Generating Pairing-Friendly Elliptic Curve Parameters Using Sparse Families

Georgios Fotiadis and Elisavet Konstantinou

Dept. of Information & Communication Systems Engineering
University of the Aegean
Karlovassi, Samos, 83200, Greece
{gfotiadis,ekonstantinou}@aegean.gr

Abstract. The majority of methods for constructing pairing-friendly elliptic curves are based on representing the curve parameters as polynomial families. There are three such types, namely complete, complete with variable discriminant and sparse families. In this paper, we present a method for constructing sparse families and produce examples of this type that have not previously appeared in the literature, for various embedding degrees. We provide numerical examples obtained by these sparse families, considering for the first time the effect of the recent progress on the tower number field sieve (TNFS) method for solving the discrete logarithm problem (DLP) in finite field extensions of composite degree.

Keywords: Pairing-based cryptography, pairing-friendly elliptic curves, sparse families, Pell equation.

1 Introduction

For a prime q, let $E/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius trace $t = q + 1 - \#E(\mathbb{F}_q)$, where $E(\mathbb{F}_q)$ is the group of $\mathbb{F}_q$-rational points, for which $\#E(\mathbb{F}_q) \approx q$. Let $E[r]$ be the r-torsion group of $E/\mathbb{F}_q$, for some $r \in \mathbb{Z}_{>0}$, containing all points of $E(\overline{\mathbb{F}}_q)$ with order r. Define also the *CM discriminant* $D > 0$ of the curve $E/\mathbb{F}_q$ as the square-free integer satisfying the *CM equation* $Dy^2 = 4q - t^2$, for some $y \in \mathbb{Z}$.

An *asymmetric pairing* on an ordinary elliptic curve $E/\mathbb{F}_q$ is a bilinear, non-degenerate, efficiently computable map of the form $\widehat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_\mathrm{T}$, where $\mathbb{G}_1, \mathbb{G}_2 \subset E(\mathbb{F}_q)$ and $\mathbb{G}_\mathrm{T} \subset \mathbb{F}_{q^k}^*$, such that $\#\mathbb{G}_1 = \#\mathbb{G}_2 = \#\mathbb{G}_\mathrm{T} = r$, for some prime r. The positive integer k is called the *embedding degree* of the curve $E/\mathbb{F}_q$ and it is the smallest integer, such that $E[r] \subseteq E(\mathbb{F}_{q^k})$. In pairing-based applications, the elliptic curves are chosen such that the following conditions are satisfied:

1. The order of the curve is $\#E(\mathbb{F}_q) = hr$, for a small *cofactor* $h \geq 1$ and a large prime r.
2. The ρ-value of the curve, defined as $\rho = \log q / \log r$ is close to 1, hence $\log q \approx \log r$.
3. The prime r must be large enough, so that the DLP in $\mathbb{G}_1$ and $\mathbb{G}_2$ is computationally hard.
4. The embedding degree k is large enough, so that the DLP in the extension field $\mathbb{F}_{q^k}$ and hence in $\mathbb{G}_\mathrm{T}$, is approximately as hard as in $\mathbb{G}_1, \mathbb{G}_2$.
5. The embedding degree k is small enough, for efficient operations in $\mathbb{G}_\mathrm{T}$.
6. The sizes of r and q^k provide at least an 128-bit security level, corresponding to an AES symmetric key, in the source groups $\mathbb{G}_1, \mathbb{G}_2$ and the target group $\mathbb{G}_\mathrm{T}$.

An elliptic curve $E/\mathbb{F}_q$ with embedding degree k satisfying these properties is called *pairing-friendly*.

Our purpose is to determine pairing-friendly elliptic curve parameters (q, t, r) satisfying the above conditions. There are two basic strategies for finding such triples, namely the Cocks-Pinch method [10] and the Dupont-Enge-Morain (DEM) method [5]. In both cases the trace of Frobenius

t is set as the lift of some integer in $(\mathbb{Z}/r\mathbb{Z})^*$. Therefore, t has approximately the same size as r, which in turn implies that the generic ρ-value is $\rho \approx 2$ in both methods. Such choices of parameters do not lead to efficient pairing computations, when considering the most well known variants of the Tate pairing, namely the Ate and twisted-Ate asymmetric pairings. This problem can be avoided by representing the elliptic curve parameters (q, t, r) as *polynomial families* $(q(x), t(x), r(x))$ in $\mathbb{Q}[x]$. There are three types of polynomial families depending on the form of the *CM polynomial* $f(x) = 4q(x) - t(x)^2$, which is the right-hand side of the CM equation expressed in polynomial terms.

Definition 1 ([3]) A polynomial family $(q(x), t(x), r(x))$ is *complete*, if there exists a $y(x) \in \mathbb{Q}[x]$, such that $f(x) = Dy(x)^2$, for some square-free $D > 0$. If $f(x) = g(x)y(x)^2$, for some $g(x) \in \mathbb{Q}[x]$ with $\deg g = 1$, the family is *complete with variable discriminant* and if $g(x)$ is quadratic, not a perfect square, with positive leading coefficient (i.e. $\mathrm{lc}(g) > 0$), the family is *sparse*.

When using polynomial families $(q(x), t(x), r(x))$, we can generate pairing-friendly triples by evaluating these polynomials at some $x_0 \in \mathbb{Z}$, such that $q(x_0)$ and $r(x_0)$ are both primes and $4q(x_0) - t(x_0)^2 = Dy^2$, for some square-free $D > 0$ and some $y \in \mathbb{Z}$. With this notation, $t(x_0)$ is the Frobenius trace, $q(x_0)$ is the base field prime and $r(x_0)$ is the prime dividing the order of the curve. The most well known method for constructing polynomial families is the Brezing-Weng method [2]. This is an extension of the Cocks-Pinch method, but now operations are performed in the polynomial field $\mathbb{Q}[x]/\langle r(x)\rangle$. In this case the size of the Frobenius trace $t(x_0)$ is smaller than the size of $r(x_0)$. More precisely, we obtain $\log t(x_0) = d \log r(x_0)$, where $d = 1/\deg r$ in the best case and $d = 1 - 1/\deg r$ in the worst case. This has several advantages compared to the Cocks-Pinch and DEM methods, implying that we can exploit the efficient Ate and twisted-Ate pairing computations when defined on Brezing-Weng elliptic curves.

Freeman et al. [10] suggested that for pairing applications, the sizes of curve parameters should be selected according to Table 1. The complexity of the DLP in the r-order subgroups

Table 1. Bit size of elliptic curve parameters and embedding degrees for various security levels.

Security Level	Subgroup Size	Extension Field Size	Embedding Degree	
			$\rho \approx 1$	$\rho \approx 2$
128	256	$3000 - 5000$	$12 - 20$	$6 - 10$
192	384	$8000 - 10000$	$20 - 26$	$10 - 13$
256	512	$14000 - 18000$	$28 - 36$	$14 - 18$

$\mathbb{G}_1, \mathbb{G}_2 \subset E(\mathbb{F}_q)$ is $O(\sqrt{r})$ (Pollard's rho method). For the DLP in finite field extensions $\mathbb{F}_{q^k}$ there has been recently a progress on the tower number field sieve (TNFS) method [13, 16] that affects its complexity when k is composite. These new improvements imply that when k is prime, we can follow the recommendations of Table 1 for selecting curve parameters, but when k is composite, Table 1 should be updated.

Complete families are studied in [1, 2, 12, 23, 24] and they are attractive for applications due to their small CM discriminant. However, in [6] it is recommended to use curves with large discriminant to avoid various attacks on the DLP. This is achieved by the other two types. Complete families with variable discriminant are studied in [3, 10, 14]. Sparse families for $k = 3, 4, 6$ are constructed in [4, 7, 11, 17, 21], but offer a low security level of 80-bits. Consequently, we need to search for

sparse families with $k \notin \{3, 4, 6\}$ and so far there are only few such examples in the literature. The first is due to Freeman for $k = 10$ and $\rho = 1$. There are also two examples for $k = 8, 12$ and $\rho \approx 1.5$ presented in [3], while in [8] we introduced sparse families for $k = 5, 10$ with $\rho \approx 1.5$.

In this paper we focus on the construction of sparse families for various embedding degrees. Particularly our contribution is threefold:

1. We propose a method for producing sparse families with for any k that combines previous work presented in [3, 14]. Firstly, we apply Lee-Park's method [14] in order to determine polynomials $r(x)$, $t(x)$ and then Dryło's method [3] for constructing CM polynomials of Definition 1.
2. We introduce more sparse families for $k \in \{5, 8, 10, 12\}$ and the first examples in the literature for a variety of other k as well, with $\rho \leq 2$.
3. We produced numerical examples of cryptographic value, considering the recent progress on the TNFS method for reducing the complexity of the DLP in finite field extensions of composite degree [13, 16].

The rest of the paper is organized as follows. In Section 2 we present the necessary background related to pairing-friendly elliptic curves and overview the most important work on the three types of polynomial families. We analyze our method in Section 3 and demonstrate our experimental results in Section 4. We conclude the paper in Section 5.

2 Background and Previous Work

Recall that our goal is to determine suitable integer triples (q, t, r) for some fixed and relatively small embedding degree k. So far, the best ρ-values are achieved when representing q, t, r as polynomial families $(q(x), t(x), r(x))$ in $\mathbb{Q}[x]$ respectively.

Definition 2 ([10]) Let $q(x), t(x), r(x) \in \mathbb{Q}[x]$ be non-zero polynomials. We say that a 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 are satisfied:

1. $q(x)$ represents primes, i.e. it is non-constant, irreducible, with positive leading coefficient. Additionally, $q(x) \in \mathbb{Z}$, for some (or infinitely many) $x \in \mathbb{Z}$ and $\gcd(\{q(x) : x, q(x) \in \mathbb{Z}\}) = 1$,
2. $r(x)$ is non-constant, irreducible, integer-valued, with positive leading coefficient,
3. $r(x)$ divides both $q(x)+1-t(x)$ and $\Phi_k(t(x)-1)$, where $\Phi_k(x)$ is the k^{th} cyclotomic polynomial,
4. there are infinitely many integer solutions (x, Y) for the *parameterized CM equation*

$$DY^2 = 4q(x) - t(x)^2. \tag{2.1}$$

The ρ-value of a polynomial family $(q(x), t(x), r(x))$ is defined as $\rho(q, t, r) = \deg q / \deg r$. The condition $r(x) \mid (q(x)+1-t(x))$ implies that $\#E(\mathbb{F}_{q(x)}) = q(x)+1-t(x) = h(x)r(x)$, for a cofactor $h(x) \in \mathbb{Q}[x]$. Substituting into Equation (2.1) we obtain:

$$DY^2 = 4h(x)r(x) - (t(x) - 2)^2. \tag{2.2}$$

The condition $r(x) \mid \Phi_k(t(x)-1)$ means that $t(x)-1$ is a primitive k^{th}-root of unity in $\mathbb{Q}[x]/\langle r(x)\rangle$. Finding polynomials $t(x), r(x)$ satisfying this condition is not straightforward. Usually $r(x)$ is taken as the k^{th} cyclotomic polynomial for some $k > 0$. More results can be obtained if we allow $r(x)$ to be an irreducible polynomial dividing $\Phi_k(t(x) - 1)$, for some $t(x) \in \mathbb{Q}[x]$ (see for example [14, 23]). Once $r(x)$ is fixed, we must obtain a solution (x_0, Y_0) for Equation (2.1), such that $q(x_0)$ and

$r(x_0)$ are large primes. Then we apply the CM method to construct an elliptic curve $E/\mathbb{F}_{q(x_0)}$, with Frobenius trace $t(x_0)$ and order $\#E(\mathbb{F}_{q(x_0)}) = h(x_0)r(x_0)$, requesting $h(x_0)$ to be small.

Let $f(x) = 4q(x) - t(x)^2 \in \mathbb{Q}[x]$ be the CM polynomial of the form $f(x) = g(x)y(x)^2$, with $y(x), g(x) \in \mathbb{Q}[x]$ and $\deg g \leq 2$. By Definition 1, if $\deg g = 0$ the family $(q(x), t(x), r(x))$ is complete and thus $f(x) = Dy(x)^2$ for some square-free $D > 0$. If $\deg g = 1$, the family is complete with variable discriminant and finally, if $\deg g = 2$, with $g(x)$ not a perfect square and $\mathrm{lc}(g) > 0$, the family is sparse.

Complete Families: The most common method for constructing complete families is due to Brezing and Weng [2]. This method starts by fixing an embedding degree k and a square-free CM discriminant D. Then, it chooses an irreducible polynomial $r(x) \in \mathbb{Q}[x]$, such that $\zeta_k, \sqrt{-D} \in \mathbb{Q}[x]/\langle r(x)\rangle$, where ζ_k is a primitive k^{th}-root of unity. Finally, it sets $t(x)$ and $y(x)$ as the polynomials mapping to ζ_k+1 and $(\zeta_k-1)/\sqrt{-D}$ respectively and $q(x) = (t(x)^2+Dy(x)^2)/4$. For more examples of this type of families, see [10, 12, 23, 24].

The small discriminants make complete families very attractive for implementations. However, according to [6] we need larger CM discriminants to avoid various attacks on the DLP. This is done by the other two types of polynomial families, for which the CM discriminant has a polynomial representation. Note however that although larger CM discriminants might be preferable, these values should not be too large, since a large D would affect the efficiency of the CM method. More precisely, the CM discriminant D should be at most 10^{13}, which is the current record for constructing Hilbert class polynomials using the Chinese Remainder Theorem (see [22]).

Complete Families with Variable Discriminant: By Definition 1 the CM polynomial is $f(x) = g(x)y(x)^2$ and $\deg g = 1$. These families can be constructed via the Brezing-Weng method by replacing the square-free integer D with a linear term $g(x)$, such that $\sqrt{-g(x)} \in \mathbb{Q}[x]/\langle r(x)\rangle$. Such examples appear in [3, 10, 14, 15]. Although this type offers more flexible CM-discriminant, the choices are still limited, especially as the value k increases. In particular, in order to find suitable parameters with this type of families, we are searching for $x_0 = Dy^2 \in \mathbb{Z}$, such that $r(x_0)$ and $q(x_0)$ are both primes of reasonable size and so as $\deg r$ grows, the choices for D are limited.

Sparse Families: The CM polynomial is $f(x) = g(x)y(x)^2$, where $g(x)$ is quadratic, non-square, with $\mathrm{lc}(g) > 0$. With sparse families, curve parameters derive from the solutions of a generalized Pell equation. The first examples were the *MNT families* (see [17] and [4, 7, 11, 21]) for $k \in \{3, 4, 6\}$ and $\rho(q, t, r) = 1$. These are ideal families in terms of the ρ-value, but correspond to a low security level of 80-bits. In [9], Freeman introduced a sparse family for $k = 10$ with $\rho(q, t, r) = 1$ and Dryło [3] proposed a method for producing sparse families offering two new examples for $k = 8, 12$ with $\rho(q, t, r) = 1.5$. We note that Freeman's family is the only known ideal sparse family in terms of ρ, for $k \neq 3, 4, 6$. Finally, in [8] we described two alternatives for producing sparse families. In the first we are searching for polynomials $r(x), t(x)$, such that $f(x) \equiv -(t(x) - 2)^2 \bmod r(x) = g(x)y(x)^2$, while in the second we are searching for a cofactor $h(x)$, such that $f(x) = 4h(x)r(x) - (t(x) - 2)^2 = g(x)y(x)^2$. We generated new examples for $k = 5, 10$ and $\rho(q, t, r) = 1.5$.

Contribution: We argue that sparse families offer more flexibility on the CM discriminant, but for $k \notin \{3, 4, 6\}$ are very rare. Additionally, numerical examples of suitable parameters (q, t, r) obtained from sparse families can be found in the literature only for Freeman's family [9] and in

our earlier work [8], for $k = 5, 10$. Motivated by these facts, we further study the construction of this type of families. In particular, our contribution is summarized as follows:

The proposed method: We propose a method that combines Lee-Park's [14] and Dryło's [3] ideas. More precisely, we first apply Lee and Park's method for constructing polynomials $t(x)$ and $r(x)$, such that $r(x) \mid \Phi_k(t(x) - 1)$. Then, we follow Dryło's process in order to fix a CM polynomial $f(x) = g(x)y(x)^2$, for some non-square $g(x) \in \mathbb{Q}[x]$, with $\deg g = 2$ and $\mathrm{lc}(g) > 0$. In particular, we are searching for an element $z(x) \in \mathbb{Q}[x]/\langle r(x)\rangle$, such that $-z(x)^2 \equiv g(x) \bmod r(x)$. This condition allowed us to produce more sparse families than any other work focusing on this type of families.

New families: Using this method, we produced new sparse families for various embedding degrees $k \neq 3, 4, 6$ that have not previously appeared in the literature, with $\rho(q, t, r) < 2$. Additionally, Table 1 indicates that families with $\rho(q, t, r) \approx 2$ are also likely to offer a balanced security level in the three groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_\mathrm{T}$ of a pairing. This motivates us to introduce the first sparse families in the literature with $\rho(q, t, r) = 2$.

Experimental results: We implemented the proposed method together with a Pell equation solver and produced several pairing-friendly parameters. Our results are aiming for security levels of at least 128-bit AES key, which is today's state of the art. The values q and r are chosen with respect to Table 1 for prime k. On the other hand, for composite k the extension field size $k \log q$ is taken larger than the recommended values of Table 1 (see [6]), in order to surpass the threat of the new variants of the TNFS method [13, 16]. Finally, in our examples we have considered CM discriminants up to $2 \cdot 10^6$. More examples can be obtained by allowing even larger D.

3 Sparse Families of Pairing-Friendly Elliptic Curves

To construct sparse families of pairing-friendly elliptic curves, the first step is to find an irreducible polynomial $r(x) \in \mathbb{Q}[x]$ and a trace polynomial $t(x) \in \mathbb{Q}[x]$, such that $r(x) \mid \Phi_k(t(x) - 1)$ for some fixed k. In order to implement this we adopt Lee and Park's method [14]. Once these polynomials are constructed, the next step is to determine a non-square polynomial $g(x)$, with $\deg g = 2$ and $\mathrm{lc}(g) > 0$, such that the CM polynomial is $f(x) = g(x)y(x)^2$, with $y(x) \in \mathbb{Q}[x]$. For this step we use Dryło's method [3]. The construction of the remaining polynomials $y(x), q(x)$ is straightforward.

Finding the polynomial r(x): Following Lee and Park [14], we start by choosing an arbitrary embedding degree $k \notin \{1, 2, 3, 4, 6\}$ and fixing an element $\theta \in \mathbb{Q}(\zeta_k)$ of the form:

$$\theta = a_0 + a_1\zeta_k + a_2\zeta_k^2 + \cdots + a_{\varphi(k)-1}\zeta_k^{\varphi(k)-1} \tag{3.1}$$

such that $u(\theta) = \zeta_k$ in $\mathbb{Q}(\zeta_k)$, for some $u(x) \in \mathbb{Q}[x]$ and $a_i \in \mathbb{Q}$, for every $i = 0, \ldots, \varphi(k) - 1$. Let $\mathcal{B}(\theta)$ and $\mathcal{B}(\zeta_k)$ be the following sets:

$$\mathcal{B}(\theta) = \left\{1, \theta, \ldots, \theta^{\varphi(k)-1}\right\} \qquad \text{and} \qquad \mathcal{B}(\zeta_k) = \left\{1, \zeta_k, \ldots, \zeta_k^{\varphi(k)-1}\right\}.$$

The polynomial $u(x)$ can be found by constructing the *transition matrix* P from the set $\mathcal{B}(\theta)$ to $\mathcal{B}(\zeta_k)$, which is a $\varphi(k) \times \varphi(k)$ matrix with elements P_{ij} obtained by the relation:

$$\theta^j = \sum_{i=0}^{\varphi(k)-1} P_{ij}\zeta_k^i, \qquad \text{for each} \qquad j = 0, 1, \ldots \varphi(k) - 1. \tag{3.2}$$

If $\det(P) \neq 0$, the transition matrix P has an inverse $P^{-1} = (P'_{ij})$ and we set $u(x)$ as:

$$u(x) = \sum_{i=0}^{\varphi(k)-1} P'_{i1} x^i. \tag{3.3}$$

By Lemma 2 in [14], $\Phi_k(u(x))$ has an irreducible factor of degree $\varphi(k)$, which is set as $r(x)$. Additionally, with this setup we get that $u(x)$ is a primitive k^{th}-root of unity in $K = \mathbb{Q}[x]/\langle r(x)\rangle$. Note also that the coefficients of $u(x)$ are multivariate polynomials in $\mathbb{Q}[a_0, a_1, \ldots, a_{\varphi(k)-1}]$ and so we need to ensure that $a_0, a_1, \ldots, a_{\varphi(k)-1} \in \mathbb{Q}$ are chosen such that $\det(P) \neq 0$.

The complexity of this procedure depends on the value $\varphi(k) = \deg r$ and as this value grows, the efficiency of the process is affected. In our examples we used this method for cases where $\varphi(k) = 4$, corresponding to embedding degrees 5, 8, 10 and 12, but the method can be applied also for higher embedding degrees. We can avoid this procedure by setting $r(x)$ as the k^{th}-cyclotomic polynomial, where in this case $u(x) = x$ represents a primitive k^{th}-root of unity in $K = \mathbb{Q}[x]/\langle r(x)\rangle$.

Searching for g(x): After constructing $u(x)$ and $r(x)$, the next step is to find a quadratic, non-square polynomial $g(x)$ with $\text{lc}(g) > 0$, such that $\sqrt{-g(x)} \in K = \mathbb{Q}[x]/\langle r(x)\rangle$. In other words, we need to find an element $z(x) \in K$, such that $-z(x)^2 = g(x)$ in K. We write:

$$z(x) = z_{\varphi(k)-1} x^{\varphi(k)-1} + \cdots + z_2 x^2 + z_1 x + z_0 \tag{3.4}$$

and we are searching for $z_0, z_1, \ldots, z_{\varphi(k)-1} \in \mathbb{Q}$, such that $-z(x)^2 \bmod r(x)$ is quadratic, non-square, with positive leading coefficient. However we do not need to search all the $\varphi(k)$ variables z_i. In particular we set:

$$-z(x)^2 \equiv \left[\sum_{i=0}^{\varphi(k)-1} g_i(z_0, z_1, \ldots, z_{\varphi(k)-1}) x^i \right] \bmod r(x), \tag{3.5}$$

where all $g_i(z_0, z_1, \ldots, z_{\varphi(k)-1})$ are multivariate polynomials with rational coefficients that represent the coefficients of $g(x)$. Since we wish $-z(x)^2$ to be a quadratic, we set $g_i(z_0, z_1, \ldots, z_{\varphi(k)-1}) = 0$, for all $i = 3, 4, \ldots, \varphi(k) - 1$. Solving this system will eliminate some of the z_i and hence improve the efficiency of the search. Finally we need $g_2(z_0, z_1, \ldots, z_{\varphi(k)-1}) > 0$ and the discriminant of $g(x)$ to be non-zero, so that $g(x)$ is not a perfect square. This process is also described in [3].

Computing the remaining polynomials: So far we have determined the polynomial $r(x)$, a polynomial $u(x)$ representing a primitive k^{th}-root of unity in $K = \mathbb{Q}[x]/\langle r(x)\rangle$, the non-square, quadratic polynomial $g(x)$, with $\text{lc}(g) > 0$ and a polynomial $z(x) = \sqrt{-g(x)}$ in K. Following the original Brezing-Weng method [2], we can compute the remaining polynomials in the following way. For each primitive k^{th}-root of unity $\zeta_k \longmapsto [u(x)^j \bmod r(x)]$, with $j = 1, 2, \ldots, \varphi(k) - 1$, such that $\gcd(j, k) = 1$ we set $t(x) \equiv [u(x)^j + 1] \bmod r(x)$ and

$$y(x) \equiv \left[\left(u(x)^j - 1 \right) z(x)^{-1} \right] \bmod r(x) = \left[\sum_{i=0}^{\varphi(k)-1} y_i(z_0, z_1, \ldots, z_{\varphi(k)-1}) x^i \right], \tag{3.6}$$

where $z(x)^{-1}$ is the multiplicative inverse of $z(x)$ in $\mathbb{Q}[x]/\langle r(x)\rangle$. We then set the CM and field polynomials as $f(x) = g(x)y(x)^2$ and $q(x) = [t(x)^2 + f(x)]/4$ respectively. Note that the field polynomial must represent primes in the sense of Definition 2. If this is true, we have a sparse family $(q(x), t(x), r(x))$ of pairing-friendly elliptic curves with embedding degree k.

Additional conditions: With our construction, we have $\deg t, \deg y \leq \varphi(k) - 1$ and $\deg f = \deg g + 2\deg y = 2 + 2\deg y \leq 2\varphi(k)$. Thus the ρ-value of these polynomial families is:

$$\rho(q,t,r) = \frac{\deg q}{\deg r} = \frac{\deg\left[t(x)^2 + f(x)\right]}{\deg r} = \frac{\max\{2\deg t, 2 + 2\deg y\}}{\deg r} \leq 2.$$

For ρ-values less than 2, we need the degree of $y(x)$ to be less than $\varphi(k) - 1$ and so we set:

$$y_{\varphi(k)-1}(z_0, z_1, \ldots, z_{\varphi(k)-1}) = 0.$$

This is an extra equation in $(z_0, z_1, \ldots, z_{\varphi(k)-1})$ and using it we can eliminate more of the z_i. However, we also give examples with $\rho(q,t,r) = 2$, in which case the above equation must be non-zero. Even more z_i can be eliminated if we allow the polynomial $g(x)$ to have the same leading coefficient and constant term. In other words this is written as:

$$g_2(z_0, z_1, \ldots, z_{\varphi(k)-1}) = g_0(z_0, z_1, \ldots, z_{\varphi(k)-1}).$$

Most of the examples presented in this work respect this additional properties.

Algorithm 1 Sparse families of pairing-friendly elliptic curves.

Input: An embedding degree $k \notin \{1, 2, 3, 4, 6\}$.
Output: A sparse family $(q(x), t(x), r(x))$ of pairing-friendly elliptic curves with embedding degree k.

1: Fix an element $\theta \in \mathbb{Q}(\zeta_k)$ as in Equation (3.1) such that $\det(P) \neq 0$.
2: Compute $u(x) \in \mathbb{Q}[x]$ by Equation (3.3).
3: Set $r(x)$ as the degree $\varphi(k)$ factor of $\Phi_k(u(x))$ and $K = \mathbb{Q}[x]/\langle r(x)\rangle$.
4: Set $z(x)$ as in Equation (3.4) and calculate the multivariate polynomials $g_i(z_0, z_1, \ldots, z_{\varphi(k)-1})$ by Equation (3.5), for all $i = 0, 1, \ldots, \varphi(k) - 1$.
5: For each $j = 1, 2, \ldots, \varphi(k) - 1$, such that $\gcd(j, k) = 1$ solve the system (3.7).
6: If a solution $(z_0, z_1, \ldots, z_{\varphi(k)-1})$ exists, set:

$$t(x) \equiv \left[u(x)^j + 1\right] \bmod r(x), \quad y(x) \equiv \left[(u(x)^j - 1)z(x)^{-1}\right] \bmod r(x), \quad g(x) = \sum_{i=0}^{2} g_i(z_0, z_1, \ldots, z_{\varphi(k)-1})x^i.$$

7: Set $f(x) = g(x)y(x)^2$ and $q(x) = [t(x)^2 + f(x)]/4$.
8: If $q(x)$ represents primes, return $(q(x), t(x), r(x))$.

Summary and the algorithm: Summarizing, the conditions that need to be met for the coefficients $(z_0, z_1, \ldots, z_{\varphi(k)-1})$ of the polynomial $z(x) \in K$, lead to the system of multivariate equations:

$$\left.\begin{aligned} g_{\varphi(k)-1}(z_0, z_1, \ldots, z_{\varphi(k)-1}) = \ldots = g_3(z_0, z_1, \ldots, z_{\varphi(k)-1}) &= 0 \\ g_2(z_0, z_1, \ldots, z_{\varphi(k)-1}) &> 0 \\ \Delta_g &\neq 0 \\ y_{\varphi(k)-1}(z_0, z_1, \ldots, z_{\varphi(k)-1}) &= 0 \quad \text{(optional)} \\ g_2(z_0, z_1, \ldots, z_{\varphi(k)-1}) - g_0(z_0, z_1, \ldots, z_{\varphi(k)-1}) &= 0 \quad \text{(optional)} \end{aligned}\right\} \tag{3.7}$$

where Δ_g denotes the discriminant of the polynomial $g(x)$. If we wish to construct sparse families with $\rho(q,t,r) = 2$, we need to exclude the fourth condition from System (3.7). Additionally, we can find more suitable polynomials $g(x)$ by excluding the last condition of System (3.7). The above process is described in Algorithm 1.

Remark 1 Note that if $(z_0, z_1, \ldots, z_{\varphi(k)-1})$ is a suitable solution of system (3.7) then the $\varphi(k)$-tuple $(nz_0, nz_1, \ldots, nz_{\varphi(k)-1})$, for any $n \in \mathbb{Q}/\{0\}$, is also a solution for this system, but it will generate the same sparse family. Furthermore two quadratic polynomials $g(x)$ and $g'(x)$ are said to be *equivalent*, if there is a linear transformation $x \to (ay + b)$, such that $g'(x) = g(ay + b)$. In this case, the polynomials $g(x)$ and $g'(x)$ also generate the same sparse family. □

Since we are searching for integer triples (q, t, r), we need to ensure that for each output of Algorithm 1 the polynomials $q(x), t(x)$ and $r(x)$ have integer coefficients. In order to do this, we need to find the smallest positive integer n, such that $nq(x) \in \mathbb{Z}[x]$ and then search for the smallest positive factor m of n, such that $q(mx + l) \in \mathbb{Z}[x]$, for some integer $l \in [-m, m]$ (see [12, 14] for details). However, such a linear transformation does not always exist. If it does, we apply it on $q(x), t(x)$ and $r(x)$ and test if $q(mx + l)$, $t(mx + l)$ and $r(mx + l)$ have integer coefficients.

3.1 Cyclotomic Sparse Families

When $r(x)$ is the k^{th} cyclotomic polynomial $\Phi_k(x)$, for some fixed k, then $u(x) = x$ and we omit the first three steps of Algorithm 1. With this setup, every power x^j for $j = 1, \ldots, \varphi(k) - 1$ such that $\gcd(j, k) = 1$ is a primitive k^{th}-root of unity in $\mathbb{Q}[x]/\langle r(x)\rangle$. We here give the first cyclotomic sparse families in the literature for embedding degrees $k \in \{5, 7, 8, 9, 10, 12, 14, 15, 18, 20, 30\}$ and $\rho(q, t, r) \leq 2$. Note that as $\varphi(k)$ grows, it is harder to determine a suitable element $z(x) \in K$. The following results are restricted for cases where $\varphi(k) \leq 8$.

The case k = 5 : We have $r(x) = \Phi_5(x)$ and thus $z(x) = z_3x^3 + z_2x^2 + z_1x + z_0$. Setting $g_3(z_0, z_1, z_2, z_4) = 0$ we get that:

$$z(x) = z_3x^3 + z_2x^2 + z_1x + \frac{z_2^2 + 2z_3z_1 - 2z_2z_1}{2z_3},$$

and in this case $\deg g = 2$. Furthermore, adding the condition $g_2(z_0, z_1, z_2, z_4) = g_0(z_0, z_1, z_2, z_4)$,

Table 2. Cyclotomic sparse families for k with $\varphi(k) = 4$ and $\rho(q, t, r) = 1.5$.

Family	k	$t(x)$	$g(x)$	$y(x)$	x_0
1	5	$x + 1$	$3x^2 - 2x + 3$	$-(2x^2 + 2x + 1)$	$x_0 \in \mathbb{Z}$
2	5	$x^3 + 1$	$4x^2 + 7x + 4$	$x^2 + 1$	1 mod 2
3	8	$-x^3 + 1$	$7x^2 - 26x + 7$	$-(3x^2 - x + 3)/17$	{8, 15} mod 17
4	8	$-x^3 + 1$	$14x^2 - 20x + 14$	$(x^2 + 2x + 1)/2$	1 mod 2
5	10	$x^3 + 1$	$12x^2 - 3x + 4$	$(x^2 + 2x + 3)/11$	{7, 13} mod 22
6	10	$x^3 + 1$	$3x^2 + 10x + 3$	$(x^2 + 3x + 1)/11$	{2, 6} mod 11
7	10	$x^3 + 1$	$15x^2 + 50x + 15$	$(7x^2 - x + 7)/55$	{2, 13, 17, 28} mod 55
8	10	$-x^3 + x^2 - x + 2$	$20x^2 - 35x + 20$	$(x^2 + x)/5$	0 mod 10

we get $z_2 = 0$ or $z_2 = 2z_3$. In the first case if we set $t(x) = x + 1$ and $y_3(z_0, z_1, z_2, z_4) = 0$ we obtain $z_3 = 2z_1$. In the second case we set $t(x) = x^3 + 1$ and then the polynomial $y(x)$ is quadratic. We conclude to the following polynomials $z(x)$:

$$z(x) = 2z_1x^3 + z_1x + z_1, \quad \text{for} \quad t(x) = x + 1$$
$$z(x) = z_3x^3 + 2z_3z^2 + z_1x + 2z_3 - z_1, \quad \text{for} \quad t(x) = x^3 + 1$$

In the first polynomial $z(x)$ we set $z_1 = 1$ and obtain the first family of Table 2. By Remark 1, taking any other $z_1 \in \mathbb{Q}$ will lead us to an equivalent family. For the second case we give an example for $(z_1, z_3) = (2, 1)$ in Table 2. Polynomial families with $k = 5$ and $\rho(q, t, r) = 1.5$ correspond to a security level below 128-bits in the extension field $\mathbb{F}_{q^5}$, for a 256-bit prime r. In order achieve a security level around 128-bits we consider sparse families with $\rho(q, t, r) = 2$. Note that in this case we require $\deg y = 3$ and hence $y_3(z_0, z_1, z_2, z_3) \neq 0$. Such examples are presented in Table 5.

The case k = 8 : Quadratic polynomials $g(x)$ can be obtained by setting the polynomial $z(x)$ as:

$$z(x) = z_3x^3 + z_2x^2 + z_1x - \frac{z_1z_2}{z_3}.$$

Adding the condition $g_2(z_0, z_1, z_2, z_3) = g_0(z_0, z_1, z_2, z_3)$ we get that $z_2 = \pm z_3$ and for $t(x) = \pm x^3+1$ respectively we have $y_3(z_0, z_1, z_2, z_3) = 0$. In other words we conclude to the polynomials $z(x)$ of the form:

$$z(x) = z_3x^3 \pm z_3x^2 + z_1x \mp z_1, \quad \text{for} \quad t(x) = \pm x^3 + 1.$$

Examples for $(z_1, z_3) \in \mathbb{Q}^2 \setminus (0, 0)$ with $\rho(q, t, r) = 1.5$ and $\rho(q, t, r) = 2$ appear in Tables 2 and 5.

The case k = 10 : In [9], Freeman presented a sparse family for $k = 10$ and $\rho(q, t, r) = 1$. This is the only known ideal sparse family in terms of the ρ-value for $k \neq 3, 4, 6$. We give more examples with $\rho(q, t, r) = 1.5$ and $\rho(q, t, r) = 2$ in Tables 2 and 5 respectively. In particular, in order to obtain a quadratic polynomial $g(x)$ we set:

$$z(x) = z_3x^3 + z_2x^2 + z_1x - \frac{z_2^2 + 2z_3z_1 + 2z_2z_1}{2z_3}.$$

Adding the constraint $g_2(z_0, z_1, z_2, z_3) = g_0(z_0, z_1, z_2, z_3)$ we get that $z_2 = 0$ or $z_2 = -2z_3$. In the first case, for $t(x) = x^3 + 1$, the polynomial $y(x)$ is quadratic and so we have:

$$z(x) = z_3x^3 + z_1x - z_1, \quad \text{for} \quad t(x) = x^3 + 1.$$

In the second case we add the condition $y_3(z_0, z_1, z_2, z_3) = 0$, in which case for $t(x) = -x^3+x^2-x+2$ we get $z_1 = 4z_3/3$. Then we have:

$$z(x) = z_3x^3 - 2z_3x^2 + \frac{4z_3}{3}x - \frac{2z_3}{3}, \quad \text{for} \quad t(x) = -x^3 + x^2 - x + 2.$$

Sparse families with $\rho(q, t, r) = 1.5$ are presented for both cases in Table 2 and with $\rho(q, t, r) = 2$ in Table 5. In these tables we also give examples of sparse families with polynomials $g(x)$ such that $g_2(z_0, z_1, z_2, z_3) \neq g_0(z_0, z_1, z_2, z_3)$.

For $k = 12$ we could not find any examples of cyclotomic sparse families. However we cover this case by taking $r(x)$ as a non-cyclotomic polynomial. For $k = 5, 8, 10$ and 12 the construction of suitable polynomials $z(x)$ is easy, since the degree of the polynomial $r(x)$ is small, i.e. $\deg r = \varphi(k) = 4$. When $\varphi(k)$ increases, this search is much harder. However we give a few examples for $\deg r = 6, 8$ in the following paragraphs.

The case where $\varphi(k) = 6$: When $\varphi(k) = 6$, the embedding degree is 7, 9, 14 or 18 and since $r(x) = \Phi_k(x)$ we have $\deg r = 6$. In such cases $z(x) \in \mathbb{Q}[x]$ is a degree 5 polynomial, written as $z(x) = z_5x^5 + z_4x^4 + z_3x^3 + z_2x^2 + z_1x + z_0$. Then we can easily eliminate at least two of its coefficients, namely z_0 and z_1, by solving the equations:

$$g_5(z_0, z_1, z_2, z_3, z_4, z_5) = g_4(z_0, z_1, z_2, z_3, z_4, z_5) = 0$$

in terms of z_0 and z_1 respectively. Examples of sparse families for these cases appear in Table 3

Table 3. Cyclotomic sparse families for k with $\varphi(k) = 6$ and $\rho(q, t, r) = 1.6667$.

Family	k	$t(x)$	$g(x)$	$y(x)$	x_0
1	7	$x^5 + 1$	$208x^2 + 375x + 208$	$(38x^4 - 23x^3 + 50x^2 - 23x + 38)/71$	$\{37, 91, 103, 119\}$ mod 142
2	9	$x^5 + 1$	$8x^2 + 35x + 8$	$-(x^4 - 18x^3 - 4x^2 - 18x + 1)/109$	$\{27, 105, 147, 175\}$ mod 218
3	9	$x^5 + 1$	$51x^2 + 126x + 51$	$(47x^4 + x^3 + 57x^2 + x + 47)/543$	$\{43, 73, 424, 442\}$ mod 543
4	14	$x^5 + 1$	$4x^2 + 5x + 4$	$-(2x^4 - 5x^3 + 6x^2 - 5x + 2)$	1 mod 2
5	18	$x^5 + 1$	$4x^2 + 9x + 4$	$-(3x^4 - 2x^3 - 8x^2 - 2x + 3)/19$	$\{3, 13, 15, 33\}$ mod 38
6	18	$x^5 + 1$	$19x^2 + 30x + 19$	$-(3x^4 + 5x^3 - 7x^2 + 5x + 3)/37$	$\{3, 4, 25, 28\}$ mod 37

for $\rho(q, t, r) = 1.6667$ and in Table 6 for $\rho(q, t, r) = 2$. These are the first sparse families in the literature for $k \in \{7, 9, 14, 18\}$. Note that when $k = 7$, we can choose suitable parameters following Table 1, since this case is not affected by the exTNFS or SexTNFS methods [13, 16]. In the other three cases, the embedding degree is composite and hence we need to update the recommendations of Table 1, in order to avoid the new TNFS attacks.

Table 4. Cyclotomic sparse families for k with $\varphi(k) = 8$, $t(x) = x^7 + 1$ and $\rho(q, t, r) = 1.75$.

k	$g(x)$	$y(x)$	x_0
30	$155x^2 + 350x + 155$	$(433x^6 - 293x^5 - 149x^4 + 637x^3 - 149x^2 - 293x + 433)/9755$	$\{707, 1003, 1228, 1348, 2658$ $3582, 5533, 6042, 7993, 8807$ $9032, 9152\}$ mod 9755

The case where $\varphi(k) = 8$: This case corresponds to embedding degrees 15, 16, 20, 24, 30. We have $\deg r = 8$ and $z(x) \in \mathbb{Q}[x]$ is written as $z(x) = z_7x^7 + z_6x^6 + z_5x^5 + z_4x^4 + z_3x^3 + z_2x^2 + z_1x + z_0$. In such cases we can eliminate the three coefficients z_0, z_1, z_2 by solving the system of equations:

$$g_7(z_0, z_1, z_2, z_3, z_4, z_5, z_6, z_7) = g_6(z_0, z_1, z_2, z_3, z_4, z_5, z_6, z_7) = g_5(z_0, z_1, z_2, z_3, z_4, z_5, z_6, z_7) = 0.$$

We have found only one such example for $k = 30$, with $t(x) = x^7 + 1$ and $\rho(q, t, r) = 1.75$ in Table 4. Two families for $k = 15, 20$ with $\rho(q, t, r) = 2$ appear in Table 7.

Sparse families with $\rho(q, t, r) = 2$: As stated in [19], elliptic curve parameters with $\rho \approx 2$ might as well offer fast pairing computations. Additionally, examples with $\rho \approx 2$ can also achieve a nice balance corresponding to security levels of 128, 256 and 512-bits. In Tables 5–7 we gather a few examples of cyclotomic sparse families, with $\rho(q, t, r) = 2$, where $\deg r = 4, 6$ and 8 respectively. Since $\rho(q, t, r) = 2$, we have excluded the condition $y_{\varphi(k)-1}(z_0, \ldots, z_{\varphi(k)-1}) = 0$ from System (3.7).

Table 5. Cyclotomic sparse families with $\deg r = 4$ and $\rho(q,t,r) = 2$.

Family	k	$t(x)$	$g(x)$	$y(x)$	x_0
1	5	$x+1$	$3x^2-10x+3$	$(4x^3+2x^2+6x+3)/11$	$\{2,5,9\} \bmod 11$
2	5	x^2+1	$3x^2+2x-1$	$-(10x^3+6x^2+x+3)/11$	$\{3,5,9\} \bmod 11$
3	8	$-x^3+1$	$x^2+10x+1$	$(3x^3-x^2+1)/7$	$9 \bmod 14$
4	8	$-x+1$	$7x^2-10x+7$	$2x^3-2x-3$	$x_0 \in \mathbb{Z}$
5	8	$-x+1$	$7x^2-26x+7$	$(2x^3-2x-5)/17$	$\{8,11,15\} \bmod 17$
6	8	$-x+1$	$14x^2-20x+14$	$-(3x^3-3x-4)/2$	$1 \bmod 2$
7	10	x^3+1	$3x^2-2x-1$	$-(8x^3-7x^2+3x-9)/11$	$\{2,6,8\} \bmod 11$
8	10	$x+1$	$3x^2+10x+3$	$(2x^3-2x^2+3)/11$	$\{2,4,6\} \bmod 11$
9	10	$x+1$	$15x^2+50x+15$	$-(8x^3-8x^2+1)/55$	$\{2,13,17,28,37,48\} \bmod 55$

Table 6. Cyclotomic sparse families with $\deg r = 6$ and $\rho(q,t,r) = 2$.

Family	k	$t(x)$	$g(x)$	$y(x)$	x_0
1	7	x^2+1	$4x^2-5x+4$	$x^5+4x^4+7x^3+8x^2+6x+2$	$1 \bmod 2$
2	7	x^4+1	$4x^2-5x+4$	$4x^5+8x^4+9x^3+6x^2+2x-1$	$1 \bmod 2$
3	7	x^5+1	$4x^2-5x+4$	$4x^5+6x^4+5x^3+2x^2-x-2$	$1 \bmod 2$
4	7	$-x^5-x^4-x^3-x^2-x$	$4x^2-5x+4$	$2x^5+2x^4+x^3-x^2-2x-2$	$0 \bmod 2$
5	7	$x+1$	$7x^2+42x+7$	$-(16x^5-4x^4-4x^3+16x^2+11)/91$	$\{5,31,57\} \bmod 91$
6	7	x^2+1	$7x^2+42x+7$	$(4x^5+24x^4+4x^3+5x+5)/91$	$\{15,54,67,80\} \bmod 91$
7	7	x^3+1	$7x^2+42x+7$	$(4x^5+4x^4-15x^2+x-15)/91$	$\{33,59,72,85\} \bmod 91$
8	7	x^4+1	$7x^2+42x+7$	$-(16x^5+15x^3+19x^2+19x+15)/91$	$\{8,47,73\} \bmod 91$
9	9	$x+1$	$4x^2-9x+4$	$-(x^5+5x^4-4x^3+6x^2+6x-2)/19$	$\{5,21,23,25,35\} \bmod 38$
10	9	$x+1$	$12x^2-33x+12$	$(9x^5-3x^4+4x^3+6x^2+6x+2)/51$	$13 \bmod 102$
11	9	$x+1$	$19x^2-30x+19$	$(8x^5+4x^4+10x^3+12x^2+12x+5)/37$	$\{4,9,12,33,34\} \bmod 37$
12	14	$-x^2+1$	$4x^2+5x+4$	$3x^5-4x^4+3x^3-2x+2$	$1 \bmod 2$
13	14	$-x^5+x^4-x^3+x^2-x+2$	$4x^2+5x+4$	$2x^5-6x^4+9x^3-9x^2+6x-2$	$0 \bmod 2$
14	18	$x+1$	$4x^2+9x+4$	$-(7x^5-x^4-6x^2-6x+10)/19$	$\{3,13,15,23,33\} \bmod 38$
15	18	$x+1$	$19x^2+30x+19$	$(26x^5-14x^4-12x^2-12x+29)/37$	$\{3,4,6,25,28\} \bmod 37$

Hence the polynomials $y(x)$ have $\deg y = \varphi(k) - 1$ and thus $\deg q = 2\varphi(k) = 2\deg r$. Furthermore, we are restricted to cases where the coefficients of the polynomials $z(x)$ are integers in the range $[-10, 10]$. More examples can be found by expanding this range, however we are aiming for polynomials that have relatively small coefficients. Additional examples can be also obtained by considering rational coefficients for $z(x)$. In our examples we generally focus on embedding degrees for which the polynomial families are likely to offer pairing-friendly parameters with a nice balance between the security levels in the three defining groups of a pairing. We note that the number of suitable sparse families decreases as the value $\varphi(k)$ grows. More precisely, we found many families for cases where $\varphi(k) = 4$ and just a few for $\varphi(k) = 8$.

3.2 Non-Cyclotomic Sparse Families

Now we present examples of sparse families where $r(x)$ is not a cyclotomic polynomial, but an irreducible polynomial in $\mathbb{Q}[x]$, satisfying condition (2) of Definition 2. So far the only known non-cyclotomic sparse families with $k \neq 3, 4, 6$, are Freeman's family for $k = 10$, with $\rho(q,t,r) = 1$, Dryło's two examples [3] for $k = 8, 12$, with $\rho(q,t,r) = 1.5$ and a few examples we presented in [8] for $k = 5, 10$, with $\rho(q,t,r) = 1.5$. We applied Algorithm 1 for embedding degrees 5, 8, 10, 12 and came up with several new sparse families with $\rho(q,t,r) \leq 2$ presented in Tables 8 and 9. The first examples for $k = 8$ and 12 in Table 8 were first produced by Dryło [3]. Recall that as k grows, then $\deg r$ grows as well and it becomes hard to determine suitable polynomials $t(x), r(x)$ and $z(x)$. This is because in Algorithm 1 the search for non-cyclotomic sparse families is affected by both the coefficients of the element θ, as well as the coefficients of the polynomial $z(x)$. In order to produce the examples of Tables 8 and 9, we used an exhaustive search for coefficients $a_i \in [-10, 10]$ of the

Table 7. Cyclotomic sparse families with $\deg r = 8$ and $\rho(q,t,r) = 2$.

Family	k	$t(x)$	$g(x)$	$y(x)$	x_0
1	15	x^2+1	$3x^2-18x+3$	$(20x^7-8x^6-22x^5+20x^4+14x^3+6x^2+7x-15)/93$	$\{9,24,45,51,69,72,90\} \bmod 93$
2	20	$x+1$	$40x^2-55$	$-(20x^7+23x^6-43x^5-4x^4+24x^3+68x^2-88x+20)/505$	$\{41,57,115,145,161,163,241,243$ $317,347,363,365,443,445,461,565$ $645,647,663,721,751,767,847,865$ $923,953,971\} \bmod 1010$

Table 8. Non-cyclotomic sparse families for k with $\varphi(k) = 4$ and $\rho(q,t,r) = 1.5$.

Family	k	$t(x)$	$r(x)$	$g(x)$	$y(x)$	x_0
1	8	$-(x^3-3x^2-5x-9)/12$	x^4-2x^2+9	$8x^2-16$	$-(x-3)/12$	$3 \bmod 12$
2	8	$(x^3+6x^2-20x+72)/96$	x^4-8x^2+144	x^2+10	$(x^2+6x)/72$	$18 \bmod 24$
3	8	$-(2x^3+5x^2+7x+6)/3$	$x^4+4x^3+8x^2+12x+9$	$2x^2-4x-14$	$(-x^2-3)/6$	$3 \bmod 6$
4	10	$-(25x^3+20x^2+10x+1)$	$25x^4+25x^3+15x^2+5x+1$	$15x^2+10x+3$	$15x^2+5x+3$	$x_0 \in \mathbb{Z}$
5	12	$-(x^3-4x^2-5x-6)/15$	$x^4-2x^3-3x^2+4x+13$	$12x^2-12x-51$	$-(x-3)/15$	$\{3,23\} \bmod 30$
6	12	$-(2x^3-17x-95)/95$	x^4-37x^2+361	x^2-37	$(3x^2+5x-38)/95$	$\{19,171\} \bmod 190$

element θ, and for the coefficients $z_i \in [-20,20]$ of the polynomial $z(x)$ (excluding duplicates as posed in Remark 1), for every $i = 0,1,\ldots,\varphi(k)-1$. In addition, in most examples of non-cyclotomic sparse families, we have considered integer values for both the coefficients of θ and $z(x)$. We argue though that even more examples of families can be constructed by allowing θ and $z(x)$ to have rational coefficients as well. Furthermore we need to establish some limit for both the coefficients of the element θ of Equation (3.1) and the polynomial $z(x) \in \mathbb{Q}[x]$ to ensure that the resulting polynomial family will have relatively small coefficients.

Remark 2 In Tables 2–9 we provide the polynomials $t(x), r(x), g(x)$ and $y(x)$. In particular, the computation of the remaining field polynomial $q(x)$ is straightforward, by using Step (7) of Algorithm 1. More precisely we use the relation:

$$q(x) = \frac{1}{4}\left[t(x)^2 + g(x)y(x)^2\right].$$

The last column, named x_0, in these tables refers to the congruential conditions that the input x_0 must satisfy, in order for the values $q(x_0), t(x_0)$ and $r(x_0)$ to be integers. The entries $x_0 \in \mathbb{Z}$ in some families indicate that the polynomials $q(x), t(x)$ and $r(x)$ are already integer-valued and so there no need to apply any linear transformation. □

Example 1 Let us consider the sparse family 4 in Table 2, for $k = 8$. This is a cyclotomic family and so $r(x) = \Phi_8(x) = x^4+1$. We set the trace polynomial as $t(x) = -x^3+1$. Taking $g(x) = 14x^2-20x+14$ and $y(x) = (x^2+2x+1)/2$, we obtain the field polynomial

$$q(x) = \frac{1}{4}\left[t(x)^2 + g(x)y(x)^2\right] = \frac{1}{8}\left(9x^6+18x^5+9x^4-8x^3+9x^2+18x+9\right).$$

The field polynomial $q(x)$ is integer-valued for all $x \equiv 1 \bmod 2$. This can be easily seen by applying on $q(x)$ the linear transformation $x \to (2z+1)$, where we obtain:

$$q(z) = 72z^6+288z^5+468z^4+388z^3+177z^2+48z+8,$$

which has integer coefficients. Hence we have a sparse family $(q(x), t(x), r(x))$ of pairing-friendly elliptic curves with embedding degree 8 and $\rho(q,t,r) = 1.5$. All families in Tables 2– 9 are created in the same way. □

Table 9. Non-cyclotomic sparse families for k with $\varphi(k) = 4$ and $\rho(q, t, r) = 2$.

Family	k	$t(x)$	$r(x)$	$g(x)$	$y(x)$	x_0
1	5	$x^2 + 2x + 2$	$x^4 + 3x^3 + 4x^2 + 2x + 1$	$3x^2 + 4x$	$-(10x^3 + 24x^2 + 19x + 2)/11$	$\{1, 5, 7\}$ mod 11
2	8	$-(x^3 - 8x - 16)/12$	$x^4 + 4x^3 + 4x^2 + 8$	$x^2 - 4x - 12$	$-(5x^3 + 33x^2 + 14x + 16)/204$	$\{14, 26, 86\}$ mod 102
3	8	$(x^3 + 3x^2 - 5x + 9)/12$	$x^4 - 2x^2 + 9$	$7x^2 + 18x - 9$	$-(8x^3 - 33x^2 - 52x - 15)/612$	$\{27, 75, 87\}$ mod 102
4	8	$(2x^3 + 5x^2 + 7x + 12)/3$	$x^4 + 4x^3 + 8x^2 + 12x + 9$	$3x^2 + 8x + 4$	$(20x^3 + 44x^2 + 91x + 117)/51$	$\{3, 18, 21\}$ mod 51
5	10	$(x + 4)/3$	$x^4 + x^3 + 6x^2 - 14x + 61$	$3x^2 - 12$	$-(4x^3 + 18x^2 - 12x + 1)/891$	$\{5, 17, 23\}$ mod 33
6	10	$-(x^2 + 2x - 3)/4$	$x^4 + 6x^3 + 16x^2 + 26x + 31$	$3x^2 - 14x - 5$	$(x^3 + 3x^2 + 4x + 4)/44$	$\{9, 15, 17\}$ mod 22
7	12	$-(x^3 - 4x^2 - 5x - 6)/15$	$x^4 - 2x^3 - 3x^2 + 4x + 13$	$2x^2 - 2x - 4$	$-(x^3 + 6x^2 - 30x + 19)/90$	23 mod 30
8	12	$-(x^3 - 4x^2 - 5x - 6)/15$	$x^4 - 2x^3 - 3x^2 + 4x + 13$	$6x^2 - 6x - 36$	$-(3x^3 - 2x^2 - 20x + 27)/150$	$\{3, 23\}$ mod 30

4 Implementation and Experimental Results

Suitable pairing-friendly triples (q, t, r) can be obtained by the solutions of a generalized Pell equation. We describe this procedure in detail and present numerical examples of pairing-friendly parameters as a result of the sparse families we constructed in the previous section.

4.1 Finding Pairing-Friendly Parameters with Sparse Families

With the notation of Section 3, let $DY^2 = f(x) = g(x)y(x)^2$ and $g(x) = ax^2 + bx + c$, for some $a, b, c \in \mathbb{Z}$. As stated in [4], we can omit the term $y(x)^2$ from calculations and so the above equation is $DY^2 = ax^2 + bx + c$. Multiplying both sides by a factor $S > 0$, such that aS is a perfect square, we obtain $SDY^2 = aSx^2 + bSx + cS$. Let $aS = A^2$ and $b = 2AB/S$, for some $A, B \in \mathbb{Z}$. Substituting, we obtain $SDY^2 = (Ax)^2 + 2ABx + cS$. Completing the squares and setting $B^2 - cS = T$ and $Ax + B = X$ we conclude to a generalized Pell equation of the form:

$$X^2 - SDY^2 = T. \tag{4.1}$$

We need to find a solution (X, Y) for square free values of D, such that $X = Ax_0 + B$, for some $x_0 \in \mathbb{Z}$. For each solution we check if $q(x_0)$ and $r(x_0)$ are both primes of a desired size and if such a x_0 exists, we set $q = q(x_0)$, $t = t(x_0)$, $r = r(x_0)$ and $\#E(\mathbb{F}_q) = q + 1 - t$. By [21], we can increase the possibility of finding such parameters by allowing r to contain a small factor. In this case we set $r = r(x_0)/n$, for some relatively small $n > 0$. This procedure is summarized in Algorithm 2.

Remark 3 If a generalized Pell equation is solvable then it has an infinite number of solutions and by Equation (4.3) it is clear that these solutions grow very fast. However, we only need a finite number of them. In particular, if (X, Y) is a solution for Equation (4.1), with $X = Ax_0 + B$, then as X grows, so does x_0. Therefore, we set a limit $X_{\max}$ for the size of X to guarantee that $q(x_0)$ and $r(x_0)$ will have approximately the size that we require. □

Details on solving generalized Pell equations of the form (4.1) can be found in [18, 20]. The main strategy requires first to find the fundamental solution of the standard Pell equation:

$$U^2 - SDV^2 = 1, \tag{4.2}$$

by computing the simple continued fraction expansion of $\sqrt{SD}$. This fundamental solution is the smallest integer pair (U_0, V_0) satisfying Equation (4.2) and according to [18, 20], such a pair always exists. On the contrary, Equation (4.1) is not necessarily solvable for every D. If it is, then there is an infinite number of solutions (X_i, Y_i) obtained by the recurrence relation:

$$X_i + Y_i\sqrt{SD} = (X_0 + Y_0\sqrt{SD})(U_0 + V_0\sqrt{SD})^i, \tag{4.3}$$

Algorithm 2 Finding pairing-friendly parameters using sparse families.

Input: A sparse family $(q(x), t(x), r(x))$ with embedding degree k, a generalized Pell equation $X^2 - SDY^2 = T$, with $X = Ax + B$ and the limits $D_{\max}$, $X_{\max}$.
Output: Suitable triples (q, t, r), with CM discriminant D and elliptic curve order N.

```
1: for D = 1 to D_max do
2:    if D: square-free and SD: not a perfect square then
3:       for all solutions (X, Y) of equation X^2 − SDY^2 = T, with X ≤ X_max do
4:          if (X − B)/A = x_0 is integer then
5:             if q(x_0) and r(x_0)/n are primes for some relatively small n ∈ Z_{>0} then
6:                q ← q(x_0), r ← r(x_0)/n, t ← t(x_0), N ← q + 1 − t = #E(F_q)
7:                return q, t, r, D, N
8:             end if
9:          end if
10:      end for
11:   end if
12: end for
```

for each $i = 0, 1, \ldots$, where $X_0, Y_0 > 0$ and Y_0 is the smallest compared to the other Y_i. The pair (X_0, Y_0) is called the fundamental solution of Equation (4.1) and all pairs (X_i, Y_i) obtained by the above relation lie in the same *class* of solutions. However a generalized Pell equation may have more than one classes of solutions and so more than one fundamental solutions (see [18, 20]).

Now consider the generalized Pell equation (4.1) and suppose that T is a perfect square. Such Pell equations have the advantage that they are always solvable for every positive and square-free integer D. Clearly if (U_0, V_0) is the fundamental solution of the standard Pell equation (4.2), then the pair $(X_0, Y_0) = (\sqrt{T}U_0, \sqrt{T}V_0)$ is a fundamental solution of Equation (4.1). This attribute increases the possibility of finding suitable elliptic curve parameters, since there are more D to test. These special Pell equations correspond to sparse families $(q(x), t(x), r(x))$ with $g(x)$ that factors as a product of two linear terms. Indeed, consider the generalized Pell equation (4.1) with T a perfect square and $X = Ax + B$. Then we have:

$$DY^2 = g(x) = \frac{A^2}{S}x^2 + \frac{2AB}{S}x + \frac{B^2 - T}{S}$$

where the discriminant of this polynomial is $4TA^2/S^2 > 0$, a perfect square. Thus $g(x)$ factors over $\mathbb{Q}[x]$. Such families are called *effective* and there are many examples for $k \in \{3, 4, 6\}$ (see [4, 7]) as well as an example for $k = 5$ in [8]. Here we introduce two effective sparse families for $k = 10$ and $\rho(q, t, r) = 1.5$ with $g(x) = 3x^2 + 10x + 3$ and $g(x) = 15x^2 + 50x + 15$ in Table 2. The families for $k = 5, 10$ in Table 5 and all non-cyclotomic sparse families of Table 9 are also effective.

4.2 Numerical Examples

Recall that for a pairing on an elliptic curve $E/\mathbb{F}_q$ is defined as $\widehat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_{\mathrm{T}}$, for some r-order subgroups $\mathbb{G}_1, \mathbb{G}_2 \subset E(\mathbb{F}_q)$ and $\mathbb{G}_{\mathrm{T}} \subseteq \mathbb{F}^*_{q^k}$. Using Algorithm 2, we are looking for pairing-friendly triples (q, t, r), for some fixed embedding degree k, such that q, r are both primes.

The prime r is chosen such that the DLP in $\mathbb{G}_1, \mathbb{G}_2$ is hard. Recall from Section 1 that the complexity of the DLP in such groups is $O(\sqrt{r})$ and the provided security level is $\log r/2$. The complexity of the DLP in a finite field $\mathbb{F}_N$ is measured asymptotically by the L-function:

$$L_N[\ell, c] = \exp\left[(c + o(1))(\ln N)^{\ell}(\ln \ln N)^{1-\ell}\right] \tag{4.4}$$

for some real constants $\ell \in [0,1]$ and $c > 0$, where in our case we have $N = q^k$. For prime embedding degrees, the complexity of the DLP in $\mathbb{F}_N$ is $L_N[1/3, 1.923]$. For composite k, this complexity is reduced to $L_N[1/3, 1.526]$, due to the exTNFS and SexTNFS methods [13, 16]. This causes us to consider larger extension fields than the ones proposed in Table 1 for this case.

Table 10. Pairing-friendly parameters from cyclotomic sparse families of Tables 2–4 with $\rho < 2$.

k	Family	D	x_0	n	$\log r$	$k \log q$	ρ
8	Table 2, Family 4	13557	$1113089949727013355037451 \equiv 1 \bmod 2$	34	314	3832	1.5255
		632901	$1252602986578658247362969 15 \equiv 1 \bmod 2$	4658	334	4160	1.5569
10	Table 2, Family 6	46169	$85646771368743786 5697 \equiv 2 \bmod 11$	11	274	4150	1.5146
		509605	$-3584494507115659240250816 7 \equiv 2 \bmod 11$	11	336	5070	1.5089
		972721	$2309325829677051348160296 33 \equiv 2 \bmod 11$	11	346	5230	1.5116
10	Table 2, Family 7	9214	$-3582385338508080720370289643 \equiv 2 \bmod 55$	11	362	5470	1.5110
		197	$1886442124591953672765645520833 \equiv 13 \bmod 55$	11	398	6010	1.5101
		192678	$9694315951769008011333333 \equiv 13 \bmod 55$	11	315	4760	1.5111
14	Table 3, Family 4	1897633	$17468982577179889797 \equiv 1 \bmod 2$	7	380	8974	1.6868
18	Table 3, Family 6	1875283	$24920919307794 \equiv 4 \bmod 37$	703	257	7974	1.7237

As stated earlier, in [6] it is recommended to use elliptic curves with large CM discriminant and particularly discriminants up to 10^{13} [22]. However a very large discriminant would affect the efficiency of the CM method. In our examples we have considered CM discriminants $D < 2000000$. We argue though that if we increase the values of D, more examples can be found. In Tables 10–13

Table 11. Pairing-friendly parameters from non-cyclotomic sparse families of Table 8 with $\rho < 2$.

k	Family	D	x_0	n	$\log r$	$k \log q$	ρ
8	Family 1	25358	$2011485707672930089848816 3579 \equiv 3 \bmod 12$	72	369	4432	1.5014
8	Family 2	246526	$9136588037365516587775386 \equiv 18 \bmod 24$	1152	321	3864	1.5047
8	Family 3	1480462	$-1278344974507416233450120697 \equiv 3 \bmod 6$	2034	349	4296	1.5387
10	Family 4	145082	$2319023040403787150051816 7$	1	341	5150	1.5103
		358403	$1647100655727790021370656557$	1	366	5520	1.5082
12	Family 5	1093821	$1390154555846465798504115769703 \equiv 23 \bmod 30$	225	392	7080	1.5051

we give our numerical examples obtained by the sparse families of Section 3 and the solutions of their corresponding Pell equations. In all cases we are aiming at a security level of at least 128-bits in all three groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_{\mathrm{T}}$. This corresponds to primes r with $\log r \geq 256$-bits. In

Table 12. Pairing-friendly parameters from cyclotomic sparse families of Tables 5–7 with $\rho \approx 2$.

k	Family	D	x_0	n	$\log r$	$k \log q$	ρ
5	Table 5, Family 1	41483	$-2111597552865494243 72 \equiv 5 \bmod 11$	11	266	2680	2.0150
7	Table 6, Family 2	74047	$403870588123653 \equiv 1 \bmod 2$	1	291	4102	2.0137
7	Table 6, Family 3	36565	$8291678367327 \equiv 1 \bmod 2$	1	257	3626	2.0156
7	Table 6, Family 5	166382	$3037040031329 \equiv 31 \bmod 91$	15863	234	3451	2.1068
8	Table 5, Family 4	568177	$24580049264790716 29 7$	9266	271	4568	2.1070
8	Table 5, Family 6	727203	$1232650031112915013871591 \equiv 1 \bmod 2$	2	319	5144	2.0157
10	Table 5, Family 7	65	$5961026402428825754 1 \equiv 8 \bmod 11$	11	259	5240	2.0232
		136307	$-62698230151597165967 63 \equiv 8 \bmod 11$	2761	278	5770	2.0755
10	Table 5, Family 8	12415	$2476393097136084172 77 \equiv 2 \bmod 11$	781	261	5360	2.0536
		2982	$-2070566347946992361640 75 \equiv 4 \bmod 11$	1	309	6140	1.9871
		26131	$-1202823396073349127466 67 \equiv 6 \bmod 11$	11	303	6080	2.0066
10	Table 5, Family 9	2549	$6029394714774273487622 73 \equiv 28 \bmod 55$	300641	297	6280	2.1145
14	Table 6, Family 12	3949	$2490181055291440308476 9697 \equiv 1 \bmod 2$	749687	486	14210	2.0885

Tables 10 and 11 we present pairing-friendly parameters with $\rho < 2$ obtained by cyclotomic and non-cyclotomic sparse families respectively. In Tables 12 and 13 we present examples of suitable parameters with $\rho \approx 2$ from cyclotomic and non-cyclotomic families of Section 3. In each table the integer x_0 refers to the input of the polynomials $q(x), t(x)$ and $r(x)$. In particular recall that x_0 satisfies the coordinate X of the solution (X, Y) of a generalized Pell equation

$$X^2 - SDY^2 = T, \quad \text{with} \quad X = Ax + B$$

and thus $x_0 = (X - B)/A$. In addition, each x_0 satisfies the congruential restrictions of Tables 2–7, which guarantee that the values $q(x_0), t(x_0)$ and $r(x_0)$ are integers.

Table 13. Pairing-friendly parameters from non-cyclotomic sparse families of Table 9 with $\rho \approx 2$.

k	Family	D	x_0	n	$\log r$	$k \log q$	ρ
5	Family 1	147043	$144981638691838509730 0 \equiv 7 \bmod 11$	301081	262	2805	2.1412
8	Family 2	305	$1711586296790372515238 \equiv 86 \bmod 102$	1224	271	4408	2.0332
8	Family 3	69529	$4089651325190536091967 21 \equiv 27 \bmod 102$	314568	295	4920	2.0847
		100622	$-12402082704006889591707 \equiv 75 \bmod 102$	500616	274	4600	2.0985
		335435	$-80890982348298788793 63 \equiv 87 \bmod 102$	1224	280	4560	2.0357
		394494	$-15168134472145211882102032569 9 \equiv 87 \bmod 102$	1224	377	6104	2.0239
10	Family 5	90041	$-56916071623564861769998 \equiv 17 \bmod 33$	188001	284	5880	2.0704
		491801	$-31738776999807971500237800 52 \equiv 23 \bmod 33$	669141	346	7140	2.0636
12	Family 7	2267	$-27150520032576257205772 87 \equiv 23 \bmod 30$	24525	310	7620	2.0484
		29307	$-34602764635774626039735847 \equiv 23 \bmod 30$	225	331	7968	2.0060
		66693	$99352416978354399948623127947 33 \equiv 23 \bmod 30$	2925	400	9708	2.0225
		69883	$-62276417310242188211778885433320 7 \equiv 23 \bmod 30$	225	427	10284	2.0070
12	Family 8	3459	$1199818192498303226112 3 \equiv 3 \bmod 30$	852925	273	6912	2.1099
		3497	$2685709058119734948293947 5003 \equiv 3 \bmod 30$	25	373	8928	1.9946
		6715	$1853884587540902700941265127 6803 \equiv 3 \bmod 30$	17725	401	9840	2.0449
		10127	$1132518462253070912433 \equiv 3 \bmod 30$	25	275	6576	1.9927
		10187	$4998022941345139622222029124003 \equiv 3 \bmod 30$	25	389	9336	2.0000
		10442	$1813086331321371689943163443 \equiv 3 \bmod 30$	25	357	8556	1.9972
		23865	$2662956911308098577720978782 0003 \equiv 3 \bmod 30$	304525	399	9888	2.0652
		25853	$7253318001042160020198102094022 43 \equiv 3 \bmod 30$	2725	425	10344	2.0282
		34770	$6054607261460072436710403 \equiv 3 \bmod 30$	322825	310	7764	2.0871
		88842	$3127909422825578669091843 \equiv 3 \bmod 30$	25	320	7680	2.0000

The integer n denotes the small factor of $r(x_0)$, in which case we set the prime r as $r = r(x_0)/n$. In our experiments, this small factor is taken to be up to 10000, or even larger (10^6) in some examples. Finally, $\log r$ and $k \log q$ refer to the size of the prime r and the size extension field $\mathbb{F}_{q^k}$ respectively. The pairing-friendly parameters presented in Tables 12 and 13 are the first examples obtained from sparse families for various embedding degrees with $\rho \approx 2$. The examples of Table 13 are produced from effective sparse families and this is why it contains more examples than the others. Particularly the examples obtained by Family 8 of Table 9 are more than any other sparse family we examined. Notice that we have found ten examples of pairing-friendly parameters in this case for $D_{\max} = 100000$.

Remark 4 Using the value x_0 in Tables 10– 13 we can extract the elliptic curve parameters q, t and r in the following way: we find the corresponding sparse family in Tables 2– 9, indicated in the second column and evaluate the polynomials $t(x)$ and $r(x)$ at x_0. Then we set $t = t(x_0)$ and $r = r(x_0)/n$, where n is given in the fifth column of Tables 10– 13. For the prime q we set

$$q = q(x_0) = \frac{1}{4}\left[t(x_0)^2 + g(x_0)y(x_0)^2\right].$$

In some cases the value $y(x_0)$ is not an integer, thus it might contain a factor $1/s$. This does not affect the elliptic curve parameters (q, t, r) since in all such examples s^2 divides $g(x_0)$ and hence

$g(x_0)y(x_0)^2$ is always an integer in our examples. Alternatively, recall that we want $g(x_0)y(x_0)^2 = DY^2$, for some square-free CM discriminant $D > 0$, which is given in the third column of Tables 10–13 and an integer Y. In all of our examples we have that $g(x_0)y(x_0)^2/D = Y^2$, i.e. a perfect square integer, where $y(x_0)$ is not necessarily an integer. □

The results in these tables, justify our claim that sparse families with $\rho(q,t,r) = 2$ are likely to offer a nice balance between the security levels in the three defining groups of a pairing. For instance, suppose that $k = 8$, $\rho(q,t,r) = 1.5$ and $\log r = 256$. Then a simple calculation using Equation (4.4) shows that the asymptotic complexity of the DLP in $\mathbb{F}_{q^8}$ is $L_{q^8}[1/3, 1.526] \approx 110$-bits. If we choose a family with $\rho(q,t,r) = 2$, then this complexity increases to approximately 124-bits, which is very close to the intended security level. On the other hand, for prime embedding degrees, consider a sparse family with $k = 5$ and $\rho(q,t,r) = 1.5$. For an 128-bit security level such families are invalid, since the complexity of the DLP in $\mathbb{F}_{q^5}$ is $L_{q^5}[1/3, 1.923] \approx 114$-bits. However, choosing a family with $\rho(q,t,r) = 2$, we obtain a security level of 128-bits in the target group.

Analogous conclusions can be made for other embedding degrees and higher security levels as well. For example Freeman's family for $k = 10$ and $\rho(q,t,r) = 1$ was considered to be one of the ideal examples for implementations, since it was designed to offer a 128-bit security level in $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_{\mathrm{T}}$, with $\log r = \log q = 256$-bits. For a 256-bit prime r, this family corresponds to an extension field of size $10 \log q = 2560$. Nowadays, since $k = 10$ is composite, the complexity of the DLP in $\mathbb{F}_{q^{10}}$ is $L_{q^{10}}[1/3, 1.526] \approx 102$-bits, far from the ideal case. In order to increase the security level in the extension field, when $k = 10$, we need to consider families with $\rho(q,t,r) \geq 1.5$. More precisely, a family with $\rho(q,t,r) = 1.5$ results in $L_{q^{10}}[1/3, 1.526] \approx 121$-bits, but if we allow a relatively small cofactor n we will achieve a 128-bits security level.

The following example describes how the first entry in Table 10 is extracted. All examples in Tables 10–13 are produced in the same manner.

Example 2 Let us consider the sparse family of Example 1 for $k = 8$. Recall that $g(x) = 14x^2 - 20x + 14$. Setting $DY^2 = g(x)$ we can construct the corresponding generalized Pell equation by multiplying by 14 and completing the squares, in which case we obtain:

$$X^2 - 14DY^2 = -96 \qquad \text{where} \qquad X = 14x - 10.$$

Solving this equation for $D = 1$ up to some bound $D_{\max}$ we get that for $D = 13557$ the pair

$$(X, Y) = (155832592961781869705243 04, 35769468027929990781812)$$

is a solution for the above generalized Pell equation, for which

$$X = 155832592961781869705243 04 = 14 \cdot 111308994972701335503745 1 - 10.$$

Thus we set $x_0 = 111308994972701335503745 1$ and since $x_0 \equiv 1 \bmod 2$, we evaluate the sparse family at x_0, where we obtain:

$$\begin{aligned}
t(x_0) &= -\,13790842048165689679335659884458782730747937886625787246297220989912448 50\\
y(x_0) &= \;\;22158635240623429255980388671224235145707357764136130917507889201547424\\
r(x_0) &= \;\;34 \times 45148375535546851220441313205535640794971749131498385771772024669829862\\
&\quad\;\; 18727874576709724164455 3\\
q(x_0) &= \;\;21396073994713668903461044298916877554056770211925786104342959575776756040 2\\
&\quad\;\; 58778587904106111926430756768095712284081067905428314844117613833844 33
\end{aligned}$$

Note that here $r(x_0)$ is nearly prime, i.e. it contains a small factor $n = 34$. Thus, the prime dividing the order of the curve is $r = r(x_0)/34$. The size of the prime r is $\log r = 314$-bits and the base prime is $q = q(x_0)$ with $\log q = 479$-bits, producing an extension field of size $8 \log q = 3832$-bits. Finally, the trace of Frobenius is $t = t(x_0)$ and for these parameters we have $\rho = 1.5255$. □

5 Conclusion

In this paper, we presented a method for constructing sparse families of pairing-friendly elliptic curves and applied it for various embedding degrees. In Section 3 we have presented examples of sparse families with ρ-values up to 2. We argue that families with $\rho(q, t, r) = 2$ are likely to offer a nice balance between the size of the prime r, representing the order of a subgroup $\mathbb{G}$ of $\#E(\mathbb{F}_q)$ and the size of the extension field $\mathbb{F}_{q^k}$. In Section 4 we presented extensive numerical results to support our claims. The pairing-friendly parameters we produced provide a balanced security level between $\mathbb{G}$ and $\mathbb{F}_{q^k}$ for both composite and prime values of k, with $\rho \leq 2$ and relatively large CM discriminant. Finally, we note that the numerical results presented in this paper are the first in the literature for sparse families of various embedding degrees.

References

1. P. S. L. M. Barreto and M. Naehrig. Pairing-Friendly Elliptic Curves of Prime Order. In G. Goos, J. Hartmanis, and J. van Leeuwen, editors, *International Workshop on Selected Areas in Cryptography–SAC'05*, pages 319–331. Springer, Berlin, Heidelberg, 2005.
2. F. Brezing and A. Weng. Elliptic Curves Suitable for Pairing Based Cryptography. *Designs, Codes and Cryptography*, 37(1):133–141, 2005.
3. R. Dryło. On Constructing Families of Pairing-Friendly Elliptic Curves with Variable Discriminant. In D. J. Bernstein and S. Chatterjee, editors, *International Conference on Cryptology in India–INDOCRYPT'11*, pages 310–319. Springer, Berlin, Heidelberg, 2011.
4. P. Duan, S. Cui, and C. W. Chan. Finding More Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems. *International Journal of Information Technology*, 2(2)(2):157–163, 2005.
5. R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small mov degree over finite prime fields. *Journal of Cryptology*, 18(1):79–89, 2005.
6. N. El Mrabet and M. Joye. *Guide to Pairing-Based Cryptography*. CRC Press, 2017.
7. G. Fotiadis and E. Konstantinou. On the Efficient Generation of Generalized MNT Elliptic Curves. In T. Muntean, D. Poulakis, and R. Rolland, editors, *International Conference on Algebraic Informatics–CAI'13*, pages 147–159. Springer, Berlin, Heidelberg, 2013.
8. G. Fotiadis and E. Konstantinou. More Sparse Families of Pairing-Friendly Elliptic Curves. In D. Gritzalis, A. Kiayias, and I. Askoxylakis, editors, *International Conference on Cryptology and Network Security–CANS'14*, pages 384–399. Springer International Publishing, 2014.
9. D. Freeman. Constructing Pairing-Friendly Elliptic Curves With Embedding Degree 10. In F. Hess, S. Pauli, and M. Pohst, editors, *International Algorithmic Number Theory Symposium–ANTS-VII'06*, pages 452–465. Springer, Berlin, Heidelberg, 2006.
10. D. Freeman, M. Scott, and E. Teske. A Taxonomy of Pairing-Friendly Elliptic Curves. *Journal of Cryptology*, 23(2):224–280, 2010.
11. S. D. Galbraith, J. F. McKee, and P. C. Valença. Ordinary Abelian Varieties Having Small Embedding Degree. *Finite Fields and Their Applications*, 13(4):800–814, 2007.
12. E. J. Kachisa, E. F. Schaefer, and M. Scott. Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field. In S. D. Galbraith and K. G. Paterson, editors, *International Conference on Pairing-Based Cryptography–Pairing'08*, pages 126–135. Springer, Berlin, Heidelberg, 2008.
13. T. Kim and R. Barbulescu. Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case. In M. Robshaw and J. Katz, editors, *Advances in Cryptology–CRYPTO'16*, pages 543–571. Springer, Berlin, Heidelberg, 2016.

14. H.-S. Lee and C.-M. Park. Generating Pairing-Friendly Curves With the CM Equation of Degree 1. In H. Shacham and B. Waters, editors, *International Conference on Pairing-Based Cryptography–Pairing'09*, pages 66–77. Springer, Berlin, Heidelberg, 2009.
15. H.-S. Lee and C.-M. Park. Constructing Pairing-Friendly Curves With Variable CM Discriminant. *Bulletin of the Korean Mathematical Society*, 49(1):75–88, 2012.
16. A. Menezes, P. Sarkar, and S. Singh. Challenges with Assessing the Impact of NFS Advances on the Security of Pairing-Based Cryptography. In *Proceedings of Mycrypt*, 2016.
17. 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.
18. R. A. Mollin. Simple Continued Fraction Solutions for Diophantine Equations. *Expositiones Mathematicae*, 19(1):55–73, 2001.
19. Y. Nogami, E. Yanagi, , T. Izuta, and Y. Morikawa. Ordinary Pairing Friendly Curve of Embedding Degree 1 Whose Order has two Large Prime Factors. *Memoirs of the Faculty of Engineering, Okayama University*, 45:46–53, 2011.
20. J. P. Robertson. *Solving the Generalized Pell Equation* $x^2 - Dy^2 = N$. `http://jpr2718.org/pell.pdf`, 2004.
21. M. Scott and P. S. L. M. Barreto. Generating More MNT Elliptic Curves. *Designs, Codes and Cryptography*, 38(2):209–217, 2006.
22. A. Sutherland. Computing hilbert class polynomials with the chinese remainder theorem. *Mathematics of Computation*, 80(273):501–538, 2011.
23. S. Tanaka and K. Nakamula. Constructing Pairing-Friendly Elliptic Curves Using Factorization of Cyclotomic Polynomials. In S. D. Galbraith and K. G. Paterson, editors, *International Conference on Pairing-Based Cryptography–Pairing'08*, pages 136–145. Springer, Berlin, Heidelberg, 2008.
24. K. Yoon. A New Method of Choosing Primitive Elements for Brezing–Weng Families of Pairing-Friendly Elliptic Curves. *Journal of Mathematical Cryptology*, 9(1):1–9, 2015.