On the near prime-order MNT curves

Duc-Phong Le[1], Nadia El Mrabet[2], Safia Haloui[3], Chik How Tan[4]

1 Institute for Infocomm Research, Singapore
2 Ecole des Mines de St Etienne, France
3 Ecole des Mines de St Etienne, France
4 National University of Singapore, Singapore

* ledp@i2r.a-star.edu.sg

Abstract

In their seminar paper, Miyaji, Nakabayashi and Takano introduced the first method to construct families of prime-order elliptic curves with small embedding degrees, namely $k = 3, 4$, and 6. These curves, so-called MNT curves, were then extended by Scott and Barreto, and also Galbraith, McKee and Valença to near prime-order curves with the same embedding degrees. In this paper, we extend the method of Scott and Barreto to introduce an *explicit* and *simple* algorithm that is able to generate *all* families of MNT curves with *any* given cofactor. Furthermore, we analyze the number of potential families of these curves that could be obtained for a given embedding degree k and a cofactor h. We then discuss the generalized Pell equations that allow us to construct particular curves. Finally, we provide statistics of the near prime-order MNT curves.

1 Introduction

Cryptographic pairings were first introduced by Menezes, Okamato and Vanstone in [18] and Frey and Ruck in [9] as a means of attacking discrete logarithm based cryptosystems. The authors showed that the discrete logarithm problem on a supersingular elliptic curve could be reduced to the discrete logarithm problem in a finite field through the Weil and Tate pairings. Cryptographic pairings on elliptic curves then become a great interest for cryptographic constructions when Joux [14] introduced the first one-round 3-party Diffie-Hellman key exchange protocol in 2000. Since then, pairing-based cryptography has had a huge success with some notable breakthroughs such as the first practical Identity-based Encryption (IBE) scheme [5]. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with a subgroup of big prime order r. We have:

$$\#E(\mathbb{F}_q) = h \times r,$$

where h is known as the cofactor. In pairing based cryptography, the elliptic curves used have to fulfill a *special* property, namely, the embedding degree k is small enough[1]. This ensures that cryptographic pairings are efficient, that is, computable over the extension finite field. An elliptic curve with such a nice property is called a *pairing-friendly* elliptic curve.

In [19], Miyaji *et al.* introduced the first method that is able to systematically construct ordinary (non-supersingular) elliptic curves of prime order with small embedding degrees $k = 3, 4$ and 6. Their curves, so-called MNT curves, are over fields with large prime characteristic q, and the number of points on these curves $E(\mathbb{F}_q)$ is *prime*, that is, the cofactor $h = 1$. As analyzed in [21], these families of curves are more efficient than supersingular elliptic curves when implementing pairing-based cryptosystems. Scott *et al.* in [22], and Galbraith *et al.* in [10] found more ordinary curves of these embedding degrees where the group order $n = \#E(\mathbb{F}_q) = h \times r$ is 'nearly prime', that is, r is a prime and $h > 1$ is small.

---

[1]The embedding degree is the smallest integer k such that r divides $(q^k - 1)$.

1.1 Contributions

While Galbraith *et al.* use the same *analytic* technique as in [19] to generate more families of curves with small cofactors $2 \leq h \leq 5$, Scott *et al.*'s method applies the Hasse's bound to generate specific elliptic curves, i.e., actual parameters q, r, h and D (see [22, Section 3]). This paper is an extension from our seminar paper presented at CAI'15 [16]. In this paper, we first extend Scott-Barreto's method [22] to introduce an *explicit* and *simple* algorithm that allows us to generate families of near prime-order MNT curves. Given an embedding degree k and *any* cofactor $h_{max} \geq 1$, we will show that our algorithm is able to effectively generate *all* families of near prime-order MNT curves having cofactors $h \leq h_{max}$. Furthermore, we provide explicit formulas for the number of these families. 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. Last but not least, we provide some statistics of these near prime-order MNT curves.

1.2 Organization

The paper is organized as follows: Section2 briefly recalls MNT curves, as well as methods to generate MNT curves with small cofactors. Section 3 describes our algorithm. We present our families of near prime-order MNT curves in Section 4. We also discuss the number of potential families and the Pell equations for some particular cases of MNT curves in this section. Statistics for near prime-order MNT curves are provided in Section 5. Finally, we conclude in Section 6.

2 Background

Let $E(\mathbb{F}_q)$ be an elliptic curve defined over the finite field $\mathbb{F}_q$, where q is a large prime number. Let t define trace and r be a prime factor of $\#E(\mathbb{F}_q)$. Let k be the embedding degree. E is a pairing-friendly elliptic curve if its embedding degree k is small enough. Balasubramanian and Koblitz [2] pointed out that ordinary elliptic curves generated randomly would have a large embedding degree. Consequently, these curves would not be suitable for efficient computation of a pairing based protocol. Ordinary elliptic curves with small embedding degrees thus require specific constructions.

2.1 MNT curves

In [19], Miyaji, Nakabayashi, and Takano presented such a construction that yields ordinary elliptic curves with embedding degree $k \in \{3, 4, 6\}$. More particularly, their curves are of prime-order, i.e., the ρ-value is 1 where the value ρ is defined as $\rho = \frac{\log(q)}{\log(r)}$. This is an interest in some applications such as short signatures [6].

The families of MNT curves are parametrized by q and t as polynomials in $\mathbb{Z}[x]$ with $\#E(\mathbb{F}_q) = n(x)$. We recall that $n(x) = q(x) + 1 - t(x)$, $n(x) \mid \Phi_k(q(x))$, where $\Phi_k(q(x))$ is the k-th cyclotomic polynomial of $q(x)$, 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]

2.2 Near prime-order MNT curves

Let $E(\mathbb{F}_q)$ be a parameterized elliptic curve with cardinality $\#E(\mathbb{F}_q) = n(x)$. We define the cofactor of $E(\mathbb{F}_q)$ as 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 [22], and Galbraith-McKee-Valença [10] extended the MNT idea by allowing small values of the cofactor $h > 1$. This allows us to find many more suitable curves with $\rho \approx 1$ than the original MNT construction.

Definition 2.1 *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. We call E a near prime order curve if its group order $\#E(\mathbb{F}_q)$ is 'nearly prime', that is, $\#E(\mathbb{F}_q) = h \times r$ where r is a large prime number and h is a small integer.*

2.2.1 Scott-Barreto's method

Let $\Phi_k(x) = d \times r$ for some x. Scott-Barreto's method [22] 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:

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

Scott and Barreto used the fact that $\Phi_k(t-1) \equiv 0 \pmod{r}$ (see Proposition 2.1). As above, the right-hand side of the equation (1) is quadratic, and hence, it can be transformed into a generalized Pell equation by a linear substitution (see [22, §2] for more details). Then, Scott-Barreto found integer solutions to this equation for small enough D (to facilitate the CM algorithm) and arbitrary m with the constraint $4h > d$. The Scott-Barreto's method [22] presented near prime-order MNT elliptic curves with actual parameters, but did not give explicit families of near prime-order MNT elliptic curves.

Proposition 2.1 *[8, 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 $\Phi_k(t-1) \equiv 0 \pmod{r}$.*

2.2.2 Galbraith McKee and Valença's method

Unlike Scott-Barreto's method, the mathematical analyses in [10] could lead to explicit families of near prime-order MNT curves. Galbraith *et al.* [10] extended the MNT method [19] and gave a complete characterization of MNT curves with small cofactors $2 \le h \le 5$. As in [19], their analysis applies the fact that $\Phi_k(q) \equiv 0 \pmod{r}$. Similar 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, $|t| \le 2\sqrt{q}$, they then analyzed and derived possible polynomials q, t from the equation $\Phi_k(q) = \lambda r$. Readers are referred to [10, Section 3] for a particular analysis in the case, in which the embedding degree is $k = 6$ and the cofactor is $h = 2$. Their results about curves having embedding degrees $k = 3, 4, 6$ with cofactors $2 \le h \le 5$ was summarized in [10, Table 3].

3 Algorithm

In this section, we present an alternative approach to generate *explicit* families of ordinary elliptic curves having the embedding degrees $3, 4$, or 6 and small cofactors. Unlike the analytic approach in [10], we obtain families of curves by presenting a very *simple* and *explicit* algorithm. Given *any* cofactor, our analyses also show that this algorithm is able to effectively find all families of near prime-order MNT elliptic curves.

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 $k = 3, 4, 6$:

$$\Phi_k(t(x) - 1) = t(x)^2 - \varepsilon t(x) + \varepsilon,$$

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

$$\Phi_k(t(x) - 1) = a^2 x^2 + a(2b - \varepsilon)x + \Phi_k(b - 1), \tag{2}$$

where $\varepsilon = 1$ (resp. 2, 3) for $k = 3$ (resp. 4, 6).

Theorem 3.1 *The quadratic polynomials $\Phi_k(t(x) - 1)$ for $k = 3, 4, 6$ are irreducible over the rational field.*

Proof We start with the following lemma that we use later to prove Theorem 3.1.

Lemma 3.2 *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 3.1. As the polynomial $\Phi_k(x) = x^2 - \varepsilon x + \varepsilon$ is irreducible in $\mathbb{Q}[x]$, according to Lemma 3.2 the polynomial $\Phi_k(t(x) - 1)$ is also irreducible in $\mathbb{Q}[x]$. ∎

Let a triple (t, r, q) parameterize a family of near prime-order 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, $n(x) = h \times r(x) = q(x) - t(x) + 1$. By Definition 2.7 in [8], we have:

$$\Phi_k(t(x) - 1) = d \times r(x), \tag{3}$$

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:

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

From Eq. (2), we can see that d is the greatest common divisor (GCD) of the coefficients appearing in this equation. 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 [11, Chapter V, §6]:

Lemma 3.3 *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 In the case of $k = 6$, suppose that $\Phi_6(ax + b') = d \times r(x)$, where $b' = b - 1$. Then d will be the greatest common divisor of a^2, $a(2b' + 1)$ and $\Phi_6(b')$. Moreover, either $d|6$ or $d \equiv 1 \pmod 6$.

Lemma 3.4 *Given $t(x) = ax + b$, if d in Eq. (3) 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 $\Phi_k(b - 1)$ (Eq. (2)). 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 3.3, 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.

- **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 $(b-1)$, and thus p must divide b.

  We have $p \mid 2b - 1 = (b-1) + b$, and $p \mid b$, and hence, p must divide $b - 1$. This contradicts with Lemma 3.3. Thus, d is square free.

- **k = 4**: We have that p divides $2(b-1)$. But, recall from Lemma 3.4 that p does not divide $(b-1)$, then $p \mid 2$. However, we can show that $\Phi_4(b - 1) \equiv \{1, 2\}$ (mod 4). It is thus impossible to have $d = 2^2 \times d'$ and $d \mid \Phi_4(b-1)$.

- **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 $(b-1)$, and so we have p divides b.

  We have p divides $2b - 3$, and p divides b, so p must divides $2b - 3 + b = 3(b-1)$. Likewise, p does not divide $(b-1)$, and so p divides 3, that is, $d = 3^2 \times d'$. But, by [20, Theorem 95], this cannot occur. Thus, d must be square free. ∎

3.2 The proposed algorithm

We start this section by presenting the following definition:

Definition 3.1 *Let* $t(x), t'(x), r(x), r'(x)$ *be polynomials with integer coefficients.*

- *The 2-tuple* $(t(x), r(x))$ *is deduced from* $(t'(x), r'(x))$ *if* $(t(x), r(x)) = (t'(ux + v), r'(ux + v))$, $u, v \in \mathbb{Z}$, $u \neq 0$.

- Equivalence relation*: The 2-tuple* $(t(x), r(x))$ *is equivalent to* $(t'(x), r'(x))$ *if both tuples can be deduced from each other, or equivalently, if* $(t(x), r(x)) = (t'(\pm x + v), r'(\pm x + v))$, $v \in \mathbb{Z}$.

- *The 2-tuple* $(t(x), r(x))$ *is primitive if it cannot be deduced from a non-equivalent tuple.*

Algorithm 1 explicitly describes our method. Given an embedding degree k and a cofactor h_{max}, Algorithm 1 will output a list of *all* possible families of near prime-order MNT curves $(t(x), r(x), q(x))$ with the cofactors $h \leq h_{max}$.

Algorithm 1: Generate families of near prime-order 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 $(t(x), r(x))$ *couldnt be deduced from any 2-tuple* $(t'(x), r'(x))$ *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

Basically, given an embedding degree k and a maximum cofactor h_{max}, our method works as follows:

1. Firstly, we set the Frobenius trace polynomial 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 3.5.

2. Next, we determine d and $r(x)$ thanks to Eq. (3).

3. If 2-tuple $(t(x), r(x))$ could not be deduced from any 2-tuple in the list T, Algorithm 1 adds this tuple into the list. This ensures that the algorithm does not generate any equivalent family of curves (see more details in Section 4).

4. Then, for given $t(x), r(x)$ and d, we compute the corresponding polynomials $q(x)$ for all cofactors $h \leq h_{max}$.

Algorithm 1 involves two parameters a_{max} and b_{max}. The following section will discuss these values.

3.3 Completeness

The Lemma 3.5 gives the boundary for the values a_{max}, b_{max} in order to find all the possible families of curves.

Lemma 3.5 *Given an embedding degree 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 3.4, d must be square free. This is a contradiction, and 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 (4), 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}. ∎

4 Families of near prime-order MNT curves

Algorithm 1 outputs a list of primitive polynomials $(t(x), r(x), q(x))$ for all cofactors $h \leq h_{max}$. The families of elliptic curves having embedding degrees $k = 3, 4, 6$ and cofactors $h \leq 6$ are summarized in Table 2. Our algorithm executes an *exhaustive search* based on the given parameters, and thus it is able to 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 given any cofactor, families of near prime-order MNT curves can be easily found by adjusting the parameters of Algorithm 1.

Theorem 4.1 *Table 2 gives all families of elliptic curves of the embedding degrees $k = 3, 4, 6$ with different cofactors $1 \leq h \leq 6$.*

In comparison to results in [10, Table 3], note that we provide the *primitive* polynomials of $t(x)$, $r(x)$ and $q(x)$ as defined in Definition 3.1. For example, for $h = 2$, $k = 3$, the family with parameters $q(x) = 8x^2 + 2x + 1$, and $t(x) = -2x$ in [10, Table 3] can be deduced to our family with parameters $q(x) = 2x^2 + x + 1$, and $t(x) = -x$. For the case of $k = 4$, even though Table 3 in [10] listed more families than our results, several families of their curves with a given cofactor in [10, Table 3] are curves with a higher cofactor. For example, when the cofactor is stated 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 equal to 4. This mismatch between the stated cofactor and the real one comes from the fact that in GMV's method the polynomial $r(x)$ does not necessarily represent primes.

We list here the similar cases in Table 3 of [10] 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 cases, the cofactors are in fact higher than that claimed in [10, Table 3]. Besides, some families of curves are equivalent by Definition 3.1. For example, the two families $(t, q) = ((-10x - 1), (60x^2 + 14x + 1))$ and $((10x + 4), (60x^2 + 46x + 9))$ are equivalent. As a result, the number of elliptic curve families is fewer than their claimed number.

Proposition 4.2 *Let $q(x), r(x)$ and $t(x)$ be non-zero polynomials that parameterize a family of near prime-order MNT curves in Table 2. Then $q'(x) = q(x) - 2t(x) + \varepsilon$, $r(x)$, and $t'(x) = \varepsilon - t(x)$ represent a family of curves with the same group order $r(x)$ and the same cofactor h, where $\varepsilon = 1$ (resp. 2, and 3) for $k = 3$ (resp. 4, and 6).*

Proof Let $q(x), r(x)$ and $t(x)$ parameterize a family of curves with embedding degrees $k = 3, 4$ or 6, a small cofactor $h \geq 1$, and let $n(x) = h \cdot r(x)$ represent the number of points on this family of curves. From Eq. (2), we have $\Phi_k(t(x) - 1) = t(x)^2 - \varepsilon t(x) + \varepsilon$. Now,

$$\Phi_k(t'(x) - 1) = \Phi_k(\varepsilon - t(x) - 1) = t(x)^2 - \varepsilon t(x) + \varepsilon$$
$$= \Phi_k(t(x) - 1).$$

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

$$q'(x) = q(x) - 2t(x) + \varepsilon = n(x) - t(x) + \varepsilon - 1$$
$$= n(x) + t'(x) - 1.$$

It is easy to verify that $q'(x)$ is the image of $q(x)$ by a $\mathbb{Z}$-linear transformation of $t(x) \mapsto \varepsilon - t(x)$. According to Lemma 3.2, since $q(x)$ is irreducible, it follows that $q'(x)$ is also irreducible. If $n'(x) = n(x)$, then the quadratic polynomial $q'(x)$ represents the characteristic of the family of curves.

Now we need to prove that $q'(x)$ and $t'(x)$ satisfy 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 $t'(x)$ satisfy Hasse's theorem whenever $q(x), t(x)$ involve some big values of x. ∎

h	k=3			k=4			k=6		
	q	**r**	**t**	**q**	**r**	**t**	**q**	**r**	**t**
1	$3x^2-1$	$3x^2+3x+1$	$-3x-1$	x^2+x+1	x^2+2x+2	$-x$	x^2+1	x^2+x+1	$-x+1$
2	$2x^2+x+1$	x^2+x+1	$-x$	$4x^2+2x+1$	$2x^2+2x+1$	$-2x$	$2x^2+x+2$	x^2+x+1	$-x+1$
	$14x^2+3x-1$	$7x^2+5x+1$	$-7x-2$				$6x^2+3x+1$	$3x^2+3x+1$	$-3x$
	$14x^2+17x+4$	$7x^2+5x+1$	$7x+3$						
3	$3x^2+2x+2$	x^2+x+1	$-x$	$5x^2+9x+9$	x^2+2x+2	$-x$	$3x^2+2x+3$	x^2+x+1	$-x+1$
				$25x^2+15x+3$	$5x^2+4x+1$	$-5x-1$	$9x^2+6x+2$	$3x^2+3x+1$	$-3x$
				$25x^2+25x+7$	$5x^2+6x+2$	$-5x-2$	$21x^2+8x+1$	$7x^2+5x+1$	$-7x-1$
							$21x^2+22x+6$	$7x^2+5x+1$	$7x+4$
4	$4x^2+3x+3$	x^2+x+1	$-x$	$8x^2+6x+3$	$2x^2+2x+1$	$-2x$	$4x^2+3x+4$	x^2+x+1	$-x+1$
	$12x^2+9x+2$	$3x^2+3x+1$	$-3x-1$				$28x^2+13x+2$	$7x^2+5x+1$	$-7x-1$
	$28x^2+13x+1$	$7x^2+5x+1$	$-7x-2$				$28x^2+27x+7$	$7x^2+5x+1$	$7x+4$
	$28x^2+27x+6$	$7x^2+5x+1$	$7x+3$				$52x^2+15x+1$	$13x^2+7x+1$	$-13x-2$
							$52x^2+41x+8$	$13x^2+7x+1$	$13x+5$
5	$5x^2+4x+4$	x^2+x+1	$-x$	$5x^2+9x+9$	x^2+2x+2	$-x$	$5x^2+4x+5$	x^2+x+1	$-x+1$
	$35x^2+18x+2$	$7x^2+5x+1$	$-7x-2$	$25x^2+15x+3$	$5x^2+4x+1$	$-5x-1$	$15x^2+12x+4$	$3x^2+3x+1$	$-3x$
	$35x^2+32x+7$	$7x^2+5x+1$	$7x+3$	$25x^2+25x+7$	$5x^2+6x+2$	$-5x-2$	$35x^2+18x+3$	$7x^2+5x+1$	$-7x-1$
	$65x^2+22x+1$	$13x^2+7x+1$	$-13x-3$	$65x^2+37x+5$	$13x^2+10x+2$	$-13x-4$	$35x^2+32x+8$	$7x^2+5x+1$	$7x+4$
	$65x^2+48x+8$	$13x^2+7x+1$	$13x+4$	$65x^2+63x+15$	$13x^2+10x+2$	$13x+6$	$65x^2+22x+2$	$13x^2+7x+1$	$-13x-2$
	$95x^2+56x+7$	$19x^2+15x+3$	$-19x-7$	$85x^2+23x+1$	$17x^2+8x+1$	$-17x-3$	$65x^2+48x+9$	$13x^2+7x+1$	$13x+5$
	$95x^2+94x+22$	$19x^2+15x+3$	$19x+8$	$85x^2+57x+9$	$17x^2+8x+1$	$17x+5$	$95x^2+56x+8$	$19x^2+5x+3$	$-19x-6$
							$95x^2+94x+23$	$19x^2+5x+3$	$19x+9$
6	$6x^2+5x+5$	x^2+x+1	$-x$	$12x^2+10x+5$	$2x^2+2x+1$	$-2x$	$6x^2+5x+6$	x^2+x+1	$-x+1$
	$18x^2+15+4$	$3x^2+3x+1$	$-3x-1$	$60x^2+26x+3$	$10x^2+6x+1$	$-10x-2$	$18x^2+15x+5$	$3x^2+3x+1$	$-3x$
	$78x^2+29x+2$	$13x^2+7x+1$	$-13x-3$	$60x^2+46x+9$	$10x^2+6x+1$	$10x+4$	$42x^2+23x+4$	$7x^2+5x+1$	$-7x-1$
	$78x^2+55x+9$	$13x^2+7x+1$	$13x+4$	$102x^2+31x+2$	$17x^2+8x+1$	$-17x-3$	$42x^2+37x+9$	$7x^2+5x+1$	$7x+4$
	$114x^2+71x+10$	$19x^2+15x+3$	$-19x-7$	$102x^2+65x+10$	$17x^2+8x+1$	$17x+5$	$78x^2+29x+3$	$13x^2+7x+1$	$-13x-2$
	$114x^2+109x+25$	$19x^2+15x+3$	$19x+8$				$78x^2+55x+10$	$13x^2+7x+1$	$13x+5$
	$126x^2+33x+1$	$21x^2+9x+1$	$-21x-4$						
	$126x^2+75x+10$	$21x^2+9x+1$	$21x+5$						

Table 2: Valid q, r, t corresponding to the embedding degrees $k = 3, 4, 6$

4.1 The number of potential families

Let $k \in \{3, 4, 6\}$. The families with parameters $(t(x), r(x), q(x))$ of near prime-order MNT curves built by Algorithm 1 are characterized by the following properties :

(1) $t(x) = ax + b$, $a, b \in \mathbb{Z}$, $a \neq 0$,

(2) $r(x)$ is the $\mathbb{Z}$-irreducible polynomial such that $\Phi_k(t(x) - 1) = d \times r(x)$ for some $d \in \mathbb{N}$,

(3) $q(x) = hr(x) - t(x) - 1$, where h is a positive integer satisfying $4h \geq d$.

If h is a fixed positive integer, we see that the number of such families is equal to

$$\sum_{d=1}^{4h} N_d,$$

where N_d is the number of primitives classes having a representation $(t(x), r(x))$ satisfying properties (1) and (2). The purpose of this section is to give an explicit formula for the value of N_d. Let us recall equations (2) and (3) in Section 3.1:

$$\Phi_k(t(x) - 1) = a^2 x^2 + a(2b - \varepsilon)x + \Phi_k(b - 1),$$

where $\varepsilon = 1$ (resp. 2, 3) for $k = 3$ (resp. 4, 6). The integer d, satisfying the equation

$$\Phi_k(t(x) - 1) = d \times r(x)$$

is the gcd of a^2, $a(2b - \varepsilon)$ and $\Phi_k(b - 1)$. It is proved in Lemmas 3.3 and 3.4 that d divides a, so d is also the gcd of a and $\Phi_k(b - 1)$. Moreover, it is easy to see that $(t(x), r(x))$ is always deduced from the couple $(dx + b, \Phi_k(dx + b - 1)/d)$, so any primitive couple must have $a = d$, or equivalently, $a | \Phi_k(b - 1)$.

Lemma 4.3 *Let d be a fixed positive integer. We have*

$$N_d = \#\{b \mod d, \quad d \mid \Phi_k(b - 1)\}.$$

Proof Taking into account the discussion above, it is easy to check that we have a bijection between the set of primitives classes having a representation $(t(x), r(x))$ satisfying (1) and (2) and $\{b \mod d, \quad d \mid \Phi_k(b - 1)\}$ which is given by $(t(x), r(x)) \mapsto b \mod d$.

Proposition 4.4 *Let d be a fixed positive integer and write $d = p^{u_0} q_1^{u_1} \ldots q_s^{u_s}$, where p is the biggest prime factor of k (so $p = 2$ or 3), $q_1, \ldots, q_s$ are distinct primes and distinct from p, and $u_0, \ldots, u_s \in \mathbb{N}$. We have that*

$$N_d = \begin{cases} 1 & \text{if } d = 1 \text{ or } d = p, \\ 2^s & \text{if } q_i \equiv 1 \mod k, i = 1, \ldots, s, \text{ and } u_0 \leq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof By Lemma 4.3, we are reduced to find the number of elements in the set $\{a \mod d, \quad d \mid \Phi_k(a)\}$. We remark that it is trivial that $N_1 = 1$. For the higher value of d, we will make use of the results from [20].

• Case $d = p$: Let $k = mp^e$, $p \nmid m$ (so $m = 1$ or 2). There is exactly one $a \in \mathbb{Z}/p\mathbb{Z}$ such that $\text{ord}_p(a) = m$, so by [20, Theorem 95], we have $N_p = 1$.

• Case $d = p^{u_0}$: We have $N_{p^{u_0}} = 0$ by [20, Theorem 95].

• Case $d = q$, q prime distinct from p: By [20, Theorem 95], N_q is the number of $a \in \mathbb{Z}/q\mathbb{Z}$ such that $\text{ord}_p(a) = k$, which is equal to $\varphi(k) = 2$ if $q \equiv 1 \mod k$ and 0 otherwise.

• Case $d = q^u$, q prime distinct from p: By Hansel's Lemma, we have $N_{q^u} = N_q$ (Hansel's Lemma applies because the only prime factor of the discriminant of Φ_k is p).

• General case: By the Chinese Remainder Theorem, we have $N_{p^{u_0} q_1^{u_1} \ldots q_s^{u_s}} = N_{p^{u_0}} N_{q_1^{u_1}} \ldots N_{q_s^{u_s}}$. ∎

4.2 Solving the Pell Equations

Solving the Pell equations for MNT curves was studied in papers [15] and [7]. The authors proved that MNT curves are *sparse*, that is, Pell equations admit only a few solutions. In this section, we extend their ideas to solve the Pell equations for near prime-order MNT curves.

Let $t(x) = ax + b$, $\Phi_k(t(x) - 1) = d \cdot r(x)$, where $k = 3, 4, 6$ and $\#E(\mathbb{F}_q) = h \cdot r(x)$. Let $\varepsilon = 1$ (resp. 2, and 3) when $k = 3$ (resp. 4, and 6). In order to remove the linear term in the CM equation $Dm^2 = 4q(x) - t^2(x)$ of the near prime order MNT curves, we substitute $x = (y - a_k)/n$, where $n = a(4h - d)$, and $a_k = 2h(2b - \varepsilon) - (b - 2)d$ for $k = 3, 4$, or 6. The CM equation can be transformed into a generalized Pell equation of the form:

$$y^2 - gm^2 = f_k, \tag{5}$$

where $g = d(4h - d)D$ and $f_k = a_k^2 - ((4h - d)b)^2 + 4(4h - d)(b - 1)(\varepsilon h - d)$.

By fixing $a = 1$ and $b = 1$, one can get the values a_k and f_k as analyzed in [22, Section 2]. Note that there is a typo in the value of f_k in [22, Section 2]. Indeed, f_k must be set to $a_k^2 - b^2$ instead of $a_k^2 + b^2$. The following section illustrates our method for $k = 6$ and $h = 4$ as follows.

4.2.1 Case $k = 6$ and $h = 4$

Elliptic curves with the cofactor $h = 4$ may be put in the 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 Eq. (5), we obtain the following Pell equations:

$$y_1^2 - g_1 m^2 = -176, \tag{6}$$
$$y_2^2 - g_2 m^2 = -80, \tag{7}$$
$$y_3^2 - g_3 m^2 = -80, \tag{8}$$
$$y_4^2 - g_4 m^2 = 16, \tag{9}$$
$$y_5^2 - g_5 m^2 = 16, \tag{10}$$

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

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

Karabina and Teske [15, Lemma 1] showed that if $4 \mid f_k$, then the set of solutions to $y^2 - gm^2 = f_k$ does not contain any *ambiguous* class, i.e., there exists no primitive solution $\alpha = y + v\sqrt{g}$ such that α and its *conjugate* $\alpha' = y - v\sqrt{g}$ are in the same class. Consequently, equations (6)–(10) do not have any solution that contains an ambiguous class.

If equations (6)–(10) have solutions with $y_i \equiv -a_i \bmod b_i$, and a fixed positive square-free integer g_i relatively prime to b_i, for $1 \leq i \leq 5$, then triple t, r, q in Table 2 with $k = 6$ and $h = 4$ represent a family of pairing-friendly Edwards curves with embedding degree 6.

5 Statistics of near prime-order MNT curves

In [13], Jiménez Urroz, Luca and Shparlinski provided statistics of MNT curves in the case $k = 6$. In this section, we generalize their arguments to the near prime-order MNT curves.

Theorem 5.1 ([13], Theorem 8) *Let $E(z)$ be the number of MNT curves with $k = 6$ and co-factor $h = 1$ having CM discriminant less than z. Then, assuming the Generalized Bateman-Horn Conjecture, the lower bound*

$$E(z) \geq (\mathfrak{S}_0 + o(1))\frac{\sqrt{z}}{\log z},$$

holds as $z \to \infty$, where $\mathfrak{S}_0 \simeq 0.237615$.

5.1 Assumptions

Let D denote the CM discriminant. We first rewrite Eq. (5) in the following form:

$$\Delta(x) = Dum^2, \tag{11}$$

where $\Delta(x) = (w_0 x + w_1)^2 + w_2$, $w_0 = a(4h - d)$, $w_1 = b(4h - d)2(\varepsilon h - d)$, $w_2 = 4h(4 - \varepsilon)(\varepsilon h - d)$, $u = d(4h - d)$, and parameters a, b, h, d and ϵ are defined as in Section 4.2. Note that these parameters were straightforwardly deduced from Eq. (5).

In order to fulfil the conditions of the *generalized Bateman-Horn conjecture* given in [13, Section 3.4], we assume that the products $r(n)q(n)\Delta(n)$, $n \in \mathbb{Z}$ have no fixed prime divisor. We have the following lemma whose proof is straightforward.

Lemma 5.2 *Under the above assumptions, for any prime p and any integer β such that $\Delta(\beta) = 0$ mod p^2, we have $\Delta'(\beta) \neq 0 \mod p$.*

Proof If p is an odd prime that doesnt divide the leading coefficient of $\Delta(x)$, then the equation $\Delta(x) = 0$ mod p^2 is equivalent to $(\Delta'(x))^2 - \mathrm{Disc}(\Delta(x)) = 0 \mod p^2$, and we see that if this equation has a solution β such that $\Delta'(\beta) = 0 \mod p$, then p^2 must divide $\mathrm{Disc}(\Delta(x))$.

If p is an odd prime dividing the leading coefficient of $\Delta(x)$. Under these conditions, it is easy to check that if $\Delta(x)$ has a root modulo p, then either $\Delta(x)$ is identically zero modulo p (which is excluded, since $\Delta(x)$ is irreducible over $\mathbb{Z}[x]$), or $\Delta'(x)$ has no root modulo p.

Finally, we can easily check that $\Delta(x)$ has no root modulo 2. ∎

Similar to Jiménez Urroz *et al.*'s analysis, we proceed in two steps:

- in the first step, let m be an fixed integer, $B(m)$ be the set of residues module m^2, and let $\beta \in B(m)$. We seek to estimate $E_{m,\beta}(z)$, the number of positive integers of the form $n = \beta + km^2$ that satisfies the following conditions:

  (1) $q(n)$ is prime,
  (2) $r(n)$ is prime,
  (3) $\Delta(n)/m^2$ is a square-free integer $\leq z$, for some positive integer m.

- the second step will give a lower bound of the sum of all the $E_{m,\beta}(z)$.

5.2 Preparations

If $n = \beta + km^2$ (that is, $n \equiv \beta \mod m^2$) satisfying the above conditions (1)–(3), then from Eq. (11), the class of n modulo m^2 is an element of the set $B(m)$ of solutions of the following equation:

$$\Delta(n) = 0 \mod m^2 \tag{12}$$

From the condition $D \leq z$, we get

$$w_0^2 k^2 m^4 \leq \Delta(n) \leq zum^2$$

11

so $k \leq \sqrt{zu}/(w_0 m)$. If the conditions (1)–(3) were independent events, the number of positive integers of the form $n = \beta + km^2$ satisfying these conditions would behave like

$$F_{m,\beta}(z) = \frac{\sqrt{zu}}{\zeta(2)w_0 m (\log(zm^2))^2}.$$

However, these events are actually not independent, so the estimate $F_{m,\beta}(z)$ needs to be corrected by a constant which takes in account the local behaviors of $q(n)$, $r(n)$, $\Delta(n)/m^2$. This gives:

$$E_{m,\beta}(z) \sim \prod_p \left(1 - \frac{N_{m,p}}{p^2}\right)\left(1 - \frac{1}{p}\right)^{-2} \frac{\sqrt{zu}}{w_0 m (\log(zm^2))^2},$$

where $N_{m,p}$ is the number of solutions in the arithmetic progression $n = \beta \mod m^2$ of the congruence

$$(q(n)r(n))^2 \frac{\Delta(n)}{m^2} = 0 \mod p^2. \tag{13}$$

Let C_p be the number of solutions of the congruence:

$$(q(n)r(n))^2 \Delta(n) = 0 \mod p^2. \tag{14}$$

1. If $p \nmid m$, then we see that $N_{m,p} = C_p$. The C_p's can be computed by using the fact that almost all primes p divide at most one of $q(n)$, $r(n)$ and $\Delta(n)$, and for these primes, we can get the solutions of (14) by counting separately the roots of $q(n)$, $r(n)$ and $\Delta(n)$ modulo p. In particular, we have $C_p = O(p)$. The remaining primes should be treated "by hand" (such primes must divide $2u$ or the resultant of two polynomials in $\{q(n), r(n), \Delta(n)\}$).

2. If $p \mid m$, then we have two possibilities:

   (i) either $p \mid q(\beta)$ (resp. $p \mid r(\beta)$) and then $q(\beta + km^2) \in \mathbb{Z}[k]$ (resp. $r(\beta + km^2)$) does not take any prime value (this can happen only for a finite number of primes, namely, the primes which divide $\mathrm{Res}\,(q(x), \Delta(x))\,\mathrm{Res}\,(r(x), \Delta(x))$);

   (ii) or $p \nmid q(\beta)r(\beta)$, so $p \nmid q(n)r(n)$ for any $n = \beta + km^2$ and the Hansel's Lemma and Lemma 5.2 ensure that there exists an unique solution modulo p^2 to the equation

   $$\frac{\Delta(\beta + km^2)}{m^2} = 0 \mod p^2,$$

   and therefore, we have $N_{m,p} = 1$.

5.3 Lower bound on near prime-order MNT curves

Let $\beta \in B'_m = \{\beta \in B_m \mid \forall p \text{ dividing } m, q(\beta)r(\beta) \neq 0 \mod p\}$, and define $\rho(m) = \#B'_m$. The following lemma gives some basic properties of the function ρ:

Lemma 5.3 *Let $\beta \in B'_m = \{\beta \in B_m \mid \forall p \text{ dividing } m, q(\beta)r(\beta) \neq 0 \mod p\}$. The function $\rho(m) = \#B'_m$ verifies that:*

1. *The function ρ is multiplicative.*

2. *For almost all primes, we have $\rho(p^e) = \rho(p)$, $\forall e \in \mathbb{N}^*$.*

3. Let w_2' be the product of the odd prime divisors of the non-square part of w_2 and $\ell = 2\varphi(w_2')$. Then there exist exactly ℓ classes $c_1, \ldots, c_\ell$ modulo $8w_2'$ (which can be explicitly computed) such that for almost all primes, we have

$$\rho(p) = \begin{cases} 2 & \text{if } p = c_i \mod 8w_2', \text{ for some } i \in \{1, \ldots, \ell\}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof Point (1) follows directly from the Chinese Remainder Theorem. For almost all primes p and all $e \in \mathbb{N}$, $\rho(p^e)$ is just the number of solutions to (12) with $m = p^e$, so point (2) follows from the Hansel Lemma. As for point (3), notice that for almost all primes p, the number of solutions to $\Delta(x) = 0$ mod p is 2 if $-w_2$ is a square modulo p, and 0 otherwise. We conclude the proof by using the Law of Quadratic Reciprocity. ∎

Let $E(z)$ be the number of near prime order MNT curves having CM discriminant $D < z$ and let M be an integer. We have

$$E(z) \geq \sum_{m \leq M} \sum_{\beta \in B_m} E_{m,\beta}(z) \geq \mathfrak{S}_1 \frac{\sqrt{zu}}{w_0} \sum_{m \leq M} \frac{f(m)}{m(\log(zm^2))^2} \tag{15}$$

where

$$\mathfrak{S}_1 = \prod_p \left(1 - \frac{C_p}{p^2}\right)\left(1 - \frac{1}{p}\right)^{-2},$$

and

$$f(m) = \prod_{p|m} \left(1 - \frac{1}{p}\right)^2 \left(1 - \frac{C_p}{p^2}\right)^{-1} \rho(p),$$

With the notation of Lemma 5.3, we have

$$f(p) = \begin{cases} 2 + O(1/p) & \text{if } p = c_i \mod 8w_2', \text{ for some } i \in \{1, \ldots, \ell\}, \\ 0 & \text{otherwise.} \end{cases} \tag{16}$$

Now, let

$$S(t) = \sum_{m \leq t} \mu(m)^2 \frac{f(m)}{m},$$

where μ is the Möbius function. By using (16), we can follow exactly the method given at the beginning of the proof of [13], Theorem 8. This gives

$$S(t) = \mathfrak{S}_2 \log(t) + O(1), \tag{17}$$

where

$$\mathfrak{S}_2 = \prod_p \left(1 - \frac{1}{p}\right)\left(1 + \frac{f(p)}{p}\right) \tag{18}$$

Still following the proof of [13], Theorem 8, we use the partial summation (see [12], Section 1.5) and Equation 17 we found that

$$\sum_{m \leq M} \mu(m)^2 \frac{f(m)}{m(\log(zm^2))^2} \geq \frac{\mathfrak{S}_2}{2}\left(\frac{-1}{\log(zM^2)} + \frac{1}{\log(z)}\right) + O\left(\frac{1}{\log(z)^2}\right) \tag{19}$$

Taking $M = z^{1/2}$ in (19), we get the following theorem.

13

Theorem 5.4 *Let $E(z)$ be the number of curves in the family with parameters (t, r, q) polynomials in x, an embedding degree k and a co-factor h having discriminant D less than z. Given:*

$$\mathfrak{S}_1 = \prod_p \left(1 - \frac{C_p}{p^2}\right) \left(1 - \frac{1}{p}\right)^{-2},$$

and

$$\mathfrak{S}_2 = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \frac{f(p)}{p}\right).$$

Then, the lower bound

$$E(z) \geq (\mathfrak{S}_0 + o(1)) \frac{\sqrt{z}}{\log(z)},$$

holds as $z \to \infty$, where $\mathfrak{S}_0 = \frac{\sqrt{u}}{4w_0} \mathfrak{S}_1 \mathfrak{S}_2$.

6 Conclusion

In this paper, we first extended Scott-Barreto's method and presented an explicit and efficient algorithm that is able to generate all families of the near prime-order MNT curves, given an embedding degree k and a cofactor h. Furthermore, we provided explicit formulas for the number of these families. Then, we analyzed the generalized Pell equations of these curves. Finally, we gave statistics of the near prime-order MNT curves.

References

[1] C. Arène, T. Lange, M. Naehrig, and C. Ritzenthaler. Faster computation of the Tate pairing. *Journal of Number Theory*, 131(5):842–857, 2011.

[2] R. Balasubramanian and N. Koblitz. The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem Under the Menezes–Okamoto–Vanstone Algorithm. *Journal of Cryptology*, 11(2):141–145, Mar. 1998.

[3] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. 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] D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In *Proceedings of the Advances in Crypotology 13th international conference on Theory and application of cryptology and information security*, ASIACRYPT'07, pages 29–50, Berlin, Heidelberg, 2007. Springer-Verlag.

[5] D. Boneh and M. 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.

[6] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In C. 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.

[7] G. Fotiadis and E. Konstantinou. On the efficient generation of generalized mnt elliptic curves. In T. Muntean, D. Poulakis, and R. Rolland, editors, *Algebraic Informatics*, volume 8080 of *Lecture Notes in Computer Science*, pages 147–159. Springer Berlin Heidelberg, 2013.

[8] D. Freeman, M. Scott, and E. Teske. A Taxonomy of Pairing-Friendly Elliptic Curves. *J. Cryptol.*, 23:224–280, April 2010.

[9] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comput.*, 62(206):865–874, 1994.

[10] S. Galbraith, J. McKee, and P. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields and Their Applications*, 13(4):800–814, 2007.

[11] P. A. Grillet. *Abstract Algebra*. Springer, July 2007.

[12] H. Iwaniec and E. Kowalski. *Analytic Number Theory*. Number vol. 53 in American Mathematical Society colloquium publications. American Mathematical Society, 2004.

[13] J. Jiménez Urroz, F. Luca, and I. E. Shparlinski. On the number of isogeny classes of pairing-friendly elliptic curves and statistics of MNT curves. *Mathematics of Computation*, 81(278):1093–1110, 2012.

[14] A. 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] K. Karabina and E. 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] D.-P. Le, N. E. Mrabet, and C. H. Tan. On near prime-order elliptic curves with small embedding degrees. In *Algebraic Informatics - 6th International Conference, CAI 2015, Stuttgart, Germany, September 1-4, 2015. Proceedings*, pages 140–151, 2015.

[17] D.-P. Le and C. H. Tan. Improved Miller's Algorithm for Computing Pairings on Edwards Curves. *IEEE Transactions on Computers*, 63(10):2626–2632, Oct 2014.

[18] A. Menezes, S. Vanstone, and T. 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] A. Miyaji, M. Nakabayashi, and S. 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] T. Nagell. *Introduction to Number Theory*. New York: Wiley, 1951.

[21] D. Page, N. Smart, and F. Vercauteren. A comparison of MNT curves and supersingular curves. *Applicable Algebra in Engineering, Communication and Computing*, 17(5):379–392, October 2006.

[22] M. Scott and P. S. Barreto. Generating More MNT Elliptic Curves. *Des. Codes Cryptography*, 38:209–217, February 2006.