An Experimental Analysis on Lattice Attacks against Ring-LWE over Decomposition Fields

Shota Terada *, Hideto Nakano †, Shinya Okumura †, Atsuko Miyaji †
* Panasonic Corporation
†Graduate School of Engineering, Osaka University

***Abstract*—The ring variant of learning with errors (Ring-LWE) problem has provided efficient post-quantum cryptographic schemes including homomorphic encryption (HE) schemes. Usually, cyclotomic fields are used as underlying number fields of Ring-LWE from the viewpoints of efficiency and security. However, especially in the case of HE schemes, improving the efficiency and ensuring the security are important tasks even now. Arita and Handa proposed to use decomposition fields as underlying number fields of Ring-LWE and successfully constructed a HE scheme which can encrypt many plaintexts efficiently at a time. However, there is no enough evidence that decomposition fields do not provide weak Ring-LWE instances.**

In this paper, we give an experimental analysis on lattice attacks against Ring-LWE over decomposition fields. More precisely, we conducted lattice attacks against Ring-LWE over decomposition fields and over the ℓ-th cyclotomic fields with some prime numbers ℓ, respectively, and compared each of the running-time, the success rate and the root hermite factor. We also compared the results of the same attacks on various decomposition fields to find decomposition fields providing weak Ring-LWE instances. As a result of our analysis, we expect that decomposition fields would provide more secure and efficient HE schemes based on Ring-LWE compared to the ℓ-th cyclotomic fields.

I. Introduction

The ring variant of learning with errors (Ring-LWE)-based cryptography [15], [16] is one of the most attractive research area in cryptography. The Ring-LWE has provided efficient and provably secure post-quantum cryptographic protocols including homomorphic encryption (HE) schemes [4], [5], [9]. Both post-quantum cryptography and HE have been strongly desired to be developed their efficiency and security. In fact, the standardization of post-quantum cryptography is underway by National Institute of Standards and Technology, and HE schemes which enable us to execute the computation on encrypted data without decrypting has many applications in cloud computing area.

The Ring-LWE is characterized by two probabilistic distributions, modulus parameters and by number fields, see Section II-C for details. Usually, cyclotomic fields are used as underlying number fields from the viewpoints of efficiency and security [17]. However, especially in the case of HE schemes, improving the efficiency of homomorphic arithmetic operations on encrypted data and ensuring the security are important tasks even now.

Arita and Handa proposed to use a decomposition field as an underlying number field of Ring-LWE to construct a HE scheme which can encrypt many plaintexts efficiently at a time [1], see Section III for details of decomposition fields and of Arita et al.'s idea. Arita et al.'s HE scheme called subring HE scheme is indistinguishably secure under the chosen plaintext attack if the decision version of Ring-LWE over decomposition fields is computationally infeasible. Arita et al.'s experiments [1, Section 5] showed that the performance of subring HE scheme is much better than that of FV scheme based on Ring-LWE over the ℓ-th cyclotomic field with a prime number ℓ, implemented in HElib [11].

As for the security of subring HE scheme, Arita et al. remarked that in the case of decomposition fields, some propeties on the security of Ring-LWE are satisfied as well as in the case of cyclotomic fields shown in [15], [16]. However, solving Ring-LWE is reduced to solving a certain problem on lattices, and the difficulty of problems on lattices depends heavily on the structure and given bases of underlying lattices. This means that underlying number fields would affect the difficulty of lattice problems coming from Ring-LWE. Hence, to ensure the security of subring HE scheme, one should give experimental or theoretical analysis on attacks, while the paper [1] did not provide such an analysis.

In this paper, we give an experimental analysis on the security of Ring-LWE over decomposition fields. More precisely, we compare the security of Ring-LWE over decomposition fields and of Ring-LWE over the ℓ-th cyclotomic fields with some prime numbers ℓ. In our experiments, we reduce the search Ring-LWE to a problem of solving the (approximate) closest vector problem (CVP) on certain lattices in the same way as Bonnoron et al.'s analysis [3] because the target of their analysis is Ring-LWE optimized for HE. We use Babai's nearest plane algorithm [2] and Kannan's embedding technique [12] to solve CVP, respectively, see Section IV-A for details of the attacks. We compare each of the running-time, the success rate and the hermite root factor. (The root hermite factor [10] is usually used to evaluate the quality of lattice attacks, see Section II-A for its definition.) We also compare experimental results on lattice attacks against Ring-LWE over various decomposition fields to find decomposition fields providing weak Ring-LWE instances.

Our experimental results indicate that the success rates and the hermite root factors for decomposition fields are the almost same as those for cyclotomic fields. However, the running-times for decomposition fields is getting longer as the ranks of lattices occurring in the above attacks increase. Therefore we expect that decomposition fields provide secure Ring-LWE

against the above lattice attacks compared to cyclotomic fields because the ranks of lattices occurring in our experiments are very low compared to practically used lattices. This means that we can use Ring-LWE over decomposition fields with relatively small parameters compared to Ring-LWE over cyclotomic fields to construct HE schemes (or schemes of other types). Consequently, although we only dealt with low rank lattices, we expect that Ring-LWE over decomposition fields would provide more efficient HE schemes.

II. Preliminaries

In this section, we briefly review notions of lattices, number fields and Ring-LWE. Throughout this paper, let $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{C}$ be the ring of (rational) integers, the field of rational numbers and the field of complex numbers, respectively. For a positive integer m, suppose that any element of $\mathbb{Z}/m\mathbb{Z}$ is represented by an integer contained in $(-m/2, m/2] \cap \mathbb{Z}$.

A. Lattices

An m-dimensional lattice is defined as a discrete additive subgroup of $\mathbb{R}^m$. It is well-known that for any lattice $\mathcal{L} \subset \mathbb{R}^m$, there are $\mathbb{R}$-linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ such that $\mathcal{L} = \sum_{1 \le i \le n} \mathbb{Z}\mathbf{b}_i := \{\sum_{1 \le i \le n} a_i \mathbf{b}_i \mid a_i \in \mathbb{Z}\}$. In other words, for a matrix $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ whose i-th column vector is $\mathbf{b}_j$, we have $\mathcal{L} = \{\mathbf{Bx} \mid \mathbf{x} \in \mathbb{Z}^n\}$. Then, we say that $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ and $\mathbf{B}$ are a lattice basis of $\mathcal{L}$ and the basis matrix of $\mathcal{L}$ with respect to $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$, respectively. The value n is called the rank of $\mathcal{L}$, and it is denoted by $\mathrm{rank}(\mathcal{L})$. An important invariant of $\mathcal{L}$ is the determinant defined as $\det(\mathcal{L}) := \sqrt{\det(\mathbf{B}\mathbf{B}^t)}$. The determinant is independent of any choice of bases.

There are various computationally hard problems on lattices. Here, we explain the closest vector problem (CVP) which is a well-known and basic problem on lattices. Given a lattice $\mathcal{L}$ and a target vector $\mathbf{t} \in \mathbb{R}^m \setminus \mathcal{L}$, CVP on $(\mathcal{L}, \mathbf{t})$ is a problem of finding a vector $\mathbf{x} \in \mathcal{L}$ such that for all vectors $\mathbf{y} \in \mathcal{L}$ we have $\|\mathbf{t} - \mathbf{x}\| \le \|\mathbf{t} - \mathbf{y}\|$. For a real number $\gamma > 1$, the approximate CVP on $(\mathcal{L}, \mathbf{t}, \gamma)$ is a problem of finding a vector $\mathbf{x} \in \mathcal{L}$ such that for all vectors $\mathbf{y} \in \mathcal{L}$, we have $\|\mathbf{t} - \mathbf{x}\| \le \gamma \|\mathbf{t} - \mathbf{y}\|$. Babai's nearest plane algorithm and Kannan's embedding technique are basic algorithms for solving the approximate CVP. Almost all known problems on lattices, which are useful for constructing cryptographic protocols, are getting more difficult as ranks of underlying lattices increase, and the quality of two algorithms mentioned earlier depends on ranks of input lattices.

Breaking some cryptographic protocols are reduced to solving certain computational problems on lattices, including the (approximate) CVP [3], [8]. To solve such problems on lattices, we usually use lattice basis reduction algorithms which transform a given basis of a lattice into a basis of the same lattice, which consists of nearly orthogonal and relatively short vectors. In fact, an input of Babai's nearest plane algorithm is a (LLL) reduced basis, and Kannan's embedding technique outputs an appropriate vector among a reduced basis. In our experiments, to solve CVP by Babai's nearest plane algorithm and by Kannan's embedding technique, we use the LLL algorithm [13] and the BKZ algorithm [7], [18] which are well-known algorithms for computing reduced bases. The quality of basis reduction algorithms is usually estimated by the root hermite factor defined as follows: Let $\mathbf{b}$ be a shortest vector among a basis of a lattice $\mathcal{L}$ with $\mathrm{rank}(\mathcal{L}) = n$, which is reduced by a basis reduction algorithm $\mathcal{A}$, and then the root hermite factor $\delta_{\mathcal{A},\mathcal{L}}$ is defined as a constant satisfying $\delta_{\mathcal{A},\mathcal{L}}^n := \|\mathbf{b}\| / \det(\mathcal{L})^{1/n}$. Better basis reduction algorithms provide smaller hermite root factors.

B. Number Fields

To describe Ring-LWE and decomposition fields, which play central roles in this paper, we need some notions from algebraic number theory.

An (algebraic) number field is a finite extension field of $\mathbb{Q}$. Let K be a number field with extension degree $[K : \mathbb{Q}] = n$. An element $a \in K$ is called an algebraic integer if there exists a monic polynomial $f \in \mathbb{Z}[x]$ satisfying $f(a) = 0$. The ring of integers O_K of K is defined as a subring of K consisting of all algebraic integers of K. The ring O_K has an integral basis ($\mathbb{Z}$-basis) $\{u_1, \ldots, u_n\}$, i.e., for any element $u \in O_K$, there exist integers $a_1, \ldots, a_n$ such that u is uniquely written as $u = \sum_{1 \le i \le n} a_i u_i$. It is well-known that any (integral) ideal I of O_K is uniquely factored into the product of some prime ideals, i.e., there exist prime ideals $\mathcal{P}_1, \ldots, \mathcal{P}_m$ satisfying $I = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_m^{e_m}$ for $e_i \ge 1$. If $I = pO_K$ for a prime number p and K is a Galois extension of $\mathbb{Q}$, then we have $O_K/\mathcal{P}_i \cong \mathbb{F}_{p^d}$ for some $d \in \mathbb{N}$ and all e_i's are mutually equal. Moreover, we have $med = n$, where $e := e_i$, and if all e_i's are equal to 1 (resp. all e_i's and d are equal to 1), then we say that p is unramified (resp. splits completely) in K. Any prime ideal of O_K is a maximal ideal in O_K, and thus we have $P_i + P_j = O_K$ for any $i \ne j$. This induces an isomorphism of rings $O_K/\mathcal{P}_1 \cdots \mathcal{P}_m \cong O_K/\mathcal{P}_1 \times \cdots \times O_K/\mathcal{P}_m$.

C. Ring-LWE Problem

Let K and O_K be as above. Let χ_{secret} and χ_{error} be probabilistic distributions on O_K, and p an integer. We denote by $O_{K,p}$ the residue ring O_K/pO_K. For a probabilistic distribution χ on a set X, we write $a \leftarrow \chi$ when $a \in X$ is chosen according to χ. We denote by $U(X)$ the uniform distribution on X. The Ring-LWE distribution on $O_{K,p} \times O_{K,p}$, denoted by $\mathrm{RLWE}_{K,p,\chi_{\mathrm{error}},\chi_{\mathrm{sec}}}$, is defined as a probabilistic distribution that takes elements of a form $(a, as+e)$ with $a \leftarrow U(O_{K,p})$, $s \leftarrow \chi_{\mathrm{secret}}$ and with $e \leftarrow \chi_{\mathrm{error}}$. The Ring-LWE problem has two variants. One is a problem of distinguishing $\mathrm{RLWE}_{K,p,\chi_{\mathrm{error}},\chi_{\mathrm{sec}}}$ from $U(O_{K,p} \times O_{K,p})$, which is called the decision Ring-LWE problem. The other is a problem that given arbitrary many samples $(a_i, a_i s + e_i) \in O_{K,p} \times O_{K,p}$ chosen according to $\mathrm{RLWE}_{K,p,\chi_{\mathrm{error}},\chi_{\mathrm{sec}}}$, find $s \in O_{K,p}$, which is called the search Ring-LWE problem.

The Ring-LWE problem has been expected to be computationally difficult even with quantum computers. It was proved that the decision Ring-LWE is equivalent to the search one if K is a cyclotomic field, and if p is a prime number

and (almost) splits completely in K [16]. In addition, this equivalence is generalized to the cases where $K/\mathbb{Q}$ is a Galois extension, and where p is unramified in K [6]. Moreover, there is a quantum polynomial-time reduction from the search Ring-LWE to the shortest vector problem on certain ideal lattices.

III. Arita et al.'s Idea

In this section, we describe the advantage of using decomposition fields as underlying number fields of Ring-LWE to construct efficient HE schemes.

A. Cyclotomic Fields and Decomposition Fields

First, we briefly review cyclotomic fields. For a positive integer m, let $\zeta_m \in \mathbb{C}$ be a primitive m-th root of unity and $n = \varphi(m)$, where $\varphi(\cdot)$ denotes Euler's totient function. Then $K := \mathbb{Q}(\zeta_m)$ is called the m-th cyclotomic field. The ring of integers of K coincides with $R := \mathbb{Z}[\zeta_m]$. Any prime number p that does not divide m is unramified in K, and if $p \equiv 1 \pmod{m}$, then p splits completely in K. The $K/\mathbb{Q}$ is a Galois extension of degree $[K : \mathbb{Q}] = n$, and its Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$.

Next, we describe decomposition fields of number fields. Let L be a number field, and suppose that $L/\mathbb{Q}$ is a Galois extension, and that its Galois group $G := \mathrm{Gal}(L/\mathbb{Q})$ is a cyclic group. Let p be a prime number which is unramified in L and satisfies $pO_L = \mathcal{P}_1 \cdots \mathcal{P}_g$, where $\mathcal{P}_i$'s are prime ideals of O_L. Let G_Z be a subgroup of G, which consists of all elements ρ fixing all $\mathcal{P}_i$, i.e., $\rho(\mathcal{P}_i) = \mathcal{P}_i$ for $1 \le i \le g$, and Z the fixed field of G_Z. Then we call Z the decomposition field with respect to p. The field Z is a number field and its ring of integers of Z is $O_Z = O_L \cap Z$. Suppose $\mathrm{p}_i := O_Z \cap \mathcal{P}_i$. Then we have $pO_Z = \mathrm{p}_1 \cdots \mathrm{p}_g$. A generator σ of G_Z acts on $O_L/\mathcal{P}_i \cong \mathbb{F}_{p^d}$ as p-th Frobenius map, i.e., $\sigma(x) \equiv x^p \pmod{\mathcal{P}_i}$ for all $x \in O_L$ and for $1 \le i \le g$. Therefore we have $O_Z/\mathrm{p}_i \cong \mathbb{F}_p$ and $[Z : \mathbb{Q}] = g$, i.e., p splits completely in Z.

B. Cyclotomic Fields v.s. Decomposition Fields

Let K, L and Z be as above and p a prime number which is unramified in K and splits completely in Z. Assume that L is the ℓ-th cyclotomic field with a prime number ℓ. As we mentioned in Section I, cyclotomic fields are usually used as underlying number fields of Ring-LWE. From the viewpoint of the efficiency of Ring-LWE based-schemes, there are good $\mathbb{Z}$-bases of the rings of integers of K and Z [1], [17]. As for the security of the Ring-LWE, in the cases of K and Z, both the equivalence and the reduction mentioned in Section II-C are satisfied since both $K/\mathbb{Q}$ and $Z/\mathbb{Q}$ are Galois extensions.

The main difference between K and Z is algebraic structures of their rings of integers modulo p. Since p is unramified in K, we have $O_{K,p} \cong O_K/\mathcal{P}_1 \times \cdots \times O_K/\mathcal{P}_k$ and $O_K/\mathcal{P}_i \cong \mathbb{F}_{p^d}$ for $1 \le i \le k$ and for $d \ge 1$, where $\mathcal{P}_i$'s are prime ideals in O_K lying over p, i.e., $pO_K = \mathcal{P}_1 \cdots \mathcal{P}_k$. FV scheme [9], which is a HE scheme based on Ring-LWE, uses $O_{K,p}$ as its plaintext slots, and thus FV scheme (or any HE scheme with same plaintext slots) can encrypt and execute some additions of $dk = n = [K : \mathbb{Q}]$ plaintexts in $\mathbb{F}_p$ at a time. However, FV scheme cannot execute a multiplication of the same number of plaintexts in $\mathbb{F}_p$ at a time. To execute a multiplication of plaintexts in $\mathbb{F}_p$, we can only use $\mathbb{F}_p \times \cdots \times \mathbb{F}_p$ (product of k finite fields) as the plaintext slots.

On the other hand, since p splits completely in Z, we have $O_{Z,p} \cong O_Z/\mathrm{p}_1 \times \cdots \times O_Z/\mathrm{p}_g$ and $O_Z/\mathrm{p}_i \cong \mathbb{F}_p$ for any $1 \le i \le g$, where p_i's are prime ideals in O_Z lying over p. This means that one can encrypt $g = [Z : \mathbb{Q}]$ plaintexts at a time. Moreover, one can execute additions and multiplications of the same number of plaintexts in $\mathbb{F}_p$ at a time. Because the extension degrees g and n are directory related to ranks of lattices occurring in known lattice attacks, we should set $g \approx n$ to compare the security of Ring-LWE over these fields. Therefore, HE scheme over Z can encrypt and operate d times as many plaintexts as FV scheme over K at a time.

Remark 1:

1) If $p \equiv 1 \pmod{m}$, then p splits completely in K (recall that K is the m-th cyclotomic field), and then there is no advantage of using decomposition fields. However, for some cryptographic applications, we want to use a small p, e.g., $p = 2$ [1]. Moreover, to avoid lattice attacks, the extension degree $[K : \mathbb{Q}]$ must be large as we discussed above. Thus we cannot expect $p \equiv 1 \pmod{m}$ for practical parameters in some application.
2) By Hensel lifting technique, for $r > 1$ and $q := p^r$, we have $O_{Z,q} \cong \mathbb{Z}/q\mathbb{Z} \times \cdots \times \mathbb{Z}/q\mathbb{Z}$.

IV. Experimental Analysis

In this section, we show our experimental results on lattice attacks against Ring-LWE over decomposition fields and over cyclotomic fields, respectively. First, we explain lattice attacks in our experiments.

A. Lattice Attacks in Our Experiments

In our experiments, we reduce the search Ring-LWE to CVP (or approximate CVP) in the same way as Bonnoron et al.'s analysis [3] because the target of Bonnoron et al.'s analysis is Ring-LWE optimized for HE. We describe it briefly in the case of decomposition fields. Let O_Z and p be as in Section III-A. Set $q := p^r$ for $r > 1$. Let $\{\mu_1, \ldots, \mu_g\}$ be a $\mathbb{Z}$-basis of O_Z, which is a good basis shown in [1, Lemma 3]. Sample vectors $\mathbf{a} = (a_1, \ldots, a_g)$, $\mathbf{s} = (s_1, \ldots, s_g)$ and $\mathbf{e} = (e_1, \ldots, e_g)$ from $U(\mathbb{Z}^g)$, $D_{\mathbb{Z}^g,\sigma_\mathrm{s}}$ and $D_{\mathbb{Z}^g,\sigma_\mathrm{e}}$, respectively, where $D_{\mathbb{Z}^g,\sigma}$ denotes the discrete Gaussian distribution with mean 0 and with variance σ^2.

Put $a := \sum_{1\le i\le g} a_i\mu_i$, $s := \sum_{1\le i\le g} s_i\mu_i$, $e := \sum_{1\le i\le g} e_i\mu_i$ and $b := as + e = \sum_{1\le i\le g} b_i\mu_i \pmod{q}$. Then (a, b) is a Ring-LWE instance over Z. Note that in order to use Ring-LWE to construct HE schemes, the value σ_s should be sufficiently small as well as σ_e because ℓ_∞-norm $\|\mathbf{s}\|_\infty$ directory affects the growth of noises after multiplication. In our experiments, we set $\sigma_\mathrm{s} = 1$ and $\sigma_\mathrm{e} = 8$ according to [14]. By comparing all coefficients of both sides, we have $\mathbf{As} + \mathbf{e} = (b_1, \ldots, b_g)^t = \mathbf{b} \pmod{q}$, where $\mathbf{A}$ is a matrix. (For any vector $\mathbf{v}$, $\mathbf{v}^t$ means its transpose.) If we set $\mathbf{A}'$ as $(\mathbf{A} \;\; \mathbf{I})$, then we have $\mathbf{A}'(\mathbf{s} \;\; \mathbf{e})^t = \mathbf{b} \pmod{q}$, where $\mathbf{I}$ denotes

TABLE I
EXPERIMENTAL RESULTS ON BABAI'S NEAREST PLANE ALGORITHM FOR $p = 2$.

ℓ	59	16183	73	2089	83	4051	131	5419	173	14449	227	9719
g	-	58	-	72	-	81	-	129	-	172	-	226
Rank of lattice	118	116	146	144	166	162	262	258	346	344	454	452
r'	20	20	20	20	20	20	30	30	30	30	30	30
Number of samples	93	100	100	100	100	100	100	100	40	37	15	14
Success rate [%]	100	100	100	100	100	100	100	100	100	89	0	0
Average of root hermite factor	1.014	1.014	1.014	1.014	1.014	1.014	1.020	1.020	1.020	1.020	1.021	1.021
Average of running-time [sec]	72.22	88.97	218.4	238.2	443.3	456.1	12790.5	11744.6	54763.0	57862.3	231816.1	237846.9
Ratio of running-time [%]	-	123.2	-	109.0	-	102.9	-	91.8	-	105.7	-	102.6

The columns which the values g are indicated show the results for decomposition fields, and other columns show the results for cyclotomic fields. The "Ratio of running-time" means the ratio "average of running-times for a decomposition field/average of running-times for a cyclotomic field" for each g.

TABLE II
EXPERIMENTAL RESULTS ON KANNAN'S EMBEDDING TECHNIQUE FOR $p = 2$.

ℓ	59	161831	73	2089	83	4051	131	5419	173	14449	227	9719
g	-	58	-	72	-	81	-	129	-	172	-	226
Rank of lattice	119	117	147	145	167	163	263	259	347	345	455	453
r'	20	20	20	20	20	20	30	30	30	30	40	40
Number of samples	100	100	100	100	100	100	100	100	100	100	23	21
Success rate [%]	100	100	100	100	100	100	100	100	100	100	100	100
Average of running-time [sec]	10.4	10.7	36.7	41.4	92.3	97.6	4714.6	5556.7	19387.5	25138.7	136978.2	159772.6
Ratio of running-time [%]	-	103.5	-	112.7	-	105.7	-	117.9	-	129.7	-	116.6

We computed the root hermite factor for reduced bases, but we omitted to show them because the results of the success rate below are 100.

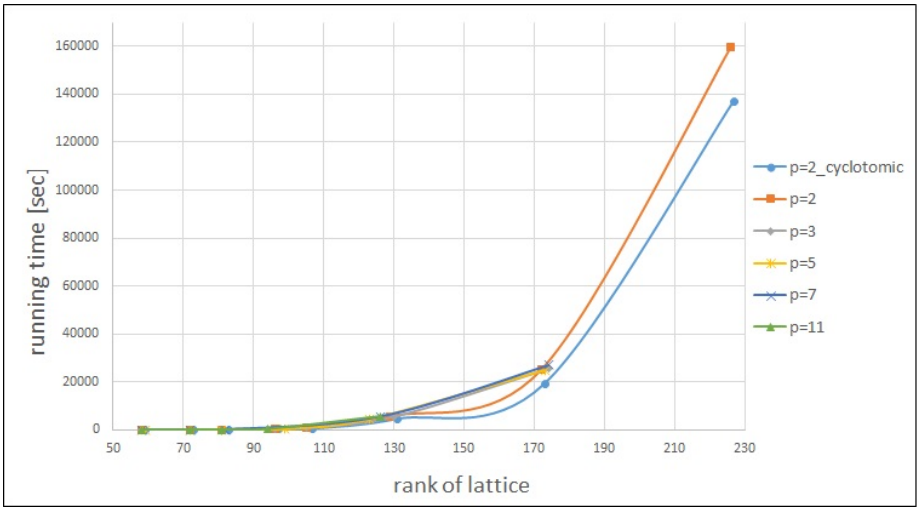

Fig. 1. The average of running-times of Kannan's embedding technique for cyclotomic fields and for decomposition fields with respect to $p = 2, 3, 5, 7, 11$. The "p = 2_cyclotomic" means the results of cyclotomic fields shown in Table II, and others mean the results of decomposition fields with respect to corresponding prime numbers p. We set modulus parameters $q = p^{r'}$ so that these moduluses have the almost same bit sizes. We only show the average results on at least 10 samples.

the $g \times g$ identity matrix. From the choice of s_i's and of e_i's, our target vector $(\mathbf{s} \quad \mathbf{e})^t$ is a very short vector among all solutions to $A'\mathbf{y} = \mathbf{b}$ (mod. q), and thus we can expect that our target vector can be found by solving (approximate) CVP on the lattice $\mathcal{L} = \{\mathbf{x} \in \mathbb{Z}^{2g} \mid \mathbf{A}'\mathbf{x} = \mathbf{0} \text{ (mod. } q)\}$ and on $\mathbf{w} := (\mathbf{0} \quad \mathbf{b})^t$ which is a solution to $\mathbf{A}'\mathbf{y} = \mathbf{b}$ (mod. q).

We take

$$\mathbf{B} = \begin{pmatrix} \mathbf{I} & \mathbf{0}_{g,g} \\ -\mathbf{A} & q\mathbf{I} \end{pmatrix}$$

as a basis matrix of $\mathcal{L}$, where $\mathbf{0}_{g,g}$ denotes the $g \times g$ zero matrix. We reduce the basis matrix $\mathbf{B}$ by the LLL algorithm and the BKZ algorithm with block size $\beta = 10$. (In practice, the β should be 10 or 20.) Let $\mathbf{B}_{\mathrm{red}}$ be a reduced basis of $\mathbf{B}$. We input $\mathbf{B}_{\mathrm{red}}$ and $\mathbf{w}$ to Babai's nearest plane algorithm. The quality of Babai's nearest plane algorithm depends on the quality of basis reduction algorithms used to compute input reduced bases, and thus we compute the root hermite factor for $\mathbf{B}_{\mathrm{red}}$.

On the other hand, Kannan's embedding technique takes a basis matrix

$$\mathbf{C} = \begin{pmatrix} \mathbf{B} & -\mathbf{w} \\ \mathbf{0}_{1\times 2g} & M \end{pmatrix}$$

as an input, and we set $M = 1$ according to a result of an experimental study on Kannan's embedding technique for LWE [19]. We also use the LLL algorithm and the BKZ algorithm with $\beta = 10$ to reduce the above basis matrix.

Remark 2: In the case of the ℓ-cyclotomic fields with prime numbers ℓ, we use $\{1, \zeta_\ell, \ldots, \zeta_\ell^{\ell-2}\}$ as a $\mathbb{Z}$-basis, which is

also a good basis [17].

Remark 3: For $1 \leq r' < r$ and $q' := p^{r'}$, we can obtain samples of $\mathrm{RLWE}_{K,q',\chi_{\mathrm{error}},\chi_{\mathrm{sec}}}$ from samples of $\mathrm{RLWE}_{K,q,\chi_{\mathrm{error}},\chi_{\mathrm{sec}}}$ by a natural projection $O_{Z,q} \to O_{Z,q'}$ via $a \mapsto a \pmod{q'}$. In our experiments, we use small r' to reduce running-times and only show r' in experimental results.

B. Experimental Results

We used a computer with 2.00GHz CPUs (Intel(R)Xeon(R) CPU E7-4830 v4 (2.00GHz) × 111) and 3TB memory. The OS is Ubuntu 16.04.4. We implemented a code for sampling Ring-LWE instances in SageMath version 7.5.1. We also used Magma V2.23-1 to execute lattice attacks. We sampled 100 samples and conducted lattice attacks for them.

We show our experimental results in Tables I and II for $p = 2$. Table I shows that there is no large difference between experimental results of cyclotomic fields and of decomposition fields. On the other hand, Table II shows that Kannan's embedding technique is much faster than Babai's nearest plane algorithm. This implies that the behaviors of basis reduction algorithms depend heavily on the structure of input lattices. This is a reason why experimental analyses are necessary for ensuring the security of lattice (or other problems) based schemes. Table II also shows that the running-times for decomposition fields are getting longer than those for cyclotomic fields as g (or $\ell - 1$) increases. Therefore we can expect that decomposition fields would provide more secure Ring-LWE against the lattice attacks described in Section IV-A compared to ℓ-th cyclotomic fields because the ranks of lattices occurring in our experiments are very low compared to practically used lattices. This means that we can use decomposition fields of relatively low extension degrees compared to the ℓ-th cyclotomic fields, and the use of such number fields makes Ring-LWE-based schemes efficient. Consequently, although we only dealt with low rank lattices, we expect that Ring-LWE over decomposition fields would provide more efficient HE schemes.

We also conducted experiments for decomposition fields with respect to $p = 3, 5, 7, 11$ to find decomposition fields providing weak Ring-LWE instances, and Fig. 1 shows the experimental results. In this experiments, we cannot find decomposition fields providing weak Ring-LWE instances.

V. Conclusion

In this paper, we gave an experimental analysis on the security against lattice attacks of Ring-LWE over decomposition fields which can provide more efficient homomorphic encryption (HE) schemes. We compared the security against lattice attacks of Ring-LWE over decomposition fields with that of Ring-LWE over the ℓ-cyclotomic fields with some prime numbers ℓ, which are usually used as underlying number fields of Ring-LWE. Although we only conducted experiments for low rank lattices, we expect that decomposition fields would provide more efficient and secure HE schemes compared to cyclotomic fields. We believe that our work will provide an opportunity for investigating new number fields that provide better cryptographic schemes based Ring-LWE compared to cyclotomic fields.

Acknowledgment

This work is partially supported by JSPS KAKENHI Grant(B) (JP17K18450), Grant (C)(JP15K00183), Microsoft Research Asia, CREST(JPMJCR1404) at Japan Science and Technology Agency, the Japan-Taiwan Collaborative Research Program at Japan Science and Technology Agency, and Project for Establishing a Nationwide Practical Education Network for IT Human Resources Development, Education Network for Practical Information Technologies. This work was conducted while Shota Terada was a student at Osaka University.

References

[1] S. Arita, S. Handa, "Subring Homomorphic Encryption", In: Proc. of ICISC 2017, LNCS, vol. 10779, pp. 112–136, Springer, Cham, (2018).
[2] L. Babai, "On Lovász' Lattice Reduction and the nearest lattice point problem," Combinatorica, vol. 6 (1), pp. 1–13, Springer-Verlag, (1986). (Preliminary version in STACS 1985)
[3] G. Bonnoron, C. Fontaine, "A Note on Ring-LWE Security in the Case of Fully Homomorphic Encryption", In: Proc. of INDOCRYPT 2017, LNCS, vol. 10698, pp. 27–43, Springer, Cham, (2017).
[4] Z. Brakerski, C. Gentry, V. Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption without Bootstrapping", In: Proc. of ITCS 2012, pp. 309–325, ACM New York, NY, USA, (2012).
[5] Z. Brakerski and V. Vaikuntanathan, "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages", In: Proc. of CRYPTO 2011, LNCS vol. 6841, pp. 505–524, Springer, Berlin, Heidelberg, (2011).
[6] H.Chen, K. Lauter, K. E. Stange, "Security considerations for Galois non-dual RLWE families", In: Proc. of SAC 2016, LNCS, vol 10532, pp. 443–462, Springer, Cham, (2016).
[7] Y. Chen, P. Q. Nguyen, "BKZ 2.0: Better Lattice Security Estimates", In: Proc. of ASIACRYPT 2011, LNCS, vol. 7073, pp. 1–20, Springer, Berlin, Heidelberg, (2011).
[8] D. Coppersmith, "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities", Journal of Cryptology, 10 (4), pp. 233260, Springer-Verlag, (1997).
[9] J. Fan, F. Vercauteren, "Somewhat Practical Fully Homomorphic Encryption", Cryptology ePrint Archive, Report 2012/144, (2012).
[10] N. Gama, P. Q. Nguyen, "Predicting Lattice Reduction", In: Proc. of EUROCRYPT 2008, LNCS, vol. 4965, pp. 31–51, Springer, Berlin, Heidelberg, (2008).
[11] S. Halevi, V. Shoup, "Algorithms in HElib", In: Proc. of CRYPTO 2014, LNCS, vol. 8616, pp. 554–571, Springer, Berlin, Heidelberg, (2014).
[12] R. Kannan, "Minkowski's Convex Body Theorem and Integer Programming", Mathematics of Operations Research, vol. 12 (3), pp. 415–440, INFORMS, Linthicum, Maryland, USA, (1987).
[13] A. K. Lenstra, H. W. Lenstra Jr., L. Lovász, "Factoring polynomials with rational coefficients", Mathematische Annalen, vol. 261 (4), pp. 515–534, Springer-Verlag, (1982).
[14] T. Lepoint, M. Naehrig, "A Comparison of the Homomorphic Encryption Schemes FV and YASHE", In: Proc. of AFRICACRYPT 2014, LNCS, vol 8469, pp. 318–335, Springer, Cham, (2014).
[15] V. Lyubashevsky, C. Peikert, O. Regev, "On Ideal Lattices and Learning with Errors over Rings", In: Proc. of EUROCRYPT 2010, LNCS, vol. 6110, pp. 1–23, Springer, Berlin, Heidelberg, (2010).
[16] V. Lyubashevsky, C. Peikert, O. Regev, "On Ideal Lattices and Learning with Errors over Rings", Journal of the ACM (JACM), vol. 60 (6), pp. 43:1–43:35, ACM New York, NY, USA, (2013).
[17] V. Lyubashevsky, C. Peikert, O. Regev, "A Toolkit for Ring-LWE Cryptography", In: Proc. of EUROCRYPT 2013, LNCS, vol. 7881, pp. 35–54, Springer, Berlin, Heidelberg, (2013).
[18] C. P. Schnorr, M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems", Mathematical Programing vol. 66 (1-3), 181–199, Springer-Verlag, (1994).
[19] Y. Wang, Y. Aono, T. Takagi, "An Experimental Study of Kannan's Embedding Technique for the Search LWE Problem", accepted to ICICS 2017, (2017).