Research Article

Georgios Fotiadis* and Elisavet Konstantinou

Generating pairing-friendly elliptic curve parameters using sparse families

<https://doi.org/10.1515/jmc-2017-0024>

Received May 11, 2017; revised February 6, 2018; accepted February 6, 2018

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

MSC 2010: 14H52, 11G20, 94A60

Communicated by: Alfred Menezes

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 $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, where $\mathbb{G}_1, \mathbb{G}_2 \subset E(\mathbb{F}_q)$ and $\mathbb{G}_T \subset \mathbb{F}_{q^k}^*$ such that $\#\mathbb{G}_1 = \#\mathbb{G}_2 = \#\mathbb{G}_T = r$, 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 $\rho = \frac{\log q}{\log r}$ 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 $\mathbb{G}_T$, is approximately as hard as in $\mathbb{G}_1, \mathbb{G}_2$.
- (5) The embedding degree k is small enough, for efficient operations in $\mathbb{G}_T$.
- (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 $\mathbb{G}_T$.

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

***Corresponding author: Georgios Fotiadis**, Department of Information & Communication Systems Engineering, University of the Aegean, Karlovassi, Samos, 83200, Greece, e-mail: gftiadis@aegean.gr

Elisavet Konstantinou, Department of Information & Communication Systems Engineering, University of the Aegean, Karlovassi, Samos, 83200, Greece, e-mail: ekonstantinou@aegean.gr

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. $\text{lc}(g) > 0$), 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 $d = \frac{1}{\deg r}$ in the best case and $d = 1 - \frac{1}{\deg r}$ 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, Scott and Teske [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 $\mathbb{G}_1, \mathbb{G}_2 \subset E(\mathbb{F}_q)$ 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.

Security level	Subgroup size	Extension field size	Embedding degree	
			$\rho \approx 1$	$\rho \approx 2$
128	256	3,000–5,000	12–20	6–10
192	384	8,000–10,000	20–26	10–13
256	512	14,000–18,000	28–36	14–18

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

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 $\gcd(\{q(x) : x \in \mathbb{Z}\}) = 1$,
- (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*

$$DY^2 = 4q(x) - t(x)^2. \quad (2.1)$$

The ρ -value of a polynomial family $(q(x), t(x), r(x))$ is defined as

$$\rho(q, t, r) = \frac{\deg q}{\deg r}.$$

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

$$DY^2 = 4h(x)r(x) - (t(x) - 2)^2.$$

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 $\text{lc}(g) > 0$, 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 $\zeta_k + 1$ and $(\zeta_k - 1)/\sqrt{-D}$, respectively, and $q(x) = \frac{1}{4}(t(x)^2 + Dy(x)^2)$. 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 $\text{lc}(g) > 0$. 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 $f(x) \equiv -(t(x) - 2)^2 \pmod{r(x)} = g(x)y(x)^2$, 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 $t(x), r(x)$ 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 $\text{lc}(g) > 0$. In particular, we are searching for an element $z(x) \in \mathbb{Q}[x]/\langle r(x) \rangle$ such that $-z(x)^2 \equiv g(x) \pmod{r(x)}$. 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 $\mathbb{G}_T$ 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 $\text{lc}(g) > 0$, 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 Drylo'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

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

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 $i = 0, \dots, \varphi(k) - 1$. Let $\mathcal{B}(\theta)$ and $\mathcal{B}(\zeta_k)$ be the following sets:

$$\mathcal{B}(\theta) = \{1, \theta, \dots, \theta^{\varphi(k)-1}\} \quad \text{and} \quad \mathcal{B}(\zeta_k) = \{1, \zeta_k, \dots, \zeta_k^{\varphi(k)-1}\}.$$

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

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

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

$$u(x) = \sum_{i=0}^{\varphi(k)-1} P'_{i1} x^i. \quad (3.2)$$

By [14, Lemma 2], $\Phi_k(u(x))$ 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 $\mathbb{Q}[a_0, a_1, \dots, a_{\varphi(k)-1}]$ and so we need to ensure that $a_0, a_1, \dots, a_{\varphi(k)-1} \in \mathbb{Q}$ 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

$$z(x) = z_{\varphi(k)-1}x^{\varphi(k)-1} + \cdots + z_2x^2 + z_1x + z_0 \quad (3.3)$$

and we are searching for $z_0, z_1, \dots, z_{\varphi(k)-1} \in \mathbb{Q}$ 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

$$-z(x)^2 \equiv \left[\sum_{i=0}^{\varphi(k)-1} g_i(z_0, z_1, \dots, z_{\varphi(k)-1}) x^i \right] \bmod r(x), \quad (3.4)$$

where all $g_i(z_0, z_1, \dots, z_{\varphi(k)-1})$ 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

$$g_i(z_0, z_1, \dots, z_{\varphi(k)-1}) = 0$$

for all $i = 3, 4, \dots, \varphi(k) - 1$. Solving this system will eliminate some of the z_i and hence improve the efficiency of the search. Finally, we need $g_2(z_0, z_1, \dots, z_{\varphi(k)-1}) > 0$ 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 $\zeta_k \mapsto [u(x)^j \bmod r(x)]$, with $j = 1, 2, \dots, \varphi(k) - 1$, such that $\gcd(j, k) = 1$ we set $t(x) \equiv [u(x)^j + 1] \bmod r(x)$ and

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

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 $q(x) = \frac{1}{4}[t(x)^2 + f(x)]$, 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

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

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

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

This is an extra equation in $(z_0, z_1, \dots, z_{\varphi(k)-1})$ 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

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

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

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

$$\left. \begin{aligned} g_{\varphi(k)-1}(z_0, z_1, \dots, z_{\varphi(k)-1}) &= \dots = g_3(z_0, z_1, \dots, z_{\varphi(k)-1}) = 0, \\ g_2(z_0, z_1, \dots, z_{\varphi(k)-1}) &> 0, \\ \Delta_g &\neq 0, \\ y_{\varphi(k)-1}(z_0, z_1, \dots, z_{\varphi(k)-1}) &= 0 \quad (\text{optional}), \\ g_2(z_0, z_1, \dots, z_{\varphi(k)-1}) - g_0(z_0, z_1, \dots, z_{\varphi(k)-1}) &= 0 \quad (\text{optional}), \end{aligned} \right\} \quad (3.5)$$

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 (3.5). Additionally, we can find more suitable polynomials $g(x)$ by excluding the last condition of system (3.5). The above process is described in Algorithm 1.

Remark 1. Note that if the $\varphi(k)$ -tuple $(z_0, z_1, \dots, z_{\varphi(k)-1})$ is a suitable solution of system (3.5), then the $\varphi(k)$ -tuple $(nz_0, nz_1, \dots, nz_{\varphi(k)-1})$, 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 $x \mapsto (ay + b)$ such that $g'(x) = g(ay + b)$. In this case, the polynomials $g(x)$ and $g'(x)$ also generate the same sparse family.

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 (3.2).
- 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 (3.3) and calculate the multivariate polynomials $g_i(z_0, z_1, \dots, z_{\varphi(k)-1})$ by equation (3.4), for all $i = 0, 1, \dots, \varphi(k) - 1$.
- 5: For each $j = 1, 2, \dots, \varphi(k) - 1$ such that $\gcd(j, k) = 1$ solve system (3.5).
- 6: If a solution $(z_0, z_1, \dots, z_{\varphi(k)-1})$ exists, set

$$\begin{aligned} t(x) &\equiv [u(x)^j + 1] \bmod r(x), \\ y(x) &\equiv [(u(x)^j - 1)z(x)^{-1}] \bmod r(x), \\ g(x) &= \sum_{i=0}^2 g_i(z_0, z_1, \dots, z_{\varphi(k)-1})x^i. \end{aligned}$$

- 7: Set $f(x) = g(x)y(x)^2$ and $q(x) = \frac{1}{4}[t(x)^2 + f(x)]$.
 - 8: If $q(x)$ represents primes, return $(q(x), t(x), r(x))$.
-

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 $j = 1, \dots, \varphi(k) - 1$ 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 $\varphi(k) \leq 8$.

3.1.1 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 $g_2(z_0, z_1, z_2, z_4) = g_0(z_0, z_1, z_2, z_4)$, 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 $z(x)$:

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

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

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	$x^3 + 1$	$4x^2 + 7x + 4$	$x^2 + 1$	$1 \bmod 2$
3	8	$-x^3 + 1$	$7x^2 - 26x + 7$	$-\frac{1}{17}(3x^2 - x + 3)$	$\{8, 15\} \bmod 17$
4	8	$-x^3 + 1$	$14x^2 - 20x + 14$	$\frac{1}{2}(x^2 + 2x + 1)$	$1 \bmod 2$
5	10	$x^3 + 1$	$12x^2 - 3x + 4$	$\frac{1}{11}(x^2 + 2x + 3)$	$\{7, 13\} \bmod 22$
6	10	$x^3 + 1$	$3x^2 + 10x + 3$	$\frac{1}{11}(x^2 + 3x + 1)$	$\{2, 6\} \bmod 11$
7	10	$x^3 + 1$	$15x^2 + 50x + 15$	$\frac{1}{55}(7x^2 - x + 7)$	$\{2, 13, 17, 28\} \bmod 55$
8	10	$-x^3 + x^2 - x + 2$	$20x^2 - 35x + 20$	$\frac{1}{5}(x^2 + x)$	$0 \bmod 10$

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

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.

3.1.2 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

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

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.

3.1.3 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

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

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 $z_1 = \frac{4}{3}z_3$. Then we have

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

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

$$g_2(z_0, z_1, z_2, z_3) \neq g_0(z_0, z_1, z_2, z_3).$$

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

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

k	$g(x)$	$y(x)$	x_0
30	$155x^2 + 350x + 155$	$\frac{1}{9755}(433x^6 - 293x^5 - 149x^4 + 637x^3 - 149x^2 - 293x + 433)$	$\{707, 1003, 1228, 1348, 2658, 3582, 5533, 6042, 7993, 8807, 9032, 9152\} \bmod 9755$

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

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.

3.1.4 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 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.

3.1.5 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 following 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.

3.1.6 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

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

from system (3.5). 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 $\varphi(k) = 8$.

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

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

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

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

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 $\rho(q, t, r) = 1$, Drylo'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 Drylo [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 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 $i = 0, 1, \dots, \varphi(k) - 1$. 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.

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

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

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

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

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

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 $y(x) = \frac{1}{2}(x^2 + 2x + 1)$, we obtain the field polynomial

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

The field polynomial $q(x)$ is integer-valued for all $x \equiv 1 \pmod{2}$. This can easily be seen by applying on $q(x)$ the linear transformation $x \mapsto (2z + 1)$, 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.

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 $b = \frac{2AB}{S}$, 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

$$X^2 - SDY^2 = T. \quad (4.1)$$

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 $r = \frac{1}{n}r(x_0)$, 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

$$U^2 - SDV^2 = 1, \quad (4.2)$$

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  $X \leq X_{\max}$  do
4:       if  $\frac{X-B}{A} = x_0$  is integer then
5:         if  $q(x_0)$  and  $\frac{r(x_0)}{n}$  are primes for some relatively small  $n \in \mathbb{Z}_{>0}$  then
6:            $q \leftarrow q(x_0), r \leftarrow \frac{r(x_0)}{n}, t \leftarrow t(x_0), N \leftarrow q + 1 - t = \#E(\mathbb{F}_q)$ 
7:           return  $q, t, r, D, N$ 
8:         end if
9:       end if
10:    end for
11:  end if
12: end for

```

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

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

for each $i = 0, 1, \dots$, 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), 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 $\frac{4TA^2}{S^2} > 0$, a perfect square. Thus the polynomial $g(x)$ 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 $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, for some r -order subgroups $\mathbb{G}_1, \mathbb{G}_2 \subset E(\mathbb{F}_q)$ and $\mathbb{G}_T \subseteq \mathbb{F}_q^*$. 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 $\frac{\log r}{2}$. The complexity of the DLP in a finite

field $\mathbb{F}_N$ is measured asymptotically by the L -function

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

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 $L_N[\frac{1}{3}, 1.923]$. For composite k , this complexity is reduced to $L_N[\frac{1}{3}, 1.526]$, 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.

As stated earlier, in [6] it is recommended to use elliptic curves with large CM discriminant and particularly discriminants up to 10^{13} (see [22]). However, a very large discriminant would affect the efficiency of the CM method. In our examples we have considered CM discriminants $D < 2,000,000$. We argue though that if we increase the values of D , more examples can be found. In Tables 10–13 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 G_1 , G_2 and G_T .

k	Family	D	x_0	n	$\log r$	$k \log q$	ρ
8	Table 2, Family 4	13,557	1113089949727013355037451 $\equiv 1 \pmod{2}$	34	314	3,832	1.5255
		632,901	125260298657865824736296915 $\equiv 1 \pmod{2}$	4,658	334	4,160	1.5569
10	Table 2, Family 6	46,169	856467713687437865697 $\equiv 2 \pmod{11}$	11	274	4,150	1.5146
		509,605	−35844945071156592402508167 $\equiv 2 \pmod{11}$	11	336	5,070	1.5089
		972,721	230932582967705134816029633 $\equiv 2 \pmod{11}$	11	346	5,230	1.5116
10	Table 2, Family 7	9,214	−3582385338508080720370289643 $\equiv 2 \pmod{55}$	11	362	5,470	1.5110
		197	1886442124591953672765645520833 $\equiv 13 \pmod{55}$	11	398	6,010	1.5101
		192,678	969431595176900801133333 $\equiv 13 \pmod{55}$	11	315	4,760	1.5111
14	Table 3, Family 4	1,897,633	17468982577179889797 $\equiv 1 \pmod{2}$	7	380	8,974	1.6868
18	Table 3, Family 6	1,875,283	24920919307794 $\equiv 4 \pmod{37}$	703	257	7,974	1.7237

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	1	25,358	20114857076729300898488163579 $\equiv 3 \pmod{12}$	72	369	4,432	1.5014
8	2	246,526	9136588037365516587775386 $\equiv 18 \pmod{24}$	1,152	321	3,864	1.5047
8	3	1,480,462	−1278344974507416233450120697 $\equiv 3 \pmod{6}$	2,034	349	4,296	1.5387
10	4	145,082	23190230404037871500518167	1	341	5,150	1.5103
		358,403	1647100655727790021370656557	1	366	5,520	1.5082
12	5	1,093,821	1390154555846465798504115769703 $\equiv 23 \pmod{30}$	225	392	7,080	1.5051

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
5	Table 5, Family 1	41,483	−211159755286549424372 $\equiv 5 \pmod{11}$	11	266	2,680	2.0150
7	Table 6, Family 2	74,047	403870588123653 $\equiv 1 \pmod{2}$	1	291	4,102	2.0137
7	Table 6, Family 3	36,565	8291678367327 $\equiv 1 \pmod{2}$	1	257	3,626	2.0156
7	Table 6, Family 5	166,382	3037040031329 $\equiv 31 \pmod{91}$	15,863	234	3,451	2.1068
8	Table 5, Family 4	568,177	2458004926479071616297	9,266	271	4,568	2.1070
8	Table 5, Family 6	727,203	1232650031112915013871591 $\equiv 1 \pmod{2}$	2	319	5,144	2.0157
10	Table 5, Family 7	65	59610264024288257541 $\equiv 8 \pmod{11}$	11	259	5,240	2.0232
		136,307	−6269823015159716596763 $\equiv 8 \pmod{11}$	2,761	278	5,770	2.0755
10	Table 5, Family 8	12,415	247639309713608417277 $\equiv 2 \pmod{11}$	781	261	5,360	2.0536
		2,982	−207056634794699236164075 $\equiv 4 \pmod{11}$	1	309	6,140	1.9871
		26,131	−120282339607334912746667 $\equiv 6 \pmod{11}$	11	303	6,080	2.0066
10	Table 5, Family 9	2,549	602939471477427348762273 $\equiv 28 \pmod{55}$	300,641	297	6,280	2.1145
14	Table 6, Family 12	3,949	24901810552914403084769697 $\equiv 1 \pmod{2}$	749,687	486	14,210	2.0885

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	1	147,043	$1449816386918385097300 \equiv 7 \pmod{11}$	301,081	262	2,805	2.1412
8	2	305	$1711586296790372515238 \equiv 86 \pmod{102}$	1,224	271	4,408	2.0332
8	3	69,529	$408965132519053609196721 \equiv 27 \pmod{102}$	314,568	295	4,920	2.0847
		100,622	$-12402082704006889591707 \equiv 75 \pmod{102}$	500,616	274	4,600	2.0985
		335,435	$-8089098234829878879363 \equiv 87 \pmod{102}$	1,224	280	4,560	2.0357
		394,494	$-151681344721452118821020325699 \equiv 87 \pmod{102}$	1,224	377	6,104	2.0239
10	5	90,041	$-56916071623566481769998 \equiv 17 \pmod{33}$	188,001	284	5,880	2.0704
		491,801	$-3173877699980797150023780052 \equiv 23 \pmod{33}$	669,141	346	7,140	2.0636
12	7	2,267	$-2715052003257625720577287 \equiv 23 \pmod{30}$	24,525	310	7,620	2.0484
		29,307	$-34602764635774626039735847 \equiv 23 \pmod{30}$	225	331	7,968	2.0060
		66,693	$9935241697835439994862312794733 \equiv 23 \pmod{30}$	2,925	400	9,708	2.0225
		69,883	$-622764173102421882117788854333207 \equiv 23 \pmod{30}$	225	427	10,284	2.0070
		3,459	$11998181924983032261123 \equiv 3 \pmod{30}$	852,925	273	6,912	2.1099
		3,497	$26857090581197349482939475003 \equiv 3 \pmod{30}$	25	373	8,928	1.9946
		6,715	$18538845875409027009412651276803 \equiv 3 \pmod{30}$	17,725	401	9,840	2.0449
		10,127	$1132518462253070912433 \equiv 3 \pmod{30}$	25	275	6,576	1.9927
12	8	10,187	$499802294134513962222029124003 \equiv 3 \pmod{30}$	25	389	9,336	2.0000
		10,442	$1813086331321371689943163443 \equiv 3 \pmod{30}$	25	357	8,556	1.9972
		23,865	$2662956911308098577209787820003 \equiv 3 \pmod{30}$	304,525	399	9,888	2.0652
		25,853	$725331800104216002019810209402243 \equiv 3 \pmod{30}$	2,725	425	10,344	2.0282
		34,770	$6054607261460072436710403 \equiv 3 \pmod{30}$	322,825	310	7,764	2.0871
		88,842	$3127909422825578669091843 \equiv 3 \pmod{30}$	25	320	7,680	2.0000

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

This corresponds to primes r with $\log r \geq 256$ -bits. In 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

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

and thus $x_0 = \frac{1}{A}(X - B)$. 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. The integer n denotes the small factor of $r(x_0)$, in which case we set the prime r as $r = \frac{1}{n}r(x_0)$. In our experiments, this small factor is taken to be up to 10,000, 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 $D_{\max} = 100,000$.

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 $r = \frac{1}{n}r(x_0)$, where n is given in the fifth column of Tables 10–13. For the prime q we set

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

In some cases the value $y(x_0)$ is not an integer, thus it might contain a factor $\frac{1}{s}$. 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 $\frac{g(x_0)y(x_0)^2}{D} = Y^2$, 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 $\log r = 256$. A simple calculation using equation (4.4) shows that the asymptotic complexity of the DLP in $\mathbb{F}_{q^8}$ is $L_{q^8}[\frac{1}{3}, 1.526] \approx 110$ -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 $L_{q^5}[\frac{1}{3}, 1.923] \approx 114$ -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 $\mathbb{G}_T$, with $\log r = \log q = 256$ -bits. For a 256-bit prime r , this family corresponds to an extension field of size $10 \log q = 2,560$. Nowadays, since $k = 10$ is composite, the complexity of the DLP in $\mathbb{F}_{q^{10}}$ is $L_{q^{10}}[\frac{1}{3}, 1.526] \approx 102$ -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 $L_{q^{10}}[\frac{1}{3}, 1.526] \approx 121$ -bits, but if we allow a relatively small cofactor n we will achieve a 128-bits security level.

The final 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

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

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

$$(X, Y) = (15583259296178186970524304, 35769468027929990781812)$$

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

$$X = 15583259296178186970524304 = 14 \cdot 1113089949727013355037451 - 10.$$

Thus we set $x_0 = 1113089949727013355037451$ and since $x_0 \equiv 1 \pmod{2}$, we evaluate the sparse family at x_0 , where we obtain

$$\begin{aligned} t(x_0) &= -1379084204816568967933565988445878273074793788662578724629722098991244850, \\ y(x_0) &= 22158635240623429255980388671224235145707357764136130917507889201547424, \\ r(x_0) &= 34 \times 45148375535546851220441313205535640794971749131498385771772024669829 \\ &\quad 862187278745767097241644553, \\ q(x_0) &= 213960739947136689034610442989168775540567702119257861043429595757767560 \\ &\quad 4025877858790410611192643075676809571228408106790542831484411761383384433. \end{aligned}$$

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 $r = \frac{1}{34}r(x_0)$. 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.

Acknowledgment: We thank the anonymous referees for their valuable comments and suggestions that helped us improve this paper.

References

- [1] P. S. L. M. Barreto and M. Naehrig, Pairing-friendly elliptic curves of prime order, in: *Selected Areas in Cryptography*, Lecture Notes in Comput. Sci. 3897, Springer, Berlin (2006), 319–331.
- [2] F. Brezing and A. Weng, Elliptic curves suitable for pairing based cryptography, *Des. Codes Cryptogr.* **37** (2005), no. 1, 133–141.
- [3] R. Dryl o, On constructing families of pairing-friendly elliptic curves with variable discriminant, in: *Progress in Cryptology – INDOCRYPT*, Lecture Notes in Comput. Sci. 7107, Springer, Berlin (2011), 310–319.
- [4] P. Duan, S. Cui and C. W. Chan, Finding more non-supersingular elliptic curves for pairing-based cryptosystems, *Int. J. Inf. Tech.* **2** (2005), no. 2, 157–163.
- [5] R. Dupont, A. Enge and F. Morain, Building curves with arbitrary small MOV degree over finite prime fields, *J. Cryptology* **18** (2005), no. 2, 79–89.
- [6] N. El Mrabet and M. Joye, *Guide to Pairing-Based Cryptography*, CRC Press, Boca Raton, 2017.
- [7] G. Fotiadis and E. Konstantinou, On the efficient generation of generalized MNT elliptic curves, in: *Algebraic Informatics*, Lecture Notes in Comput. Sci. 8080, Springer, Berlin (2013), 147–159.
- [8] G. Fotiadis and E. Konstantinou, More sparse families of pairing-friendly elliptic curves, in: *Cryptology and Network Security – CANS’14*, Lecture Notes in Comput. Sci. 8813, Springer, Cham (2014), 384–399.
- [9] D. Freeman, Constructing pairing-friendly elliptic curves with embedding degree 10, in: *Algorithmic Number Theory*, Lecture Notes in Comput. Sci. 4076, Springer, Berlin (2006), 452–465.
- [10] D. Freeman, M. Scott and E. Teske, A taxonomy of pairing-friendly elliptic curves, *J. Cryptology* **23** (2010), no. 2, 224–280.
- [11] S. D. Galbraith, J. F. McKee and P. C. Valença, Ordinary abelian varieties having small embedding degree, *Finite Fields Appl.* **13** (2007), no. 4, 800–814.
- [12] E. J. Kachisa, E. F. Schaefer and M. Scott, Constructing Brezing–Weng pairing-friendly elliptic curves using elements in the cyclotomic field, in: *Pairing-Based Cryptography – Pairing 2008*, Lecture Notes in Comput. Sci. 5209, Springer, Berlin (2008), 126–135.
- [13] T. Kim and R. Barbulescu, Extended tower number field sieve: A new complexity for the medium prime case, in: *Advances in Cryptology – CRYPTO 2016. Part I*, Lecture Notes in Comput. Sci. 9814, Springer, Berlin (2016), 543–571.
- [14] H.-S. Lee and C.-M. Park, Generating pairing-friendly curves with the CM equation of degree 1, in: *Pairing-Based Cryptography – Pairing 2009*, Lecture Notes in Comput. Sci. 5671, Springer, Berlin (2009), 66–77.
- [15] H.-S. Lee and C.-M. Park, Constructing pairing-friendly curves with variable CM discriminant, *Bull. Korean Math. Soc.* **49** (2012), no. 1, 75–88.
- [16] A. Menezes, P. Sarkar and S. Singh, Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography, preprint (2016), <https://eprint.iacr.org/2016/1102.pdf>.
- [17] A. Miyaji, M. Nakabayashi and S. Takano, New explicit conditions of elliptic curve traces for FR-reduction, *IEICE Trans Fundam. Electron. Commun. Comput. Sci.* **84** (2001), no. 5, 1234–1243.
- [18] R. A. Mollin, Simple continued fraction solutions for Diophantine equations, *Expo. Math.* **19** (2001), no. 1, 55–73.
- [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, *Mem. Fac. Eng. Okayama Univ.* **45** (2011), 46–53.
- [20] J. P. Robertson, Solving the generalized Pell equation $x^2 - Dy^2 = N$, preprint (2004), <http://jpr2718.org/pell.pdf>.
- [21] M. Scott and P. S. L. M. Barreto, Generating more MNT elliptic curves, *Des. Codes Cryptogr.* **38** (2006), no. 2, 209–217.
- [22] A. V. Sutherland, Computing Hilbert class polynomials with the Chinese remainder theorem, *Math. Comp.* **80** (2011), no. 273, 501–538.
- [23] S. Tanaka and K. Nakamura, Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials, in: *Pairing-Based Cryptography – Pairing 2008*, Lecture Notes in Comput. Sci. 5209, Springer, Berlin (2008), 136–145.
- [24] K. Yoon, A new method of choosing primitive elements for Brezing–Weng families of pairing-friendly elliptic curves, *J. Math. Cryptol.* **9** (2015), no. 1, 1–9.