How to construct pairing-friendly elliptic curves for the embedding degree $2n$, n is an odd prime

Abstract. Pairing based cryptography is a new public key cryptographic scheme. The most popular one is constructed by using the Weil or Tate pairing of elliptic curves. An elliptic curve suitable for pairing based cryptography is called a "pairing-friendly" elliptic curve. Freeman-Scott-Teske proposed a new method to obtain pairing-friendly elliptic curves over a finite prime field, improving Brezing and Weng's result. In this article, for the embedding degree in the form $2n$ with an odd prime n, we propose an improved method which produces more pairing-friendly elliptic curves than the Freeman-Scott-Teske method does for a given range of the group order. Moreover, we study how to avoid an attack based on Cheon's algorithm.

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 [14], Sakai, Ohgishi and Kasahara [20] 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.

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

Roughly speaking, pairing based cryptography uses the fact that the subgroup $G \subset E[\ell]$ can be embedded into the multiplicative group μ_ℓ of ℓ-th roots of unity in $\mathbb{F}_{q^k}^*$ for some positive integer k by using the Weil pairing or some other pairing map. The extension degree k is called *embedding degree*.

In pairing based cryptography, it is required that ℓ and q^k should be sufficiently large but k and the ratio $\rho := \lg q / \lg \ell$ should be appropriately small. An elliptic curve satisfying these conditions is called a "pairing-friendly" elliptic curve. It is very important to construct an efficient method to find pairing-friendly elliptic curves. There are many works on this topic: [17], [9], [8], [1], [19] and so on. Recently, Freeman, Scott and Teske [11] proposed a method to obtain pairing-friendly elliptic curves over a finite prime field $\mathbb{F}_p$ with a small ρ,

following Brezing and Weng's result [8] which uses cyclotomic fields. In [11], they take $\ell(x)$ as a cyclotomic polynomial $\Phi_{ck}(x)$ for some integer c and set a prime number $\ell := \ell(g)$ if $\ell(g)$ is a prime for some positive integer g. Note that g is a primitive ck-th root of unity in $\mathbb{Z}/\ell\mathbb{Z}$. As is stated in [11], the polynomial degree of $\ell(x)$ is important to obtain enough pairing-friendly elliptic curves with the appropriate size of ℓ and p. The method in [11] needs an extension field $\mathbb{Q}(\zeta_{ck})$ of a cyclotomic field $\mathbb{Q}(\zeta_k)$ for some $c > 1$. So the degree of $\ell(x)$ becomes large and therefore ℓ and p of pairing-friendly elliptic curves become extremely large, greater than 200 bits in many cases.

In this article, we propose an improved method which enables us to take $c = 1$. In particular, for the case that $k = 2n$ with an odd prime n, asymptotic values of the ratio ρ as $p, \ell \to \infty$ are as follows:

	Our result		Freeman et al.	
k	ρ	$\deg \ell(x)$	ρ	$\deg \ell(x)$
14	$3/2(= 1.5)$	6	$4/3(= 1.33333\ldots)$	12
22	$13/10(= 1.3)$*	10	$13/10(= 1.3)$	20
26	$7/6(= 1.16666\ldots)$*	12	$7/6(= 1.16666\ldots)$	24
34	$9/8(= 1.125)$*	16	$9/8(= 1.125)$	32
38	$7/6(= 1.16666\ldots)$	18	$10/9(= 1.11111\ldots)$	36

In the above table, the symbol * means that the ratio is as same as the result of [11]. We emphasize that our result is obtained without extending a cyclotomic field $\mathbb{Q}(\zeta_k)$, whereas in [11] the case $k = 2n$ with an odd n needs a field extension. Therefore the degree of $\ell = \ell(g)$ is relatively small in our method. As we show in Section 3 and 4, our method produces more pairing-friendly elliptic curves than the Freeman-Scott-Teske method does for a given range of ℓ.

After Mitsunari, Sakai and Kasahara's work [16], many protocols without random oracles have been proposed based on weak Diffie-Hellman-like problems, e.g. [2], [3], [4], [18]. In Eurocrypt 2006, Cheon [7] proposed an algorithm to solve the q-weak/strong Diffie-Hellman problem. Very recently, Kutsuma-Matsuo [15] improved 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 $O(\sqrt{\ell/d})$ group operations using space for $O(\sqrt{\ell/d})$ group elements. There also exists the $\ell + 1$ variant of their algorithm. For Brezing and Weng' method [8], Freeman, Scott and Teske's method [11] and our method proposed in Section 3, 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, $\ell - 1$ has a polynomial factor $x(x \pm 1)$ or x^2. The size of x is about $\lg \ell/\varphi(ck)$ bits, where φ is the Euler phi function. So if we consider an attack based on Cheon's algorithm, we should study how to avoid this situation. In Section 5, we show that we can avoid this problem by taking ℓ as a proper divisor of $\Phi_k(x)$.

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 describe our method and analyze the probability of obtaining

pairing-friendly elliptic curves as compared to the Freeman-Scott-Teske method. In Section 4, we show examples of pairing-friendly elliptic curves obtained by using our method. In Section 5, we remark on an attack based on the Cheon's algorithm. 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. Assume that $E(K)$ has a subgroup G of a large prime order. Let ℓ be the order of G.

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 [21] 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 How to construct pairing-friendly elliptic curves

In this section, we describe our method to find pairing-friendly elliptic curves. Our method uses the CM method.

First of all, we recall the framework of generating pairing-friendly elliptic curves for a given embedding degree k by using the CM method. The procedure is described as follows:

Step 1 : Find integers ℓ, p, a, b and a positive integer D satisfying the following conditions :

1. $4p - a^2 = Db^2$,
2. $p + 1 - a \equiv 0 \pmod{\ell}$,
3. k is the smallest positive integer such that $p^k - 1 \equiv 0 \pmod{\ell}$,
4. p and ℓ are primes and
5. $-D \equiv 0$ or $1 \pmod 4$.

Step 2 : Using the CM method, find an elliptic curve E defined over $\mathbb{F}_p$ such that

1. $\#E(\mathbb{F}_p) = p + 1 - a$ and
2. E has complex multiplication by an order in $\mathbb{Q}(\sqrt{-D})$.

Note that conditions 2 and 3 in Step 1 yield that $a-1$ is a primitive k-th root of unity in $\mathbb{Z}/\ell\mathbb{Z}$. Our method which we describe later gives an improved algorithm for Step 1 in the above framework.

3.1 Our method

In the following, we only consider the case that k is in the form $k = 2n$ where n is odd.

First note that for $k = 2n$ with an odd 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 $\ell := \Phi_k(g)$ is a prime number. 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 $\ell = O(g^{\varphi(n)})$, where φ denotes the Euler phi function.

Hence, in this case, we have $\rho \sim (n+2)/\varphi(n)$ as $p, \ell \to \infty$. In particular, if n is a prime number, we obtain $\rho \sim (n+2)/(n-1)$.

Remark 1. The above method works well in most cases but there are some unfortunate cases. When $k = 30$, a^2+Db^2 in the above has no chance to be divisible by 4. Taking b as $b = (g-1)g^{(n-1)/2} = g^8 - g^7$ without reducing modulo ℓ, we can make $a^2 + Db^2$ divisible by 4, but it makes ρ greater than 2.

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

Let g be a positive integer such that $\ell := \Phi_k(g)$ is a prime number. 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 $\ell = O(g^{\varphi(n)})$.

Hence, in this case, we have $\rho \sim (n+1)/\varphi(n)$ as $p, \ell \to \infty$. In particular, if n is a prime number, we obtain $\rho \sim (n+1)/(n-1)$.

In the following, we only consider the case that n is prime.

3.2 Asymptotic values of ρ as $p, \ell \to \infty$.

In Table 1, we show asymptotic values of ρ obtained by using our method for $k = 2n$ with an odd n, $6 < n < 20$ but $n \neq 15$.

Table 1. The value of ρ for various k

k	ρ	$\deg \ell(x)$
14	3/2(= 1.5)	6
22	13/10(= 1.3)*	10
26	7/6(= 1.16666 . . .)*	12
34	9/8(= 1.125)*	16
38	7/6(= 1.16666 . . .)	18

In Table 1, the symbol * means that the ratio is the same value achieved by [11]. We emphasize that our result is obtained without extending a cyclotomic field $\mathbb{Q}(\zeta_k)$, whereas in [11] the case $k = 2n$ with an odd n needs a field extension. Therefore the degree of $\ell = \ell(g)$ is not large in our method. As we show in the following pages, our method produces more pairing-friendly elliptic curves than the Freeman-Scott-Teske method does, for a given range of ℓ.

3.3 Probability of obtaining primes p and ℓ

We roughly estimate the probability that p and ℓ are both prime in our method. First we discuss the general situation. Let n_1 and n_2 be integers and put $\rho = \frac{\ln n_2}{\ln n_1}$. From the prime number theorem, the probability that an integer n is a prime is approximately $\frac{1}{\ln n}$. We denote the probability that n_1 and n_2 are both prime by $\Pr_{n_1,n_2}$. If a pair (n_1, n_2) is randomly chosen, $\Pr_{n_1,n_2}$ is approximately $\frac{1}{\ln n_1 \ln n_2} = \frac{1}{\rho(\ln n_1)^2}$.

Let $f(x)$ be a polynomial of degree d with coefficients in $\mathbb{Z}$. Fix a positive real number ρ. Set $\ell = f(g)$ for an integer g and let p be an integer determined by g such that $\frac{\log p}{\log \ell} = \rho$. Since ℓ is described as a polynomial of g, it is not known whether ℓ and p take infinitely many primes. But we assume that the pair (ℓ, p) satisfies $\Pr_{\ell,p} = \frac{1}{\rho(\ln \ell)^2} = \frac{1}{\rho(\ln f(g))^2}$. We consider the case a pair (ℓ, p) runs through $2^m \le \ell < 2^{m+\alpha}$ for some fixed integer m and a small integer α. To simplify, let $\ell \sim g^d$. Then $\Pr_{\ell,p} \sim \frac{1}{\rho d^2(\ln g)^2}$. For $2^{m/d} \le g < 2^{(m+\alpha)/d}$, the average of the probability that ℓ and p are both prime is approximately

$$\frac{1}{\rho d^2(2^{\frac{m+\alpha}{d}} - 2^{\frac{m}{d}})} \int_{2^{\frac{m}{d}}}^{2^{\frac{m+\alpha}{d}}} \frac{1}{(\ln g)^2} dg.$$

Then we can estimate the probability that there exists at least a couple of primes (p, ℓ) for the interval $2^{m/d} \le g < 2^{(m+\alpha)/d}$ as

$$1 - \left(1 - \frac{1}{\rho d^2(2^{\frac{m+\alpha}{d}} - 2^{\frac{m}{d}})} \int_{2^{\frac{m}{d}}}^{2^{\frac{m+\alpha}{d}}} \frac{1}{(\ln g)^2} dg\right)^{2^{\frac{m+\alpha}{d}} - 2^{\frac{m}{d}}}.$$

We regard this value as the function of d and m, and denote it by $\mathrm{P}(d, m)$.

Now we compare the above probability for our method and the one for the Freeman-Scott-Teske method.

Since f is the k-th cyclotomic polynomial in our method, $d = \varphi(k)$. We show the smallest integer value of m for various k such that $\mathrm{P}(\varphi(k), m)$ is greater than $\frac{1}{2}$ in Table 2.

Table 2. The smallest value of m for various k which gives $\mathrm{P}(d, m) > 1/2$

k	$d = \deg \ell$	ρ	m ($\alpha = 1$)	m ($\alpha = 2$)	m ($\alpha = 3$)
14	6	3/2	91	83	78
22	10	13/10	176	163	155
26	12	7/6	220	205	196
34	16	9/8	315	296	284
38	18	7/6	367	345	332

In [11], to make and the value of ρ as small as possible, they use the ck-th cyclotomic polynomial as ℓ for some integer c. For this method, the smallest integer value of m for various k such that $\mathrm{P}(d, m)$ is greater than $\frac{1}{2}$ is as in Table 3.

Table 3. the smallest value of m for various k which gives $\mathrm{P}(d, m) > 1/2$ in [11]

k	$d = \deg \ell$	ρ	m ($\alpha = 1$)	m ($\alpha = 2$)	m ($\alpha = 3$)
14	12	4/3	176	161	151
22	20	13/10	360	335	320
26	24	7/6	436	405	388
34	32	9/8	668	630	608
38	36	10/9	723	681	655

From Table 2, it is expected that one can obtain sufficiently many pairing-friendly elliptic curves of order about 2^{160} for the embedding degree $k = 2$. Table 3 indicates that m should be considerably large to get many pairs of primes (p, ℓ). In practice, one can obtain smaller primes ℓ by using our method than using the Freeman-Scott-Teske method; see Table 4 and 5.

Table 4. The smallest three primes ℓ obtained by using our method

k	$\lg \ell$		
14	23.3	26.2	44.3
22	92.8	107.0	122.1
26	54.2	135.8	145.7
34	182.7	225.4	228.3
38	189.6	213.6	230.6

Table 5. The smallest three primes ℓ by using the Freeman-Scott-Teske method [11]

k	$\lg \ell$		
14	70.3	123.1	123.3
22	92.8	206.5	250.7
26	349.3	350.2	354.5
34	442.7	447.4	472.2
38	284.2	357.9	369.8

These tables shows that our method can produce more pairing-friendly elliptic curves than the Freeman-Scott-Teske method does.

Remark 2. 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 [13] 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 [11], 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 Examples

We show some examples of pairing-friendly elliptic curves obtained by our method. As in the following tables, we can take $\ell \in [2^{160}, 2^{200}]$ for $k \in \{14, 26, 34, 38\}$.

The case $k = 2n$ with $n \equiv 3 \pmod 4$.

k	14
g	94907647 (square free)
$\lg g$	26.5
a	94907648
b	81134361081873541386683178009858
ℓ	730814630451781170954872473773075062791521390343
p	156189148043546959726960325690688260554901983647491100761\\ 04666801301503
$\lg l$	159.0
$\lg p/\lg \ell$	1.48742
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	312074680843180077100702058525280424134192726192264327132\\ 49182826793377
B	728680280707276583823669124652481151272468429619813220625\\ 34344151629419

k	22
g	64537 (square free)
$\lg g$	15.9
a	64538
b	722513407850377499835120689 52
ℓ	125337493206561491302002774509050371347204186335 3
p	842249193246934375142646270334739427165774508904778427134 3\ 9673
$\lg \ell$	159.8
$\lg p/\lg \ell$	1.28748
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	755175504725507725547560647584404452629894705049767004264 1\ 9648
B	784200067565983275412589188501182777475187973001437478554 2\ 6323

k	38
g	1483 (square free)
$\lg g$	10.5
a	1484
b	514184005254749571381406231184 46
ℓ	120295108610045149810234079960945054936220646874278584444 7
p	980208096595769061399824580668089368168014940054616269874 1\ 27960671
$\lg l$	189.6
$\lg p/\lg \ell$	1.15611
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	330778111596940849550933423520331062816845702374429453110 9\ 26299761
B	177785299809937845496300083424347013830249751265698201577 5\ 76696370

The case $k = 2n$ with $n \equiv 1 \pmod 4$.

k	26
g	9779 (square free)
$\lg g$	13.2
a	85518706402103806148139720 60
b	$-$87451381943045102922732 2
ℓ	76469622258134114865051140877371924019569791957 3
p	18285492543987287680645893866289922483693928837435505359
$\lg \ell$	159.1
$\lg p/\lg \ell$	1.15410
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	42593820367147628399642416166902604799136691253340005 51
B	42914471542511191764165046457825688129483664313191595 85

k	34
g	2743 (square free)
$\lg g$	11.4
a	879087831360502649020330672114 4
b	$-$320484079971018100262606880 2
ℓ	102672614740265380619530298014630943099440571466571572 01
p	193269287225239708232113920498060961978433390944432895073 6\ 8327
$\lg \ell$	182.7
$\lg p/\lg \ell$	1.11406
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	886774159343118028130417363748474694472850276735457522486 8\ 122
B	378990034807197317339872272520769488530389043192419807306 9\ 304

5 Remarks on Cheon's algorithm

5.1 The q-weak Diffie-Hellman problem

After Mitsunari, Sakai and Kasahara's work [16], many protocols without random oracles have been proposed based on weak Diffie-Hellman-like problems, e.g. [2], [3], [4], [18]. In the following, we call such kind of problems the "pairing-related problems." The definition of the q-weak Diffie-Hellman problem is as follows.

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

For the definition of other pairing-related problems, e.g. the q-strong Diffie-Hellman problem, the q-bilinear Diffie-Hellman inversion problem, the $(q+1)$-bilinear Diffie-Hellman exponent problem, see [2], [3], [4] and so on.

5.2 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, Kutsuma and Matsuo [15] improved 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 $O(\sqrt{\ell/d})$ group operations using space for $O(\sqrt{\ell/d})$ group elements. There also exists an $\ell + 1$ variant of this algorithm.

5.3 How to avoid an attack based on Cheon's algorithm

In order to escape beyond the ability of Cheon's algorithm and its improvement, the most simple way is to take a larger ℓ. However, for the Brezing-Weng method [8], the Freeman-Scott-Teske method [11] and our method described in Section 3, the situation is not so easy. 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 $O(\sqrt{\ell^{1-1/\varphi(ck)}})$ (resp. $O(\sqrt{\ell^{1-2/\varphi(ck)}})$) group operations.

Here we consider another approach. The key idea is to take ℓ as a proper divisor of $\Phi_k(x)$. Note that when $k = 2n$ and n is an odd prime, $\Phi_{2n}(x) = \Phi_n(-x)$. We start from the following lemma.

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, $\ell \equiv 1 \pmod{n}$. □

Proposition 1. *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 ($>> n$) and s a small integer such that $\Phi_k(x) = s\ell$. Then the following hold:*

1. *If n divides s, then $x \equiv -1 \pmod{n}$ and $n^2 \not| s$.*
2. *If $s = n$ then $x + 1$ divides $\ell - 1$.*
3. *If n does not divide s, then $x \not\equiv -1 \pmod{n}$.*

Remark 3. In Proposition 1, note that by the assumption $\ell >> n$ and Lemma 1, n divides $\ell - 1$. Moreover, it is easy to see that $\ell^2 - 1$ is divisible by 24. Hence $(\ell + 1)(\ell - 1)$ is divible by $24n$.

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 $n^2 \not| s$. Write $s = tn$ where t is an integer. Since $\ell \equiv 1 \pmod{n}$ from the assumption of the proposition 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, $n^2 \not| s$.

(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 the above proposition is not suitable if we consider an attack based on Cheon's algorithm.

5.4 Examples

Here we show examples of pairing-friendly elliptic curves which are suitable even if we consider an attack based on Cheon's algorithm.

k	14
x	1083603511
s	29
ℓ	558244461317143757104672701626918998407404333205677 39 (176bit)
p	5149601701498901149849436799809351834489449663566405000139 9\ 1240135020678496405311
ρ	1.53017
$\ell-1$	$2 \cdot 7 \cdot 473632918148007086057 \cdot 841888366537383245365669459053 1$ where the smallest prime factor greater than $n = k/2$ is 69 bits.
$\ell+1$	$2^2 \cdot 3 \cdot 5 \cdot 19135609389442190543 \cdot 486217823845167137652399200315 03$ where the smallest prime factor greater than $n = k/2$ is 65 bits.

k	22
x	2169245
s	67
ℓ	3443586908389364671503933551495445912546234980894932315809 9\ 743 (205bit)
p	5887778651704515848057946195601171633901757087143749298020 1\ 25450311726006289864629
ρ	1.32879
$\ell-1$	$2 \cdot 11 \cdot 15828246210282269526689$ $\cdot$ 98890727105558870788821495077490125549 where the smallest prime factor greater than n is 74 bits.
$\ell+1$	$2^5 \cdot 3 \cdot 9058407505366397011987$ $\cdot$ 39599341209962829220904617618609338497 where the smallest prime factor greater than n is 73 bits.

k	26
x	83647
s	131
ℓ	895628588110024088164630713805121667532341241783716653231 (190bit)
p	2052345035175498040876970342827233281136809297495235578441 6\ 0697479999
ρ	1.19947
$\ell-1$	$2 \cdot 5 \cdot 13 \cdot 33591629474234771$ $\cdot$ 20509426859014734190306263804584075710 1 where the smallest prime factor greater than n is 55 bits.
$\ell+1$	$2^4 \cdot 3 \cdot 17076787506992460196737701$ $\cdot$ 10926486560378252018263410143 09 where the smallest prime factor greater than n is 84 bits.

k	34
x	1575639
s	2381
ℓ	606105016959858394374658461570366195071087972347952639529 84\ 865106400744592030329203141465137051 7 (319bit)
p	895697326487576290429590075861602614611117146049907424592 99\ 785389127915761456665464214236093710379119973406595 9
ρ	1.15838
$\ell - 1$	$2^2 \cdot 17^2 \cdot 388875735183433410518777 3$ $\cdot$ 134827722835641290843714300170152344449480622946333867621 5\ 52648314057 where the smallest prime factor greater than n is 82 bits.
$\ell + 1$	$2 \cdot 3 \cdot 11 \cdot 90576333827341044792990822674370634 91$ $\cdot$ 10138861841529483037453152617284449024380964395291649465 53 where the smallest prime factor greater than n is 123 bits.

k	34
x	1730735
s	$17 \cdot 137$
ℓ	27830402151707213772790243425060710128851524965270716441651\ 113285546630638085671924440248448543 29 (321bit)
p	48538978648626809809653096381338491065159598631595616079566\ 883218153181245685226258972434857628427544612641045 59
ρ	1.15803
$\ell - 1$	$2^3 \cdot 17 \cdot 49292468473184612044377297 47$ $\cdot$ 41514518602440537725112521829410081846914632498111851871 94\ 625694509 where the smallest prime factor greater than n is 92 bits.
$\ell + 1$	$2 \cdot 3 \cdot 5 \cdot 36156571954065562171893868510 07$ $\cdot$ 25657301607633807706083532626246386356270927862763452889 42\ 0876973 where the smallest prime factor greater than n is 102 bits.

k	38
x	422017
s	2281
ℓ	790337723267050188305022454444094380417744794380570733637 11\ 630220987237178915490932609778746724313 (326bit)
p	338740258071382406654996234276460244971409999229416672234 98\ 129270813557418676502941719082024509639338661194665709118 73
ρ	1.20054
$\ell - 1$	$2^3 \cdot 3 \cdot 19 \cdot 561154900084540540 19 \cdot 1680365814167200027103$ $\cdot$ 53264476031140610360764 07 $\cdot$ 34508303784719182295675287847 3 where the smallest prime factor greater than n is 66 bits.
$\ell + 1$	$2 \cdot 7 \cdot 11397078001996904390827$ $\cdot$ 29068966361582186149370371893995719 3 $\cdot$ 17039685153035820527466707419056164804 41 where the smallest prime factor greater than n is 74 bits.

6 Conclusion

In this article, we proposed an improved method to construct pairing-friendly elliptic curves over a finite prime field. More precisely, we improved the Freeman-Scott-Teske method ([11]) for the case that the embedding degree $2n$ where n is an odd prime. Though asymptotic values of ρ are not improved, our method improves the range of ℓ in which we can find a pairing-friendly elliptic curves of order ℓ. Our probabilistic analysis indicates that for a given range of ℓ, the probability of finding a pairing-friendly elliptic curve by using our method is much greater than the one by using the Freeman-Scott-Teske method. In fact, by using our method, we provided pairing-friendly elliptic curves for a range $[2^{160}, 2^{200}]$ of ℓ, for which the Freeman-Scott-Teske method hardly produce a pairing-friendly elliptic curve. Moreover, we studied the influence of an attack based on Cheon's algorithm and improved our method to avoid the attack. As we showed examples, the improved method also produce pairing-friendly elliptic curves.

References

1. P.S.L.M. Barreto, 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, 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, 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, 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, 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, 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, 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, M. Scott, E. Teske, *A taxonomy of pairing-friendly elliptic curves*, Cryptology ePrint Archive, Report 2006/372, 2006 http://eprint.iacr.org/

12. S. Galbraith, J. McKee, 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.
13. IEEE Computer Society, New York, USA. *IEEE Standard Specifications For Public-Key Cryptography - IEEE Std 1363-2000*, 2000.
14. 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.
15. T. Kutsuma, K. Matsuo, *Remarks on Cheon's algorithms for pairing-related problems*, In 2007 Symposium on Cryptography and Information Security (SCIS2007), Nagasaki, Japan, 2007.
16. S. Mitsunari, R. Sakai, M. Kasahara, *A new traitor tracing*, IEICE Trans. Fundamentals **E85-A** (2002), no. 2, pp. 481–484.
17. A. Miyaji, M. Nakabayashi, S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Transactions on Fundamentals **E84-A**(5) (2001), pp. 1234–1243.
18. 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.
19. M. Scott, P.S.L.M. Barreto, *Generating more MNT elliptic curves*, Designs, Codes and Cryptography **38** (2006), pp. 209–217.
20. R. Sakai, K. Ohgishi, M. Kasahara, *Cryptosystem based on pairing*, In 2000 Symposium on Cryptography and Information Security (SCIS 2000), Okinawa, Japan, 2000.
21. J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, GTM 106, 1986.