On the Efficient Generation of Generalized MNT Elliptic Curves

Georgios Fotiadis Elisavet Konstantinou *

May 23, 2013

Abstract

Finding suitable elliptic curves for pairing-based cryptosystems is a crucial step for their actual deployment. Miyaji, Nakabayashi and Takano [11] (MNT) were the first to produce ordinary pairing-friendly elliptic curves of prime order with embedding degree $k \in \{3, 4, 6\}$. Scott and Barreto [15] as well as Galbraith et al. [9] extended this method by allowing the group order to be non-prime. The advantage of this idea is the construction of much more suitable elliptic curves, which we will call *generalized MNT curves*. A necessary step for the construction of such elliptic curves is finding the solutions of a generalized Pell equation. However, these equations are not always solvable and this fact considerably affects the efficiency of the curve construction. In this paper we discuss a way to construct generalized MNT curves through Pell equations which are always solvable and thus considerably improve the efficiency of the whole generation process. We provide analytic tables with all polynomial families that lead to non-prime pairing-friendly elliptic curves with embedding degree $k \in \{3, 4, 6\}$ and discuss the efficiency of our method through extensive experimental assessments.

Keywords: Pairing-based cryptography, MNT elliptic curves, effective polynomial families, Pell equations.

1 Introduction

Pairing-based cryptography has gained much interest during the past few years. Several pairing-based protocols have been proposed such as the well known Boneh et al.'s ID-based encryption [4] and short signatures schemes [5]. All these cryptographic schemes are based on the construction of elliptic curves that satisfy certain properties. Clearly, generating suitable elliptic curves for pairing-based cryptosystems is a very important issue in pairing-based cryptography. These curves are known as *pairing-friendly* elliptic curves [7].

Let $E/\mathbb{F}_q$ be an elliptic curve of order $\#E(\mathbb{F}_q) = n$ defined over a prime field $\mathbb{F}_q$. In most pairing-based cryptographic protocols the ideal case is to construct elliptic curves of prime order. However, such curves are rare and so the ideal case is hard to achieve in practice. To this end we may relax this condition and allow the use of curves with $\#E(\mathbb{F}_q) = hr$ for a small cofactor $h > 1$ and r a large prime. The ρ-value is defined as $\rho = \log(q)/\log(r)$ and shows how close to the ideal case is the constructed curve. Clearly, we require the ρ-value to be as

*Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Karlovassi, Samos, Greece. Emails: {gfotiadis, ekonstantinou} @aegean.gr

close to 1 as possible. Furthermore, let $E[r]$ denote the set of r-torsion points of $E/\mathbb{F}_q$. Then the embedding degree of $E[r]$ is the smallest positive integer $k > 1$, such that $E[r] \subseteq E(\mathbb{F}_{q^k})$, or equivalently the smallest positive integer such that $r \mid q^k - 1$, where $\mathbb{F}_{q^k}$ is a finite extension of $\mathbb{F}_q$ of degree k. According to [7], an elliptic curve E defined over a prime field $\mathbb{F}_q$ with small embedding degree and large prime order subgroup is called pairing-friendly.

A well known method to construct elliptic curves over a large prime field is the Complex Multiplication (CM) method [1]. By Hasse's theorem, $Z = 4q - t^2$ must be positive and, thus, there is a unique factorization $Z = DY^2$, with D a square free positive integer. Therefore

$$4q = t^2 + DY^2 \tag{1}$$

is satisfied for a given pair (q, t). The negative parameter $-D$ is called a *CM discriminant for the prime* q. For convenience throughout the paper, we will use (the positive integer) D to refer to the CM discriminant. Knowing the values of q and t, an elliptic curve E defined over $\mathbb{F}_q$ with $n = q + 1 - t$ number of $\mathbb{F}_q$-rational points can be constructed. The triple (q, t, n) represents the curve parameters, i.e. the order of the finite field, the Frobenius trace and the group order of $E(\mathbb{F}_q)$ respectively.

A pairing on an elliptic curve $E/\mathbb{F}_q$ is a map of the form $e : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k}) \to \mathbb{F}^*_{q^k}$ which is bilinear, non-degenerate and efficiently computable. As mentioned in [15] the most commonly used pairings are the Weil and Tate pairings [**?**, 8], while most recent implementations include the Eta and the Ate pairings [**?**, **?**]. In order to use pairings in cryptography, we must guarantee that the discrete logarithm problem (DLP) in both $E(\mathbb{F}_q)[r]$ and $\mathbb{F}^*_{q^k}$ is computationally infeasible. Thus the embedding degree must be chosen to be large enough in order to keep the DLP in $\mathbb{F}^*_{q^k}$ as hard as possible, but also k must be small enough for the efficient arithmetic in $\mathbb{F}^*_{q^k}$. As stated in [15], a good choice for an 80-bit security level is $\log r \approx 160$ and $k \log q \approx 1024$ bits, so that the cryptosystem can resist attacks both in elliptic curve groups and in finite fields.

Miyaji, Nakabayashi and Takano in 2001 [11] were the first who proposed a method (the so called MNT method) for the construction of prime order pairing-friendly elliptic curves with embedding degrees $k \in \{3, 4, 6\}$. Using the CM equation (1) and representing the elliptic curve parameters (q, t, n) as polynomials in $\mathbb{Z}[x]$, they created three Pell-type equations, one for each $k \in \{3, 4, 6\}$. The solutions of these equations lead to potential suitable curve parameters (q, t, n). Scott and Barreto [15] extended the idea of Miyaji et al. by allowing the group order to contain a large prime factor r and a positive small integer $h > 1$ called *cofactor*. In particular, they describe an explicit algorithm that constructs more Pell-type equations for $h > 1$, whose solutions lead to the generation of much more suitable elliptic curves when $k \in \{3, 4, 6\}$. Galbraith, McKee and Valença [9] also extended the MNT method for $k \in \{3, 4, 6\}$ by using non-prime elliptic curves. The difference of their work from [15] is that Galbraith et al. represent the curve parameters (q, t, r) as polynomial families $(q(x), t(x), r(x))$. In their paper they give all polynomial families for $h \in \{2, 3, 4, 5\}$ when $k \in \{3, 4, 6\}$. In [6], Duan, Cui and Wah Chan present a general algorithm for the construction of pairing friendly elliptic curves with arbitrary embedding degree and similarly to [9] they represent the curve parameters as polynomial families. In their method they also construct Pell-type equations from which they obtain suitable curve parameters. Furthermore they introduce the term of *effective polynomial families* by inducing some restrictions on the choice of polynomials $(q(x), t(x), r(x))$.

In this paper we further investigate the construction of generalized MNT elliptic curves with embedding degree $k \in \{3, 4, 6\}$ by using quadratic families that have better chances in producing suitable elliptic curve parameters. In particular we extend the idea of effective polynomial families, first introduced in [6], and enhance them with the ability to lead to generalized Pell equations which are always solvable. The solutions of these Pell equations can be tested for suitability in more than one quadratic families. This observation increases the chances of finding suitable parameters and speeds up the method considerably. While previous works in [9, 15] study cases where $h \leq 5$ we extend the search to families with larger cofactors $h > 5$, but not too large since we wish to keep the ρ-value as close to one as possible. The advantage of our method is that we avoid solving Pell equations leading to a small number of suitable curve parameters. We also present experimental evidence that our method can considerably speed up the generation of generalized MNT elliptic curves.

The paper is organized as follows. In Section 2 we present previous work for the generation of MNT elliptic curves with embedding degree $k \in \{3, 4, 6\}$. In Section 3 we describe our method for the construction of generalized MNT curves. In Section 4 we present our experimental results and we conclude the paper in Section 5.

2 Previous Work

In this section we give a brief overview of previous work concerning the generation of pairing-friendly elliptic curves with embedding degree $k \in \{3, 4, 6\}$. All methods share a common characteristic: in order to generate the curve parameters, they use the solutions of some Pell-type equations. These equations are of the form

$$X^2 - SDY^2 = m \tag{2}$$

where $S, m \in \mathbb{Z}$ and $S > 0$. The integer D represents the CM discriminant and it is positive and square-free. If a Pell equation of this form is solvable, then there is an infinite number of integral pairs (X_i, Y_i) satisfying it. For more detailed analysis on the theory of Pell equations the interested reader can consult [12]. Throughout the paper we will consider elliptic curves E defined over a finite field $\mathbb{F}_q$ where q is a large prime and $\#E(\mathbb{F}_q) = n = hr$ for some large prime r and a cofactor $h \geq 1$.

Miyaji, Nakabayashi and Takano were the first to describe a method for producing ordinary pairing-friendly elliptic curves of prime order with embedding degree $k \in \{3, 4, 6\}$ (e.g. $\#E(\mathbb{F}_q) = n$ is a large prime number). In their work they represent the values (q, t) as polynomials $q(x), t(x) \in \mathbb{Z}[x]$, such that the polynomial $n(x) = q(x) + 1 - t(x)$ divides $\Phi_k(q(x))$, where $\Phi_k(x)$ is the k^{th}-cyclotomic polynomial for $k \in \{3, 4, 6\}$. When the polynomial $q(x)$ is quadratic, we will refer to the families $(q(x), t(x), n(x))$ as *quadratic polynomial families*.

Table 1: **MNT Families**

k	**q(x)**	**t(x)**	**n(x)**	**Pell Equation**	**Suitable X**
3	$12x^2 - 1$	$\pm 6x - 1$	$12x^2 \pm 6x + 1$	$X^2 - 3DY^2 = 24$	$X = 6x \pm 3$
4	$x^2 + x + 1$	$-x, x + 1$	$x^2 + 2x + 2, x^2 + 1$	$X^2 - 3DY^2 = -8$	$X = 3x + 2, 3x + 1$
6	$4x^2 + 1$	$\pm 2x + 1$	$4x^2 \pm 2x + 1$	$X^2 - 3DY^2 = -8$	$X = 6x \mp 1$

The quadratic polynomial families of Miyaji et al. are presented in Table 1 and are known as the MNT families. For any pair $(q(x), t(x))$ of Table 1 substitute them into the CM equation (Eq. 1) to get

$$4q(x) - t^2(x) = DY^2 \tag{3}$$

Multiplying by a constant factor and completing the squares yields to the Pell-type equations of Table 1. We refer to these equations as the MNT equations. Suppose that the integral pair (X_i, Y_i) represents a solution of an equation in Table 1, for some $i \in \mathbb{N}$. Then check if there is an integer x_0 such that X_i is suitable, i.e. if it is written in the form given in the last column of Table 1. If such a x_0 exists, substitute x_0 into the corresponding polynomials $q(x), t(x)$ and $r(x)$ and check if $q(x_0)$ is prime, $|t(x_0)| \leq 2\sqrt{q(x_0)}$ and $n(x_0)$ is also prime. If these conditions hold, the triple $(q(x_0), t(x_0), n(x_0))$ represents the suitable elliptic curve parameters. An implementation of the MNT method can be found in [10].

In [15], Scott and Barreto argue that by using the MNT method we can find few curves for actual deployment and furthermore these are the only curves available if we insist on constructing prime order pairing-friendly elliptic curves with $k \in \{3, 4, 6\}$. To overcome this problem, they generalized the method by allowing the use of curves with nearly prime order, i.e. $\#E(\mathbb{F}_q) = n = hr$ where r is a large prime and $h > 1$. Note that in this case the field size q satisfies the relation $q = hr + t - 1$. The advantage of this idea is the construction of more Pell-type equations leading to the generation of much more suitable curve parameters.

Since the group $E(\mathbb{F}_q)$ has a subgroup of prime order r and k is the embedding degree of this subgroup, we must have $r \mid q^k - 1$ and $r \nmid q^i - 1$ for any $i \in \{1, \ldots, k-1\}$, according to the definition of the embedding degree. This condition is equivalent to $r \mid \Phi_k(t-1)$ and $r \nmid \Phi_i(t-1)$ for any $i \in \{1, \ldots, k-1\}$, as shown in Lemma 1 in [2]. Thus we may assume that $\Phi_k(t-1) = ar$ for some positive integer a. Now substitute q, $x = t - 1$ and $r = \Phi_k(t-1)/a$ into Eq. (1) to obtain the equivalent equation

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

By setting $x = (X - a_k)/(4h - a)$, $\lambda = -2\lfloor k/2 \rfloor + 4$, $a_k = \lambda h + a$ and $f_k = a_k^2 - (4h - a)^2$ Eq. (4) is transformed into

$$X^2 - a(4h - a)DY^2 = f_k. \tag{5}$$

This equation has the form of Eq. (2) where D is the CM discriminant. Thus $a(4h - a) > 0$ forcing $a < 4h$. If the above Pell equation is solvable for some values D, h and a with solution an integral pair (X_i, Y_i), then it is checked if $x_0 = (X_i - a_k)/(4h - a)$ is integer. If this is the case, check if $q = hr + x_0$ is prime and $r = \Phi_k(x_0)/a$ is also prime. As mentioned in [15], we may further relax the condition on the group order by allowing r to contain itself a large prime factor, i.e. $r = ms$, for some $m \geq 1$ and s a large prime. If both conditions hold, the integers (q, t, r) are suitable elliptic curve parameters.

Galbraith, McKee and Valença [9] (GMV) also generalize the MNT method by using non-prime elliptic curves. In their work they present a complete characterization of all polynomial families $(q(x), t(x), r(x))$ with cofactors $h \in \{2, 3, 4, 5\}$ for cases where $k \in \{3, 4, 6\}$. Their polynomial families appear in [9] and lead to the same Pell equations as in the case of Scott and Barreto method. In order to find suitable curve parameters for a fixed embedding degree k and a cofactor h, the GMV method proceeds as the original MNT method.

In [6], Duan, Cui and Wah Chan present an alternative way for producing pairing-friendly elliptic curves with arbitrary embedding degree k. Following the same approach as [9], they

represent the curve parameters as polynomials $q(x), t(x), r(x) \in \mathbb{Z}[x]$. Furthermore they introduce the concept of *effective polynomial families*. According to their definition a polynomial family $(q(x), t(x), r(x))$ is called effective if the polynomial $f(x) = 4q(x) - t^2(x)$ can be factorized with one square polynomial, or it is quadratic and factorable, or it only contains terms with smaller degree compared to $q(x)$. An example for the first case is studied by Barreto and Naehrig in [3] for $k = 12$. Duan et al. argue that an effective polynomial family has better chances in producing suitable elliptic curve parameters.

Although the method of Duan et al. is suitable for any k we focus on the case where $k \in \{3, 4, 6\}$. If we substitute $q(x) = hr(x) + 1 - t(x)$ in Eq. (3) we have that

$$f(x) = DY^2 = 4hr(x) - (t(x) - 2)^2. \tag{6}$$

Then, we choose a quadratic polynomial $r(x)$ and since we wish r to be prime, the polynomial $r(x)$ must be irreducible over $\mathbb{Z}[x]$. A linear trace polynomial $t(x)$ must also be chosen, such that $r(x) \mid \Phi_k(t(x) - 1)$. Knowing $r(x)$ and $t(x)$ we may compute $f(x)$ and $q(x)$. Since $\deg r(x) = 2$, the polynomial $f(x)$ is quadratic and a generalized Pell equation should be solved. Using the solutions of these equations we may search for suitable curve parameters in the usual way.

3 The Proposed Method

We focus on the generation of pairing-friendly elliptic curves with embedding degree $k \in \{3, 4, 6\}$ and we determine a way to construct quadratic polynomial families that have better chances in producing suitable elliptic curve parameters. To this end we adopt the remarks from the work of Duan, Cui and Wah Chan [6] about effective polynomial families. In our study we will consider effective polynomial families where the polynomial $f(x) = 4q(x) - t^2(x)$ is quadratic and factorable. We present a complete characterization of all such polynomial families and we argue that these families lead to a special kind of Pell equations which are always solvable and this fact considerably improves the efficiency of the whole generation method. We also extend the ideas presented in the previous section by allowing the cofactor to take values larger than the ones studied by Scott and Barreto and Galbraith et al. i.e. $h > 5$. We begin our study by analyzing the case $k = 6$, while the same ideas hold for the other two cases $k \in \{3, 4\}$.

3.1 The case of k = 6

Suppose that $q(x), t(x), r(x) \in \mathbb{Z}[x]$ is a polynomial representation for the field size, the trace polynomial and the subgroup order respectively. Let a be a positive integer and suppose that the trace polynomial is linear of the form $t(x) = ax + b$ for some $b \in \mathbb{Z}$. Substitute $t(x) - 1$ into $\Phi_6(x)$ to obtain

$$\Phi_6(t(x) - 1) = a^2x^2 + a(2b - 3)x + b^2 - 3b + 3. \tag{7}$$

Since $\Phi_6(t(x) - 1)$ must be divisible by $r(x)$, we may set

$$r(x) = ax^2 + (2b - 3)x + \frac{b^2 - 3b + 3}{a}. \tag{8}$$

and thus a must be chosen such that the congruence $b^2 - 3b + 3 \equiv 0 \bmod a$ is satisfied for some $b \in \mathbb{Z}$. The polynomial $r(x)$ is irreducible over $\mathbb{Z}[x]$, since its discriminant is equal to $\Delta_r = -3 < 0$. Because $r(x)$ represents the order of a subgroup of $E(\mathbb{F}_q)$, it has to represent primes and therefore the condition that $r(x)$ is irreducible over $\mathbb{Z}[x]$ is essential. We may then assume that the order of $E(\mathbb{F}_q)$ is given by a small integer cofactor h times the polynomial $r(x)$, i.e. $\#E(\mathbb{F}_q) = hr(x)$. Now substitute $r(x)$ into $q(x) = hr(x) + t(x) - 1$ to obtain the corresponding field polynomial

$$q(x) = ahx^2 + (2bh - 3h + a)x + \frac{b^2h - 3bh + 3h + ab - a}{a}. \tag{9}$$

Note that $(b^2h - 3bh + 3h + ab - a)/a \in \mathbb{Z}$, since we have chosen $a \mid (b^2 - 3b + 3)$. Furthermore the field size must be prime and thus the polynomial $q(x)$ must be irreducible over $\mathbb{Z}[x]$. This means that the integer $\Delta_q = (a - h)^2 - 4h^2$ must not be a perfect square and also the coefficients of $q(x)$ must not have a common factor. Now substitute $q(x)$ and $t(x)$ into Eq. (3) represented in polynomial field and set $f(x) = 4q(x) - t^2(x)$. We obtain the quadratic polynomial

$$f(x) = a(4h - a)x^2 + 2\big((4h - a)b + 2a - 6h\big)x + \frac{(4h - a)b^2 + 2(2a - 6h)b + 12h - 4a}{a}.$$

Table 2: **Some effective polynomial families for k = 6**

h	**t(x)**	**q(x)**	**r(x)**	**Pell Equation**
4	$13x + 5$	$52x^2 + 41x + 8$	$13x^2 + 7x + 1$	$(39x + 17)^2 - 39DY^2 = 4^2$
	$13x + 11$	$52x^2 + 89x + 38$	$13x^2 + 19x + 7$	$(39x + 35)^2 - 39DY^2 = 4^2$
9	$31x + 7$	$279x^2 + 130x + 15$	$31x^2 + 11x + 1$	$(155x + 43)^2 - 155DY^2 = 12^2$
	$31x + 27$	$279x^2 + 490x + 215$	$31x^2 + 51x + 21$	$(155x + 143)^2 - 155DY^2 = 12^2$
12	$39x + 18$	$468x^2 + 435x + 101$	$39x^2 + 33x + 7$	$(117x + 56)^2 - 39DY^2 = 4^2$
	$39x + 24$	$468x^2 + 579x + 179$	$39x^2 + 45x + 13$	$(117x + 74)^2 - 39DY^2 = 4^2$
16	$49x + 20$	$784x^2 + 641x + 131$	$49x^2 + 37x + 7$	$(735x + 302)^2 - 735DY^2 = 8^2$
	$49x + 32$	$784x^2 + 1025x + 335$	$49x^2 + 61x + 19$	$(735x + 482)^2 - 735DY^2 = 8^2$
25	$79x + 25$	$1975x^2 + 1254x + 199$	$79x^2 + 47x + 7$	$(1659x + 533)^2 - 1659DY^2 = 20^2$
	$79x + 57$	$1975x^2 + 2854x + 1031$	$79x^2 + 111x + 39$	$(1659x + 1205)^2 - 1659DY^2 = 20^2$
25	$91x + 11$	$2275x^2 + 566x + 35$	$91x^2 + 19x + 1$	$(819x + 131)^2 - 819DY^2 = 40^2$
	$91x + 18$	$2275x^2 + 916x + 92$	$91x^2 + 33x + 3$	$(819x + 194)^2 - 819DY^2 = 40^2$
	$91x + 76$	$2275x^2 + 3816x + 1600$	$91x^2 + 149x + 61$	$(819x + 716)^2 - 819DY^2 = 40^2$
	$91x + 83$	$2275x^2 + 4166x + 1907$	$91x^2 + 163x + 73$	$(819x + 779)^2 - 819DY^2 = 40^2$
36	$109x + 47$	$3924x^2 + 3385x + 730$	$109x^2 + 91x + 19$	$(3815x + 1647)^2 - 3815DY^2 = 12^2$
	$109x + 65$	$3924x^2 + 4681x + 1396$	$109x^2 + 127x + 37$	$(3815x + 2277)^2 - 3815DY^2 = 12^2$

Since $\deg f(x) = 2$, this will lead us to a generalized Pell equation. Following the definition of Duan et al. when $f(x)$ is factorable over $\mathbb{Z}[x]$ we have better chances in finding suitable pairing-friendly elliptic curves and in this case the triple $(q(x), t(x), r(x))$ is an effective polynomial family. In particular suppose that the above polynomial $f(x)$ is factorable over $\mathbb{Z}[x]$. Then the integer $\Delta_f = 16h(a - 3h)$ must be positive and perfect square. Moreover

since $\Delta_f > 0$ we get that $a > 3h$. Multiplying the relation $f(x) = 4q(x) - t^2(x) = DY^2$ by $a(4h-a)$, completing the squares and setting $X = a(4h-a)x + (4h-a)b + 2a - 6h$ we obtain an equation of the form

$$X^2 - a(4h-a)DY^2 = \left(2\sqrt{h(a-3h)}\right)^2. \tag{10}$$

This is a generalized Pell equation and in fact it is the same as the one found by Scott and Barreto, since $f_6 = 4h(a-3h)$. The difference is that we consider these equations only when f_6 is a perfect square. Furthermore, combining the two inequalities for a we conclude that an equation of the form of Eq. (10) is possible, if a is chosen in the range $3h < a < 4h$.

Conversely, suppose that the polynomial $f(x)$ is quadratic of the form $f(x) = ax^2+bx+c \in \mathbb{Z}[x]$ that leads to a generalized Pell equation of the form $X^2 - SDY^2 = m$ with m a perfect square. Multiply $f(x)$ by $4a$ and complete the squares to obtain the Pell equation $(2ax+b)^2 - aD(2Y)^2 = b^2 - 4ac$ where $S = a$ and $m = b^2 - 4ac$. Since m is a perfect square, we have that the integer $b^2 - 4ac$ must be a perfect square which in turn means that $f(x)$ is factorable over $\mathbb{Z}[x]$. Hence we have shown that in order to get a generalized Pell equation of the form of Eq. (10) we must have $f(x)$ factorable and thus $h(a-3h)$ must be a perfect square. The above discussion actually indicates that these are the only Pell equations of this form for $k = 6$. We conclude that *all* effective polynomial families for $k = 6$ have the next parametric polynomial representation

$$\begin{aligned} t(x) &= ax + b \\ r(x) &= ax^2 + (2b-3)x + \frac{b^2 - 3b + 3}{a} \\ q(x) &= ahx^2 + (2bh - 3h + a)x + \frac{b^2h - 3bh + 3h + ab - a}{a} \end{aligned}$$

where the following conditions must be satisfied: (i) the integer $h(a-3h)$ is a perfect square, (ii) the congruence $b^2 - 3b + 3 \equiv 0 \bmod a$ is solvable, (iii) the integer $(a-h)^2 - 4h^2$ is not a perfect square and (iv) the coefficients of $q(x)$ have no common factor. The last two conditions guarantee that $q(x)$ has no constant or linear factors. Some examples of Pell equations of the form of Eq. (10), obtained by effective polynomial families are given in Table 2.

Pell equations of the form of Eq. (10) are considered as a special case and this is because they have a very usefull advantage compared to others. In particular consider the standard Pell equation

$$U^2 - a(4h-a)DV^2 = 1. \tag{11}$$

By Theorem 4.1 [13] Eq. (11) is always solvable for every positive integer D, such that $a(4h-a)D$ is not a perfect square. Suppose that the pairs (U_i, V_i) define a sequence of solutions for Eq. (11), with $i \in \mathbb{N}$. Then the pairs $(X_i, Y_i) = (2\sqrt{h(a-3h)}U_i, 2\sqrt{h(a-3h)}V_i)$ represent the corresdonding solutions of the generalized Pell equation (10). Thus there is always at least one class of solutions for Eq. (10) arising from the units in the quadratic field $\mathbb{Q}(\sqrt{a(4h-a)D})$. Of course in most cases there are more than one classes of solutions. This is a very important observation because the more integer solutions we have to test, the more possibilities we have to generate suitable curve parameters. Once a solution (X_i, Y_i) of the appropriate size is obtained, we follow the standard MNT method in order to construct the curve parameters. More precisely check if there is a $x_0 \in \mathbb{Z}$ such that X_i is written

as $X_i = a(4h-a)x_0 + (4h-a)b + 2a - 6h$, for some $b \in \mathbb{Z}$ satisfying the congruence $b^2 - 3b + 3 \equiv 0 \bmod a$. If such a x_0 exists, substitute into $q(x)$ and $r(x)$ and check if $q(x_0)$ is prime and $r(x_0)$ is prime or nearly prime.

The above procedure generalizes the work of Duan et al. [6] since it defines a parametric representation of all effective polynomial families $(q(x), t(x), r(x))$ such that $f(x)$ is quadratic and factorable. This analysis also shows that for a chosen pair (a, h) such that $h(a-3h)$ is a perfect square and $b^2 - 3b + 3 \equiv 0 \bmod a$ is solvable there are more than one effective polynomial families and the number of these families depends on the number of different $b \in \mathbb{Z}_a$ satisfying the above congruence. All these different families lead to the same generalized Pell equation. For example the effective polynomial family proposed in [6] for $k = 6$, $h = 9$ and $t(x) = 31x + 7$ is not the only one. In Table 2 we have shown that there is a second family for $t(x) = 31x + 27$. Thus in our case we solve this generalized Pell equation only once and we are searching for suitable values $q(x_0)$ and $r(x_0)$ for all effective polynomial families leading to this Pell equation. Following the strategy of Duan et al., the same Pell equation may be solved more than once which induces a considerable delay in the execution time.

3.2 The case of $\mathbf{k = 3, 4}$

For the cases where $k = 3, 4$ we follow the same arguments as in the case of $k = 6$. In particular when $k = 3$ we may represent the quadratic families $(q(x), t(x), r(x))$ by the parametrization

$$\begin{aligned} t(x) &= ax + b \\ r(x) &= ax^2 + (2b-1)x + \frac{b^2 - b + 1}{a} \\ q(x) &= ahx^2 + (2bh - h + 1)x + \frac{b^2h - bh + h + ab - a}{a} \end{aligned}$$

where the following conditions are satisfied: (1) the integer $48h(a-h)$ is a perfect square, (2) the congruence $b^2 - b + 1 \equiv 0 \bmod a$ is solvable, (3) the integer $(a+h)^2 - 4h^2$ is not a perfect square and (4) the coefficients of $q(x)$ are coprime. Furthermore a and h must also satisfy the relations $4h - a > 0$ and $a - h > 0$ and thus a lies in the range $h < a < 4h$. Multiplying the relation $f(x) = 4q(x) - t^2(x)$ by $a(4h-a)$, completing the squares and setting $X = a(4h-a)x + (4h-a)b + 2a - 2h$ we conclude to the special Pell equation

$$X^2 - a(4h-a)DY^2 = \left(2\sqrt{3h(a-h)}\right)^2. \tag{12}$$

In the same way if $k = 4$ then there is a parametrization of the quadratic families $(q(x), t(x), r(x))$ as

$$\begin{aligned} t(x) &= ax + b \\ r(x) &= ax^2 + 2(b-1)x + \frac{b^2 - 2b + 2}{a} \\ q(x) &= ahx^2 + (2bh - 2h + a)x + \frac{b^2h - 2bh + 2h + ab - a}{a} \end{aligned}$$

where the following conditions are satisfied: (1) the integer $32h(a-2h)$ is a perfect square, (2) the congruence $b^2 - 2b + 2 \equiv 0 \bmod a$ is solvable, (3) the integer $a^2 - 4h^2$ is not a perfect square and (4) the coefficients of $q(x)$ have no common factor. Multiplying the relation

$f(x) = 4q(x) - t^2(x)$ by $a(4h - a)$, completing the squares and setting $X = a(4h - a)x + (4h - a)b + 2a - 4h$ yields the special Pell equation

$$X^2 - a(4h - a)DY^2 = \left(2\sqrt{2h(a - 2h)}\right)^2. \tag{13}$$

If we wish to find suitable curve parameters in both cases we proceed in the usual way. Note here that the number of effective polynomial families decreases as the value of k increases in $\{3, 4, 6\}$. The reason is that the choices for a are decreased. In particular when $k = 3$ the integer a is chosen in the range $(h, 4h)$ while if $k = 6$, the integer a lies in $(3h, 4h)$.

4 Experimental Results

The most crucial step in the above procedure is solving a generalized Pell equation of the form of Eq. (2). A well known method used to solve any kind of Pell equations is the LMM algorithm [13, 14]. Alternative ways are also presented in [14]. One of these methods finds all solutions of an equation of the form (2) by computing the simple continued fraction expansion of the quadratic irrational $\sqrt{SD}$, but it is only suitable for values of the CM discriminant D such that $m^2/S < D$. This method is also implemented by Karabina and Teske in [10] for the

Table 3: **Suitable parameters for $\mathbf{k} \in \{3, 4, 6\}$ and $\mathbf{h} > 1$ from effective polynomial families ($\mathbf{768 \leq k \log q \leq 1536}$, $\log \mathbf{s} > \mathbf{128}$ and $\mathbf{D < 10^5}$)**

k = 3				**k = 4**				**k = 6**		
Cofactor h	**a**	**Suitable (q, t, r)**		**Cofactor h**	**a**	**Suitable (q, t, r)**		**Cofactor h**	**a**	**Suitable (q, t, r)**
4	7	392		8	17	52		4	13	384
12	21	46		8	25	19		9	31	13
12	37	45		16	34	52		12	39	72
16	19	57		16	50	19		16	49	37
16	43	10		18	37	60		25	79	7
36	111	36		18	61	23		25	91	17
48	49	33		32	65	53		36	109	40

original MNT equations. When $m^2/S > D$ this procedure finds only some of the solutions for some D. Thus in our implementation we might lost a few suitable parameters. For more precise results, one should implement the LMM algorithm when $m^2/S > D$.

Table 3 presents the number of suitable curve parameters obtained by effective polynomial families for certain choices of h when $k \in \{3, 4, 6\}$. The criteria for suitability are the same as those in [15]. In particular the field size q is chosen such that $768 \leq k \log q \leq 1536$ and the group order r is chosen to be a product $r = ms$ for some prime s with $\log s > 128$ bits.

For example when $k = 6$ we are looking for primes q such that $128 \leq \log q \leq 256$ bits. In this case the most lucky families appear when $h = 4$ and $a = 13$ where we found 384 suitable triples (q, t, r). When $k = 3$ the field size q must be chosen between the sizes $256 \leq \log q \leq 512$. The most lucky case appears when $h = 4$ and $a = 7$ where we found 392 suitable curve parameters. When $k = 4$ the best results appear when $h = 18$ and $a = 37$ where we found 60 suitable triples (q, t, r) with $192 \leq \log q \leq 384$.

Table 4: **Time required for the generation of suitable triples $(\mathbf{q}, \mathbf{t}, \mathbf{r})$ when $\mathbf{k} \in \{3, 4, 6\}$ ($\mathbf{768} \leq \mathbf{k} \log \mathbf{q} \leq \mathbf{1536}$ and $\log \mathbf{s} > \mathbf{128}$)**

	k = 3			**k = 4**			**k = 6**		
Triples	**h**	**SB Method (sec)**	**Effective Families (sec)**	**h**	**SB Method (sec)**	**Effective Families (sec)**	**h**	**SB Method (sec)**	**Effective Families (sec)**
	4		**a = 7**	**8**		**a = 17**	**4**		**a = 13**
1		9.01	18.03		20.43	3.38		0.26	0.82
5		212.38	50.87		733.42	25.29		36.94	9.24
10		739.51	76.68		2717.25	100.61		377.71	11.69
20		1172.41	208.80		3670.81	383.85		1809.48	23.84
30		1641.05	310.70		6053.82	962.65		1874.23	45.34
	12		**a = 21**	**16**		**a = 34**	**9**		**a = 31**
1		8.68	9.26		4.82	3.45		12.49	18.58
5		279.08	132.92		240.88	27.50		72.48	226.62
10		931.51	1635.00		1112.30	121.02		3773.71	3176.45
	16		**a = 19**	**18**		**a = 37**	**12**		**a = 39**
1		2.60	12.62		21.40	44.23		111.06	0.19
5		1303.61	70.88		92.37	255.47		3118.85	50.67
10		3135.41	165.36		3869.22	638.52		6537.99	275.64
	48		**a = 49**	**32**		**a = 65**	**16**		**a = 49**
1		1.68	0.51		307.74	5.65		0.94	11.96
5		157.48	99.35		5899.03	44.15		298.87	35.30
10		6386.99	1170.49		13121.12	199.86		1168.44	141.01

According to our earlier analysis we expect that the number of suitable parameters obtained from effective polynomial families is larger than the number of parameters from non-effective ones. Thus we argue that one may use only the effective polynomial families for finding suitable triples (q, t, r) when $k \in \{3, 4, 6\}$. In order to show the efficiency of our method, we implemented the algorithm proposed by Scott and Barreto and compared the time required for the construction of a fixed number of suitable parameters with their method and our proposal. The results appear in Table 4. In the case where there are more than one effective polynomial families, we studied only the first one, i.e. the first $a \in \mathbb{Z}$ leading to an effective polynomial family.

In almost all cases, we observe that our method is faster than the method of Scott and Barreto, especially as the number of the desired suitable triples (q, t, r) increases. This is because the Pell equations from non-effective polynomial families are not always solvable and thus there might be a large distance between the suitable values of D. For example consider the case where $k = 6$ and $h = 4$. If we wish to construct only one elliptic curve (e.g. one triple (q, t, r)), the algorithm of Scott and Barreto requires 0.26 seconds, while our method needs 0.82 seconds. If we wish to construct 5 elliptic curves (or the first 5 triples), Scott and Barreto method requires 36.94 seconds, while our method needs only 9.24. For a required number of 10 parameters, the difference is more clear. Taking the number of suitable parameters even further, say 20 or 30 the method of Scott and Barreto needs to solve more than one

Pell equations. This fact provides a considerable delay in the whole procedure. The same remarks hold also for the case $k = 3$ and $h = 4$. Furthermore since the density of the values of D is larger in our case, we expect that for a fixed number of suitable triples the values of the discriminants will be smaller in the case of effective polynomial families than in the case of Scott and Barreto method. For example when $k = 6$ and $h = 4$ the first 30 suitable triples appear for values of $D \leq 2221$, while in the case of Scott and Barreto the same number of triples were found for $D \leq 97282$. In order to achieve higher security levels, we may change our requirements to accept larger values for the prime q. In this case we observe the same behaviour as in the results of Table 4. See Table 5 for example.

Table 5: **Time required for the generation of suitable triples $(\mathbf{q}, \mathbf{t}, \mathbf{r})$ when $\mathbf{k = 6}$ and $\mathbf{3072 \leq k \log q \leq 4608}$**

Triples	**h**	**SB Method (sec)**	**Effective Families (sec)**	**h**	**SB Method (sec)**	**Effective Families (sec)**	**h**	**SB Method (sec)**	**Effective Families (sec)**
	4		**a = 13**	**9**		**a = 31**	**16**		**a = 49**
1		3.68	9.60		1208.45	18.15		15.13	35.75
5		1004.76	106.19					1465.73	356.10

5 Conclusion

According to Scott and Barreto [15] the construction of generalized MNT elliptic curves is based on solving several Pell-type equations of the form of Eq. (2). For certain choices of cofactor h, some of these equations have more chances than others in producing suitable elliptic curve parameters. In particular the most lucky quadratic polynomial families $(q(x), t(x), r(x))$ are those for which $f(x) = 4q(x) - t^2(x)$ is quadratic and factorable. The Pell equations obtained by such families have the advantage that they are always solvable for every positive and square-free integer D and thus the more solutions we have to test for suitability, the higher is the probability to get suitable curve parameters. This observation also implies that this special kind of Pell equations provides even more flexibility on the CM discriminant, since there are no congruential restrictions on D. In this work we isolate these equations and introduce a procedure that uses only these special equations to construct the desired generalized MNT elliptic curves. Based on our experimental assessments, we argue that our method can considerably speed up the algorithm proposed in [15]. This is theoretically explained (mainly) from the fact that we manage to avoid the solution of "unlucky" Pell equations.

References

[1] A.O.L. Atkin, F. Morain, Elliptic Curves and Primality Proving, in *Journal of Mathematics of Computation*, Vol. 61, No. 203, pp. 29-68, (1993).

[2] P.S.L.M. Barreto, B. Lynn, M. Scott, Constructing Elliptic Curves with Prescribed Embedding Degrees, in *Security in Communication Networks – SCN '2002*, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2576, pp. 263-273, (2002).

[3] P.S.L.M. Barreto, M. Naehrig, Pairing-Friendly Elliptic Curves of Prime Order, in *Selected Areas in Cryptography – SAC '2005*, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3897, pp. 319-331, (2006).

[4] D. Boneh, M. Franklin, Identity-Based Encryption from the Weil Pairing, in *SIAM Journal of Computing*, Vol. 32, No. 3, pp. 586-615, (2003).

[5] D. Boneh, B. Lynn, H. Shacham, Short Signatures from the Weil Pairing, in *Advances in Cryptology - Asiacrypt 2001*, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2248, pp. 514-532, (2002).

[6] P. Duan, S. Cui, C. Wah Chan, Finding More Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems, in *International Journal of Information Technology*, Vol. 2, No. 2, pp. 157-163, (2005).

[7] D. Freeman, M. Scott, E. Teske, A Taxonomy of Pairing-Friendly Elliptic Curves, in *Journal of Cryptology*, Vol. 23, pp. 224-280, (2010).

[8] S.D. Galbraith, K. Harrison, D. Soldera, Implementing the Tate Pairing, in *Algorithmic Number Theory Symposium – ANTS V*, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2369, pp. 324-337, (2002).

[9] S.D. Galbraith, J. McKee, P. Valença, Ordinary Abelian Varieties Having Small Embedding Degree, in *Finite Field Applications*, Vol. 13, pp. 800-814, (2007).

[10] K. Karabina, E. Teske, On Prime-Order Elliptic Curves with Embedding Degrees $k = 3, 4$ and 6, in *Algorithmic Number Theory Symposium – ANTS-VIII*, Lecture Notes in Computer Science, Springer-Verlag, Vol. 5011, pp. 102-117, (2008).

[11] A. Miyaji, M. Nakabayashi, S. Takano, New Explicit Conditions of Elliptic Curve Traces for FR-Reduction, in *IEICE Transactions Fundamentals*, Vol. E84-A, No. 5, pp. 1234-1243, (2001).

[12] R.A. Mollin, Fundamental Number Theory with Applications, CRC Press, Boca Raton, New York, London, Tokyo, (1998).

[13] R.A. Mollin, Simple Continued Fraction Solutions for Diophantine Equations, in *Expositines Mathematicae*, Vol. 19, pp. 55-73, (2001).

[14] J.P. Robertson, Solving the Generalized Pell Equation $x^2 - Dy^2 = N$, (2004), `http://hometown.aol.com/jpr2718/`

[15] M. Scott, P.S.L.M. Barreto, Generating more MNT Elliptic Curves, in *Designs, Codes and Cryptography*, Vol. 38, pp. 209-217, (2006).