Construction of Pairing-Friendly Elliptic Curves by Cocks-Pinch Method

Woo-Sug Kang

Department of Mathematics
Korea University
Seoul, 136-701, Korea
wsgkang@korea.ac.kr

Abstract. We explain a method of finding the polynomials representing $\sqrt{-D}$ and ζ_k over the field containing $\sqrt{-D}$ and ζ_k. By using this method, we make a construction of pairing-friendly elliptic curves based on Cocks-Pinch method.

1 Introduction

Recently, many people are interested in the pairing based cryptography. It use the fact that a weil pairing, a tate pairing or other pairings change the discrete logarithm problem in an elliptic curve $E(\mathbb{F}_q)$ into the discrete logarithm problem in a finite field $\mathbb{F}_{q^k}^*$. An elliptic curve E is said to have an embedding degree k if its subgroup order r divides $q^k - 1$, but does not divide $q^i - 1$ for all $0 < i < k$ and set $\rho = \log q / \log r$. The pairing based cryptography needs elliptic curves with a small embedding degree k and a large prime order subgroup. i.e. ρ is near to 1. Such curves are called pairing friendly elliptic curves. For the case of supersingular curves, there is a well known fact that its embedding degrees are less than or equal to 6 [16].

We consider nonsupersingular elliptic curves. There are several methods of constructing elliptic curves with prescribed embedding degree k ([1], [2], [3], [7], [8], [9], [15], [18]). The goal of these methods is finding the polynomials $t(x)$, $r(x)$ and $q(x)$ satisfying the followings:

(1) $q(x)$ and $r(x)$ represent primes.
(2) $r(x)$ divides $q(x) + 1 - t(x)$.
(3) $r(x)$ divides $\Phi_k(t(x) - 1)$, where Φ_k is the k-th cyclotomic polynomial.
(4) $Dy(x)^2 = 4q(x) - t(x)^2$ has infinitely many integer solutions.

Barreto, Lynn and Scott [2] and Brezing and Weng [3] give the construction based on Cocks-Pinch method [6].

Cocks-Pinch method by Brezing and Weng [3]

1. Fix D, $k \in \mathbb{N}$.
2. Choose an irreducible polynomial $r(x)$ such that ζ_k, $\sqrt{-D} \in\ K$,

where ζ_k is a primitive k-th root of unity and $K = \mathbb{Q}[x]/(r(x))$.
3. Choose $t(x)$ to be a polynomial representing $1 + \zeta_k$ in K.
4. Choose $u(x)$ to be a polynomial representing $\sqrt{-D}$ in K.
5. Compute $y(x) = (t(x) - 2)u(x)/D$ in K.
6. Compute $q(x) = (t(x)^2 + Dy(x)^2)/4 \in \mathbb{Q}[x]$.
7. If $q(x)$ and $r(x)$ represent prime for some x, by the CM method, construct an elliptic curve over $\mathbb{F}_{q(x)}$ with an order $r(x)$ subgroup.

The elliptic curves constructed by this method have ρ less than 2. The difficult point of Cocks-Pinch method is to find a polynomial $r(x)$ satisfying the followings;

(1) $K = \mathbb{Q}[x]/(r(x))$ contains ζ_k and $\sqrt{-D}$.
(2) The polynomials represent ζ_k and $\sqrt{-D}$ are easily found.
(3) $r(x)$ and $q(x)$ represent primes.

The smallest field satisfying (1) is $\mathbb{Q}(\zeta_k, \sqrt{-D})$. But if this field is not a cyclotomic field, denominators of coefficients of $t(x)$ and $u(x)$ are very large in generally. We give some example for this in section 3.

Most previous results are produced when $\mathbb{Q}(\zeta_k, \sqrt{-D})$ is a cyclotomic field. i.e. D's are 1, 2 and 3. In this paper, how to construct a pairing friendly elliptic curves over some extension fields of $\mathbb{Q}(\zeta_k, \sqrt{-D})$ for arbitrary k and D. First, we work over cyclotomic field. One of advantages of cyclotomic field is that the ring of algebraic integer of cyclotomic field $\mathbb{Q}(\zeta_l)$ is $\mathbb{Z}[\zeta_l]$.

Lemma 1. *If $\sqrt{-D}$ is contained in $\mathbb{Q}(\zeta_l)$, $\sqrt{-D}$ is represented by ζ_l with integer coefficients.*

Proof. The ring of algebraic integer of $\mathbb{Q}(\zeta_l)$ is $\mathbb{Z}[\zeta_l]$ and $\sqrt{-D}$ is an algebraic integer. Thus there is $\sqrt{-D}$ in $\mathbb{Z}[\zeta_l]$.

Since $\sqrt{-D}$ is represented by ζ_l with integer coefficient, Lemma 1 guarantees (2) and (3) for many cases of $q(x)$. Another advantage is that $r(x)$ always satisfies (3).(In Section 2.4)

The remaining problem is how to find polynomials representing $\sqrt{-D}$ and ζ_k. In previous works, they found such polynomials with some conditions of k and D. In Section 2, we explain the method of finding the polynomials representing $\sqrt{-D}$ and ζ_k over cyclotomic fields without any conditions. By using this method , we make a general construction over cyclotomic fields. In section 2.4, we give some results over extension of finite field. Second, we explain the consruction over $\mathbb{Q}(\zeta_k, \sqrt{-D})$ where this is not a cyclotomic field and its problems, in Section 3. We give the results for Section 2, in Section 4.

2 Construction over $\mathbb{Q}(\zeta_k, \zeta_d)$

Main Construction

1. Fix D, $k \in \mathbb{N}$, where D is a square free integer.
2. Let d be D if $D \equiv 3 \bmod 4$, $4D$ if $D \equiv 1$ or $2 \bmod 4$.
3. Let $l = \mathrm{lcm}(k, d)$.
4. Let $r(x) = \Phi_l(x)$, where $\Phi_l(x)$ is l-th cyclotomic polynomial.
5. Let $K = \mathbb{Q}[x]/(r(x)) = \mathbb{Q}(\zeta_l)$.
6. Let $t(x) = 1 + x^\alpha$, where α is multiple of l/k.
7. By the code in Section 2.3, find $u(x)$ representing to $\sqrt{-D}$ in K.
8. Compute $y(x) = (t(x) - 2)u(x)/D$ in K.
9. Compute $q(x) = (t(x)^2 + Dy(x)^2)/4$ in $\mathbb{Q}[x]$.
10. If $q(x)$ and $r(x)$ represent prime for some x, by the CM method, construct an elliptic curve over $\mathbb{F}_{q(x)}$ with an order $r(x)$ subgroup.

Since $\rho \approx \deg q(x)/\deg r(x)$ and $\deg r(x)$ increases as D increases, we can expect that ρ will be more near to 1 for large D. But we almost obtain the best ρ values when D is small. We compute that for $\deg r(x) \leq 100$ and $k \leq 50$. When D is equal to 1, 2 or 3, ρ is the minimum value, except $k = 7$, 10 and 14. We give the result table in section 4.

Now we explain each steps.

2.1 Step 1-5 : Initialization

We have to construct the field K which has ζ_k and $\sqrt{-D}$. For any square free integer D, let d be D if D is equivalent to 3 modulo 4, $4D$ otherwise i.e. $-d$ is the discriminant of $\mathbb{Q}(\sqrt{-D})$. The following lemma explains the method of choice of cyclotomic field containing $\sqrt{-D}$.

Lemma 2. *$\mathbb{Q}(\zeta_d)$ is the minimal cyclotomic field containing $\sqrt{-D}$, where $-d$ is the discriminant of $\mathbb{Q}(\sqrt{-D})$.*

Proof. By Conductor-discriminant Formula [20], $-d$ is equal to its conductor.

Lemma 2 shows that K, in step 5, is l-th cyclotomic field which has ζ_k and $\sqrt{-D}$.

2.2 Step 6 : Polynomial representing ζ_k

There are $\varphi(k)$ numbers of primitive k-th roots of unity and the polynomial $x^{l/k}$ is one of k-th roots of unity in K. If $\gcd(\alpha, k) = 1$, $(x^{1/k})^\alpha$ is also a primitive k-th root of unity. Thus we can choose $\varphi(k)$ numbers of polynomials representing primitive k-th roots of unity.

2.3 Step 7 : Polynomial representing $\sqrt{-D}$

The polynomial $x^{l/d}$ is corresponding to ζ_d in K. There are $\varphi(d)$ numbers of primitive d-th roots of unity, but square root of $-D$ has only two possibility, $\pm\sqrt{-D}$. So if we represent $\sqrt{-D}$ by one of primitive d-th roots of unity, we can find the polynomial corresponding to $\sqrt{-D}$ in K. Since $\sqrt{-D}$ is in $\mathbb{Q}(\zeta_d)$ and integral, we can find the solutions of the polynomial $x^2 + D$ in K, moreover $\mathbb{Z}[\zeta_d]$. Its solutions are found easily by solving the following equation;

$$(a_0 + a_1\zeta_d + \cdots + a_{d-1}\zeta_d^{d-1})^2 = -D \tag{1}$$

Using the relation $\zeta_d^d = 1$, (1) changes

$$b_0 + b_1\zeta_d + \cdots + b_{d-1}\zeta_d^{d-1} = 0 \tag{2}$$

(2) is easily computed by the simple matrix calculation.

We compute this equation by **PARI** [11]. There is a function in **PARI** which gives the roots of the polynomial in number field. The following is the Code of finding the representation of $\sqrt{-D}$ in ζ_d

PARI Code : Find the representation of $\sqrt{-D}$ in ζ_d

` Input : D`
`Output : polynomial corresponding to` $\sqrt{-D}$ `in` $\mathbb{Q}(\zeta_d)$

```
Represent_D(D) = \
{
  local( d,f,nf,sqD ) ; \
  if ( issquarefree(D) , \
       d = -quaddisc(-D) ; \
       f=polcyclo(d,y) ; \
       nf=nfinit(f) ; \               \\ initialize of number field nf
       sqD=nfroots(nf,x^2+D) ; \      \\ roots of x^2+D in nf
       sqD=subst(sqD[2].pol,y,x) ; \  \\ change the variable y to x
  ) ; \
  sqD
}
```

2.4 Step 10

We have to check whether $q(x)$ and $r(x)$ represent primes for some x. To do it, we need the following Conjecture.([9], [12]) *Conjecture 1.* There are infinitely many $a \in \mathbb{Z}$ such that $f(a)$ is prime if the following three conditions are satisfied:

(1) The leading coefficient of f is positive.
(2) f is irreducible.
(3) The set of values $f(\mathbb{Z}^+)$ has no common divisor > 1.

For any l, $r(x)$ satisfies this conjecture. But we have to check for $q(x)$.

2.5 Some results when $q(x)$ is reducible

If $q(x)$ is a power of irreducible polynomial, we can construct a pairing friendly elliptic curve over extension of finite field. The followings are only results in our computation when $q(x)$ is a power over irreducible polynomial.

Case 1. $k = 3$, $D = 3$

$r(x) = x^2 + x + 1$

$q(x) = (x + 1)^2$

If $x + 1$ is prime or prime power and $x^2 + x + 1$ is prime, we can construct an elliptic curve over $\mathbb{F}_{(x+1)^2}$ with embedding degree 3 and $\rho = 1$.

Case 2. $k = 4$, $D = 1$

$r(x) = x^2 + 1$

$q(x) = 1/2(x + 1)^2$

If $q(x)$ is prime power, $x + 1$ is a power of 2. Then $x^2 + 1$ is always divided by 2. i.e. $r(x)$ cannot be prime. So the construction is impossible.

Case 3. $k = 6$, $D = 3$

$r(x) = x^2 - x + 1$

$q(x) = 1/3(x + 1)^2$

If $q(x)$ is prime power, $x + 1$ is a power of 3. Then $x^2 - x + 1$ is always divided by 3. i.e. $r(x)$ cannot be prime. So the construction is also impossible.

3 Construction on $\mathbb{Q}(\zeta_k, \sqrt{-D})$

Let $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$. We also construct pairing friendly elliptic curves over K by PARI, where this field is not a cyclotomic field i.e. d does not divide k. The following is the PARI code of finding the representation of ζ_k and $\sqrt{-D}$.

PARI Code : Find the representation of ζ_k and $\sqrt{-D}$ in $\mathbb{Q}(\zeta_k, \sqrt{-D})$

Input : k, D
Output : r(x), t(x) and u(x) in $\mathbb{Q}(\zeta_k, \sqrt{-D})$

```
Represent_kD(k,D)= \
{
 local(POLCOMP,r,sq_D,ZETA_k) ; \
 if ( issquarefree(D),\
      POLCOMP=polcompositum(x^2+D,polcyclo(k),1)[1] ; \
      r=POLCOMP[1] ; \
      sq_D=POLCOMP[2].pol ; \
      ZETA_k=POLCOMP[3].pol ; \
 ) ; \
 [r,ZETA_k+1,sq_D]
}
```

We only use the PARI function **polcompositum**. This gives the polynomial $r(x)$, and the roots of $x^2 + D = 0$ and $\Phi_k(x) = 0$ as elements of $\mathbb{Q}[x]/(r(x))$. If d does not divide k, The denominator of coefficients of $r(x)$ are growing as D and k increases. **polred** in PARI, makes its coefficient small. But degree of decrease is only a little and this function is very slow. So this method is not good for large discriminant and large k.

Example 1. $k = 8$, $D = 17$

$K = \mathbb{Q}(\zeta_8, \sqrt{-17})$

$r(x) = x^8 + 68x^6 + 1736x^4 + 19448x^2 + 84100$

$t(x) = -17/267960x^7 - 607/133980x^5 - 17221/133980x^3 - 39268/33495x + 1$

$u(x) = -17/267960x^7 - 607/133980x^5 - 17221/133980x^3 - 72763/33495x$

$q(x) = 17/15956124800x^{14} - 1/2475950400x^{13} + 186583/1220643547200x^{12} - \cdots - 41207687/30949380x + 1921757/853776$

Example 2. $k = 7$, $D = 1$

$K = \mathbb{Q}(\zeta_7, \sqrt{-1})$

$r(x) = x^{12} + 2x^{11} + 9x^{10} + 14x^9 + 31x^8 + 34x^7 + 41x^6 + 12x^5 - 23x^4 - 28x^3 + 11x^2 + 8x + 1$

$t(x) = -114243472/65265341x^{11} - 204769600/65265341x^{10} - 988109696/65265341x^9 - 1398866651/65265341x^8 - 3273455408/65265341x^7 - 3238008452/65265341x^6 - 4092584160/65265341x^5 - 608191962/65265341x^4 + 2627467472/65265341x^3 + 2600701292/65265341x^2 - 1754413800/65265341x - 439258918/65265341$

$u(x) = -114243472/65265341x^{11} - 204769600/65265341x^{10} - 988109696/65265341x^9 - 1398866651/65265341x^8 - 3273455408/65265341x^7 - 3238008452/65265341x^6 - 4092584160/65265341x^5 - 608191962/65265341x^4 + 2627467472/65265341x^3 + 2600701292/65265341x^2 - 1819679141/65265341x - 504524259/65265341$

$q(x) = 8021189411500160/4259564735846281x^{22} + 28586727396255616/4259564735846281x^{21} + 163906886117738456/4259564735846281x^{20} + 441581971739245064/4259564735846281x^{19} + \cdots - 7277214974278758957/4259564735846281x^3 + 564967616779787218/4259564735846281x^2 + 1002227778135310510/4259564735846281x + 124828323194560706/4259564735846281$

Example 3. $k = 7$, $D = 1$

By the method in section 2,

$K = \mathbb{Q}(\zeta_7, \zeta_4)$

$r(x) = x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$

$t(x) = x^4 + 1$

$u(x) = x^7$

$q(x) = 1/4(x^{22} - 2x^{18} + x^{14} + x^8 + 2x^4 + 1)$

Remark 1. Example 1, 2 show that the degree of increase of coefficients is more influenced by k than D. Strictly speaking, it is influenced by the degree $\varphi(k) = [\mathbb{Q}(\zeta_k) : \mathbb{Q}]$.

Remark 2. Example 2, 3 are constructed over the same field $\mathbb{Q}(\zeta_7, \sqrt{-1}) = \mathbb{Q}(\zeta_7, \zeta_4)$. These examples show that the results are very different as the choice of $r(x)$.

4 Results

We compute ρ's for deg $r(x) \leq 100$ and $k \leq 50$. When D is equal to 1, 2 or 3, ρ is the minimum value, except $k = 7$, 10 and 14.

Table 1. The best ρ value

k	ρ	D	α	$deg(r(x))$
2	1.000	1	1	2
		3	1	2
3	1.000	3	1,2	2
4	1.000	1	1,3	2
5	1.500	3	2	8
6	1.000	3	1,5	2
7	1.333	1	2	12
		3	5	12
		7	4	6
8	1.250	3	3,7	8
9	1.333	3	1,4,7	6
10	1.500	1	3,9	8
		3	7	8
		5	3	8
11	1.200	1	3	20
		3	4	20
12	1.500	3	1,5,7,11	4
13	1.167	3	9	24
14	1.333	3	5	12
		7	11	6
15	1.500	3	1,11	8
16	1.375	3	1,9	16
17	1.125	3	6	32
18	1.583	2	1	24
19	1.111	1	5	36
		3	13	36
20	1.375	3	7,17	16
21	1.333	3	1,8	12
22	1.300	1	1	20
		3	19	20
23	1.091	1	6	44
		3	8	44
24	1.250	3	1,5,13,17	8
25	1.300	3	17	40

k	ρ	D	α	$deg(r(x))$
26	1.167	1	7	24
		3	9	24
27	1.111	3	1,10,19	18
28	1.333	1	1,15	12
29	1.071	3	10	56
30	1.500	3	1,11	8
31	1.067	1	8	60
		3	21	60
32	1.063	3	11,27	32
33	1.200	3	1,23	20
34	1.125	1	9	32
		3	23	32
35	1.500	1	9	48
		3	12	48
36	1.417	2	1	24
37	1.056	3	25	72
38	1.111	3	13	36
39	1.167	3	1,14	24
40	1.438	3	1,21	32
41	1.050	3	14	80
42	1.333	3	1,29	12
43	1.048	1	11	84
		3	29	84
44	1.150	3	15,37	40
45	1.333	3	1,16,31	24
46	1.136	1	1	44
		3	39	44
47	1.043	1	12	92
		3	16	92
48	1.125	3	1,17,25,41	16
49	1.190	3	33	84
50	1.300	1	13	40
		3	17	40

Note that when $k = 12$, Barreto and Naehrig make a pairing friendly elliptic curve with $\rho = 1$ by MNT method [14].

5 Conclusion

We have proposed a general construction of pairing friendly elliptic curves over an extension field L of $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$. If the field L is not a cyclotomic field, our method is not useful. If we find an extension field L of $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$ which has a simple ring of integer, specially a power integral basis, we can easily find $t(x)$, $u(x)$ in L and its denominate of coefficient may be small.

References

1. P.Barreto and M.Naehrig, *Pairing-friendly elliptic curves of prime order*, Cryptology ePrint Archive Report 2005/133.
2. P.S.L.M.Barreto, B.Lynn and M.Scott. *Constructing elliptic curves with prescribed embedding degrees* , Security in Communication Networks - SCN'2002, volumn 2576 of *Lecture Note in Computer Science*, Springer-Verlag, (2002), 263–273.
3. F.Brezing and A. Weng. *Elliptic curves sutable for pairing based cryptography*, Designs, Codes and Cryptography, **37**:133-141, 2005.
4. H.Cohen. *A course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, **138**, Springer-Verlag,Berlin, 2000.
5. D.A.Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, New York 1989.
6. C.Cocks and R.G.E.Pinch, *Identity-based cryptosystems based on the Weil pairing*, unpublished manuscript, (2001).
7. Regis Dupont, Andreas Enge, Francois Morain. *Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields*, J. Cryptology. **18(2)** (2005), 79–89.
8. D. Freeman. *Constructing pairing-friendly elliptic curves with embedding degree 10*, In Algorithmic Number Theory Symposium ANTS-VII, volumn 4076 of lecture Notes in Computer Science, Springer-Verlag, (2006) 452-465.
9. D.Freeman, M.Scott, E.Teske. *A taxonomy of pairing-friendly elliptic curves*, Cryptology ePrint Archive Report 2006/372. Available at:**http://eprint.iacr.org/2006/372/**.
10. S. Galbraith, J. McKee, and P.Valença. *Ordinary abelian varieties having small embedding degree*, In Proc. Workshop on Mathematical Problems and Techniques in Cryptology, page 29-45. CRM, Barcelona, 2005.
11. C.Batat, D.Bernardi, H.Cohen, M.Olivier. *PARI-GP Version 2.3.1*
12. S.Lang. *Algebra* Addison-Wesley, Reading, MA, 1993 (3rd ed.)
13. G.-J.Lay and H.G.Zimmer, *Constructing elliptic curves with given group order over large finite fields*, In L.M. Adleman and M.-D. Huang, editors. *ANTS-1: Algorithmic Number Theory*, Springer-Verlag, LNCS 877 (1994), 250–263.
14. A. Murphy and N. Fitzpatrick *Elliptic curves for pairing applications*, Cryptology ePrint Archive Report 2005/302. Available at:**http://eprint.iacr.org/2005/302/**.
15. 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), 1234–1243.
16. A.Menezes, T.Okamoto and S.Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **39** (1993), 1639-1646.
17. A.Menezes and S.Vanstone, *Isomorphism classes of elliptic curves over finite fields of characteristic 2*, Utilitas Mathematica. **38** (1990), 135–153.

18. M.Scott and P.S.L.M.Barreto, *Generating more MNT elliptic curves*, Cryptology ePrint Archive: Report 2004.
19. J.H.Silverman, *The Arithmetic of Elliptic Curves. Springer*, Springer (1986).
20. L.C.Washington, *Introduction to Cyclotomic Fields*, Springer (1997).