# More Sparse Families of Pairing-Friendly Elliptic Curves

**Abstract.** Generating pairing-friendly elliptic curves is a crucial step in the deployment of pairing-based cryptographic applications. The most efficient method for their construction is based on polynomial families, namely complete families, complete families with variable discriminant and sparse families. In this work we further study the case of sparse families which seem to produce more pairing-friendly elliptic curves than the other two polynomial families and also can lead to better $\rho$-values in many cases. We present two general methods for producing sparse families and we apply them for four embedding degrees $k \in \{5, 8, 10, 12\}$. Particularly for $k = 5$ we introduce for the first time the use of Pell equations by setting a record with $\rho = 3/2$ and we present a family that has better chances in producing suitable curve parameters than any other reported family for $k \notin \{3, 4, 6\}$. In addition we generalise some existing examples of sparse families for $k = 8, 12$ and provide extensive experimental results for every new sparse family for $k \in \{5, 8, 10, 12\}$ regarding the number of the constructed elliptic curve parameters.

**Keywords:** Pairing-based cryptography, pairing-friendly elliptic curves, polynomial families, Pell equations.

## 1 Introduction

Over the past few years, pairing-based cryptography has gained much attention and a variety of pairing-based protocols have been developed (e.g. Joux's one-round tripartite key agreement protocol [11], Boneh and Franklin's identity-based encryption [3] etc.). All these protocols require the construction of a special type of elliptic curves that satisfy certain properties and are known as *pairing-friendly* elliptic curves [9]. Generating these elliptic curves is a crucial step in pairing-based applications and even though many methods have been proposed, it is still an active field.

For a large prime $q$, let $E/\mathbb{F}_q$ be an ordinary elliptic curve of order $\#E(\mathbb{F}_q) = hr$ where $r$ is a large prime and $h$ is a small integer called the *cofactor*. Let also $t = q + 1 - \#E(\mathbb{F}_q)$ be the Frobenius trace of the curve. In many pairing-based protocols, it is required that $h = 1$ (prime order curves). However such curves are rare and in most applications a small $h > 1$ is acceptible. In this latter case, we define the security parameter $\rho = \log(q)/\log(r)$ measuring how close to the ideal case is the constructed curve. Clearly, $\rho$ should be as close to 1 as possible. The *embedding degree* of the curve $E/\mathbb{F}_q$, is the smallest positive integer $k > 1$, such that $E[r] \subseteq E(\mathbb{F}_{q^k})$, where $E[r]$ is the group of $r$-torsion points of $E/\mathbb{F}_q$. Equivalently we can say that $k$ is the smallest positive integer such that

$r \mid q^k - 1$ (see [8], [9]). The embedding degree $k$ must be carefully chosen to be large enough ensuring the hardness of the DLP in $\mathbb{F}^*_{q^k}$ and simultaneously small enough in order to keep an efficient arithmetic in $\mathbb{F}^*_{q^k}$. Current requirements indicate that a good security level is around 128 bits or more, in which case $3000 < k \log q < 5000$ [9]. Determining suitable integer triples $(q, t, r)$ satisfying the above properties, for a specific $k > 1$, and requiring at the same time that $\rho \approx 1$, is one of the most demanding tasks in pairing-based cryptography. Once these parameters are generated, the Complex Multiplication (CM) method [1] can be used for the construction of the curve equation. The efficiency of the CM method is closely related to the size of an integer $D$ (called the *CM discriminant*) which is the square free positive value satisfying the CM equation $DY^2 = 4q - t^2$ for a given pair $(q, t)$. The value of $D$ must be relatively small (e.g. $D < 10^{10}$ or even smaller) in order to implement the CM method efficiently.

Since 2001 a variety of methods have been proposed for constructing pairing-friendly elliptic curves, most of which are based on parameterizing the curve parameters as *polynomial families* $(q(x), t(x), r(x))$ in $\mathbb{Q}[x]$. There are three types of such polynomial families depending on the form of the polynomial $4q(x) - t^2(x)$ representing the right hand side of the CM equation expressed in polynomial field.

**Definition 1 ([5],[9]).** A polynomial family $(q(x), t(x), r(x))$ is said to be *complete*, if there exists an $s(x) \in \mathbb{Q}[x]$, such that $4q(x) - t^2(x) = Ds^2(x)$, for some positive, square-free integer $D$ representing the CM discriminant. If the polynomials $q(x)$ and $t(x)$ satisfy $4q(x) - t^2(x) = g(x)s^2(x)$ for some $g(x) \in \mathbb{Q}[x]$ with $\deg g = 1$ then the polynomial family is called *complete with variable discriminant.* If $\deg g > 1$, then the family is called *sparse.*

In this paper we further investigate the construction of sparse families of pairing-friendly elliptic curves using the solutions of a generalized Pell equation. We present two methods for generating sparse families for arbitrary $k$ and focus on four embedding degrees $k \in \{5, 8, 10, 12\}$. Especially when $k = 5$ we introduce for the first time the use of Pell equations and set a record with $\rho = 3/2$. Additionally, we produce some new sparse polynomial families for $k \in \{8, 10, 12\}$ achieving $\rho = 3/2$, which is the smallest value reported in the literature for variable discriminant. Furthermore, the proposed methods generate pairing-friendly elliptic curves with smaller CM discriminant than other existing methods, improving the efficiency of the CM method. Finally, we have conducted extensive experimental assessments which show that the proposed new polynomial families lead to the construction of many elliptic curves, achieving at the same time a relatively small value for the CM discriminant.

The paper is organized as follows. In Section 2 we present some background related to pairing-friendly elliptic curves as well as some of the most important methods for generating suitable curve parameters for the three types of families in Definition 1. We analyze our proposed methods in Sections 3 and 4 and proceed by demonstrating our experimental results in Section 5. Finally, we conclude the paper in Section 6.

## 2 Preliminaries and Previous Work

In this Section, we will give the notion of *polynomial families* of pairing-friendly elliptic curves and proceed by analyzing the existing methods for their construction. Our goal is to find suitable integers $(q, t, r)$ for a fixed embedding degree $k > 0$, such that $\rho \approx 1$. The best $\rho$-values in the literature are achieved by representing the parameters $(q, t, r)$ as polynomials $q(x), t(x), r(x) \in \mathbb{Q}[x]$ respectively.

**Definition 2 ([9]).** Let $q(x), t(x), r(x) \in \mathbb{Q}[x]$ be non-zero polynomials. Then the polynomial triple $(q(x), t(x), r(x))$ parameterizes a *family of pairing-friendly ordinary elliptic curves* with embedding degree $k$ and CM discriminant $D$ if the following conditions are satisfied:

1. the polynomial $q(x)$ represents primes,
2. the polynomial $r(x)$ is non-constant, irreducible, integer-valued, with positive leading coefficient,
3. $r(x)$ divides the polynomials $q(x) + 1 - t(x)$ and $\Phi_k(t(x) - 1)$, where $\Phi_k(x)$ is the $k^{\text{th}}$ cyclotomic polynomial and
4. there are infinitely many integer solutions $(x, Y)$ for the parameterized CM equation
$$DY^2 = 4q(x) - t^2(x) = 4h(x)r(x) - (t(x) - 2)^2. \qquad (1)$$

The $\rho$-value of a polynomial family is measured by the ratio $\rho(q, t, r) = \deg q(x)/\deg r(x)$. The condition $r(x) \mid (q(x)+1-t(x))$ implies that $\#E(\mathbb{F}_{q(x)}) = h(x)r(x)$, where $h(x) \in \mathbb{Q}[x]$ is the cofactor. Our problem now reduces in finding a suitable solution $(x_0, Y_0)$ of Equation (1) such that $q(x_0)$ and $r(x_0)$ are prime integers. Then, we can use the CM method to construct an elliptic curve $E/\mathbb{F}_{q(x_0)}$ with Frobenius trace $t(x_0)$ and order $\#E(\mathbb{F}_{q(x_0)}) = h(x_0)r(x_0)$, where $h(x_0) = 1$ is the ideal case. Let $f(x) = 4q(x) - t^2(x) \in \mathbb{Q}[x]$ be the *CM polynomial*. Most methods focus on CM polynomials of the form $f(x) = g(x)s^2(x)$ for some $g(x), s(x) \in \mathbb{Q}[x]$, where $\deg s$ is arbitrary, but $\deg g \leq 2$. By Definition 1, when $\deg g = 0$ the polynomial family $(q(x), t(x), r(x))$ is complete with $f(x) = Ds^2(x)$, for some square-free positive $D$. When $\deg g = 1$ we have a complete family with variable discriminant and finally when $\deg g = 2$ but $g(x)$ is not a square, the family is sparse.

***Complete Families:*** The most well known method in this case is the Brezing and Weng method [4] and its variants [9], [12], [17], [19]. These methods start by fixing a $k > 1$ and some square-free CM discriminant $D$. They choose an irreducible polynomial $r(x) \in \mathbb{Q}[x]$, such that $K \cong \mathbb{Q}[x]/(r(x))$, where $K$ is the field containing a primitive $k^{\text{th}}$-root of unity $\zeta_k$. Then, let $t(x)$ and $s(x)$ be the polynomials mapping to $\zeta_k + 1$ and $(\zeta_k - 1)/\sqrt{-D}$ in $K$ respectively. The resulting CM polynomial will be of the form $f(x) = Ds^2(x)$. The best family in this case is given in [2] for $k = 12$ and $D = 3$, with $\rho(q, t, r) = 1$. Additional examples appear also in [9], [12], [17], [19].

***Complete Families with Variable Discriminant:*** Such families are constructed in the work of Lee and Park [13] and additionally in [5]. The method of Lee and Park sets the polynomial $r(x)$ to be an irreducible factor of the cyclotomic polynomial $\Phi_k(u(x))$, for some $u(x) \in \mathbb{Q}[x]$. The challenging part of the method is to determine a suitable polynomial $u(x)$. This is accomplished by fixing an embedding degree $k$ and an element $\theta = a_0 + a_1\zeta_k + \ldots + a_{\varphi(k)-1}\zeta_k^{\varphi(k)-1}$ in $\mathbb{Q}(\zeta_k)$. Then, the transition matrix $P$ from the set $\mathcal{B}_\theta = \{1, \theta, \ldots, \theta^{\varphi(k)-1}\}$ to the basis $\mathcal{B}_{\zeta_k} = \{1, \zeta_k, \ldots, \zeta_k^{\varphi(k)-1}\}$ is constructed, which is a $\varphi(k) \times \varphi(k)$ matrix with elements $P_{ij}$ obtained by the relation $\theta^j = \sum_{i=0}^{\varphi(k)-1} P_{ij}\zeta_k^i$, for each $j \in \{0, 1, \ldots, \varphi(k)-1\}$. If $\det(P) \neq 0$ then $P$ has an inverse $P^{-1} = (P'_{ij})$ and the polynomial $u(x)$ will be equal to $u(x) = \sum_{i=0}^{\varphi(k)-1} P'_{i1}x^i$. Finally, they set $t(x) = u(x) + 1$ and $f(x) \equiv -(u(x)-1)^2 \bmod r(x)$.

Propositions 1 and 2 in [13] guarantee that if $\theta = a_0 - 2a_1\zeta_k + a_1\zeta_k^2$ for some non-zero $a_0, a_1 \in \mathbb{Q}$, then $\deg f = 1$. Several examples of such polynomial families appear in [13]. However, they all lead to large CM discriminants $D > 10^7$. Clearly, the method of Lee and Park gathers all CM polynomials of the form $f(x) = g(x)s^2(x)$ with $\deg s = 0$ and $\deg g = 1$, but misses the cases where $\deg s > 0$. Such cases are studied in greater detail in [5]. Additional examples appear in [9].

***Sparse Families:*** In this case $f(x) = (ax^2 + bx + c)s^2(x)$, where $a, b, c \in \mathbb{Q}$. Substituting into Equation (1) and excluding the perfect square term $s^2(x)$, we get $DY^2 = g(x) = ax^2 + bx + c$. Multiplying by $4a$ and completing the squares yields a generalized Pell equation of the form

$$X^2 - aD(2Y)^2 = b^2 - 4ac, \qquad \text{where} \qquad X = 2ax + b. \tag{2}$$

If Equation (2) is solvable for some square-free $D$, then it has an infinite number of integral solutions $(X_i, Y_i)$ (see [15]). In order to generate the elliptic curve, we firstly check if $X_i = 2ax_0 + b$, for some $x_0 \in \mathbb{Z}$. If this is the case, then we check if $q(x_0)$ and $r(x_0)$ are primes and if $t(x_0)$ satisfies the Hasse's bound.

The first method for generating sparse families is due to Miyaji, Nakabayashi and Takano [14] (MNT method) for $k \in \{3, 4, 6\}$. In their method they describe polynomial families $(q(x), t(x), r(x))$ such that $h(x) = 1$ (ideal case) and so $\rho(q, t, r) = 1$. Several generalizations and extensions of the MNT method have been proposed in [6], [7], [10], [18] allowing $h(x) > 1$. Particularly, in [6] and [7] the notion of *effective polynomial families* is introduced. These are sparse polynomial families leading to CM polynomials of the form $f(x) = g(x)s^2(x)$ with $g(x)$ quadratic and factorable. In this case, the constructed Pell equations have the advantage that they are always solvable for every square-free $D$ and so the sparse family has better chances in producing suitable curve parameters. For $k \notin \{3, 4, 6\}$, the best known result is reported in [8] for $k = 10$ and achieves a value $\rho(q, t, r) = 1$. Another method for constructing sparse families is discussed in [5], where the author starts by fixing an embedding degree $k > 1$ and constructing a number field $K$ containing a primitive $k^{\text{th}}$ root of unity. Then, an irreducible polynomial $r(x) \in \mathbb{Q}[x]$ is chosen so that $K = \mathbb{Q}[x]/(r(x))$ and the algorithm searches for a quadratic polynomial $g(x) \in \mathbb{Q}[x]$ so that $-g(x)$ is a square in $K$. Finally, $t(x)$ and $s(x)$ are set as polynomials mapping to $\zeta_k + 1$ and $(\zeta_k - 1)/\sqrt{-g(x)}$ respectively. The constructed CM polynomial is not necessarily quadratic, but has a perfect square factor $s^2(x)$ with $\deg s > 1$. An alternative method is described in [6] which starts by fixing a $k > 1$ and chooses an irreducible polynomial $r(x) \in \mathbb{Q}[x]$. Then searches for a trace polynomial $t(x)$, such that $r(x) \mid \Phi_k(t(x) - 1)$. Once these polynomials are determined, the CM polynomial is equal to $f(x) \equiv -(t(x) - 2)^2 \bmod r(x)$.

***Our Contribution:*** Summarizing, Brezing-Weng like polynomial families produce the best $\rho$-values in the literature for $k \notin \{3, 4, 6, 10\}$. However, they work for a fixed and very small discriminant $D$ which according to the German Information Security Agency may lead to vulnerable elliptic curves. On the other hand, polynomial families with variable discriminant provide some flexibility on $D$, but result in large CM discriminants which make the CM method very inefficient. In this paper, we argue that sparse families using solutions of generalized Pell equations are more attractive in applications that require variable but relatively small CM discriminants.

We here present two methods for the generation of sparse families of pairing-friendly elliptic curves. The first method is based on [6] and [13]. It extends the ideas in [13] by searching for CM polynomials $f(x) = g(x)s^2(x)$ with $\deg g = 2$ instead of linear polynomials $f(x)$ and it is more efficient compared to the method in [6]. Using the new method, we obtained for the first time sparse families based on Pell equations for $k = 5$, setting at the same time a record with $\rho = 3/2$. Among these families, we found an effective polynomial family for $k = 5$ leading to a generalized Pell equation that is always solvable for every positive and square-free $D$. Based on our new method, we also obtained some sparse families for $k = 10$ with $\rho = 3/2$. The second method is more general and can be implemented for any $k > 1$ and arbitrary CM polynomials $f(x) = g(x)s^2(x)$, with $g(x) \in \mathbb{Q}[x]$ quadratic and not a perfect square. Using this method, we give a generalization of the examples presented in [5] for $k = 8, 12$ and $\rho = 3/2$. Finally, we provide experimental results on the number of suitable curve parameters obtained from our newly proposed polynomial families. Our experiments indicate that our effective family for $k = 5$ produces more curve parameters than any other polynomial family for $k \notin \{3, 4, 6\}$.

## 3 Sparse Families with $\deg \mathbf{f} < \deg \mathbf{r}$

In this section we present a method for constructing sparse families of pairing-friendly elliptic curves with embedding degree $k > 1$, such that the CM polynomial is of the form $f(x) = g(x)s^2(x)$ with $\deg g = 2$ and $g(x)$ not a perfect square.

Our method starts by choosing an arbitrary embedding degree $k > 1$ and fixing an element $\theta \in \mathbb{Q}(\zeta_k)$ of the form

$$\theta = a_0 + a_1\zeta_k + a_2\zeta_k^2 + \ldots + a_{\varphi(k)-1}\zeta_k^{\varphi(k)-1} \tag{3}$$

such that $u(\theta) = \zeta_k$ in $\mathbb{Q}(\zeta_k)$ for some $u(x) \in \mathbb{Q}[x]$. We then construct the transition matrix $P$ from the set $\mathcal{B}(\theta)$ to the basis $\mathcal{B}(\zeta_k)$ using the relation

$$\theta^j = \sum_{i=0}^{\varphi(k)-1} P_{ij}\zeta_k^i, \qquad \text{for} \qquad j = 0, 1, \ldots, \varphi(k) - 1. \tag{4}$$

Since $\Phi_k(u(x))$ should contain an irreducible factor of degree $\varphi(k)$, we need to ensure that $a_0, a_1, \ldots, a_{\varphi(k)-1}$ are chosen so that $\det(P) \neq 0$. Then, the coefficients of the polynomial $u(x)$ are given by the second column of the inverse matrix $P^{-1} = (P'_{ij})$ of $P$ using the relation:

$$u(x) = \sum_{i=0}^{\varphi(k)-1} P'_{i1}x^i. \tag{5}$$

Setting the polynomial $u(x)$ as

$$u(x) = u_{\varphi(k)-1}x^{\varphi(k)-1} + \ldots + u_2x^2 + u_1x + u_0 \in \mathbb{Q}[x] \tag{6}$$

Equation (5) implies that the coefficients of $u(x)$ are actually multivariate polynomials in $\mathbb{Q}[a_0, a_1, \ldots, a_{\varphi(k)-1}]$. Once the polynomial $u(x)$ is created, then we set $t(x) = u(x) + 1$ to find the polynomial representing the Frobenius trace. The polynomial $r(x)$ is set to be the irreducible factor of $\Phi_k(u(x))$ with $\deg r = \varphi(k)$ and it is the minimal polynomial of $\theta$ over $\mathbb{Q}(\zeta_k)$. Thus, we set

$$r(x) = r_{\varphi(k)}x^{\varphi(k)} + \ldots + r_2x^2 + r_1x + r_0 \in \mathbb{Q}[x]. \tag{7}$$

The coefficients of $r(x)$ are multivariate polynomials in $\mathbb{Q}[a_0, a_1, \ldots, a_{\varphi(k)-1}]$ and can be obtained by solving the system $r(\theta) = 0$.

**Algorithm 1** Families of Pairing-Friendly Elliptic Curves with $\deg g = 2$

```
Input: The embedding degree $k$
Output: Suitable polynomials $q(x), t(x), r(x), h(x), f(x) \in \mathbb{Q}[x]$

Step 1: For each $a_0, a_1, a_2, \ldots, a_{\varphi(k)-1} \in \mathbb{Q}$ do
Step 2: Calculate the transition matrix $P$ from $\mathcal{B}(\theta)$ to $\mathcal{B}(\zeta_k)$ by Equation (4)
Step 3: If $\det(P) \neq 0$ compute the coefficients of the polynomials $u(x)$ and $r(x)$
    using the Equation (5) and $r(\theta) = 0$ respectively; else return to Step 1
Step 4: Set the CM polynomial to $f(x) \equiv -(u(x) - 1)^2 \bmod r(x)$
Step 5: If $f(x) = g(x)s^2(x)$ with $g(x)$ quadratic and not a perfect square, with
    positive leading coefficient, then set $h(x) = (f(x) + (u(x) - 1)^2)/4r(x)$, $q(x) =$
    $h(x)r(x) + u(x)$ and $t(x) = u(x) + 1$; else return to Step 1
Step 6: If $q(x)$ is irreducible over $\mathbb{Q}[x]$ and $q(x_0) \in \mathbb{Z}$ for some $x_0 \in \mathbb{Z}$, output the
    polynomials $(t(x), r(x), q(x), h(x), f(x))$; else return to Step 1
```

After obtaining $u(x)$ and $r(x)$, we set the CM polynomial as $f(x) \equiv -(u(x)-1)^2 \bmod r(x)$ and we also require that $\deg g = 2$. Additionally, we must also ensure that the leading coefficient of $g(x)$ is positive and that $g(x)$ is not a perfect square. The corresponding generalized Pell equation can be constructed by setting $DY^2 = g(x)$ and following the procedure described in Section 2.

The above method is summarized in Algorithm 1. The proposed algorithm differs from the work of Lee and Park [13] in that we are actually searching for CM polynomials of the form $f(x) = g(x)s^2(x)$, for some quadratic and non-square polynomial $g(x)$. On the other hand, our method is faster than the one proposed in [6], since in this work the authors start by randomly choosing an irreducible polynomial $r(x)$ and then search for a trace polynomial $t(x)$, such that $r(x) \mid \Phi_k(t(x)-1)$. Clearly, this is a very demanding and time consuming step.

### 3.1 Families with Embedding Degree k = 5

The 5th-cyclotomic polynomial is represented by $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$. Set the element $\theta \in \mathbb{Q}(\zeta_5)$ to be of the general form in Equation (3), for some $a_0, a_1, a_2, a_3 \in \mathbb{Q}$ such that $\det(P) \neq 0$, where $P$ is the $4 \times 4$ transition matrix from $\mathcal{B}_\theta$ to $\mathcal{B}_{\zeta_5}$. This choice will ensure that $\Phi_5(u(x))$ has a quartic irreducible factor $r(x) \in \mathbb{Q}[x]$. Based on Algorithm 1 and setting $f(x) \equiv -(u(x)-1)^2 \bmod r(x)$, we will get a CM polynomial $f(x)$ of degree 3. Since we are searching for sparse families we add the condition $\deg f = 2$. Based on our extensive experimental assessments, we realized that $\theta$ can be of a special form that leads to quadratic CM polynomials. This special form depends only on the choice of $a_0$ and $a_1$ (in an analogy to Proposition 1 of Lee and Park [13]). Randomly choosing integer pairs $(a_0, a_1) \in \mathbb{Q}^2$ we can produce different polynomial families.

**Family 1** Let $\theta = a_0 + 7a_1\zeta_5 - 2a_1\zeta_5^2 + 4a_1\zeta_5^3$, for $a_0, a_1 \in \mathbb{Q}$ and $a_1 \neq 0$. The transition matrix has $\det(P) = 55^3 a_1^6$. We then obtain the polynomials:

$$\begin{aligned}
u(x) &= (4x^3 - (12a_0 - 62a_1)x^2 - (124a_0a_1 - 12a_0^2 - 887a_1^2)x \\
&\quad - (4a_0^3 - 62a_0^2a_1 + 887a_0a_1^2 - 1104a_1^3))/55^2a_1^3 \\
r(x) &= x^4 + (9a_1 - 4a_0)x^3 + (6a_0^2 - 27a_0a_1 + 121a_1^2)x^2 \\
&\quad + (27a_0^2a_1 - 4a_0^3 - 242a_0a_1^2 - 31a_1^3)x \\
&\quad + (a_0^4 - 9a_0^3a_1 + 121a_0^2a_1^2 + 31a_0a_1^3 + 1231a_1^4) \\
f(x) &= ((-x + a_0 - 21a_1)(-x + a_0 - a_1))/55a_1^2
\end{aligned}$$

with $\rho(q,t,r) = 3/2$. This is an effective polynomial family, since the polynomial $f(x)$ factorizes in $\mathbb{Q}[x]$. Therefore, this family will lead to a larger number of suitable curve parameters compared to other sparse families.

**Family 2** Let $\theta = a_0 + a_1\zeta_5 - 8a_1\zeta_5^2 + 20a_1\zeta_5^3$, with $a_0, a_1 \in \mathbb{Q}$ and $a_1 \neq 0$. The transition matrix has $\det(P) = -5^2 151^3 a_1^6$ and we obtain the following polynomials $\rho(q,t,r) = 3/2$:

$$\begin{aligned}
u(x) &= (-4x^3 + (12a_0 + 264a_1)x^2 - (12a_0^2 + 528a_0a_1 + 1931a_1^2)x \\
&\quad + (4a_0^3 + 264a_0^2a_1 + 1931a_0a_1^2 + 81040a_1^3))/5 \cdot 151^2 a_1^3 \\
r(x) &= x^4 + (13a_1 - 4a_0)x^3 + (6a_0^2 - 39a_0a_1 + 969a_1^2)x^2 \\
&\quad + (12177a_1^3 - 4a_0^3 + 39a_0^2a_1 - 1938a_0a_1^2)x \\
&\quad + (a_0^4 - 13a_0^3a_1 + 969a_0^2a_1^2 - 12177a_0a_1^3 + 246341a_1^4) \\
f(x) &= (x^2 + (6a_1 - 2a_0)x + (a_0^2 - 6a_0a_1 + 273a_1^2))/151a_1^2
\end{aligned}$$

### 3.2 Families with Embedding Degree $\mathbf{k = 10}$

For embedding degree $k = 10$ we have an ideal polynomial family given by David Freeman [8] with $\rho(q,t,r) = 1$. It may be useful in applications that do not require $\rho = 1$, to use families that provide larger $\rho$-value. Such examples are obtained by our method with $\rho(q,t,r) = 3/2$. When $k = 10$, the $10^{\text{th}}$-cyclotomic polynomial is given by $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$. We set $\theta \in \mathbb{Q}(\zeta_{10})$ to be of the form in Equation (3), for some $(a_0, a_1, a_2, a_3) \in \mathbb{Q}^4$, such that $\det(P) \neq 0$. As in the case $k = 5$ we obtained certain special forms for $\theta$ depending only on $a_0, a_1 \in \mathbb{Q}$, that lead to quadratic CM polynomials.

**Family 3 (Freeman [8])** Let $\theta = a_0 + a_1\zeta_{10} - 2a_1\zeta_{10}^2$, for some $a_0, a_1 \in \mathbb{Q}$, with $a_1 \neq 0$. The transition matrix has $\det(P) = -25a_1^6$ and we obtain the following polynomials with $\rho(q,t,r) = 1$:

$$\begin{aligned}
u(x) &= (2x^2 - (4a_0 + 3a_1)x + (2a_0^2 + 3a_0a_1 + 8a_1^2))/5a_1^2 \\
r(x) &= x^4 - (4a_0 + 3a_1)x^3 + (6a_0^2 + 9a_0a_1 + 9a_1^2)x^2 \\
&\quad - (4a_0^3 - 9a_0^2a_1 - 18a_0a_1^2 - 7a_1^3)x + (a_0^4 + 3a_0^3a_1 + 9a_0^2a_1^2 + 7a_1a_1^3 + 11a_1^4) \\
f(x) &= (3x^2 - (6a_0 + 2a_1)x + (3a_0^2 + 2a_0a_1 + 7a_1^2))/5a_1^2
\end{aligned}$$

**Family 4** Let $\theta = a_0 + 7a_1\zeta_{10} - 6a_1\zeta_{10}^2 + 4a_1\zeta_{10}^3$, with $a_0, a_1 \in \mathbb{Q}$ and $a_1 \neq 0$. The transition matrix has $\det(P) = 31^3a_1^6$ and we obtain the following polynomial family with $\rho(q,t,r) = 3/2$:

$$\begin{aligned}
u(x) &= (4x^3 - (12a_0 + 38a_1)x^2 + (12a_0^2 + 76a_0a_1 + 391a_1^2)x \\
&\quad - (4a_0^3 + 38a_0^2a_1 + 391a_0a_1^2 + 80a_1^3))/31^2a_1^3 \\
r(x) &= x^4 - (4a_0 + 17a_1)x^3 + (6a_0^2 + 51a_0a_1 + 169a_1^2)x^2 \\
&\quad - (4a_0^3 + 51a_0^2a_1 + 338a_0a_1^2 + 633a_1^3)x + (a_0^4 + 17a_0^3a_1 + 169a_0^2a_1^2 + 1111a_1^4) \\
f(x) &= (4x^2 - 2(a_0 + a_1)x + (a_0^2 + 2a_0a_1 + 13a_1^2))/31a_1^2
\end{aligned}$$

## 4 Sparse Families for Arbitrary CM polynomials

In this section we present a more general method for the construction of polynomial families of pairing-friendly elliptic curves. This approach can be applied for

CM polynomials of any form, but as in the previous section we focus on cases where $f(x) = g(x)s^2(x)$ for some quadratic, non-square polynomial $g(x)$ (sparse families). The proposed method is based on the remarks in [10], [13].

We start by fixing an element $\theta \in \mathbb{Q}(\zeta_k)$ such that $\det(P) \neq 0$, where $P$ is the transition matrix form $\mathcal{B}(\theta)$ to the basis $\mathcal{B}(\zeta_k)$. The polynomials $u(x)$ and $r(x)$ are determined in the same way as described in Algorithm 1 where the coefficients of $u(x)$ and $r(x)$ are all multivariate polynomials in $\mathbb{Q}[a_0, a_1, \ldots, a_{\varphi(k)-1}]$. We compute these polynomials according to Equations (6) and (7) and we set the trace polynomial to $t(x) = u(x) + 1$. The next step is to construct the cofactor $h(x)$ by setting

$$h(x) = h_{\varphi(k)-2}x^{\varphi(k)-2} + \ldots + h_2x^2 + h_1x + h_0 \in \mathbb{Q}[x]. \tag{8}$$

We require that $\deg h = \varphi(k) - 2$ or smaller, because in this case $\rho = (2\varphi(k) - 2)/\varphi(k) < 2$ (since $\deg(u-1)^2 = 2\varphi(k) - 2$, while $\deg r = \varphi(k)$). Substituting the polynomials $h(x), r(x)$ and $t(x)$ into the parameterized CM equation (1) we will get a degree $2\varphi(k) - 2$ CM polynomial of the form

$$f(x) = f_{2\varphi(k)-2}x^{2\varphi(k)-2} + f_{2\varphi(k)-3}x^{2\varphi(k)-3} + \ldots + f_2x^2 + f_1x + f_0. \tag{9}$$

The only unknown values are the coefficients of the cofactor which must be determined. Suppose that we are searching for CM polynomials with $\deg f = i$, for some even $i = 2, 4, \ldots 2\varphi(k) - 2$. Then the first $2\varphi(k) - i - 2$ coefficients of $f(x)$ in Equation (9) must satisfy $f_{2\varphi(k)-2} = f_{2\varphi(k)-3} = \ldots = f_{i+1} = 0$. Using this system we can calculate some, or all the coefficients of the cofactor $h(x)$. If we set $\deg f < \deg r = \varphi(k)$, then all coefficients of $h(x)$ can be determined by the above system. Otherwise, for the remaining coefficients of $h(x)$ we will have to do some additional search.

For example, when $\varphi(k) = 4$, (i.e. $k \in \{5, 8, 10, 12\}$) the polynomials $f(x)$ and $h(x)$ will have $\deg f = 6$ and $\deg h = 2$ respectively. For CM polynomials of the form $f(x) = g(x)s^2(x)$, with $g(x)$ quadratic and non-square, the possible values for the degree of $f(x)$ are $\deg f \in \{2, 4, 6\}$. Setting $\deg f = 2$, we have $f_6 = f_5 = f_4 = f_3 = 0$. From $f_6 = f_5 = f_4 = 0$ we determine $h(x)$ and we must also guarantee that $f_3 = 0$. When $\deg f = 4$, we require some search for $h_0$, while when $\deg f = 6$ we need to search for all coefficients of $h(x)$. We applied this idea for $k = 8, 12$ and we obtained a generalization of Drylo's examples given in [5], by representing $\theta$ in two variables $a_0, a_1 \in \mathbb{Q}$.

**Family 5** Let $\theta = a_0 + a_1\zeta_8 + a_1\zeta_8^2 - a_1\zeta_8^3$, with $a_0, a_1 \in \mathbb{Q}$ and $a_1 \neq 0$. The transition matrix has $\det(P) = -24a_1^6$ and setting $h(x) = (x - a_0 - 3a_1)^2/(576a_1^6)$ we obtain the next polynomial family with $\rho(q, t, r) = 3/2$:

$$\begin{aligned} u(x) &= (-x^3 + 3(a_0 + a_1)x^2 - (3a_0^2 + 6a_0a_1 - 5a_1^2)x \\ &\quad + (a_0^3 + 3a_0^2a_1 - 5a_0a_1^2 - 3a_1^3))/12a_1^3 \\ r(x) &= x^4 - 4a_0x^3 + (6a_0^2 - 2a_1^2)x^2 - (4a_0^3 - 4a_0a_1^2)x + (a_0^4 - 2a_0^2a_1^2 + 9a_1^4) \\ f(x) &= (x^2 - 2a_0x + a_0^2 - a_1^2)(x - a_0 - 3a_1)^2/18a_1^4 \end{aligned}$$

**Family 6** Let $\theta = a_0 + 2a_1\zeta_{12} + a_1\zeta_{12}^2 - a_1\zeta_{12}^3$, with $a_0, a_1 \in \mathbb{Q}$ and $a_1 \neq 0$. The transition matrix has $\det(P) = -45a_1^6$ and setting $h(x) = (x-a_0-3a_1)^2/(900a_1^6)$ we obtain the next polynomials with $\rho(q,t,r) = 3/2$:

$$\begin{aligned}
u(x) &= (-x^3 + (3a_0 + 4a_1)x^2 - (3a_0^2 + 8a_0a_1 - 5a_1^2)x \\
&\quad + (a_0^3 + 4a_0^2a_1 - 5a_0a_1^2 - 9a_1^3))/15a_1^3 \\
r(x) &= x^4 - (4a_0 - 2a_1)x^3 + (6a_0^2 + 6a_0a_1 - 3a_1^2)x^2 \\
&\quad - (4a_0^3 + 6a_0^2a_1 - 6a_0a_1^2 - 4a_1^3)x + (a_0^4 + 2a_0^3a_1 - 3a_0^2a_1^2 - 4a_0a_1^3 + 13a_1^4) \\
f(x) &= (4x^2 - 4(2a_0 + a_1)x + 4a_0^2 + 4a_0a_1 + 17a_1^2)(x - a_0 - 3a_1)^2/75a_1^4
\end{aligned}$$

## 5 Experimental Results

We demonstrate some experimental results obtained by every polynomial family described in Sections 3 and 4. Recall that each representative comes of a random choice $a_0, a_1 \in \mathbb{Q}$. For each polynomial family, different $a_0, a_1$ will result in different polynomials $q(x), t(x), r(x)$, producing the same curve parameters. Before constructing the generalized Pell equation, we need to apply a linear transformation on each family in order to make the polynomials integer valued (See [12], [13]). Furthermore, evaluating Families 5, 6 at $(a_0, a_1) = (0, 1)$ we get Drylo's examples [5].

**Example 1 (k = 5)** Set $(a_0, a_1) = (1, 1)$ in Family 1 and apply the transformation $x \to (55x - 20)$ to obtain the next polynomial family with $\rho(q,t,r) = 3/2$:

$$\begin{aligned}
t(x) &= 220x^3 + 470x^2 + 345x + 87 \\
r(x) &= 55x^4 + 145x^3 + 145x^2 + 65x + 11 \\
q(x) &= 12100x^6 + 51700x^5 + 93175x^4 + 90645x^3 + 50215x^2 + 15030x + 1901
\end{aligned}$$

with CM polynomial $f(x) = 5(x + 1)(11x + 7)$ and generalized Pell equation:

$$(55x - 10)^2 - 55DY^2 = 100 \tag{10}$$

**Example 2 (k = 5)** Set $(a_0, a_1) = (0, 1)$ in Family 7 and apply the transformation $x \to (755x + 223)$ to get the polynomial family with $\rho(q,t,r) = 3/2$:

$$\begin{aligned}
t(x) &= -15100x^3 - 12060x^2 - 3185x - 276 \\
r(x) &= 3775x^4 + 4525x^3 + 2040x^2 + 410x + 31 \\
q(x) &= 57002500x^6 + 91053000x^5 + 60407650x^4 + 21289350x^3 + 4201280x^2 \\
&\quad + 440095x + 19129
\end{aligned}$$

with CM polynomial is $f(x) = 3775x^2 + 2260x + 340$ and generalized Pell equation:

$$(755x + 226)^2 - 151DY^2 = -264. \tag{11}$$

**Example 3 (Freeman for $\mathbf{k = 10}$)** Set $(a_0, a_1) = (0, 1)$ in Family 3 and apply the transformation $x \to (5x + 2)$ to obtain the following polynomial family with $\rho(q, t, r) = 1$:

$$\begin{aligned} t(x) &= 10x^2 + 5x + 3 \\ r(x) &= 25x^4 + 25x^3 + 15x^2 + 5x + 1 \\ q(x) &= 25x^4 + 25x^3 + 25x^2 + 10x + 3 \end{aligned}$$

with CM polynomial $f(x) = 15x^2 + 10x + 3$ and generalized Pell equation:

$$(15x + 5)^2 - 15DY^2 = -20. \tag{12}$$

**Example 4 ($\mathbf{k = 10}$)** Set $(a_0, a_1) = (0, 1)$ in Family 4 and apply the transformation $x \to (31x - 8)$ to obtain the next polynomial family with $\rho(q, t, r) = 3/2$:

$$\begin{aligned} t(x) &= 124x^3 - 134x^2 + 57x - 7 \\ r(x) &= 31x^4 - 49x^3 + 31x^2 - 9x + 1 \\ q(x) &= 3844x^6 - 8308x^5 + 8023x^4 - 4253x^3 + 1289x^2 - 204x + 13 \end{aligned}$$

with CM polynomial $f(x) = 31x^2 - 18x + 3$ and generalized Pell equation:

$$(31x - 9)^2 - 31DY^2 = -12 \tag{13}$$

**Example 5 ($\mathbf{k = 8}$)** Set $(a_0, a_1) = (1, 1)$ in Family 5 and apply the transformation $x \to (12x + 4)$ to conclude to the polynomial family with $\rho(q, t, r) = 3/2$:

$$\begin{aligned} t(x) &= -144x^3 - 72x^2 - 4x + 2 \\ r(x) &= 288x^4 + 288x^3 + 104x^2 + 16x + 1 \\ q(x) &= 5184x^6 + 5184x^5 + 1872x^4 + 144x^3 - 54x^2 - 4x + 1 \end{aligned}$$

Setting $h(x) = 18x^2$ we get the CM polynomial $f(x) = 8x^2(144x^2 + 72x + 7)$ and the generalized Pell equation:

$$(24x + 6)^2 - 2DY^2 = 8 \tag{14}$$

**Example 6 ($\mathbf{k = 12}$)** Set $(a_0, a_1) = (1, 1)$ in Family 6 and apply the transformation $x \to (30x + 24)$ to conclude to the polynomial family with $\rho(q, t, r) = 3/2$:

$$\begin{aligned} t(x) &= -1800x^3 - 3900x^2 - 2796x - 662 \\ r(x) &= 3600x^4 + 10800x^3 + 12132x^2 + 6048x + 1129 \\ q(x) &= 810000x^6 + 3510000x^5 + 6329700x^4 + 6078600x^3 + 3277725x^2 \\ &\quad + 940704x + 112237 \end{aligned}$$

Setting $h(x) = 25(3x + 2)^2$ we get the CM polynomial $f(x) = 12(400x^2 + 600x + 223)(3x + 2)^2$ and the generalized Pell equation:

$$(60x + 45)^2 - 3DY^2 = 18 \tag{15}$$

A different transformation in each example may result in some different curve parameters. Recall that we are searching for $x_0 \in \mathbb{Z}$ such that $q(x_0)$ and $r(x_0)$ are both primes. However, this condition can be further loosened if we allow $r(x_0)$ to contain a small cofactor $s$ [18]. Pell Equation (10) is considered as special because it is always solvable, for any positive and square free integer $D$. This is because the standard Pell equation $U^2 - 55DV^2 = 1$ is always solvable (see Theorem 4.1 [16]) and if $(U_i, V_i)$ is a solution of this equation, then $(10U_i, 10V_i)$ is a solution for (10). Thus we expect that Family 1 will produce more curve parameters compared to the other sparse families (see [7] for details). In Table 1 we present the number of suitable parameters obtained from Examples 1 to 6. The field size is between 128 and 960 bits, while for $D$ we set a limit up to $10^6$ which is a reasonable value in order to keep CM method efficient. For Examples 2 and 6, increasing the bound for $D$ will result in more suitable triples $(q, t, r)$. The table justifies our earlier claim that Family 1 has better chances in generating suitable curve parameters than any other family reported for $k \notin \{3, 4, 6\}$. We also found several examples for $k = 5$ that improve the examples appeared in [13] where a 252-bit prime $q$ is constructed using a CM discriminant $D$ with 7 decimal digits. Some examples of suitable parameters $(q, t, r)$ are given in the Appendix A.

**Table 1. Suitable parameters for $\mathbf{k} \in \{\mathbf{5}, \mathbf{8}, \mathbf{10}, \mathbf{12}\}$ $(\mathbf{128} \leq \log \mathbf{q} \leq \mathbf{960})$**

| **Construction** | **k** | $\mathbf{D < 10^5}$ | $\mathbf{D < 10^6}$ | $\rho(\mathbf{q}, \mathbf{t}, \mathbf{r})$ |
|---|---|---|---|---|
| **Example 1** | 5 | 12 | 47 | 3/2 |
| **Example 2** | 5 | 0 | 1 | 3/2 |
| **Example 3** | 10 | 2 | 4 | 1 |
| **Example 4** | 10 | 2 | 5 | 3/2 |
| **Example 5** | 8 | 1 | 5 | 3/2 |
| **Example 6** | 12 | 0 | 1 | 3/2 |

## 6 Conclusion

We presented two different methods for producing sparse families of pairing-friendly elliptic curves. We focus on the cases $k \in \{5, 8, 10, 12\}$, but our methods can be applied for every embedding degree. Particularly for $k = 5$, we introduce for the first time the use of Pell equations and presented an effective polynomial family leading to a Pell equation that produces more curve parameters than others. Furthermore our $\rho$-value $3/2$ sets a record on sparse families with $k = 5$. We also presented experimental results for the number of suitable triples $(q, t, r)$ obtained by every family of Section 5 for $k \in \{5, 8, 10, 12\}$.

## References

1. Atkin, A.O.L., Morain, F.: *Elliptic Curves and Primality Proving*. Mathematics of Computation, Vol. 61, pp. 29–68 (1993).
2. Barreto, P.S.L.M., Naehrig, M.: *Pairing-Friendly Elliptic Curves of Prime Order*. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331, Springer, Heidelberg (2006).
3. Boneh, D., Franklin, M.: *Identity-Based Encryption from the Weil Pairing*. SIAM Journal of Computing, Vol. 32(3). 586–615 (2003).
4. Brezing, F., Weng, A.: *Elliptic Curves Suitable for Pairing Based Cryptography*. Designs, Codes and Cryptography, Vol. 37, pp. 133–141 (2005).
5. Drylo, R.: *On Constructing Families of Pairing-Friendly Elliptic Curves with Variable Discriminant*. In: Bernstein, D.J., Chatterjee, S. (eds.) INDOCRYPT 2011. LNCS, vol. 7107, pp. 310–319, Springer, Heidelberg (2011).
6. Duan, P., Cui, S., Chan, C.W.: *Finding More Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems*. International Journal of Information Technology 2 (2), pp. 157–163 (2005).
7. Fotiadis, G., Konstantinou, E.: *On the Efficient Generation of Generalized MNT Elliptic Curves*. In: Muntean, T., Poulakis, D., Rolland, R. (eds.) CAI 2013. LNCS, vol. 8080, pp. 147–159. Springer, Berlin Heidelberg (2013).
8. Freeman, D.: *Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10*. In: Hess, F., Pauli, S., Pohst, M. (eds.) ANTS-VII 2006. LNCS, vol. 4076, pp. 452–465, Springer, Berlin (2006).
9. Freeman, D., Scott, M., Teske, E.: *A Taxonomy of Pairing-Friendly Elliptic Curves*. Journal of Cryptology, Vol. 23, pp. 224–280 (2010).
10. Galbraith, S.D., McKee, J., Valença, P.: *Ordinary Abelian Varieties Having Small Embedding Degree*. Finite Fields and Their Applications 13 (4), pp. 800–814 (2007).
11. Joux, A.: *A One Round Protocol for Tripartite Diffie-Hellman*. In: Bosma, W. (ed.) ANTS 2000. LNCS, vol. 1838, pp. 385–394, Springer, Heidelberg (2000).
12. Kachisa, E.J., Schaefer, E.F., Scott, M.: *Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field*. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 126–135, Springer, Heidelberg (2008).
13. Lee, H.S., Park, C.M.: *Generating Pairing-Friendly Elliptic Curves with the CM Equation of Degree 1*. In: Shacham, H., Waters, B. (eds.) Pairing 2009. LNCS, vol. 5671, pp. 66–77, Springer, Berlin Heidelberg (2009).
14. Miyaji, A., Nakabayashi, M., Takano, S.: *New Explicit Conditions of Elliptic Curve Traces for FR-Reduction*. IEICE Transactions Fundamentals E84-A (5), pp. 1234–1243 (2001).
15. Mollin, R.A.: *Fundamental Number Theory with Applications*. CRC Press, Boca Raton (1998).
16. Mollin, R.A.: *Simple Continued Fraction Solutions for Diophantine Equations*. Expositines Mathematicae 19, pp. 55–73 (2001).
17. Murphy, A., Fitzpatrick, N.: *Elliptic Curves for Pairing Applications*. IACR Eprint archive (2005). `http://eprint.iacr.org/2005/302/`
18. Scott, M., Barreto, P.S.L.M.: *Generating more MNT Elliptic Curves*. Designs, Codes and Cryptography, Vol. 38, pp. 209–217 (2006).
19. Tanaka, S., Nakamula, K.: *Constructing Pairing-Friendly Elliptic Curves Using Factorisation of Cyclotomic Polynomials*. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 136–145, Springer, Heidelberg (2008).

# A Additional Polynomial Families and Parameters of Proper Cryptographic Size

## A.1 Additional Polynomial Families for $\mathbf{k \in \{5, 10\}}$

We present two additional examples of sparse families for $k = 5, 10$. The following families are constructed from elements $\theta$ which depend only on $a_0, a_1 \in \mathbb{Q}$.

**Family 7** Let $\theta = a_0 + a_1\zeta_5 + 2a_1\zeta_5^2 + 6a_1\zeta_5^3$, with $a_0, a_1 \in \mathbb{Q}$ and $a_1 \neq 0$. The transition matrix has $\det(P) = -11^3a_1^6$ and we obtain the polynomials:

$$\begin{aligned}
u(x) &= (-6x^3 + (18a_0 + 22a_1)x^2 + (39a_1^2 - 18a_0^2 - 44a_0a_1)x \\
&\quad + (6a_0^3 + 22a_0^2a_1 - 39a_0a_1^2 - 1328a_1^3))/(11a_1)^3 \\
r(x) &= x^4 + (9a_1 - 4a_0)x^3 + (6a_0^2 - 27a_0a_1 + 21a_1^2)x^2 \\
&\quad + (27a_0^2a_1 - 4a_0^3 - 42a_0a_1^2 + 139a_1^3)x \\
&\quad + (a_0^4 - 9a_0^3a_1 + 21a_0^2a_1^2 - 139a_0a_1^3 + 881a_1^4) \\
f(x) &= (x^2 + (2a_1 - 2a_0)x + (a_0^2 - 2a_0a_1 - 19a_1^2))/11a_1^2
\end{aligned}$$

with $\rho(q, t, r) = 3/2$.

**Family 8** Let $\theta = a_0 + 4a_1\zeta_{10} - 9a_1\zeta_{10}^2 + 6a_1\zeta_{10}^3$, with $a_0, a_1 \in \mathbb{Q}$ and $a_1 \neq 0$. The transition matrix has $\det(P) = 5^2 11^3 a_1^6$ and we obtain the polynomials:

$$\begin{aligned}
u(x) &= (-3x^3 + (9a_0 + 72a_1)x^2 - (9a_0^2 + 144a_0a_1 + 490a_1^2)x \\
&\quad + (3a_0^3 + 72a_0^2a_1 + 490a_0a_1^2 - 324a_1^3))/605b^3 \\
r(x) &= x^4 - (4a_0 + 19a_1)x^3 + (6a_0^2 + 57a_0a_1 + 91a_1^2)x^2 \\
&\quad - (4a_0^3 + 57a_0^2a_1 + 182a_0a_1^2 - 371a_1^3)x \\
&\quad + (a_0^4 + 19a_0^3a_1 + 91a_0^2a_1^2 - 371a_0a_1^3 + 331a_1^4) \\
f(x) &= (2x^2 - (4a_0 + 19a_1)x + (2a_0^2 + 19a_0a_1 - 13a_1^2))/55a_1^2
\end{aligned}$$

with $\rho(q, t, r) = 3/2$.

## A.2 Curve Parameters of Proper Cryptographic Size

We give some examples of suitable integer triples $(q, t, r)$ obtained from the polynomial families described in Section 5. Recall that we considered cases where the order $r$ is not necessarily prime but it may contain a small cofactor $s$, in which case $r = s \cdot \tilde{r}$ for some large prime $\tilde{r}$. We also give some examples obtained by Freeman's family again considering $r$ as a nearly prime integer.

**Family of Example 1** (**$\mathbf{k = 5}$**)

$D = 107$

$x_0 = 1170622244439162529$

$q = 3113766234382774455114270638589661530299726194594217012542485406289821156755337582732809$

441432034923364570532141 (374 bits)

$t = 352917340712114878936613350792963264809459350656454770167$

$\tilde{r} = 153924325441846702408790989300257953361367647121303724027660177936902261$ (237 bits)

$s = 671$

$\rho = 1.5802$

---

$D = 141811$

$x_0 = -11994919643295$

$q = 36038725807179632846121982264894020506015116280644554421295633955149244889919168941$ (275 bits)

$t = -379677367285328888596979964823118201071433$

$r = 1138549877741377933395022094278669277536945192203801451$ (180 bits)

$\rho = 1.5272$

---

$D = 227715$

$x_0 = -6451333850566315667727$

$q = 87233333991933520436364492086029196902705342851777194616867647955622986668808024860010894$

0348738715309158652494135718896119867350695181 (449 bits)

$t = -59070579476397053688101033517360218652807824815338621499478343551033$

$r = 95271007237162045789384923633955286139031806991393577973739432727800408780288403427388411$

(296 bits)

$\rho = 1.5165$

---

$D = 383259$

$x_0 = -4133570859843463005$

$q = 60358396257221629182345603319603709624185200112850740092554000742162689307714418757327712$

558715354305776137285883341 (385 bits)

$t = -15538133254316186251355289076376868368098140548317354327583$

$\tilde{r} = 517967539003274709960997568423373862586544447314877703857401093284827959671$ (249 bits)

$s = 31$

$\rho = 1.5496$

---

$D = 584915$

$x_0 = 923586152635579344325$

$q = 75101713820205889762723839841611970090249093111475504738731273047109345166689007527938953$

26903475129355677294315246233807405985141 (432 bits)

$t = 173322489966196700451126893215802355630442497676479648477965499867$

$\tilde{r} = 629525458436623677361367527688019566219283592204259776270209146137288982600232581$ (269 bits)

$s = 63571$

$\rho = 1.6074$

---

$D = 879515$

$x_0 = -44614321100137293687$

$q = 95418174239059772134251115900324243294147299645849145168155742349228224690584734518526584$

469902051743344078888187791164381 (406 bits)

$t = -19536445351092892419034920540489034583449754390490653292958433$

$r = 217901311512235692233368368115403359841826330176190408953014913308137507745536211$ (267 bits)

$\rho = 1.5183$

---

**Family of Example 3 (k = 10)**

$D = 35707$

$x_0 = 184968976005653327177798$

$q = 29264127335801009923075618730398332208277331379369690762853077974906042604288972945954982$

$83$ (301 bits)

$t = 342135220845799562782407456500213155772327703 3$

$\tilde{r} = 57260607882184639852175799183316565623469177348339331566461603130898144603670340016 1$

(279 bits)

$s = 5110691$

$\rho = 1.08$

**Family of Example 4 (k = 10)**

$D = 203547$

$x_0 = 22135059892867860$

$q = 45213443809488309090269664562338678320921402080888190758160941573203714103166816660827656$

$4827307572973$ (338 bits)

$t = 1344818854857237775934665018462083587567592383545613$

$\tilde{r} = 950314324394168276687704680443726100035400288573930051829637131$ (210 bits)

$s = 7831$

$\rho = 1.6141$

**Family of Example 5 (k = 8)**

$D = 123998$

$x_0 = -4905703988594849146021$

$q = 72255852307496602190358838372039620872388857865993606551782283905685268613721698290007633$

$186373043500929463962638466668310049924398799$ (445 bits)

$t = 1344818854857237775934665018462083587567592383545613$

$r = 166800690696195508912807274002584741056682578896316371026683908097448317598808893213388889$

(279 bits)

$\rho = 1.5003$

$D = 249614$

$x_0 = -12121921090938970$

$q = 16447265702239232230524893751417864688297201974229296032271581948519955327250225227613898$

$691712275281$ (333 bits)

$t = 2564937870767183493536509519392814735984622274830 82$

$\tilde{r} = 10486332031231303372764054074012739342556761692856009203286692017$ (213 bits)

$s = 593$

$\rho = 1.5654$