Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/100218

Families of Pairing-Friendly Elliptic Curves from a Polynomial Modification of the Dupont-Enge-Morain Method

Hyang-Sook Lee[*] *and Pa-Ra Lee*[*]

Department of Mathematics, Ewha Womans University, Seoul, South Korea

Received: 5 Sep. 2014, Revised: 1 May 2015, Accepted: 12 Jun. 2015
Published online: 1 Mar. 2016

Abstract: A general method for constructing families of pairing-friendly elliptic curves is the Brezing-Weng method. In many cases, the Brezing-Weng method generates curves with discriminant $D = 1$ or 3 and restricts the form of $r(x)$ to be a cyclotomic polynomial. However, since we desire a greater degree of randomness on curve parameters to maximize security, there have been studies to develop algorithms that are applicable for almost arbitrary values of D and more various forms of $r(x)$. In this paper, we suggest a new method to construct families of pairing-friendly elliptic curves with variable D and no restriction on the form of $r(x)$ for arbitrary k by extending and modifying the Dupont-Enge-Morain method. As a result, we obtain complete families of curves with improved ρ-values for $k = 8, 12, 16, 20$ and 24. We present the algorithm and some examples of our construction.

Keywords: Pairing-friendly elliptic curves, Complete families, Dupont-Enge-Morain method

1 Introduction

Pairings have been crucial primitives for a number of novel and functional cryptographic schemes such as one round tripartite key-exchange [16], identity-based encryption [5], short signatures [6] etc. Up to now, several efficient pairings have been suggested such as the Eta$_T$ pairing [2], the Ate pairing [14], the Ate$_i$ pairing [26], the R-ate pairing [19] and the optimal ate pairing [25]. Since all these pairings are usually defined on elliptic curves over finite fields, it is important to construct suitable elliptic curves in order to build an efficient pairing-based system for all kinds of applications as well as for all desired levels of security. Freeman, Scott and Teske [12] called such an elliptic curve E over a finite field $\mathbb{F}_q$, where q is a prime or a prime power, as a *pairing-friendly* curve which has a large prime factor r of the order of the elliptic curve group $E(\mathbb{F}_q)$ and a small embedding degree k with respect to r. Here, the embedding degree k is defined as the smallest integer such that r divides $q^k - 1$.

To construct a pairing-friendly elliptic curve E over a finite field $\mathbb{F}_q$, we usually follow two common steps. The first step is to look for suitable values for curve parameters (t, r, q) where q is the size of the finite field, r is the prime subgroup order and t is the trace of the Frobenius endomorphism of the curve. The second step is to find the equation of E which is usually done by the Complex Multiplication(CM) method [1]. Considering the current computational power, the method is valid when a CM discriminant D defined by a positive square-free part of $4q - t^2$ is less than 10^{15} [24]. For secure cryptographic schemes based on pairings on elliptic curves, we consider two values, namely, the ratio ρ of the size of the base field relative to that of the prime-order subgroup on the curve and the embedding degree k. When k is given, curves with smaller ρ-values are often more desirable to speed up the arithmetic on the elliptic curves.

The Cocks-Pinch method [8] and the Dupont-Enge-Morain method [10] are well-known methods that generate pairing-friendly ordinary elliptic curves with $\rho \approx 2$ for arbitrary embedding degrees. These methods produce individual curves that do not belong to a type of a *family* where the curve parameters are represented by polynomials. For the parameters in polynomials, we define the rho-value as $\rho = \frac{degree\ of\ q(x)}{degree\ of\ r(x)}$. The Cocks-Pinch method has been generalized to the more efficient method, due to Brezing and Weng [7], that

[*] Corresponding author e-mail: hsl@ewha.ac.kr, paraleeprl@gmail.com

provides curve parameters in polynomial types for ordinary elliptic curves with $\rho < 2$. However, the Dupont-Enge-Morain method has yet to be generalized to produce families of curves with significantly improved ρ-values. In this paper, we extend and modify the Dupont-Enge-Morain method and contribute to overcoming its downside regarding ρ-values.

Families of elliptic curves are classified into complete families and sparse families depending on the existence of $y(x) \in \mathbb{Q}[x]$ satisfying the equation $Dy(x)^2 = 4q(x) - t(x)^2$ which is called *CM equation*. If there exists such a $y(x)$, then we say that the family is complete. Otherwise, we define the family as a sparse family [12]. When we construct elliptic curves via the CM method, complete families are more efficient than sparse families in obtaining elliptic curves because generating elliptic curves from sparse families involves transformations on the CM equation into a generalized Pell equation for finding solutions (x,y) satisfying $Dy^2 = 4q(x) - t(x)^2$. Because of the inefficiency, we prefer complete families to sparse families to construct elliptic curves.

A general approach for constructing complete families of ordinary elliptic curves is the Brezing-Weng method [7]. The method provides a bulk of existing constructions for ordinary curves with various embedding degrees. However, it restricts $r(x)$ to be a cyclotomic polynomial and mostly deals with a small CM discriminant D such as $D = 1$ or 3. Thus there have been studies to overcome such limits on the Brezing-Weng construction. First, Barreto and Naehrig [3] applied the work, due to Galbraith, McKee and Valenca [13], on factorizations of k-th cyclotomic polynomial $\Phi_k(u(x))$ for some quadratic polynomials $u(x)$ in $\mathbb{Z}[x]$ and $k \in \{5,8,10,12\}$ to the Brezing-Weng method for generating a complete family of pairing-friendly elliptic curves which have a non-cyclotomic polynomial $r(x)$ for $k = 12$ and $D = 3$. The curves are called *BN curves*, which is the only currently-known complete family of elliptic curves with $\rho = 1$. After, Kachisa, Schaefer and Scott [17] suggested a curve construction method with a non-cyclotomic polynomial $r(x)$, which can be computed as the minimal polynomial of a randomly chosen element of $\mathbb{Q}(\zeta_l)$, where ζ_l is a primitive l-th root of unity in $K = \mathbb{Q}[x]/(r(x))$.

Next, for security reason, some methods with various discriminants D have been suggested which are also based on the Brezing-Weng method ([4], [9], [12], [20], [21] etc.). For example, Freeman, Scott and Teske [12] suggested families of curves with a variable discriminant by substituting x with Dx^2 on the existing Brezing-Weng construction. However, because these families preserved the ρ-values, the method could not provide improvements on ρ-values.

On the other hand, Scott and Barreto [23] proposed an algorithm to remove the restrictions on $r(x)$ and D which does not rely on the Brezing-Weng method but it is computationally inefficient due to its exhaustive searching step for the suitable values for curve parameters.

In this paper, we present a new construction of pairing-friendly ordinary elliptic curves by extending and modifying the Dupont-Enge-Morain method. Our new method enables to derive families having various polynomials $r(x)$, and it also produces the curve parameters for variable discriminants D without an assumption that a field K contains a square root of a given $-D$, which is required for the Brezing-Weng method.

As a result, our construction provides complete families for $k = 8, 12, 16, 20$ and 24 with improved ρ-values. These improvements compared to the known best results are given in Table 1.

The paper is organized as follows. In Section 2, we review basic definitions and properties related to the construction of pairing-friendly elliptic curves. We propose a new approach to construct families of curves by extending and modifying the Dupont-Enge-Morain method in Section 3. We provide examples of curves constructed by our new method in Section 4. Finally, we draw conclusions in Section 5.

2 Preliminaries

In this section, we review basic definitions, properties and some well-known methods for constructing pairing-friendly elliptic curves. Refer to the paper [12] for further details.

Let E be an elliptic curve defined over a prime field $\mathbb{F}_q$ and r be a large prime number which divides the order of $E(\mathbb{F}_q)$. A pairing-friendly curve is formally defined as follows.

Definition 1([12], Def.2.3). *Suppose E is an elliptic curve defined over a finite field $\mathbb{F}_q$. We say that E is pairing-friendly if the following two conditions hold:*

(1) there is a prime $r \geq \sqrt{q}$ dividing the order of $E(\mathbb{F}_q)$, and

(2) the embedding degree k of E with respect to r is less than $\frac{1}{8}\log_2 r$.

Such pairing-friendly ordinary elliptic curves can be constructed if and only if the following conditions hold:

(C1) q is a prime or a prime power.
(C2) r is a prime.
(C3) t is relatively prime to q.
(C4) r divides $q + 1 - t$
(C5) $r | q^k - 1$ and $r \nmid q^i - 1$ for $1 \leq i < k$.
(C6) $Dy^2 = 4q - t^2$ for some sufficiently small positive integer D and some integer y.

Now we recall two typical algorithms, due to Cocks-Pinch and Dupont-Enge-Morain, to generate individual pairing-friendly elliptic curves that take constant parameters (t,r,q) satisfying the above six conditions. In other words, both the Cocks-Pinch algorithm and the Dupont-Enge-Morain algorithm gives elliptic curves not in families.

Algorithm 1 Cocks-Pinch method [8]

```
Input: a positive integer $k$, a positive square-free integer $D < 10^{15}$
Output: $t$, $r$, $q$
Let $r$ be a prime such that $k|r-1$ and $(\frac{-D}{r}) = 1$.
Let $z$ be a $k$-th primitive root of unity in $\mathbb{Z}/r\mathbb{Z}$.
Let $t_0 = z+1$.
Let $y_0 = \frac{(t_0-2)}{\sqrt{-D}} \pmod{r}$.
Choose $t,y \in \mathbb{Z}$ such that $t \equiv t_0 \bmod r$ and $y \equiv y_0 \bmod r$.
Let $q = \frac{1}{4}(t^2+Dy^2)$ . If $q$ is a prime, then return $t,r,q$.
```

Dupont *et al* used the following property to determine r that satisfies the three conditions (C4), (C5) and (C6) simultaneously.

Lemma 1([18], Corollary IV 8.4). *Let $f(x),g(x)$ be polynomials in a field K. Then $f(x)$ and $g(x)$ have a common zero in $\bar{K}$ if and only if $Res_x(f(x),g(x)) = 0$.*

Algorithm 2 Dupont-Enge-Morain method [10]

```
Input: a positive integer $k$
Output: $t$, $r$, $q$
Compute the resultant $R(a) = \mathrm{Res}_x(\Phi_k(x-1), a+(x-2)^2) \in \mathbb{Z}[a]$.
Choose $a \in \mathbb{Z}$ of the form $Dy^2$ with a positive square-free integer $D \leq 10^{15}$ such that $R(a)$ is a prime.
Set $r = R(a)$.
Compute $g(x) = \mathrm{GCD}(\Phi_k(x-1), a+(x-2)^2)$ in $\mathbb{F}_r[x]$.
Let $t_0 \in \mathbb{F}_r$ be a root of the polynomial $g(x)$.
Let $t \in \mathbb{Z}$ such that $t \equiv t_0 \pmod{r}$.
Let $q = \frac{1}{4}(t^2+Dy^2)$. If $q$ is a prime, then return $t,r,q$.
```

Both methods produce individual curves with $\rho \approx 2$ for arbitrary embedding degrees. Brezing-Weng [7] generalizes the Cocks-Pinch method whereby the unknowns (t,r,q) live in the ring of polynomials with rational coefficients instead of in the ring of integers with $\rho < 2$.

To extend constant curve parameters to polynomial types, we give the definition of polynomials representing primes.

Definition 2([12], Def.2.5). *Let $f(x)$ be a polynomial with rational coefficients. We say f represents 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 $x \in \mathbb{Z}$, and
(5) $gcd(f(x) : x, f(x) \in \mathbb{Z}) = 1$.

Definition 3([12], Def.2.6). *A polynomial $f(x) \in \mathbb{Q}[x]$ is integer-valued if $f(x) \in \mathbb{Z}$ for every $x \in \mathbb{Z}$.*

Next we define families of pairing-friendly curves.

Definition 4([12], Def.2.7). *Let $t(x), r(x)$, and $q(x)$ be nonzero polynomials with rational coefficients.*

(i) For a given positive integer k and a positive square-free integer D, the triple (t,r,q) parameterizes a family of elliptic curves with embedding degree k and discriminant D if the following conditions are satisfied:

(1) $q(x) = p(x)^m$ for some $m \geq 1$ and $p(x)$ that represents primes,
(2) $r(x)$ is non-constant, irreducible, integer-valued, and has a positive leading coefficient,
(3) $r(x)$ divides $q(x)+1-t(x)$,
(4) $r(x)$ divides $\Phi_k(t(x)-1)$, where Φ_k is the k^{th} cyclotomic polynomial,
(5) the CM equation $Dy^2 = 4q(x)-t(x)^2$ has infinitely many integer solutions (x,y).

If these conditions are satisfied, we refer to the triple $(t(x),r(x),q(x))$ as a family.

(ii) For $(t(x),r(x),q(x))$ as in (i), if x_0 is an integer and E is an elliptic curve over $\mathbb{F}_{q(x_0)}$ with the trace $t(x_0)$, then we say E is a curve in the family $(t(x),r(x),q(x))$.

(iii) We say that a family $(t(x),r(x),q(x))$ is ordinary if $gcd(t(x),q(x)) = 1$.

(iv) We say that a family $(t(x),r(x),q(x))$ is complete if there is some $y(x) \in \mathbb{Q}[x]$ such that $Dy(x)^2 = 4q(x)-t(x)^2$; otherwise we say that the family is sparse.

Now, we recall the Brezing-Weng method. The output $(t(x),r(x),q(x))$ parameterizes a complete family of elliptic curves for a given embedding degree k and a fixed discriminant D.

Algorithm 3 Brezing-Weng method [7]

```
Input: a positive integer $k$, a positive square-free integer $D < 10^{15}$
Output: $t(x)$, $r(x)$, $q(x)$ in $\mathbb{Q}[x]$
Find an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ with a positive leading coefficient such that $K = \mathbb{Q}[x]/(r(x))$ is a number field containing $\sqrt{-D}$ and the cyclotomic field $\mathbb{Q}(\zeta^k)$.
Choose a primitive $k^{th}$ root of unity $\zeta_k \in K$.
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 $\frac{(\zeta_k-1)}{\sqrt{-D}}$ in $K$.
(So if $\sqrt{-D} \mapsto s(x)$, then $y(x) \equiv -\frac{1}{D}(t(x)-2)s(x) \bmod r(x)$).
Let $q(x) \in \mathbb{Q}[x]$ be given by $\frac{1}{4}(t(x)^2+Dy(x)^2)$.
If $q(x)$ represents prime and $y(x_0) \in \mathbb{Z}$ for some $x_0 \in \mathbb{Z}$, then return $t(x), r(x), q(x)$.
```

The Brezing-Weng method places some restrictions on the selection of $r(x)$. One is that $r(x)$ is only considered to be in a cyclotomic polynomial form. The other is the assumption that the number field $K = \mathbb{Q}[x]/(r(x))$ contains $\sqrt{-D}$. Scott and Barreto proposed an algorithm to improve the restrictions by adopting a cofactor polynomial $h(x)$ and exhaustive searching suitable values for variables $(h'_0, h'_1, \ldots, h'_n, d)$.

Algorithm 4 Scott-Barreto method [23]

```
Input: a positive integer $k$
Output: $h(x), t(x), r(x), q(x)$ in $\mathbb{Q}[x]$
Choose a polynomial $t(x)$ such that $\Phi_k(t(x)-1)$ has a suitable irreducible factor $r(x)$ satisfying Definition 4 $(i)(2)$.
Write $h^{'}(x) = h'{}_0 + h'_1 x + h'_2 x^2 + \ldots + h'_n x^n$ for a small $n \in \mathbb{Z}$
    Use an exhaustive search over the variables $(h'_0, h'_1, \ldots, h'_n, d)$
    until $d(t(x)-2)^2 - 4h'(x)r(x)$ is a perfect square.
Compute $h(x) = \frac{h'(x)}{d}, D \in \mathbb{Z}$ the square-free part of $d$.
Set $q(x) = h(x)r(x) + t(x) - 1$ and $y(x) = \frac{\sqrt{(d(t(x)-2)^2 - 4h'(x)r(x)}}{D}$.
    If $q(x)$ represents prime, then return $t(x), r(x), q(x)$.
```

Similar to Scott-Barreto method, we provide a new algorithm to generate families of elliptic curves with various $r(x)$ and CM discriminants D by adopting variables (c_0, c_1, c_2, D) in a modification of the Dupont-Enge-Morain method. However, our method does not need exhaustive searching steps to obtain a suitable irreducible factor $r(x)$ of $\Phi_k(t(x)-1)$ and suitable values of (c_0, c_1, c_2, D). Now, we recall the following lemmas and the definitions, which will be used in our new proposed method in Section 3.

Lemma 2([11], Lemma 5.1). *Fix k. Let $t(x)$ be a polynomial and $r(x)$ be an irreducible factor of $\Phi_k(t(x)-1)$. Then the degree of $r(x)$ is a multiple of $\varphi(k)$, where φ is the Euler phi function.*

Definition 5([15], Definition V 4.4). *Let K be a field with $\mathrm{char} K \neq 2$ and $f(x) \in K[x]$ a polynomial of degree n with n distinct roots $u_1, \ldots, u_n$ in some splitting field $\mathbb{F}$ of $f(x)$ over K. Let $\triangle = \prod(u_i - u_j)$ for $i < j$. Then the discriminant of f is defined as $\mathrm{disc}(f) = \triangle^2$.*

Lemma 3([12], Prop.6.22). *Let $f(x) = \sum a_i x^i \in \mathbb{Z}[x]$, $i = 1, \cdots, n$, be irreducible. Let α be a square-free integer such that $\alpha \nmid a_0 a_n \mathrm{disc}(f)$. Then $f(\alpha x^2)$ is irreducible.*

3 Main Algorithm

Most of previous works for constructing complete families of pairing-friendly curves are based on the Brezing-Weng method. However we propose a new method that produces complete families of ordinary elliptic curves having various $r(x)$ and D, which is built on the Dupont-Enge-Morain method with polynomial curve parameters. Furthermore, our construction gives better ρ-values less than 2 for arbitrary k.

If we try to extend the original Dupont-Enge-Morain method by simply substituting constant parameters with polynomial ones, then we face a difficulty as to how to choose the input polynomial $y(x)$ for achieving a small ρ-value since a ρ-value is automatically determined by the output $t(x)$ corresponding to the input $y(x)$. To solve this problem, we express the input polynomial $y(x)$ as a linear combination of $t(x)$, x, and variables c_i's, where c_i's are chosen as some proper rational numbers which reduce the degree of the output $t(x)$ for a smaller ρ-value. Note that the parameter $t(x)$ in Definition 4 is replaced with $u(x)+1$ in our algorithm.

With this construction, one can compute a number of well-known non-cyclotomic curves including BN curves [3] and Scott-Barreto curves [23] without exhaustive efforts. Moreover, if one sets $Dy(x)^2$ as a linear combination of $t(x)$, x, and variables c_i's, then the sparse families such as MNT curves [22] and Freeman curves [11] are also obtained easily.

Now, we start from several notations for simplicity in the description of our method.

Notation Let $f(x,y)$ and $g(x,y)$ be multivariate polynomials with variables x, y and rational coefficients.

$\deg_x f(x,y)$
:= the degree of $f(x,y)$ with respect to the variable x,

$\mathrm{Res}_x(f(x,y), g(x,y))$
:= the resultant of $f(x,y)$ and $g(x,y)$ with respect to the variable x,

$f(x,y) \bmod_x g(x,y)$
:= the residue of $f(x,y)$ with respect to $g(x,y)$ as a polynomial in x.

From now we describe how to produce polynomials $(t(x), r(x), q(x))$ for the goal of achieving various $r(x)$ and D in our construction. For a fixed embedding degree k, the starting point of our method is the setting of $y(x,u)$ as $c_2 u + c_1 x + c_0 \in \mathbb{Q}[x,u]$. From Definition 4 (i) (3), (4) and (5), we find $r(x)$ satisfying both congruent equations $(u-1)^2 + Dy(x,u)^2 \equiv 0$ and $\Phi_k(u) \equiv 0$ for mod $r(x)$ using the property of the resultant. We compute the resultant of $(u-1)^2 + Dy(x,u)^2$ and $\Phi_k(u)$ with respect to u, and set it to be $R(x)$ in $\mathbb{Q}[x]$. By Lemma 1, both $(u-1)^2 + Dy(x,u)^2$ and $\Phi_k(u)$ should be congruent to 0 $\mathrm{mod}_x R(x)$. Hence we need to compute u so that the both equations are congruent to 0 $\mathrm{mod}_x R(x)$. Here, since there is no u-term in $R(x)$, from the former modular equation,

$$\begin{aligned}
&(u-1)^2 + Dy(x,u)^2 \\
&= (Dc_2^2+1)u^2 + 2(Dc_2c_1x + Dc_2c_0 - 1)u \\
&\quad + \ (Dc_1^2x^2 + 2Dc_1c_0x + Dc_0^2 + 1) \\
&\equiv 0 \ \mathrm{mod}_x R(x),
\end{aligned}$$

and we can derive the following relation

$$u^2 \equiv -\frac{1}{(Dc_2^2+1)}\{2(Dc_2c_1x+Dc_2c_0-1)u \\ +(Dc_1^2x^2+2Dc_1c_0x+Dc_0^2+1)\} \ \ \mathrm{mod}_x R(x).$$

Then we reduce the later modular equation, the k^{th} cyclotomic polynomial of degree $\phi(k)$ expressed in u terms, to the linear form of u as follows,

$$\Phi_k(u) \equiv G(x)u+H(x) \ \mathrm{mod}_u((u-1)^2+Dy(x,u)^2).$$

Since $\Phi_k(u)$ should be divided by $R(x)$, $G(x)u+H(x)$ should be congruent to 0 in $K=\mathbb{Q}[x]/(R(x))$. Now the inverse polynomial of $G(x)$ in K, $G^{-1}(x)$ can be computed by using the extended Euclidean algorithm. Here we note that since $R(x)$ is an irreducible polynomial, K is a field and $\mathrm{GCD}(R(x),G(x))=1$. Thus, there exists $G^{-1}(x)$ in K. Therefore u can be determined as a polynomial in x such as $u(x) \equiv -G^{-1}(x)\cdot H(x)$ $\mathrm{mod}_x R(x)$. With the derived $u(x)$, we obtain $t(x)$ by setting $t(x)=u(x)+1$. From the CM equation, we set $q(x)=\frac{1}{4}((u(x)+1)^2+Dy(x,u)^2)$. Next we choose rational numbers (c_2,c_1,c_0) so that the coefficient of the highest degree of $u(x)$ is 0 and $q(x)$ is irreducible if there exist such rational numbers c_i's. Otherwise, choose any proper rational numbers (c_2,c_1,c_0). After determining c_i's, make $R(x)$ to be an integer coefficient irreducible polynomial with a positive leading coefficient by multiplying some $C \in \mathbb{Q}$ and letting the polynomial be $r(x)$.

According to Lemma 3, choose a positive square-free integer D that does not divide both $\mathrm{disc}(r(x))$ and $\mathrm{disc}(q(x))$ to preserve the irreducibilities of $r(x)$ and $q(x)$. Finally, if $q(x)$ represents primes, then $(t(x),r(x),q(x))$ parameterizes a complete family of paring-friendly curves with embedding degree k and discriminant D. Algorithm 5 gives a brief description of our method.

Algorithm 5 New method : Modified Dupont-Enge-Morain method

```
Input: a positive integer $k$
Output: $D$, $t(x)$, $r(x)$, $q(x)$ in $\mathbb{Q}[x]$
 1: Set $y(x,u)=c_2u+c_1x+c_0 \in \mathbb{Q}[x,u]$ with variables $c_i$'s in $\mathbb{Q}$.
 2: Compute the resultant with an additional variable $D$ in $\mathbb{Z}$
        $R(x) := \mathrm{Res}_u(\Phi_k(u),(u-1)^2+Dy(x,u)^2) \in \mathbb{Q}[x]$.
 3: Compute $G(x)$ and $H(x)$ such that
        $\Phi_k(u)\ \mathrm{mod}_u((u-1)^2+Dy(x,u)^2)=G(x)\cdot u+H(x)$.
 4: Compute the inverse polynomial $G^{-1}(x)$ of $G(x)$ $\mathrm{mod}_x R(x)$.
 5: Obtain $u$ as a polynomial in $x$ by
        $u(x) \equiv -G^{-1}(x)\cdot H(x)\ \mathrm{mod}_x R(x)$.
 6: Let $t(x)=u(x)+1$, $q(x)=\frac{1}{4}((u(x)+1)^2+Dy(x)^2)$.
 7: Choose $(c_0,c_1,c_2) \in \mathbb{Q}$ that make the leading coefficient of $u(x)$ to be zero and preserve the irreducibilities of both $q(x)$ and $R(x)$.
 8: Choose $C \in \mathbb{Q}$ such that $C\cdot R(x) \in \mathbb{Z}[x]$ and set $r(x)=C\cdot R(x)$.
 9: Determine a positive square-free integer $D$ that does not divide both $\mathrm{disc}(r(x))$ and $\mathrm{disc}(q(x))$.
10: If $q(x)$ represents primes, then return $D, t(x), r(x), q(x)$.
```

(**Note**) We treat u merely as a variable from Step 1 to Step 4 before u is determined as the x-polynomial in Step 5.

Remark. In Step 9, if a square-free positive integer D_0 that makes $R(x)$ be decomposed into irreducible polynomials $R_1(x)$ and $R_2(x)$ in $\mathbb{Q}[x]$ with $deg_xR_i=\phi(k)$, $i=1,2$, where ϕ is the Euler phi function, is chosen, then just follow from Step 6 to Step 10 except Step 9 with $D:=D_0$ and $u_i(x):=u(x)\ \mathrm{mod}_x R_i(x)$ for $i=1,2$. We demonstrate this relation in the following statement.

Suppose that a chosen D_0 makes $R(x)$ be factored into $R_1(x)\cdot R_2(x)$, with $deg_xR_i=\phi(k)$, $i=1,2$, then we perform modular $R_i(x)$ to the result $u(x)$, and call it $u_i(x)$, where $i=1,2$. Then

$$\begin{aligned}
&(u_i(x)-1)^2+D_0y(x)^2\\
&=(u(x)\ \mathrm{mod}_x R_i(x)-1)^2+D_0y(x)^2\\
&=(u(x)-R_i(x)T(x)-1)^2+D_0y(x)^2\\
&=(u(x)-1)^2+D_0y(x)^2-2R_i(x)T(x)(u(x)-1)+(R_i(x)T(x))^2,\\
&\quad for\ some\ T(x)\in\mathbb{Q}[x]\ \ and\ \deg T(x)=\deg u(x)-\deg R_i(x).
\end{aligned}$$

Since each $R_i(x,D_0)$ for $i=1,2$ is a factor of $R(x)$, $(u_i(x)-1)^2+D_0y(x)^2 \equiv 0\ \mathrm{mod}_x\ R_i(x)$. Therefore, for the specific D_0 such that $R(x)$ can be factored into $R_1(x)\cdot R_2(x)$ with $\deg_x R_i=\phi(k)$ for $i=1,2$, compute $u_i(x)$= $u(x)\ \mathrm{mod}_x R_i(x)$. Then we obtain $(t_i(x),r_i(x),q_i(x))$ for each i.

4 Examples

4.1 Applications to the Barreto-Naehrig curves

Now we apply our new method to derive the *Barreto-Naehrig curves* for embedding degree $k=12$, $D=3$ without the analysis of factorizations of cyclotomic polynomials.

Example 1. For embedding degree $k=12$ and CM discriminant $D=3$, set

$$\begin{aligned}
u(x) &= \ \tfrac{3}{8}(c_1x+c_0+1)^2,\\
t(x) &= \ \tfrac{1}{8}\{3c_1^2x^2+6(c_1c_0+1)x+3c_0^2+6c_0+11\},\\
y(x) &= -\tfrac{1}{8}\{3c_1^2x^2+2(3c_1c_0-c_1)x+3c_0^2-2c_0+3\},\\
r(x) &= \ \tfrac{1}{64}\{9c_1^4x^4+36c_1^3c_0x^3+18(3c_1^2c_0^2+c_1^2)x^2+12(3c_1
\end{aligned}$$

$$
\begin{aligned}
&\cdot c_0^3 + 3c_1c_0 - 2c_1)x + 9c_0^4 + 18c_0^2 - 24c_0 + 13\},\\
q(x) = \ &\tfrac{1}{64}\{9c_1^4x^4 + 36c_1^3c_0x^3 + 6(9c_1^2c_0^2 + 7c_1^2)x^2 + 12(3c_1\\
&\cdot c_0^3 + 7c_1c_0 + 2c_1)x + 9c_0^4 + 42c_0^2 + 24c_0 + 37\}.
\end{aligned}
$$

Then for suitable c_i's, $(t(x), r(x), q(x))$ parameterizes a complete family of elliptic curves with embedding degree $k = 12$, discriminant $D = 3$, $\rho = 1$ and a prime order.

Proof. After setting $y(x,u) = c_2u + c_1x + c_0$, we compute the resultant $R(x)$ of the 12^{th} cyclotomic polynomial $\Phi_{12}(u) = u^4 - u^2 + 1$ and the CM equation $(u-1)^2 + Dy(x,u)^2$ as the following

$$
\begin{aligned}
R(x) := \ &\mathrm{Res}_u(u^4 - u^2 + 1, (u-1)^2 + Dy(x,u)^2),\\
= \ &D^4c_1^8x^8 + 8D^4c_1^7c_0x^7 + \ldots - 16Dc_2c_0 - 6Dc_0^2 + 1.
\end{aligned}
$$

and let $K = \mathbb{Q}[x]/(R(x))$.

Now, we reduce $u^4 - u^2 + 1$ in K by the relation

$$
\begin{aligned}
u^2 \equiv -\frac{1}{(Dc_2^2+1)}\{&2(Dc_2c_1x + Dc_2c_0 - 1)u\\
&+ (Dc_1^2x^2 + 2Dc_1c_0x + Dc_0^2 + 1)\} \bmod_x R(x).
\end{aligned}
$$

Then we obtain
$u^4 - u^2 + 1 = G(x)u + H(x)$ *in* K, *where*

$$
\begin{cases}
G(x) = -\frac{(4D^3c_2^3c_1^3 - 4D^2c_2c_1^3)x^3 + .. + 4Dc_0^2 - 2}{(Dc_2^2+1)^3},\\
H(x) = -\frac{(3D^3c_2^2c_1^4 - D^2c_1^4)x^4 + .. + Dc_0^2 + 1}{(Dc_2^2+1)^3}
\end{cases}
$$

By using the extended Euclidean algorithm, we can compute

$$
G^{-1}(x) = \frac{(63D^{13}c_2^{19}c_1^7 + .. + 220319D^7c_2^7c_1^7)x^7 + .. + 2850Dc_0^2 + 225}{2(81D^{13}c_2^{26} + .. + 625)},
$$

and find u as an x-polynomial by,

$$
\begin{aligned}
u(x) &\equiv -G^{-1}(x) \cdot H(x) \bmod_x R(x)\\
&= \frac{-(12D^6c_2^5c_1^7 + .. + 3D^7c_2^7c_1^7)x^7 + .. + 155D_0c_0^2 + 5}{2(9D^7c_2^{14} + .. + 25)}.
\end{aligned}
$$

In the case of $k = 12$, only two CM discriminants $D = 1, 3$ allows $R(x)$ to be factored into $R_1(x)$ and $R_2(x)$ with $\deg_x R_i = \phi(k)$.

When $D = 3$, if we take $R_1(x)$ for $r(x)$, where

$$
\begin{aligned}
R_1(x) = \ &9c_1^4x^4 + 36c_1^3c_0x^3 - (9c_2^2c_1^2 + 18c_2c_1^2 - 54c_1^2c_0^2\\
&- 9c_1^2)x^2 - (18c_2^2c_1c_0 + 18c_2^2c_1 + 36c_2c_1c_0 - 12c_2c_1\\
&- 36c_1c_0^3 - 18c_1c_0 - 6c_1)x + (9c_2^4 - 9c_2^2c_0^2 - 18c_2^2c_0\\
&+ 9c_2^2 - 18c_2c_0^2 + 12c_2c_0 + 6c_2 + 9c_0^4 + 9c_0^2 + 6c_0 + 1),
\end{aligned}
$$

then

$$
\begin{aligned}
&u_1(x,3) \bmod_x R_1(x)\\
&=\\
&-\frac{1}{(81c_2^6 - 108c_2^5 - 63c_2^4 - 144c_2^3 - 45c_2^2 - 36c_2 - 5)}\{(\mathbf{54c_2^2c_1^3 + 36c_2c_1^3 - 18c_1^3})\mathbf{x^3}\\
&\quad + (54c_2^3c_1^2 + 162c_2^2c_1^2c_0 + 108c_2c_1^2c_0 + 54c_2c_1^2\\
&\quad - 54c_1^2c_0 + 12c_1^2)x^2 + (81c_2^5c_1 - 135c_2^4c_1 + 108c_2^3c_1c_0\\
&\quad - 162c_2^3c_1 + 162c_2^2c_1c_0^2 - 72c_2^2c_1 + 108c_2c_1c_0^2 + 108c_2c_1c_0\\
&\quad + 45c_2c_1 - 54c_1c_0^2 + 24c_1c_0 - 21c_1)x + (81c_2^5c_0 - 27c_2^5\\
&\quad - 135c_2^4c_0 - 135c_2^4 + 54c_2^3c_0^2 - 162c_2^3c_0 + 54c_2^2c_0^3 - 72c_2^2c_0\\
&\quad + 30c_2^2 + 36c_2c_0^3 + 54c_2c_0^2 + 45c_2c_0 + 15c_2 - 18c_0^3 + 12c_0^2\\
&\quad - 21c_0 - 3)\}
\end{aligned}
$$

The coefficient of the highest degree of $u_1(x)$ which is written as bold types has factors $c_1, (c_2+1)$ and $(c_2 - \frac{1}{3})$. If $c_1 = 0$, then $\deg_x R_1 = 2$. Since the degree of $r(x)$ is a multiple of $\phi(12) = 4$ by Lemma 2, this is impossible. Thus, we take $c_2 = -1$ or $\frac{1}{3}$. If we want to produce the original BN curves with $D = 3$, then take $c_2 = -1$, $u(x) = \frac{3}{8}(c_1x + c_0 + 1)^2$. There are infinitely many possible choices of c_1 and c_0. For simplicity, we take $c_1 = 4$, $c_0 = -1$. Finally, we obtain the BN curves with $u(x) = 6x^2$, $t(x) = 6x^2 - 1$, $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$ and $q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.

4.2 Some examples

Now we suggest several examples which parameterize the complete families and have improvements on ρ-values. Note that we state examples with a variable D to show that one can obtain abundant families by choosing D. For embedding degrees $k = 5$, 8, 12, 16, 20 and 24, we obtain complete families of ordinary elliptic curves with improved ρ-values. As we explained in the Introduction, sparse families are less efficient than complete families in computing elliptic curves via the CM method. Therefore, we prefer to use complete families to construct pairing-friendly elliptic curves. For $k = 5$, there exist a sparse family with the best record $\rho = 1.5$ [20] and a complete family having $\rho = 1.750$ [12]. In these examples, we provide the complete family of elliptic curves with embedding degree $k = 5$ and the best record $\rho = 1.50$. For the cases of $k = 8$, 16, 20 and 24, there exist only sparse families of curves proposed by [21]. For those embedding degrees, our construction allows to obtain the complete type of families. Moreover, these complete families have better ρ-values. For the case of $k = 12$, we obtain the complete family with improved value $\rho = 1.5$, which is better than the previously-known complete type of family with $\rho = 1.75$. We compare the previously-known smallest records of ρ-values and our improved ρ-values for $k = 5, 8, 12, 16, 20, 24$ with the types of the families in Table 1.

(**Note**) We denote our improved ρ-values and previously known best ρ-values with variable discriminants as ρ_{new} and ρ_{record}, respectively.

Example 2. For embedding degree $k = 5$,

$$
\begin{aligned}
t(x,D) &= \tfrac{1}{11}(3125D^3x^6 + 875D^2x^4 + 175Dx^2 + 14),\\
r(x,D) &= 15625D^4x^8 + 3125D^3x^6 + 250D^2x^4 + 1,\\
q(x,D) &= \tfrac{1}{484}(9765625D^6x^{12} + 5468750D^5x^{10}\\
&\quad + 1859375D^4x^8 + 393750D^3x^6 + 55125D^2x^4\\
&\quad + 7925Dx^2 + 196).
\end{aligned}
$$

Let D be a square-free positive integer not dividing $2 \cdot 5 \cdot 7 \cdot 11 \cdot 4430894490089$. Then $(t(x,D), r(x,D), q(x,D))$ parameterizes a complete family of curves with $\rho_{new} = 1.50$, where $\rho_{record} = 1.50$ for the sparse family and $\rho_{record} = 1.75$ for the complete family.

Proof. By substituting Dx^2 with z, we obtain the irreducible polynomial $\widetilde{r}(z) = 15625z^4 + 3125z^3 + 250z^2 + 1$.

Since the discriminant of $\widetilde{r}(z)$ is $5^{19}\cdot 11^2$, by Lemma 3, when D does not divide $5^{25}\cdot 11^2$, $r(x,D)$ is irreducible. Moreover, since $\widetilde{q}(z)\ =\frac{1}{484}(9765625z^6+5468750z^5+1859375z^4+393750z^3+55125z^2+7925z+196)$ is irreducible, and $q(x,D)$ is also irreducible if D does not divide $2^2\cdot 5^{59}\cdot 7^2\cdot 11^6\cdot 4430894490089$. Since D is square-free, it is sufficient to take D that does not divide $2\cdot 5\cdot 7\cdot 11\cdot 4430894490089$. Thus $(t(x,D),r(x,D),q(x,D))$ parameterizes a complete family of curves with embedding degree 5 and discriminant D that does not divide $2\cdot 5\cdot 7\cdot 11\cdot 4430894490089$.

Example 3. For embedding degree $k=8$,

$$\begin{aligned}
t(x,D) &= \tfrac{1}{6}(32D^3x^6+40D^2x^4+32Dx^2+7),\\
r(x,D) &= 64D^4x^8+64D^3x^6+32D^2x^4-8Dx^2+1,\\
q(x,D) &= \tfrac{1}{144}(1024D^6x^{12}+2560D^5x^{10}+3648D^4x^8\\
&\quad +3008D^3x^6 \qquad +1584D^2x^4+592Dx^2+49).
\end{aligned}$$

Let D be a square-free positive integer not dividing $2\cdot 3\cdot 5\cdot 7\cdot 151\cdot 112237$. Then $(t(x,D),r(x,D),q(x,D))$ parameterizes a complete family of curves with $\rho_{new}=1.50$, where $\rho_{record}=1.75$.

Proof. By substituting Dx^2 with z, we obtain the irreducible polynomial $\widetilde{r}(z)\ =64z^4+64z^3+32z^2-8z+1$. Since the discriminant of $\widetilde{r}(z)\ =2^{28}\cdot 3^2$, by Lemma 3, when D does not divide $2^{34}\cdot 3^2$, $r(x,D)$ is irreducible. Moreover, since $\widetilde{q}(z)\ =\frac{1}{144}(1024z^6+2560z^5+3648z^4+3008z^3+1584z^2+592z+49)$ is irreducible, $q(x,D)$ is also irreducible if $D\nmid 2^{72}\cdot 3^6\cdot 5\cdot 7^2\cdot 151\cdot 112237$. Since D is square-free, it is sufficient to take D that does not divide $2\cdot 3\cdot 5\cdot 7\cdot 151\cdot 112237$. Thus $(t(x,D),r(x,D),q(x,D))$ parameterizes a complete family of curves with $k=8$ and discriminant $D\nmid 2\cdot 3\cdot 5\cdot 7\cdot 151\cdot 112237$.

Example 4. For embedding degree $k=12$,

$$\begin{aligned}
t(x,D) &= \tfrac{1}{10}(2D^3x^6+13D^2x^4+31Dx^2+11),\\
r(x,D) &= D^4x^8+6D^3x^6+11D^2x^4-6Dx^2+1,\\
q(x,D) &= \tfrac{1}{400}(4D^6x^{12}+52D^5x^{10}+293D^4x^8+850D^3x^6\\
&\quad +1247D^2x^4+782Dx^2+121).
\end{aligned}$$

Let D be a square-free positive integer not dividing $2\cdot 3\cdot 5\cdot 11\cdot 17\cdot 31\cdot 9181$. Then $(t(x,D),r(x,D),q(x,D))$ parameterizes a complete family of curves with$\rho_{new}=1.50$, where $\rho_{record}=1.75$.

Proof. By substituting Dx^2 with z, we obtain the irreducible polynomial $\widetilde{r}(z)\ =z^4+6z^3+11z^2-6z+1$. Since the discriminant of $\widetilde{r}(z)\ =2^8\cdot 3^2\cdot 5^2$, by Lemma 3, when D does not divides $2^8\cdot 3^2\cdot 5^2$, $r(x,D)$ is irreducible. Moreover, since $\widetilde{q}(z)\ =\frac{1}{400}(4z^6+52z^5+293z^4+850z^3+1247z^2+782z+121)$is irreducible, $q(x,D)$ is also irreducible if $D\nmid 2^{19}\cdot 5^6\cdot 11^2\cdot 17^2\cdot 31\cdot 9181$. Since D is square-free, it is sufficient to take D that does not divide $2\cdot 3\cdot 5\cdot 11\cdot 17\cdot 31\cdot 9181$. Thus $(t(x,D),r(x,D),q(x,D))$ parameterizes a complete family of curves with embedding degree 12 and discriminant with $D\nmid 2\cdot 3\cdot 5\cdot 11\cdot 17\cdot 31\cdot 9181$.

Example 5. For embedding degree $k=16$,

$$\begin{aligned}
t(x,D) &= \tfrac{1}{15368}(492D^7x^{14}+4044D^6x^{12}+14683D^5x^{10}\\
&\quad +30957D^4x^8+43038D^3x^6+11994D^2x^4\\
&\quad +94858Dx^2+15970),\\
r(x,D) &=D^8x^{16}+8D^7x^{14}+28D^6x^{12}+56D^5x^{10}\\
&\quad +72D^4x^8+168D^2x^4-48Dx^2+4,\\
q(x,D) &= \tfrac{1}{944701696}(242064D^{14}x^{28}+3979296D^{13}x^{26}\\
&\quad +30802008D^{12}x^{24}+149217792D^{11}x^{22}\\
&\quad +508320097D^{10}x^{20}+1268976702D^9x^{18}\\
&\quad +2412537501D^8x^{16}+3799796520D^7x^{14}\\
&\quad +5509631348D^6x^{12}+7374408776D^5x^{10}\\
&\quad +9297619824D^4x^8+3650087424D^3x^6\\
&\quad +9381128524D^2x^4+3265939944Dx^2\\
&\quad +255040900).
\end{aligned}$$

Let D be a square-free positive integer not dividing $2\cdot 3\cdot 5\cdot 17\cdot 23\cdot 41\cdot 109\cdot 113\cdot 1597\cdot 565604969$. Then $(t(x,D),r(x,D),q(x,D))$ parameterizes a complete family of curves with with $\rho_{new}=1.750$, where $\rho_{record}=1.875$.

Proof. By substituting Dx^2 with z, we obtain the irreducible polynomial $\widetilde{r}(z)=z^8+8z^7+28z^6+56z^5+72z^4+168z^2-48z+4$. Since the discriminant of $\widetilde{r}(z)=2^{48}\cdot 17^4\cdot 113^2$, by Lemma 3, when D does not divide $2^{50}\cdot 17^4\cdot 113^2$, $r(x,D)$ is irreducible. Moreover, since $\widetilde{q}(z)=\frac{1}{944701696}(242064z^{14}+3979296z^{13}+30802008z^{12}+149217792z^{11}+508320097z^{10}+1268976702z^9+241253701z^8+3799796520z^7+5509631348z^6+7374408776z^5+9297619824z^4+3650087424z^3+9381128524z^2+3265939944z+255040900)$ is irreducible, $q(x,D)$ is also irreducible whenever $D\nmid\ 2^{112}\cdot 3^{17}\cdot 5^2\cdot 17^{14}\cdot 23\cdot 41^{15}\cdot 109\cdot 113^{14}\cdot 1597^2\cdot 565604969$. Note that we do not consider the factors of $\mathrm{disc}(q(z))$ that are larger than 10^{15}. Since D is square-free, it is sufficient to take D that does not divide $2\cdot 3\cdot 5\cdot 17\cdot 23\cdot 41\cdot 109\cdot 113\cdot 1597\cdot 565604969$. Thus $(t(x,D),r(x,D),q(x,D))$ parameterizes a complete family of curves with embedding degree 8 and discriminant $D\nmid\ 2\cdot 3\cdot 5\cdot 17\cdot 23\cdot 41\cdot 109\cdot 113\cdot 1597\cdot 565604969$.

Example 6. For embedding degree $k=20$,

$$\begin{aligned}
t(x,D) &=\tfrac{1}{3169178}(304480D^7x^{14}+3089993D^6x^{12}\\
&\quad +12948870D^5x^{10}+26353063D^4x^8\\
&\quad +18270164D^3x^6-17618777D^2x^4+35118045Dx^2\\
&\quad +3039654),\\
r(x,D) &=D^8x^{16}+10D^7x^{14}+41D^6x^{12}+80D^5x^{10}\\
&\quad +46D^4x^8-70D^3x^6+116D^2x^4-20Dx^2+1,\\
q(x,D) &=\tfrac{1}{40174756782736}(92708070400D^{14}x^{28}\\
&\quad +1881682137280D^{13}x^{26}+17433400615249D^{12}x^{24}\\
&\quad +96071796560300D^{11}x^{22}+341660593743458D^{10}x^{20}\\
&\quad +784665001073404D^9x^{18}+1080141575997407D^8x^{16}\\
&\quad +725543114107894D^7x^{14}+333444429942138D^6x^{12}\\
&\quad +1285860383086774D^5x^{10}+1753854572714893D^4x^8\\
&\quad -1126404052895418D^3x^6+1126167112655709D^2x^4\\
&\quad +223537101108544Dx^2+9239496439716).
\end{aligned}$$

Let D be a square-free positive integer not dividing $2\cdot 3\cdot 5\dot{}11\cdot 29\cdot 37\cdot 101\cdot 173\cdot 239\cdot 541\cdot 506609\cdot 6811303\cdot 17244169$. Then $(t(x,D),r(x,D),q(x,D))$ parameterizes a complete family of curves with $\rho_{new}=1.750$ where $\rho_{Record}=1.875$.

Proof. By substituting Dx^2 with z, we obtain the irreducible polynomial $\widetilde{r}(z) = z^8 + 10z^7 + 41z^6 + 80z^5 + 46z^4 - 70z^3 + 116z^2 - 20z + 1$. Since the discriminant of $\widetilde{r}(z) = 2^{16} \cdot 5^6 \cdot 29^2 \cdot 101^2 \cdot 541^2$, by Lemma 3, when D does not divide $2^{16} \cdot 5^6 \cdot 29^2 \cdot 101^2 \cdot 541^2$, $r(x,D)$ is irreducible. And $\widetilde{q}(z) = \frac{1}{40174756782736}(92708070400z^{14} + 1881682137280z^{13} + 17433400615249z^{12} + 96071796560300z^{11} + 341660593743458z^{10} + 784665001073404z^9 + 1080141575997407z^8 + 725543114107894z^7 + 333444429942138z^6 + 1285860383086774z^5 + 1753854572714893z^4 - 1126404052895418z^3 + 1126167112655709z^2 + 223537101108544z + 9239496439716)$ is irreducible, $q(x,D)$ is also irreducible if $D \nmid 2^{107} \cdot 3^6 \cdot 5^{15} \cdot 11^{15} \cdot 29^{14} \cdot 37 \cdot 101^{14} \cdot 173^{15} \cdot 239 \cdot 541^{14} \cdot 506609^2 \cdot 6811303 \cdot 17244169$. Note that we do not consider the factors of $\mathrm{disc}(q(z))$ that are larger than 10^{15}. Since D is square-free, it is sufficient to take D that does not divide $2 \cdot 3 \cdot 5 \cdot 11 \cdot 29 \cdot 37 \cdot 101 \cdot 173 \cdot 239 \cdot 541 \cdot 506609 \cdot 6811303 \cdot 17244169$. Thus $(t(x,D), r(x,D), q(x,D))$ parameterizes a complete family of curves with embedding degree 20 and discriminant $D \nmid 2 \cdot 3 \cdot 5^{\cdot}11 \cdot 29 \cdot 37 \cdot 101 \cdot 173 \cdot 239 \cdot 541 \cdot 506609 \cdot 6811303 \cdot 17244169$.

Example 7. For embedding degree $k = 24$,

$$\begin{aligned} t(x,D) = {} & \tfrac{1}{392700}(24503D^7x^{14} + 198575D^6x^{12} \\ & + 658203D^5x^{10} + 1542931D^4x^8 + 2800473D^3x^6 \\ & + 1821521D^2x^4 + 5485400Dx^2 + 402966), \\ r(x,D) = {} & D^8x^{16} + 8D^7x^{14} + 26D^6x^{12} + 60D^5x^{10} \\ & + 107D^4x^8 + 60D^3x^6 + 206D^2x^4 - 28Dx^2 + 1, \\ q(x,D) = {} & \tfrac{1}{616853160000}(600397009D^{14}x^{28} \\ & + 9731366450D^{13}x^{26} + 71687926843D^{12}x^{24} \\ & + 337018198036D^{11}x^{22} + 1183246215697D^{10}x^{20} \\ & + 3232596936062D^9x^{18} + 7059430108349D^8x^{16} \\ & + 13238008748048D^7x^{14} + 20844662879131D^6x^{12} \\ & + 27659895033862D^5x^{10} + 35284865408533D^4x^8 \\ & + 22240533392636D^3x^6 + 31557635222572D^2x^4 \\ & + 4575072682800Dx^2 + 162381597156) \,. \end{aligned}$$

Let D be a square-free positive integer not dividing $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 47 \cdot 61 \cdot 107 \cdot 229 \cdot 367 \cdot 56531 \cdot 69846486007 \cdot 209843489291$.

Then $(t(x,D), r(x,D), q(x,D))$ parameterizes a complete family of curves with $\rho_{new} = 1.750$ where $\rho_{record} = 1.875$.

Proof. By substituting Dx^2 with z, we obtain the irreducible polynomial $\widetilde{r}(z) = z^8 + 8z^7 + 26z^6 + 60z^5 + 107z^4 + 60z^3 + 206z^2 - 28z + 1$. Since the discriminant of $\widetilde{r}(z) = 2^{32} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 17^2$, by Lemma 3, when D does not divide $2^{32} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 17^2$, $r(x,D)$ is irreducible. Moreover, since $\widetilde{q}(z) = \frac{1}{616853160000}(600397009z^{14} + 9731366450z^{13} + 71687926843z^{12} + 337018198036z^{11} + 1183246215697z^{10} + 3232596936062z^9 + 7059430108349z^8 + 13238008748048z^7 + 20844662879131z^6 + 2765989503386 2z^5 + 35284865408533z^4 + 22240533392636z^3 + 31557635222572z^2 + 4575072682800z + 162381597156)$ is irreducible, $q(x,D)$ is also irreducible if $D \nmid 2^{56} \cdot 3^{26} \cdot 5^{28} \cdot 7^{14} \cdot 11^{14} \cdot 17^{14} \cdot 19 \cdot 47 \cdot 61^2 \cdot 107^{15} \cdot 229^{15} \cdot 367^2 \cdot 56531 \cdot 69846486007 \cdot 209843489291$. Note that we do not consider the factors of $\mathrm{disc}(q(z))$ that are larger than 10^{15}. Since D is square-free, it is sufficient to take D that does not divide $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 47 \cdot 61 \cdot 107 \cdot 229 \cdot 367 \cdot 56531 \cdot 69846486007 \cdot 209843489291$.

Therefore, $(t(x,D), r(x,D), q(x,D))$ parameterizes a complete family of curves with embedding degree 24 and discriminant $D \nmid 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 47 \cdot 61 \cdot 107 \cdot 229 \cdot 367 \cdot 56531 \cdot 69846486007 \cdot 209843489291$.

Table 1: Comparison of the recorded ρ-values and the improved ρ-values of families of elliptic curves having variable D.

$\phi(k)$	k	ρ_{rec}	*Family Type*$_{rec}$	$\deg_x r(x)_{rec}$
		ρ_{new}	*Family Type*$_{new}$	$\deg_x r(x)_{new}$
2	4	1.000	sparse	2
		-	complete	-
		1.000†	sparse	2
		1.500	**complete**	**4**
	6	1.000	sparse	2
		-	complete	-
		1.000†	sparse	2
		1.500	**complete**	**4**
4	5	1.500	sparse	8
		1.750	**complete**	**8**
		1.500†	sparse	4
		1.500	**complete**	**8**
	8	1.750	sparse	4
		1.500	**complete**	**8**
	10	1.000	sparse	4
		-	complete	-
		1.000†	sparse	4
		1.500	**complete**	**8**
	12	1.750	complete	8
		1.500	**complete**	**8**
8	16	1.875	sparse	8
		1.750	**complete**	**16**
	20	1.875	sparse	8
		1.750	**complete**	**16**
	24	1.875	sparse	8
		1.750	**complete**	**16**

(**Note**) $^{(1)}$By setting $Dy(x)^2$ as $c_2u + c_1x + c_0$ in Step 1 of the Algorithm 5, we can also produce the sparse families. We describe the ρ-values marked with † for the comparison.
$^{(2)}$The entries in bold indicate our improved results.

We have summarized the ρ-values, the family types and the degrees of $r(x)$ from the new modified Dupont-Enge-Morain method according to $\phi(k)$ and have compared them with the previously reported best records including both complete families and sparse families in Table 1. The compared previous works in Table 1 are contained in [4], [9], [12], [20] and [21].

5 Conclusion

In this paper, we propose a new algorithm for constructing complete families of pairing friendly elliptic curves having various $r(x)$ and D for arbitrary embedding degrees by extending and modifying the original the Dupont-Enge-Morain method. The Dupont-Enge-Morain method is known to have constant curve parameters (t,r,q) and the weakness of $\rho \approx 2$. In our modification, by choosing a special form of the input polynomial parameter $y(x)$, families of elliptic curves can be constructed by polynomial curve parameters $(t(x),r(x),q(x))$ having $\rho < 2$ with variable CM discriminants D. Moreover, for $k = 5,8,12,16,20$ and 24, the family types and the ρ-values have been improved.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT and Future Planning (Grant No.: 2012R1A2A1A03006706), and Priority Research Centers Program of the Ministry of Education (Grant No.: 2009-0093827).

References

[1] A.O.L. Atkin and F. Morain. Elliptic Curves and Primality Proving. *Mathematic of Computation*, **61**, pp.29-68, 1993.

[2] P.S.L.M. Barreto, S. Galbraith, C. ÓhÉigeartaigh, and M. Scott. Efficient pairing computation on supersingular abelian varieties, *Designs, Codes and Cryptography*, **42**, pp.239-271, 2007.

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

[4] G. Bisson and T. Satoh. More Discriminants with the Brezing-Weng Method. Gaetan Bisson, and Takakazu Satoh. INDOCRYPT, volume **5365** of *Lecture Notes in Computer Science*, pp.389-399. Springer, 2008.

[5] D. Boneh, and M. Franklin. Identity-based encryption from the Weil pairing, Advances in Cryptology, volume **2139** of *Lecture Notes in Computer Science*, pp.213 - 229. Springer, 2001.

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

[7] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Designs, Codes and Cryptography*, **37**: pp.133-141, 2005.

[8] C. Cocks and R. G. E. Pinch. ”Identity-based cryptosystems based on the Weil pairing,” unpublished manuscript, 2001.

[9] R. Dryło. On constructing families of pairing-friendly elliptic curves with variable discriminant. *INDOCRYT 2011*, volume **7017** of *Lecture Notes in Computer Science*, pp.310-319. Springer,2011.

[10] R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. *Journal of Cryptology*, **18**, pp.79-89, 2005.

[11] D. Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. *In Algorithmic Number Theory Symposium — ANTS-VII*, volume **4076** of *Lecture Notes in Computer Science*, pp.452-465. Springer, 2006.

[12] D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology* **23**, pp. 224-280, 2010.

[13] S. Galbraith, J. McKee, and P. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields and their Applications*, **13**, pp.800-814, 2007.

[14] F. Hess, N.P. Smart, and F. Vercauteren. The Eta Pairing Revisited. *IEEE Trans. Information Theory* **52**, pp.4595-4602, 2006.

[15] T. W. Hungerford. *Algebra*, New York, Springer-Verlag , 1996.

[16] A. Joux. A one round protocol for tripartite Diffie-Hellman, *Algorithmic Number Theory - ANTS-IV*, volume **1838** of *Lecture Notes in Computer Science*, pp.385-393, Springer, 2000. Full version : *Journal of Cryptology*, **17**, pp.263-247, 2004.

[17] E. Kachisa, E. Schaefer, and M. Scott. Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. In Pairing-Based Cryptography-Pairing 2008, volume **5209** of *Lecture Notes in Computer Science*, pp.126-135. Springer, 2008.

[18] S. Lang. *Algebra*,revised 3rd edition. Springer, 2005.

[19] E.J. Lee, H.S. Lee, and C.M. Park. Efficient and generalized pairing computation on abelian varieties. *IEEE Trans. Information Theory* **55**, pp.1793-1803, 2009.

[20] H.S. Lee and C.M. Park. Generating Pairing-Friendly Curves with the CM Equation of Degree 1. *Pairing 2009*, volume **5671** of *Lecture Notes in Computer Science*, pp.66-77, Springer, 2009.

[21] H.S. Lee and C.M. Park. Constructing pairing-friendly curves with variable CM discriminant. *Bull. Korean Mathmetic Society*. **49**, No.1, pp.75-88, 2012.

[22] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals*, E**84**-A(5), pp.1234-1243, 2001.

[23] M. Scott and P.S.L.M. Barreto. Generating more MNT elliptic curves. *Designs, Codes and Cryptography*, **38**, pp.209-217, 2006.

[24] A. V. Sutherland. Accelerating the CM method. *LMS J. Comput. Math.*, **15**, pp.172-204, 2012.

[25] F. Vercauteren. Optimal pairings. *IEEE Trans. Information Theory*, **56** pp.455-461, 2010.

[26] C. Zhao, F. Zhang, and J. Huang. A note on the Ate pairing. *Int. J. Inf. Security*, vol.**7**, no. 6, pp.379-382. Springer, 2008.

Hyang-Sook Lee is a Professor at the Department of Mathematics, Ewha Womans University, Seoul in Korea. She received the Ph.D from Northwestern University, USA in 1993. Her research interests are pairing based cryptography, especially pairing computations and constructing pairing friendly curves etc. Now she is also working on the Lattice based cryptosystem. She served as a Vice-Chair General of Organizing Committee and Executive Committee of 2014 ICM (International Congress of Mathematicians). She served as Co-Chair of Program Committee of Algorithmic Number Theory Symposium in 2014. She has served on the Steering Committee of National Science and Technology Council in Korea, and she is currently a member of Expert Committee of Basic Science and Technology in The National Science & Technology Council in Korea.

Pa-Ra Lee is a Ph.D student at the Department of Mathematics, Ewha Womans University, Seoul in Korea. Her research interests are: computations and applications of pairings, constructing algebraic curves especially elliptic curves and hyperelliptic curves, polynomial algebra such as evaluation of modular polynomials and factorization of polynomials over finite fields.