Memoirs of the Faculty of Engineering, Okayama University, Vol. 44, pp. 60-68, January 2010

Ordinary Pairing Friendly Curve of Embedding Degree 3 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

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 17, 2009)

This paper proposes a method for generating a certain composite order *ordinary* pairing–friendly elliptic curve of embedding degree 3. In detail, the order has two large prime factors such as the modulus of RSA cryptography. The method is based on the property that the order of the target pairing–friendly curve is given by a polynomial as $r(\chi)$ of degree 2 with respect to the integer variable χ. When the bit size of the prime factors is about 500 bits, the proposed method averagely takes about 15 minutes on Core 2 Quad (2.66Hz) for generating one.

1 INTRODUCTION

Recently, pairing–based cryptographic applications such as ID–based cryptography [13] have received much attention. 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 $\mathbb{G}_3$. In addition, these groups 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 rational points are defined over a certain *pairing–friendly* elliptic curve. In other words, the security of pairing–based cryptography partially depends on elliptic curve cryptography. 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. Accordingly, the *symmetric* and *non–symmetric* pairings have some different advantages.

RSA cryptography has a long history compared to elliptic curve cryptography and pairing–based cryptography. Thus, various RSA–based cryptographic applications and mathematical techniques have been proposed. RSA cryptography is defined over an integer ring of a certain *secure* composite order r, in detail r needs to have two large prime factors such as more than 500–bit. As also introduced in [5], in order to apply these RSA–based conventional techniques to pairing–based cryptography, pairing–friendly elliptic curve also needs to have such a *secure* and *large* composite order r [3]. According to [5], such a *large* composite order pairing–friendly curve has been already introduced as

- super–singular pairing–friendly curve of $k = 2$ with $\rho = 1$,
- ordinary pairing–friendly curve of $k = 1$ with $\rho = 2$,

where $\rho = \lfloor \log_2 p \rfloor / \lfloor \log_2 r \rfloor$. From the viewpoint of efficiency, $\rho \cdot k$ is preferred to be small. According to [5], $\rho \cdot k = 2$ is recommended and the above curves satisfy it. However, this paper especially focuses on that, in the cases of the above curves, the order r is given by a polynomial of degree 1 with respect to the integer variable χ, that is denoted by $r(\chi)$ in this paper, and thus it is possible to efficiently generate such a *secure* and *large* composite order pairing–friendly curve. When the degree of $r(\chi)$ is larger than or equal to 2 such as the following Eq.(1c), it becomes difficult. Though $\rho \cdot k$ will become a little larger, it will be one of theoretically interesting problems. This paper deals with the case that the degree of $r(\chi)$ with respect to the integer variable χ is equal to 2.

This paper proposes a method for generating *ordinary* pairing–friendly curves of composite order especially when the embedding degree k is equal to 3. Let v

*nogami@cne.okayama-u.ac.jp
†morikawa@cne.okayama-u.ac.jp

and w be 500–bit prime numbers, construct the order r such that vw divides r. In the case that $k = 3$, according to [10], a class of *ordinary* pairing–friendly curves whose parameters are given as follows is known.

$$E \;:\; y^2 = x^3 + b,\ b \in \mathbb{F}_p, \tag{1a}$$
$$p(\chi) = (\chi^4 - \chi^3 + 2\chi + 1)/3, \tag{1b}$$
$$r(\chi) = \chi^2 + \chi + 1, \tag{1c}$$

where χ is an integer parameter. Then, this paper proposes an efficient algorithm that generates *ordinary* pairing–friendly curves whose order r has two almost 500–bit prime factors by changing χ. It can achieve $\rho \cdot k = 6$. The basic idea first solves $r(\chi) = 0$ modulo a certain prime number v. Then, using the result α and β, those are certain positive integers, the idea checks the *almost* primarities of $r(\alpha)/v$ and $r(\beta)/v$ since it is shown in this paper that $r(\chi)$ is divisible by 3. If either of them becomes an *almost* prime number w, the idea correspondingly checks the primarities of $p(\alpha)$ and $p(\beta)$ for preparing the prime field $\mathbb{F}_p$. Then, one obtains an *ordinary* pairing–friendly curve $E(\mathbb{F}_p)$ with $p(\alpha)$ or $p(\beta)$. Otherwise, try another prime number v. After that, this paper experiments how much calculation time is required for generating an *ordinary* pairing–friendly curve whose order has such two large prime factors. Let the bit sizes of the prime factors be about 500–bit, it is shown that it averagely takes 15 minutes on Core 2 Duo (3.0GHz). After that, in order to check the efficiency, some experimental results of Ate pairing and some other elliptic curve operations are shown. The proposed method is basically available for some other pairing–friendly curves whose order is given as a polynomial of degree 2 such as Eq.(1c).

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 and capital alphabets such as a and A denote elements in prime and extension fields, respectively. $X \mid Y$ and $X \nmid Y$ mean that X divides and does not divide Y, respectively.

2 FUNDAMENTALS

This section briefly reviews elliptic curve, a class of *pairing–friendly* curves of embedding degree 3, cubic twist, and Ate pairing.

2.1 Elliptic curve and pairing–friendly curve of embedding degree 3

Let $\mathbb{F}_p$ be prime field and E be an 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

$$\#E(\mathbb{F}_p) = p + 1 - t, \tag{2}$$

where t is the Frobenius trace of $E(\mathbb{F}_p)$. The target *pairing–friendly* curve whose embedding degree k is 3 has the following parameters with a certain integer χ.

$$p(\chi) = (\chi^4 - \chi^3 + 2\chi + 1)/3, \tag{3a}$$
$$r(\chi) = \chi^2 + \chi + 1, \tag{3b}$$
$$t(\chi) = \chi + 1, \tag{3c}$$

where $r(\chi)$ is the order of groups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_3$. In addition, since the discriminant D is equal to 3 in this case, the defining equation E is given as

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

As also introduced in [5], the parameters of recent *ordinary* pairing–friendly curves are mostly given as Eqs.(3). In this case,

$$\rho = \lfloor \log_2 p \rfloor / \lfloor \log_2 r \rfloor = 2. \tag{5}$$

This ratio ρ is often used for evaluating the redundancy between the order r and the characteristic p. Especially based on Eq.(3b), this paper considers how to generate an ordinary pairing–friendly curve of embedding degree 3 whose order has two large prime factors as the modulus of RSA cryptography.

2.2 Twist

When the embedding degree k is equal to $3e$, where e is a positive integer, *cubic* twisted curve E' of Eq.(4) and the isomorphic map ψ_3 that accelerates not only pairing calculation but also some other operations such as a scalar multiplication in $\mathbb{G}_2$ [1],[6] are given as follows.

- $k = 3e$ (cubic twist)

$$E : \quad y^2 = x^3 + b,\ b \in \mathbb{F}_p, \tag{6a}$$
$$E' : \quad y^2 = x^3 + bz^{-2}, \tag{6b}$$

where z is a cubic non residue in $\mathbb{F}_{p^e}$ and $3 \mid (p-1)$.

$$\psi_3 : \begin{cases} E'(\mathbb{F}_{p^e}) & \to E(\mathbb{F}_{p^{3e}}), \\ (x, y) & \mapsto (xz^{2/3}, yz). \end{cases} \tag{6c}$$

In this paper, the case of $e = 1$ is mainly dealt with. Thus, ψ_3 and its inverse ψ_3^{-1} needs two multiplications between $\mathbb{F}_p$ and $\mathbb{F}_{p^3}$ elements as Eq.(6c).

2.3 Cross twisted (Xt) Ate pairing

Let $E(\mathbb{F}_{p^3})$ be a *pairing–friendly* curve of embedding degree 3 and $E(\mathbb{F}_{p^3})[r]$ be its subgroup of rational points of order r. Then, consider two rational point groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of order r as follows.

$$\mathbb{G}_1 = E(\mathbb{F}_{p^3})[r] \cap \mathrm{Ker}(\phi - [1]),\ \mathbb{G}_1 \subseteq E(\mathbb{F}_p), \tag{7a}$$
$$\mathbb{G}_2 = E(\mathbb{F}_{p^3})[r] \cap \mathrm{Ker}(\phi - [p]),\ \mathbb{G}_2 \subset E(\mathbb{F}_{p^3}), \tag{7b}$$

where ϕ and $[l]$ denotes Frobenius map with respect to $\mathbb{F}_p$ and l times scalar multiplication for a rational point in $E(\mathbb{F}_{p^3})$, respectively. Then, for $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, Ate pairing $e(Q, P)$ is defined as

$$e : \begin{cases} \mathbb{G}_2 \times \mathbb{G}_1 & \to \mathbb{F}^*_{p^3}/(\mathbb{F}^*_{p^3})^r, \\ (Q, P) & \mapsto e(Q, P). \end{cases} \tag{8}$$

Let t be the Frobenius trace of E over $\mathbb{F}_p$ and let $f_{t-1,Q}$ be a certain rational function, $e(Q, P)$ is given by

$$e(Q, P) = f_{t-1,Q}(P)^{(p^3-1)/r}, \tag{9}$$

where $f_{t-1,Q}(P)$ is efficiently calculated by Miller's algorithm [8]. Suppose the twist degree 3, according to Eq.(6c), the cubic twisted groups $\mathbb{G}'_1$ and $\mathbb{G}'_2$ are respectively given as

$$\mathbb{G}'_1 = \psi_3^{-1}(\mathbb{G}_1), \tag{10a}$$
$$\mathbb{G}'_2 = \psi_3^{-1}(\mathbb{G}_2). \tag{10b}$$

Fig.1 shows an image of the relation among $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}'_1$, and $\mathbb{G}'_2$. In this case, based on the parameters Eqs.(3), cross twist (Xt) Ate pairing $e(\cdot, \cdot)$ [1] achieves an efficient bilinear map by

$$e(Q, P) = f_{\chi,Q'}(P')^{(p^3-1)/r}, \tag{11}$$

where $Q' = \psi_3(Q)$ and $P' = \psi_3^{-1}(P)$. Then, according to the algorithm **Fig**.2 and also **Fig**.1, most of calculations are carried out in the prime field $\mathbb{F}_p$.

3 MAIN IDEA FOR GENERATING AN OBJECTIVE CURVE

The purpose of this paper is to generate pairing–friendly curves of embedding degree 3 whose order r has two large prime factors. In detail, when $r(\chi)$ is given as Eq.(3b), one would like to find an integer χ such that $r(\chi)$ has two large prime factors v and w. **Fig**.3 shows the calculation procedure. In what follows, each calculation step is explained.

3.1 Step 1 : preparation of the first prime factor v

Prepare the first prime number v ob bit size b such that $3 \mid (v-1)$. It is the necessary and sufficient condition that the following **Step** 2 has two roots α and β in $\mathbb{Z}_v$ since $r(\chi) = x^2 + x + 1$ is the cyclotomic polynomial of order 3.

3.2 Step2 : calculation of the two roots of $r(\chi)$ mod$v$

Calculate the two roots α and β of $\chi^2+\chi+1$ mod v. First, generate a random number γ less than v. Then, calculate $\gamma^{(v-1)/3}$ mod v. If the result is not equal to 1, it is α and then $\beta = \alpha^2$ 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.

3.3 Step3 : primarity check for obtaining 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. Strictly speaking, w maybe 1–bit smaller than v at least because, as previously introduced, $r(\chi)$ is divisible by 3. Otherwise, return to **Step 1**. Of course, one can try $r(jv + \alpha)/v$ and $r(jv + \beta)/v$, where j is some integer. If one would like to make the bit sizes of v and w the same, at **Step 2** solve two roots α and β of $\chi^2+\chi+1$ modulo $3v$ though much more calculation time will be needed. Thus, the second prime number w is embedded.

3.4 Step4 : primarity check for $p(\chi)$ as the characteristic of $\mathbb{F}_p$

Corresponding to the almost primarity of $r(\alpha)/v$ or $r(\beta)/v$, $p(\alpha)$ or $p(\beta)$ needs to be a prime number for preparing the prime field $\mathbb{F}_p$. Finally, since r is divisible by two large prime numbers v and w, the purpose is achieved.

3.5 Remark

The reasons why this paper mainly considers the pairing–friendly elliptic curve introduced in **Sec**.2.1, it is related to the proposed algorithm, are as follows.

- Though $\rho \cdot k = 2$ will be the best [5], this curve can achieve $\rho \cdot k = 6$.
- Since the discriminant D is equal to 3, a lot of pairing–friendly curves can be generated. It contributes to the proposed *probablistic* algorithm.
- In addition, the implementation of *pairing* such as Ate pairing becomes efficient because *cubic* twist is available.

If it is allowed that the bit sizes of two prime factors v and w are different such as 500–bit and 1000–bit, the proposed method will be directly used for the cases that the degree of $r(\chi)$ is larger than 2 though $\rho \cdot k$ will become worse.

4 EXPERIMENTAL RESULT

In order to check the efficiency, under the computational environment shown in **Table** 1, the following sections show some experimental results with $b = 500$, where b also defined in **Fig**.3 is related to the bit size of prime factors v and w.

4.1 Generating the objective curve

Table 2 shows the average computation time for generating one *objective* pairing–friendly curve. In the

Table 1: Computational environment

CPU	Core 2 Quad *† 2.66GHz
Cash size	4096KB
OS	Linux(R)† 2.6.27
Language	C
Compiler	gcc 4.3.2
Library	GNU MP 4.2.2 [7]

*Pentium(R) is a registered trademark of Intel Corporation. †Linux(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.
†Only single core is used though it has four cores.

simulation, 30 pairing–friendly curves of embedding degree 3 whose order is a $2b$–bit composite number and has two almost b–bit prime factors have been generated. For example, generating one *objective* curve with $b = 500$ averagely took about 15 minutes. An example is shown in **App**.A. Thus, the proposed calculation procedure is sufficient practical. The proposed method can be applied for the other cases that the order $r(\chi)$ is given as a polynomial of degree 2 such as Eq.(3b).

It has been theoretically found that $r(\chi)$ is divisible by not only v, w but also 3, thus in this paper w is an *almost* b–bit prime. In order to obtain just b–bit prime factors v, w, α and β at **Step 2** can be calculated by $\chi^2 + \chi + 1 \bmod 3v$. For example, when the bit size of v and w is 512 bit, the calculation for generating *one* curve took a few hours on average although it will become more efficient.

4.2 Arithmetic operations in $\mathbb{F}_{p^3}$

For the following experiment, the base extension field $\mathbb{F}_{p^3}$ needs to have efficient arithmetic operations such as multiplication. According to the characteristic p given by Eq.(3a), the integer parameter χ at least needs to be chosen such that the denominator 3 divides the numerator $\chi^4 - \chi^3 + 2\chi + 1$. In detail, χ mod 3 must be 1. Then, using such an integer χ, it is theoretically shown that $p(\chi) - 1$ is also divisible by 3. It is an important property because it means that OEF (optimal extension field) technique [2] is always available for constructing the base extension field $\mathbb{F}_{p^3}$. OEF has efficient arithmetic operations including Frobenius map. **Table** 3 shows the average timings of arithmetics in $\mathbb{F}_{p^3}$.

4.3 Miller's algorithm of Xt–Ate pairing

In the case of Barreto–Neahrig (BN) curve, it is well–known that the Hamming weight of the loop parameter χ for Xate pairing is easily optimized so as to be small [11]; however, it is difficult for the target purpose. Thus, this paper has also applied NAF technique for the Miller's algorithm.

Since the embedding degree is equal to 3, many inversions by the vertical lines at **Step 4** and **7** in the Miller's algorithm **Fig**.2 are needed. According to the original paper [10], an efficient technique is introduced. It needs 10 $\mathbb{F}_p$–multiplications. In what follows, based on OEF technique, this paper introduces a more efficient inversion of the vertical lines.

Let a be the value of vertical line that is a certain non–zero element in $\mathbb{F}_{p^3}$ such as $v_{2T'}(P')$ in **Fig**.2. According to Itoh–Tsujii inversion algorithm [9], the inverse of a is given by

$$a^{-1} = N(a)^{-1} \cdot a^{p+p^2}, \tag{12}$$

where $N(a) \in \mathbb{F}_p$ is the norm of a. Since the *final exponentiation* is carried out after Miller's algorithm calculation, $N(a)^{-1}$ automatically becomes 1. Thus, only a^{p+p^2} needs to be calculated. Then, let a be represented as $a = a_0 + a_1\omega + a_2\omega^2$, where $a_0, a_1, a_2 \in \mathbb{F}_p$ and $\{1, \omega, \omega^2\}$ is the polynomial basis of OEF with $x^3 - u$ as the modular polynomial, a^{p+p^2} is efficiently calculated as follows.

$$\begin{aligned} a^{p+p^2} &= (a_0^2 - a_1 a_2 u) + (a_2^2 u - a_0 a_1)\omega \\ &\quad + (a_1^2 - a_0 a_2)\omega^2. \end{aligned} \tag{13a}$$

The following relation also helps the calculation.

$$\begin{aligned} a_1^2 - a_0 a_2 &= (a_0 + a_1 + a_2/2)(-a_0 + a_1 - a_2/2) \\ &\quad - a_0^2 - a_2^2/4. \end{aligned} \tag{13b}$$

Table 4 shows the average computation time of Xt–Ate pairing.

4.4 Final exponentiation

Let n be $(\chi-1)/3$. In this case, according to Eq.(3a), $\chi - 1$ needs to be divisible by 3. Based on Eqs.(14), the *final exponentiation* is optimized as shown in **Fig**.4. **Table** 5 shows the average computation time of *final exponentiation.*

$$\frac{p(\chi)^3 - 1}{r(\chi)} = (p(\chi) - 1) \cdot \frac{p(\chi)^2 + p(\chi) + 1}{r(\chi)}, \tag{14a}$$

$$\begin{aligned} \frac{p(\chi)^2 + p(\chi) + 1}{r(\chi)} &= \frac{\chi^6 - 3\chi^5 + 3\chi^4 + 4\chi^3 - 6\chi^2 - 3\chi + 13}{9} \\ &= \frac{(\chi^2 - 2\chi + 1)}{3} p(\chi) + \frac{\chi^3 - \chi^2 - \chi + 4}{3}, \end{aligned} \tag{14b}$$

$$\frac{p(\chi)^2 + p(\chi) + 1}{r(\chi)} = (3n^2)p(\chi) + (9n^3 + 6n^2 + 1). \tag{14c}$$

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

bit size b	average computation time [min.]
500	15

Table 3: Average timings of arithmetic operations in $\mathbb{F}_{p^3}$

bit size b	bit size of p	field	operation	timing [μsec.]
500	2000	$\mathbb{F}_p$	S_1	16.0
			M_1	16.1
			I_1	119
		$\mathbb{F}_{p^3}$	S_3	68.1
			M_3	68.7
			I_3	317

4.5 Other operations

Pairing–based cryptography needs not only pairing but also some other elliptic curve operations. **Table** 6 shows the average computation times of scalar multiplications in $\mathbb{G}_1, \mathbb{G}'_2$ and an exponentiation in $\mathbb{G}_3$.

According to Sakemi et al. [14], an arbitrary rational point $P(x_P, y_P)$ in $\mathbb{G}_1$, strictly speaking in $E(\mathbb{F}_p)$, satisfies the following relation. Thus, χ–adic representation of scalar $s < r$ accelerates scalar multiplication $[s]P$ in $\mathbb{G}_1$.

$$[p]P = [t-1]P = [\chi]P = (\epsilon x_P, y_P), \tag{15a}$$

where $\epsilon \in \mathbb{F}_p$ is a primitive cubic root of unity such that $\epsilon = z^{(p-1)/3}$. On the other hand, according to Galbraith et al. [6] and Nogami et al. [12], an arbitrary rational point $Q'(x_{Q'}, y_{Q'}) \in \mathbb{G}'_2$ satisfies the following relation.

$$[p]Q' = [t-1]Q' = [\chi]P = \tilde{\phi}(Q') = (\epsilon^2 x_{Q'}, y_{Q'}), \tag{15b}$$

where, according to OEF technique, the vector representation of ϵ^2 can be $(0, c, 0)$ or $(0, 0, c)$ with a certain non–zero $c \in \mathbb{F}_p$. It helps the calculation of Eq.(15b). In the same of Eq.(15a), $A \in \mathbb{G}_3$ satisfies the following relation.

$$A^{\chi} = A^p. \tag{15c}$$

Then, A^{χ} is calculated by Frobenius map with respect to $\mathbb{F}_p$. Thus, as shown in Eqs.(15), χ–adic representation plays an important role. For this experiment, that is **Table** 6, *joint–sparse form* (JSF) technique [15] is additionally applied.

In this case, co–factors $\#E(\mathbb{F}_{p^3})/r(\chi)$ and $\#E'(\mathbb{F}_{p^3})/r(\chi)$ are respectively given as follows. Thus, as Scott et al. [4] have introduced, the above relations will also accelerate *hashing* for $\mathbb{G}_1$ and $\mathbb{G}'_2$ in $E(\mathbb{F}_p)$ and $E'(\mathbb{F}_p)$, respectively.

$$\frac{\#E(\mathbb{F}_p)}{r(\chi)} = \frac{\chi^2 - 2\chi + 1}{3}, \tag{16a}$$

$$\frac{\#E'(\mathbb{F}_p)}{r(\chi)} = \frac{\chi^2 - 2\chi + 4}{3} = \frac{\#E(\mathbb{F}_p)}{r(\chi)} + 1. \tag{16b}$$

As previously introduced, $r(\chi)$ is divisible by 3, therefore the denominator 3 of the above equations can be canceled by $r(\chi)$.

5 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 parameter χ. As a future work, the cases that the degree of $r(\chi)$ is more than 2 should be considered.

REFERENCES

[1] M. Akane, Y. Nogami, and Y. Morikawa, "Fast Ate Pairing Computation of Embedding Degree 12 Using Subfield–Twisted Elliptic Curve," IEICE Trans., vol. E92–A, no. 2, pp. 508–516, Feb. 2009.

[2] D. Bailey and C. Paar, "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms," *Crypto' 98*, LNCS 1462, pp. 637–650, 1998.

[3] D. Boneh, "Bilinear Groups of Composite Order," *Pairing 2007*, LNCS 4575, Springer–Verlag, pp.1–1, 2007.

[4] A. Devegili, M. Scott, and R. Dahab, "Implementing Cryptographic Pairings over Barreto-Naehrig Curves," *Pairing 2007*, LNCS 4575, pp. 197–207, 2007.

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

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

Table 4: Average computation time of Xt–Ate pairing

bit size b	representation	average computation time [$m$sec.]
500	binary	372
	non–adjacent form	346

Table 5: Average computation time of *final exponentiation*

bit size b	average computation time [$m$sec.]
500	134

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

[8] F. Hess et al., "The Eta Pairing Revisited," IEEE Trans. Information Theory, pp. 4595–4602, 2006.

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

[10] X. Lin, C. Zhao, F. Zhang, and Y. Wang, "Computing the Ate Pairing on Elliptic Curves with Embedding Degree $k = 9$," available at http://eprint.iacr.org/2007/434.pdf.

[11] Y. Nogami et al. , "Integer Variable χ–based Ate Pairing," *Pairing 2008*, LNCS 5209, Springer–Verlag, pp. 178–191, 2008.

[12] Y. Nogami et al. , "Scalar Multiplication Using Frobenius Expansion over Twisted Elliptic Curve for Ate Pairing Based Cryptography," IEICE Trans., vol. E92–A, no. 1, pp. 182–189, Jan., 2009

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

[14] 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.

[15] 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.

A EXAMPLE (almost 500–bit prime factors case)

The following case has the order $r = v \cdot w \cdot a_1 \cdot a_2$.

$$\begin{aligned} v \;=\; & 2670084106973277813511449549453434609405319 6666 \\ & 1605977569516357782043166568301733849696177 2468 \\ & 0358079434917372258624519711953990374189607 8195 \\ & 0836010287927 \text{ (510–bit)} \end{aligned} \tag{17a}$$

$$\begin{aligned} w \;=\; & 32855552531522278212685340392885576388313543114 \\ & 24555503779720722424349615003749310188863960566 \\ & 09938913630219340628856422967691440527271102130 \\ & 9073672543 \text{ (501–bit)} \end{aligned} \tag{17b}$$

$$a_1 = 3 \text{ (2–bit)} \tag{18a}$$

$$a_2 = 79 \text{ (7–bit)} \tag{18b}$$

$$\begin{aligned} \chi \;=\; & 14419195541963378620756941490381165192261844 6 \\ & 64653230469468366172923202540902805216710928 7 \\ & 20188244002015987785722638563994858357012103 3 \\ & 2437354990985337892 \text{ (509–bit)} \end{aligned} \tag{19}$$

$$\begin{aligned} r(\chi) \;=\; & 20791320007737657210735453993273552995871405 73 \\ & 99691962973862109463790069718669650886684256 02 \\ & 00562693796725290570715232930529243877929218 87 \\ & 27552350692463703623868419310555373003873009 91 \\ & 70887899146172687056877447201031460802254607 60 \\ & 77405872905475058023977074844751497223222537 65 \\ & 6444603995609212807912396341557 \text{ (1018–bit)} \end{aligned} \tag{20a}$$

Table 6: Average computation times of scalar multiplications in $\mathbb{G}_1, \mathbb{G}_2'$ andan exponentiation in $\mathbb{G}_3$

bit size b	operation	calculation time $[ms]$
500	scalar multiplications † in $\mathbb{G}_1$ and $\mathbb{G}_2'$	65.6
	exponentiation in $\mathbb{G}_3$	33.5

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

$$
\begin{aligned}
p(\chi) \quad = \quad & 14409299588805073809909595258323431387871194 71\\
& 45645893924085377179202046863312972277475726 45\\
& 88619264518069829281838577122868310957333130 71\\
& 11098682550281974098080683567419799061425288 02\\
& 18512208736779975007152369619346255957846864 72\\
& 05921942980412954328833693789137032379600221 83\\
& 51743753008033792718747314923027712498094017 39\\
& 72768191661898038561819049206848922701919657 64\\
& 27876133264869797270394058698318358154581936 46\\
& 79615836481158675313618663482909437797818019 87\\
& 95938690607326081614048958627324791096710095 63\\
& 67696367703077238828878271327129612676867005 58\\
& 86374670353904229890965058232037610957951124 45\\
& 865235300688131 \text{ (2034–bit)} \qquad (20b)
\end{aligned}
$$

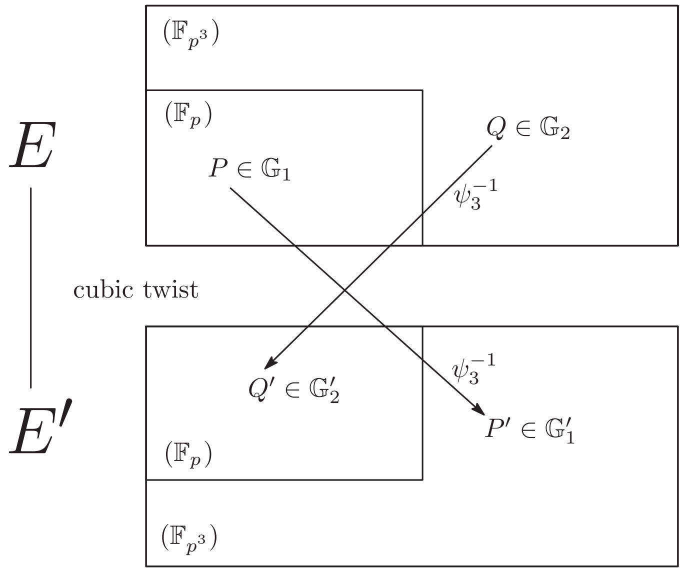

Figure 1: Relation among $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}'_1$, and $\mathbb{G}'_2$

Input : $s = t - 1 = \chi$, $P(x_P, y_P) \in \mathbb{G}_1$, $Q(x_Q, y_Q) \in \mathbb{G}_2$
Output : $f_{s,Q}(P)$

$P'(x_{P'}, y_{P'}) \leftarrow \psi_3^{-1}(P)$, $Q'(x_{Q'}, y_{Q'}) \leftarrow \psi_3^{-1}(Q)$
$f \leftarrow 1$, $T' \leftarrow Q'$
for $i = \lfloor \log_2 s \rfloor$ downto 1 do
    $f \leftarrow f^2 \cdot l_{T',T'}(P')/v_{2T'}(P')$
    $T' \leftarrow 2T'$
    if $s[i] = 1$ then
        $f \leftarrow f \cdot l_{T',Q'}(P')/v_{T'+Q'}(P')$
        $T' \leftarrow T' + Q'$
    end if
end for
return f

Figure 2: Miller's algorithm of Xt–Ate pairing

Input: bit size b
Output: an integer χ such that $r(\chi)$ has two almost b–bit prime factors

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

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

Figure 3: Proposed calculation procedure

Input :	$f,\ p,\ n = (\chi - 1)/3$
Output :	$f^{(p^3-1)/r} = \left(f^{p-1}\right)^{(3n^2)p+(9n^3+6n^2+1)}$
1.	$f \leftarrow f^p \cdot f^{-1}$
2.	$a \leftarrow (f^3)^{n^2}$
3.	$b \leftarrow (a^3)^n \cdot a^2 \cdot f$
4.	$f \leftarrow a^p \cdot b$
5.	return f

Figure 4: Final exponentiation