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 the group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of an elliptic curve E defined over a finite field $\mathbb{F}_q$ and a large prime ℓ which divides $E(\mathbb{F}_q)$, a subgroup G generated by a $\mathbb{F}_q$-rational point P of order ℓ is embedded into $\mathbb{F}_{q^k}$ by using the Weil pairing for some positive integer k. Suitable curves for pairing based cryptography, which is called pairing-friendly curves, are required to have appropriately large q and ℓ, and appropriately small k and $\rho := \log_2 q / \log_2 \ell$. Recently, Freeman-Scott-Teske proposed a method to obtain pairing-friendly curves over a finite prime field $\mathbb{F}_p$ with small $\rho = \log_2 p / \log_2 \ell$ for each fixed k, following Brezing-Weng's result which uses a cyclotomic field $\mathbb{Q}(\zeta_k)$. But since their method needs an extension of $\mathbb{Q}(\zeta_k)$ in many cases, p and ℓ become extremely large. In this article, for $k = 2n$ where n is an odd prime, we propose an improved method which achieves small ρ without a field extension. Though asymptotic values of ρ are not improved, our method produces more pairing-friendly curves than the Freeman-Scott-Teske's method does, for a given range of ℓ.

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 [10], Sakai-Ohgishi-Kasahara [13] 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 $\#E(\mathbb{F}_q)$, 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 $\lg q / \lg \ell$ should be appropriately small. An elliptic curve satisfying these conditions is called a "pairing-friendly curve". It is very important to construct an efficient method to find pairing-friendly curves. There are many works on this topic: [11], [5], [4], [1], [12] and so on. Recently, Freeman-Scott-Teske [7] proposed a method to obtain pairing-friendly curves over a finite prime field $\mathbb{F}_p$ with small ρ, following Brezing-Weng's result [4] which uses cyclotomic fields. In [7], 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 [7], the degree of $\ell(x)$ is important to obtain enough pairing-friendly curves with appropriate size of ℓ and p. The method in [7] 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 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 for finding pairing-friendly curves, where we can take $c = 1$. In particular, for the case that n is an odd prime, 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 [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. Therefore the degree of $\ell = \ell(g)$ is not large in our method. As we show in Section 3 and 4, our method produces more pairing-friendly curves than the Freeman-Scott-Teske's method does, for a given range of ℓ.

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 to obtain pairing-friendly curves compared with Freeman-Scott-Teske's method. In Section 4, we show examples of pairing-friendly curves obtained by using our method. Finally, we summarize our result in Section 5.

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 a 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 [14] 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,
- 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,

– 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 curves. Our method uses the CM method.

First of all, we recall the framework of generating pairing-friendly 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,
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. $\#E(\mathbb{F}_p) = p + 1 - a$,
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 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's 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 taking 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 under 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 $\rho \sim (n+1)/(n-1)$.

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 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
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 Table 1, 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. Therefore the degree of $\ell = \ell(g)$ is not large in our method. As we show in the following, our method produces more pairing-friendly curves than the Freeman-Scott-Teske's method does, for a given range of ℓ.

3.3 Probability of obtaining primes p and ℓ

We 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 $\frac{1}{\ln n}$. So the probability that n_1 and n_2 are both prime is approximately $\frac{1}{\ln n_1 \ln n_2} = \frac{1}{\rho(\ln n_1)^2}$. We denote the probability by Pr_{n_1,n_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 infinite many prime values. But we assume that $\mathrm{Pr}_{\ell,p} = \frac{1}{\rho(\ln \ell)^2} = \frac{1}{\rho(\ln f(g))^2}$. We consider the case a pair (ℓ, p) runs through $2^m \leq \ell < 2^{m+\alpha}$ 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 $2^{m/d} \leq g < 2^{(m+\alpha)/d}$, 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 $2^{m/d} \leq g < 2^{(m+\alpha)/d}$ 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 Freeman-Scott-Teske's 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
18	6	11/6	84	76	71
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 [7], 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 [7]

k	$d = \deg \ell$	ρ	m ($\alpha = 1$)	m ($\alpha = 2$)	m ($\alpha = 3$)
14	12	4/3	176	161	151
18	24	19/12	447	418	401
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 $k \in \{18, 22\}$. 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 Freeman-Scott-Teske's 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
18	50.5	56.8	56.9
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 Freeman-Scott-Teske's method [7]

k	$\lg \ell$		
14	70.3	123.1	123.3
18	38.0	331.0	332.4
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 curves than the Freeman-Scott-Teske's method does.

Remark 2. Using the CM method, we can construct an ordinary elliptic curves with complex multiplication by the order of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, $D > 0$. (Refer to [9] for the detail 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 [7], we can construct an elliptic curve by using the CM method for $D < 10^{10}$. Hence our method is effective to construct pairing-friendly curves.

4 Examples

We show some examples of pairing-friendly curves obtained by our method. As in the following tables, we can take $\ell \in [2^{160}, 2^{200}]$ for $k \in \{14, 18, 26, 34, 38\}$.

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	156189148043546959726960325690688260554901983647491100761104666801301503
$\lg l$	160
$\lg p$	237
$\lg p / \lg \ell$	1.48742
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	312074680843180077100702058525280424134192726192264327132491828267933 77
B	728680280707276583823669124652481151272468429619813220625343441516294 19

k	22
g	64537 (square free)
$\lg g$	15.9
a	64538
b	72251340785037749983512068952
ℓ	1253374932065614913020027745090503713472041863353
p	84224919324693437514264627033473942716577450890477842713439673
$\lg \ell$	160
$\lg p$	206
$\lg p / \lg \ell$	1.28748
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	75517550472550772554756064758440445262989470504976700426419648
B	78420006756598327541258918850118277747518797300143747855426323

k	38
g	1483 (square free)
$\lg g$	10.5
a	1484
b	51418400525474957138140623118446
ℓ	1202951086100451498102340799609450549362206468742785844447
p	980208096595769061399824580668089368168014940054616269874127960671
$\lg l$	190
$\lg p$	219
$\lg p / \lg \ell$	1.15611
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	330778111596940849550933423520331062816845702374429453110926299761
B	177785299809937845496300083424347013830249751265698201577576696370

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

k	18
g	94906623 (square free)
$\lg g$	26.5
a	7699855983294175985742107952727180889344
b	$-81130860417340694818970726128642$
ℓ	730767328960794658374478759845478477419642392323
p	148219456970417656877736253822173212415791168671331480760944628140120587583 52127
$\lg l$	160
$\lg p$	264
$\lg p / \lg \ell$	1.65409
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	610587211902217729893806958821687111566883129507949202467723803382033767538 3850
B	901122997836204009521658818621702115763892648576404404181631296055091136970 6609

k	26
g	9779 (square free)
$\lg g$	13.2
a	8551870640210380614813972060
b	$-8745138194304510292273322$
ℓ	764696222581341148650511408773719240195697919573
p	18285492543987287680645893866289922483693928837435505359
$\lg \ell$	160
$\lg p$	184
$\lg p / \lg \ell$	1.15410
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	4259382036714762839964241616690260479913669125334000551
B	4291447154251119176416504645782568812948366431319159585

k	34
g	2743 (square free)
$\lg g$	11.4
a	879087831360502649020330672114 4
b	$-32048407997101810026260688 02$
ℓ	102672614740265380619530298014630943099440571466571572 01
p	1932692872252397082321139204980609619784333909444328950736832 7
$\lg \ell$	183
$\lg p$	204
$\lg p / \lg \ell$	1.11406
Elliptic curve $E : y^2 = x^3 + Ax + B$	
A	8867741593431180281304173637484746944728502767354575224868122
B	3789900348071973173398722725207694885303890431924198073069304

5 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's method ([7]) for the case that the embedding degree $k = 2n$ 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 curves of order ℓ. Our probabilistic analysis indicates that for a given range of ℓ, the probability of finding a pairing-friendly curve by using our method is much greater than the one by using the Freeman-Scott-Teske's method. Moreover, 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's method hardly produce a pairing-friendly curve.

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*, Cryptology ePrint Archive, Report 2006/372, 2006 http://eprint.iacr.org/
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. IEEE Computer Society, New York, USA. *IEEE Standard Specifications For Public-Key Cryptography - IEEE Std 1363-2000*, 2000.
10. 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.
11. 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.
12. M. Scott, P.S.L.M. Barreto, *Generating more MNT elliptic curves*, Designs, Codes and Cryptography **38** (2006), pp. 209–217.
13. R. Sakai, K. Ohgishi, M. Kasahara, *Cryptosystem based on pairing*, In 2000 Symposium on Cryptography and Information Security (SCIS 2000), Okinawa, Japan, 2000.
14. J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, GTM 106, 1986.