Chapter 2
Cryptography Core Technology

Chen-Mou Cheng, Kenta Kodera, Atsuko Miyaji, and Shinya Okumura

Abstract In this chapter, we describe the analysis of security basis. One is the analysis of elliptic curve discrete logarithm problem (ECDLP). ECDLP is one of the public-key cryptosystems that can achieve a short key size but it is not a post-quantum cryptosystem. Another is analysis to learning with error (LWE), which is a post-quantum cryptosystem and has the functionality of *homomorphic encryption*. These two security bases have important roles in each protocol described in Sect. 2.2.4.2

2.1 Analysis on ECDLP

2.1.1 Introduction

In recent years, elliptic curve cryptography is gaining momentum in deployment because it can achieve the same level of security as RSA using much shorter keys and ciphertexts. The security of elliptic curve cryptography is closely related to the computational complexity of the elliptic curve discrete logarithm problem (ECDLP). Let p be a prime number and E, a nonsingular elliptic curve over $\mathbb{F}_{p^n}$, which is a finite field of p^n elements. That is, E is a plane algebraic curve defined by the equation $y^2 = x^3 + ax + b$ for $a, b \in \mathbb{F}_{p^n}$ such that $\Delta = -16(4a^3 + 27b^2) \neq 0$. Along with a point O at infinity, the set of rational points $E(\mathbb{F}_{p^n})$ forms an abelian group with O as the identity. Given $P \in E(\mathbb{F}_{p^n})$ and Q in the subgroup generated by P, ECDLP is the problem of finding an integer α such that $Q = \alpha P$.

C.-M. Cheng · K. Kodera · A. Miyaji (✉) · S. Okumura
Osaka University, Suita, Japan
e-mail: miyaji@comm.eng.osaka-u.ac.jp

C.-M. Cheng
e-mail: ccheng@cy2sec.comm.eng.osaka-u.ac.jp

K. Kodera
e-mail: kodera@cy2sec.comm.eng.osaka-u.ac.jp

S. Okumura
e-mail: okumura@comm.eng.osaka-u.ac.jp

A. Miyaji and T. Mimoto (eds.), *Security Infrastructure Technology for Integrated Utilization of Big Data*,
https://doi.org/10.1007/978-981-15-3654-0_2

Today, the best practical attacks against ECDLP are exponential-time, generic discrete logarithm algorithms such as Pollard's rho method [34]. However, recently, a line of research has been dedicated to the index calculus for ECDLP which was started by Semaev, Gaudry, and Diem [25, 30, 35]. Under certain heuristic assumptions, such algorithms could lead to subexponential attacks to ECDLP in some cases [27, 31, 33]. The interested reader is referred to a survey paper by Galbraith and Gaudry for a more comprehensive and in-depth account of the recent development of ECDLP algorithms along various directions [28].

In this section, we investigate the computational complexity of ECDLP for elliptic curves in various forms—including Hessian [36], Montgomery [32], (twisted) Edwards [23, 24], and Weierstrass, using index calculus. Recently, elliptic curves of various forms such as Curve25519 [22] have been drawing considerable attention in deployment partly because some of them allow fast implementation and security against timing-based side-channel attacks. Furthermore, we can construct these curves not only over prime fields (such as the field of $2^{255} - 19$ elements as used in Curve25519) but also over extension fields. In this section, we will focus on curves over optimal extension fields (OEFs) [21]. An OEF is an extension field from a prime field $\mathbb{F}_p$ with p close to 2^8, 2^{16}, 2^{32}, 2^{64}, etc. Such primes fit nicely into the processor words of 8-, 16-, 32-, or 64-bit microprocessors and hence are particularly suitable for software implementation, allowing efficient utilization of fast integer arithmetic on modern microprocessors [21]. As we will see, our experimental results show considerably significant differences in the computational complexity of ECDLP for elliptic curves in various forms over OEFs.

2.1.2 *Previous Works*

2.1.2.1 Index Calculus for ECDLP

Let E be an elliptic curve defined over a finite field $\mathbb{F}_{p^n}$. For cryptographic applications, we are mostly interested in a prime-order subgroup generated by a rational point $P \in E(\mathbb{F}_{p^n})$. Here, we first give a high-level overview of a typical index-calculus algorithm for finding an integer α such that $Q = \alpha P$ for $Q \in \langle P \rangle$.

1. Determine a *factor base* $\mathcal{F} \subset E(\mathbb{F}_{p^n})$.
2. Collect a set $\mathcal{R}$ of *relations* by decomposing random points $a_i P + b_i Q$ into a sum of points from $\mathcal{F}$, i.e.,

$$\mathcal{R} = \left\{ a_i P + b_i Q = \sum_j P_{i,j} \,:\, P_{i,j} \in \mathcal{F} \right\}.$$

3. When $|\mathcal{R}| \approx |\mathcal{F}|$, eliminate the right-hand side using linear algebra to obtain an equation of the form $aP + bQ = \mathcal{O}$ and $\alpha = -a/b \bmod \operatorname{ord} P$.

The last step of linear algebra is relatively well studied in the literature, so we will focus on the subproblem in the second step, namely, the point decomposition problem (PDP) on an elliptic curve in the rest of this section.

Definition 2.1 (*Point Decomposition Problem of mth Order*) Given a rational point $R \in E(\mathbb{F}_{p^n})$ on an elliptic curve E and a factor base $\mathcal{F} \subset E(\mathbb{F}_{p^n})$, find, if they exist, $P_1, \ldots, P_m \in \mathcal{F}$ such that

$$R = P_1 + \cdots + P_m.$$

2.1.2.2 Semaev's Summation Polynomials

We can solve PDP by considering when the sum of a set of points becomes zero on an elliptic curve. It is straightforward that if two points sum to zero on an elliptic curve $E : y^2 = x^3 + ax + b$ in Weierstrass form, then their x-coordinates must be equal. Let us now consider the simplest yet nontrivial case where three points on E sum to zero. Let

$$Z = \left\{ \begin{array}{r} (x_1, y_1, x_2, y_2, x_3, y_3) \in \mathbb{F}_{p^n}^6 : (x_i, y_i) \in E(\mathbb{F}_{p^n}), i = 1, 2, 3; \\ (x_1, y_1) + (x_2, y_2) + (x_3, y_3) = O \end{array} \right\}.$$

Clearly, Z is in the variety of the ideal $I \subset \mathbb{F}_{p^n}[X_1, Y_1, X_2, Y_2, X_3, Y_3]$ generated by

$$\left\{ \begin{array}{l} Y_i^2 - (X_i^3 + aX_i + b), i = 1, 2, 3; \\ (X_3 - X_1)(Y_2 - Y_1) - (X_2 - X_1)(Y_3 - Y_1) \end{array} \right\}.$$

Now let $J = I \cap \mathbb{F}_{p^n}[X_1, X_2, X_3]$. Using MAGMA's `EliminationIdeal` function, we find that J is actually a principal ideal generated by the polynomial $(X_2 - X_3)(X_1 - X_3)(X_1 - X_2) f_3$, where

$$\begin{aligned} f_3 =& X_1^2X_2^2 - 2X_1^2X_2X_3 + X_1^2X_3^2 - 2X_1X_2^2X_3 - 2X_1X_2X_3^2 - 2aX_1X_2 - 2aX_1X_3 \\ & - 4bX_1 + X_2^2X_3^2 - 2aX_2X_3 - 4bX_2 - 4bX_3 + a^2. \end{aligned}$$

Clearly, the linear factors of this generator correspond to the degenerated case where two or more points are the same or of opposite signs, and f_3 is the 3rd *summation polynomial*, that is, the summation polynomial for three distinct points summing to zero.

Starting from the 3rd summation polynomial, we can recursively construct the subsequent summation polynomials f_m for $m > 3$ by taking resultants. As a result, the degree of each variable in f_m is 2^{m-2}, which grows exponentially as m. This is the observation Semaev made in his seminal work [35]. In short, his proposal is to consider factor bases of the following form:

$$\mathcal{F} = \Big\{(x, y) \in E(\mathbb{F}_{p^n}) : x \in V \subset \mathbb{F}_{p^n}\Big\},$$

where V is a subset of $\mathbb{F}_{p^n}$. Then, we solve PDP of mth order by solving the corresponding $(m+1)$th summation polynomial $f_{m+1}(X_1, \ldots, X_m, \tilde{x}) = 0$, where $\tilde{x}$ is the x-coordinate of the point to be decomposed.

Note that this factor base is naturally invariant under point negation. That is, $P_i \in \mathcal{F}$ implies $-P_i \in \mathcal{F}$. In this case, we have about $|\mathcal{F}|/2$ (trivial) relations $P_i + (-P_i) = O$ for free, so we only need to find the other $|\mathcal{F}|/2$ nontrivial relations. In general, we will only discuss factor bases that are invariant under point negation, so by abuse of language, both $\mathcal{F}$ and $\mathcal{F}$ modulo point negation may be referred to as a factor base in the rest of this section.

2.1.2.3 Weil Restriction

Restricting the x-coordinates of the points in a factor base to a subset of $\mathbb{F}_{p^n}$ is important from the viewpoint of polynomial system solving. Take f_3 as an example. When decomposing a random point $aP + bQ$, we first substitute its x-coordinate into say X_3, projecting the ideal onto $\mathbb{F}_{p^n}[X_1, X_2]$. The dimension of the variety of this ideal is nonzero. Therefore, we would like to pose some restrictions on X_1 and X_2 to reduce the dimensions to zero so that the solving time can be more manageable.

When looking for solutions to a polynomial $f = \sum a_i X^i \in \mathbb{F}_{p^n}[X]$ in $\mathbb{F}_{p^n}$, we can view $\mathbb{F}_{p^n}[X]$ as a commutative affine algebra $\mathcal{A} = \mathbb{F}_{p^n}[X]/(X^{p^n} - X) \cong \mathbb{F}_{p^n}[X_1, \ldots, X_n]/(X_1^p - X_1, \ldots, X_n^p - X_n)$. This can be done by identifying the indeterminate X as $X_1\theta_1 + \cdots + X_n\theta_n$, where $(\theta_1, \ldots, \theta_n)$ is a basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Hence, f can be identified as a polynomial $f_1\theta_1 + \cdots + f_n\theta_n$, where $f_1, \ldots, f_n \in \mathcal{A}' = \mathbb{F}_p[X_1, \ldots, X_n]/(X_1^p - X_1, \ldots, X_n^p - X_n)$, by appropriately sending each coefficient $a_i \in \mathbb{F}_{p^n}$ to $a_i^{(1)}\theta_1 + \cdots + a_i^{(n)}\theta_n$ for $a_i^{(1)}, \ldots, a_i^{(n)} \in \mathbb{F}_p$. Therefore, an equation $f = 0$ over $\mathbb{F}_{p^n}$ will give rise to a system of equations $f_1 = \cdots = f_n = 0$ over $\mathbb{F}_p$. This technique is known as the *Weil restriction* and is used in the Gaudry–Diem attack, where the factor base is chosen to consist of points whose x-coordinates lie in a subspace V of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ [25, 30].

2.1.2.4 Exploiting Symmetry

Naturally, the symmetric group S_m acts on a point decomposition $P_1 + \cdots + P_m$ because elliptic curve groups are abelian. As noted by Gaudry in his seminal work [30], we can therefore rewrite the variables $x_1, \ldots, x_m \in \mathbb{F}_{p^n}$ by elementary symmetric polynomials $e_1, \ldots, e_m$, where $e_1 = \sum x_i$, $e_2 = \sum_{i \neq j} x_i x_j$, $e_3 = \sum_{i \neq j, i \neq k, j \neq k} x_i x_j x_k$, etc. Such rewriting can reduce the degree of summation polynomials and significantly speed up point decomposition [27, 31].

We might be able to exploit additional symmetry brought by actions of other groups, e.g., when the factor base is invariant under addition of small torsion points. For example, consider a decomposition of a point R under the action of addition of a 2-torsion point T_2:

$$R = P_1 + \cdots + P_n = (P_1 + u_1 T_2) + \cdots + (P_{n-1} + u_{n-1} T_2) + \left(P_n + \left(\sum_{i=1}^{n-1} u_i \right) T_2 \right).$$

Clearly, this holds for any $u_1, \ldots, u_{n-1} \in \{0, 1\}$, so a decomposition can give rise to $2^{n-1} - 1$ other decompositions. Similar to rewriting using the elementary symmetric polynomials for the action of S_m, we can also take advantage of this additional symmetry by appropriately rewriting [26].

Naturally, such speedup is curve-specific. Furthermore, even if the factor base is invariant under additional group actions, we may or may not be able to exploit such symmetry to speed up the point decomposition depending on whether the action is "easy to handle in the polynomial system solving process" [26].

2.1.2.5 PDP on (Twisted) Edwards Curves

Faugère, Gaudry, Hout, and Renault studied PDP on twisted Edwards, twisted Jacobi intersections, and Weierstrass curves [26]. For the sake of completeness, we include some of their results here. An Edwards curve over $\mathbb{F}_{p^n}$ for $p \neq 2$ is defined by the equation $x^2 + y^2 = 1 + dx^2y^2$ for certain $d \in \mathbb{F}_{p^n}$ [24]. A twisted Edwards curve $tE_{a,d}$ over $\mathbb{F}_{p^n}$ for $p \neq 2$ is defined by the equation $ax^2 + y^2 = 1 + dx^2y^2$ for certain $a, d \in \mathbb{F}_{p^n}$ [23]. A twisted Edwards curve is a quadratic twist of an Edwards curve by $a_0 = 1/(a - d)$. For $P = (x, y) \in tE_{a,d}$, $-P = (-x, y)$. Furthermore, the addition and doubling formulae for $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ are given as follows:

$$\text{When } (x_1, y_1) \neq (x_2, y_2) : \begin{cases} x_3 = \dfrac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \\ y_3 = \dfrac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2}. \end{cases}$$

$$\text{When } (x_1, y_1) = (x_2, y_2) : \begin{cases} x_3 = \dfrac{2 x_1 y_1}{1 + d x_1^2 y_1^2}, \\ y_3 = \dfrac{y_1^2 - a x_1^2}{1 - d x_1^2 y_1^2}. \end{cases}$$

The 3rd summation polynomial for twisted Edwards curves is [26]:

$$\begin{aligned} f_{tE,3}(Y_1, Y_2, Y_3) = &\left(Y_1^2 Y_2^2 - Y_1^2 - Y_2^2 + \frac{a}{d} \right) Y_3^2 \\ &+ 2\frac{d-a}{d} Y_1 Y_2 Y_3 + \frac{a}{d} \left(Y_1^2 + Y_2^2 - 1 \right) - Y_1^2 Y_2^2. \end{aligned}$$

Again, the subsequent summation polynomials are obtained by taking resultants.

2.1.2.6 Symmetry and Decomposition Probability

Symmetry brought by group action on point decomposition will inevitably be accompanied by a *decrease in decomposition probability*. For example, if a factor base $\mathcal{F}$ is invariant under addition of a 2-torsion point, then the decomposition probability for PDP of the mth order should decrease by a factor of 2^{m-1}. This is due to the same reason that the decomposition probability decreases by a factor of $m!$ because the symmetric group S_m acts on $\mathcal{F}$.

However, this simple fact seems to have been largely ignored in the literature. For example, Faugère, Gaudry, Hout, and Renault explicitly stated in Sect. 5.3 of their study that "[the] probability to decompose a point [into a sum of n points from the factor base] is $\frac{1}{n!}$" for twisted Edwards or twisted Jacobi intersections curves, despite the fact that the factor base is invariant under the addition of 2-torsion points [26]. At first glance, this may not seem a problem, as we would expect to obtain 2^{n-1} solutions if we can successfully solve a PDP instance. (Unfortunately, this is also *not true* in general. We will return to it in more detail in Sect. 2.1.5.3.) However, when estimating the cost of a complete ECDLP attack, they proposed to *collapse* these 2^{n-1} relations into one to reduce the size of the factor base and thus the cost of the linear algebra, cf. Remark 5 of the paper. In this case, the decrease in decomposition probability *does* have an adverse effect, and their estimation for the overall ECDLP cost ended up being overoptimistic by a factor of at least 2^{n-1}.

2.1.3 Montgomery and Hessian Curves

2.1.3.1 Montgomery Curves

A Montgomery curve $M_{A,B}$ over $\mathbb{F}_{p^n}$ for $p \neq 2$ is defined by the equation

$$By^2 = x^3 + Ax^2 + x \tag{2.1}$$

for $A, B \in \mathbb{F}_{p^n}$ such that $A \neq \pm 2$, $B \neq 0$, and $B(A^2-4) \neq 0$ [32]. For $P = (x, y) \in M_{A,B}$, $-P = (x, -y)$. Furthermore, the addition and doubling formulae for $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ are given as follows. When $(x_1, y_1) \neq (x_2, y_2)$:

$$\begin{cases} x_3 = B\left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - A - x_1 - x_2 = \dfrac{B(x_2y_1 - x_1y_2)^2}{x_1x_2(x_2-x_1)^2}, \\ y_3 = \dfrac{(2x_1 + x_2 + A)(y_2 - y_1)}{x_2 - x_1} - \dfrac{B(y_2-y_1)^3}{(x_2-x_1)^3} - y_1. \end{cases}$$

When $(x_1, y_1) = (x_2, y_2)$:

$$\begin{cases} x_3 = \dfrac{(x_1^2 - 1)^2}{4x_1(x_1^2 + Ax_1 + 1)}, \\ y_3 = \dfrac{(2x_1 + x_1 + A)(3x_1^2 + 2Ax_1 + 1)}{2By_1} - \dfrac{B(3x_1^2 + 2Ax_1 + 1)^3}{(2By_1)^3} - y_1. \end{cases}$$

It was noted by Montgomery himself in his original paper that such curves can give rise to efficient scalar multiplication algorithms [32]. That is, consider a random point $P \in M_{A,B}(\mathbb{F}_{p^n})$ and $nP = (X_n : Y_n : Z_n)$ in projective coordinates for some integer n. Then

$$\begin{cases} X_{m+n} = Z_{m-n}[(X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)]^2, \\ Z_{m+n} = X_{m-n}[(X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)]^2. \end{cases}$$

In particular, when $m = n$

$$\begin{cases} X_{2n} = (X_n + Z_n)^2(X_n - Z_n)^2, \\ Z_{2n} = (4X_nZ_n)\left((X_n - Z_n)^2 + ((A+2)/4)(4X_nZ_n)\right), \\ 4X_nZ_n = (X_n + Z_n)^2 - (X_n - Z_n)^2. \end{cases}$$

In this way, scalar multiplication on the Montgomery curve can be performed without using y-coordinates, leading to fast implementation.

2.1.3.2 Summation Polynomials for Montgomery Curves

Following Semaev's approach [35], we can construct summation polynomials for Montgomery curves. Like Weierstrass curves, the 2nd summation polynomial for Montgomery curves is simply $f_{M,2} = X_1 - X_2$. Now, we consider $P, Q \in M_{A,B}$ for $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Let $P + Q = (x_3, y_3)$ and $P - Q = (x_4, y_4)$. By the addition formula, we have

$$x_3 = \frac{B(x_2y_1 - x_1y_2)^2}{x_1x_2(x_2 - x_1)^2}, x_4 = \frac{B(x_2y_1 - x_1y_2)^2}{x_1x_2(x_2 + x_1)^2}.$$

It follows that

$$\begin{cases} x_3 + x_4 = \dfrac{2\left((x_1 + x_2)(x_1x_2 + 1) + 2Ax_1x_2\right)}{(x_1 - x_2)^2}, \\ x_3x_4 = \dfrac{(1 - x_1x_2)^2}{(x_1 - x_2)^2}. \end{cases}$$

Using the relationship between the roots of a quadratic polynomial and its coefficients, we obtain

$$(x_1 - x_2)^2 x^2 - 2\left((x_1 + x_2)(x_1 x_2 + 1) + 2Ax_1 x_2\right)x + (1 - x_1 x_2)^2.$$

From here, we can obtain for Montgomery curve which is the 3rd summation polynomial:

$$\begin{aligned} f_{M,3}(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2((X_1 + x_2)(X_1 X_2 + 1) \\ + 2AX_1 X_2)X_3 + (1 - X_1 X_2)^2, \end{aligned}$$

as well as the subsequent summation polynomials by taking resultants:

$$\begin{aligned} f_{M,m}(X_1, \ldots, X_m) = \operatorname{Res}_X \big(f_{M,m-k}(X_1, \ldots, X_{m-k-1}, X), \\ \times\ f_{M,k+2}(X_{m-k}, \ldots, X_m, X)\big)\,. \end{aligned}$$

2.1.3.3 Small Torsion Points on Montgomery Curves

A Montgomery curve always contains an affine 2-torsion point T_2. Because $T_2 + T_2 = 2T_2 = \mathcal{O}$, $-T_2 = T_2$. If we write $T_2 = (x, y)$, then we can see that $y = 0$ in order for $-T_2 = T_2$ as $p \neq 2$. Substituting $y = 0$ into Eq. (2.1), we get an equation $x^3 + Ax^2 + x = 0$. The left-hand side factors into $x(x^2 + Ax + 1) = 0$, so we get

$$x = 0,\ \frac{-A \pm \sqrt{A^2 - 4}}{2}.$$

Therefore, the set of rational points over the definition field F_{p^n} of a Montgomery curve includes at least two 2-torsion points, namely $\mathcal{O}$ and $(0, 0)$. The other 2-torsion points may or may not be rational, so we will focus on $(0, 0)$ in this section. Substituting $(x_2, y_2) = (0, 0)$ into the addition formula for Montgomery curves, we get that for any point $P = (x, y) \in M_{A,B}$, $P + (0, 0) = (1/x, -y/x^2)$.

To be able to exploit the symmetry of addition of $T_2 = (0, 0)$, we need to choose the factor base $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{p^n}) : x \in V \subset \mathbb{F}_{p^n}\}$ invariant under addition of T_2. This means that V needs to be closed by undertaking multiplicative inverses. In other words, V needs to be a *subfield* of $\mathbb{F}_{p^n}$, i.e., $V = \mathbb{F}_{p^\ell}$ for some integer ℓ that divides n. In this case, f_m is invariant under the action of $x_i \mapsto 1/x_i$. Unfortunately, such an action is not linear and hence not easy to handle in polynomial system solving. How to take advantage of such kind of symmetry in PDP is still an open research problem.

2.1.3.4 Hessian Curves

A Hessian curve H_d over $\mathbb{F}_{p^n}$ for $p^n = 2 \bmod 3$ is defined by the equation

$$x^3 + y^3 + 1 = 3dxy \tag{2.2}$$

for $d \in \mathbb{F}_{p^n}$ such that $27d^3 \neq 1$ [36]. For $P = (x, y) \in H_d$, $-P = (y, x)$. Furthermore, the addition and doubling formulae for $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ are given as follows.

$$\text{When } (x_1, y_1) \neq (x_2, y_2): \begin{cases} x_3 = \dfrac{y_1^2 x_2 - y_2^2 x_1}{x_2 y_2 - x_1 y_1}, \\ y_3 = \dfrac{x_1^2 y_2 - x_2^2 y_1}{x_2 y_2 - x_1 y_1}. \end{cases}$$

$$\text{When } (x_1, y_1) = (x_2, y_2): \begin{cases} x_3 = \dfrac{y_1(1 - x_1^3)}{x_1^3 - y_1^3}, \\ y_3 = \dfrac{x_1(y_1^3 - 1)}{x_1^3 - y_1^3}. \end{cases}$$

2.1.3.5 Summation Polynomials for Hessian Curves

Following a similar approach outlined by Galbraith and Gebregiyorgis [29], we can construct summation polynomials for Hessian curves. First, we introduce a new variable $T = X + Y$, which is invariant under point negation. The 2nd summation polynomial for Hessian curves is simply $f_{H,2} = T_1 - T_2$. Now let

$$Z = \left\{ \begin{array}{r} (x_1, y_1, t_1, x_2, y_2, t_2, x_3, y_3, t_3) \in \mathbb{F}_{p^n}^9 : (x_i, y_i) \in H_d(\mathbb{F}_{p^n}), i = 1, 2, 3; \\ (x_1, y_1) + (x_2, y_2) + (x_3, y_3) = O; x_i + y_i = t_i, i = 1, 2, 3 \end{array} \right\}.$$

Clearly, Z is in the variety of the ideal $I \subset \mathbb{F}_{p^n}[X_1, Y_1, T_1, X_2, Y_2, T_2, X_3, Y_3, T_3]$ generated by

$$\left\{ \begin{array}{l} X_i^3 + Y_i^3 + 1 - 3dX_iY_i, i = 1, 2, 3; \\ (X_3 - X_1)(Y_2 - Y_1) - (X_2 - X_1)(Y_3 - Y_1); \\ X_i + Y_i - T_i, i = 1, 2, 3 \end{array} \right\}.$$

Again, we compute the elimination ideal $I \cap \mathbb{F}_{p^n}[T_1, T_2, T_3]$ and obtain a principal ideal generated by some polynomial. After removing the degenerate factors, we can obtain for Hessian curve the 3rd summation polynomial:

$$\begin{aligned} f_{H,3}(T_1, T_2, T_3) = & T_1^2T_2^2T_3 + dT_1^2T_2^2 + T_1^2T_2T_3^2 + dT_1^2T_2T_3 + dT_1^2T_3^2 - T_1^2 + \\ & T_1T_2^2T_3^2 + dT_1T_2^2T_3 + dT_1T_2T_3^2 + 3d^2T_1T_2T_3 + 2T_1T_2 + 2T_1T_3 + \\ & 2dT_1 + dT_2^2T_3^2 - T_2^2 + 2T_2T_3 + 2dT_2 - T_3^2 + 2dT_3 + 3d^2, \end{aligned}$$

as well as the subsequent summation polynomials by taking resultants:

$$f_{H,m}(T_1,\ldots,T_m) = \mathrm{Res}_T\left(f_{H,m-k}(T_1,\ldots,T_{m-k-1},T), f_{H,k+2}(T_{m-k},\ldots,T_m,T)\right).$$

2.1.3.6 Small Torsion Points on Hessian Curves

As we shall see in Sect. 2.1.4.1, we will compare elliptic curves in various forms that are isomorphism to one another over the same definition field. As a result, we will only experiment with those Hessian curves that include 2-torsion points like Montgomery or (twisted) Edwards curves. Because $T_2 + T_2 = 2T_2 = \mathcal{O}$, it follows that $-T_2 = T_2$. If we write $T_2 = (x, y)$, then we can see that $x = y$ in order for $-T_2 = T_2$ as $-T_2 = (y, x)$. Substituting $x = y$ into Eq. (2.2), we get an equation $2x^3 - 3dx^2 + 1 = 0$. Therefore, a Hessian curve $H_d(\mathbb{F}_{p^n})$ has a 2-torsion point (ζ, ζ) if the polynomial $2X^3 - 3dX^2 + 1$ has a root ζ in $\mathbb{F}_{p^n}$. In this case, the addition of this 2-torsion point to a point (x, y) would give a point (x', y'), where

$$\begin{cases} x' = \dfrac{\zeta y^2 - \zeta^2 x}{\zeta^2 - xy}, \\ y' = \dfrac{\zeta x^2 - \zeta^2 y}{\zeta^2 - xy}. \end{cases}$$

Obviously, the typical factor bases are not invariant under addition of this 2-torsion point in general.

A Hessian curve always contains a 3-torsion point T_3 such that $3T_3 = \mathcal{O}$ [36]. If we let $T_3 = (x, y)$, then we see that $2(x, y) = -(x, y) = (y, x)$, substituting which into the doubling formula, we get

$$\begin{cases} \dfrac{y(1 - x^3)}{x^3 - y^3} = y, \\ \dfrac{x(y^3 - 1)}{x^3 - y^3} = x. \end{cases}$$

Because x and y cannot be zero at the same time, we have $x^3 - y^3 = 1 - x^3 = y^3 - 1$, or $x^3 = y^3 = 1$. Now because $p^n = 2 \bmod 3$, $\mathbb{F}_{p^n}$ does not have any primitive cubic roots of unity, $x = y = 1$ and $T_3 = (1, 1)$. By the addition formula, if $P = (x, y)$, then

$$P + T_3 = (x, y) + (1, 1) = \left(\frac{y^2 - x}{1 - xy}, \frac{x^2 - y}{1 - xy}\right).$$

However, for $P \in \mathcal{F}$, we only know that $t = x + y \in V \subset \mathbb{F}_{p^n}$, but we know nothing about $1 - xy$, which can lie outside of V. Therefore, again, typical factor bases are not invariant under addition of this 3-torsion point in general. Therefore, it is not

Fig. 2.1 Experimental results on PDP solving for the case of $n = 5$

m	p	Curve	Time	Dreg	Matcost	Rank
3	239	Hessian	0	6	42336.8	1
		Weierstrass	0	6	41259.0	1
		Montgomery	0	6	61239.0	4
		tEdwards	0	6	6308.4	4
	251	Hessian	0	6	41420.4	1
		Weierstrass	0	6	42132.0	1
		Montgomery	0	6	61127.9	4
		tEdwards	0	6	6308.4	4
4	239	Hessian	3.990	19	12066100000	1
		Weierstrass	3.680	19	12064700000	1
		Montgomery	3.489	18	11399100000	5
		tEdwards	0.150	18	54093000	5
	251	Hessian	3.459	19	12069800000	1
		Weierstrass	3.659	19	12066400000	1
		Montgomery	3.280	18	11401700000	5
		tEdwards	0.119	18	54102900	5

clear how to exploit such symmetry brought by addition of small torsion points for Hessian curves.

2.1.4 *Experiments on PDP Solving*

This section shows the results of our experiments conducted to compare the computational complexity of PDP on four different curves: Hessian(H), Weierstrass(W), Montgomery(M), and twisted Edwards(tE).

2.1.4.1 Experimental Setup

As explained in Sect. 2.1.2.1, we focus on PDP in these experiments as the linear algebra step is already well understood. Furthermore, we focus on the bottleneck computation in PDP, namely, the cost of the F4 algorithm for computing Gröbner bases of the polynomial systems obtained after rewriting using the elementary symmetric polynomials and applying the Weil restriction technique to summation polynomials. This way we will be taking advantage of the symmetry of S_m acting on point decompositions. However, we *did not* exploit symmetry of any other group actions. This is because we want to compare the *intrinsic* computational complexity of PDP and hence only consider the symmetry that is present in *all* curves. Exploiting further curve-specific symmetry whenever possible will result in a further speedup, but it would be independent of our findings here.

2.1.4.2 Experimental Results

Figure 2.1 presents our experimental results for the case of $n = 5$. Here, we choose our factor base by taking V as the base field $\mathbb{F}_p$ of $\mathbb{F}_{p^n}$. All our experiments were performed using the MAGMA computation algebra system (version 2.23-1) on a single core of an Intel Xeon CPU E7-4830 v4 running at 2 GHz. Comparisons to solve each PDP were performed by running time (in second), Dreg, Matcost, and Rank. The "Dreg" is the maximum step degree reached during the execution of the F4 algorithm, which is referred to as the "degree of regularity" in the literature [29] and provides an upper bound for the sizes of the Macaulay submatrices involved in the computation, the "Matcost" is a number output by the MAGMA implementation of the F4 algorithm and provides an estimate of the linear algebra cost during the execution of the F4 algorithm, and finally, the "Rank" is the number of linearly independent relations we obtain once successfully solving a PDP instance. It is an important factor to consider, as it determines how many PDP instances we need to successfully solve to have enough relations for a complete ECDLP attack using index calculus. We can clearly see that the PDP solving time and Matcost for twisted Edwards curves are much smaller than those for the other curves. In contrast, the degrees of regularity for Montgomery and twisted Edwards curves are smaller than those of the other curves in the case of $m = 4$. In addition, we can see that the rank for Hessian and Weierstrass curves is 1 in all cases, whereas for Montgomery and twisted Edwards curves, it is 4 and 5 in the case of $m = 3$ and $m = 4$, respectively. Last but not least, although we only present the results for small p (around 8-bit long), here, we have some preliminary results for larger p (around 16-bit and 32-bit long). Apart from the slight difference in the absolute running time, all other results such as Dreg, Matcost, and Rank are similar, so we do not repeat them here.

2.1.5 Analysis

2.1.5.1 Revisit Summation Polynomial in Each Form

As we have seen in Sect. 2.1.4.2, PDP on (twisted) Edwards curves seems easier to solve than on other curves. The explanation offered by Faugère, Gaudry, Hout, and Renault is "due to the smaller degree appearing in the computation of Gröbner basis of $\mathscr{S}_{D_n}$ in comparison with the Weierstrass case," cf. Sect. 4.1.1 of their paper [26]. Unfortunately, this *cannot* explain the difference between (twisted) Edwards and Montgomery curves as the highest degrees appearing in the computation of Gröbner bases are *the same* for these two curves. Therefore, there must be other reasons. We have found that the total number of terms for twisted Edwards curves is significantly lower than that for the other curves in all cases. Naturally, this could lead to faster solving time with the F4 algorithm. We also note that, except for the twisted Edwards curves, the summation polynomials before Weil restriction for the other curves are all 100% dense without any missing terms.

2.1.5.2 Missing Terms of Summation Polynomials in (Twisted) Edwards Curves

In this section, we will show that the summation polynomials for (twisted) Edwards curves *mainly* have terms of *even* degrees. The set of terms of even degrees is closed under multiplication, so intuitively, such polynomials are easier to solve, which can be the main reason for the efficiency gain observed in the case of (twisted) Edwards curves.

We shall make this intuition precise in Theorem 2.1, but before we state the main result, we need to clarify our terminology for ease of exposition. When a multivariate polynomial is regarded as a univariate polynomial in one of its variables T, we say that the coefficient a_i of a term $a_i T^i$ is an *even or odd-degree coefficient* depending on whether i is even or odd, respectively. Note that these coefficients are themselves multivariate polynomials in one fewer variable.

We say that a monomial $m = \prod_{i=1}^{n} x_i^{e_i}$, $e_i \geq 0$ in a multivariate polynomial in n variables is *of even degree* or simply an *even-degree monomial* if $\sum_i e_i$ is even; that it is *of odd degree* or simply an *odd-degree monomial* otherwise. In contrast, a monomial is *of (homogeneous) even parity* if all e_i are even; it is *of (homogeneous) odd parity* if all e_i are odd. A monomial is *of homogeneous parity* if it is either of homogeneous even or odd parity. Note that the definition of monomials of odd parity depends on the total number of variables in the polynomial, which is not the case for monomials of even parity because we regard 0 as even. For example, the monomial $x_1 x_2$ is a monomial of odd parity in a polynomial in x_1 and x_2 but not so in another polynomial in $x_1, \ldots, x_n$ for $n > 2$.

By abuse of language, we say that a polynomial is *of even or odd parity* if it is a linear combination of monomials of even or odd parity, respectively; that a polynomial is *of homogeneous parity* if it is a linear combination of monomials of homogeneous parity. The set of polynomials of even parity is closed under polynomial addition and multiplication and hence forms a subring. In contrast, a polynomial f in $x_1, \ldots, x_n$ of odd parity must have the form $\sum_i c_i \left(\prod_{j=1} x_j^{e_{ij}} \right)$, for e_{ij} odd. Therefore, if f is a polynomial of odd parity and g, a polynomial of even parity, then fg must be of odd parity.

Theorem 2.1 *Let $\mathcal{E}$ be a family of elliptic curves such that its 3rd summation polynomial $f_{\mathcal{E},3}(X_1, X_2, X_3)$ is of degree 2 in each variable X_i and of homogeneous parity. Let $g_{\mathcal{E},m}$ be the polynomial corresponding to the PDP of mth order for $\mathcal{E}$ as described in Sect. 2.1.2.2. That is, $g_{\mathcal{E},m}(X_1, \ldots, X_m) = f_{\mathcal{E},m+1}(X_1, \ldots, X_m, x)$, where x is a constant depending on the point to be decomposed.*

1. *If m is even, then $g_{\mathcal{E},m}$ has no monomials of odd degrees.*
2. *If m is odd, then $g_{\mathcal{E},m}$ has some but not all monomials of odd degrees.*

Among the four forms of elliptic curves that we investigated in this section, only the (twisted) Edwards form satisfies the premises of Theorem 2.1. As we have seen in Sect. 2.1.4, the PDP solving time for the (twisted) Edwards form is thus significantly faster than that for the other forms.

We will prove Theorem 2.1 in the rest of this section, for which we will need the following lemmas.

Lemma 2.1 *Let $f_1(T_1, \dots, T_r, T) = a_0 + a_1T + \cdots + a_mT^m$ and $f_2(T_1, \dots, T_r, T) = b_0 + b_1T + \cdots + b_nT^n$ be two polynomials in $r + 1$ variables, where a_i and b_i are polynomials in $T_1, \dots, T_r$. Let $f(T_1, \dots, T_r) = \mathrm{Res}_T(f_1, f_2)$ be the resultant of f_1 and f_2 regarded as two univariate polynomials in T. If both m and n are even, then every monomial of f is a product of an even number or none of the odd-degree coefficients of f_1 and f_2 and some or none of the even-degree coefficients of f_1 and f_2. Specifically, the odd-degree coefficients a_{2k+1} and b_{2k+1} of f_1 and f_2, respectively, appear in total an even number of times in each monomial of f.*

Proof The resultant $\mathrm{Res}_T(f_1, f_2)$ of f_1 and f_2 is the determinant of the following $(m + n) \times (m + n)$ matrix S:

$$S = \begin{bmatrix} a_m & a_{m-1} & \dots & a_0 & & & \\ & a_m & a_{m-1} & \dots & a_0 & & \\ & & \ddots & & & \ddots & \\ & & & a_m & a_{m-1} & \dots & a_0 \\ b_n & b_{n-1} & \dots & b_0 & & & \\ & b_n & b_{n-1} & \dots & b_0 & & \\ & & \ddots & & & \ddots & \\ & & & b_n & b_{n-1} & \dots & b_0 \end{bmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \end{array} . \tag{2.3}$$

We denote s_{ij} as the entry at the ith row and jth column of S for $1 \le i, j \le m + n$. Because both m and n are even, an even-degree coefficient a_{2k} or b_{2k} will appear in s_{ij} for which the sum of indices $i + j$ is even. Similarly, an odd-degree coefficient a_{2k+1} or b_{2k+1} will appear in s_{ij} for which the sum of indices $i + j$ is odd. Now recall that the determinant of S is defined as

$$\sum_{\sigma \in S_{n+m}} \mathrm{sgn}(\sigma) s_{1,\sigma(1)} \cdot s_{2,\sigma(2)} \cdots s_{m+n,\sigma(m+n)}.$$

We note that the sum of the indices of any summand is

$$\sum_{i}^{m+n} i + \sigma(i) = (m + n)(m + n + 1),$$

which is always even. Therefore, the odd-degree coefficients must appear an even number of times, thus completing the proof.

Lemma 2.2 *Let $\mathcal{E}$ be a family of elliptic curves such that its 3rd summation polynomial $f_{\mathcal{E},3}(X_1, X_2, X_3)$ is of degree 2 in each variable X_i and of homogeneous parity. Then, any subsequent summation polynomial $f_{\mathcal{E},m}(X_1, \dots, X_m)$ for $m > 3$ is of homogeneous parity.*

Proof As the summation polynomial $f_{\mathcal{E},m+1}$ for $m \geq 3$ is defined recursively from $f_{\mathcal{E},m}$ and $f_{\mathcal{E},3}$ by taking resultants

$$f_{\mathcal{E},m+1}(X_1,\dots,X_{m+1}) = \mathrm{Res}_X\left(f_{\mathcal{E},m}(X_1,\dots,X_{m-1},X), f_{\mathcal{E},3}(X_m,X_{m+1},X)\right),$$

we shall prove this lemma by induction on m. Let $f_{\mathcal{E},m}(X_1,\dots,X_{m-1},X) = a_{2^{m-2}}X^{2^{m-2}} + \cdots + a_1X + a_0$ and $f_{\mathcal{E},3}(X_m,X_{m+1},X) = b_2X^2 + b_1X + b_0$. By the premise that $f_{\mathcal{E},3}$ is of homogeneous parity, b_0 and b_2 must consist only of monomials (in X_m and X_{m+1}) of even parity. Furthermore, $b_1 = cX_mX_{m+1}$ for some constant c. This is because $f_{\mathcal{E},3}$ is of degree 2 in each variable, for which the only monomial of odd parity is $X_mX_{m+1}X$.

Now consider a term $c_kX_{m+1}^k$ of

$$f_{\mathcal{E},m+1}(X_1,\dots,X_m,X_{m+1}) = c_{2^{m-1}}X_{m+1}^{2^{m-1}} + \cdots + c_1X_{m+1} + c_0$$

as a univariate polynomial in X_{m+1}. Again as $f_{\mathcal{E},3}$ is of degree 2 in X, we have the case of $n = 2$ in Eq. 2.3. Now X_{m+1} must come from b_1, so we can conclude that

$$c_kX_{m+1}^k = \sum_i \alpha_i a_{\beta_i} a_{\gamma_i} b_0^{\delta_i} b_2^{\epsilon_i} X_m^k X_{m+1}^k,$$

where α_i a constant, $\beta_i, \gamma_i \in \{0,\dots,2^{m-2}\}$, and δ_i, ϵ_i nonnegative integers such that $\delta_i + \epsilon_i + k = 2^{m-2}$. We will complete the proof by showing that $c_kX_{m+1}^k$ is a polynomial in $X_1,\dots,X_{m+1}$ of homogeneous parity for all k as follows.

1. If k is even, then by Lemma 2.1, β_i and γ_i are both even or both odd in each summand. In either case, the product $a_{\beta_i}a_{\gamma_i}$ is a polynomial in $X_1,\dots,X_{m-1}$ of even parity. It follows that each summand is a polynomial of even parity because it is a product of polynomials of even parity. Hence, $c_kX_{m+1}^k$ is a polynomial of even parity.
2. If k is odd, the situation is similar but slightly more complicated. By Lemma 2.1, exactly one of β_i and γ_i is odd in each summand, say β_i. By induction hypothesis, a_{β_i} is a polynomial in $X_1,\dots,X_{m-1}$ of odd parity because it comes from $a_{\beta_i}X^{\beta_i}$ in $f_{\mathcal{E},m}$. It follows that each summand is a polynomial of odd parity because it is a product of a polynomial of even parity $a_{\gamma_i}b_0^{\delta_i}b_2^{\epsilon_i}$ and a polynomial of odd parity $a_{\beta_i}X_m^kX_{m+1}^k$. Hence, $c_kX_{m+1}^k$ is a polynomial of odd parity.

By Lemma 2.2, $g_{\mathcal{E},m}(X_1,\dots,X_m) = f_{\mathcal{E},m+1}(X_1,\dots,X_m,x)$ is of homogeneous parity. Obviously, the monomials of even parity will remain of even degree after x is substituted. If m is even, then the monomials of odd parity in $f_{\mathcal{E},m+1}$ will become of even degree after x is substituted because an even number of odd numbers sum to an even number. Similarly, if m is odd, then the monomials of odd parity in $f_{\mathcal{E},m+1}$ will become of odd degree after x is substituted. However, those odd-degree monomials that are *not* of homogeneous parity, e.g., $X_1^2X_2$, cannot appear in $g_{\mathcal{E},m}$ by Lemma 2.2. This completes the proof of Theorem 2.1.

2.1.5.3 What Price for a Highly Symmetric Factor Base?

Last but not least, we discuss the price needed to pay to have a highly symmetric factor base $\mathcal{F}$ that is invariant under more group actions in addition to that of the symmetric group S_m. As previewed in Sect. 2.1.2.6, we would expect that the effect of the decrease in decomposition probability due to additional symmetry in $\mathcal{F}$ could be offset by that of the increase in number of solutions. For example, let us reconsider the group action of addition of T_2 in Sect. 2.1.2.4. If we could get 2^{m-1} solutions, then the loss of the factor of 2^{m-1} in decomposition probability would be compensated. This way everything would be the same as if there were no such symmetry, and we could exploit the additional symmetry at no cost.

Unfortunately, this proposition is *false* in general. Consider an example of $m = 4$. Let $Q_i = P_i + T_2$ for $i = 1, 2, 3, 4$. We can write down all $2^{m-1} = 8$ possible ways of a point decomposition under this group action:

$$\begin{aligned} P_1 + P_2 + P_3 + P_4 =& Q_1 + Q_2 + P_3 + P_4 \\ = Q_1 + P_2 + Q_3 + P_4 =& Q_1 + P_2 + P_3 + Q_4 \\ = P_1 + Q_2 + Q_3 + P_4 =& P_1 + Q_2 + P_3 + Q_4 \\ = P_1 + P_2 + Q_3 + Q_4 =& Q_1 + Q_2 + Q_3 + Q_4. \end{aligned}$$

It is easy to find that we have only five linearly independent relations from these eight relations, as there are nontrivial linear combinations summing to zero, e.g.:

$$\begin{aligned} &(P_1 + P_2 + P_3 + P_4) - (Q_1 + Q_2 + P_3 + P_4) - (P_1 + P_2 + Q_3 + Q_4) \\ &\quad + (Q_1 + Q_2 + Q_3 + Q_4) = O. \end{aligned}$$

As explained in Sect. 2.1.4.1, the factor bases for Montgomery and twisted Edwards curves are invariant under addition of 2-torsion points. For $m = 3$, we achieve maximum rank of $2^{m-1} = 4$. For $m = 4$, as we have explained above, we can only have rank 5, which is strictly less than the maximum possible rank $2^{m-1} = 8$.

Finally, we note that we have not exploited any symmetry for Hessian curves in our experiments. However, the rank for Hessian curves is always 1 in all our experiments. This shows that the factor base we have chosen for Hessian curves is *not* invariant under addition of small torsion points, as the rank would be > 1 otherwise.

2.1.6 Concluding Remarks

In this section, we experimentally explored index-calculus attack on ECDLP over different forms such as twisted Edwards, Montgomery, Hessian, and Weierstrass curves under the totally fair conditions as they are isomorphic to each other over the same definition field $\mathbb{F}_{p^n}$ and showed that twisted Edwards curves are clearly faster than others. We investigated the summation polynomials of all forms in detail, found that big differences exist in the number of terms, and proved that monomials of odd degrees in summation polynomials on twisted Edwards curves do not exist. We showed that this difference causes less solving time of index-calculus attack on ECDLP over twisted Edwards than others.

2.2 Analysis on Ring-LWE over Decomposition Fields

2.2.1 Introduction

The ring variant of learning with errors (Ring-LWE) based cryptography [15, 16] is one of the most attractive research areas in cryptography. Ring-LWE has provided efficient and provably secure post-quantum cryptographic protocols, which include homomorphic encryption (HE) schemes [4, 5, 9]. The development of the efficiency and security of both post-quantum cryptography and HE is strongly desirable. In fact, the standardization of post-quantum cryptography is under development by the National Institute of Standards and Technology. Moreover, HE schemes that enable us to execute the computation on encrypted data without decryption have many applications in cloud computing.

Ring-LWE is characterized by two probabilistic distributions, modulus parameters (integers) and number fields, as detailed in Sect. 2.2.2.4. Usually, cyclotomic fields are used as the underlying number fields to increase efficiency and security [17]. However, especially in the case of HE schemes, improving the efficiency of the encryption/decryption procedures and homomorphic arithmetic operations on encrypted data while ensuring security remain important tasks.

To construct an HE scheme that can simultaneously encrypt many plaintexts efficiently, Arita and Handa proposed the use of a decomposition field, which is contained in a cyclotomic field with prime conductors, as an underlying number field for Ring-LWE [1]. (Sect. 2.2.3 presents the details of decomposition fields and of Arita and Handa's idea.) Arita and Handa's HE scheme, which is called the subring HE scheme, is indistinguishably secure under a chosen-plaintext attack if the decision variant of Ring-LWE over the decomposition fields is computationally infeasible. Arita and Handa's experiments [1, Sect. 5] showed that the performance of the subring HE scheme is much better than that of the FV scheme based on Ring-LWE over ℓth cyclotomic fields with prime numbers ℓ, as implemented in HElib [11].

As for the security of the subring HE scheme, Arita and Handa remarked that in the case of decomposition fields, some of the security properties of Ring-LWE in the case of cyclotomic fields are also satisfied. More concretely, there exists a quantum polynomial-time reduction from the approximate shortest vector problem on certain ideal lattices to Ring-LWE over decomposition fields, and the equivalence between the decision and search variants of Ring-LWE over decomposition fields is satisfied.

However, solving Ring-LWE is reduced to solving certain problems on lattices, such as the closest vector problem (CVP) and the shortest vector problem, and the difficulty of problems on lattices depends heavily on the structure and given bases of the underlying lattices. For example, if the shortest vector is much shorter than the second shortest vector in a certain lattice $\mathcal{L}$, then the shortest vector problem for lattice $\mathcal{L}$ would be easy. This means that the underlying number fields affect the difficulty of lattice problems arising in Ring-LWE. Hence, to ensure the security of the subring HE scheme, experimental or theoretical analyses of (lattice) attacks should be performed. However, [1] does not provide any such analysis.

In this study, we provide an experimental analysis of 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 ℓth cyclotomic fields with some prime numbers ℓ. In our experiments, we reduce the search Ring-LWE to the (approximate) CVP on certain lattices 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 use Babai's nearest plane algorithm [2] and Kannan's embedding technique [12] to solve the CVP. We then compare the running times, success rates, and Hermite root factors. (The root Hermite factor [10] is usually used to evaluate the quality of lattice attacks.) We also compare the experimental results of lattice attacks against Ring-LWE over various decomposition fields to find those fields that provide weak Ring-LWE.

Our experimental results indicate that the success rates and Hermite root factors for the decomposition fields are almost the same as those for the cyclotomic fields. However, the running time for decomposition fields is longer than that for cyclotomic fields. Moreover, the difference in running time increases as the rank of the lattices increases.

Therefore, we believe that Ring-LWE over decomposition fields is more secure against the above lattice attacks than that over cyclotomic fields because the ranks of the lattices occurring in our experiments are much lower than the ranks of the lattices used in practice. This means that to construct HE schemes (or schemes of other types), fewer parameters are needed for Ring-LWE over decomposition fields than for Ring-LWE over cyclotomic fields. Therefore, as a result of our analysis, we believe that Ring-LWE over decomposition fields can be used to construct more efficient HE schemes.

2.2.2 Preliminaries

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

2.2.2.1 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 exist $\mathbb{R}$-linearly independent vectors $\mathbf{b}_1, \ldots, and\, \mathbf{b}_n \in \mathbb{R}^m$ 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 ith column vector is $\mathbf{b}_j$, we have $\mathcal{L} = \{\mathbf{Bx} \mid \mathbf{x} \in \mathbb{Z}^n\}$. Then, we say that $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ is a lattice basis of $\mathcal{L}$, and $\mathbf{B}$ is the basis matrix of $\mathcal{L}$ with respect to $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. The value n is called the rank of $\mathcal{L}$, and it is denoted by $\mathrm{rank}(\mathcal{L})$. There are infinite bases for a lattice. In fact, for any unimodular matrix $\mathbf{U}$, all column vectors of $\mathbf{UB}$ also form a basis of $\mathcal{L}$. An important invariant of $\mathcal{L}$ is the determinant defined as $\det(\mathcal{L}) := \sqrt{\det(\mathbf{BB}^t)}$. This determinant is independent of basis.

There are various computationally hard problems on lattices. Here, we explain the CVP, which is a well-known problem on lattices. Given a lattice $\mathcal{L}$ and target vector $\mathbf{t} \in \mathbb{R}^m \setminus \mathcal{L}$, the CVP on $(\mathcal{L}, \mathbf{t})$ is the 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 the 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 that are useful for constructing cryptographic protocols become more difficult as the ranks of the underlying lattices increase, and the quality of the two algorithms mentioned earlier depends on ranks of input lattices.

Breaking some cryptographic protocols can be 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 that consists of nearly orthogonal and relatively short vectors. In fact, an input of Babai's nearest plane algorithm is an (LLL) reduced basis, and Kannan's embedding technique outputs an appropriate vector from the reduced basis. In our experiments, to solve CVP using Babai's nearest plane algorithm and Kannan's embedding technique, we use the LLL algorithm [13] and BKZ algorithm [7, 19], which are well-known algorithms for computing such bases.

The quality of basis reduction algorithms is usually estimated by the root Hermite factor, which is defined as follows: Let $\mathbf{b}$ be the shortest vector of a basis of a lattice $\mathcal{L}$ with rank n, which has been reduced by a basis reduction algorithm $\mathcal{A}$. Then, the root Hermite factor $\delta_{\mathcal{A},\mathcal{L}}$ is defined as a constant satisfying $\delta^n_{\mathcal{A},\mathcal{L}} := \|\mathbf{b}\| / \det(\mathcal{L})^{1/n}$. Better basis reduction algorithms provide smaller Hermite root factors.

2.2.2.2 Galois Theory

To describe decomposition fields, we need to describe Galois theory.

Let K be a field and L an extension field of K; we denote this situation by L/K. The field L is a K-vector space, and the degree of extension of L/K, denoted by

$[L : K]$, is defined as the dimension of L as K-vector space. If M is a subfield of L containing K as a subfield, i.e., $K \subset M \subset L$, then we call M an intermediate field of L/K. If L/K satisfies $[L : K] < \infty$, then L/K is called a finite extension of K. If M is an intermediate field of L/K with $[L : K] < \infty$, then we have $[L : K] = [L : M][M : K]$. If for any $\alpha \in L$, there exists a nonzero polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$, then L/K is called an algebraic extension of K. It is known that all finite extensions are algebraic extensions.

From now on, we suppose that L/K is a finite algebraic extension. For any $\alpha \in L$, the minimal polynomial over K of α is defined as the monic polynomial $f(x) \in K[x]$ with the lowest degree of all polynomials in $K[x]$ that vanish at α. We denote $\mathrm{Irr}(\alpha, K)(x)$ as the minimal polynomial over K of α. Note that the minimal polynomial over K of α coincides with the monic irreducible polynomial over K that vanishes at α. For a subset $S \subset L$, we denote $K(S)$ as the smallest subfield of L among subfields containing K and S. We call $K(S)$ the field generated by S over K. If L is generated by one element $\theta \in L$ over K, i.e., $L = K(\theta)$, then we have an isomorphism $L \cong K[x]/\left(\mathrm{Irr}(\theta, K)(x)\right)$ by $\theta \mapsto x$ (mod. $(\mathrm{Irr}(\theta, K)(x))$. This implies that $[K(\theta) : K] = \deg \mathrm{Irr}(\alpha, K)$.

Next, we describe separable, normal, and Galois extensions of fields. If $\mathrm{Irr}(\alpha, K)(x)$ for any α that has no multiple roots, then L/K is called a separable extension of K. If L contains all roots of $\mathrm{Irr}(\alpha, K)(x)$ for any $\alpha \in L$, then L/K is called a normal extension of K. If all algebraic extensions of K, including infinite algebraic extensions, are separable, then K is called a perfect (field). It is known that fields with characteristic zero and any finite field are perfect, and that any finite separable extension field can be generated by one element. If L/K is a separable and normal extension of K, then L/K is called a Galois extension of K. Let Ω be a sufficiently large field containing K such that any ring-homomorphism ϕ fixing K, i.e., $\phi(a) = a$ for any $a \in K$, to L satisfies $\phi(L) \subset \Omega$. We define the set of all ring-homomorphisms by fixing K to the range L to Ω as follows:

$$\mathrm{Hom}_K(L, \Omega) := \{\sigma : L \hookrightarrow \Omega \mid \sigma(a) = a, \forall a \in K\}.$$

(Note that any nonzero ring-homomorphism between fields is injective.) Let L/K be separable with $[L : K] = n$ and $L = K(\theta)$. Let $\theta = \theta_1, \ldots, \theta_n$ be all roots of $\mathrm{Irr}(\theta, K)(x)$. For any $\sigma \in \mathrm{Hom}_K(L, \Omega)$, we have $\sigma\left(\mathrm{Irr}(\theta, K)(\theta)\right) = \mathrm{Irr}(\theta, K)$ $(\sigma(\theta)) = 0$. This means that $\sigma(\theta) = \theta_i$ for some $i = 1, \ldots, n$. This then implies $\#\mathrm{Hom}_K(L) = n$. (Any $\tau \in \mathrm{Hom}_K(L, \Omega)$ is completely determined by the image of θ under τ because τ fixes K.)

Moreover, if L/K is normal, then σ induces an isomorphism $L \cong L$. Note that $L = K(\theta) \cong K(\theta_i)$ for any $i = 1, \ldots, n$ because these fields are isomorphic to $K[X]/\left(\mathrm{Irr}(\theta, K)\right)$. Therefore, we may take L as Ω and can write $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, \Omega)$.

Now, we can describe the fundamental theorem of Galois theory (for finite field extensions). Let L/K be a finite Galois extension of K. Then, we can write $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$. For any subgroup $H \subset \mathrm{Gal}(L/K)$ and an intermediate field M of L/K, we define

$$\begin{aligned} L^H &:= \{a \in L \mid \sigma(a) = a, \forall \sigma \in H\}, \\ G_M &:= \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(a) = a, \forall a \in M\}. \end{aligned}$$

We note that L/M is a Galois extension with $\mathrm{Gal}(L/M) = G_M$. It is not difficult to see that L^H is an intermediate field of L/K and that G_M is a subgroup of $\mathrm{Gal}(L/K)$. We can define two maps with respect to L/K. One is a map Φ from $A := \{M \subset L \mid M$ is an intermediate field of $L/K\}$ to $B := \{H \subset \mathrm{Gal}(L/K) \mid$ H is a subgroup of $\mathrm{Gal}(L/K)\}$ by $M \mapsto G_M$. The other is a map Ψ from B to A by $H \mapsto L^H$. The fundamental theorem of Galois theory is as follows:

Theorem 2.2 *Let L/K, A, B, Φ, and Ψ be as above. Then, the following statements are true:*

(1) There is a one-to-one correspondence between A and B. More precisely, Φ and Ψ are inverse maps of each other.
(2) If M_1 and M_2 are intermediate fields of L/K with $M_1 \subset M_2$, then we have $\Phi(M_2) \subset \Phi(M_1)$. Similarly, if H_1 and H_2 are subgroups of $\mathrm{Gal}(L/K)$ *with $H_1 \subset H_2$, then we have $\Psi(H_2) \subset \Psi(H_1)$.*
(3) Let M_1, M_2, H_1 and H_2 be as in (2). Then, we have $(H_2 : H_1) = \#H_2/H_1 = [\Psi(H_1) : \Psi(H_2)]$ and $[M_2 : M_1] = (\Phi(M_1) : \Phi(M_2))$.
(4) A subfield M of L/K is a Galois extension of K if and only if $G_M = \Phi(M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$*. Moreover, if $G_M =$* $\mathrm{Gal}(L/M)$ *is a normal subgroup of* $\mathrm{Gal}(L/K)$*, then we have*

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \cong Gal(M/K).$$

In particular, if $\mathrm{Gal}(L/K)$ *is an abelian group, then all subfields of L/K are Galois extensions of K.*

For a proof of Theorem 2.2, see [18] for example. (It is easy to prove (2) of Theorem 2.2 from the definitions of Φ and Ψ.)

2.2.2.3 Number Fields

To describe Ring-LWE and decomposition fields, which play central roles in this paper, we need some notations 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 $f \in \mathbb{Z}[x]$ such that $f(a) = 0$. 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 products 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 $O_K/\mathcal{P}_i = \mathbb{F}_{p^d}$ 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 $i \neq j$. This induces an isomorphism of rings $O_K/\mathcal{P}_1 \cdots \mathcal{P}_m \cong O_K/\mathcal{P}_1 \times \cdots \times O_K/\mathcal{P}_m$.

2.2.2.4 Ring-LWE Problem

Let K and O_K be as above. Let χ_{secret} and χ_{error} be probabilistic distributions on O_K and let p be 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 $U(X)$ as the uniform distribution on X. The Ring-LWE distribution on $O_{K,p}$, denoted by $\text{RLWE}_{K,p,\chi_{\text{error}},\chi_{\text{sec}}}$, is defined as a probabilistic distribution that takes elements of the form $(a, as + e)$ with $a \leftarrow U(O_{K,p})$, $s \leftarrow \chi_{\text{secret}}$, and with $e \leftarrow \chi_{\text{error}}$. The Ring-LWE problem has two variants. One is the problem of distinguishing $\text{RLWE}_{K,p,\chi_{\text{error}},\chi_{\text{sec}}}$ from $U(O_{K,p} \times O_{K,p})$, which is called the decision Ring-LWE problem. The other is a problem of finding $s \in O_{K,p}$, given arbitrarily many samples $(a_i, a_i s + e_i) \in O_{K,p} \times O_{K,p}$ chosen according to $\text{RLWE}_{K,p,\chi_{\text{error}},\chi_{\text{sec}}}$, which is called the search Ring-LWE problem.

The Ring-LWE problem is expected to be computationally difficult even with quantum computers. It is proved that the decision Ring-LWE problem is equivalent to the search problem 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.

2.2.3 Ring-LWE over Cyclotomic and Decomposition Fields

In this section, we describe why Arita and Handa proposed the use of decomposition fields as the underlying number fields of Ring-LWE to construct efficient HE schemes.

2.2.3.1 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 mth root of unity and $n = \varphi(m)$, where $\varphi(\cdot)$ denotes Euler's totient function. Then, $K := \mathbb{Q}(\zeta_m)$ is called the mth 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. Here, $K/\mathbb{Q}$

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 the 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 that is unramified in L and satisfies $pO_L = \mathcal{P}_1 \cdots \mathcal{P}_g$, where the $\mathcal{P}_i$'s are the prime ideals of O_L. Let G_Z be a subgroup of G that consists of all elements ρ fixing all $\mathcal{P}_i$, i.e., $\rho(\mathcal{P}_i) = \mathcal{P}_i$ for $1 \leq i \leq g$, and Z is 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 the ring of integers of Z is $O_Z = O_L \cap Z$. Suppose $\mathfrak{p}_i := O_Z \cap \mathcal{P}_i$. Then, we have $pO_Z = \mathfrak{p}_1 \cdots \mathfrak{p}_g$. A generator σ of G_Z acts on $O_L/\mathcal{P}_i \cong \mathbb{F}_{p^d}$ as the pth Frobenius map, i.e., $\sigma(x) \equiv x^p \pmod{\mathcal{P}_i}$ for all $x \in O_L$ and for $1 \leq i \leq g$. Therefore, we have $O_Z/\mathfrak{p}_i \cong \mathbb{F}_p$ and $[Z : \mathbb{Q}] = g$, i.e., p splits completely in Z.

2.2.3.2 Cyclotomic Fields Versus Decomposition Fields

Let K, L, and Z be as above and p be a prime number that is unramified in K and splits completely in Z. Assume that L is the ℓth cyclotomic field with a prime number ℓ. As we mentioned in Sect. 2.2.1, cyclotomic fields are usually used as the 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 Sect. 2.2.2.4 are satisfied because both $K/\mathbb{Q}$ and $Z/\mathbb{Q}$ are Galois extensions.

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

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

Remark 2.1 1. If $p \equiv 1 \pmod{m}$, then p splits completely in K (recall that K is the mth cyclotomic field), and then there is no advantage to 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 applications.

2. By the Hensel lifting technique, for $r > 1$ and $q := p^r$, we have $O_{Z,q} \cong \mathbb{Z}/q\mathbb{Z} \times \cdots \times \mathbb{Z}/q\mathbb{Z}$.

2.2.4 *Our Experimental Analysis*

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

2.2.4.1 Lattice Attack in Our Experiments

In our experiments, we reduce the search Ring-LWE to a 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 this approach briefly in the case of decomposition fields. Let O_Z and p be as in Sect. 2.2.3.1. 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, as shown in [1, Lemma 3]. We 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 variance σ^2.

We 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 to use Ring-LWE to construct HE schemes, the value σ_s and σ_e should be sufficiently small because the ℓ_∞-norm $\|\mathbf{s}\|_\infty$ directly affects the growth of noise after multiplication. In our experiments, we set $\sigma_\mathrm{s} = 1$ and $\sigma_\mathrm{e}^2 = 8$ according to [14]. By comparing all coefficients of both sides, we get $\mathbf{A}\mathbf{s} + \mathbf{e} = (b_1, \ldots, b_g)^t = \mathbf{b}$, 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 the $g \times g$ identity matrix. From the choice of s_i's and e_i's, our target vector $(\mathbf{s}\ \ \mathbf{e})^t$ is a very short vector from among all solutions to $A'\mathbf{y} = \mathbf{b}$, and thus, we can expect that our target vector can be found by solving the (approximate) CVP on the lattice $\mathcal{L} = \{\mathbf{x} \in \mathbb{Z}^{2g} \mid \mathbf{A}'\mathbf{x} = \mathbf{0} \pmod{q}\}$ and on $\mathbf{w} := (\mathbf{0}\ \ \mathbf{b})^t$, which is a solution to $\mathbf{A}'\mathbf{y} = \mathbf{b}$.

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 $\mathbf{B}$ using the LLL and BKZ algorithms with block size $\beta = 10$. (In practice, β should be 10 or 20.) Let $\mathbf{B}_{\text{red}}$ be a reduced basis of $\mathbf{B}$. We input $\mathbf{B}_{\text{red}}$ and $\mathbf{w}$ to Babai's nearest plane algorithm. The quality of the results of Babai's nearest plane algorithm depends on the quality of the basis reduction algorithms used to compute the reduced input bases, and thus, we compute the root Hermite factor for $\mathbf{B}_{\text{red}}$.

In contrast, 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 input, and we set $M = 1$ according to the result of an experimental study on Kannan's embedding technique for LWE [20]. We also use the LLL and BKZ algorithms with $\beta = 10$ to reduce the above basis matrix.

Remark 2.2 In the case of 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 2.3 For $1 \leq r' < r$ and $q' := p^{r'}$, we can obtain samples of $\text{RLWE}_{K,q',\chi_{\text{error}},\chi_{\text{sec}}}$ from samples of $\text{RLWE}_{K,q,\chi_{\text{error}},\chi_{\text{sec}}}$ by a natural projection $O_{Z,q} \to O_{Z,q'}$ by $a \mapsto a \pmod{q'}$. In our experiments, we use a small r' to reduce running times. In our experimental results, we only show r'.

2.2.4.2 Experimental Results

We used a computer with 2.00 GHz CPUs (Intel(R) Xeon(R) CPU E7-4830 v4 (2.00GHz)x111) and 3 TB memory to conduct the experiments. The OS was Ubuntu 16.04.4. We implemented the code for sampling Ring-LWE instances in SageMath version 7.5.1. We also used Magma V2.23-1 to execute lattice attacks. We took 100 samples and performed lattice attacks on them.

We show our experimental results in Tables 2.1 and 2.2 for $p = 2$. Table 2.1 shows that there is not a considerable difference between the experimental results of cyclotomic fields and those for decomposition fields. In contrast, Table 2.2 shows that Kannan's embedding technique is much faster than Babai's nearest plane algorithm.

This implies that the behaviors of the basis reduction algorithms heavily depend on the structure of the input lattices. This is a reason why experimental analyses are necessary for ensuring the security of lattice-based schemes (or other problems). Table 2.2 also shows that the running times for the decomposition fields become longer than those for cyclotomic fields as g (or $\ell - 1$) increases. Therefore, we can expect that decomposition fields provide Ring-LWE that is more secure against the lattice attacks described in Sect. 2.2.4.1 than ℓth cyclotomic fields because the ranks of the lattices occurring in our experiments are very low compared to the ranks of lattices used in practice. This means that we can use decomposition fields with lower extension degrees than would be needed for ℓth cyclotomic fields, and the use of such number fields makes Ring-LWE-based schemes more efficient. Therefore, as a

Table 2.1 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
Lattice rank	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 root Hermite factor	1.014	1.014	1.014	1.014	1.014	1.014	1.020	1.020	1.020	1.020	1.089	1.021
Average running time (s)	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 times (%)	–	123.2	–	109.0	–	102.9	–	91.8	–	105.7	–	102.6

The columns for which the values g are indicated show the results for decomposition fields; the other columns show the results for cyclotomic fields

The "ratio of running times" is the ratio of the average of running time for a decomposition field to that of a cyclotomic field for each g

Table 2.2 Experimental results on Kannan's embedding technique for $p = 2$

ℓ	59	16183	73	2089	83	4051	131	5419	173	14449	227	9719
g	–	58	–	72	–	81	–	129	–	172	–	226
Lattice rank	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 running time (s)	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 times (%)	–	103.5	–	112.7	–	105.7	–	117.9	–	129.7	–	116.6

We computed the root Hermite factor for the reduced bases, but we do not show them because the success rates in these results are 100%

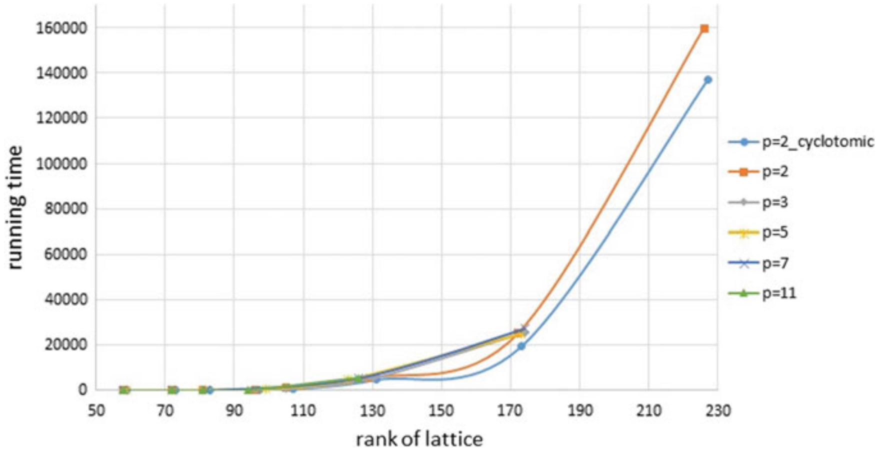

Fig. 2.2 Average running times of Kannan's embedding technique for cyclotomic and decomposition fields with respect to $p = 2, 3, 5, 7, 11$. The label "$p = 2$_cyclotomic" indicates the results of the cyclotomic fields shown in Table 2.2, and the other labels indicate the results for decomposition fields with respect to the corresponding prime numbers p. We set modulus parameter $q = p^{r'}$ so that these moduli have the almost same bit sizes. We only show the average results on at least 10 samples

result of our analysis, we believe that Ring-LWE over decomposition fields can be used to construct more efficient HE schemes.

We also conducted experiments for decomposition fields with respect to $p = 3, 5, 7, 11$ to find decomposition fields that provide weak Ring-LWE instances (Fig. 2.2). In these experiments, we could not find decomposition fields that provide weak Ring-LWE.

References

1. S. Arita, S. Handa, Subring homomorphic encryption, in *Proceedings of ICISC 2017*. LNCS, vol. 10779 (Springer, Cham, 2018), pp. 112–136
2. L. Babai, On Lovász' Lattice reduction and the nearest lattice point problem. Combinatorica **6**(1), 1–13 (1986). Springer (Preliminary version in STACS 1985)
3. G. Bonnoron, C. Fontaine, A note on ring-LWE security in the case of fully homomorphic encryption, in *Proceedings of INDOCRYPT 2017*. LNCS, vol. 10698 (Springer, Cham, 2017), pp. 27–43
4. Z. Brakerski, C. Gentry, V. Vaikuntanathan, (Leveled) fully homomorphic encryption without bootstrapping, in *Proceedings of ITCS 2012* (ACM New York, NY, USA, 2012), pp. 309–325
5. Z. Brakerski, V. Vaikuntanathan, Fully homomorphic encryption from ring-LWE and security for key dependent messages, in *Proceedings of CRYPTO 2011*. LNCS, vol. 6841 (Springer, Berlin, Heidelberg, 2011), pp. 505–524
6. H. Chen, K. Lauter, K.E. Stange, Security considerations for Galois non-dual RLWE families, in *Proceedings of SAC 2016*. LNCS, vol. 10532 (Springer, Cham, 2016), pp. 443–462

7. Y. Chen, P.Q. Nguyen, BKZ 2.0: better lattice security estimates, in *Proceedings of ASIACRYPT 2011*. LNCS, vol. 7073 (Springer, Berlin, Heidelberg, 2011), pp. 1–20
8. D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. **10**(4), 233–260 (1997). Springer
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 *Proceedings of EUROCRYPT 2008*. LNCS, vol. 4965. Springer, Berlin, Heidelberg, 2008), pp. 31–51
11. S. Halevi, V. Shoup, Algorithms in HElib, in *Proceedings of CRYPTO 2014*. LNCS, vol. 8616. (Springer, Berlin, Heidelberg, 2014), pp. 554–571
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, Math. Ann. **261**(4), 515–534 (1982). Springer
14. T. Lepoint, M. Naehrig, A comparison of the homomorphic encryption schemes FV and YASHE, in *Proceedings of AFRICACRYPT 2014*. LNCS, vol 8469. (Springer, Cham, 2014), pp. 318–335
15. V. Lyubashevsky, C. Peikert, O. Regev, On ideal lattices and learning with errors over rings, in *Proceedings of EUROCRYPT 2010*. LNCS, vol. 6110 (Springer, Berlin, Heidelberg, 2010), pp. 1–23
16. V. Lyubashevsky, C. Peikert, O. Regev, On ideal lattices and learning with errors over rings. J. ACM (JACM) **60**(6), 43:1–43:35 (2013), ACM New York, NY, USA
17. V. Lyubashevsky, C. Peikert, O. Regev, A toolkit for ring-LWE cryptography, in *Proceedings of EUROCRYPT 2013*. LNCS, vol. 7881 (Springer, Berlin, Heidelberg, 2013), pp. 35–54
18. P. Morandi, Field and galois theory, *Graduate Texts in Mathematics*, vol. 167 (Springer-Verlag, New York, 1996)
19. C.P. Schnorr, M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems. Math. Progr. **66**(1-3), 181–199 (1994). Springer
20. Y. Wang, Y. Aono, T. Takagi, An experimental study of Kannan's embedding technique for the search LWE problem, in: *Proceedings of ICICS 2017*. LNCS, vol. 10631 (Springer, Cham, 2018), pp. 541–553
21. D.V. Bailey, C. Paar, Optimal extension fields for fast arithmetic in public-key algorithms, in *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings* (Springer, 1998), pp. 472–485
22. D.J. Bernstein, Curve25519: new diffie-hellman speed records. in *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings* (Springer, 2006) pp. 207–228
23. D.J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, Twisted Edwards curves. IACR Cryptology ePrint Archive **2008**, 13 (2008)
24. D.J. Bernstein, T. Lange, Faster addition and doubling on elliptic curves. IACR Cryptology ePrint Archive **2007**, 286 (2007)
25. C. Diem, On the discrete logarithm problem in class groups of curves. Math. Comput. **80**(273), 443–475 (2011)
26. J. Faugère, P. Gaudry, L. Huot, G. Renault, Using symmetries in the index calculus for elliptic curves discrete logarithm. J. Cryptol. **27**(4), 595–635 (2014)
27. J. Faugère, L. Perret, C. Petit, G. Renault, Improving the complexity of index calculus algorithms in elliptic curves over binary fields. in *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings* (Springer, 2012) pp. 27–44
28. S.D. Galbraith, P. Gaudry, Recent progress on the elliptic curve discrete logarithm problem. Des. Codes Cryptogr. **78**(1), 51–72 (2016)
29. S.D. Galbraith, S.W. Gebregiyorgis, Summation polynomial algorithms for elliptic curves in characteristic two. in *Progress in Cryptology - INDOCRYPT 2014 - 15th International*

Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings (Springer, 2014), pp. 409–427

30. P. Gaudry, Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. J. Symb. Comput. **44**(12), 1690–1702 (2009)
31. Y. Huang, C. Petit, N. Shinohara, T. Takagi, Improvement of Faugère et al.'s Method to Solve ECDLP, in *Advances in Information and Computer Security - 8th International Workshop on Security, IWSEC 2013, Okinawa, Japan, November 18-20, 2013, Proceedings* (Springer, 2013), pp. 115–132
32. P.L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization. Math. Comput. **48**, 243–264 (1987). URLhttp://links.jstor.org/sici?sici=0025-5718(198701)48:177<243:STPAEC>2.0.CO;2-3
33. C. Petit, J. Quisquater, On polynomial systems arising from a weil descent. IACR Cryptology ePrint Archive **2012**, 146 (2012)
34. J.M. Pollard, Monte Carlo methods for index computation mod p. Math. Comput. **32**, 918–924 (1978)
35. I.A. Semaev, Summation polynomials and the discrete logarithm problem on elliptic curves. IACR Cryptology ePrint Archive **2004**, 31 (2004)
36. N.P. Smart, The hessian form of an elliptic curve, in *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, number Generators. (Springer, 2001), pp. 118–125