE Tech. Rep.*, ser. IT2021-106, ISEC2021-71, WBS2021-74, RCC2021-81, vol. 121, no. 429, Online, March 2022, pp. 138–144, thu, Mar 10, 2022 - Fri, Mar 11 : Online (IT, ISEC, RCC, WBS).
- [6] S. Uesugi, S. Okumura, and M. Atsuko, “Security analysis for ring-lwe problem the maximal real and complex subfields in cyclotomic field,” in *IEICE Tech. Rep.*, ser. IT2022-75, ISEC2022-54, WBS2022-72, RCC2022-72, vol. 122, no. 428, Yamaguchi, March 2023, pp. 49–53, tue, Mar 14, 2023 - Wed, Mar 15 : (RCC, ISEC, IT, WBS).
- [7] S. Terada, H. Nakano, S. Okumura, and A. Miyaji, “An experimental analysis on lattice attacks against ring-lwe over decomposition fields,” in *2018 International Symposium on Information Theory and Its Applications (ISITA)*, 2018, pp. 306–310.
- [8] S. ARITA and S. HANDA, “Fully homomorphic encryption scheme based on decomposition ring,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E103.A, no. 1, pp. 195–211, 2020.
- [9] E. Wenger, M. Chen, F. Charton, and K. Lauter, “Salsa: Attacking lattice cryptography with transformers,” in *Advances in Neural Information Processing Systems*, vol. 36, 2022.
- [10] G. Bonnoron and C. Fontaine, “A note on ring-lwe security in the case of fully homomorphic encryption,” in *Progress in Cryptology – INDOCRYPT 2017*, A. Patra and N. P. Smart, Eds. Cham: Springer International Publishing, 2017, pp. 27–43.
- [11] N. Gama and P. Q. Nguyen, “Predicting lattice reduction,” in *Advances in Cryptology – EUROCRYPT 2008*, N. Smart, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 31–51.
- [12] Z. Brakerski and V. Vaikuntanathan, “Fully homomorphic encryption from ring-lwe and security for key dependent messages,” in *Advances in Cryptology – CRYPTO 2011*, P. Rogaway, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 505–524.
- [13] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, “(leveled) fully homomorphic encryption without bootstrapping,” in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ser. ITCS’12. New York, NY, USA: Association for Computing Machinery, 2012, pp. 309–325. [Online]. Available: <https://doi.org/10.1145/2090236.2090262>
- [14] Y. Aono, X. Boyen, L. T. Phong, and L. Wang, “Key-private proxy re-encryption under lwe,” in *Progress in Cryptology – INDOCRYPT 2013*, G. Paul and S. Vaudenay, Eds. Cham: Springer International Publishing, 2013, pp. 1–18.
- [15] S. Arita. (2014) [introduction to ideal lattice cryptography] idearu koushi angou nyuumon (in japanese). [Comprehensive Science of Information Security] Jouhou Sekyuritei Sougou Kagaku (in Japanese). <https://www.iisec.ac.jp/proc/vol0006/arita14.pdf>, [published in Japanese].

©2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.