Bull. Korean Math. Soc. **49** (2012), No. 1, pp. 75–88
http://dx.doi.org/10.4134/BKMS.2012.49.1.075

CONSTRUCTING PAIRING-FRIENDLY CURVES WITH VARIABLE CM DISCRIMINANT

Hyang-Sook Lee and Cheol-Min Park

Abstract. A new algorithm is proposed for the construction of Brezing-Weng-like elliptic curves such that polynomials defining the CM discriminant are linear. Using this construction, new families of curves with variable discriminants and embedding degrees of $k \in \{8, 16, 20, 24\}$, which were not covered by Freeman, Scott, and Teske [9], are presented. Our result is useful for constructing elliptic curves with larger and more flexible discriminants.

1. Introduction

Over the past few years, a great deal of attention has been focused on pairing-based cryptography. Since 2000, a number of new and novel protocols based on pairings have been proposed such as one-round tripartite key agreement [12], identity-based encryption [4], short digital signature [5] and identity-based key exchange [15] etc. For a practical realization of these protocols, pairings must be implemented efficiently.

For efficient pairing computation over elliptic curves, the curves should have large prime order subgroups and embedding degrees should be small enough so that computations in finite fields are feasible. However, the size of finite fields must be large enough so that discrete log problems in finite fields are hard to compute for security purposes. We call such curves pairing friendly.

One such useful pairing-friendly curves are supersingular elliptic curves with distortion maps. However, these have small embedding degrees limited up to 6 and only a small number of curves exist. Another possible pairing friendly curves are ordinary elliptic curves with a greater choice of embedding degrees. Since these curves are rare according to a study by Balasubramanian and

Received May 12, 2010; Revised April 6, 2011.

2010 *Mathematics Subject Classification.* Primary 11T71, 94A60.

Key words and phrases. elliptic curves, pairing-friendly curves, CM discriminant.

An extended abstract of this paper appears in the proceedings of Pairing 2009, vol. 5671, LNCS, pages 66–77, Springer-Verlag, 2009.

This work was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD, Basic Research Promotion Fund)(KRF-314-2008-1-C00040).

Koblitz [2], it is necessary to develop appropriate algorithms to construct suitable pairing-friendly curves. Many algorithms have been proposed to construct pairing-friendly ordinary elliptic curves. One general method is the Brezing and Weng method [7], which generates polynomial families of curves by using a defining polynomial $r(x)$ of a cyclotomic field or its extension field. Usually, the defining polynomial of cyclotomic field $\mathbb{Q}(\zeta_k)$ for a primitive kth root of unity ζ_k is the kth cyclotomic polynomial $\Phi_k(x)$. But if we use an irreducible factor of $\Phi_k(u(x))$ for some $u(x) \in \mathbb{Q}[x]$, we can obtain a different defining polynomial of the cyclotomic field $\mathbb{Q}(\zeta_k)$ or its extension field. Using this idea, Galbraith, Mckee and Valenca [10] demonstrated the existence of ordinary abelian varieties of dimension 2 having small embedding degrees. Building on this work, Barreto and Naehrig [3], and Freeman [8] constructed pairing-friendly elliptic curves of prime order. If we choose an irreducible factor $r(x)$ of $\Phi_k(u(x))$ such that the degree of $r(x)$ is $\varphi(k)$, $r(x)$ will define the same cyclotomic field $\mathbb{Q}(\zeta_k)$. But in some cyclotomic fields, a careful choice of $r(x)$ can produce a pairing-friendly curve with better ρ-value than curves constructed from $\Phi_k(x)$, where $\rho = \deg q(x)/\deg r(x)$. Working from this idea, Kachisa, Schaefer and Scott [13] developed a method for constructing pairing-friendly elliptic curves with better ρ-values.

In [8], Freeman observed that, if $4q(x) - t(x)^2$ is square-free and has degree larger than 2, the equation $Dy^2 = 4q(x) - t(x)^2$ has finitely many integer solutions (x, y) by Siegel's theorem [16], where $q(x), t(x)$ are the polynomials parameterizing the finite field size and the elliptic curve trace, respectively. Therefore, it is a natural approach to consider the algorithm to find $q(x), t(x)$ which provide pairing-friendly curves such that $4q(x) - t(x)^2$ is not square-free or has a degree less than 3.

We are interested in the case of pairing-friendly curves with the CM equation of degree 1. To construct these curves, we find a necessary and sufficient condition of pairing-friendly curves with the CM equation of degree 1 (Proposition 3.1 and Proposition 3.2). The key idea to find this condition is that the problem becomes more manageable when they are suitably recast in terms of the root of $r(x)$, where $r(x)$ is the polynomial defining the order of elliptic curve group. By the condition of degree 1, we can predetermine the form of the root of $r(x)$ in the cyclotomic field $\mathbb{Q}(\zeta_k)$ to construct curves with the CM equation of degree 1. From this condition and some calculations, we can classify all of the cases such that $q(x), r(x), t(x)$ represent a family of elliptic curves and $4q(x) - t(x)^2$ has a degree of 1 (Theorem 3.6). However, there are some cases in Theorem 3.6 that we cannot find such curves. To cover these cases, we consider the CM discriminant with square part. By finding the condition to have CM discriminant of the form $xf(x)^2$, we can construct more pairing-friendly curves.

Our method is useful for constructing elliptic curves with larger and more flexible discriminants. In the method proposed in this paper, since CM discriminants are not fixed but parameterized by the variable x, we can obtain various and larger discriminants by a suitable x. Moreover, by making proper substitutions in discriminant polynomials, it is possible to construct pairing-friendly elliptic curves with predetermined discriminants. Note that the method to find pairing-friendly curves with variable discriminants is also proposed in [9]. However, there are some cases which are not covered by that paper (See Table 5 in [9]). We fill the gaps by providing method and examples.

The paper is organized as follows: Section 2 reviews the basic definitions related to pairing-friendly curves and methods involved in the construction of the curves. Section 3 presents the complete classification of pairing-friendly elliptic curves with the CM equation of degree 1. We propose a method that provides a more general form of discriminants and an algorithm and examples of the method in Section 4. Section 5 concludes.

2. Pairing-friendly elliptic curves

In this section, we briefly review the definitions and methods involved in the construction of pairing-friendly curves. The background of this section is based on the comprehensive summary of the known constructions of pairing-friendly elliptic curves in [9].

Let E be an elliptic curve defined over a prime finite field $\mathbb{F}_q$. Let r be a large prime factor of $\#E(\mathbb{F}_q)$, and let k be the smallest integer such that $r|(q^k-1)$; such a k is called *the embedding degree with respect to* r. A pairing-friendly curve is formally defined as follows [9].

Definition 2.1. We say that E is pairing-friendly if the following two conditions hold:
(1) there is a prime $r \geq \sqrt{q}$ dividing $\#E(\mathbb{F}_q)$, and
(2) the embedding degree of E with respect to r is less than $\log_2(r)/8$.

There are a number of methods for constructing pairing-friendly elliptic curves with the prescribed embedding degree k. These methods all have the following essential steps:

(1) Look for suitable values of the parameters, including embedding degree k; the cardinality of the finite field q; the trace of the Frobenius endomorphism of the curve t; the prime order of the subgroup r.
(2) Use the Complex Multiplication(CM) method to find the equation of the curve [1].

Like Proposition 2.4 in [9], if we assume $k \nmid r$, the definition of embedding degree k with respect to r is equivalent to

$$\Phi_k(q) \equiv 0 \pmod{r},$$

where $\Phi_k(x)$ is the kth cyclotomic polynomial. Since r is a factor of $\#E(\mathbb{F}_q) = q+1-t$, it is also equivalent to

$$\Phi_k(t-1) \equiv 0 \pmod{r}.$$

For Step (2), we need an additional parameter, the CM discriminant which is defined as the square-free part D of the nonnegative integer $4q - t^2$. For practical reasons, D must be less than 10^{13} by the recent work of Sutherland [17].

Brezing and Weng constructed a family of pairing-friendly curves using polynomials to represent the parameters q, t and r. To describe this method, we first need the following definitions.

Definition 2.2 ([9])**.** Let $f(x)$ be a polynomial with rational coefficients. We say f represent primes if the following conditions are satisfied:
(1) $f(x)$ is non-constant.
(2) $f(x)$ has a positive leading coefficient.
(3) $f(x)$ is irreducible.
(4) $f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$.
(5) $\gcd\{f(x) |\ x, f(x) \in \mathbb{Z}\} = 1$.

Definition 2.3 ([9])**.** Let $t(x), r(x), q(x)$ be polynomials with rational coefficients.

For a given positive integer k and a positive square-free integer D, the triple (t, r, q) represents a family of elliptic curves with embedding degree k and discriminant D if the following conditions are satisfied:
(1) $q(x) = p(x)^d$ where $d \geq 1$ and where $p(x)$ represents primes.
(2) $r(x) = c \cdot \widetilde{r}(x)$, where $\widetilde{r}(x)$ represents primes and $c \in \mathbb{N}$ is a constant.
(3) $q(x) = h(x)r(x) - 1 + t(x)$ for some $h(x) \in \mathbb{Q}[x]$.
(4) $r(x)$ divides $\Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial.
(5) The equation $Dy^2 = 4q(x) - t(x)^2$ has infinitely many integer solutions (x, y).

The equation in condition (5) is called *the CM equation.* Note that since $q(x) + 1 - t(x) = h(x)r(x)$, the CM equation is equivalent to

$$Dy^2 = f(x) = 4h(x)r(x) - (t(x) - 2)^2.$$

If c and $h(x)$ are equal to 1 in conditions (2) and (3), respectively, the elliptic curve group has prime order. This is the ideal case for security and efficiency. The ρ-value that represents how close a given family of curves is to the ideal curve is defined as follow:

Definition 2.4 ([9])**.** Let $t(x), r(x), q(x) \in \mathbb{Q}[x]$, and suppose that $(t(x), r(x), q(x))$ represents a family of elliptic curves with embedding degree k. The ρ-value of the family represented by $(t(x), r(x), q(x))$ is:

$$\rho = \lim_{x \to \infty} \frac{\log(q(x))}{\log(r(x))} = \frac{\deg q(x)}{\deg r(x)}.$$

The Brezing-Weng method [7, 9] is summarized below as Algorithm 1.

Algorithm 1 The Brezing-Weng method

```
INPUT: embedding degree $k$, CM discriminant $D$.
OUTPUT: $t(x), r(x), q(x)$
Choose a number field $K$ containing $\sqrt{-D}$ and a primitive $k$th root of unity $\zeta_k$.
Find an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ such that $\mathbb{Q}[x]/(r(x)) \cong K$.
Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta_k + 1 \in K$.
Let $y(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D} \in K$.
Let $q(x) = (t(x)^2 + Dy(x)^2)/4$. If $q(x)$ and $r(x)$ represent primes,
then output $t(x), r(x), q(x)$.
```

3. New families of pairing-friendly curves with the CM equation of degree 1

Throughout the paper, we denote by ζ_k the primitive kth root of unity for $k \geq 3$.

Proposition 3.1. *Suppose $(q(x), r(x), t(x))$ represents a family of elliptic curve with embedding degree k and $d(x) = 4q(x) - t(x)^2$ has degree 1. Then $r(x)$ has a root θ such that $\theta = a_1(\zeta_k^l - 1)^2 + a_0$, where a_0, a_1 are some rational numbers, a_1 is nonzero and $l \in (\mathbb{Z}/k\mathbb{Z})^*$.*

Proof. Since $q(x) = r(x)\cdot h(x) + t(x) - 1$, we have $d(x) = 4r(x)\cdot h(x) - (t(x)-2)^2$. Let θ be a root of $r(x)$ and $d(x) = b_0 + b_1 x \in \mathbb{Q}[x]$. Note that $r(x)$ is a factor of $\Phi_k(t(x) - 1)$. Hence $\Phi_k(t(\theta) - 1) = 0$ and $t(\theta) = \zeta_k^l + 1$ for some $l \in (\mathbb{Z}/k\mathbb{Z})^*$. We have $b_0 + b_1\theta = d(\theta) = -(\zeta_k^l - 1)^2$. If we set $a_0 = -b_0/b_1$ and $a_1 = -1/b_1$, this finishes the proof. □

By the above proposition, if we want to construct a pairing-friendly elliptic curve such that $d(x) = 4q(x) - t(x)^2$ is linear, we only have to consider $r(x)$ that has the root $\theta = a_1(\zeta_k^l - 1)^2 + a_0$. Note that $r(x)$ is irreducible over $\mathbb{Q}$ and $\theta = \sigma_l(a_1(\zeta_k - 1)^2 + a_0)$ for $\sigma_l \in \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_k)$. Therefore, it is enough to consider the case of $l = 1$. In the following proposition, we propose a method to construct a family of pairing-friendly elliptic curves with embedding degree k from $\theta = a_1(\zeta_k - 1)^2 + a_0$.

Proposition 3.2. *Let $\theta = a_1(\zeta_k - 1)^2 + a_0$, where a_0, a_1 are some rational numbers and a_1 is nonzero. Fix a positive integer k and the kth cyclotomic field $\mathbb{Q}(\zeta_k)$. Execute the following steps.*

(1) *Find an irreducible (but not necessarily monic) polynomial $r(x) \in \mathbb{Z}[x]$ such that $r(\theta) = 0$.*
(2) *Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta_k + 1$ in $\mathbb{Q}(\zeta_k)$.*
(3) *Let $d(x) = -\frac{1}{a_1}x + \frac{a_0}{a_1} \in \mathbb{Q}[x]$.*
(4) *Let $q(x) \in \mathbb{Q}[x]$ be given by $(t(x)^2 + d(x))/4$.*

Suppose $q(x)$ and $r(x)$ represent primes and $t(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$. Then $(t(x), r(x), q(x))$ represents a family of elliptic curves with embedding degree k such that $d(x) = 4q(x) - t(x)^2$ is linear.

Proof. First, we show that the kth cyclotomic field $\mathbb{Q}(\zeta_k)$ is isomorphic to $\mathbb{Q}[x]/(r(x))$. Consider the Galois group of $\mathbb{Q}(\zeta_k)$ over $\mathbb{Q}$, $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_k)$. Then $\sigma_i(\zeta_k) = \zeta_k^i$ for $\sigma_i \in \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_k)$ and $i \in (\mathbb{Z}/k\mathbb{Z})^*$ by Theorem 8.1 in [11]. Since $\theta = a_1(\zeta_k - 1)^2 + a_0$ and $(\sigma_i(\zeta_k) - 1)^2 \neq (\sigma_j(\zeta_k) - 1)^2$ for $i \neq j \in (\mathbb{Z}/k\mathbb{Z})^*$, we have $\sigma_i(\theta) \neq \sigma_j(\theta)$. Thus $r(x)$ must have at least $\varphi(k)$ roots and $\mathbb{Q}(\zeta_k)$ is equal to $\mathbb{Q}(\theta)$ which is isomorphic to $\mathbb{Q}[x]/(r(x))$. Then, it is enough to show that $(q(x), r(x), t(x))$ satisfies the conditions (3) and (4) in Definition 2.3. By Step 2, $r(x)$ divides $\Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial. Note that $x \in \mathbb{Q}[x]$ is a polynomial mapping to $a_1(\zeta_k - 1)^2 + a_0$ in $\mathbb{Q}(\zeta_k)$ because $\theta = a_1(\zeta_k - 1)^2 + a_0$ is the root of $r(x)$. Hence x is equal to $a_1(t(x) - 2)^2 + a_0$ in $\mathbb{Q}[x]/(r(x))$. Let x be $a_1(t(x) - 2)^2 + a_0 + h(x)r(x)$ for some $h(x) \in \mathbb{Q}[x]$. Then, we have

$$\begin{aligned} q(x) &= (t(x)^2 + d(x))/4 = (t(x)^2 - \frac{1}{a_1}x + \frac{a_0}{a_1})/4 \\ &= (t(x)^2 - \frac{1}{a_1}\{a_1(t(x) - 2)^2 + a_0 + h(x)r(x)\} + \frac{a_0}{a_1})/4 \\ &= (t(x)^2 - (t(x) - 2)^2 - \frac{h(x)}{a_1}r(x))/4 \\ &= t(x) - 1 + \widetilde{h(x)}r(x), \end{aligned}$$

where $\widetilde{h(x)} = -\frac{h(x)}{4a_1}$. □

Remark 3.3. Changing a_0, a_1 in the condition of Proposition 3.1 dose not affect the construction of a new pairing-friendly curves such that $d(x) = 4q(x) - t(x)^2$ is linear: θ and θ' obtained by changing a_0, a_1 in the condition of Proposition 3.1 must have the following relation:

$$\theta' = b_1\theta + b_0 \text{ for } b_0, b_1(\neq 0) \in \mathbb{Q}.$$

Therefore, changing a_0, a_1 corresponds to applying an affine change of variable to the polynomials $(q(x), r(x), t(x))$ does not produce anything new.

3.1. Searching for families of curves with $3 \leq k \leq 50$ such that $4q(x) - t(x)^2$ is linear

We searched for families of pairing-friendly curves with $3 \leq k \leq 50$ using Algorithm 2. For any embedding degree k, Algorithm 2 outputs a potential family of elliptic curves with the CM equation of degree 1. But the problem is whether $q(x)$ in Step 6 is an integer-valued polynomial or not. Since $Dy^2 = 4q(x) - t(x)^2$ must have integral solution (x, y) and $q(x), t(x)$ from Algorithm 2 have the relation $4q(x) - t(x)^2 = x$, it is enough to consider the evaluation of $q(x)$ at integers x. If $q(x)$ from Step 5 in Algorithm 2 is not an integer for every

Algorithm 2

```
INPUT: embedding degree $k$, primitive $k$th root of unity $\zeta_k$.
OUTPUT: $q(x), r(x), t(x)$ with embedding degree $k$ such that
$4q(x) - t(x)^2 = x$.
 1: $\theta \leftarrow -(\zeta_k - 1)^2$.
 2: Find an irreducible (but not necessarily monic) polynomial $r(x) \in \mathbb{Z}[x]$
    such that $r(\theta) = 0$.
 3: Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta_k + 1$ in $\mathbb{Q}(\zeta_k)$.
 4: Let $d(x) = x \in \mathbb{Q}[x]$.
 5: $q(x) \leftarrow (t(x)^2 + d(x))/4$.
 6: If $q(x)$ and $r(x)$ represent primes,
 7: then output $t(x), r(x), q(x)$.
```

integer x, then $q_1(x)$ obtained by applying any affine change of variable over $\mathbb{Q}$ to $q(x)$ also cannot represent families of elliptic curves. In this case, there exist no polynomials $(q(x), r(x), t(x))$ representing families of elliptic curves with embedding degree k and the CM equation of degree 1.

The following lemma based on the Chinese Remainder Theorem reduces the complexity to find an integer x such that $q(x)$ is an integer.

Lemma 3.4. *Let $f(x) = \frac{a}{b} \cdot g(x)$ for some $a, b \in \mathbb{Z}$ and $g(x) \in \mathbb{Z}[x]$ where $\gcd(a, b) = 1$. Let b be factorized as $\prod_{i=1}^{n} p_i^{e_i}$ for some prime p_i and positive integer e_i. Then $f(x_0) \in \mathbb{Z}$ for some $x_0 \in \mathbb{Z}$ if and only if there exist some $x_i \in \mathbb{Z}$ with $0 \le x_i < p_i^{e_i}$ such that $g(x_i) \equiv 0 \bmod p_i^{e_i}$ for each $p_i^{e_i}$.*

Remark 3.5. (1) Since $q(x)$ has a positive leading coefficient, so does $q_1(x)$.

(2) In Step 4, if $p_i^{e_i}$ is small, it is efficient to find x_i such that $q_1(x_i) \equiv 0 \bmod p_i^{e_i}$ by the evaluation of $q_1(x)$ at x for $0 \le x < p_i^{e_i}$. However, in case of a large number $p_i^{e_i}$, finding the root x_i of $q_1(x)$ in a finite field $\mathbb{F}_{p_i}$ and then computing $q_1(x_i) \bmod p_i^{e_i}$ may be more efficient.

Theorem 3.6. *Let $K = \{i \in \mathbb{Z} | 3 \le i \le 50\} \backslash \{3, 4, 6, 8, 10, 12, 15, 16, 24, 30, 32, 39, 40, 48\}$. Then there exist polynomials $(q(x), r(x), t(x))$ representing family of elliptic curves with embedding degree k and the CM equation of degree 1 for $k \in K$.*

Proof. In case of $k = 10$, $q(x)$ is reducible. In case of $k \in \{3, 4, 6, 8, 12, 15, 16, 24, 30, 32, 39, 40, 48\}$, $q(x)$ has no integer value. In all other cases, we can obtain $(q(x), r(x), t(x))$ from Algorithm 2 and Algorithm 3. □

Example 3.1 ([14])**.** $k = 5$

$$r = x^4 - 3x^3 + 4x^2 - 12x + 41$$

$$q = (x^6 + 2x^5 + 39x^4 + 78x^3 + 401x^2 + 3785x - 5650)/12100$$

$$t = (x^3 + x^2 + 19x + 20)/55$$

$$\rho = 1.5.$$

When $x \equiv -3 \bmod 220$, $t(x)$ represents integers, $q(x)$ and $\widetilde{r}(x) = r(x)/275$ represent primes. For $x_0 = 220 \cdot 103905194262 - 3$, we find a 252-bit prime $q(x_0)$, a 169-bit prime $\widetilde{r}(x_0)$ and a 9-digit discriminant D.

Other examples can be found in [14].

Algorithm 3

```
INPUT: $q(x), r(x), t(x)$ from Algorithm 2.
OUTPUT: $q(x), r(x), t(x)$ such that $4q(x) - t(x)^2 = ax + b$ for some integer $a, b$.
Let $q(x)$ be $\frac{a_1}{b_1} \cdot q_1(x)$ for $a_1, b_1 \in \mathbb{N}$ and $q_1(x) \in \mathbb{Z}[x]$ where $\gcd(a_1, b_1) = 1$.
if $q(x)$ is irreducible and $a_1 = 1$, then
    let $b_1$ be factorized as $\prod_{i=1}^{n} p_i^{e_i}$ for some prime $p_i$ and positive integer $e_i$.
    find the smallest $x_i \in \mathbb{Z}$ in $0 \leq x_i < p_i^{e_i}$ such that $q_1(x_i) \equiv 0 \bmod p_i^{e_i}$ for each $1 \leq i \leq n$.
    if there exist $x_i$ for all $1 \leq i \leq n$, then
        let $x_0$ be the solution of CRT such that $x_0 \equiv x_i \bmod p_i^{e_i}$ for $1 \leq i \leq n$.
        let $m$ be $\prod_{i=1}^{n} p_i^{e_i}$.
        find the smallest factor $l$ of $m$, such that $q(lx + x_1) \in \mathbb{Z}[x]$ where $x_1 \equiv x_0 \bmod l$.
        let $r(lx + x_1) = e\widetilde{r}(x)$, where $e$ is a constant and $\widetilde{r}(x)$ represent primes,
        output $q(lx + x_1), \widetilde{r}(x), t(lx + x_1)$.
    else
        output "There exist no polynomials"
    end if
else
    output "There exist no polynomials"
end if
```

4. New families of pairing-friendly curves with the CM discriminant of $xf(x)^2$

By Theorem 3.6, we cannot find polynomials $(q(x), r(x), t(x))$ representing family of elliptic curves with embedding degree k and the CM equation of degree 1 for some k such as $k = 8, 16, 24$. In this section, we will show that these examples can be found if we consider the discriminant of the form $xf(x)^2$. For this purpose, Proposition 3.2 can be modified as follows.

Proposition 4.1. *Let ζ_ℓ be the primitive ℓth root of unity, where ℓ is some multiple of k. Suppose α is a non-zero element of $\mathbb{Q}(\zeta_\ell)$ such that $\mathbb{Q}(\theta)$ is equal to $\mathbb{Q}(\zeta_\ell)$ where $\theta = -(\frac{\zeta_k - 1}{\alpha})^2$. Fix a positive integer k and execute the following steps.*

(1) *Find an irreducible (but not necessarily monic) polynomial $r(x) \in \mathbb{Z}[x]$ such that $r(\theta) = 0$ and $\mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$.*

(2) *Let $x \in \mathbb{Q}[x]$ be a polynomial mapping to $-(\frac{\zeta_k - 1}{\alpha})^2$ in $\mathbb{Q}(\zeta_\ell)$.*

(3) *Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta_k + 1$ in $\mathbb{Q}(\zeta_\ell)$.*

(4) *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial mapping to α in $\mathbb{Q}(\zeta_\ell)$.*

(5) *Let $q(x) \in \mathbb{Q}[x]$ be given by $(t(x)^2 + xf(x)^2)/4$.*

Suppose $q(x)$ and $r(x)$ represent primes and $t(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$. Then $(t(x), r(x), q(x))$ represents a family of elliptic curves with embedding degree k such that $4q(x) - t(x)^2 = xf(x)^2$.

Proof. We show that $(q(x), r(x), t(x))$ satisfies the condition (3) in Definition 2.3. By Step (2), Step (3) and Step (4), x is equal to $-((t(x) - 2)/f(x))^2$ in $\mathbb{Q}[x]/(r(x))$. Let $xf(x)^2$ be $-(t(x)-2)^2 + h(x)r(x)$ for some $h(x) \in \mathbb{Q}[x]$. Then we have

$$\begin{aligned} q(x) &= (t(x)^2 + xf(x)^2)/4 \\ &= (t(x)^2 - (t(x) - 2)^2 + h(x)r(x))/4 \\ &= t(x) - 1 + \widetilde{h(x)}r(x), \end{aligned}$$

where $\widetilde{h(x)} = -\frac{h(x)}{4a_1}$. The remaining parts of the proof are the same as those of Proposition 3.1.

□

Remark 4.2. (1) If $\alpha = 1$ and $\ell = k$, then Proposition 4.1 is the same as Proposition 3.1.

(2) Note that ℓ can be a multiple of k. By selecting α in $\mathbb{Q}(\zeta_\ell)$, it is possible for $\mathbb{Q}(\theta)$ to be equal to $\mathbb{Q}(\zeta_\ell)$. This is a big difference from Proposition 3.1.

(3) As in Remark 3.3, a family of curves with the CM equation $4q_1(x) - t_1(x)^2 = (ax+b)f_1(x)^2$ can be constructed via applying affine change of variable to $q(x), r(x), t(x)$ such that $4q(x) - t(x)^2 = xf(x)^2$.

(4) Let α be a nonzero element of $\mathbb{Q}(\zeta_\ell)$. Then $\mathbb{Q}(-(\frac{\zeta_k - 1}{\alpha})^2)$ is equal to $\mathbb{Q}(\zeta_\ell)$ if and only if $\pm\frac{\sigma_i(\alpha)}{\alpha} \neq \frac{\sigma_i(\zeta_k)-1}{\zeta_k - 1}$ for all $\sigma_i \in \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_\ell)$.

4.1. Examples

In Algorithm 4, it is difficult to predetermine θ for producing good results. For a suitable selection of θ, we performed an exhaustive search through all coefficients between -3 and 3 that will appear in the representation of α or $(\zeta_k - 1)/\alpha$ by the basis $\{1, \zeta_k, \ldots, \zeta_k^{\varphi(k)-1}\}$ of $\mathbb{Q}(\zeta_k)$. In the search, we chose θ that gave the minimal difference between the first x_0 and the second x_1 such that $q(x_i)$ is an integer for $x_i \in \mathbb{N}$. But we cannot conclude that these are the best results.

Example 4.1. $k = 8$

$\alpha = 2\zeta_k^3 - \zeta_k^2 - \zeta_k + 2$

$r = x^4 + 34x^2 + 1$

$q = (49x^7 + 51x^6 + 3349x^5 + 3415x^4 + 57559x^3 + 57109x^2 + 11187x + 49)/2304$

Algorithm 4

```
INPUT: embedding degree $k$, primitive $k$th($\ell$th) root of unity $\zeta_k(\zeta_\ell)$ for some multiple $\ell$ of $k$.
OUTPUT: $t(x), r(x), q(x)$
Repeat
Choose a random nonzero element $\alpha \in \mathbb{Q}(\zeta_\ell)$.
Until $\pm\frac{\sigma_i(\alpha)}{\alpha} \neq \frac{\sigma_i(\zeta_k)-1}{\zeta_k-1}$ for all $\sigma_i \in \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_\ell)$.
$\theta \leftarrow -((\zeta_k - 1)/\alpha)^2$.
Find an irreducible (but not necessarily monic) polynomial $r(x) \in \mathbb{Z}[x]$
  such that $r(\theta) = 0$ and $\mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$.
Let $x \in \mathbb{Q}[x]$ be a polynomial mapping to $-(\frac{\zeta_k-1}{\alpha})^2$ in $\mathbb{Q}(\zeta_\ell)$.
Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta_k + 1$ in $\mathbb{Q}(\zeta_\ell)$.
Let $f(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\alpha$ in $\mathbb{Q}(\zeta_\ell)$.
$q(x) \leftarrow (t(x)^2 + xf(x)^2)/4$.
If $q(x)$ is irreducible and $q(x_0), t(x_0)$ are integers for some $x_0 \in \mathbb{Z}$,
then output $t(x), r(x), q(x)$.
```

$$t = (3x^3 - x^2 + 99x + 7)/24$$
$$\rho = 1.75.$$

When $x \equiv c \bmod 12$, where $c = 7, 11$, $t(x)$ represents integers, $q(x)$ and $\widetilde{r}(x) = r(x)/6^2$ represent primes.

Example 4.2. $k = 16$

$$\begin{aligned}
\alpha &= \zeta_k^4 - 2\zeta_k^3 + 2\zeta_k^2 - \zeta_k \\
r &= x^8 + 332x^6 + 678x^4 + 76x^2 + 1 \\
q &= (117310561x^{15} + 39039455x^{14} + 77892835753x^{13} + 25919226855x^{12} \\
&\quad + 13088598379413x^{11} + 4354049399243x^{10} + 52676581062573x^9 \\
&\quad + 17249623655107x^8 + 59240325856323x^7 + 18576763413053x^6 \\
&\quad + 11456416399483x^5 + 2590174825717x^4 + 621744760071x^3 \\
&\quad + 91546735321x^2 + 4130262255x + 113569)/928055296 \\
t &= (-1673x^7 - 131x^6 - 555345x^5 - 43523x^4 - 1104075x^3 \\
&\quad - 99081x^2 - 63931x - 337)/15232 \\
\rho &= 1.875.
\end{aligned}$$

When $x \equiv c \bmod 2^2{\cdot}17{\cdot}7$, where $c = 67, 87, 115, 123, 151, 171, 291, 319, 339, 375, 395, 423$, $q(x), t(x)$ represents integers, $q(x)$ and $\widetilde{r}(x)$ represent primes, where

$$\widetilde{r}(x) = \begin{cases} r(x)/(2^6 \cdot 7^2 \cdot 17) & c = 67, 115, 123, 171, 319, 339, 375, 395, \\ r(x)/(2^6 \cdot 7^2 \cdot 17^2) & c = 87, 151, 291, 423. \end{cases}$$

Example 4.3. $k = 20$

$$\begin{aligned}
\alpha &= -\zeta_k^4 + \zeta_k^3 - \zeta_k^2 \\
r &= x^8 + 716x^6 + 486x^4 + 76x^2 + 1 \\
q &= (1879641x^{15} + 1012474x^{14} + 2691199323x^{13} + 1449408872x^{12} \\
&\quad + 964796804001x^{11} + 519385215086x^{10} + 1079147931643x^9 \\
&\quad + 471940038900x^8 + 374562480771x^7 + 136911017622x^6 \\
&\quad + 35030676649x^5 + 16607083680x^4 - 2271180669x^3 + 1912901570x^2 \\
&\quad - 322130687x + 129367876)/110166016 \\
t &= (-13x^7 + 93x^6 - 9337x^5 + 66581x^4 - 27071x^3 \\
&\quad + 40183x^2 - 7131x + 5687)/2624 \\
\rho &= 1.875.
\end{aligned}$$

When $x \equiv c \bmod 2 \cdot 41$, where $c = 31, 33, 39, 43, 49, 51$, $t(x)$ represents integers, $q(x)$ and $\widetilde{r}(x)$ represent primes, where

$$\widetilde{r}(x) = \begin{cases} r(x)/(2^8 \cdot 41^2) & c = 31, 51, \\ r(x)/(2^8 \cdot 41) & c = 33, 39, 43, 49. \end{cases}$$

Example 4.4. $k = 24$

$$\begin{aligned}
\alpha &= 2\zeta_k^7 - 2\zeta_k^6 - 2\zeta_k^5 + 2\zeta_k^3 + 2\zeta_k^2 - \zeta_k - 1 \\
r &= 50625x^8 - 48600x^7 + 129564x^6 - 39528x^5 + 4870x^4 + 13592x^3 \\
&\quad + 2460x^2 - 88x + 1 \\
q &= (27542461768326562500x^{15} - 47364507274264734375x^{14} \\
&\quad + 15601306111455142125 0x^{13} - 145508290162914512925x^{12} \\
&\quad + 192756685714928626176x^{11} - 56558367114155802783x^{10} \\
&\quad + 7795297932034415 58x^9 + 33827583641994995427x^8 \\
&\quad + 20595017423351059 72x^7 - 1557154304712471869x^6 \\
&\quad + 2114008998248547438x^5 + 1156974973788911617x^4 \\
&\quad + 196711255882533064x^3 + 10082489228030595x^2 \\
&\quad - 32616400227974x + 54012084025)/4261681299456 \\
t &= (1720794375x^7 - 1633079475x^6 + 4393526499x^5 - 1303164351x^4 \\
&\quad + 171245365x^3 + 455207175x^2 + 90977697x - 232405)/1032192 \\
\rho &= 1.875.
\end{aligned}$$

When $x \equiv c \bmod 2^2 \cdot 3 \cdot 7$, where $c = 31, 43, 55$, $t(x)$ represents integers, $q(x)$ and $\widetilde{r}(x)$ represent primes, where

$$\widetilde{r}(x) = \begin{cases} r(x)/(2^{16} \cdot 3^2 \cdot 7^2) & c = 31, 43, \\ r(x)/(2^{16} \cdot 3^2) & c = 55. \end{cases}$$

We also found $(q(x), r(x), t(x))$ representing a family of pairing-friendly curves with embedding degree $k \in \{32, 40, 48\}$ such that $4q(x) - t(x)^2 = xf(x)^2$. These curves had $\rho = 31/16$. We chose $\alpha = -\zeta_k^6$, ζ_k^{10}, ζ_k for $k = 32, 40, 48$, respectively. However, $q(x) \in \mathbb{Z}[x]$ had a large coefficient. For example, $q(1)$'s values were a 2654, 2664, 2764 bits numbers for $k = 32, 40, 48$, respectively.

4.2. A variable discriminant

To construct curves using the CM method, we need the CM discriminant D, which must be less than approximately 10^{13} for practical reasons. We can obtain D from the square-free part of the CM equation. There is an another approach to obtain a proper CM discriminant D. Since the curves from the proposed method have the CM discriminant $d(x) = ax + b$ ignoring square part, we choose some D and make the substitution $x \mapsto \frac{Dx^2 - b}{a}$ in $(q(x), r(x), t(x))$. Then, the discriminant become $d(x) = Dx^2$. In this approach, the selection of D is restricted: Given $a, b \in \mathbb{Z}$, D must be chosen such that the following equation has a solution.

$$Dx^2 \equiv b \bmod a.$$

Let x_0 be the solution of the above equation. Then we apply the substitution, $x \mapsto \frac{D(ax + x_0)^2 - b}{a}$, to $(q(x), r(x), t(x))$.

Algorithm 5

```
INPUT: Embedding degree $k$.
OUTPUT: $t(x), r(x), q(x) \in \mathbb{Z}[x]$ such that $4q(x) - t(x)^2 = Df(x)^2$ for some $D \in \mathbb{Z}$ and $f(x) \in \mathbb{Z}[x]$.
$q(x), r(x), t(x) \leftarrow$ Algorithm 2 or Algorithm 4.
$q_1(x), r_1(x), t_1(x) \leftarrow$ Algorithm 3$(q(x), r(x), t(x))$.
Let $4q_1(x) - t_1(x)^2 = (ax + b)f(x)^2$.
Find $D, x_0 \in \mathbb{Z}$ such that $Dx_0^2 \equiv b \bmod a$.
Let $s(x)$ be $\frac{D(ax+x_0)^2 - b}{a}$.
Let $q_2(x) = q_1(s(x)), r_2(x) = r_1(s(x)), t_2(x) = t_1(s(x))$.
If $q_2(x), \widetilde{r_2}(x)$ represent prime, where $r_2(x) = e\widetilde{r_2}(x)$ for some constant $e$,
then output $q_2(x), \widetilde{r_2}(x), t_2(x)$.
```

After this substitution, if $q(x)$ represents prime, then (q, r, t) represents a family of pairing-friendly curves with the discriminant D.

5. Conclusion

A family of pairing-friendly curves with the CM equation of degree 1 is completely classified, and families of curves with embedding degree $3 \leq k \leq 50$ are presented. A new algorithm that can be used to construct a family of pairing-friendly curves with the CM discriminant of $xf(x)^2$ is proposed. Using this algorithm, new families of curves with variable discriminants and embedding degree $k \in \{8, 16, 20, 24\}$ have been presented.

References

[1] R. M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, Sydney, 2006.

[2] R. Balasubramanian and N. Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Cryptology **11** (1998), no. 2, 141–145.

[3] P. S. L. M. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, Proceedings of SAC 2005-Workshop on Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 3897, pp 319-331, Springer-Verlag, 2006.

[4] D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing. Advances in Cryptography*, Proceedings of Crypto 2001, Lecture Notes in Computer Science, Vol. 2139, pp. 213-229, Springer-Verlag, 2001.

[5] D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, Advances in Cryptology: Proceedings of Asiacrypt 2001, Lecture Notes in Computer Science, Vol. 2248, pp. 514–532, Springer-Verlag, 2002.

[6] W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[7] F. Brezing and A. Weng, *Elliptic curves suitable for pairing based cryptography*, Des. Codes Cryptogr. **37** (2005), no. 1, 133–141.

[8] D. Freeman, *Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10*, Algorithmic Number Theory Symposium ANTS-VII, Lecture Notes in Computer Science, Vol. 4076, pp. 452-465, Springer-Verlag, 2006.

[9] D. Freeman, M. Scott, and E. Teske, *A taxonomy of pairing-friendly elliptic curves*, J. Cryptology **23** (2010), no. 2, 224–280.

[10] S. Galbraith, J. McKee, and P. Valenca, *Ordinary abelian varieties having small embedding degree*, Finite Fields Appl. **13** (2007), no. 4, 800–814.

[11] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, Vol. 73, Springer, Heidelberg, 1996.

[12] A. Joux, *A one round protocol for tripartite Diffie-Hellman*, Proceedings of Algorithmic Number Theory Symposium, ANTS-IV, Lecture Notes in Computer Science, Vol. 1838, pp. 385–394, Springer-Verlag, 2000.

[13] E. Kachisa, E. Schaefer, and M. Scott, *Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field*, Pairing-based cryptography–Pairing 2008, 126–135, Lecture Notes in Comput. Sci., 5209, Springer, Berlin, 2008.

[14] H.-S. Lee and C.-M. Park, *Generating pairing-friendly curves with the CM equation of degree 1*, Pairing 2009, vol. 5671, Lecture Notes in Computer Science, page 66–77, Springer-Verlag, 2009.

[15] R. Sakai, K. Ohgishi and M. Kasahara, *Cryptosystems based on pairing*, The 2000 Symposium on Cryptography and Information Security(SCIS 2000), 2000.

[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, Germany, 1986.

[17] A. V. Sutherland, *Computing Hilbert class polynomials with the Chinese Remainder Theorem*, Math. Comp. **80** (2011), no. 273, 501–538.

Hyang-Sook Lee
Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea
E-mail address: hsl@ewha.ac.kr

Cheol-Min Park
Institute of Mathematical Sciences
Ewha Womans University
Seoul 120-750, Korea
Current Address
National Institute for Mathematical Sciences
Daejeon 305-811, Korea
E-mail address: mpcm@ewha.ac.kr, mpcm@nims.re.kr