Pairing-friendly elliptic curves with small security loss by Cheon's algorithm

Aya Comuta[1], Mitsuru Kawazoe[2], and Tetsuya Takahashi[2]

[1] Graduate School of Science
Osaka Prefecture University
[2] Faculty of Liberal Arts and Sciences
Osaka Prefecture University
1-1 Gakuen-cho Naka-ku Sakai Osaka 599-8531 Japan
{kawazoe, takahasi}@las.osakafu-u.ac.jp

Abstract. Pairing based cryptography is a new public key cryptographic scheme. An elliptic curve suitable for pairing based cryptography is called a "pairing-friendly" elliptic curve. After Mitsunari, Sakai and Kasahara's traitor tracing scheme and Boneh and Boyen's short signature scheme, many protocols based on pairing-related problems such as the q-weak Diffie-Hellman problem have been proposed. In Eurocrypt 2006, Cheon proposed a new efficient algorithm to solve pairing-related problems and recently the complexity of Cheon's algorithm has been improved by Kozaki, Kutsuma and Matsuo. Due to these two works, an influence of Cheon's algorithm should be considered when we construct a suitable curves for the use of a protocol based on a pairing-related problem. Among known methods for constructing pairing-friendly elliptic curves, ones using cyclotomic polynomials such as the Brezing-Weng method and the Freeman-Scott-Teske method are affected by Cheon's algorithm. In this paper, we study how to reduce a security loss of a cyclotomic family by Cheon's algorithm. The proposed method constructs many pairing-friendly elliptic curves with small security loss by Cheon's algorithm suitable for protocols based on pairing-related problems.

Keywords: Pairing based cryptosystem, Elliptic curves, Weil pairing

1 Introduction

Pairing based cryptography is a new public key cryptographic scheme, which was proposed around 2000 by three important works due to Joux [15], Sakai, Ohgishi and Kasahara [22] and Boneh and Franklin [5]. In these last two papers, the authors constructed an identity-based encryption scheme by using the Weil pairing of elliptic curves. An elliptic curve suitable for pairing-based cryptography is called a "pairing-friendly" elliptic curve. It is very important to find an efficient method to construct pairing-friendly elliptic curves. There are many works on this topic: Miyaji, Nakabayashi and Takano [19], Cocks and Pinch [9],

Brezing and Weng [8], Barreto and Naerig [1], Scott and Barreto [21], Freeman, Scott and Teske [12] and so on.

In 2002, Mitsunari, Sakai and Kasahara proposed a new traitor tracing scheme based on the q-weak Diffie-Hellman problem [18]. The q-weak Diffie-Hellman problem is described as follows: Let g be an element of prime order ℓ in an abelian group and $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$. Then the q-weak Diffie-Hellman problem asks $[1/\alpha]g$ for given g, $[\alpha]g$, $[\alpha^2]g$,..., $[\alpha^q]g$. In 2004, Boneh and Boyen proposed a short signature scheme based on the q-strong Diffie-Hellman problem. After these two works, many protocols have been proposed based on q-weak Diffie-Hellman-like problems: [2], [3], [4], [20] and so on.

Before 2006, there had been no known efficient algorithm to solve the discrete logarithm problem related to the above protocols which works faster than the rho method and the square root method. However, in Eurocrypt 2006, Cheon proposed a new efficient algorithm which compute the discrete logarithm of the q-strong Diffie-Hellman problem [7]. Let ℓ be a group order, and g, $[\alpha]g$, $[\alpha^d]g$ given elements where d is a positive divisor of $\ell - 1$. Cheon's algorithm can compute α from these data in $O(\log \ell(\sqrt{\ell/d} + \sqrt{d}))$ group operations. In the same paper, Cheon gave an algorithm which computes α for a given g, $[\alpha^i]g$ for $i = 1, 2, \ldots, 2d$ in $O(\log \ell(\sqrt{\ell/d} + d))$ group operations where d is a divisor of $\ell + 1$. Recently, Kozaki, Kutsuma and Matsuo showed that the complexity of Cheon's algorithm can be reduced to $O(\sqrt{\ell/d}+\sqrt{d})$ for $d|(\ell-1)$ and $O(\sqrt{\ell/d}+d)$ for $d|(\ell+1)$, respectively [16]. It is obvious that the complexity is reduced when $d(< \sqrt{\ell})$ becomes larger. When $d = O(\ell^{1/2})$, the cost becomes $O(\ell^{1/4})$ which is much smaller than the rho method and the square root method. Hence, one should be careful about the order of an elliptic curve used for protocols based on the q-weak Diffie-Hellman problem, the q-strong Diffie-Hellman problem or other related problems. In all methods for constructing pairing-friendly elliptic curves except for the Cocks-Pinch method, the order of an elliptic curve is given by an irreducible polynomial $\ell(x)$. If $\ell(x) \pm 1$ is reducible, there is a big security loss due to Cheon's algorithm. In fact, for an example for $k = 10$ in [11], for $k = 12$ in [1], all examples in [8], and curves obtained by using cyclotomic fields in [12], the polynomials have a polynomial factor of degree 1 or 2. Though the advantage of cyclotomic methods is that one can take the ratio ρ of bit length between the size of the defining field and the order of the group less than two, these are affected by Cheon's algorithm for the use of protocols based on pairing-related problems.

In this paper, we study how to reduce a security loss of a cyclotomic family by Cheon's algorithm keeping its advantage for the value of ρ. We propose an improved method by which we can obtain pairing-friendly elliptic curves with a small security loss. The key idea is to take ℓ as a proper divisor of $\Phi_k(x)$ where $k = 2n$ for a prime n and Φ_k is the k-th cyclotomic polynomial. Heuristically, the proposed method gives pairing-friendly elliptic curves curves whose security loss by Cheon's algorithm is within 5 bits for $k \leq 38$. We note that ρ of constructed curves is kept as $\rho < 2$, moreover almost same as the Freeman-Scott-Teske method.

We give the outline of this article. In Section 2, we recall the Weil paring and the condition to construct a secure and efficient pairing based cryptosystem. In Section 3, we recall the q-weak/strong Diffie-Hellman problem and Cheon's algorithm. In Section 4, for known methods of constructing pairing-friendly elliptic curves, we study the affect of Cheon's algorithm on them. In Section 5, we study how to reduce the security loss of cyclotomic methods and give an improved method to construct pairing-friendly elliptic curves with small security loss. We also gives examples obtained by using the proposed method. Finally, we summarize our result in Section 6.

2 Pairing based cryptosystem

Let $K := \mathbb{F}_q$ be a finite field with q elements and E an elliptic curve defined over K. The finite abelian group of K-rational points of E and its order are denoted by $E(K)$ and $\#E(K)$, respectively. Assume that $E(K)$ has a subgroup G of a large prime order. The most simple case is that $E(K) = G$, that is, the order of $E(K)$ is prime. Let ℓ be the order of G. We denote by $E[\ell]$ the group of ℓ-torsion points of $E(\overline{K})$ where $\overline{K}$ is an algebraic closure of K. In the following, we denote $\log_2 x$ by $\lg x$.

For a positive integer ℓ coprime to the characteristic of K, the Weil pairing is a map

$$e_\ell : E[\ell] \times E[\ell] \to \mu_\ell \subset \hat{K}^*$$

where $\hat{K}$ is the field extension of K generated by coordinates of all points in $E[\ell]$, $\hat{K}^*$ is the multiplicative group of $\hat{K}$ and μ_ℓ is the group of ℓ-th roots of unity in $\hat{K}^*$. For the details of the Weil pairing, see [23] for example. The key idea of pairing based cryptography is based on the fact that the subgroup $G = \langle P \rangle$ is embedded into the multiplicative group $\mu_\ell \subset \hat{K}^*$ via the Weil pairing or some other pairing map.

The extension degree of the field extension $\hat{K}/K$ is called the embedding degree of E with respect to ℓ. It is known that E has the embedding degree k with respect to ℓ if and only if k is the smallest integer such that ℓ divides $q^k - 1$. In pairing based cryptography, the following conditions must be satisfied to make a system secure:

- the order ℓ of a prime order subgroup of $E(K)$ should be large enough so that solving a discrete logarithm problem on the group is computationally infeasible and
- q^k should be large enough so that solving a discrete logarithm problem on the multiplicative group $\mathbb{F}_{q^k}^*$ is computationally infeasible.

Moreover for an efficient implementation of a pairing based cryptosystem, the following are important:

- the embedding degree k should be appropriately small and
- the ratio $\lg q / \lg \ell$ should be appropriately small.

Elliptic curves satisfying the above four conditions are called "pairing-friendly" elliptic curves.

In practice, it is currently recommended that ℓ should be larger than 2^{160} and q^k should be larger than 2^{1024}.

In the following, we only consider the case $K = \mathbb{F}_p$ where p is an odd prime.

3 Protocols based on pairing-related problem and Cheon's algorithm

3.1 Pairing-related problems

A new traitor tracing scheme proposed by Mitsunari, Sakai and Kasahara [18] in 2002 is based on the q-weak Diffie-Hellman problem. The definition of the q-weak Diffie-Hellman problem is as follows.

Definition 1 (The q-weak Diffie-Hellman problem). *Let G be an abelian group whose order is a large prime number ℓ. The q-weak Diffie-Hellman problem asks $[1/\alpha]g$ for a $(q+1)$-tuple $(g, [\alpha]g, [\alpha^2]g, \ldots, [\alpha^q]g)$ where $g \in G$ and $\alpha \in (\mathbb{Z}/\ell\mathbb{Z})^\times$.*

The q-weak Diffie-Hellman problem is also called the "q-Diffie-Hellman inversion problem" in [2].

In 2004, Boneh and Boyen proposed a short signature scheme based on the q-strong Diffie-Hellman problem which is defined as follows [3].

Definition 2 (The q-strong Diffie-Hellman problem). *Let G be an abelian group whose order is a large prime number ℓ. The q-strong Diffie-Hellman problem asks a pair $([1/(\alpha+a)]h, a)$ where a is any element in $(\mathbb{Z}/\ell\mathbb{Z})^\times$ for a $(q+2)$-tuple $(h \in H, g, [\alpha]g, [\alpha^2]g, \ldots, [\alpha^q]g)$ where H is an abelian group of order ℓ, $g \in G$ and $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$.*

After Mitsunari, Sakai and Kasahara's work [18] and Boneh and Boyen's work [3], many protocols without random oracles have been proposed based on weak Diffie-Hellman-like problems, e.g. [2], [4], [20]. In the following, we call such kind of problems the "pairing-related problems".

For the definition of other pairing-related problems, e.g. the q-bilinear Diffie-Hellman inversion problem and the $(q+1)$-bilinear Diffie-Hellman exponent problem, see [2], [4] and so on.

3.2 Cheon's algorithm and its improvement

In Eurocrypt 2006, Cheon [7] proposed an algorithm to solve the q-weak/strong Diffie-Hellman problem. Very recently, Kozaki, Kutsuma and Matsuo [16] improved the complexity of Cheon's algorithm for the q-weak Diffie-Hellman problem. For an abelian group G of prime order ℓ, if $\ell - 1$ has a positive divisor less than or equal to q, then their improved algorithm can solve the q-weak

Diffie-Hellman problem within $O\left(\sqrt{\ell/d}+\sqrt{d}\right)$ group operations using space for $O\left(\max\left(\sqrt{\ell/d},\sqrt{d}\right)\right)$ group elements. There also exists an $\ell+1$ variant of this algorithm. The details of the results in [16] are as follows:

Theorem 1 ([16]). *Let g be an element of prime order ℓ in an abelian group. Suppose that d is a positive divisor of $\ell-1$. If g, $[\alpha]g$ and $[\alpha^d]g$ are given, α can be computed within $O\left(\sqrt{\ell/d}+\sqrt{d}\right)$ group operations using space for $O\left(\max\left(\sqrt{\ell/d},\sqrt{d}\right)\right)$ group elements.*

Theorem 2 ([16]). *Let g be an element of prime order ℓ in an abelian group. Suppose that d is a positive divisor of $\ell+1$ and $[\alpha^i]g$ for $i=1,2,\ldots,2d$ are given. Then α can be computed within $O\left(\sqrt{\ell/d}+d\right)$ group operations using space for $O\left(\max\left(\sqrt{\ell/d},\sqrt{d}\right)\right)$ group elements.*

Remark 1. In the original result of Cheon [7], the complexity in the above two theorems were given by $O\left(\log\ell\left(\sqrt{\ell/d}+\sqrt{d}\right)\right)$ and $O\left(\log\ell\left(\sqrt{\ell/d}+d\right)\right)$ group operations, respectively.

3.3 The Effect of Cheon's algorithm for constructing pairing-friendly elliptic curves

In this section, we consider the effect of Cheon's algorithm on known methods which construct pairing-friendly elliptic curves.

With respect to Cocks-Pinch method, the group size ℓ can be randomly chosen. So it is not difficult to avoid the security loss by Cheon's algorithm. See Section 6 of [16] for the details.

Except for Cocks-Pinch method, since the group order ℓ is given by a polynomial $\ell(x)$, we should be careful about the effect of Cheon's algorithm. More precisely, if a polynomial $\ell(x)\pm1$ is reducible and its non-trivial polynomial factor $h(x)$ has a small degree, there is a $(\lg h(x))/2$ bits security loss by Cheon's algorithm. In the following, we see the security loss by Cheon's algorithm for each method using polynomials.

The MNT method and its variant. In the MNT method based on Miyaji, Nakabayashi and Takano's result [19], the following polynomials are used: $\ell(x)=12x^2\pm6x+1$ for $k=3$, $\ell(x)=x^2+2x+2$ or x^2+1 for $k=4$ and $\ell(x)=4x^2\pm2x+1$ for $k=6$. Except for $\ell(x)=\ell^2+2\ell+2$ in the case $k=4$, $\ell(x)-1$ is divisible by x. For the generalized MNT method such as Galbraith, McKee and Valença's method [13], there are some cases that $\ell(x)\pm1$ are reducible. Since the degree of $\ell(x)$ equals two, this fact does not lead directly that Cheon's algorithm affects on these methods.

A Cyclotomic Family. There are some methods using a cyclotomic polynomial as $\ell(x)$, e.g. Brezing and Weng's method [8] and Freedman, Scott and Teske's method [12]. We call these methods a "cyclotomic family". The advantage of a cyclotomic family is that one can take curves with relatively small $\rho(< 2)$.

All of them use a cyclotomic polynomial to set a prime ℓ as $\ell = \Phi_k(x)$ or $\ell = \Phi_{ck}(x)$ for some $c > 1$ where k is the embedding degree. Then, $\ell - 1$ is factored by x at least. Moreover, if $ck = 2^m$, then $\ell - 1$ is factored by $x^{2^{m-1}}$, otherwise $\ell - 1$ is factored by $x(x + 1)$ or $x(x - 1)$. The size of x is about $\lg \ell/\varphi(ck)$ bits, $c \geq 1$, where φ is the Euler phi function. Hence, if $x < q$ (resp. $x(x + 1) < q$), the complexity to solve the q-weak Diffie-Hellman problem is reduced to $O(\sqrt{\ell^{1-1/\varphi(ck)}} + \sqrt{\ell^{1/\varphi(ck)}})$ (resp. $O(\sqrt{\ell^{1-2/\varphi(ck)}} + \sqrt{\ell^{2/\varphi(ck)}})$) group operations.

Other methods. For $k = 10$, Freeman gave the following family [11].

$$p(x) = 25x^4 + 25x^3 + 25x^2 + 10x + 3$$
$$\ell(x) = 25x^4 + 25x^3 + 15x^2 + 5x + 1$$
$$Dy^2 = 15x^2 + 10x + 3$$

For this family, $\ell(x) \pm 1$ factor as

$$\ell(x) - 1 = 5x(5x^3 + 5x^2 + 3xz + 1)$$
$$\ell(x) + 1 = (5x^2 + 1)(5x^2 + 5x + 2).$$

The following two examples are given in [11].

$$\ell = 5031898990973855325985710847786081764109733 51$$
$$\ell = 6109996327108312874607376956745050221908714591643483962630 1$$

The former is a 149 bit prime and the latter is a 196 bit prime. For each example, $\ell - 1$ factors as

$$\ell - 1 = 2 \cdot 5^2 \cdot 853 \cdot (\text{a 33 bit prime}) \cdot (\text{a 39 bit prime}) \cdot (\text{a 63 bit prime})$$
$$\ell - 1 = 2^2 \cdot 5^2 \cdot 7 \ \cdot (\text{a 29 bit prime}) \cdot (\text{a 44 bit prime}) \cdot (\text{a 114 bit prime})$$

respectively. Cheon's algorithm affects on each case.

For $k = 12$, Barreto and Naerig gave the following family [1].

$$\ell(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$
$$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$
$$Dy^2 = 3(6x^2 + 4x + 1)$$

For this family, $\ell(x) \pm 1$ factor as

$$\ell(x) - 1 = x(6x^3 + 6x^2 + 3x + 1)$$
$$\ell(x) + 1 = (3x^2 + 3x + 1)(6x^2 + 1).$$

The following example is given in [1].

$$\ell = 146150162449679026514544738099497118849930002761 3 \text{ (160 bit)}$$

For this example, we have

$$\begin{aligned}\ell - 1 =& 2^2 \cdot 3 \cdot (\text{a 24 bit prime}) \cdot (\text{a 38 bit prime}) \cdot (\text{a 39 bit prime}) \\ & \cdot (\text{a 57 bit prime}) \\ \ell + 1 =& 2 \cdot 7 \cdot 13 \cdot 19 \cdot 1279 \cdot 1861 \cdot 21227 \cdot (\text{a 19 bit prime}) \cdot (\text{a 21 bit prime}) \\ & \cdot (\text{a 24 bit prime}) \cdot (\text{a 50 bit prime}).\end{aligned}$$

Hence Cheon's algorithm affects on it.

4 How to reduce a security loss of a cyclotomic family

In this section, we consider the way to reduce the security loss by Cheon's algorithm for a cyclotomic family with embedding degree $k = 2n$, n an odd prime. The idea is to take ℓ as a proper divisor of $\Phi_k(x)$.

4.1 The condition of a large prime factor of $\Phi_k(x)$

We study the condition for the large prime factor ℓ of $\Phi_k(x)$. Note that when $k = 2n$ and n is an odd prime, $\Phi_{2n}(x) = \Phi_n(-x)$.

Lemma 1. *Let n and ℓ be primes and x an integer. If $\Phi_n(x) \equiv 0 \pmod{\ell}$, then $\ell = n$ or $\ell \equiv 1 \pmod{n}$.*

Proof. Assume that $\Phi_n(x) \equiv 0 \pmod{\ell}$ and $\ell \neq n$. Then $\Phi_n(x) \equiv 0 \pmod{\ell}$ yields that x gives a primitive n-th root of unity in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. Hence n divides $\#(\mathbb{Z}/\ell\mathbb{Z})^\times = \ell - 1$; that is, $\ell \equiv 1 \pmod{n}$. □

Theorem 3. *Let k be a positive integer of the form $k = 2n$, where n is an odd prime. Let x be an integer, ℓ a large prime greater than n and s a small integer such that $\Phi_k(x) = s\ell$. Then the following hold:*

1. *If s is divisible by n, then $x \equiv -1 \pmod{n}$ and s is not divisible by n^2.*
2. *If $s = n$, then $\ell - 1$ is divisible by $x + 1$.*
3. *If s is not divisible by n, then $x \not\equiv -1 \pmod{n}$.*

Remark 2. In Theorem 3, note that by the assumption $\ell > n$ and Lemma 1, $\ell - 1$ is divisible by n. Moreover, it is easy to see that $\ell^2 - 1$ is divisible by 24. Hence $(\ell + 1)(\ell - 1)$ is divisible by $24n$. We also note that If s is a small prime which divides $\Phi_k(x)$ for an integer x, then $s = n$ or $s \equiv 1 \mod n$.

Proof. First, note that $\ell - 1 = \Phi_k(x)/s - 1 = (\Phi_n(-x) - s)/s$. Second, note that if $x \not\equiv -1$, then $\Phi_k(x) = \Phi_n(-x) = ((-x)^p - 1)/(-x-1) \equiv (-x-1)/(-x-1) = 1 \pmod{n}$ and hence, if n divides s, we have $x \equiv -1 \pmod{n}$.

(1) From the above, if n divides s, then $x \equiv -1 \pmod{n}$. Hence we only have to show that n^2 does not divide s. Write $s = tn$ where t is an integer. Since $\ell \equiv 1 \pmod{n}$ from the assumption of the theorem and $\Phi_n(-x) - tn = \Phi_k(x) - tn = tn(\ell - 1)$, we have that $\Phi_n(-x) - tn \equiv 0 \pmod{n^2}$. Since $\Phi_n(-x) \equiv n \pmod{n^2}$ in this case, we have that $t \not\equiv 0 \pmod{n}$; that is, n^2 does not divide s.

(2) If $s = n$, then since $\Phi_k(-1) - s = \Phi_n(1) - n = 0$, $\Phi_k(x) - s$ has a factor $x + 1$. More precisely, we have $\Phi_k(x) - n = \Phi_n(-x) - n = -(x+1)((-x)^{n-2} + 2(-x)^{n-3} + \cdots + (n-2)x + (n-1))$. Since $x + 1 \equiv 0 \pmod{n}$ in this case and n is an odd prime, $(-x)^{n-2} + 2(-x)^{n-3} + \cdots + (n-2)(-x) + (n-1) \equiv n(n-1)/2 \equiv 0 \pmod{n}$. Hence we have $\ell - 1 = (\Phi_n(-x) - n)/n$ has a factor $x + 1$.

(3) Suppose that $x \equiv -1 \pmod{n}$. Then $\Phi_k(x) \equiv \Phi_n(1) \equiv 0 \pmod{n}$. This contradicts the assumption that n does not divide s. □

In particular, the case (2) in Theorem 3 is not suitable for the protocols based on pairing-related problems if we consider an affect of Cheon's algorithm.

Remark 3. For the case that k is an odd prime, that is $k = n$, we have a similar result.

4.2 Our construction

From the result of the previous section, we propose a method to construct pairing-friendly elliptic curves with small security loss by Cheon's algorithm.

We only consider the case that k is in the form $k = 2n$ where n is an odd prime. Our construction is an improved version of the Freeman-Scott-Teske method. Since the Freeman-Scott-Teske method needs a field extension, we should use $\Phi_{ck}(x)$ where c is an extension degree. So when we take ℓ as a proper divisor of a cyclotomic polynomial in the Freeman-Scott-Teske method, ℓ and p become much larger. Here we improve the Freeman-Scott-Teske method such that we can obtain the small ρ value with not so much large ℓ and p even when we take ℓ as a proper divisor of a cyclotomic polynomial.

First note that for $k = 2n$ with an odd prime n, if g is a primitive k-th root of unity in a field K, then $\sqrt{-g} = g^{(n+1)/2}$ belongs to K. Our idea is to use this $\sqrt{-g} = g^{(n+1)/2}$ as $\sqrt{-D}$. The advantage to use such $\sqrt{-D}$ is that we do not need to extend a cyclotomic field $\mathbb{Q}(\zeta_k)$ to obtain a small value of $\rho = \lg p / \lg \ell$. In the following, we describe our method which is divided into two cases: (1) the case of a general n, (2) the case of $n \equiv 1 \pmod{4}$.

The general case. Let g be a positive integer such that $\Phi_k(g) = s\ell$ for a very small integer s and a large prime ℓ. Then, g is a primitive k-th root of unity modulo ℓ and $\sqrt{-g} \equiv g^{(n+1)/2} \pmod{\ell}$. Take D, a, b $(0 < D, a, b < \ell)$ as follows:

$$D := g, \qquad a := g + 1, \qquad b :\equiv (g-1)g^{(n+1)/2}/g \pmod{\ell}.$$

Then, $p = (a^2 + Db^2)/4 = O(g^{n+2})$ and $\ell = O(g^{\varphi(n)}) = O(g^{n-1})$, where φ denotes the Euler phi function.

Since s is very small, we have $\rho \sim (n+2)/(n-1)$ as $p, \ell \to \infty$.

Improvement for $n \equiv 1 \pmod 4$. When $n \equiv 1 \pmod 4$, we can improve the asymptotic value of ρ.

Let g, $\Phi_k(g) = s\ell$ be as in the general case. Then, g is a primitive k-th root of unity modulo ℓ and $\sqrt{-g} \equiv g^{(n+1)/2} \pmod \ell$. Note that $g^{(n+1)/2}$ is also a primitive k-th root of unity modulo ℓ. Take D, a, b $(0 < D, a, b < \ell)$ as follows:

$$D := g, \qquad a := g^{(n+1)/2} + 1, \qquad b :\equiv (g^{(n+1)/2} - 1)g^{(n+1)/2}/g \pmod \ell.$$

Then, since

$$b \equiv (g^{(n+1)/2} - 1)g^{(n-1)/2} \equiv g^n - g^{(n-1)/2} \equiv -1 - g^{(n-1)/2} \pmod \ell,$$

$p = (a^2 + Db^2)/4 = O(g^{n+1})$ and $\ell = O(g^{\varphi(n)}) = O(g^{n-1})$.

Since s is very small, we have $\rho \sim (n+1)/(n-1)$ as $p, \ell \to \infty$.

The algorithm of our construction is given as follows.

Algorithm 1 *(Curve construction with small security loss by Cheon's algorithm)*

Input:	*n: an odd prime; α, β, q: positive integers*
Output:	*p, ℓ : primes,*
	$E/\mathbb{F}_p$: an elliptic curve over $\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = \ell$ and its embedding degree equals $k = 2n$.
Step 1:	*Find $g \in \mathbb{Z}_{>0}$ such that $\Phi_k(g) = s\ell$ where ℓ is a large prime, s is a small prime ($\neq n$) or $n\cdot$(a small prime) and* $$\ell - 1 = 2n(a \text{ positive integer} \leq 2^\alpha)\prod(\text{prime} \geq q)$$ $$\ell + 1 = 2(a \text{ positive integer} \leq 2^\beta)\prod(\text{prime} \geq q)$$
Step 2:	*Set $a := g$ if $n \equiv 3 \pmod 4$ and $a := g^{(n+1)/2}$ if $n \equiv 1 \pmod 4$. Take b as a positive integer ($< \ell$) such that $b \equiv (a-2)g^{(n+1)/2}/g \pmod \ell$. Set $D := g$ and check whether $p := (a^2 + Db^2)/4$ is prime or not. If not, return to Step 1.*
Step 3:	*Use the CM method and output the result.*

Remark 4. The positive integer q in the input is a parameter of the q-weak/strong Diffie-Hellman problem. The size of q depends on a protocol and the ability of attackers. The positive integers α and β in the input are parameters which determine the bound of the security loss by Cheon's algorithm. We take $\alpha = \beta = 6$ for examples in the next section.

Remark 5. Using the CM method, we can construct an ordinary elliptic curves with the complex multiplication by an order of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, $D > 0$. Refer to [14] for the details of the calculation. In general, for a large D, it is hard to construct the elliptic curve by the CM method. Therefore we must be careful with the size of D.

In our method, we set $D = g$. If g is not square free, then we set the square free part of g as D. So the size of g is important when we construct the elliptic curve using the CM method. But as stated in [12], we can construct an elliptic curve by using the CM method for $D < 10^{10}$. Hence our method is effective to construct pairing-friendly elliptic curves.

4.3 Examples

Here we show examples of pairing-friendly elliptic curves with small security loss by Cheon's algorithm. The following examples are obtained by using Algorithm 1 with $q = 2^{50}$ and $\alpha = \beta = 6$ for $14 \leq k \leq 38$. The security loss of these examples is within 5 bits, if the parameter q in the weak/strong Diffie-Hellman problem is less than 50 bits.

k	14
x	1083603511
s	29
ℓ	558244461317143757104672701626918998407404333205677 39 (176 bit)
p	514960170149890114984943679980935183448944966356640500013 99\ 1240135020678496405311
ρ	1.53017
$\ell - 1$	$2 \cdot 7 \cdot$ (a 69 bit prime) $\cdot$ (a 103 bit prime)
$\ell + 1$	$2^2 \cdot 3 \cdot 5 \cdot$ (a 65 bit prime) $\cdot$ (a 106 bit prime)

k	22
x	2169245
s	67
ℓ	3443586908389364671503933551495445912546234980894932315809 9\ 743 (205 bit)
p	588777865170451584805794619560117163390175708714374929802 01\ 25450311726006289864629
ρ	1.32879
$\ell - 1$	$2 \cdot 11 \cdot$ (a 74 bit prime) $\cdot$(a 127 bit prime)
$\ell + 1$	$2^5 \cdot 3 \cdot$ (a 73 bit prime) $\cdot$ (a 125 bit prime)

k	26
x	83647
s	131
ℓ	895628588110024088164630713805121667532341241783716653231 (190 bit)
p	205234503517549804087697034282723328113680929749523557844160697479999
ρ	1.19947
$\ell-1$	$2\cdot 5\cdot 13\cdot$ (a 55 bit prime) $\cdot$ (a 128 bit prime)
$\ell+1$	$2^4\cdot 3\cdot$ (an 84 bit prime) $\cdot$ (a 100 bit prime)

k	34
x	1730735
s	$17\cdot 137$
ℓ	27830402151707213772790243425060710128851524965270716441651\ 11328554663063808567192444024844854329 (321 bit)
p	48538978648626809809653096381338491065159598631595616079566\ 88321815318124568522625897243485762842754461264104559
ρ	1.15803
$\ell-1$	$2^3\cdot 17\cdot$ (a 92 bit prime) $\cdot$ (a 222 bit prime)
$\ell+1$	$2\cdot 3\cdot 5\cdot$ (a 102 bit prime) $\cdot$ (a 214 bit prime)

k	38
x	422017
s	2281
ℓ	790337723267050188305022454444094380417744794380570733637116302209872371789154909326097787467243 13 (326 bit)
p	338740258071382406654996234276460244971409999229416672234981292708135574186765029417190820245096393386611946657091187 3
ρ	1.20054
$\ell-1$	$2^3\cdot 3\cdot 19\cdot$(a 66 bit prime)$\cdot$(a 71 bit prime)$\cdot$ (an 83 bit prime)$\cdot$(a 99 bit prime)
$\ell+1$	$2\cdot 7\cdot$ (a 74 bit prime) $\cdot$ (a 118 bit prime) $\cdot$ (a 131 bit prime)

5 Conclusion

In this article, we studied the effect of Cheon's algorithm on known methods of constructing pairing-friendly elliptic curves. We showed that Cheon's algorithm affects on methods using cyclotomic polynomials. We considered the way to reduce the security loss of a cyclotomic family by Cheon's algorithm and proposed a method to construct pairing-friendly elliptic curves with small security loss by Cheon's algorithm. Also we showed examples of curves obtained by using our method.

References

1. P.S.L.M. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, In Proceedings of SAC 2005 Workshop on Selected Areas in Cryptography, LNCS3897, pp. 319–331. Springer, 2006.
2. D. Boneh and X. Boyen, *Efficient selective-ID secure identity-based encryption without random oracles*, Advances in Cryptology – EUROCRYPT 2004 (C. Cachin and J. Camenisch, eds.), LNCS 3027, Springer-Verlag, 2004, pp. 223–238.
3. D. Boneh and X. Boyen, *Short signatures without random oracles*, Advances in Cryptology – EUROCRYPT 2004 (C. Cachin and J. Camenisch, eds.), LNCS 3027, Springer-Verlag, 2004, pp. 56–73.
4. D. Boneh, X. Boyen and E.-J. Goh, *Hierarchical identity based encryption with constant size ciphertext*, Cryptology ePrint Archive, Report 2005/015, 2005, An extended abstract appears in Advances in Cryptology - EUROCRYPT 2005 (R. Cramer, ed.), LNCS 3494, Springer-Verlag, 2005, pp. 440–456.
5. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, SIAM Journal of Computing, **32**(3) (2003), pp. 586–615.
6. I.-F. Blake, G. Seroussi and N.-P. Smart, Advances in Elliptic Curve Cryptography, Cambridge University Press, 2005.
7. J. H. Cheon, *Security Analysis of the Strong Diffie-Hellman Problem*, Advances in Cryptology - EUROCRYPT 2006, LNCS 4004, pp. 1–11, Springer, 2006.
8. F. Brezing and A. Weng, *Elliptic curves suitable for pairing based cryptography*, Design, Codes and Cryptography, **37** (2005), pp. 133–141.
9. C. Cocks and R. G. E. Pinch, *Identity-based cryptosystems based on the Weil pairing*, Unpublished manuscript, 2001.
10. D. Freeman, *Methods for constructing pairing-friendly elliptic curves*, 10th Workshop on Elliptic Curves in Cryptography (ECC 2006), Toronto, Canada, September 2006.
11. D. Freeman, *Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10*, Cryptology ePrint Archive, Report 2006/026, 2006 http://eprint.iacr.org/.
12. D. Freeman, M. Scott and E. Teske, *A taxonomy of pairing-friendly elliptic curves*, Cryptology ePrint Archive, Report 2006/372, 2006 http://eprint.iacr.org/.
13. S. Galbraith, J. McKee and P. Valença, *Ordinary abelian varieties having small embedding degree*, In Proc. Workshop on Mathematical Problems and Techniques in Cryptology, pp. 29–45. CRM, Barcelona, 2005.
14. IEEE Computer Society, New York, USA. *IEEE Standard Specifications For Public-Key Cryptography - IEEE Std 1363-2000*, 2000.
15. A. Joux, *A one round protocol for tripartite Diffie-Hellman*, In Algorithmic Number Theory Symposium ANTS-IV, volume 1838 of Lecture Notes in Computer Science, pp. 385–393. Springer-Verlag, 2000. Full version: Journal of Cryptology **17** (2004), 263–276.
16. S. Kozaki, T. Kutsuma and K. Matsuo, *Remarks on Cheon's algorithms for pairing-related problems*, to appear in the proceedings of "Pairing 2007", Yokohama, Japan, 2007.
17. T. Kutsuma and K. Matsuo, *Remarks on Cheon's algorithms for pairing-related problems*, In 2007 Symposium on Cryptography and Information Security (SCIS2007), Nagasaki, Japan, 2007.
18. S. Mitsunari, R. Sakai and M. Kasahara, *A new traitor tracing*, IEICE Trans. Fundamentals **E85-A** (2002), no. 2, pp. 481–484.

19. A. Miyaji, M. Nakabayashi and S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Transactions on Fundamentals **E84-A**(5) (2001), pp. 1234–1243.
20. T. Okamoto, *Efficient blind and partially blind signatures without random oracles*, TCC 2006 (S. Halevi and T. Rabin, eds.), LNCS 3876, Springer-Verlag, 2006, pp. 80–99.
21. M. Scott and P.S.L.M. Barreto, *Generating more MNT elliptic curves*, Designs, Codes and Cryptography **38** (2006), pp. 209–217.
22. R. Sakai, K. Ohgishi and M. Kasahara, *Cryptosystem based on pairing*, In 2000 Symposium on Cryptography and Information Security (SCIS 2000), Okinawa, Japan, 2000.
23. J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, GTM 106, 1986.