Ordinary Pairing Friendly Curve of Embedding Degree 1 Whose Order Has Two Large Prime Factors

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

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

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

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

(Received November 16, 2010)

Recently, *composite order* pairing–based cryptographies have received much attention. The *composite order* needs to be as large as the RSA modulus. Thus, they require a certain *pairing–friendly* elliptic curve that has such a large composite order. This paper proposes an efficient algorithm for generating an *ordinary* pairing–friendly elliptic curve of the embedding degree 1 whose order has two large prime factors as the RSA modulus. In addition, the generated pairing–friendly curve has an efficient structure for the Gallant–Lambert–Vanstone (GLV) method.

1 INTRODUCTION

Recently, *composite order* pairing–based cryptographies have received much attention [2], [3], [5]. The *composite order* needs to be as large as the RSA modulus, for example 1000 bits. Thus, they require a certain *pairing–friendly* elliptic curve that has such a large composite order. On the other hand, pairing is a bilinear map from two rational point groups denoted by $\mathbb{G}_1$ and $\mathbb{G}_2$ to a multiplicative group denoted by $\mathbb{G}_3$. These three groups have the same order r and are defined over a certain extension field $\mathbb{F}^*_{p^k}$, where p is the characteristic and k is the extension degree, especially called *embedding* degree. The ratio $\rho = \lfloor \log_2 p \rfloor / \lfloor \log_2 r \rfloor$ is often used for evaluating the redundancy between the order r and the characteristic p from the security viewpoint. Since the rational points are defined over the *pairing–friendly* curve, the security of pairing–based cryptography partially depends on elliptic curve discrete logarithm problem (ECDLP) in $E(\mathbb{F}_p)$ and discrete logarithm problem (DLP) in $\mathbb{F}^*_{p^k}$. The size of the preceding *composite order* is quite redundant for the security of elliptic curve cryptography. Thus, according to [6], in order to balance the security level of the DLP at least, $\rho \cdot k$ is preferred to be small especially in the case of the preceding *large composite order pairing*. Note that, for *pairing*, the minimum of $\rho \cdot k$ is 2. This paper mainly discusses the case that the ratio $\rho \approx 2$ and the embedding degree $k = 1$.

Since *pairing–friendly* elliptic curve is a special class of elliptic curves, the parameters p, k, and the defining equation of elliptic curve are restricted by some tight conditions. Pairings are simply classified into two types. One is *symmetric* pairing and the other is *non–symmetric* pairing. The former uses *super–singular* curve and the latter does *non super–singular*, in other words *ordinary*, pairing–friendly curve. Especially in the case of *ordinary* pairing for example with Barreto–Naehrig curve [1], it is known that Gallant–Lambert–Vanstone (GLV) method [8] accelerates not only pairing calculation [12] but also scalar multiplications [10], [7]. The *symmetric* and *non–symmetric* pairings have some different advantages; however, this paper discusses an efficient algorithm for generating an *ordinary* pairing–friendly curve of the embedding degree $k = 1$ whose order r has two large prime factors v and w as the RSA modulus. In addition, the generated pairing–friendly curve has an efficient structure for the GLV method. There were some probablistic difficulties for generating

*{nogami,yanagi,izuta,morikawa}@cne.okayama-u.ac.jp

such a *large composite order* pairing–friendly curve.

It is well known that Cocks–Pinch (CP) method [4] is efficient for generating such a *composite order* ordinary pairing–friendly curve. It is based on complex multiplication (CM) method and thus practically supports most of parameter settings of characteristic p, embedding degree k, discriminant D, order r, and Frobenius trace t. An important point is that the ratio ρ of the pairing–friendly curve generated by CP method becomes more than 2. It is an advantage for the purpose of this paper because CP method efficiently supports the case that the ratio $\rho \approx 2$ and the embedding degree $k = 1$. However, it originally has no viewpoints of GLV–based efficiencies such as reported in [10], [7]. Based on CP method, Takashima embedded an GLV–based efficient structure to a certain ordinary pairing–friendly curve by restricting the order r [12]. Then, a pairing calculation became more efficient with some efficient endomorphisms. It is basically available for ordinary pairing–friendly curves whose embedding degree is more than or equal to 2, moreover, it leaves *composite order* ordinary pairing–friendly curves of embedding degree 1 dealt with in this paper out of view.

In the same of Takashima's approach [12], this paper focuses on cyclotomic polynomials of periods 3 (cubic), 4 (quatic), and 6 (sextic), where GLV method relates these periods to efficiently computable endomorphisms with scalar multiplications. In detail, it is important that the degrees of these cyclotomic polynomials are 2. Denoting the cyclotomic polynomial of period n by $\Phi_n(\chi)$, where $n = 3,\ 4,\ 6$, the algorithm proposed in this paper sets the order as $r(\chi) = \Phi_n(\chi)$ and then finds $\chi = \lambda_n$ such that $r(\lambda_n)$ has two large prime factors $v,\ w$. Then, based on CP method, it determines the characteristic p such that a rank 2 *torsion* group structure for *pairing* is embedded in $E(\mathbb{F}_p)$ with the embedding degree $k = 1$. After the proposal of the generating algorithm, some experimental results show that it efficiently generates *ordinary* pairing–friendly elliptic curves of the embedding degree $k = 1$ whose order r has two large prime factors v and w with about 500 or 1000 bits. Moreover, the generated pairing–friendly curve has an efficient structure for the GLV method. It is also shown that a scalar multiplication on the generated *composite order* pairing–friendly curve is about two times accelerated by applying GLV method and joint sparse form (JSF) technique [11] with multi–scalar multiplication.

Throughout this paper, p, k, and r denote characteristic, embedding degree, and order, respectively. $\mathbb{F}_p$ denotes a prime field and $\mathbb{F}_{p^k}$ does its extension field. Small alphabets such as a denote elements in prime. $X \mid Y$ and $X \nmid Y$ mean that X divides and does not divide Y, respectively. $\Phi_n(x)$ denotes the cyclotomic polynomial of order n.

2 FUNDAMENTALS

Let us briefly review elliptic curve, *pairing–friendly* curve of composite order, complex multiplication (CM) technique, Gallant–Lambert–Vanstone (GLV) method [8], Cocks–Pinch (CP) method [4], and Takashima's approach for accelerating *pairing* calculation with GLV viewpoints [12].

2.1 Ordinary pairing–friendly curve of composite order

Let $\mathbb{F}_p$ be prime field and E be an *ordinary* elliptic curve over $\mathbb{F}_p$. $E(\mathbb{F}_p)$ that denotes the set of rational points on the curve, including the *infinity point* $\mathcal{O}$, forms an additive Abelian group. Let $\#E(\mathbb{F}_p)$ be its order, consider a large prime number r that divides $\#E(\mathbb{F}_p)$. The smallest positive integer k such that r divides $p^k - 1$ is especially called *embedding degree.* One can consider a pairing such as Tate and Ate pairings on $E(\mathbb{F}_{p^k})$. Usually, $\#E(\mathbb{F}_p)$ is written as

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

where t is the Frobenius trace of $E(\mathbb{F}_p)$.

This paper especially deals with a certain *ordinary* pairing–friendly curve $E(\mathbb{F}_{p^k})$ of composite order as the RSA modulus. In detail, suppose that the order r of a certain subgroup in $E(\mathbb{F}_{p^k})$ has two large prime factors v and w. As also introduced in [6], define the following parameter ρ.

$$\rho = \lfloor \log_2 p \rfloor / \lfloor \log_2 r \rfloor. \tag{2}$$

This ratio ρ is often used for evaluating the redundancy between the order r and the characteristic p. In the case of Barreto–Naehrig curve, ρ is almost 1 and thus it is quite efficient [1]. For *pairing*, $\rho{\cdot}k$ becomes more than or equal to 2 since it needs to have a rank 2 *torsion group* structure. According to [6], in the case of *composite order* pairing, it is preferred to be small and the minimum is 2. It is briefly because, since the order r becomes more than 1000–bit as the RSA modulus, $\rho \cdot k \approx 2$ will be the best as the size of the discrete logarithm problem in the embedded extension field $\mathbb{F}^*_{p^k}$. On the same reason, this paper mainly discusses the case of $\rho \cdot k \approx 2$, especially $\rho \approx 2$ and $k = 1$.

2.2 Complex multiplication (CM) technique

The following equation is often called *CM equation* that has the parameters p (characteristic), t (trace of Frobenius), and D (discriminant).

$$4p = t^2 - Ds^2. \tag{3}$$

Note here that, especially when the discriminant D is 1 or 3, the defining equation of elliptic curve is respectively given as

$$E_a : y^2 \ = \ x^3 + ax,\ a \in \mathbb{F}_p, \tag{4a}$$

$$E_b : y^2 \ = \ x^3 + b,\ b \in \mathbb{F}_p. \tag{4b}$$

It is important that, for these cases, some CM–based complicated calculations such as Hilbert polynomial determination are not needed because the orders of these special form curves have only several variants, respectively. For example, $\#E_b(\mathbb{F}_p)$ has six variants at most. These forms of elliptic curve are closely related to the following GLV method.

2.3 Gallant–Lambert–Vanstone (GLV) method

According to [8], some special elliptic curves have efficient endomorphisms related to certain scalar multiplications. The scalar multiplications are respectively obtained by the endomorphisms without any complicated arithmetic operations for rational points. It is generally called GLV technique. Among them, this paper focuses on the following three cases.

2.3.1 Cubic GLV :

Let $3 \mid (p-1)$ and consider $E: y^2 = x^3 + b, b \in \mathbb{F}_p$, where $D = 3$. For a certain positive integer r such that $r \mid \#E(\mathbb{F}_p)$ and $3 \mid (r-1)$, there exists a certain positive integer λ_3 that satisfies

$$\lambda_3^2 + \lambda_3 + 1 \equiv 0 \bmod r. \tag{5}$$

In addition, the following endomorphism of period 3 is given.

$$\begin{aligned} \psi_3 : E(\mathbb{F}_p)[r] &\rightarrow E(\mathbb{F}_p)[r], && \text{(6a)} \\ (x, y) &\mapsto (\epsilon x, y), && \text{(6b)} \end{aligned}$$

where $E(\mathbb{F}_p)[r]$ denotes the additive group of rational points of order r and ϵ is a primitive cubic root of unity in $\mathbb{F}_p^*$. Then, $P \in E(\mathbb{F}_p)[r]$ holds $[\lambda_3]P = \psi_3(P)$.

2.3.2 Quatic GLV :

Let $4 \mid (p-1)$ and consider $E: y^2 = x^3 + ax, a \in \mathbb{F}_p$, where $D = 1$. For a certain positive integer r such that $r \mid \#E(\mathbb{F}_p)$ and $4 \mid (r-1)$, there exists a certain positive integer λ_4 that satisfies

$$\lambda_4^2 + 1 \equiv 0 \bmod r. \tag{7}$$

In addition, the following endomorphism of period 4 is given.

$$\begin{aligned} \psi_4 : E(\mathbb{F}_p)[r] &\rightarrow E(\mathbb{F}_p)[r], && \text{(8a)} \\ (x, y) &\mapsto (-x, \zeta y). && \text{(8b)} \end{aligned}$$

ζ is a primitive quatic root of unity in $\mathbb{F}_p^*$. $P \in E(\mathbb{F}_p)[r]$ holds $[\lambda_4]P = \psi_4(P)$.

2.3.3 Sextic GLV :

Let $6 \mid (p-1)$ and consider $E: y^2 = x^3 + b, b \in \mathbb{F}_p$, where $D = 3$. For a certain positive integer r such that $r \mid \#E(\mathbb{F}_p)$ and $3 \mid (r-1)$, there exists a certain positive integer λ_6 that satisfies

$$\lambda_6^2 - \lambda_6 + 1 \equiv 0 \bmod r. \tag{9}$$

In addition, the following endomorphism of period 6 is given.

$$\begin{aligned} \psi_6 : E(\mathbb{F}_p)[r] &\rightarrow E(\mathbb{F}_p)[r], && \text{(10a)} \\ (x, y) &\mapsto (\epsilon x, -y). && \text{(10b)} \end{aligned}$$

Then, $P \in E(\mathbb{F}_p)[r]$ holds $[\lambda_6]P = \psi_6(P)$.

2.4 Cocks–Pinch (CP) method

Cocks–Pinch (CP) method [4] is well known as an efficient method for generating ordinary pairing–friendly curve. As shown in **Fig**.1, it is closely related to CM method and generates a pairing–friendly elliptic curve of $\rho \geq 2$ with a certain set of parameters (p, t, r, k, D). As previously introduced, in the case of composite order pairing, $\rho \approx 2$ with $k = 1$ is efficient. Thus, CP method efficiently works for generating an ordinary pairing–friendly curve of composite order. Boneh et al.'s work [3] has dealt with pairing–friendly curves of composite order with $k = 1$ but does not have viewpoints of applying GLV technique.

2.5 Takashima's approach

Takashima [12] has proposed a technique for accelerating pairing calculation with the efficient endomorphisms as the preceding GLV method does. It also refers to CP method for preparing a pairing–friendly elliptic curve; however, Takashima's approach basically supports pairings with the embedding degree $k \geq 2$ and a certain prime order r. In detail, restricting the group order $r = \lambda_3^2 + \lambda_3 + 1$ prime, pairing calculation is accelerated with the endomorphism ψ_3. In addition, the GLV method with λ_3 and ψ_3 also accelerates a scalar multiplication of a rational point P of the order r based on $[\lambda_3]P = \psi_3(P)$.

3 MAIN PROPOSAL

This paper shows an efficient algorithm for generating ordinary pairing–friendly elliptic curves of embedding degree 1 and $\rho \approx 2$ whose order r has two large prime factors v and w as the RSA modulus. In addition, the generated pairing–friendly curve has an efficient structure for GLV technique since its order r is given as $r = \lambda_3^2 + \lambda_3 + 1$ for example. **Fig**.2 shows the algorithm. The most important point is that the order r is given as a cyclotomic polynomial of degree 2 such as $r(\chi) = \Phi_n(\chi)$, $n = 3$ (cubic), 4 (quatic), 6 (sextic), where χ is a certain integer. Then, the algorithm finds a certain integer χ such that

- the order r has two large prime factors v and w,
- for the rank 2 *torsion* group structure, $r \mid (p-1)$ and $r^2 \mid \#E(\mathbb{F}_p)$,
- $E(\mathbb{F}_p)[r]$ has an efficient structure for GLV technique based on the relation $r(\chi) = \Phi_n(\chi)$, where $\lfloor \log_2 \lambda_n \rfloor$ becomes about $\lfloor \log_2 r \rfloor / 2$.

```
Input :   bit size $b$ of prime factors, positive square-free discriminant $D$,
          embedding degree $k$
Output :  parameters $(p,r,t)$ of an objective pairing–friendly curve

1.  Generate $b$-bit prime number $v$ and $w$ such that $k \mid (v-1)$ and $k \mid (w-1)$.
2.  If $\left(\frac{-D}{r}\right) = 1$, let $r = v \cdot w$. Otherwise return to Step 1.
3.  Calculate $s \pmod r$ such that $s^2 \equiv -D \pmod r$
4.  Choose an integer $X$ that has order $k$ in $\mathbb{Z}_{vw}$.
5.  Take an integer $Y$ congruent to $\pm(X-1)s^{-1} \pmod r$.
6.  Let $p = ((X+1)^2 + DY^2)/4$, if $p$ is a prime number, output $p$, $r$, $t = X+1$.
    Otherwise return to Step 1 or Step 6 with changing $Y = Y + ir,\ i = 1, 2, \cdots$.
```

Figure 1: Calculation procedure of Cocks–Pinch method

As introduced in **Sec**.2.3, corresponding to the discriminant D, GLV technique requires special forms of elliptic curve such as $y^2 = x^3 + b$. Thus, this paper also deals with the pairs $(n, D) = (3, 3)$, $(4, 1)$, and $(6, 3)$. Then, the defining equation of the curve that has the objective order is easily determined.

In what follows, each calculation step of **Fig**.2 is explained.

Step 1 : prepare the first prime factor v

Prepare the first prime number v of bit size b such that $n \mid (v-1)$, where n is the order of cyclotomic polynomial $\Phi_n(\chi)$ of degree 2. It is necessary for the following **Step** 2 to calculate two roots α and β of $r(\chi) = \Phi_n(\chi)$ mod v in $\mathbb{Z}_v$, where this paper deals with the cases of $n = 3, 4$, and 6.

Step 2 : calculate the two roots of $r(\chi) = \Phi_n(\chi)$ mod v

Calculate the two roots α and β of $r(\chi) = \Phi_n(\chi)$ mod v. First, generate a random number γ less than v. Then, calculate $\gamma^{(v-1)/n}$ mod v. If the result is not equal to 1, it is α and then $\beta = \alpha^{-1}$ mod v. The most important point is that, of course these roots are smaller than v, $\lfloor \log_2 \alpha \rfloor$ and $\lfloor \log_2 \beta \rfloor$ are mostly equal to $\lfloor \log_2 v \rfloor = b$. Accordingly, $\lfloor \log_2 r(\alpha) \rfloor$ and $\lfloor \log_2 r(\beta) \rfloor$ mostly become $2b$, moreover $r(\alpha)$ and $r(\beta)$ are divisible by v because α and β are the roots of $r(\chi)$ mod v. Thus, the first prime number v is embedded.

Step 3 : obtain the second prime factor w

Check the *almost* primarities of $r(\alpha)/v$ and $r(\beta)/v$. If either $r(\alpha)/v$ or $r(\beta)/v$ is an *almost* prime, a certain almost b–bit prime number is obtained as the second prime number w. Of course, one can try $r(hv + \alpha)/v$ and $r(hv+\beta)/v$, where h is an integer. Thus, the second prime number w is embedded to the order r.

Step 4 and Step 5 : determine the characteristic p of $\mathbb{F}_p$

Search a prime number p as the characteristic of $\mathbb{F}_p$ by changing X and Y with adding the order r so as to satisfy $r \mid (p-1)$ and $r^2 \mid (p+1-t)$. Finally, output the parameters λ_n, p, r, and $t = X + 1$. Otherwise, one can repeatedly try Step 5 with changing X and Y at Step 4. Especially, λ_n that is smaller than v is used for the GLV–based scalar multiplication. Step 5 is just a probablistic calculation step of the proposed algorithm.

4 VARIOUS TARGETS OF THE PROPOSED METHOD

One of the technical essences of the proposed algorithm shown in **Fig**.2 is that the objective order r is given as a polynomial of degree 2 with an integer variable χ such as $r(\chi) = \Phi_n(\chi),\ n = 3, 4, 6$. Thus, as shown in **Fig**.3, it is adaptable for several kinds of cyclotomic families of pairing–friendly curve shown below. Note that, different from **Fig**.2 that is based on CP method, **Fig**.3 repeats two probablistic calculation steps as Step 3 and Step 4.

4.1 Cyclotomic family of embedding degree 1

The following three cases are ordinary pairing–friendly elliptic curves of embedding degree 1 and small ρ. Thus, they are efficient for composite order pairing. **Fig**.3 also helps their GLV accelerations for a scalar multiplication.

4.1.1 Case 1 : $(k, \rho, D) = (1, 2, 1)$

$$\begin{aligned} p(\chi) &= l^2\chi^2 + 1, && \text{(11a)} \\ r(\chi) &= \Phi_1(\chi) = \chi, && \text{(11b)} \\ t(\chi) &= 2, && \text{(11c)} \\ E : y^2 &= x^3 - x \quad (l\chi \equiv 0 \bmod 4), && \text{(11d)} \\ E : y^2 &= x^3 - 4x \quad (l\chi \equiv 2 \bmod 4). && \text{(11e)} \end{aligned}$$

$$E(\mathbb{F}_p) \simeq \mathbb{Z}_{lr} \oplus \mathbb{Z}_{lr} \tag{12}$$

This class of ordinary pairing–friendly curve is interesting. Two large prime factors are easily embedded by $r(\chi) = \chi = vw$; however, an efficient GLV structure would be also embedded by $r(\chi) = \chi = \Phi_4(z) = z^2 + 1$, where z is an intervening integer variable.

```
Input :   bit size $b$ of prime factors $v$ and $w$, positive square-free discriminant $D$,
          embedding degree $k$, cyclotomic polynomial $r(\chi) = \Phi_n(\chi)$ of degree 2
Output :  parameters $(\lambda_n, p, r, t)$ of an objective pairing–friendly curve

1.  Generate $b$–bit prime number $v$ such that $n \mid (v-1)$.
2.  Find two roots $\alpha = \gamma^{(v-1)/n} \neq 1$ and $\beta = \alpha^{-1}$ of $r(\chi) = \Phi_n(\chi) \bmod v$,
    where $\gamma \in \mathbb{Z}_v$ is randomly chosen.
3.  Check the *almost* primarities of $w_\alpha = r(\alpha)/v$ and $w_\beta = r(\beta)/v$. †
    If either $w_\alpha$ or $w_\beta$ is an *almost* prime, let $\lambda_n$ be $\alpha$ or $\beta$ correspondingly.
4.  Set $X = 1 + ir$ and $Y = jr$ as $i = 0, 1, 2, \cdots$ and $j = 0, 1, 2, \cdots$, respectively.
5.  Calculate $p = \left((X+1)^2 + DY^2\right)/4$. If $p$ is a prime number,
    output $\lambda_n, p, r, t = X + 1$. Otherwise return to **Step 4** or Step 1.
```

† One can try $r(hv+\alpha)/v$ and $r(hv+\beta)/v$, where h is some integer.

Figure 2: Calculation procedure of the proposed method based on Cocks–Pinch method

```
Input:   bit size $b$, order $n$ cyclotomic polynomial $r(\chi) = \Phi_n(\chi)$ of degree 2
Output:  an integer $\chi$ such that $r(\chi)$ has two almost $b$–bit prime factors

1.  Generate $b$–bit prime number $v$ such that $n \mid (v-1)$.
2.  Find two roots $\alpha = \gamma^{(v-1)/n} \neq 1$ and $\beta = \alpha^{-1}$ of $r(\chi) = \Phi_n(\chi) \bmod v$,
    where $\gamma \in \mathbb{Z}_v$ is randomly chosen.
3.  Check the *almost* primarities of $w_\alpha = r(\alpha)/v$ and $w_\beta = r(\beta)/v$. †
4.  If either $w_\alpha$ or $w_\beta$ is prime, correspondingly check the *almost* primarity of
    $p_\alpha = p(\alpha)$ and $p_\beta = p(\beta)$. Otherwise, return to Step.1.
5.  If either $p_\alpha$ or $p_\beta$ is a prime, output $\alpha$ or $\beta$ correspondingly.
    Otherwise, return to **Step 1**.
```

† One can try $r(hv+\alpha)/v$ and $r(hv+\beta)/v$, where h is some integer.

Figure 3: Calculation procedure based on the proposed idea for some cyclotomic families

4.1.2 Case 2 : $(k, \rho, D) = (1, 3, 1)$

$$\begin{aligned} p(\chi) &= (\chi^6 + 3\chi^4 - \chi^2 + 1)/4, && (13a)\\ r(\chi) &= \Phi_4(\chi) = \chi^2 + 1, && (13b)\\ t(\chi) &= -\chi^2 + 1, && (13c)\\ E : y^2 &= x^3 + ax,\ a \in \mathbb{F}_p. && (13d) \end{aligned}$$

$$E(\mathbb{F}_p) \simeq \mathbb{Z}_{r^2/2} \oplus \mathbb{Z}_{r/2}. \quad (14)$$

4.1.3 Case 3 : $(k, \rho, D) = (1, 2, 1)$

$$\begin{aligned} p(\chi) &= (\chi^2 + 1)(\chi^2 - \chi + 1)/3 - \chi^3, && (15a)\\ r(\chi) &= \Phi_6(\chi) = \chi^2 - \chi + 1, && (15b)\\ t(\chi) &= -\chi^2 + \chi + 1, && (15c)\\ E : y^2 &= x^3 + b,\ b \in \mathbb{F}_p. && (15d) \end{aligned}$$

$$E(\mathbb{F}_p) \simeq \mathbb{Z}_r \oplus \mathbb{Z}_{r/3} \quad (16)$$

4.2 Cyclotomic families of embedding degrees 3 and 4

Since the following ordinary pairing–friendly elliptic curves have $\rho \cdot k = 6$ and 8, respectively, they may not be efficient for composite order pairings. However, according to **Table** 3, a scalar multiplication in $E(\mathbb{F}_p)[r]$ will be efficiently carried out by applying GLV technique because the ratio ρ and the degree of $p(\chi)$ with respect to χ are the same of Cases 1 and 3. Thus, **Fig**.3 helps generating pairing–friendly curves of these classes efficient for the GLV–based scalar multiplication.

4.2.1 Case 4 : $(k, \rho, D) = (3, 2, 3)$

$$\begin{aligned} p(\chi) &= (\chi^4 - \chi^3 + 2\chi + 1)/3, && (17a)\\ r(\chi) &= \Phi_3(\chi) = \chi^2 + \chi + 1, && (17b)\\ t(\chi) &= \chi + 1, && (17c)\\ E : y^2 &= x^3 + b,\ b \in \mathbb{F}_p. && (17d) \end{aligned}$$

$$E(\mathbb{F}_p) \simeq \mathbb{Z}_r \oplus \mathbb{Z}_r. \quad (18)$$

4.2.2 Case 5 : $(k, \rho, D) = (4, 2, 1)$

$$\begin{aligned} p(\chi) &= (\chi^4 - 2\chi^3 + 2\chi^2 + 2\chi + 1)/4, && (19a)\\ r(\chi) &= \Phi_4(\chi) = \chi^2 + 1, && (19b)\\ t(\chi) &= \chi + 1, && (19c)\\ E : y^2 &= x^3 + ax,\ a \in \mathbb{F}_p. && (19d) \end{aligned}$$

$$E(\mathbb{F}_p) \simeq \mathbb{Z}_r \oplus \mathbb{Z}_r. \quad (20)$$

5 EXPERIMENTAL RESULT

In order to check the efficiency of the proposed idea, with the computational environment shown in **Table** 1, some experimental results with $b \approx 500$ and 1000 are shown, where b is the bit size of prime factors v and w.

5.1 Calculation time for generating an objective curve

Table 2 shows that ordinary pairing–friendly elliptic curves of embedding degree $k = 1$ and a certain composite order r are efficiently generated. In the case of the proposed CP–based algorithm **Fig**.2, even when the bit size b of prime factors v and w of order r are about 1000, accordingly that of r becomes about 2000–bit, it just takes several minutes. **App**.A shows an example of *large composite order* ordinary pairing–friendly curve generated by **Fig**.2.

On the other hand, the *non* CP–based algorithm **Fig**.3 takes a little more calculation time since it has two probablistic calculation steps as previously introduced. As described in the next section, they are efficient for the GLV–based scalar multiplication technique.

5.2 Scalar multiplication with GLV method

Suppose that $E(\mathbb{F}_p)$ is generated by the proposed algorithm **Fig**.2 or **Fig**.3. Then, let P be a rational point in a certain subgroup of $E(\mathbb{F}_p)[r]$ and consider a scalar multiplication $[s]P$, $s < r$. Then, λ_n–adic expansion of the scalar s accelerates the scalar multiplication as

$$[s]P \quad = \quad [s_0 + s_1\lambda_n]P = [s_0]P + [s_1]\psi_n(P), \quad (21)$$

where $\lfloor \log_2 \lambda_n \rfloor \approx \lfloor \log_2 r \rfloor / 2$ as previously introduced. For the above calculation, multi–scalar multiplication and joint sparse form (JSF) techniques [11] are applied. **Table** 3 shows the average computation time for a scalar multiplication. Compared to the plain binary method, (GLV+JSF) multi–scalar multiplication technique could accelerate the average calculation time about two times.

6 FUTURE WORK

The proposed method is basically applicable for the other cases that the order $r(\chi)$ is given as a polynomial of degree 2 with an integer variable χ. As a future work, the cases that the degree of $r(\chi)$ is more than 2 would be considered. Though this paper has focused on accelerating a scalar multiplication with GLV technique, a pairing calculation on the generated *large composite order* pairing–friendly curve will become more efficient from GLV viewpoint such as Takashima's approach. The security viewpoint for the *composite order* needs to be carefully discussed as the factoring problem of RSA modulus.

References

[1] P. S. L. M. Barreto, and M. Naehrig. "Pairing-Friendly Elliptic Curves of Prime Order", *SAC 2005*, LNCS 3897, Springer–Verlag, pp. 319–331, 2006.

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

[3] D. Boneh, K. Rubin, and A. Silverberg, "Finding Composite Order Ordinary Elliptic Curves Using The Cocks–Pinch Method," available at http://eprint.iacr.org/2009/533.pdf.

[4] C. Cocks and R. G. E. Pinch, "Indentity-based Cryptosystems Based on the Weil Pairing," unpublished manuscript, 2001, *see also* [3].

[5] D. Freeman, "Converting Pairing–Based Cryptosystems from Composite–Order Groups to Prime-Order Groups," available at http://eprint.iacr.org/2009/540.pdf.

[6] D. Freeman, M. Scott, and E. Teske, "A Taxonomy of Pairing–Friendly Elliptic Curves," available at http://eprint.iacr.org/2006/372.pdf.

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

[8] R. P. Gallant, R. J. Lambert and S. A. Vanstone, "Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms," *CRYPTO 2001*, LNCS 2139, Springer–Verlag, pp. 190–200, 2001.

[9] GNU MP, http://gmplib.org/

[10] 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.

[11] J. A. Solinas, "Low-weight Binary Representations for Pairs of Integers," Technical Report CORR 2001-41, CACR, available at http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-41.ps, 2001.

[12] K. Takashima, "Scaling Security of Elliptic Curves with Fast Pairing Using Efficient Endomorphisms," IEICE Trans., vol. E90–A, no. 1, pp. 152-159, 2007.

A Example of parameters when the bit size $b \approx 500$

The following ordinary pairing–friendly elliptic curve has an composite order $r = 3 \cdot v \cdot w$, where v and w are about 500–bit prime numbers.

$$k = 1,\ D = 3,\ \rho = 2.008,\ E : y^2 = x^3 + 6. \tag{22a}$$

$$\begin{aligned} \lambda_3 = {} & 43950410055833446962179539656807527150817740902021307185608796626 3\\ & 308949982459312798740295215184333437287670434715396957740392811149\\ & 429392558481782527083 \text{ (\textbf{508} bits).} \end{aligned} \tag{22b}$$

$$\begin{aligned} r = {} & 193163854407590577451946432273441588398505282915869374688062386409\\ & 071562276781019229599509102781843363234521581599411142855806848305\\ & 107079823772487043588680396409877106139506035327287285936956373540\\ & 057823920653021402263658948122015678343548990558778050445694945223\\ & 37304525192311753552329109258896341101597 3 \text{ (\textbf{1015} bits).} \end{aligned} \tag{22c}$$

$$\begin{aligned} v = {} & 876183709456790113044766360041675052176461166376658216092747185276\\ & 085608109660545289297642276920920615824193920722148535685484957510\\ & 065202532261645098695 7 \text{ (\textbf{512} bits).} \end{aligned} \tag{22d}$$

$$\begin{aligned} w = {} & 734868164909338755332360613339244105567429182946839672388091534053\\ & 927456452794749056235276473081928567960827188933888223414172076082\\ & 9219450498812214163 \text{ (\textbf{502} bits).} \end{aligned} \tag{22e}$$

$$\begin{aligned} t = {} & 148736167893844744637998752850550023066849067845219418509808037534\\ & 985102953121384806791622009142019389690581617831546579998971273194\\ & 932451464304815023563283905235605371727419647202011210171456407625\\ & 844524418902826479743017390053952072324532722730259098843185107821\\ & 997244843980800502352934141293501826482299 23 \text{ (\textbf{1021} bits).} \end{aligned} \tag{22f}$$

$$\begin{aligned} p = {} & 555579769532497092859946289542681346166459665128183250548144731540\\ & 583246675149400030672806107316000532876866012934494846475041438274\\ & 138643552843279798607192283052019869980471309281521794787096118221\\ & 316552173940149131997654394634995165617213361824140113144793622877\\ & 258352951963418314559858085309809204647653647055665586533131610570\\ & 036235790970746572954934696867842105613521778563176160876016162328\\ & 815513073551482481451629382408666471559133253974666802089740888552\\ & 746504364782892034460710040589753613683427773407873891300109347439\\ & 708940835904753855510960845477678195714253881154555198945231860161\\ & 704271348656808194 03 \text{ (\textbf{2039} bits).} \end{aligned} \tag{22g}$$

Table 1: Computational environment

CPU	Core 2 Duo *† 3GHz
Cash size	4096KB
OS	Linux(R)‡ 2.6.26
Language	C
Compiler	gcc 4.1.2
Library	GNU MP 4.2.2 [9]

[*] Core 2 Duo is a registered trademark of Intel Corporation.

[†] Only single core is used though it has two cores.

[‡] Linux(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.

Table 2: Average computation time for generating an *objective* pairing–friendly curve

[sec]

class of pairing–friendly curve		bit size of prime factors v and w	
		≈ 500	≈ 1000
Fig.2 (**Sec**.3)	$l = 3$	45	3.3×10^2
	$l = 4$	44	5.1×10^2
	$l = 6$	41	4.4×10^2
Fig.3 (**Sec**.4)	Case 1[†]	4.4	4.4×10
	Case 2	2.9×10^3	1.8×10^5
	Case 3	3.3×10^3	1.4×10^5

[†] The intervening integer variable z was not used for this experiment.

Table 3: Average computation times of scalar multiplications

[sec]

class of pairing–friendly curve			bit size b of prime factors v and w	
			≈ 500	≈ 1000
Sec.3	$l = 3$	binary	0.27	1.73
		GLV + multi-scalar	0.17	1.12
		GLV + JSF + multi-scalar	**0.13**	**0.90**
	$l = 4$	binary	0.27	1.69
		GLV + multi-scalar	0.17	1.10
		GLV + JSF + multi-scalar	**0.14**	**0.88**
	$l = 6$	binary	0.27	1.68
		GLV + multi-scalar	0.17	1.09
		GLV + JSF + multi-scalar	**0.14**	**0.87**
Sec.4	Case 1[‡]	binary	0.27	1.65
		GLV + multi-scalar	0.17	1.06
		GLV + JSF + multi-scalar	**0.14**	**0.85**
	Case 2	binary	0.52	3.10
		GLV + multi-scalar	0.34	2.01
		GLV + JSF + multi-scalar	**0.27**	**1.61**
	Case 3	binary	0.26	1.65
		GLV + multi-scalar	0.17	1.07
		GLV + JSF + multi-scalar	**0.14**	**0.86**

[†] : scalar multiplications are implemented with *mixed coordinates*.

[‡] : GLV structure was embedded with the intervening integer variable z.