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

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. The most popular one is constructed by using the Weil pairing of elliptic curves. For a large prime ℓ which devides $E(\mathbb{F}_q)$, a subgroup G generated by $\mathbb{F}_q$-rational point P of order l is embedded into $\mathbb{F}_{q^k}$ by using the Weil pairing for some positive integer k. Pairing-friendly curves are required to have appropriately large q and ℓ, and appropriately small k and $\rho := \log q/\log \ell$. Recently, Freeman-Scott-Teske proposed a method to obtain curves with small ρ for each fixed k, following Brezing-Weng's result which uses a cyclotomic field $\mathbb{Q}(\zeta_k)$. But their result needs an extension of $\mathbb{Q}(\zeta_k)$ in many cases and therefore q and ℓ becomes extremely large. In this article, for $k = 2n$ with odd n, we propose an improved method without field extensions which achieves small ρ. In some cases, we achieve the same value of ρ as in Freeman-Scott-Teske's result, but with smaller q and ℓ than Freeman-Scott-Teske's result.

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 [9], Sakai-Ohgishi-Kasahara [12] and Boneh-Franklin [2]. Sakai-Ohgishi-Kasahara and Boneh-Franklin 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 $\sharp E(\mathbb{F}_q)$, 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 $\mathbb{F}_q$.

Roughly speaking, pairing based cryptography uses the fact that $E(\mathbb{F}_q) \subset E[\ell]$ can be embedded into $\mu_\ell \subset \mathbb{F}_{q^k}$ 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 $\log q/\log \ell$ should be sufficiently small. An elliptic curve satisfying these conditions is called a "pairing-friendly curve". It is very important how to find pairing-friendly curves. There are many works on this topic [10], [5], [4], [1], [11] and so on. Recently, Freeman-Scott-Teske [7] proposed a method to obtain curves with small ρ, following Brezing-Weng's result [4] which uses cyclotomic fields. In Freeman-Scott-Teske's method, take $\ell(x)$ as a cyclotomic polynomial Φ_{ck} for some integer c and set a prime number $\ell := \ell(g)$ if $\ell(g)$ is prime for some positive integer g. Note that g is a primitive ckth root of unity in $\mathbb{Z}/\ell\mathbb{Z}$. As is stated in [7], the degree of $\ell(x)$ is important to obtain enough pairing-friendly curves with appropriate size of ℓ and q. Freeman-Scott-Teske's method in [7] needs extension of cyclotomic fields $\mathbb{Q}(\zeta_k)$, that is, $c > 1$. So the degree of $\ell(x)$ becomes large and therefore ℓ and q of obtained pairing-friendly curves become extremely large, greater than 200-bit in many cases. In this article, for the case that the embedding degree is in the form $k = 2n$ with odd n, we propose an improved method which avoids to suitable curves for pairing based cryptosystem. We show the table of values of the ratio ρ obtained by using our method 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 has the same value achieved by [7]. We emphasis that our result is obtained without extending a cyclotomic field $\mathbb{Q}(\zeta_k)$, whereas in [7] the case $k = 2n$ with odd n needs a field extension. Hence in the above cases, we achieve the same value of ρ as in Freeman-Scott-Teske's result [7], but with smaller q and ℓ than ones in [7].

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 $\sharp E(K)$, 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.

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 a multiplicative group of $\hat{K}$ and μ_ℓ is the group of ℓth root of unity in $\hat{K}^*$. For the details of the Weil pairing, see [13] 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.

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 m 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 $E(\mathbb{F}_q)$ should be large enough so that the discrete logarithm on the group is computationally infeasible,
- q^k should be large enough so that the discrete logarithm on the multiplicative group $\mathbb{F}_{q^k}^*$ is computationally infeasible.

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

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

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

3 How to construct pairing-friendly elliptic curves

Here we consider a method to generate pairing-friendly elliptic curves for a given k using the CM method. The aim of this method is to find an elliptic curve E over $\mathbb{F}_q$ with complex multiplication with respect to $-D$ such that $\sharp E(\mathbb{F}_q) = q + 1 - a$ has a large prime factor ℓ and k is the smallest positive integer $q^k - 1$ divisible by ℓ. Note that the minimality condition of k yields that ℓ divides $\Phi_k(q)$ where $\Phi_k(x)$ is the kth cyclotomic polynomial.

Required conditions for elliptic curves in this method are summarized as follows:

1. $4q - a^2 = Db^2$,
2. $q + 1 - a \equiv 0 \pmod{\ell}$,
3. k is the smallest positive integer such that $q^k - 1 \equiv 0 \pmod{\ell}$.

Note that conditions (2) and (3) yield $a - 1$ is a primitive kth root of unity in $\mathbb{F}_\ell$.

3.1 Our method

In the following, we only consider the case that $q = p$ is prime and k is of the form $k = 2n$ where n is odd.

First note that for $k = 2n$ with odd n, if g is a primitive kth root of unity in a field K, then $\sqrt{-g} = g^{(n+1)/2}$ lives in 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 $\rho = \log p / \log \ell$.

Our method based on this idea is divided into two cases. In the following, we describe our method.

Let g be a positive integer such that $\ell := \Phi_k(g)$ is a prime number. Then, g is a primitive kth root of unity under 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's phi function.

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

Remark 1. The above method works well in most cases, but there are some unfortunate cases, for example, $n = 30$. For $n = 30$, $a^2 + Db^2$ 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 taking $\pmod{\ell}$, we can make $a^2 + Db^2$ divisible by 4, but it makes ρ greater than 2.

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

Let g be a positive integer such that $\ell := \Phi_k(g)$ is a prime number. Then, g is a primitive kth root of unity under modulo ℓ and $\sqrt{-g} \equiv g^{(n+1)/2} \pmod{\ell}$. Note that $g^{(n+1)/2}$ is also a primitive kth root of unity under 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 $\rho = (n+1)/\varphi(n)$ as $p, \ell \to \infty$. In particular, if n is a prime number, we obtain $\rho = (n+1)/(n-1)$.

3.2 Table of values of ρ (as $p, \ell \to \infty$).

We show the table of values of ρ obtained by our method for $k = 2n$ with odd n, $6 < n < 20$ but $n \neq 15$.

k	ρ	$\deg \ell(x)$
14	$3/2(= 1.5)$	6
18	$5/3(= 1.66666\ldots)$	6
22	$13/10(= 1.3)$*	10
26	$7/6(= 1.16666\ldots)$*	12
34	$9/8(= 1.125)$*	16
38	$7/6(= 1.16666\ldots)$	18

In the above table, the symbol * means that the ratio is the same value achieved by [7]. We emphasis that our result is obtained without extending a cyclotomic field $\mathbb{Q}(\zeta_k)$, whereas in [7] the case $k = 2n$ with odd n needs a field extension. Hence in the above cases, we achieve the same value of ρ as in Freeman-Scott-Teske's result [7], but with smaller q and ℓ than ones in [7].

3.3 Examples

We show some examples obtained by our method.
The case $k = 2n$ with $n \equiv 3 \pmod 4$.

k	14
g	$94906471 = 11^2 \cdot 784351$ (not square free)
$\log g$	26.500003121967254
a	94906472
b	81130339815368566417287197368170
b'	$11b$ =892433737969054230590159171049870
l	730760299020460302123530927476913237603395176511
p	156171730858874425623130807894467741045481485260496599196627111790004671
$\log l$	160
$\log p$	237
$\log p/\log l$	1.48742
g	94907647 (square free)
$\log g$	26.500020998502315
a	94907648
b	81134361081873541386683178009858
l	730814630451781170954872473773075062791521390343
p	156189148043546959726960325690688260554901983647491100761104666801301503
$\log l$	160
$\log p$	237
$\log p/\log l$	1.48742

k	22
g	64537 (square free)
$\log g$	15.977838895308661
a	64538
b	72251340785037749983512068952
l	1253374932065614913020027745090503713472041863353
p	84224919324693437514264627033473942716577450890477842713439673
$\log l$	160
$\log p$	206
$\log p/\log l$	1.28748

k	38
g	1483 (square free)
$\log g$	10.53430288245463
a	1484
b	5141840052547495713814062311844 6
l	12029510861004514981023407996094505493622064687427858444 47
p	9802080965957690613998245806680893681680149400546162698741279606 71
$\log l$	190
$\log p$	219
$\log p / \log l$	1.15611

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

k	18
g	94906623 (square free)
$\log g$	26.500005432552275
a	769985598329417598574210795272718088934 4
b	-811308604173406948189707261286 42
l	730767328960794658374478759845478477419642392323
p	1482194569704176568777362538221732124157911686713314807609446281401205875835212 7
$\log l$	160
$\log p$	264
$\log p / \log l$	1.65409

k	26
g	9779 (square free)
$\log g$	13.255471227467067
a	855187064021038061481397206 0
b	-8745138194304510292273 22
l	764696222581341148650511408773719240195697919573
p	182854925439872876806458938662899224836939288374355053 59
$\log l$	160
$\log p$	184
$\log p / \log l$	1.15410

k	34
g	2743 (square free)
$\log g$	11.421538906848276
a	879087831360502649020330672114 4
b	-3204840799710181002626068802
l	1026726147402653806195302980146309430994405714665715720 1
p	193269287225239708232113920498060961978433390944432895073683 27
$\log l$	183
$\log p$	204
$\log p / \log l$	1.11406

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, M. Franklin, *Identity-based encryption from the Weil pairing*, SIAM Journal of Computing, **32**(3) (2003), pp. 586–615.
3. I.-F. Blake, G. Seroussi, N.-P. Smart, Advances in Elliptic Curve Cryptography, Cambridge University Press, 2005.

4. F. Brezing and A. Weng, *Elliptic curves suitable for pairing based cryptography*, Design, Codes and Cryptography, **37** (2005), pp. 133–141.
5. C. Cocks, R. G. E. Pinch, *Identity-based cryptosystems based on the Weil pairing*, Unpublished manuscript, 2001.
6. D. Freeman, *Methods for constructing pairing-friendly elliptic curves*, 10th Workshop on Elliptic Curves in Cryptography (ECC 2006), Toronto, Canada, September 2006.
7. D. Freeman, M. Scott, E. Teske, *A taxonomy of pairing-friendly elliptic curves*, preprint, 2006.
8. 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.
9. 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.
10. 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.
11. M. Scott, P.S.L.M. Barreto, *Generating more MNT elliptic curves*, Designs, Codes and Cryptography **38** (2006), pp. 209–217.
12. R. Sakai, K. Ohgishi, M. Kasahara, *Cryptosystem based on pairing*, In 2000 Symposium on Cryptography and Information Security (SCIS 2000), Okinawa, Japan, 2000.
13. J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, GTM 106, 1986.