Memoirs of the Faculty of Engineering, Okayama University, Vol. 47, pp. 19-24, January 2013

Representation of Torsion Points on Pairing Curves of Embedding Degree 1

Yasuyuki NOGAMI*
Graduate School of Natural Science and Technology, Okayama University
3-1-1, Tsushima-naka, Kita-ku, Okayama, Okayama 700-8530, Japan

Taichi SUMO*
Graduate School of Natural Science and Technology, Okayama University
3-1-1, Tsushima-naka, Kita-ku, Okayama, Okayama 700-8530, Japan

(Received November 30, 2012)

Recent efficient pairings such as Ate pairing use two efficient rational point subgroups such that $\pi(P) = P$ and $\pi(Q) = [p]Q$, where π, p, P, and Q are the Frobenius map for rational point, the characteristic of definition field, and torsion points for *pairing*, respectively. This relation accelerates not only *pairing* but also pairing–related operations such as scalar multiplications. It holds in the case that the embedding degree k divides $r-1$, where r is the order of torsion rational points. Thus, such a case has been well studied. Alternatively, this paper focuses on the case that the degree divides $r+1$ but does not divide $r-1$. Then, this paper shows a multiplicative representation for r–torsion points based on the fact that the characteristic polynomial $f(\pi)$ becomes irreducible over $\mathbb{F}_r$ for which π also plays a role of variable.

keywords pairing–friendly curve, torsion point, group structure, rank

1 Introduction

Pairing–based cryptographies have attracted many researchers in these years since it realizes some innovative cryptographic applications such as ID–based cryptography [1] and group signature authentication [2]. Pairing is a bilinear map between two rational point groups on a certain *pairing–friendly* curve and a multiplicative group in a certain finite field, for which rational points need to form a *torsion* group structure of rank 2 [3]. Since it takes a lot of calculation time compared to other operations such as a scalar multiplication for rational point, Ate pairing [4], for example, applies two special rational point subgroups for accelerating *pairing.* The two *special* rational point groups are identified by the factorization of the characteristic polynomial of pairing–friendly curve. In detail, let $E(\mathbb{F}_p)$ be a pairing–friendly curve over prime field $\mathbb{F}_p$ of embedding degree k and thus $E(\mathbb{F}_{p^k})$ has a torsion group structure, where p is the characteristic. Then, let t be the Frobenius trace of $E(\mathbb{F}_p)$ and r be the order of one cyclic group in the torsion group, the characteristic polynomial $f(\pi)$ is given by and factorized over $\mathbb{F}_r$ as

$$\begin{aligned} f(\pi) &= \pi^2 - t\pi + p \\ &\equiv (\pi-1)(\pi-p) \mod r, \end{aligned} \tag{1}$$

where π is Frobenius map for rational points in $E(\mathbb{F}_{p^k})$ with respect to $\mathbb{F}_p$. Ate pairing applies the kernels of the maps $(\pi-1)$ and $(\pi-p)$. Then, several efficient techniques are available not only for accelerating *pairing* [4] but also scalar multiplications [5], [6]. Thus, these special groups of r–torsion points have play important roles and been well researched. For those efficiencies, the embedding degree k and the group order r need to satisfy $k \mid (r-1)$ and implicitly $k > 1$. In what follows, let r be a prime, $E(\mathbb{F}_{p^k})[r]$ denotes the torsion group of which every rational point has the order r.

This paper alternatively deals with *ordinary*, in other words *non–supersingular*, pairing–friendly elliptic curve $E(\mathbb{F}_{p^n})$ such that $n \nmid (r-1)$ especially with the *minimal embedding field* $\mathbb{F}_{p^l}$, $l = 1, 2$ [8]. The motivation of this research comes from the fact that it has not been well researched [7], [9] and thus there are some *unclear* properties especially for its torsion group structure. First, this paper reviews that the characteristic polynomial $f(\pi)$ becomes an irreducible polynomial over $\mathbb{F}_r$ with respect to π. In other words, $f(\pi)$ cannot be factorized to the form of Eq.(1) with some scalars modulo r for which π also plays a role of *variable.* Then, using $f(\pi)$ as the modular polynomial, this paper gives a multiplicative representation of every r–torsion point for which two cases of definition field $\mathbb{F}_p$ and $\mathbb{F}_{p^n}$ are considered, where n is a certain prime number. In de-

*{nogami,sumou}@trans.cne.okayama-u.ac.jp

tail for the former case, *skew* Frobenius map $\hat{\pi}_d$ with *twist* technique of degree $d = 3$, 4, and 6 is applied [5] in which the *twisted* characteristic polynomial $f'(\hat{\pi}_d)$ is applied as the modular polynomial. Then, every r–torsion point is represented in the same manner of elements in the second extension field $\mathbb{F}_{r^2}$ such as $([a_0] + [a_1]\pi)P$, $P \in E(\mathbb{F}_{p^n})[r]$, where $E(\mathbb{F}_{p^n})[r]$ denotes the set of r–torsion points and $a_0, a_1 \in \mathbb{F}_r$. Thus, they form groups with respect to not only elliptic curve addition but also a *multiplicative operation* defined as

$$P_{\mathcal{A}} = [\mathcal{A}]P = ([a_0] + [a_1]\pi)P, \quad (2a)$$

$$P_{\mathcal{B}} = [\mathcal{B}]P = ([b_0] + [b_1]\pi)P, \quad (2b)$$

$$P_{\mathcal{C}} = [\mathcal{C}]P = [\mathcal{A} \cdot \mathcal{B}]P, \quad (2c)$$

where $a_0, a_1, b_0, b_1 \in \mathbb{F}_r$, $\mathcal{C} \equiv \mathcal{A} \cdot \mathcal{B}$ modulo $f(\pi)$. It will be easily induced from *complex number* field. Then, this paper also shows some properties and how to prepare such pairing–friendly elliptic curves. According to the technical term *minimal embedding field* proposed in [8], it is shown that the cases considered in this paper have the *minimal embedding field* $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$. Restricting d is equal to 3 and n is an odd prime, this paper especially deals with the cases of *minimal embedding field* $\mathbb{F}_p$.

Throughout this paper, let p, r, and n be different prime numbers as the characteristic of finite field, the order of group, and the extension degree, respectively. Let d be the twist degree. Then, $\mathbb{F}_p$, $\mathbb{F}_{p^d}$, and $\mathbb{F}_{p^n}$ respectively denote a prime field, extension fields of extension degrees d and n, respectively. In addition, this paper especially deals with *ordinary*, in other words *non–supersingular*, elliptic curves.

2 Fundamentals

On the viewpoint of *torsion* group, this section briefly reviews elliptic curve, pairing–friendly elliptic curve, minimal embedding field, twist, Frobenius map π, *skew* Frobenius map $\hat{\pi}_d$, characteristic polynomials $f(\pi)$ and $f'(\hat{\pi}_d)$, and some conventional researches.

2.1 Elliptic curve, its order, and Frobenius map

Let E be an elliptic curve defined over $\mathbb{F}_p$ as

$$E \;:\; y^2 = x^3 + ax + b, \; a, b \in \mathbb{F}_p. \quad (3)$$

The set of rational points including the *infinity point* $\mathcal{O}$ on the curve forms an additive Abelian group. It is denoted by $E(\mathbb{F}_p)$. When the definition field is its extension field $\mathbb{F}_{p^n}$, rational points on the curve E also forms an additive Abelian group denoted by $E(\mathbb{F}_{p^n})$. In the case that the extension degree $n > 1$, since the coefficient field $\mathbb{F}_p$ of the elliptic curve E is a proper subfield of the definition field $\mathbb{F}_{p^n}$, $E(\mathbb{F}_{p^n})$ is especially called *subfield* elliptic curve.

For rational points $R(x_R, y_R) \in E(\mathbb{F}_{p^n})$, where x_R, y_R are elements in $\mathbb{F}_{p^n}$, consider Frobenius map π with respect to the coefficient field $\mathbb{F}_p$. In detail, π becomes an endomorphism defined by

$$\begin{aligned} \pi \quad : \quad & E(\mathbb{F}_{p^n}) \to E(\mathbb{F}_{p^n}) \\ & (x_R, y_R) \mapsto (x_R^p, y_R^p). \end{aligned} \quad (4)$$

Thus, $\pi^n = 1$. On the other hand, it is well known that every rational point R in $E(\mathbb{F}_{p^n})$ satisfies

$$(\pi^2 - [t]\pi + [p])R = \mathcal{O}, \quad (5)$$

and the order $\#E(\mathbb{F}_p)$ is written by

$$\#E(\mathbb{F}_p) = p + 1 - t, \quad (6)$$

where t denotes the Frobenius trace of $E(\mathbb{F}_p)$. Then, consider a polynomial $f(\pi)$ with respect to the preceding Frobenius map π as follows.

$$f(\pi) = \pi^2 - t\pi + p, \quad (7)$$

it is often called *characteristic polynomial*. Since p is a prime number and $|t| \leq 2\sqrt{p}$ [3], $f(\pi)$ is obviously irreducible over integers. Then, according to the Weil's theorem [3], the order $\#E(\mathbb{F}_{p^n})$ is given by

$$\#E(\mathbb{F}_{p^n}) = p^n + 1 - t_n, \quad (8)$$

where $t_n = \alpha^n + \beta^n$ for which α and β are *conjugate* complex numbers such that

$$f(\alpha) = f(\beta) = 0. \quad (9)$$

Using Dickson's polynomial [10], t_n is recursively determined from $p = \alpha\beta$ and $t_1 = \alpha + \beta$. In addition, it is easily found that $\#E(\mathbb{F}_p)$ divides $\#E(\mathbb{F}_{p^n})$. It ensures that $E(\mathbb{F}_p)$ is a subgroup of $E(\mathbb{F}_{p^n})$. If the extension degree n is a prime, the period of Frobenius map π for rational points becomes 1 or n. The former period corresponds to the rational points in $E(\mathbb{F}_p)$.

In what follows, let the extension degree n be a prime number for making the discussions simple. Let r be a prime such that $r \mid \#E(\mathbb{F}_{p^n})$ and $r^2 \nmid \#E(\mathbb{F}_{p^n})$, then the subgroup of rational points of order r denoted by $E(\mathbb{F}_{p^n})[r]$ exists in $E(\mathbb{F}_{p^n})$ as a cyclic group. If $r \nmid E(\mathbb{F}_p)$, it is found that the extension degree n divides $r - 1$ because n is the period of the map [11].

2.2 Pairing–friendly elliptic curve

Let r be a prime such that $r \mid \#E(\mathbb{F}_p)$. In general, the smallest positive integer k such that r divides $p^k - 1$ is called *embedding degree*. When k is larger than 1, it is well–known that $E(\mathbb{F}_{p^k})[r]$ consists of *torsion* points of order r under $r^2 \mid E(\mathbb{F}_{p^k})$ [3]. In detail,

- there are $r^2 - 1$ points of order r,
- $E(\mathbb{F}_{p^k})[r]$ forms a rank 2 group structure,
- there are $r + 1$ cyclic groups order r in $E(\mathbb{F}_{p^k})[r]$,
- one of the $r + 1$ groups belongs to $E(\mathbb{F}_p)$.

In addition, since $r \mid \#E(\mathbb{F}_p)$, the characteristic polynomial Eq.(7) modulo r becomes reducible as

$$f(\pi) \equiv (\pi - 1)(\pi - p) \pmod{r}. \tag{10}$$

Among the $r+1$ cyclic groups of order r in $E(\mathbb{F}_{p^k})[r]$, according to [3], Eq.(10) implicitly shows the existence of the cyclic subgroup $\mathbb{C}^{[p]}$ such that

$$(\pi - [p])A = \mathcal{O},\ A \in \mathbb{C}^{[p]}. \tag{11}$$

It is just understood that $\mathbb{C}^{[p]} \not\subset E(\mathbb{F}_p)$. Since Eq.(11) means that a scalar multiplication $[p]A$ is easily determined by a Frobenius map $\pi(A)$, pairing–based cryptographies mostly apply this efficiency for accelerating pairing calculations, scalar multiplications, and exponentiations [4], [6]. Alternatively, this paper deals with some cases that the characteristic polynomial becomes irreducible modulo r.

In the case that embedding degree $k = 1$ with *ordinary* pairing–friendly curves, there are some *unclear* properties [7] though some researchers have studied [12] and there are some pairing–based applications that uses composite order pairing–friendly curves of embedding degree $k = 1$ [13]. Especially, if the curve has some *twisted* variants introduced in the next section, the same efficiencies of Eq.(11) are available together with *skew* Frobenius map [14].

2.3 Minimal embedding field [8]

The calculation result of a pairing of group order r becomes a certain non–zero element of the same order r in the multiplicative subgroup of a certain extension field $\mathbb{F}_{p^l}$ such that

$$r \mid (p^l - 1) \text{ but } r \nmid (p^i - 1),\ 0 \le i < l. \tag{12}$$

Let the embedding degree of pairing be k, the extension degree l of $\mathbb{F}_{p^l}$ is equal to k in general. For example, in the case of Barreto–Naehrig curve, $k = l = 12$ [15]. However, l sometimes becomes smaller than k. Thus, Hirasawa et al. [8] have especially named the preceding $\mathbb{F}_{p^l}$ *minimal embedding field*. This paper deals with the case that the *minimal embedding field* $\mathbb{F}_{p^l}$ is the prime field $\mathbb{F}_p$ and accordingly $r \mid (p-1)$.

2.4 Twists and *skew* Frobenius map

Let the twist degree for elliptic curve $E(\mathbb{F}_p)$ be d such as $2, 3, 4$, and 6, then its twisted curve E' defined over the extension field $\mathbb{F}_{p^d}$ has its isomorphic subgroup [4], where $d \mid (p-1)$. Let ψ_d be the isomorphic map from $E(\mathbb{F}_p)$ to the isomorphic subgroup of order $\#E(\mathbb{F}_p)$ in $E'(\mathbb{F}_{p^d})$ [4], then *skew* Frobenius map $\hat{\pi}_d$ for rational points in $E(\mathbb{F}_p)$ is defined by $\hat{\pi}_d = \psi_d^{-1}\pi\psi_d$ [5]. Thus, *skew* Frobenius map satisfies $\hat{\pi}_d^d = 1$. Since $\hat{\pi}_2$ is just the *negation* map [11], this paper focuses on only the cases that $d = 3$, 4, and 6. These twists are available for some special forms of curve as

$$d = 4 \ :\ y^2 = x^3 + ax, \tag{13}$$
$$d = 3, 6 \ :\ y^2 = x^3 + b, \tag{14}$$

where $a, b \in \mathbb{F}_p$. In what follows, these curves are denoted by E_d and thus $\hat{\pi}_d$ is available on $E_d(\mathbb{F}_p)$.

For example, in the case that the twist degree d is equal to 3, the twisted curve E_3 and the skew Frobenius map $\hat{\pi}_3$ is given as follows [5].

$$E_d \ :\ y^2 = x^3 + bv, \tag{15}$$

where v is a certain cubic non residue in $\mathbb{F}_p$. Then, the skew Frobenius map $\hat{\pi}_3$ for $R \in E(\mathbb{F}_p)$ is given by

$$\begin{aligned} \hat{\pi}_3 \quad : \quad & E(\mathbb{F}_p) \to E(\mathbb{F}_p) \\ & (x_R, y_R) \mapsto (\epsilon x_R, y_R), \end{aligned} \tag{16}$$

where ϵ is a primitive cubic root of unity that belongs to $\mathbb{F}_r$ under $3 \mid (p-1)$.

Consider a prime number r such that $r \mid \#E_d(\mathbb{F}_p)$ and $d \mid (r-1)$. Let t' and λ_d be the Frobenius trace of its twisted curve $E'_d(\mathbb{F}_p)$ and a primitive d–th root of unity modulo r, respectively. The *twisted* characteristic polynomial $f'(\hat{\pi}_d)$ is given by and factorized as

$$\begin{aligned} f'(\hat{\pi}_d) &= \hat{\pi}_d^2 - t'\hat{\pi}_d + p && \text{(17a)} \\ &\equiv (\hat{\pi}_d - \lambda_d)(\hat{\pi}_d - \lambda_d^{-1}) \pmod{r}. && \text{(17b)} \end{aligned}$$

Since ${}^{\forall}R \in E_d(\mathbb{F}_p)$ satisfies

$$(\hat{\pi}_d^d - [1])R = f'(\hat{\pi}_d)R = \mathcal{O}, \tag{18}$$

the factorization Eq.(17b) is also found as the greatest common divisor of $\hat{\pi}_d^d - 1$ and $f'(\hat{\pi}_d)$). If $E_d(\mathbb{F}_p)[r]$ is a cyclic group of order r, in other words rank 1, an arbitrary rational point P in $E_d(\mathbb{F}_p)[r]$ satisfies

$$(\hat{\pi}_d - \lambda_d)P = \mathcal{O} \ \text{ or } \ (\hat{\pi}_d - \lambda_d^{-1})P = \mathcal{O}, \tag{19}$$

where it is uniquely determined by the isomorphic map ψ_d [14]. If $E_d(\mathbb{F}_p)[r]$ consists of torsion points of order r with rank 2, in the same of **Sec.**2.2, among the $r+1$ cyclic groups of order r in $E_d(\mathbb{F}_p)[r]$, Eq.(19) shows the existence of cyclic subgroups $\mathbb{C}^{[\lambda_d]}$ and $\mathbb{C}^{[\lambda_d^{-1}]}$ such that

$$\begin{aligned} (\hat{\pi}_d - [\lambda_d])B &= \mathcal{O},\ B \in \mathbb{C}^{[\lambda_d]}, && \text{(20a)} \\ (\hat{\pi}_d - [\lambda_d^{-1}])C &= \mathcal{O},\ C \in \mathbb{C}^{[\lambda_d^{-1}]}. && \text{(20b)} \end{aligned}$$

Then, these relations are available for accelerating some pairing– related calculations such as pairing calculation and scalar multiplication [5].

2.5 Viewpoint of ECDLP

While *pairing* for cryptographic applications such as ID–based cryptography [1] has been well studied in these years, Menezes–Okamoto–Vanstone (MOV) and Frey–Rück (FR) reductions [3] have been well known for attacking elliptic curve discrete logarithm problem (ECDLP) on pairing–friendly curve. In the case that the embedding degree k is small, they successfully solve the ECDLPs in the multiplicative group of the *embedded* definition field $\mathbb{F}_{p^k}$. Let $e(,)$ be the Weil pairing [3], the following properties are known :

- $e(P, P) = 1$,
- $e(P, Q) = e(Q, P)^{-1}$,
- $e(P, Q + R) = e(P, Q) \cdot e(P, R)$,
- $e([a]P, [b]Q) = e(P, Q)^{ab}$, $0 \le a, b \le r - 1$,

where P, Q, and R are r–torsion points in $E(\mathbb{F}_{p^k})[r]$. For $e(P, [x]Q) = e(P, Q)^x$, the scalar x is written as

$$x = \log_{e(P,Q)} e(P, [x]Q). \tag{21}$$

If the size of $\mathbb{F}_{p^k}$ is not sufficient for security, the logarithm x will be computationally solved in the multiplicative group of order r in $\mathbb{F}^*_{p^k} = \mathbb{F}_{p^k} - \{0\}$.

2.6 Conventional researches

As previously introduced, it is quite important that the twist degree d or the extension degree n divides $r-1$ whichever the group of rational points of order r has a rank 1 or 2 group structure. Then, the calculation costs of some pairing–related operations are substantially reduced [4]–[6]. On the other hand, the other cases such that $d \nmid (r - 1)$ or $n \nmid (r - 1)$ are briefly introduced [7], [12] of which some properties have been unsolved as

- the relation of n, d, r, π, and $\hat{\pi}_d$,
- how to obtain such pairing–friendly curves [9],
- properties on self–pairings [7].

This paper considers a multiplicative extension for representing the group structure that will give some useful viewpoints for accelerating pairing–based operations and solving discrete logarithms on such pairing–friendly curves.

3 Multiplicative extension

As introduced in **Sec**.1, this paper considers the cases that *twist* degree d or *extension* degree n respectively for $E_d(\mathbb{F}_p)[r]$ or $E(\mathbb{F}_{p^n})[r]$ does not divide $r - 1$. In addition, among such cases, this paper especially focuses on the following two cases[1]:

- d is equal to 3 and divides $r + 1$,
- n is an odd prime such that $r \nmid \#E(\mathbb{F}_{p^n})$, $n \ne r$, and $n \mid (r + 1)$.

Such a curve explicitly has a *torsion* group structure, in other words it is a pairing–friendly curve. Then, this paper shows that every r–torsion rational point of order r on such a pairing–friendly curve is able to be represented as and dealt with in the same manner of an element in $\mathbb{F}_{r^2}$.

In what follows, for the simplicity of notations, the case of $E_d(\mathbb{F}_p)$ with twist degree d is mainly discussed. Just replacing d, $\hat{\pi}_d$, and $f'(\hat{\pi}_d)$ to n, π, and $f(\pi)$, respectively, the same result with $E(\mathbb{F}_{p^n})$ is obtained.

[1]There will be some other cases such that $n = r$.

3.1 Variety of group structures

When the embedding degree $k > 1$, it is found that d divides $r(r-1)$. Thus, when r is a large prime number for ensuring cryptographic security, $d \mid (r - 1)$ will be satisfied. Such a case has been well researched as introduced in **Sec**.2.2. Alternatively, there are other cases such that d divides $r^2 - 1$. Thus, this paper deals with the case that d divides $r + 1$. Then, the order r satisfies that $r \mid (p^l - 1)$, where $l = 1$ or 2. Since r is a prime number,

$$p \equiv \begin{cases} 1 & l = 1 \\ -1 & l = 2 \end{cases} \pmod r, \tag{22}$$

In brief, $p \equiv \pm 1 \pmod r$. Note here that $l = 1$ and $p \equiv 1 \pmod r$ when $d = 3$ or n is an odd prime. Then, there are the following two cases:

1. $E_d(\mathbb{F}_p)[r]$ has an r–torsion structure of rank 2,
2. $E(\mathbb{F}_{p^n})[r]$ has an r–torsion structure of rank 2 such that $r^2 \mid \#E(\mathbb{F}_{p^n})$ and $r \nmid \#E(\mathbb{F}_p)$.

They are the *target* cases of this research. For the above two cases, the embedded multiplicative group of order r belongs to the multiplicative group of $\mathbb{F}_p$. Especially for the latter case, this paper introduces a technical term *minimal embedding field* [8]. In detail, $E(\mathbb{F}_{p^n})$ is defined over $\mathbb{F}_{p^n}$ but its minimal embedding field is $\mathbb{F}_p$. In brief, it is said that both of the above two cases under $d \mid (r + 1)$ and $n \mid (r + 1)$ have the minimal embedding field $\mathbb{F}_p$, respectively. In what follows, the case of $E_d(\mathbb{F}_p)$ is mainly dealt with. Note that d and r are the periods of *skew* Frobenius map $\hat{\pi}_d$ and Frobenius map π, respectively. Thus, they are closely related to the divisibilities of $d \mid (r - 1)$ and $n \mid (r - 1)$.

3.2 Irreducibility of $f'(\hat{\pi}_d)$

In the case that d does not divide $r - 1$, $\hat{\pi}_d$ does not correspond to any scalar multiplications. It is because any primitive d–th roots of unity does not exist in $\mathbb{F}^*_r$. Thus, it is easily found that the *twisted* characteristic polynomial $f'(\hat{\pi}_d)$ becomes an irreducible polynomial of degree 2 with respect to $\hat{\pi}_d$ over $\mathbb{F}_r$ for which $\hat{\pi}_d$ also plays a role of a *variable*.

It is also understood from the viewpoint of cyclotomic polynomials. In detail, let $d = 3$ for $f'(\hat{\pi}_d)$ given by Eq.(17a), substitute $p \equiv 1 \pmod r$ and $t' \equiv -1 \pmod r$ [14], where the former is introduced in **Sec**.3.1 and the latter is obtained. Then, $f'(\hat{\pi}_d)$ in the case of $d = 3$ is given by

$$f'(\hat{\pi}_d) = f'(\hat{\pi}_3) = \hat{\pi}_3^2 + \hat{\pi}_3 + 1 \equiv 0 \pmod r. \tag{23}$$

It is the cyclotomic polynomial of period 3 with respect to $\hat{\pi}_3$. Since $3 \nmid (r - 1)$, it does not correspond to any scalar multiplication and thus it is shown that $f'(\hat{\pi}_3)$ becomes irreducible over $\mathbb{F}_r$. In what follows, this paper briefly uses the notation d such as $f'(\hat{\pi}_d)$.

Using $f'(\hat{\pi}_d)$ as the modular polynomial enables to construct the second extension field $\mathbb{F}_{r^2}$. An arbitrary element $\mathcal{A} \in \mathbb{F}_{r^2}$ is represented as

$$\mathcal{A} = a_0 + a_1\hat{\pi}_d,\ a_0, a_1 \in \mathbb{F}_r. \tag{24}$$

The above representation is *polynomial* representation with the polynomial basis $\{1, \hat{\pi}_d\}$. Thus, all of the r–torsion rational points are able to be represented in the same manner of elements $\mathbb{F}_{r^2}$.

Let $\mathcal{G} = g_0 + g_1\hat{\pi}_d,\ g_0, g_1 \in \mathbb{F}_r$ be a generator of the multiplicative *cyclic* group $\mathbb{F}^*_{r^2}$, every element in $\mathbb{F}^*_{r^2}$ is represented as a certain power $\mathcal{G}^i$, where $1 \le i \le r^2 - 1$. Accordingly, let $\mathcal{G}^i = g_{i_0} + g_{i_1}\hat{\pi}_d, g_{i_0}, g_{i_1} \in \mathbb{F}_r$, every r–torsion points in $E_d(\mathbb{F}_p)[r]$ are represented as

$$\begin{aligned}[\mathcal{G}^i]P &= ([g_{i_0}] + [g_{i_1}]\hat{\pi}_d)\, P \\ &= [g_{i_0}]P + [g_{i_1}]\hat{\pi}_d(P),\end{aligned} \tag{25}$$

where P is an arbitrary r–torsion point in $E_d(\mathbb{F}_p)[r] - \{\mathcal{O}\}$. It enables *multiplicative* representaions for r–torsion points. The property that every r–torsion point is represented as Eq.(25) corresponds to the fact that the *skew* Frobenius map $\hat{\pi}_d$ is not congruent to any scalar multiplications in $E_d(\mathbb{F}_p)[r]$ when $d \nmid (r+1)$. Thus, each cyclic subgroup of rational points of order r corresponds to the prime field $\mathbb{F}_r$.

3.2.1 Viewpoint of discrete logarithms

Consider a non–zero r–torsion point P in $E_d(\mathbb{F}_p)[r]$. Using Weil pairing $e(,)$, determine $e(P, \hat{\pi}_d(P))$ that is a certain element in the multiplicative subgroup of order r in $\mathbb{F}_p$. Let $\mathcal{A}$ be $a_0 + a_1\hat{\pi}_d$, where a_0, $a_1 \in \mathbb{F}_r$, consider an r–torsion point $P_{\mathcal{A}} = [\mathcal{A}]P$. In detail,

$$P_{\mathcal{A}} = [\mathcal{A}]P = [a_0]P + [a_1]\hat{\pi}_d(P). \tag{26}$$

According to the properties of Weil pairing,

$$e(P, P) = e(\hat{\pi}_d(P), \hat{\pi}_d(P)) = 1. \tag{27}$$

Thus, since the following relations hold,

$$\begin{aligned}e(\hat{\pi}_d(P), P_{\mathcal{A}}) &= e(\hat{\pi}_d(P), [a_0]P + [a_1]\hat{\pi}_d(P)) \\ &= e(\hat{\pi}_d(P), [a_0]P) \cdot e(\hat{\pi}_d(P), [a_1]\hat{\pi}_d(P)) \\ &= e(\hat{\pi}_d(P), P)^{a_0}, \qquad (28a) \\ e(P, P_{\mathcal{A}}) &= e(P, [a_0]P + [a_1]\hat{\pi}_d(P)) \\ &= e(P, [a_0]P) \cdot e(P, [a_1]\hat{\pi}_d(P)) \\ &= e(P, \hat{\pi}_d(P))^{a_1}, \qquad (28b)\end{aligned}$$

the coefficients a_0 and a_1 of $\mathcal{A}$ are given as

$$\begin{aligned}a_0 &= \log_{e(\hat{\pi}_d(P),P)} e(\hat{\pi}_d(P), P_{\mathcal{A}}), \qquad (29a) \\ a_1 &= \log_{e(P,\hat{\pi}_d(P))} e(P, P_{\mathcal{A}}). \qquad (29b)\end{aligned}$$

As shown above, if P and $P_{\mathcal{A}}$ are known, the coefficients a_0 and a_1 of $\mathcal{A}$ are uniquely obtained.

Let us remember that the *minimal* embedding field in this paper is $\mathbb{F}_p$. Its size for pairing–based cryptographic use with sufficient security, for example, needs to be more than 1024 bits in which the above logarithms will not be practically computed. Thus, as introduced in **Sec**.1, the above and below considerations will just give some theoretic properties of r–torsion group structures regardless of their contributions to cryptographic applications or attacks.

3.3 Multiplicative operation for r–torsion points

If the discrete logarithms are easily solved by calculating some pairings as Eqs.(29), one can newly consider a *multiplication* for r–torsions points as follows.

Let $P_{\mathcal{A}}$ and $P_{\mathcal{B}}$ be given by

$$\begin{aligned}P_{\mathcal{A}} &= [\mathcal{A}]P = ([a_0] + [a_1]\hat{\pi}_d)P, \qquad (30a) \\ P_{\mathcal{B}} &= [\mathcal{B}]P = ([b_0] + [b_1]\hat{\pi}_d)P, \qquad (30b)\end{aligned}$$

where a_0, a_1, b_0, and b_1 are in $\mathbb{F}_r$. Then, corresponding to the following $\mathcal{C} \equiv \mathcal{A} \cdot \mathcal{B}$ modulo $f'(\hat{\pi}_d)$,

$$\begin{aligned}\mathcal{C} &= (a_0 + a_1\hat{\pi}_d)(b_0 + b_1\hat{\pi}_d) \\ &= a_0b_0 + (a_1b_0 + a_0b_1)\hat{\pi}_d + a_1b_1\hat{\pi}_d^2 \\ &= (a_0b_0 - a_1b_1) + (a_1b_0 + a_0b_1 + a_1b_1)\hat{\pi}_d,\end{aligned} \tag{31}$$

where note that $f'(\hat{\pi}_d) = 0$ is given by Eq.(23). Thus, the following *multiplication* for r–torsion points $P_{\mathcal{A}}$ and $P_{\mathcal{B}}$ is explicitly defined.

$$P_{\mathcal{C}} = [\mathcal{C}]P = [\mathcal{A} \cdot \mathcal{B}]P = P_{\mathcal{A}} \cdot P_{\mathcal{B}}. \tag{32}$$

Together with the above *multiplicative law* for r–torsion points, let $\mathcal{G}$, P, and $+$ be a generator of $\mathbb{F}^*_{p^2}$, a non–zero r–torsion point, and the usual elliptic curve addition for rational points, respectively, $\left\langle \{[\mathcal{G}^i]P, \mathcal{O}\},\ +,\ \cdot \right\rangle$ forms an extension field isomorphic to $\mathbb{F}_{r^2}$. In the case that the twist degree d is equal to 3, the isomorphic relation is easily understood.

Let us consider how to carry out a multiplication for non–zero r–torsion points. Consider two r–torsion points R_1 and R_2. They will be written as follows.

$$\begin{aligned}R_1 &= [\mathcal{G}^{i_1}]P = ([r_{10}] + [r_{11}]\hat{\pi}_d)P, \qquad (33) \\ R_2 &= [\mathcal{G}^{i_2}]P = ([r_{20}] + [r_{21}]\hat{\pi}_d)P, \qquad (34)\end{aligned}$$

where $1 \le i_1, i_2 \le r^2 - 1$, $r_{10}, r_{11}, r_{20}, r_{21} \in \mathbb{F}_r$. According to Eq.(31), $R_3 = R_1 \cdot R_2$ is given as

$$\begin{aligned}R_3 &= [\mathcal{G}^{i_1+i_2}]P \\ &= (r_{10}r_{20} - r_{11}r_{21}) \\ &\quad +(r_{11}r_{20} + r_{10}r_{21} + r_{11}r_{21})\hat{\pi}_d \qquad (35a) \\ &= [\mathcal{G}^{i_3}]P = (r_{30} + r_{31}\hat{\pi}_d)P, \qquad (35b)\end{aligned}$$

where $1 \le i_3 \le r^2 - 1$, $r_{30}, r_{31} \in \mathbb{F}_r$. Note here that r_{10}, r_{11}, r_{20}, and r_{21} are possible to be determined as Eqs.(29) with P and $\hat{\pi}_d(P)$ even if they are *random* r–torsion points. After solving the logarithms, r_{30} and r_{31} are constructed as Eq.(35a) though the determination of i_3 is another discrete logarithm problem.

3.3.1 Division

Division will be defined as a multiplication by the inverse. For $P_{\mathcal{A}}$ and $P_{\mathcal{B}}$ shown in Eqs.(30), consider

$$P_{\mathcal{C}} = [\mathcal{C}]P = [\mathcal{A} \cdot \mathcal{B}^{-1}]P = P_{\mathcal{A}} \cdot P_{\mathcal{B}}^{-1}. \tag{36}$$

According to Itoh–Tsujii inversion algorithm [16] with Eq.(31), the inverse $\mathcal{B}^{-1}$ for $P_{\mathcal{B}}^{-1} = [\mathcal{B}^{-1}]P$ in the case of $d = 3$, for example, is given by

$$\begin{aligned} \mathcal{B}^{-1} &= \mathcal{B}^r \cdot (\mathcal{B} \cdot \mathcal{B}^r)^{-1} \\ &= (b_0 + b_1\hat{\pi}_3) \cdot \{(b_0 + b_1\hat{\pi}_3) \cdot (b_0 + b_1\hat{\pi}_3^r))\}^{-1} \\ &= (b_0 + b_1\hat{\pi}_3) \cdot \left\{(b_0 + b_1\hat{\pi}_3) \cdot (b_0 + b_1\hat{\pi}_3^{-1}))\right\}^{-1} \\ &= (b_0 + b_1\hat{\pi}_3) \cdot \left(b_0^2 + b_1^2 - b_0 b_1\right)^{-1} \\ &= w \cdot b_0 + w \cdot b_1\hat{\pi}_3, \end{aligned} \tag{37}$$

where $w = (b_0^2 + b_1^2 - b_0 b_1)^{-1} \bmod r$ and $\hat{\pi}_3^r = \hat{\pi}_3^{-1}$ modulo $f'(\hat{\pi}_3) = 0$. Thus, *division* is also available with the same manner of that of $\mathbb{F}_{r^2}$.

4 Future works

This paper has given a *multiplicative* representation of r–torsion rational points in the same manner of elemenets in the second extension field $\mathbb{F}_{r^2}$. Then, it was shown that all of r–torsion points except for the infinity $\mathcal{O}$ form a cyclic group in the same of the multiplicative group $\mathbb{F}_{r^2}^*$. As a future work, based on the approach shown in this paper, some cryptographic applications or attacks toghther with *pairing* will be given. Though this paper did not deal with, the case that period n divides order r will have some interesting properties.

References

[1] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," *SCIS 2000*, Jan. 2000.

[2] T. Nakanishi and N. Funabiki, "Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps," Asiacrypt 2005, LNCS, vol. 3788, pp. 443-454, 2005.

[3] H. Cohen and G. Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, *Discrete Mathematics and Its Applications*, Chapman & Hall CRC, 2005.

[4] Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa, "Integer Variable χ–based Ate Pairing," *Pairing 2008*, LNCS 5209, pp. 178–191, 2008.

[5] Y. Sakemi, Y. Nogami, K. Okeya, H. Kato, and Y. Morikawa, "Skew Frobenius Map and Efficient Scalar Multiplication for Pairing–based Cryptography," *CANS 2008*, LNCS 5339, Springer–Verlag, pp. 226-239, 2008.

[6] S. D. Galbraith and M. Scott , "Exponentiation in Pairing–Friendly Groups Using Homomorphisms," *Pairing 2008*, LNCS 5209, Springer–Verlag, pp. 211–224, 2008.

[7] N. Smart, I. F. Blake, and G. Seroussi, *Elliptic Curves in Cryptography*," LMS Lecture Note Series, Cambridge University Press, 1999.

[8] S. Hirasawa and A. Miyaji, "Elliptic Curves with a Pre–determined Embedding Degree," IEICE Tech. Rep., ISEC2008–82, pp. 63–66, 2008.

[9] K. Ohta and K. Shiota, "Construction of CM Curves Suitable for Cryptosystem from the Weil Pairing," Memoirs of the Faculty of Science, Kochi Univ., Vol. 27, No. 1, 2007.

[10] L. E. Dickson, "The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group," Ann. of Math., 1897.

[11] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curves Cryptography*, Springer–Verlag, 2004.

[12] D. Charles, "On the existence of distortion maps on ordinary elliptic curves," in Cryptology ePrint Archive, Report 2006/128, 2006.

[13] D. Boneh, A. Sahai, and B. Waters, "Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys," *Eurocrypt 2006*, LNCS 4004, pp. 573–592, 2006.

[14] T. Izuta, S. Takeuchi, K. Nishii, Y. Nogami, and Y. Morikawa, "GLV Subgroups on Non–supersingular Pairing–friendly Curves of Embedding Degree 1," *Computer Security Symposium 2010*, pp. 249 – 254, 2010.

[15] P. S. L. M. Barreto, and M. Naehrig, "Pairing–Friendly. Elliptic Curves of Prime Order," SAC2005, LNCS 3897, pp. 319-331, 2006.

[16] T. Itoh and S. Tsujii, "A Fast Algorithm for Computing Multiplicative Inverses in GF(2^m) Using Normal Bases," *Inf. and Comp.*, vol. 78, pp. 171–177, 1988.