Pairing-Friendly Elliptic Curves With Various Discriminants

Woo Sug Kang · Ki Taek Kim

Abstract In this paper, we extend the Brezing-Weng method by parameterizing the discriminant D by a polynomial $D(x)$ and give a construction of families of pairing-friendly elliptic curves with various discriminants. For $k = 5$, 8, 9, 15, 16, 20, 24 and 28, our method gives smaller ρ value than the ones in previous results.

Keywords pairing · pairing-friendly elliptic curves · embedding degree · elliptic curves · Brezing-Weng method

1 Introduction

Many researchers have been interested in the pairing based cryptography. Elliptic curves suitable for the pairing based cryptography have to satisfy special properties which most randomly generated curves will not have. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with a prime or prime power integer q and the order of $E(\mathbb{F}_q)$ equal to $q + 1 - t = hr$, where t is the trace of the Frobenius automorphism and r the largest prime number dividing the order of $E(\mathbb{F}_q)$. The embedding degree is the smallest positive integer k such that r divides $q^k - 1$, that is, r divides $q^k - 1$ but does not divide $q^i - 1$ for all $0 < i < k$. The parameter ρ, which is the ratio of the size of q to the the size of r, is defined by $\log q / \log r$. A pairing-friendly elliptic curve is an elliptic curve with small embedding degree and large prime divisor.

The Complex Multiplication method(CM method) is a useful method that constructs elliptic curves. The CM method needs integral solutions of the following diophantine equation:

$$Dy^2 = 4q - t^2,$$

Woo Sug Kang
Department of Mathematics, Korea University 136-701, Seoul, Korea
Tel.: +82-2-3290-3070 (Department Office)
Fax: +82-2-929-8562 (Department Office)
E-mail: wsgkang@korea.ac.kr

Ki Taek Kim
Department of Mathematics, Korea University 136-701, Seoul, Korea
Tel.: +82-2-3290-3070 (Department Office)
Fax: +82-2-929-8562 (Department Office)
E-mail: choyp71@korea.ac.kr

which is called the CM equation.

Consequently, to construct pairing-friendly elliptic curves using the CM method, one needs the following conditions for the triple (t, r, q):

1 q is prime or prime power and r prime.
2 $hr = q + 1 - t$ for some small integer h.
3 r divides $q^k - 1$ but does not divide $q^i - 1$ for all $0 < i < k$.
4 $Dy^2 = 4q - t^2$ for some integer y.

Note that condition 3 can be restated as follows:

$$r \mid \Phi_k(t-1) \quad \text{and} \quad r \not\mid \Phi_i(t-1)$$

for all $0 < i < k$, where $\Phi_k(x)$ is the kth cyclotomic polynomial [1,9].

There are many well-known strategies for constructing pairing-friendly elliptic curves: Miyaji, Nakabayashi and Takano developed the MNT method [15]. Cocks and Pinch [6] presented their general method of constructing curves of arbitrary embedding degree. Barreto, Lynn and Scott [1] described a simple algebraic construction for certain pairing-friendly families of elliptic curves with low discriminant. This idea was generalized and extended by the work of Brezing and Weng [3]. Freeman [8] presented a general method of constructing families of elliptic curves with prescribed embedding degree and prime order.

Among them, we are interested in Brezing-Weng method(BW method). Brezing and Weng parameterize integer triple (t, r, q) by polynomial triple $(t(x), r(x), q(x))$. Now, we write down a definition of polynomial type, which is similar to the above conditions.

Definition 1 [9] Let $t(x)$, $r(x)$ and $q(x)$ be polynomials with rational coefficients. For a given positive integer k and positive square free integer D, we say that the triple $(t(x), r(x), q(x))$ represents a family of elliptic curves with embedding degree k and discriminant D if the following conditions are satisfied:

1. $q(x)$ represents prime or prime power integers.
2. $r(x)$ has a large prime divisor for some $x \in \mathbb{Z}$.
3. $h(x)r(x) = q(x) + 1 - t(x)$ for some $h(x)$ in $\mathbb{Q}[x]$.
4. $r(x)$ divides $\Phi_k(x)$.
5. $Dy^2(x) = 4q(x) - t^2(x)$ has infinitely many integral solutions.

In this paper, we extend the BW method by parameterizing discriminant D as polynomial $D(x)$, that is, we replace $Dy^2(x) = 4q(x) - t^2(x)$ in Definition 1 by

$$D(x)y^2(x) = 4q(x) - t^2(x).$$

Up to now, the maximum of CM discriminant that we can handle well is about 10^{14} [17]. Thus degree of the square free part of $D(x)$ has to be sufficiently small. By making the square free part of $D(x)$ a linear monomial, we give a new construction of families of pairing-friendly elliptic curves with the discriminant $D(x)$ of which the degree of the square free part is small as well as various discriminants. This construction gives smaller ρ value than ones in [9, Table 8.2]. Moreover, in the case that the square free part of $D(x)$ is not equal to x, we also found families with smaller ρ value than ones in [9, Table 8.2].

This paper is organized as follows, In Section 2, we introduce the BW method. In Section 3, we describe the main idea and the algorithm. In Section 4 and Appendix, we give explicit results.

Table 1

	CM equation
BW method	$Dy(x)^2 = 4q(x) - t(x)^2$
Our method	$D(x)y(x)^2 = 4q(x) - t(x)^2$

2 Brezing and Weng's Method

We now introduce the BW method. It is based on the Cocks-Pinch's method(CP method) [6]. They use the parametrization of r, q, and t by polynomials $r(x)$, $q(x)$ and $t(x)$ respectively. The basic idea of this method is as follows. ζ_k and $\sqrt{-D}$ are considered as elements in $\mathbb{Q}[x]/(r(x))$, that is, they are regarded as some polynomials modulo $r(x)$ and then set $t(x)$ the polynomial which represents $1+\zeta_k$ in $\mathbb{Q}[x]/r(x)$. To do it, $r(x)$ must be chosen an irreducible polynomial in $\mathbb{Q}[x]$ such that it defines the field $K = \mathbb{Q}[x]/(r(x))$ with ζ_k, $\sqrt{-D} \in K$.

Construction 1 (Brezing and Weng's method : BW-method)

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 kth root of unity and $K = \mathbb{Q}[x]/(r(x))$.
3. Choose $t(x)$ mapping to $1 + \zeta_k$ in K.
4. Choose $b(x)$ mapping to $\sqrt{-D}$ in K.
5. Compute $y(x) = (t(x) - 2)b(x)/D$ 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 integers for some x, by the CM method, construct an elliptic curve over $\mathbb{F}_{q(x)}$ with an order $r(x)$ subgroup.

This method gives elliptic curves with $1 < \rho < 2$, where the parameter ρ is defined by the ratio $\deg q(x)/\deg r(x)$. This method gives goodρ values in the case when $D = 1$ and 3(ρ is sufficiently close to 1). Freeman, Scott and Teske gave also the families in the case D equal to 2. In these cases, they let $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$ and $r(x)$ be a cyclotomic polynomial which means the field K is a cyclotomic field. There are some advantages in this setting. The main point is that the ring of algebraic integers of the cyclotomic field $\mathbb{Q}(\zeta_k)$ is $\mathbb{Z}[\zeta_k]$. Since ζ_k and $\sqrt{-D}$ are algebraic and ζ_k is corresponding to a polynomial x, we can choose $t(x)$ and $b(x)$ as polynomials with integer coefficients. Thus for any integer x, $t(x)$ always represents an integer. Moreover, the following conjecture tells us that $\Phi_k(x)$ represents prime integers for infinitely many integers x.

Conjecture 1 [13] There are infinitely many $x \in \mathbb{Z}$ such that $f(x)$ is prime if the following conditions are satisfied :

1. The leading coefficient of f is positive.
2. The polynomial f is irreducible.
3. The set of integers $\{f(n)|n \in \mathbb{Z} \text{ and } n > 0\}$ has no common divisor larger than 1.

Lemma 1 *$\Phi_k(x)$ represents prime integers for infinitely many integers x.*

Proof If k is equal to 1, it is clear. Suppose that k is larger than 1.
Recall that

$$x^k - 1 = \prod_{d|k} \Phi_d(x).$$

Since $\Phi_1(x) = x - 1$, $\Phi_k(x)$ divides

$$\frac{x^k - 1}{x - 1} = x^{k-1} + x^{k-2} + \cdots + 1.$$

Thus $\Phi_k(1)$ divides k and $\Phi_k(k)$ divides $k^{k-1} + k^{k-2} + \cdots + 1$. Since $\gcd(k,\ k^{k-1} + \cdots + 1) = 1$, $\gcd(\Phi_k(1),\ \Phi_k(l)) = 1$. □

3 The main idea

Construction 2 (main idea)

1. For fixed $k \in \mathbb{N}$, choose an irreducible polynomial $r(x)$ such that $\zeta_k \in K = \mathbb{Q}[x]/(r(x))$.
2. Choose $t(x) \in \mathbb{Q}[x]$ mapping to $1 + \zeta_k \in K$.
3. Choose $b(x) \in \mathbb{Q}[x]$ mapping to an element in K^* and let $D(x) = -b(x)^2$ in K.
4. Compute $y(x) = (t(x) - 2)/b(x)$ in K.
5. Compute $q(x) = (t(x)^2 + D(x)y(x)^2)/4$ in $\mathbb{Q}[x]$.
6. If the the leading coefficient of $D(x)$ is negative and the power of leading term is odd, then set $t(x) := t(-x)$, $r(x) := r(-x)$, $q(x) := q(-x)$ and $D(x) := D(-x)$.
7. If $q(x)$ and $r(x)$ represent prime integers, then $(t(x),\ r(x),\ q(x))$ represents a family of elliptic curves with embedding degree k and discriminant $D(x)$.

In construction 2, we have to choose $D(x)$ carefully, because the maximum CM discriminants that we can currently handle is about 10^{14}[17]. The currently accepted minimum bits of $r(x)$ for implements is 160.

Suppose that $D(x)$ represents a positive square free integer and $t(x)$ represents an integer and $r(x)$ represents an 160-bit prime number and $q(x)$ represents also a prime integer for some $x \in \mathbb{Z}$. Then $r(x)$ is larger than 2^{160}. Since $\deg r(x) \geq \phi(k)$, the minimum bits of x is asymptotically greater than $160/\phi(k)$. In order that $D(x)$ is less than $10^{14} (\approx 2^{42})$, the maximum bits of x is asymptotically $42/\deg D(x)$. Thus the degree of $D(x)$ has to be asymptotically less than $\phi(k)/4$.

$D(x)$ must represent positive integers for some positive integer x. Since $\zeta_k \in K = \mathbb{Q}[x]/(r(x))$, the power of the leading term of $r(x)$ is always even. Since $q(x) = (t(x)^2 + D(x)y(x)^2)/4$, the sign of the leading coefficient of $q(x)$ is positive or the same of $D(x)$'s. Thus if the leading coefficient of $D(x)$ is negative and the power of leading term is odd then $(t(-x),\ r(-x),\ q(-x))$ forms a family with a discriminant $D(-x)$.

In Step 5,

$$\deg q(x) = \max\{2\deg t(x),\ \ \deg D(x) + 2\deg y(x)\}.$$

Since the degrees of $t(x)$, $D(x)$, $y(x)$ are less than the degree of $r(x)$,

$$\rho = \frac{\deg q(x)}{\deg r(x)} < \frac{3\deg r(x)}{\deg r(x)} = 3.$$

But, in our computation, there are sufficiently many cases that ρ values are close to 1.

Finally, we check whether $q(x)$ represents a prime number for some $x \in \mathbb{Z}$ by Conjecture1.

Now, we introduce some methods to apply Construction 2.

Table 2

k	$p(x)$	square root of $p(x)$	$r(x)$
1 mod 2	x	$x^{(k+1)/2}$	$\Phi_k(x)$
2 mod 4	$-x$	$x^{(k/2+1)/2}$	$\Phi_k(x)$
4 mod 8	$2x$	$x^{(3k+4)/8} - x^{(k+4)/8}$	$\Phi_k(x)$

3.1 The square free part of $D(x)$ is of the form ax.

Let $(t(x), r(x), q(x))$ represent a family of pairing-friendly with a discriminant $D(x)$ of which the square free part is equal to x. If $r(\alpha x^2)$ has a large prime divisor for some x and $q(\alpha x^2)$ represents infinitely many primes then $(t(\alpha x^2), r(\alpha x^2), q(\alpha x^2))$ represents a family with a discriminant α. If $r(x)$ is especially $\Phi_k(x)$ then there are some advantages.

The following lemma gives the sufficient condition of the irreducibility of $r(\alpha x^2)$.

Lemma 2 [22, Lemma 4.4] *Suppose that $\Phi_k(\alpha x^2)$ splits into the different irreducible polynomials over $\mathbb{Q}$, where α is a square free integer. Then*

$$\alpha \ \ divides \ \begin{cases} k & if \ \ k \ \ is \ \ odd \\ k/2 & if \ \ k \ \ is \ \ even. \end{cases}$$

Specially, if k is odd and α is congruent to 1 modulo 4, then the converse is true.

Proof Suppose that $\Phi_k(\alpha x^2)$ splits into different irreducible polynomials over $\mathbb{Q}$. By lemma [10, Lemma 12], $\alpha x^2 - \zeta_k$ has a solution in $\mathbb{Q}(\zeta_k)$. Let k be odd. Then ζ_k is a square in $\mathbb{Q}(\zeta_k)$. So α is also a square in $\mathbb{Q}(\zeta_k)$ i.e. $\mathbb{Q}(\sqrt{\alpha}) \subset \mathbb{Q}(\zeta_k)$. By Conductor-Discriminant Formula [21], the field discriminant of $\mathbb{Q}(\sqrt{\alpha})$ divides k and so $\alpha \equiv 1 \bmod 4$. Thus α divides k. Conversely if $\alpha \equiv 1 \bmod 4$ and α divides k, α is a square in $\mathbb{Q}(\zeta_k)$. Since ζ_k is also a square, $\alpha x^2 - \zeta_k$ has a solution in $\mathbb{Q}(\zeta_k)$. By lemma [10, Lemma 12], $\Phi_k(\alpha x^2)$ is reducible over $\mathbb{Q}$. Let k be even. $\alpha x^2 - \zeta_k$ has also a solution in $\mathbb{Q}(\zeta_{2k})$. Since ζ_k is a square in $\mathbb{Q}(\zeta_{2k})$, α is also a square in $\mathbb{Q}(\zeta_{2k})$. By Conductor-Discriminant Formula, 4α divides $2k$. □

First, we set $r(x) = \Phi_k(x)$ and $K = \mathbb{Q}[x]/(r(x)) = \mathbb{Q}(\zeta_k)$. Then ζ_k is corresponding to a polynomial x. So we can choose $t(x)$ equal to $x^i + 1$ for some i with $\gcd(i, k) = 1$. By Proposition 2, $r(x)$ represents prime integers for infinitely many integers x. In the Construction 2, in order that a square free part of $D(x)$ is of the form ax, ax has to be a square element in K. If k is not a multiple of 4, x is a square in K. If $k \equiv 4 \bmod 8$, $2x$ is a square in K. The Table 2 gives square roots of x, $-x$ or $2x$ modulo $r(x)$.

The following is an algorithm to find families of paring-friendly curves with $D(x)$ of which the square free part of the form ax when $r(x)$ is a cyclotomic polynomial.

Algorithm 3

Input	$k \in \mathbb{N}$, $k \neq 0 \bmod 8$.
Output	pairing-friendly families with embedding degree k.
1.[initialize]	Set $r(x) \leftarrow \Phi_k(x)$.
	For $i = 1, \ldots k-1$ set $t(x) \leftarrow x^i + 1$.
2.[make $D(x)$]	Set $b_0(x) \leftarrow$ a square root in Table 2 and $b_1(x) \leftarrow$ a divisor of $(t(x)-2) \cdot b_0(x)^{-1}$ in $\mathbb{Q}[x]$. Set $D(x) \leftarrow -xb_1(x)^2$ if k is odd, $D(x) \leftarrow xb_1(x)^2$ if $k \equiv 2 \bmod 4$, $D(x) \leftarrow -2xb_1(x)^2$ if $k \equiv 4 \bmod 8$ in $\mathbb{Q}[x]$.
3.[make family]	Compute $$y(x) \leftarrow \frac{t(x)-2}{b_0(x)b_1(x)} \mod r(x).$$
	Compute $q(x) = (t(x)^2 + D(x)y(x)^2)/4$ in $\mathbb{Q}[x]$.
	If k is odd or $k \equiv 4 \bmod 8$, set $t(x) \leftarrow t(-x)$, $r(x) \leftarrow r(-x)$, $q(x) \leftarrow q(-x)$, $D(x) \leftarrow D(-x)$.
4.[check $q(x)$]	Set $j \leftarrow 1$, $g \leftarrow q(1)$. While $\gcd(g, q(j)) \neq 1$ and $j \leq 1000$ set $j \leftarrow j+1$, $g \leftarrow \gcd(g, q(j))$.
5.[conclude]	If $g \neq 1$ go to step 2. $(t(x), r(x), q(x))$ is a pairing friendly families with embedding degree k and discriminant $D(x)$.

By this method, we find pairing friendly families with embedding degree 20 and 28, and update the table in [9].

Remark 1 If $b_1(x)$ is an element in the ring of algebraic integers $\mathbb{Z}[\zeta_k]^*$ of K, its inverse is also in $\mathbb{Z}[\zeta_k]^*$. Thus $4q(x)$ has integer coefficients and such a $q(x)$ will represent integers for some integer x in high provability. But to lower the degree of $q(x)$, we chose $b_1(x)$ as divisors of $t(x)-2$. The reason is that $b_1(x)$ can be chosen throughout several ways, since $t(x) - 2 = x^i - 1$ is always factored for $i > 1$.

In first strategy, we cannot treat the case that k is congruent to 0 modulo 8, because we did not find a square element of the form ax. We use the method in [12] to overcome it. It is the idea to change the representative of elements in the field K as follows.

Second, let $\theta = a_0 + a_1\zeta_k + \ldots + a_{k-1}\zeta_k^{k-1} \in \mathbb{Q}(\zeta_k)$. Let

$$\begin{aligned} 1 &= 1 \\ \theta^2 &= a_{12} + a_{22}\zeta_k + a_{32}\zeta_k^2 + \ldots a_{k2}\zeta_k^{k-1} \\ \theta^4 &= a_{13} + a_{23}\zeta_k + a_{33}\zeta_k^2 + \ldots a_{k3}\zeta_k^{k-1} \\ &\vdots \\ \theta^{2(k-1)} &= a_{1k} + a_{2k}\zeta_k + a_{3k}\zeta_k^2 + \ldots a_{kk}\zeta_k^{k-1} \end{aligned}$$

Table 4

k	ρ	$d(x)$	ρ_1	D	$\deg r(x)$
5	1.500	x	1.750	any odd	8
8	1.750	x	-	-	-
9	1.667	x	1.833	any odd	12
15	1.625	x	1.750	any even	32
16	1.875	x	-	-	-
20	1.875	x	-	-	-
	1.875	$2x$	-	-	-
24	1.875	x	-	-	-
28	1.750	$2x$	1.917	6 mod 8	24

k : an embedding degree
$d(x)$: a square free part of $D(x)$
ρ_1 : each ones of the case "variable D" in Table 8.2 of [9]

Then the matrix

$$A = \begin{bmatrix} 1 & a_{12} & a_{13} & \dots & a_{1k} \\ 0 & a_{22} & a_{23} & \dots & a_{2k} \\ 0 & a_{32} & a_{33} & \dots & a_{3k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_{k2} & a_{k3} & \dots & a_{kk} \end{bmatrix}$$

changes the basis representation of elements from $\mathbb{Q}(\theta^2)$ to $\mathbb{Q}(\zeta_k)$. If the determinant of A is not 0, $\mathbb{Q}(\theta^2)$ is equal to $\mathbb{Q}(\zeta_k)$ and a irreducible polynomial of θ^2 is equal to

$$\begin{aligned} r(x) &= \prod_{\varphi \in \mathrm{Aut}(\mathbb{Q}(\zeta_k))} \left(x - \varphi(\theta^2)\right) \\ &= \prod_{\substack{\gcd(i,k)\neq 1 \\ 1 \le i \le k-1}} \left(x - a_{12} - a_{22}\zeta_k^i - a_{32}\zeta_k^{2i} - \dots a_{k2}\zeta_k^{(k-1)i}\right) \end{aligned}$$

In $\mathbb{Q}(\theta^2)$, the representation of ζ_k and a square root of x is

$$\zeta_k \leftarrow A^{-1}\begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \qquad \text{a square root of } x \leftarrow A^{-1}\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{bmatrix}.$$

If step 1, step2 in Algorithm 3 are modified as above, then we can apply the Algorithm 4 to the case k is congruent to 0 modulo 8. But if $\phi(k)$ is large, then denominators of coefficients of $q(x)$ is very large, so it is very difficult that $q(x)$ represents primes.

By using this method, we found families of pairing-friendly curves with embedding degree 5, 8, 9, 15, 16, 20 and 24, and improve the table in [9](See Table 4).

3.2 Large discriminants

We choose a polynomial $b(x)$ as an element in the ring of algebraic integers $\mathbb{Z}[\zeta_k]^*$ and set $D(x) = -b(x)^2$. If we choose a polynomial $b(x)$ arbitrarily, even we choose $b(x)$ with integer coefficients, its inverse does not have integer coefficients. Then $q(x)$ has rational coefficients generally. In this case, it is disadvantageous that $q(x)$ represents primes. But if we choose $b(x) \in \mathbb{Z}[\zeta_k]^*$, its inverse is also in $\mathbb{Z}[\zeta_k]^*$. Thus $4q(x)$ has integer coefficients and such a $q(x)$ will represent integers for some integer x in high provability. By the Dirichlet unit theorem, the rank of the unit group $\mathbb{Z}[\zeta_k]^*$ is equal to $\phi(k)/2 - 1$.

The unit group of $\mathbb{Z}[\zeta_k]$

$$\mathbb{Z}[\zeta_k]^* \cong \mathbb{Z}_{tor} \oplus \mathbb{Z}^r \cong \langle x \rangle \oplus \langle b_1(x) \rangle \oplus \cdots \oplus \langle b_r(x) \rangle.$$

$$b(x) = x^{i_0} b_1^{i_1}(x) \cdots b_r^{i_r}(x), \quad 0 \leq i_0 \leq k-1$$

Here, we compute the generators of the unit group by PARI GP and they are easily computed. There are infinitely many choices of $b(x)$. Since the rank of $\mathbb{Z}[\zeta_k]^*$ is $\phi(k)/2-1$,the rank increases as k increases. We compute families of pairing-friendly elliptic curves when $3 \leq k \leq 50$ and choose $b(x)$ the product of the generators of $\mathbb{Z}[\zeta_k]^*$,

$$b(x) = x^{i_0} b_1^{i_1}(x) \cdots b_r^{i_r}(x), \quad 0 \leq i_0 \leq k-1, \quad -1 \leq i_j \leq 1, \quad j = 1, 2, \cdots, r.$$

For sufficiently larger k's with $1 \leq k \leq 50$, we find families with good ρ values, but the degree of a square free part of $D(x)$ is very large. Thus these are not available.

Example 1 When $k = 14$, we get a family with $\rho = 1.167$ (In [9, Table 8.2], $\rho = 1.833$.).

$$\begin{aligned}
r(x) &= \Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1. \\
\mathbb{Z}[\zeta_k]^* &= \langle x \rangle \oplus \langle x^2 - x \rangle \oplus \langle x^3 - 1 \rangle. \\
t(x) &= -x^2 + 1. \\
b(x) &= x^3 b_1(x)^{-1} b_2(x)^{-1} = x^5 - x^4 + x^3 - x^2 - 1. \\
D(x) &= x^5 - x^2 - 2. \\
q(x) &= (1/4)(x^7 - 4x^4 + 1).
\end{aligned}$$

The ratio of the degree of $r(x)$ to the degree of $D(x)$ is small. If the square free part of $D(x)$ is less than 10^{14} and $r(x)$ has large prime factor (asymptotically 160-bits) and $q(x)$ are primes for some integer x, then we make a pairing-friendly curve but we cannot find such integers.

4 Finding the curves

In the section, we give actual curves from the families with ρ values in Table 4. The Example 2−10 described pairing-friendly families and elliptic curves over $\mathbb{F}_{q(i)}$ for some integer i, defined by equations of the form

$$E \ : \ Y^2 = X^3 + aX + b, \quad a, \quad b \ \in \ \mathbb{F}_{q(i)}$$

Example 2 $k = 5$, $\rho = 1.500$, $\theta = \zeta_5^3 - \zeta_5^2 - \zeta_5$, $D(x) = x$.

$$
\begin{aligned}
t(x) &= 1/55(-4x^3 + 31x^2 - 86x + 154) \\
r(x) &= x^4 - 11x^3 + 46x^2 - 96x + 121 \\
q(x) &= 1/12100(16x^6 - 199x^5 + 1005x^4 - 3650x^3 + 11700x^2 - 23239x + 23716)
\end{aligned}
$$

$$
\begin{aligned}
i &= 195593505304 \\
D(i) &= 886 \cdot 14858 \\
t(i) &= -5442025739431292721114116816488 90 \\
r(i) &= 3025 \cdot 48382949559648749597165444117359981116228 1 \\
&= 14635842241793746753142546845501394287659000 25 \\
q(i) &= 74039110372741036110595689827548994519051195571787209728370532879 \\
j &= 64752591869714152811256730172279880579448403321515657295993909314 \\
a &= 1 \\
b &= 59597852623099057163355022678916117855059525119755147790288371 88
\end{aligned}
$$

Remark 2 $r(i)$ does not divide $q(i) + 1 - t(i)$ but $r(i)/3025$ divide because coefficients of $q(x)$ are rational numbers.

The other examples are provided in Appendix.

5 Conclusion

We have extended the BW-method by parameterizing the discriminant D as a polynomial $D(x)$, and by making the square free part of $D(x)$ a linear monomial, we have given a new construction of families of pairing-friendly elliptic curves with various discriminants. This method has updated results for k is equal to 5, 8, 9, 15, 16, 20, 24, and 28 in [9]

Example 3 $k = 8$, $\rho = 1.750$, $\theta = \zeta_8^2 - \zeta_8 - 1$, $D(x) = x$.

$$
\begin{aligned}
t(x) &= 1/72(x^3 - 9x^2 - 23x + 135) \\
r(x) &= x^4 - 14x^2 + 81 \\
q(x) &= 1/186624(25x^7 + 279x^6 + 137x^5 - 3897x^4 - 2201x^3 - 855x^2 - 20169x + 164025) \\
i &= 194552503893 \\
D(i) &= 25933 \cdot 2739^2 \\
t(i) &= 10227699915984676666304373192871 46 \\
r(i) &= 324 \cdot 44218325062513197303639007330095291780315 29 \\
q(i) &= 14132867486678524041799711064414365664290749718137722344493528448477712956 29 \\
j &= 13132501116921353302420634786670124433770045709944290777244039388829412813 27 \\
a &= 1, \quad b = 33026598352928473531659793750184610914593551152740464413170189623375770306 8
\end{aligned}
$$

Example 4 $k = 9$, $\rho = 1.667$, $\theta = \zeta_9^4 - \zeta_9$, $D(x) = x$.

$$
\begin{aligned}
t(x) &= 1/243(x^5 + 243) \\
r(x) &= x^6 + 27x^3 + 729 \\
q(x) &= 1/236196(x^{10} + x^9 + 12x^8 + 36x^7 + 108x^6 + 1296x^5 + 972x^4 + 2916x^3 + 8748x^2 + 6561x + 59049) \\
i &= 68373837 \\
D(i) &= 133 \cdot 717^2 \\
t(i) &= 61495521373943529699475567931890924 00 \\
r(i) &= 729 \cdot 14015615848840103156256522099854554086379896 1 \\
q(i) &= 94542480109057755518930624499913503986864388420749518505348308708611977 33 \\
j &= 72375653952258572478689865073291376781070139033740943275606865041460072 77 \\
a &= 1, \quad b = 35638606112041486780119410986183829876933176803100299208863688505725126 03
\end{aligned}
$$

Example 5 $k = 15$, $\rho = 1.625$, $\theta = \zeta_{15}^6 - \zeta_{15}$, $D(x) = x$.

$$
\begin{aligned}
t(x) &= 1/9(x^2 + 9) \\
r(x) &= x^8 - 3x^7 + 27x^5 - 81x^4 + 243x^3 - 2187x + 6561 \\
q(x) &= 1/19131876(x^{13} - 36x^{11} + 54x^{10} + 486x^9 - 972x^8 - 729x^7 + 4374x^6 - 19683x^5 + 98415x^4 + 118098x^3 + 1062882x^2 + 531441x + 4782969) \\
i &= 747477 \\
D(i) &= 157 \cdot 69^2 \\
t(i) &= 62080207282 \\
r(i) &= 6561 \cdot 14852887454655073291040904745058562272715361 \\
q(i) &= 11885413154877701166373441791911986877458237992592863810612151708316 81 \\
j &= 82177736067510478895649778550833374998690016576664243292140711791062 5 \\
a &= 1, \quad b = 68034269976022518486850374760987017262521957100948950897049255760634 5
\end{aligned}
$$

Example 6 $k = 16$, $\rho = 1.875$, $\theta = \zeta_{16}^3 - \zeta_{16}^2 + \zeta_{16}$, $D(x) = x$.

$$
\begin{aligned}
t(x) &= 1/15232(805x^7 + 29x^6 + 61173x^5 + 2173x^4 + 545167x^3 + 17175x^2 + 257271x + 9455) \\
r(x) &= x^8 + 76x^6 + 678x^4 + 332x^2 + 1 \\
q(x) &= 1/928055296(1071225x^{15} + 1184155x^{14} + 163062101x^{13} + 180084143x^{12} + 7675844277x^{11} + 8459288319x^{10} + 112790539217x^9 + 123452816371x^8 \\
&\quad +570916933563x^7 + 612444226337x^6 + 600345335791x^5 + 568302416637x^4 + 205078397143x^3 + 148393676933x^2 + 16190423851x + 89397025) \\
i &= 1772479 \\
D(i) &= 631 \cdot 53^2 \\
t(i) &= 290473586675134493270124005038085235578 1328 \\
r(i) &= 974201485748931383139300055162029306683177594890 88 \\
q(i) &= 618049975769586460968602325490839448675938230505192754584034729256545083274363861087170060 7 \\
j &= 246180408479753594324487008664160173814172836314814603285659818939649188087981514557068 25 \\
a &= 1, \quad b = 54527615139011124868102810860908177097277236038723911543989341855139875422024802703411373 33
\end{aligned}
$$

Example 7 $k = 20$, $\rho = 1.875$, $\theta = \zeta_{20}^4 - \zeta_{20}^3 + \zeta_{20}^2 - \zeta_{20}$, $D(x) = x$.

$$
\begin{aligned}
t(x) &= 1/80000(29x^7 - 5x^6 + 6365x^5 - 1125x^4 + 116975x^3 - 26375x^2 + 84375x + 625)\\
r(x) &= x^8 + 220x^6 + 4150x^4 + 5500x^2 + 625\\
q(x) &= 1/25600000000(5184x^{15} + 6313x^{14} + 2284994x^{13} + 2779835x^{12} + 295707620x^{11} + 358867025x^{10} + 9751592750x^9 + 11711694875x^8\\
&\quad +109202235000x^7 + 127205981875x^6 + 313291818750x^5 + 315762615625x^4 + 299707262500x^3 + 231741921875x^2 + 55213031250x + 390625)\\
i &= 1123875\\
D(i) &= 555\\
t(i) &= 8209827254103471820738118226929400924 17\\
r(i) &= 2^8 \cdot 5^4 \cdot 15908312104649987181207741869379410799071521\\
q(i) &= 11673354066578992295149608491156342297091926381221763241038504857636045106761548504 61\\
j &= 10269111407101666417756629602398237147027695459379053100885482907429049298735202606 92\\
a &= 1, \quad b = 643330466372358748699758204040177563909871963494394905678571169655887414694971960885
\end{aligned}
$$

Example 8 $k = 20$, $\rho = 1.875$, $D(x) = 2x$.

$$
\begin{aligned}
t(x) &= -x + 1\\
r(x) &= x^8 - x^6 + x^4 - x^2 + 1\\
q(x) &= 1/8(x^{15} + 2x^{14} + x^{13} - 2x^{12} + 6x^{10} + 5x^9 - 4x^8 - 5x^7 + 4x^6 + 6x^5 - 2x^4 - 4x^3 + 2x^2 - 3x + 2)\\
i &= 839318\\
D(i) &= 499 \cdot 58^2\\
t(i) &= -839317\\
r(i) &= 5 \cdot 4925408917511444963257019703142097346418062 1001\\
r(i) &= 2462704458755722481628509851571048673209031050 05\\
q(i) &= 9032523583439828681435793188873823269252144396574481242621511678009705686827391234999017\\
j &= 6478666610891970744441315527890412541700207604591334162362165986585186839932119275345661\\
a &= 2, b = 64747030181143104893179365705400349478347051147791183117146650113078012671085942464992 42
\end{aligned}
$$

Example 9 $k = 24$, $\rho = 1.875$, $\theta = \zeta_{24}^5 - \zeta_{24}^4 + \zeta_{24}^3 - \zeta_{24}^2 + \zeta_{24}$, $D(x) = x$.

$$
\begin{aligned}
t(x) &= 1/23040(1047x^7 + 67x^6 + 498375x^5 + 31875x^4 + 1414845x^3 + 82305x^2 + 487077x + 29177) \\
r(x) &= x^8 + 476x^6 + 1350x^4 + 476x^2 + 1 \\
q(x) &= 1/2123366400(380689x^{15} + 648267x^{14} + 362753397x^{13} + 617163199x^{12} + 87604086285x^{11} + 148644371055x^{10} + 566963598673x^9 \\
&\quad +836673547299x^8 + 1292135368899x^7 + 1472610151153x^6 + 1203868542735x^5 + 808441906605x^4 + 426073979359x^3 + 144465131157x^2 \\
&\quad +45508779627x + 851297329) \\
i &= 684383 \\
D(i) &= 13967 \cdot 7^2 \\
t(i) &= 319564656055701151399066748335203328257 8 \\
r(i) &= 57600 \cdot 835547650642495749795064041731113469411497 \\
r(i) &= 4812754467700775518819568880371213583810222720 0 \\
q(i) &= 60678476256420269150741937094461909491300001864264319008045971147487196739267458152 1 \\
j &= 57719754825503086248408569113880268460568197318214097917285987825104241386533934630 6 \\
a &= 1, b = 436742299333639250226599680722783224604493348066195145530835086006442029475326564518
\end{aligned}
$$

Example 10 $k = 28$, $\rho = 1.750$, $D(x) = 2x$.

$$
\begin{aligned}
t(x) &= -x^9 + 1 \\
r(x) &= x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1 \\
q(x) &= 1/8(4x^{21} - 4x^{19} + 2x^{18} + 5x^{17} - 4x^{16} - 6x^{15} + 6x^{14} + 7x^{13} - 4x^{12} - 7x^{11} + 4x^{10} - x^9 - 4x^8 - 3x^7 + 4x^6 + 3x^5 - 2x^4 - 2x^3 + x + 2) \\
i &= 16230 \\
D(x) &= 8115 \\
t(x) &= -781387893992636735502322278629999999 99 \\
r(x) &= 29 \cdot 11519250917219676764933655331140962146283621861969 \\
r(x) &= 3340582765993706261830760046030879022422250339971 01 \\
q(x) &= 13051454661141123258135950949380281191245025170650024335529330033478574418877842386670279 \\
j &= 10879610693014955554140064479343473463546940837748708368465939378315924549486521484824922 \\
a &= 1, b = 5120690481325659159770007421510241378236727514950747983329093283850693112823440170194067
\end{aligned}
$$

References

1. P.S.L.M. Barreto, B. Lynn, and M. Scott, Constructing elliptic curves with prescribed embedding degrees, Security in Communication Networks - SCN'2002, Lecture Note in Computer Science, 2576, 263-273 (2002)
2. P.S.L.M. Barreto and M. Naehrig, Pairing-friendly elliptic curves of prime order, Workshop on Selected Areas in Cryptography - In Proceedings of SAC 2005, Lecture Notes in Computer Science, 3897, 319-331 (2006)
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 (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. R. Dupont, A. Enge, and F. Morain. Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields, J. Cryptology, 18(2), 79-89 (2005)
8. D. Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10, In Algorithmic Number Theory Symposium - ANTS-VII, lecture Notes in Computer Science, 4076, 452-465 (2006)
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, CRM, Barcelona, 29-45 (2005)
11. The PARI Group, Bordeaux, PARI-GP Version 2.3.2.
12. E. J. Kachisa, E. F. Schaefer, and M. Scott, Construction Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field, Cryptology ePrint Archive Report 2007/452 Available at: http://eprint.iacr.org/2007/452/
13. S. Lang. Algebra, Addison-Wesley, Reading, MA, 1993, 3rd ed.
14. G.-J. Lay and H.G. Zimmer, Constructing elliptic curves with given group order over large finite fields, In Algorithmic Number Theory Symposium - ANTS-1, Lecture Notes in Computer Science, 877, 250-263 (1994)
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), 1234-1243 (2001)
16. Jürgen Neukirch, Algebraic Number Theory, Springer-Verlag (1991)
17. Andrew V. Sutherland, See www-math.mit.edu/ drew(10/31/2008)
18. M. Scott and P.S.L.M. Barreto, Generating more MNT elliptic curves, Designs, Codes and Cryptography, 38, 209-217 (2006)
19. J.H. Silverman, The Arithmetic of Elliptic Curves. Springer, Graduate Texts in Mathematics, 106, Springer-Verlag (1986)
20. V. Miller, The Weil pairing, and its efficient calculation, J. Cryptology, 17, 235-261 (2004)
21. L.C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, (1997)
22. WS Kang, Construction of pairing friendly elliptic curves, Cryptology ePrint Archive Report 2007/110, Available at: http://eprint.iacr.org/2007/110/