On near prime-order elliptic curves with small embedding degrees (Full version)*

Duc-Phong Le[1], Nadia El Mrabet[2**], and Chik How Tan[1]

[1] Temasek Laboratories, National University of Singapore
{tslld,tsltch}@nus.edu.sg
[2] LIASD, University Paris 8, France
SAS team CMP, Ecole des Mines de St Etienne, France
nadia.el-mrabet@emse.fr

Abstract. In this paper, we extend the method of Scott and Barreto and present an *explicit* and *simple* algorithm to generate families of generalized MNT elliptic curves. Our algorithm allows us to obtain *all* families of generalized MNT curves with any given cofactor. Then, we analyze the complex multiplication equations of these families of curves and transform them into generalized Pell equation. As an example, we describe a way to generate Edwards curves with embedding degree 6, that is, elliptic curves having cofactor $h = 4$.
Keywords: Pairing Friendly Elliptic Curve, MNT curves, Complex Multiplication, Pell's equation.

1 Introduction

Pairings used in cryptology are efficiently *computable* bilinear maps on torsion subgroups of points on an elliptic curve that map into the multiplicative group of a finite field. We call such a map a *cryptographic pairing*. The first notable application of pairings to cryptology was the work of Menezes, Okamato and Vanstone [18]. They showed that the discrete logarithm problem on a supersingular elliptic curve can be reduced to the discrete logarithm problem in a finite field through the Weil pairing. Then, Frey and Ruck [10] also consider this situation using the Tate pairing. Pairings were thus used as a means of attacking cryptosystems.

However, pairings on elliptic curves only become a great interest since their first application in constructing cryptographic protocols in [14]. Joux described an one-round 3-party Diffie-Hellman key exchange protocol in 2000. Since then, the use of cryptographic protocols based on pairings has had a huge success with some notable breakthroughs such as practical Identity-based Encryption (IBE) schemes [6], short signature schemes [5]. Unlike standard elliptic curve cryptosystems, pairing-based cryptosystems require elliptic curves with *special* properties, namely, the embedding degree k is small enough[3]. Balasubramanian and Koblitz [2] showed that ordinary elliptic curves with such a property are *very rare*. An elliptic curve with such nice properties is called a *pairing-friendly* elliptic curve.

Miyaji, Nakabayashi and Takano introduced the concept of "family of pairing-friendly elliptic curves" in [19]. They provided families of *prime-order* elliptic curves with embedding degrees $k = 3, 4$ and 6, such that the number of points on these curves $E(\mathbb{F}_q)$ are prime. As analyzed in [20], these families of curves, so-called MNT curves, are more efficient than supersingular elliptic curves when implementing pairing-based cryptosystems. Later, Scott and Barreto [21], and Galbraith *et al.* [11] extended and introduced more MNT curves. These curves are of *near prime-order*, that is, curves with small cofactors $h \geq 2$. The

* Please cite the conference version of this work published at CAI'15 [16]

** This work was supported in part by the French ANR-12-INSE-0014 SIMPATIC Project.

[3] Let q be a prime number or a power of a prime, let E be an elliptic curve defined over $\mathbb{F}_q$ with a subgroup of prime order r. Then the embedding degree is the smallest integer such that r divides $(q^k - 1)$.

number of points on these curves is $\#E(\mathbb{F}_q) = h \cdot r$, where r is a big prime number. While Galbraith *et al.*'s method allows generating explicit families of curves, Scott-Barreto's method only generates particular elliptic curves.

In this paper we extend the method of Scott and Barreto in [21] and present an explicit, simple algorithm to generate families of ordinary elliptic curves of prime order (or near prime order with any cofactor) with small embedding degrees. Given an embedding degree k and a cofactor h, we demonstrate that our algorithm will output *all* possible families. We then point out a one-to-one correspondence between families of MNT curves having the same embedding degree and the same cofactor (Theorems 2, 3, and 4). We also analyze the complex multiplication equations of these families of curves and show how to transform these complex multiplication equations into generalized Pell equations that allow us to find particular curves. We illustrate our analysis for constructing Edwards curves with embedding degree 6.

The paper is organized as follows: Section 2 briefly recalls MNT curves, as well as methods to generate MNT curves with small cofactors. Section 3 presents our alternative method to generate such curves. We give our results in Section 4. We also discuss the Pell equation for some particular cases of MNT curves in this section. Finally, we conclude in Section 5.

2 Backgrounds

2.1 MNT curves

An elliptic curve generated randomly would have a large embedding degree. As a consequence, a random elliptic curve would not be suitable for efficient computation of a pairing based protocol. Supersingular elliptic curves have small embedding degree. However, such curves are limited to embedding degree $k = 2$ for prime fields and $k \leq 6$ in general [18]. If we want to vary the embedding degree to achieve a high security level, we must construct *pairing-friendly ordinary elliptic curves*. However, a study by Balasubramanian and Koblitz in [2] showed that ordinary elliptic curves with such a small embedding degree are *very rare* and thus require specific constructions.

In [9], Freeman *et al.* gave a taxonomy of existing constructions and families of pairing-friendly elliptic curves. They define precisely what a parameterization of a pairing friendly elliptic curve is.

Definition 1 (Freeman-Scott-Teske, [9], Definition 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, p) parameterizes a family of elliptic curves with embedding degree k and discriminant D if the following conditions are satisfied:
   1. *$q(x) = p(x)^d$ for some integer $d \geq 1$ and $p(x)$ a polynomial representing primes.*
   2. *$r(x)$ is non-constant, irreducible, integer-valued and has 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 equation $D \cdot y^2 = 4q(x) - t(x)^2$ has infinitely many integer solutions (x, y).*

   If these conditions are satisfied, we often refer to the triple (t, r, p) as a family.

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

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

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

(v) We say that (t, r, q) parameterizes a potential family of curves if conditions (2)–(5) of (i) are satisfied; in this case $p(x)$ may or may not represent primes.

The integer $t(x)$ represents the trace of the elliptic curve over $\mathbb{F}_{p(x)}$ with prime order $r(x)$.

The construction of elliptic curves is based on the Complex Multiplication method (CM for short). The most interesting construction of pairing-friendly elliptic curves is the one such that the result is a parameterization of a family of elliptic curve. Using the CM method of elliptic curve, the ρ value verifies that $1 \leq \rho \leq 2$, where the value ρ is defined as $\rho = \frac{\log(q)}{\log(r)}$. In order to save bandwidth during the calculation we are looking for ρ as small as possible.

Miyaji, Nakabayashi, and Takano [19] presented the first parameterized families that yield ordinary elliptic curves with embedding degree $k \in \{3, 4, 6\}$. These curves have a ρ-value equals to 1. The families are given by parameterization for q and t as polynomials in $\mathbb{Z}[x]$ with $\#E(\mathbb{F}_q) = n(x)$. We recall that $n(x) = q(x) + 1 - t(x)$, $n(x) \mid \Phi_k(q(x))$, and $n(x)$ represents primes in the MNT construction. Their results are summarized in Table 1.

k	$q(x)$	$t(x)$
3	$12x^2 - 1$	$-1 \pm 6x$
4	$x^2 + x + 1$	$-x$ or $x + 1$
6	$4x^2 + 1$	$1 \pm 2x$

Table 1: Parameters for MNT curves [19]

The construction of MNT curves is based on the Complex Multiplication method (CM for short). That is, we have to find solutions of (x_0, V_0) in the following CM equation:

$$DV^2 = 4q(x) - t^2(x)$$

for small values of D. The right-hand side of this equation is of quadratic form and can be transformed into a generalized Pell equation. Since the construction depends on solving a Pell-like equation, MNT curves of prime order are *sparse* [9]. It means that the equation admits only a few solutions.

2.2 MNT curves with small cofactors

Let $E(\mathbb{F}_q)$ be a parameterized elliptic curve with cardinality $\#E(\mathbb{F}_q) = n(x)$. We call the cofactor of $E(\mathbb{F}_q)$, the integer h such that $n(x) = h \times r(x)$, where $r(x)$ is a polynomial representing primes. The original construction of MNT curves gives families of elliptic curves with cofactor $h = 1$. Scott-Barreto [21], and Galbraith-McKee-Valença [11] extended the MNT idea by allowing small values of the cofactor $h > 1$. This allows to find many more suitable curves with $\rho \approx 1$ than original MNT construction. Let $\Phi_k(x)$ be the k-th *cyclotomic polynomial*, we have the following proposition.

Proposition 1. *[9, Proposition 2.4] Let k be a positive integer, $E(\mathbb{F}_q)$ be an elliptic curve defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t = hr$, where r is prime, and let t be the trace of $E(\mathbb{F}_q)$. Assume that $r \nmid kq$. Then $E(\mathbb{F}_q)$ has embedding degree k with respect to r if and only if $\Phi_k(q) \equiv 0 \pmod{r}$, or equivalently, if and only if $\Phi_k(t-1) \equiv 0 \pmod{r}$.*

Scott-Barreto's method Let $\Phi_k(x) = d \times r$ for some x. Scott-Barreto's method [21] first fixes small integers h and d and then substitutes $r = \Phi_k(t-1)/d$, where $t = x + 1$ to obtain the following CM equation:

$$DV^2 = 4h\frac{\Phi_k(x)}{d} - (x-1)^2. \tag{1}$$

Actually, Scott and Barreto used the fact that $\Phi_k(t-1) \equiv 0 \pmod{r}$. As above, the right-hand side of the Equation (1) is quadratic, hence it can be transformed into a generalized Pell equation by a linear substitution (see [21, §2] for more details). Then, Scott-Barreto found integer solutions to this equation for small D and arbitrary V with the constraint $4h > d$. The Scott-Barreto's method [21] presented generalized MNT elliptic curves with particular parameters. However it failed to give explicit families of generalized MNT elliptic curves.

Galbraith McKee and Valença's method Unlike Scott-Barreto's method, the mathematical analyses in [11] could lead to explicit families of generalized MNT curves. Galbraith *et al.* [11] extended the MNT method [19] and gave a complete characterization of MNT curves with small cofactors h. Actually, they used the fact that $\Phi_k(q) \equiv 0 \pmod{r}$. Similarly to the method in [19], Galbraith *et al.* defined λ by the equation $\Phi_k(q) = \lambda r$. For example, in the case $k = 6$, they required $\lambda r = \Phi_k(q) = q^2 - q + 1$. By using Hasse's bound, $|t| \leq 2\sqrt{q}$, they then analyzed and derived possible polynomials q, t from the equation $\Phi_k(q) = \lambda r$. Readers are referred to [11, Section 3] for a particular analysis in the case, in which the embedding degree is $k = 6$ and the cofactor is $h = 2$.

Remark 1. In the [11, Table 3], for $k = 4$, there are some pair (q, t) that don't correspond to *right* cofactor h. For example, when the cofactor is announced to be $h = 2$, with $q(x) = 8x^2+6x+3$, and $t(x) = -2x$, we find that the polynomial $r(x)$ is the following: $r(x) = 2(2x^2 + 2x + 1)$. In this form, $r(x)$ must be divided by 2 before representing primes. Consequently, the cofactor for this family of curves is in fact equals to 4. This mismatch between the announced cofactor and the real one comes from the fact that in GMV's method the polynomial $r(x)$ doesn't necessarily represent primes.

We list here the similar cases in Table 3 of [11] in the case $k = 4$:

- $h = 2$: $t = -2x$.
- $h = 3$: $t = -2x, t = -10x - 2$, and $t = 10x + 4$.
- $h = 4$: $t = -2x, t = -10x - 2$, $t = 10x + 4$, $t = 26x - 4$, and $t = 26x + 6$.
- $h = 5$: $t = -2x$, $t = 26x - 4$, $t = 26x + 6$, and $t = -34x - 12$, $t = 34x + 14$.

For all these case, the cofactor must be higher than that claimed in [11, Table 3].

3 An alternative approach to Galbraith *et al.*'s method

In this section, we present an alternative approach to generate explicit families of ordinary elliptic curves with embedding degree $3, 4$, or 6 and small cofactors. Different from the analytic approach in [11], we obtain families of curves by presenting a very *simple* and *explicit* algorithm. Our analyses also show that this algorithms can find all families of generalized MNT elliptic curves with any given cofactor.

3.1 Preliminary observations and facts

Some well-known facts and observations that can be used to find families of curves are noted in this section. Similar to Scott-Barreto's method, we use the fact that $\Phi_k(t-1) \equiv 0 \bmod r$. Consider cyclotomic polynomials corresponding to embedding degrees $k = 3, 4, 6$:

$$\begin{aligned}\Phi_3(t(x)-1) &= t(x)^2 - t(x) + 1,\\ \Phi_4(t(x)-1) &= t(x)^2 - 2t(x) + 2,\\ \Phi_6(t(x)-1) &= t(x)^2 - 3t(x) + 3.\end{aligned}$$

By setting $t(x) = ax + b$, we have the following equations:

$$\Phi_3(t(x)-1) = a^2x^2 + a(2b-1)x + \Phi_3(b-1), \tag{2}$$
$$\Phi_4(t(x)-1) = a^2x^2 + 2a(b-1)x + \Phi_4(b-1), \tag{3}$$
$$\Phi_6(t(x)-1) = a^2x^2 + a(2b-3)x + \Phi_6(b-1). \tag{4}$$

Theorem 1. *The quadratic polynomials $\Phi_3(t(x)-1)$, $\Phi_4(t(x)-1)$ and $\Phi_6(t(x)-1)$ are irreducible over the rational field.*

Proof. We start with the following lemma.

Lemma 1. *Let $f(x)$ be a quadratic irreducible polynomial in $\mathbb{Q}[x]$. If we perform any $\mathbb{Z}$-linear change of variables $x \mapsto ax + b$ for any $a \in \mathbb{Q} \setminus \{0\}$ and $b \in \mathbb{Q}$, $f(x)$ will still be a quadratic irreducible polynomial in $\mathbb{Q}[x]$.*

Proof. If we assume that $f(ax+b)$ is not irreducible in $\mathbb{Q}[X]$, then as $f(x)$ is a quadratic polynomial it means that $f(ax+b)$ admits a decomposition of the form $f(ax+b) = c(x-c_1)(x-c_2)$, for $c, c_1, c_2 \in \mathbb{Q}$. The values c_1 and c_2 are rational roots of $f(ax+b) = 0$. It is easy to see that $ac_1 + b$ and $ac_2 + b$ would then be rational roots of $f(x) = 0$. □

We now prove Theorem 1. As the polynomial $\Phi_3(x) = x^2 - x + 1$ is irreducible in $\mathbb{Q}[x]$, according to Lemma 1 the polynomial $\Phi_3(t(x)-1)$ is also irreducible in $\mathbb{Q}[x]$. The same argument ensures that $\Phi_4(t(x)-1)$ and $\Phi_6(t(x)-1)$ are irreducible in $\mathbb{Q}[x]$. □

Let a triple (t, r, q) parameterize a family of generalized MNT curves, and let h be a small cofactor. Let $n(x)$ be a polynomial representing the cardinality of elliptic curves in the family (t, r, q). That is, $n(x) = h \cdot r(x) = q(x) - t(x) + 1$. By Definition 1, we have:

$$\Phi_k(t(x)-1) = d \times r(x), \tag{5}$$

where $d \in \mathbb{Z}$, and $r(x)$ is a quadratic irreducible polynomial. By Hasse's bound, $4q(x) \geq t^2(x)$, we get the inequality:

$$4h \geq d \tag{6}$$

From equations (2)–(4), we can see that d is the greatest common divisor of the coefficients appearing in these equations. For instance, when $k = 3$, d is the GCD of $\Phi_3(b-1)$, a^2, and $a(2b-1)$. We recall the following well-known Lemma, which can be found in [12, Chapter V, §6]:

Lemma 2. *Let d be prime and $k, n > 0$. If d divides $\Phi_k(n)$, then d does not divide n, and either d divides k or $d \equiv 1 \pmod{k}$.*

The above lemma points out that if $\Phi_k(n)$ can be factorized by prime factors d_i, i.e. $\Phi_k(n) = \prod d_i$, then, either $d_i \mid k$ or $d_i \equiv 1 \pmod{k}$.

Example 1. In the case of $k = 6$, suppose that $\Phi_6(ax + b') = m \cdot r(x)$, where $b' = b - 1$. Then m will be the greatest common divisor of a^2, $a(2b' + 1)$ and $\Phi_6(b')$, and either $m|6$ or $m \equiv 1 \pmod{6}$.

Lemma 3. *Given $t(x) = ax + b$, if d in Eq. (5) does not divide a, then d is square free.*

Proof. We know that $d \in \mathbb{Z}$, and d is the greatest common divisor of factors of $\Phi_k(t(x) - 1)$, i.e. d divides a^2, $2a(2b - 1)$ or $2a(b - 1)$ or $2a(2b - 3)$ and $\Phi_k(b - 1)$ (Equations (2)–(4)). Suppose that d is not square free, that is $d = p^2 \times d'$ with p a prime number greater or equal to 2. By Lemma 2, p does not divide $(b - 1)$ and either p divides k or $p \equiv 1 \pmod{k}$. We also assume that d divides a^2, but does not divide a, and hence $p^2 \nmid a$, and p is a prime factor of a.

- $\mathbf{k = 3}$: As p divides $\Phi_3(b-1) = b^2-b+1$ and p divides $2b-1$ we have that p divides $(2b-1)+\Phi_3(b-1)$, *i.e.* p divides $b(b - 1)$. We know that p does not divide $(b - 1)$, thus p must divide b.
  We have $p \mid 2b - 1 = (b - 1) + b$, and $p \mid b$, hence p must divide $b - 1$. This is contradictory with Lemma 2. Thus, d is square free.
- $\mathbf{k = 4}$: We have that p divides $2(b - 1)$. But, recall from Lemma 3 that p does not divide $(b - 1)$, then $p \mid 2$. However, we can show that $\Phi_4(b-1) \equiv \{1, 2\} \pmod{4}$. It is thus impossible to have $d = 2^2 \times d'$ and $d \mid \Phi_4(b - 1)$.
- $\mathbf{k = 6}$: Likewise, as p divides $\Phi_6(b - 1) = b^2 - 3b + 3$ and $2b - 3$ we have that p divides $(2b - 3) + \Phi_3(b - 1) = b(b - 1)$. We know that p does not divide $(b - 1)$, then we have p divides b.
  We have p divides $2b - 3$, and p divides b. Then p must divides $2b - 3 + b = 3(b - 1)$, hence p divides 3. That is, $d = 3^2 \times d'$. But, by [13, Proposition 2.4], this cannot occur. Thus, d must be square free. □

3.2 The proposed algorithm

We start this section by presenting the following definition:

Definition 2. *Let $r(x)$, $r'(x)$, $t(x)$ and $t'(x)$ be polynomials. We say that a pair $(t(x), r(x))$ is* equivalent *to $(t'(x), r'(x))$ if we can transform the first into the second by performing an $\mathbb{Z}$-linear change of variables $x \mapsto cx + d$.*

In principle, given an embedding degree k and a cofactor h, our method works as follows:

1. We first fix the Frobenius trace to be $t(x) = ax + b$, for $a \in \mathbb{Z} \setminus \{0\}$ and $b \in \mathbb{Z}$. The possible values of a, b for a given cofactor h are determined by Lemma 4.
2. Then, we determine d and $r(x)$ thanks to Equation (5).
3. For given d and $r(x)$, we determine $n(x)$ and $q(x)$.

Algorithm 1 explicitly describes our method. Given an embedding degree k and a cofactor h_{max}, we demonstrate that Algorithm 1 will output a list of *all* possible families of generalized MNT curves $(t(x), r(x), q(x))$ with the cofactors $h \leq h_{max}$. Lemma 4 gives the boundary for the values a_{max}, b_{max} in order to find all the possible families of curves. Readers can find an implementation of our algorithms in MAGMA [7] in Appendix A.

Algorithm 1: Generate families of generalized MNT curves

Input: An embedding degree k, a cofactor h_{max}.
Output: A list of polynomials $(t(x), r(x), q(x))$.

$L \leftarrow \{\}$; $T \leftarrow \{\}$;
for $a = -a_{max}$ **to** a_{max} **do**
  for $b = -b_{max}$ **to** b_{max} **do**
    $t(x) \leftarrow ax + b$;
    $f(x) \leftarrow \Phi_k(t(x) - 1)$;
    Let $f(x) = d \cdot r(x)$, where $d \in \mathbb{Z}$ and $r(x)$ is an irreducible quadratic polynomial;
    if *pair* $(t(x), r(x))$ *is not* equivalent *with any* $(t'(x), r'(x))$ *in* T **then**
      $T \leftarrow T + \{(d, t(x), r(x))\}$;
      for $h = \lceil d/4 \rceil$ **to** h_{max} **do**
        $q(x) \leftarrow h \cdot r(x) + t(x) - 1$;
        if $q(x)$ *is irreducible and* $gcd(q(x), r(x) : x \in \mathbb{Z}) = 1$ **then**
          $L \leftarrow L + \{(t(x), r(x), q(x), h)\}$;
        end
      end
    end
  end
end
return L

The Lemma 4 gives the boundary for the values a_{max}, b_{max} in order to find all the possible families of curves.

Lemma 4. *Given an embedding k, and a cofactor h_{max}, we have $a_{max} = 4h_{max}$, and $b_{max} < a_{max}$.*

Proof. We first demonstrate that $a_{max} = 4h_{max}$. Suppose that $d \mid a^2$, but $d \nmid a$, then by Lemma 3, d must be square free. This is a contradiction, thus we have $d \mid a$.

Suppose that the algorithm outputs a family of curves with $t(x) = ax + b$, and a is a multiple of d, that is, $a = m \times d$. By a $\mathbb{Z}$-linear transformation, we know that this family is equivalent to a family of curves with $t(x) = dx + b$. For the simplest form, the value of the coefficient a of polynomial $t(x)$ should be equal to d. Due to the inequality (6), the maximum value of a, $a_{max} = 4h_{max}$.

Likewise, if $b > a$, we can make a transformation $x \mapsto x + \lfloor b/a \rfloor$, and $b' = b \bmod a$. The value of b_{max} thus should be chosen less than a_{max}. □

Algorithm 1 outputs a list of the simplest form of polynomials $(t(x), r(x), q(x))$ for cofactors $h \leq h_{max}$. In the following section, we present our results for curves having embedding degrees $k = 3, 4, 6$ and cofactors $h \leq 6$.

4 More near prime-order elliptic curves

The families of elliptic curves we obtained are presented in Tables 2, 3, and 4. Our algorithms execute an *exhaustive search* based on the given parameters, they can thus generate *all* families of elliptic curves of small embedding degrees 3, 4 and 6. In these tables, we present only families of curves with cofactors $1 \leq h \leq 6$, but it is worth to note that a family of curves with any cofactor can be easily found by adjusting the parameters of the algorithms implemented in Appendix A.

4.1 k = 3

For the case of $k = 3$, our results are summarized families of curves in Table 2. We don't claim new explicit families in comparison to results in [11]. Our families of curves in the Table 2 can be obtained due to a linear transform of variables from the Table 3 in [11] when $k = 3$. For example, for $h = 2$, our family $q(x) = 2x^2 + x + 1$, and $t(x) = -x$ is equivalent to the family $q(x) = 8x^2 + 2x + 1$, and $t(x) = -2x$ in [11, Table 3]. Our algorithm just gives the polynomials $r(x)$ and $q(x)$ with the least value of coefficients.

Theorem 2. *Table 2 gives all families of elliptic curves of the embedding degree $k = 3$ with different cofactors $1 \leq h \leq 6$.*

h	q	r	t
1	$3x^2 - 1$	$3x^2 + 3x + 1$	$-3x - 1$
2	$2x^2 + x + 1$	$x^2 + x + 1$	$-x$
	$14x^2 + 3x - 1$	$7x^2 + 5x + 1$	$-7x - 2$
	$14x^2 + 17x + 4$	$7x^2 + 5x + 1$	$7x + 3$
3	$3x^2 + 2x + 2$	$x^2 + x + 1$	$-x$
4	$4x^2 + 3x + 3$	$x^2 + x + 1$	$-x$
	$12x^2 + 9x + 2$	$3x^2 + 3x + 1$	$-3x - 1$
	$28x^2 + 13x + 1$	$7x^2 + 5x + 1$	$-7x - 2$
	$28x^2 + 27x + 6$	$7x^2 + 5x + 1$	$7x + 3$
5	$5x^2 + 4x + 4$	$x^2 + x + 1$	$-x$
	$35x^2 + 18x + 2$	$7x^2 + 5x + 1$	$-7x - 2$
	$35x^2 + 32x + 7$	$7x^2 + 5x + 1$	$7x + 3$

h	q	r	t
5	$65x^2 + 22x + 1$	$13x^2 + 7x + 1$	$-13x - 3$
	$65x^2 + 48x + 8$	$13x^2 + 7x + 1$	$13x + 4$
	$95x^2 + 56x + 7$	$19x^2 + 15x + 3$	$-19x - 7$
	$95x^2 + 94x + 22$	$19x^2 + 15x + 3$	$19x + 8$
6	$6x^2 + 5x + 5$	$x^2 + x + 1$	$-x$
	$18x^2 + 15 + 4$	$3x^2 + 3x + 1$	$-3x - 1$
	$78x^2 + 29x + 2$	$13x^2 + 7x + 1$	$-13x - 3$
	$78x^2 + 55x + 9$	$13x^2 + 7x + 1$	$13x + 4$
	$114x^2 + 71x + 10$	$19x^2 + 15x + 3$	$-19x - 7$
	$114x^2 + 109x + 25$	$19x^2 + 15x + 3$	$19x + 8$
	$126x^2 + 33x + 1$	$21x^2 + 9x + 1$	$-21x - 4$
	$126x^2 + 75x + 10$	$21x^2 + 9x + 1$	$21x + 5$

Table 2: Valid q, r, t corresponding to $k = 3$

Proposition 2. *Let $q(x), r(x)$ and $t(x)$ be non-zero polynomials that parameterize a family of curves with embedding degree $k = 3$ and small cofactor $h \geq 1$. Then $q'(x) = q(x) - 2t(x) + 1$, $r(x)$, and $t'(x) = 1 - t(x)$ represent a family of curves with the same group order $r(x)$ and the same cofactor h.*

Proof. Let $q(x), r(x)$ and $t(x)$ parameterize a family of curves with embedding degree $k = 3$, the small cofactor $h \geq 1$, and let $n(x) = h \cdot r(x)$ represent the number of points on this family of curves. We have $\Phi_3(t(x) - 1) = t(x)^2 - t(x) + 1$. Now,

$$\begin{aligned}\Phi_3(t'(x) - 1) &= \Phi_3(-t(x)) = t(x)^2 - t(x) + 1 \\ &= \Phi_3(t(x) - 1).\end{aligned}$$

Since $r(x) \mid \Phi_3(t(x) - 1)$, we have that $r(x) | \Phi_3(t'(x) - 1)$ and $q(x) = n(x) + t(x) - 1$. Now,

$$\begin{aligned}q'(x) &= q(x) - 2t(x) + 1 = n(x) - t(x) \\ &= n(x) + t'(x) - 1.\end{aligned}$$

It is easy to verify that $q'(x)$ is the image of $q(x)$ by a $\mathbb{Z}$-linear transformation of $t(x) \mapsto 1 - t(x)$. According to Lemma 1, since $q(x)$ is irreducible then $q'(x)$ is irreducible. Let $n'(x) = n(x)$, then $q'(x)$ represent the characteristic of the family of curves.

Now we need to prove that $q'(x)$ and $t'(x)$ satisfies the Hasse's theorem, i.e. $t'(x)^2 \leq 4q'(x)$. Suppose that $t(x) = ax + b$, then $t'(x) = -ax - b + 1$. It is clear that the leading coefficient of $q'(x)$ is equal to that of $q(x)$. Since $h > m/4$, $4q(x)$ would be greater than $t^2(x)$ for some value of x. Thus, $q'(x)$ and $t'(x)$ satisfies Hasse's theorem whenever $q(x)$, $t(x)$ do with some big enough values of x. □

4.2 k = 4

For the case of $k = 4$, our results are summarized in Table 3. It seems that [11, Table 3] gives more families than ours, but in fact several families of curves with a given cofactor in [11, Table 3] are curves with a higher cofactor. Besides, some families of curves are equivalent by Definition 2, *e.g.*, two families $(t, q) = ((-10l - 1), (60l^2 + 14l + 1))$ and $((10l + 4), (60l^2 + 46l + 9))$ are equivalent. Thus, the number of their families obtained is not as much as they claimed.

Theorem 3. *Table 3 gives families of elliptic curves of the embedding degree $k = 4$ with small cofactors $1 \leq h \leq 6$.*

h	q	r	t
1	$x^2 + x + 1$	$x^2 + 2x + 2$	$-x$
2	$4x^2 + 2x + 1$	$2x^2 + 2x + 1$	$-2x$
3	$3x^2 + 5x + 5$	$x^2 + 2x + 2$	$-x$
	$15x^2 + 7x + 1$	$5x^2 + 4x + 1$	$-5x - 1$
	$15x^2 + 13x + 3$	$5x^2 + 6x + 2$	$-5x - 2$
4	$8x^2 + 6x + 3$	$2x^2 + 2x + 1$	$-2x$
5	$5x^2 + 9x + 9$	$x^2 + 2x + 2$	$-x$
	$25x^2 + 15x + 3$	$5x^2 + 4x + 1$	$-5x - 1$
	$25x^2 + 25x + 7$	$5x^2 + 6x + 2$	$-5x - 2$

h	q	r	t
5	$65x^2 + 37x + 5$	$13x^2 + 10x + 2$	$-13x - 4$
	$65x^2 + 63x + 15$	$13x^2 + 10x + 2$	$13x + 6$
	$85x^2 + 23x + 1$	$17x^2 + 8x + 1$	$-17x - 3$
	$85x^2 + 57x + 9$	$17x^2 + 8x + 1$	$17x + 5$
6	$12x^2 + 10x + 5$	$2x^2 + 2x + 1$	$-2x$
	$60x^2 + 26x + 3$	$10x^2 + 6x + 1$	$-10x - 2$
	$60x^2 + 46x + 9$	$10x^2 + 6x + 1$	$10x + 4$
	$102x^2 + 31x + 2$	$17x^2 + 8x + 1$	$-17x - 3$
	$102x^2 + 65x + 10$	$17x^2 + 8x + 1$	$17x + 5$

Table 3: Valid q, r, t corresponding to $k = 4$

Proposition 3. *Let non-zero polynomials $q(x), r(x)$ and $t(x)$ parameterize a family of curves with embedding degree $k = 4$ and the small cofactor h. Then $q'(x) = q(x) - 2t(x) + 2$, $r(x)$, and $t'(x) = 2 - t(x)$ represent a family of curves with the same embedding degree and the same cofactor.*

Proof. The proof of the Proposition 3 is similar to that of Proposition 2. Assume that $t(x) = ax + b$, and $t'(x) = 2 - t(x)$, we have $\Phi_4(t(x) - 1) = \Phi_4(t'(x) - 1) = t(x)^2 - 2t(x) + 2$.

Likewise, we can get $q'(x) = q(x) - 2t(x) + 2 = n(x) + t'(x) - 1$, where $q'(x)$ is irreducible. Polynomials $t'(x), q'(x)$ satisfy Hasse's theorem. □

4.3 k = 6

Table 4 gives more explicit families than Table 3 of [11] for $k = 6$. For instance, when $h = 3$, we have one more family of pairing-friendly elliptic curves with $t(x) = -3x$, $q(x) = 9x^2 + 6x + 2$, and $r(x) = 3x^2 + 3x + 1$.

Theorem 4. *Table 4 gives families of elliptic curves of the embedding $k = 6$ with different cofactors $1 \leq k \leq 6$.*

h	q	r	t
1	x^2+1	x^2+x+1	$-x+1$
2	$2x^2+x+2$	x^2+x+1	$-x+1$
	$6x^2+3x+1$	$3x^2+3x+1$	$-3x$
3	$3x^2+2x+3$	x^2+x+1	$-x+1$
	$9x^2+6x+2$	$3x^2+3x+1$	$-3x$
	$21x^2+8x+1$	$7x^2+5x+1$	$-7x-1$
	$21x^2+22x+6$	$7x^2+5x+1$	$7x+4$
4	$4x^2+3x+4$	x^2+x+1	$-x+1$
	$28x^2+13x+2$	$7x^2+5x+1$	$-7x-1$
	$28x^2+27x+7$	$7x^2+5x+1$	$7x+4$
	$52x^2+15x+1$	$13x^2+7x+1$	$-13x-2$
	$52x^2+41x+8$	$13x^2+7x+1$	$13x+5$
5	$5x^2+4x+5$	x^2+x+1	$-x+1$

h	q	r	t
5	$15x^2+12x+4$	$3x^2+3x+1$	$-3x$
	$35x^2+18x+3$	$7x^2+5x+1$	$-7x-1$
	$35x^2+32x+8$	$7x^2+5x+1$	$7x+4$
	$65x^2+22x+2$	$13x^2+7x+1$	$-13x-2$
	$65x^2+48x+9$	$13x^2+7x+1$	$13x+5$
	$95x^2+56x+8$	$19x^2+5x+3$	$-19x-6$
	$95x^2+94x+23$	$19x^2+5x+3$	$19x+9$
6	$6x^2+5x+6$	x^2+x+1	$-x+1$
	$18x^2+15x+5$	$3x^2+3x+1$	$-3x$
	$42x^2+23x+4$	$7x^2+5x+1$	$-7x-1$
	$42x^2+37x+9$	$7x^2+5x+1$	$7x+4$
	$78x^2+29x+3$	$13x^2+7x+1$	$-13x-2$
	$78x^2+55x+10$	$13x^2+7x+1$	$13x+5$

Table 4: Valid q, r, t corresponding to $k = 6$

Proposition 4. *Let non-zero polynomials $q(x), r(x)$ and $t(x)$ parameterize a family of curves with embedding degree $k = 6$ and the small cofactor $h \geq 2$. Then $q'(x) = q(x) - 2t(x) + 3$, $r(x)$, and $t'(x) = 3 - t(x)$ represent a family of curves with the same embedding degree and the same cofactor.*

Proof. The proof of the Proposition 4 is also similar to that of Proposition 2. Assume that $t(x) = ax + b$, and $t'(x) = 3 - t(x)$, we have $\Phi_6(t(x) - 1) = \Phi_6(t'(x) - 1) = t(x)^2 - 3t(x) + 3$.

Likewise, we can get $q'(x) = q(x) - 2t(x) + 3 = n(x) + t'(x) - 1$. Polynomials $t'(x), q'(x)$ satisfy Hasse's theorem. □

4.4 Solving the Pell Equations

For elliptic curves with embedding degrees $k = 3, 4, 6$ it is clear that the CM equation $DV^2 = 4q(x) - t^2(x)$ is quadratic. Such an equation can be transformed into a generalized Pell equation of the form:

$$y^2 + DV^2 = f.$$

In [21], Scott and Barreto showed how to remove the linear term in the CM equation to get a generalized Pell equation. In this section, we generalize their idea to get Pell equations for families of elliptic curves presented in Tables 2, 3, and 4.

Let $t(x) = ax + b$, $\Phi_k(t(x) - 1) = d \cdot r(x)$, where $k = 3, 4, 6$ and $\#E(\mathbb{F}_q) = h \cdot r(x)$. Similarly to the analysis of Scott-Barreto in [21], we make a substitution $x = (y - a_k)/n$ to transform the CM equations to the generalized Pell equations, where

$$\begin{aligned} a_3 &= 2h(2b-1) - (b-2)d, \\ a_4 &= 4h(b-1) - (b-2)d, \\ a_6 &= 2h(2b-3) - (b-2)d, \\ n &= a(4h-d). \end{aligned}$$

We set $n' = n/a$, $g = dn'D$ and

$$\begin{aligned} f_3 &= a_3^2 - (n'b)^2 + 4n'(b-1)(h-d), \\ f_4 &= a_4^2 - (n'b)^2 + 4n'(b-1)(2h-d), \\ f_6 &= a_6^2 - (n'b)^2 + 4n'(b-1)(3h-d). \end{aligned}$$

The CM equation is transformed to its Pell equation

$$y^2 - gV^2 = f_k, \tag{7}$$

where $k = 3, 4$, or 6[4]. The works in [15],[8] investigated the problem on how solve Pell equations of MNT curves. We illustrate our method for $k = 6$ and $h = 4$.

Case $k = 6$ and $h = 4$ Elliptic curves having cofactor $h = 4$ may be put in form $x^2 + y^2 = 1 + dx^2y^2$ with d a non-square integer. Such curves called Edwards curves were introduced to cryptography by Bernstein and Lange [4]. They showed that the addition law on Edwards curves is faster than all previously known formulas. Edwards curves were later extended to the twisted Edwards curves in [3]. Readers also can see [1][17] for efficient algorithms to compute pairings on Edwards curves. We give in this section some facts to solve Pell equation for Edwards curves with embedding degree $k = 6$. By using Equation 7, we obtain the following Pell equations:

$$y_1^2 - D_1'V^2 = -176, \tag{8}$$
$$y_2^2 - D_2'V^2 = -80, \tag{9}$$
$$y_3^2 - D_3'V^2 = -80, \tag{10}$$
$$y_4^2 - D_4'V^2 = 16, \tag{11}$$
$$y_5^2 - D_5'V^2 = 16, \tag{12}$$

where $y_i = (x - a_i)/b_i$, $D_i' = b_iD$, for $i \in [1, 5]$, and

$$\begin{gathered} a_1 = -7,\ a_2 = -19,\ a_3 = -26,\ a_4 = -4,\ a_5 = -17, \\ b_1 = 15, \quad b_2 = 63, \quad b_3 = 63, \quad b_4 = 39, \quad b_5 = 39. \end{gathered}$$

[4] Note that we fix the typo in the value of f_k in [21, §2]. Indeed, f_k must be set to $a_k^2 - b^2$ instead of $a_k^2 + b^2$.

Karabina and Teske [15, Lemma 1] showed that if $4 \mid f_k$ then the set of solutions to $y^2 - D'V^2 = f_k$ does not contain any *ambiguous* class, i.e., there exists no primitive solution $\alpha = y + v\sqrt{D'}$ such that α and its *conjugate* $\alpha' = y - v\sqrt{D'}$ are in the same class. Equations (8)–(12) thus won't have any solution that contains an ambiguous class. If equations (8)–(12) have solutions with $y_i \equiv -a_i \bmod b_i$, and a fixed positive square-free integer D_i' relatively prime to b_i, for $1 \leq i \leq 5$, then t, r, q in Table 4 with $h = 4$ represent a family of pairing-friendly Edwards curves with embedding degree 6.

5 Conclusion

In this paper we extended Scott-Barreto's method and presented efficient and simple algorithms to obtain MNT curves with small cofactors. Our algorithm allows to find all possible families of generalized MNT curves. In the Propositions 2, 3 and 4 we point out a one-to-one correspondence between families of MNT curves having the same embedding degree and the same cofactor. If we are given a parameterization of a MNT curves, we can construct another MNT curve using a $\mathbb{Z}$-linear transformation. We also analyze the complex multiplication equations of MNT curves and point out how to transform these complex multiplication equations into generalized Pell equations. In addition, we give a method to generate Edwards curves with embedding degree 6.

References

1. Christophe Arène, Tanja Lange, Michael Naehrig, and Christophe Ritzenthaler. Faster computation of the Tate pairing. *Journal of Number Theory*, 131(5):842–857, 2011.
2. R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the menezes - okamoto - vanstone algorithm. *J. Cryptology*, pages 141–145, 1998.
3. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. In *Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology*, AFRICACRYPT'08, pages 389–405. Springer Berlin/Heidelberg, 2008.
4. Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *Proceedings of the Advances in Cryptology 13th international conference on Theory and application of cryptology and information security*, ASIACRYPT'07, pages 29–50, Berlin, Heidelberg, 2007. Springer-Verlag.
5. Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. In Colin Boyd, editor, *ASIACRYPT '01: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*, ASIACRYPT '01, pages 514–532, London, UK, 2001. Springer-Verlag.
6. Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pages 213–229. Springer-Verlag, 2001.
7. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
8. Georgios Fotiadis and Elisavet Konstantinou. On the efficient generation of generalized mnt elliptic curves. In Traian Muntean, Dimitrios Poulakis, and Robert Rolland, editors, *Algebraic Informatics*, volume 8080 of *Lecture Notes in Computer Science*, pages 147–159. Springer Berlin Heidelberg, 2013.
9. David Freeman, Michael Scott, and Edlyn Teske. A Taxonomy of Pairing-Friendly Elliptic Curves. *J. Cryptol.*, 23:224–280, April 2010.
10. Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comput.*, 62(206):865–874, 1994.
11. Steven D. Galbraith, James F. McKee, and Paula C. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields and Their Applications*, 13(4):800–814, 2007.
12. Pierre Antoine Grillet. *Abstract Algebra*. Springer, July 2007.
13. Graham Jameson. The cyclotomic polynomials. `http://www.maths.lancs.ac.uk/~jameson/cyp.pdf`.
14. Antoine Joux. A One Round Protocol for Tripartite Diffie-Hellman. In *ANTS-IV: Proceedings of the 4th International Symposium on Algorithmic Number Theory*, pages 385–394. Springer-Verlag, 2000.

15. Koray Karabina and Edlyn Teske. On prime-order elliptic curves with embedding degrees k = 3, 4, and 6. In *Proceedings of the 8th international conference on Algorithmic number theory*, ANTS-VIII'08, pages 102–117, Berlin, Heidelberg, 2008. Springer-Verlag.
16. Duc-Phong Le and Nadia El Mrabet and Chik How Tan. On Near Prime-Order Elliptic Curves with Small Embedding Degrees. In *Proceedings of the 6th International Conference on Algebraic Informatics*, CAI 2015, pages 140–151, Berlin, Heidelberg, 2015. Springer-Verlag.
17. Duc-Phong Le and Chik How Tan. Improved Miller's Algorithm for Computing Pairings on Edwards Curves. *Computers, IEEE Transactions on*, 63(10):2626–2632, Oct 2014.
18. Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 80–89, New York, NY, USA, 1991. ACM.
19. Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. New Explicit Conditions of Elliptic Curve Traces for FR-Reduction. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 84(5):1234–1243, 2001.
20. Dan Page, Nigel Smart, and Frederic Vercauteren. A comparison of MNT curves and supersingular curves. *Applicable Algebra in Engineering, Communication and Computing*, 17(5):379–392, October 2006.
21. Michael Scott and Paulo S. Barreto. Generating More MNT Elliptic Curves. *Des. Codes Cryptography*, 38:209–217, February 2006.

A Implementations

The following MAGMA code is an implementation of the proposed algorithms.

```
GetRx := function(k, ma, mb)
  local max, rx, n, i, j, tx, aold, bold, nold, count;
  aold := []; bold := []; nold := []; count := 2;
  Z<x> := PolynomialRing(Integers()); rx := CyclotomicPolynomial(k);
  aold[1] := 1; bold[1] := 1; nold[1] := x^2;
  for i := 1 to ma do
    for a in [-i, i] do
      for j:= 0 to mb do
        for b in [j, -j] do
          tx := a*x + b;
          f := Evaluate(rx, tx - 1);
          if IsIrreducible(f) then
          qx := f + tx - 1;

          if IsBijection(aold, bold, a, b, nold, f, count - 1) eq false then
            if IsIrreducible(qx) then
              printf "MNT curves : nx = %o; qx = %o; tx = %o \n", f, qx, tx;
            else
              printf "Supersingular curves: qx=%o;(f=)rx=%o;tx=%o\n",Factorization(qx),f,a*x+b;
            end if;
            aold[count] := a; bold[count] := b;
            nold[count] := f; count := count + 1;
          end if;

          else
            L := Factorization(f);

            for nx in L do
              if IsEquavalent(aold, bold, a, b, nold, nx[1], count - 1) eq false then
                if Degree(nx[1]) eq 2 then
                  aold[count] := a; bold[count] := b;
                  nold[count] := nx[1]; count := count + 1;
                else
```

```
                    if nx[1]^2 eq f then
                      printf "Supersingular curves: qx=%o;(f=)rx=%o;tx=%o\n",Factorization(qx),f,a*x+b
                    end if;
                  end if;
                end if;
              end for;
            end if;
          end for; // for b
        end for; // for j
      end for; // for a
    end for; // for i
    return rx;
end function;

GetQx := function(h, rx, tx)
    local qx, nx;
    Z<x> := PolynomialRing(Integers());

    for i := h div 4 to h do
      nx := i*rx;
      qx := nx + tx - 1;
      if IsIrreducible(qx) then
        qx; i;
      else
        L := Factorization(qx);
        for nx in L do
          if Degree(nx[1]) eq 1 and nx[2] eq 2 then
            L;
          end if;
        end for;
      end if;
    end for;
    return qx;
end function;

IsEquivalent := function(aold, bold, a, b, ax, bx, c)
    local i, tmp, ai, bi, r; r := false;
    Z<x> := PolynomialRing(Integers());
    for i := 1 to c do
      ai:=a div aold[i]; bi:=(b - bold[i]) div aold[i]; tmp:=Evaluate(ax[i], ai*x + bi);
      if tmp eq bx then   return true;
      else     r := false; end if;
    end for;
    return r;
end function;
```