



# TNFS resistant families of pairing-friendly elliptic curves

Georgios Fotiadis\*, Elisavet Konstantinou

Department of Information & Communication Systems Engineering, University of the Aegean, Karlovassi, Samos 83200, Greece



## ARTICLE INFO

### Article history:

Available online 15 October 2019

### Keywords:

Pairings  
Elliptic curves  
Pairing-friendly parameters  
Embedding degree  
TNFS attacks

## ABSTRACT

Recently there has been a significant progress on the tower number field sieve (TNFS) method, reducing the complexity of the discrete logarithm problem (DLP) in finite field extensions of composite degree. These new variants of the TNFS attacks have a major impact on pairing-based cryptography and particularly on the selection of the underlying elliptic curve groups and extension fields. In this paper we revise the criteria for selecting pairing-friendly elliptic curves considering these new TNFS attacks in finite extensions of composite embedding degree. Additionally we update the criteria for finite extensions of prime degree in order to meet today's security requirements.

© 2019 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Let  $E/\mathbb{F}_p$  be an ordinary elliptic curve over a prime field  $\mathbb{F}_p$  and  $E(\mathbb{F}_p)$  the group of  $\mathbb{F}_p$ -rational points whose order satisfies  $\#E(\mathbb{F}_p) \approx p$ . Let also  $t = p + 1 - \#E(\mathbb{F}_p)$  be the trace of Frobenius and  $D > 0$  the *CM discriminant*. This is the square-free integer satisfying the *CM equation*  $Dy^2 = 4p - t^2$ , for some  $y \in \mathbb{Z}$ . We further assume that the order of the curve contains a large prime factor  $r$ , hence  $\#E(\mathbb{F}_p) = hr$ , for some *cofactor*  $h \geq 1$ . To complete the elliptic curve notation, we denote by  $E[r]$  the group of  $r$ -torsion points on the curve, i.e. all points with coordinates in  $\overline{\mathbb{F}_p}$  whose order is equal to  $r$ .

Let  $\mathbb{G}_1, \mathbb{G}_2$  and  $\mathbb{G}_T$  be three cyclic groups with  $\mathbb{G}_1 \neq \mathbb{G}_2$  and  $\#\mathbb{G}_1 = \#\mathbb{G}_2 = \#\mathbb{G}_T = r$ . An *asymmetric pairing* is a bilinear, non-degenerate, efficiently computable (polynomial time) map of the form:

$$\hat{e}: \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T.$$

Asymmetric pairings are defined on ordinary elliptic curves  $E/\mathbb{F}_p$  and they are considered to be more efficient than the symmetric ones ( $\mathbb{G}_1 = \mathbb{G}_2$ ), which are defined on supersingular curves. In the asymmetric case, the groups  $\mathbb{G}_1$  and  $\mathbb{G}_2$  are distinct,  $r$ -order subgroups of  $E(\mathbb{F}_{p^k})$ , while  $\mathbb{G}_T$  is an  $r$ -order subgroup of the multiplicative group of the extension field  $\mathbb{F}_{p^k}$ . Thus, in practice, an asymmetric pairing takes two points on the curve of order  $r$  and coordinates in an extension  $\mathbb{F}_{p^k}$  and maps them via some formula to an integer of order  $r$ , hence an  $r$ th root of unity in  $\mathbb{F}_{p^k}^*$ . The positive integer  $k$  is called the *embedding degree of the curve  $E/\mathbb{F}_p$  with respect to  $r$*  and it is defined as the smallest positive integer such that  $\mathbb{F}_{p^k}$  contains all primitive  $r$ th roots of unity. Equivalently,  $k$  is the smallest positive integer, such that all  $r$ -torsion points have coordinates in  $\mathbb{F}_{p^k}$  instead of the whole algebraic closure  $\overline{\mathbb{F}_p}$ . In pairing-based cryptography, an elliptic curve must satisfy certain rules, in order to be suitable for applications. In particular:

\* Corresponding author.

E-mail addresses: [gfotiadis@aegean.gr](mailto:gfotiadis@aegean.gr) (G. Fotiadis), [ekonstantinou@aegean.gr](mailto:ekonstantinou@aegean.gr) (E. Konstantinou).

URL: <http://www.icsd.aegean.gr/gfotiadis> (G. Fotiadis).

**Table 1**  
Bit size of curve parameters and embedding degrees for a desired security level.

| Security level<br>in bits | Subgroup size<br>$\log r$ | Extension field size<br>$k \log p$ | 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            |

1. The prime  $r$  must be large enough, so that the DLP in  $\mathbb{G}_1, \mathbb{G}_2$  is computationally hard.
2. The embedding degree  $k$  must be large enough, so that the DLP in  $\mathbb{G}_T \subseteq \mathbb{F}_{p^k}^*$  is approximately as hard as in  $\mathbb{G}_2, \mathbb{G}_2$ .
3.  $k$  must be relatively small in order to ensure that operations in  $\mathbb{G}_T$  are performed efficiently. The  $\rho$ -value defined as  $\rho = \deg p / \log r$  must be close to 1, so that  $\log r \approx \log p$ .

An elliptic curve  $E/\mathbb{F}_p$  with embedding degree  $k$  and  $r \mid \#E(\mathbb{F}_p)$ , satisfying these properties is called *pairing-friendly* [8]. Conditions (1) and (2) are the core of security for every pairing-based protocol. The third condition ensures that the arithmetic in the extension field  $\mathbb{F}_{p^k}$  is still efficiently performed and condition (4) saves bandwidth. As  $\rho$  gets larger than 1, the prime  $p$ , and hence  $\mathbb{F}_{p^k}$  gets larger. This results in large coordinates of points on the curve which in turn affects the efficiency of operations and the memory usage requirements.

A survey on methods for constructing pairing-friendly elliptic curves is presented in [8]. Examples with the smallest  $\rho$ -values are obtained by the Brezing-Weng method [2]. These are achieved by representing the curve parameters  $p, t, r$  as polynomial families  $p(x), t(x), r(x) \in \mathbb{Q}[x]$  respectively (see Section 2 for the precise definition). In this case, pairing-friendly parameters are derived from the evaluation of these polynomials at some  $x_0 \in \mathbb{Z}$ , such that  $p(x_0)$  and  $r(x_0)$  are both primes and  $4p(x_0) - t(x_0)^2 = Dy^2$ , for some square-free  $D > 0$  and some  $y \in \mathbb{Z}$ . Freeman et al. [8] suggested that pairing-friendly parameters should be chosen according to Table 1. Although these recommendations have been followed for quite a while, recently there has been a significant progress on reducing the complexity of the DLP in finite extensions of composite degree. This leads us to a reconsideration concerning the sizes of the extension fields proposed in Table 1 (3rd column), especially for composite embedding degrees  $k$ .

The complexity of the DLP in the *source groups*  $\mathbb{G}_2, \mathbb{G}_2$  is  $O(\sqrt{r})$  and it is achieved by Pollard's rho algorithm. In practice this means that a  $n$ -bit AES symmetric key provides an equivalent security level as an elliptic curve whose order contains a  $2n$ -bits prime. Contemporary security requirements suggest that a safe choice for the security level must be larger than 128-bits achieved by curves whose order contain a prime factor larger than 256-bits (see Table 1). On the other hand, the complexity of the DLP in a finite extension  $\mathbb{F}_{p^k}$  depends on the choice of the embedding degree  $k$  and the characteristic of the extension field. In particular, we recall the usual  $L$ -notation given by the formula:

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

for some real constants  $\ell \in [0, 1]$  and  $c > 0$ , where  $N = p^k$ . In general for a finite field extension, the NFS attack applies with complexity  $L_N[1/3, 1.923]$ . This complexity still holds today for finite extensions of prime degree. When  $k$  is composite and  $p$  has a special form, i.e. it derives from the evaluation of a polynomial at some value, recent variants of the TNFS method, such as the extended TNFS (exTNFS) or special exTNFS (SextTNFS) algorithms [9,11] reduce the complexity of the DLP to  $L_N[1/3, 1.526]$ .

The new improvements have a major effect on the construction of pairing-friendly curves with composite embedding degree. An immediate consequence is that the extension field should be larger than before and therefore the requirement  $\rho \approx 1$  may not be an ideal choice for composite  $k$  any more. For example, the Barreto-Naehrig (BN) curves [1] for  $k = 12$  were ideal for generating a 256-bit prime and a 3072-bit extension field (i.e.  $\rho \approx 1$ ). Such parameters in the pre-TNFS period would correspond to an 128-bit security level. After the improvements of the TNFS method and according to Equation (1), an extension field of this size reaches a security level of 110-bits. In order to achieve an extension field with 128-bit security level, one should choose  $p^{12}$  around 4608-bits. Since  $\rho \approx 1$  in BN-curves, this results in  $\log r \approx 384$  and hence a mismatch between the security level in  $\mathbb{G}_1, \mathbb{G}_2$  and the security level in the target group  $\mathbb{G}_T$ .

In this paper we revise the criteria for constructing polynomial families  $(p(x), t(x), r(x))$  considering the impact of the TNFS variants, presented in [9,11]. For composite embedding degrees we propose the use of optimal families that are likely to provide a balanced security level in the three pairing groups  $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$  and produce pairing-friendly parameters that are resistant to TNFS attacks. Additionally, for prime values of  $k$  we recommend the use of polynomial families that achieve balanced security levels, but were not considered before due to a larger  $\rho$ -value. All families presented in this paper provide a security level of 128, 256 or 512 bits. We produce numerical examples of cryptographic value obtained by our recommended families based on the asymptotic complexity of the DLP in the finite extensions  $\mathbb{F}_{p^k}$ . This is measured by the usual  $L$ -function presented in Equation (1) and ignoring the constant  $o(1)$ . Therefore, the scope of this paper is to provide a guideline on how to choose pairing-friendly elliptic curves that are resistant to the new TNFS attacks.

In Section 2 we give an overview of families of pairing-friendly elliptic curves and focus on the Brezing-Weng method [2] for their construction. In Sections 3 and 4 we present our recommendations on selecting Brezing-Weng polynomial families

that are suitable for producing pairing-friendly parameters resistant to the TNFS variants. We also give numerical examples of pairing-friendly parameters with cryptographic value for various embedding degrees. Finally, we conclude this paper in Section 5, summarizing our recommendations for selecting suitable pairing-friendly parameters.

## 2. Families of pairing-friendly elliptic curves

For a prime  $p$ , let  $E/\mathbb{F}_p$  be an ordinary elliptic curve with trace  $t$  and order  $\#E(\mathbb{F}_p) = hr$ , for some  $h \geq 1$  and a prime  $r$ . In addition, for the rest of this paper we assume that  $p(x), t(x)$  and  $r(x)$  are non-zero polynomials with coefficients in  $\mathbb{Q}$ .

**Definition 1** (Freeman et al. [8]). A polynomial triple  $(p(x), t(x), r(x))$  parameterizes a family of pairing-friendly elliptic curves with embedding degree  $k$  and CM discriminant  $D$  if:

1.  $p(x)$  represents primes, i.e. it is irreducible, with  $\deg p > 0$  and  $\text{lc}(p) > 0$ . Additionally,  $p(x) \in \mathbb{Z}$ , for some (or infinitely many)  $x \in \mathbb{Z}$  and  $\gcd(\{p(x) : x, p(x) \in \mathbb{Z}\}) = 1$ .
2.  $r(x)$  represents primes, i.e. satisfies the same conditions as  $p(x)$ .
3.  $r(x)$  divides  $p(x) + 1 - t(x)$  and  $\Phi_k(t(x) - 1)$ , where  $\Phi_k(x)$  is the  $k$ th cyclotomic polynomial.
4. there are infinitely many solutions  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$  for the parameterized CM equation

$$Dy^2 = 4p(x) - t(x)^2. \quad (2)$$

The  $\rho$ -value of a polynomial family is defined as the ratio  $\rho(p, t, r) = \deg p / \deg r$ . The third condition of Definition 1 implies that the order of the curve has a polynomial representation  $\#E(\mathbb{F}_{p(x)}) = h(x)r(x)$ , where  $h(x) \in \mathbb{Q}[x]$  is the polynomial representing the cofactor. In addition, the fact that  $r(x)$  divides  $\Phi_k(t(x) - 1)$  in Condition (3) means that  $t(x) - 1$  is a primitive  $k$ th root of unity modulo  $r(x)$ . There are three types of polynomial families depending on the form of the polynomial  $f(x) = 4p(x) - t(x)^2$ , which is called the *CM polynomial*.

**Definition 2** (Dryło [3]). A polynomial family  $(p(x), t(x), r(x))$  is called:

1. *complete* if  $f(x) = Dy^2$ , for some square-free  $D > 0$  and  $y(x) \in \mathbb{Q}[x]$ .
2. *complete with variable discriminant* (CVD) if  $f(x) = g(x)y(x)^2$ , for a linear  $g(x) \in \mathbb{Q}[x]$ .
3. *sparse*, if  $f(x) = g(x)y(x)^2$ , where  $g(x)$  is quadratic, non-square, with  $\text{lc}(g) > 0$ .

Using any type of family  $(p(x), t(x), r(x))$ , we can generate pairing-friendly elliptic curve parameters by evaluating these polynomials at some  $x_0 \in \mathbb{Z}$ , such that  $p(x_0), t(x_0)$  and  $r(x_0)$  are integers and  $p(x_0), r(x_0)$  are both primes. However we can relax this strict condition and allow  $r(x_0)$  to contain a small factor  $s$  and a large prime. This extra condition increases the number of suitable parameters that can be generated by a polynomial family. If such a  $x_0$  exists, then we obtain an elliptic curve  $E/\mathbb{F}_{p(x_0)}$ , with trace of Frobenius  $t(x_0)$  and order  $\#E(\mathbb{F}_{p(x_0)}) = h(x_0)r(x_0)$ .

Examples of complete families can be found in [1,2,8,10,15,16]. Complete families with variable discriminant are presented in [3,8,12,13]. Finally, examples of sparse families appear in [3,5–8,14]. In this paper we will focus on the first two types of families of Definition 2, namely complete and complete with variable discriminant families.

### 2.1. The Brezing-Weng method

The most well known method for constructing polynomial families of pairing-friendly elliptic curves in the sense of Definition 2 is the Brezing-Weng method [2]. This method was originally applied for the case of complete families. Several modifications were presented in [10,15,16] in order to construct more examples of complete families. In [3], Robert Dryło

---

#### Algorithm 1 The Brezing-Weng method [2].

---

**Input:** A number field  $K$  containing the  $k$ th roots of unity and  $\sqrt{-D}$ , for some square-free  $D > 0$  and a fixed  $k > 0$ .

**Output:** A complete family with embedding degree  $k$  and discriminant  $D$ .

- 1: Find a polynomial  $r(x) \in \mathbb{Q}[x]$ , such that  $K \cong \mathbb{Q}[x]/\langle r(x) \rangle$ .
  - 2: Choose a primitive  $k$ th root of unity  $\zeta_k \in K$ .
  - 3: Let  $t(x), y(x) \in \mathbb{Q}[x]$  mapping to  $\zeta_k + 1$  and  $(\zeta_k - 1)/\sqrt{-D}$  in  $K$  respectively.
  - 4: Compute  $p(x)$  by the relation  $4p(x) = t(x)^2 + Dy(x)^2$ .
  - 5: If  $p(x)$  represents primes, return  $(p(x), t(x), r(x))$ .
- 

presented a variant of the Brezing-Weng method for constructing the other two types of Definition 2, namely complete families with variable discriminant and sparse families. The original Brezing-Weng method is described in Algorithm 1.

The number field  $K$  in Algorithm 1 was set as the  $l$ th cyclotomic field  $\mathbb{Q}(\zeta_l)$ , for some  $l > 0$ , such that  $k \mid l$ , which implies that  $\zeta_k \in K$  and we also need  $\sqrt{-D} \in K$ . The polynomial  $r(x)$  is taken as the  $l$ th cyclotomic polynomial, in which case  $K \cong \mathbb{Q}[x]/\langle r(x) \rangle$ . Then we fix  $t(x)$  and  $y(x)$  as the polynomials representing the elements  $\zeta_k + 1$  and  $(\zeta_k - 1)/\sqrt{-D}$

in  $\mathbb{Q}[x]/(r(x))$ . Once these polynomials are determined, the calculation of the field polynomial  $p(x)$  is straightforward. It remains to examine whether  $p(x)$  satisfies the necessary conditions of Definition 1 and if this the case, we have a complete family of pairing-friendly elliptic curves with embedding degree  $k$ . A more detailed description of the Brezing-Weng method for constructing complete families is discussed in Section 3.

In [3] (Algorithm 5, p. 312), Robert Dryło extended the Brezing-Weng method in order to produce CVD families of pairing-friendly elliptic curves. His method works by fixing a number field  $K$  containing the primitive  $k$ th roots of unity and taking  $r(x)$  as the minimal polynomial of  $-z^2$ , for some  $z \in K$ , such that  $z^2$  is a primitive element of  $K$ . The difference between complete and CVD families is that the CM discriminant in the first case is some fixed, non-square positive value  $D$ , while in the case of CVD families it is represented by some linear polynomial  $g(x) = cx + d \in \mathbb{Q}[x]$ . However, we can always apply the linear transformation  $x \rightarrow (x - d)/c$  so that  $g(x) = x$ . This transformation is important as it makes the generation of pairing-friendly parameters easier for CVD families. We give a full analysis on how to construct this type of families via the Brezing and Weng method in Section 4.

Sparse families can also be constructed by modifying the Brezing-Weng method (see [3]). This type of families is probably the hardest one to study. This is due to the fact that it is computationally difficult to construct CM polynomials having a factorization as in Definition 2, namely  $f(x) = g(x)y(x)^2$ , for some quadratic, non-square polynomial  $g(x)$ , with positive leading coefficient. Another hard part in sparse families is that suitable elliptic curve parameters derive from the solutions of a generalized Pell equation and hence their generation is slightly more complicated than in the other two types of families. We do not consider this type of families in this paper, however several construction methods and various interesting examples can be found in [3,5,6,8,14].

A common characteristic in all three methods is that we need to ensure that the polynomials  $p(x)$ ,  $t(x)$  and  $r(x)$  are likely to extract integer values, or in other words they are *integer-valued*. This condition can be tested by examining whether there exists a linear transformation  $x \rightarrow (az + b)$  such that  $p(az + b)$ ,  $t(az + b)$  and  $r(az + b)$  have integer coefficients. When  $(p(x), t(x), r(x))$  is a complete family, we can generate suitable pairing-friendly parameters by searching for some  $x_0 \in \mathbb{Z}$ , such that  $p(x_0)$  and  $r(x_0)$  are both primes of a desired size (see Section 3 for details). On the other hand, when  $(p(x), t(x), r(x))$  is a CVD family, we are searching for some  $x_0 \in \mathbb{Z}$ , such that  $g(x_0) = x_0$  is a product of a square-free positive  $D$  times some perfect square  $y^2$  and  $p(x_0)$ ,  $r(x_0)$  are both primes of a desired size (see Section 4 for the precise algorithm). As stated earlier, more examples can be obtained by allowing  $r(x_0)$  to contain itself a small cofactor.

## 2.2. Our contribution

Numerous examples can be found in the literature for both complete and CVD families of pairing-friendly elliptic curves with various embedding degrees (see for example [1,2,8,3,10,15,13,16]). The families in these papers focus on  $\rho$ -values that are close to 1, in order to get the smallest possible extension fields  $\mathbb{F}_{p^k}$  that would in turn determine the efficiency of pairing calculations in the target group of a pairing. Unfortunately, this condition may not be ideal any more for a composite embedding degree  $k$ , due to the improvements of the TNFS method [9,11] for extension fields of composite degree. These TNFS variants lead to the conclusion that the previous examples we considered as optimal, may not still provide the same security level. Consequently, the searching for suitable elliptic curves that are ideal for implementation in pairing-based applications is still an open problem.

Motivated by these facts, in this paper we revise the criteria for selecting polynomial families of pairing-friendly elliptic curves for composite and prime embedding degrees in the range  $5 \leq k \leq 39$ . More precisely, the scope of this work is threefold:

1. **Composite  $k$ :** We construct complete and CVD families of pairing-friendly elliptic curves for various composite embedding degrees, which are likely to generate suitable curve parameters resistant to the new TNFS attacks presented in [9,11]. These families have larger  $\rho$ -values compared to previous results in order to enlarge the extension field size  $k \log p$  and hence increase the complexity of the DLP in the target group  $\mathbb{G}_T$  of asymmetric pairings.
2. **Prime  $k$ :** We present recommendations of complete and CVD families of pairing-friendly elliptic curves for prime embedding degrees that have not previously appeared in the literature, due to a larger  $\rho$ -value. Since this case is not affected by the new TNFS variants, pairing-friendly elliptic curve parameters can be chosen according to the recommendations in Table 1. We argue that our proposals in this case are capable in producing a balanced security level in the three pairing groups  $\mathbb{G}_1$ ,  $\mathbb{G}_2$  and  $\mathbb{G}_T$ .
3. **Numerical Examples:** For every recommended family with either composite or prime embedding degree we present numerical examples of pairing-friendly elliptic curve parameters achieving a security level of 128, 192 and 256-bits. For extension fields  $\mathbb{F}_{p^k}$  of composite degree, the asymptotic complexity of the DLP in the multiplicative group  $\mathbb{F}_{p^k}^*$  is calculated by  $L_N[1/3, 1.526]$  group operations achieved by the SexTNFS [9,11,4]. Since these new attacks do not apply for prime degree extension fields, the complexity of the DLP in  $\mathbb{F}_{p^k}^*$  is computed by  $L_N[1/3, 1.923]$ , where in both cases  $N = p^k$ .

We argue that at present, finding families with the smallest  $\rho$ -value is not of the main concern. The families we choose must have  $\rho$ -values such that the DLP in the extension field is resistant to the new TNFS attacks and approximately as hard

as in the source groups  $\mathbb{G}_1, \mathbb{G}_2$ . Therefore our recommendations consist of families of pairing-friendly elliptic curves with  $\rho(p, t, r) \leq 2$ .

### 3. Complete families revised

We give a detailed description of the Brezing-Weng method, presented in Algorithm 1, for constructing complete families of pairing-friendly elliptic curves. By earlier discussion in Section 2, in order to apply this method, we first fix a number field  $K$  containing the primitive  $k$ th roots of unity and the element  $\sqrt{-D}$ , for some square-free positive CM discriminant  $D$ . By [15] we know that the element  $\sqrt{-D}$  is contained in some cyclotomic field  $\mathbb{Q}(\zeta_m)$ , for some  $m > 0$ . Thus for a given

---

**Algorithm 2** The Brezing-Weng method for complete families of pairing-friendly elliptic curves.

---

**Input:** An embedding degree  $k$ , a square-free  $D > 0$ , such that  $\sqrt{-D} \in \mathbb{Q}(\zeta_m)$ , for some  $m > 0$ .

**Output:** A complete family  $(p(x), t(x), r(x))$  with embedding degree  $k$  and discriminant  $D$ .

- 1: Set  $K = \mathbb{Q}(\zeta_l)$ , where  $l = \text{lcm}(k, m)$  and  $r(x) = \Phi_l(x)$ , so that  $K \cong \mathbb{Q}[x]/\langle r(x) \rangle$ .
- 2: Let  $u(x)$  and  $z(x)$  be the polynomial mapping to  $\zeta_l$  and  $\sqrt{-D}$  respectively in  $\mathbb{Q}[x]/\langle r(x) \rangle$ .
- 3: For every  $i = 1, \dots, \varphi(l) - 1$ , such that  $l/\text{gcd}(i, l) = k$  set:

$$t(x) \equiv [u(x)^i + 1] \pmod{r(x)} \quad \text{and} \quad y(x) \equiv [(u(x)^i - 1)z(x)^{-1}] \pmod{r(x)}. \tag{3}$$

4: Compute  $p(x)$  by the relation  $4p(x) = t(x)^2 + Dy(x)^2$ .

5: If  $p(x)$  represents primes, return  $(p(x), t(x), r(x))$ .

---

embedding degree  $k$  and a CM discriminant  $D$  we can fix the number field  $K$  as  $\mathbb{Q}(\zeta_l)$ , where  $l = \text{lcm}(k, m)$ . In this case we set  $r(x) = \Phi_l(x)$ , where  $\text{deg } r = \phi(l)$  and such a choice ensures that  $K = \mathbb{Q}(\zeta_l) \cong \mathbb{Q}[x]/\langle r(x) \rangle$ . Our examples of complete families are based on this setting, however  $r(x)$  can be also chosen as any irreducible polynomial with respect to condition (2) of Definition 1 (see for example [1,10,16]).

This analysis leads us to the modified Brezing-Weng method presented in Algorithm 2. The complete families obtained by this algorithm have  $\rho$ -values less than 2 and particularly:

$$\rho(p, t, r) = \frac{\text{deg } p}{\text{deg } r} = \frac{2 \max\{\text{deg } t, \text{deg } y\}}{\text{deg } r} \leq \frac{2(\varphi(l) - 1)}{\varphi(l)} < 2.$$

This derives from the fact that  $t(x)$  and  $y(x)$  are polynomials in  $\mathbb{Q}[x]/\langle r(x) \rangle$  and hence their degree is less than the degree of the polynomial  $r(x)$ .

**Remark 3.** As we will see later on, sometimes it is helpful to search for polynomial families with  $\rho(p, t, r) = 2$ , especially for small embedding degrees. Such families can be obtained by choosing constant lifts of the polynomials  $t(x)$  and  $y(x)$  in  $\mathbb{Q}[x]$  (see [2,3]). In practice this means that in Equation (3) we can set:

$$t(x) = t_1 r(x) + [u(x)^i + 1] \pmod{r(x)}, \quad y(x) = y_1 r(x) + [(u(x)^i - 1)z(x)^{-1}] \pmod{r(x)},$$

for some lifts  $t_1, y_1 \in \mathbb{Q}[x]$ .  $\square$

The conditions for the element  $\sqrt{-D}$  to lie in the number field  $K = \mathbb{Q}(\zeta_l)$ , as well as the representation of  $\sqrt{-D}$  in a cyclotomic field are given in the next lemma, which taken from Murphy and Fitzpatrick [15].

**Lemma 4.** Let  $\zeta_l$  be a primitive  $l$ th root of unity and  $D$  a square-free positive integer.

1. If  $2 \nmid D, 4 \nmid D$  and  $D \mid l$ , then:

$$\begin{aligned} \sqrt{D} \in \mathbb{Q}(\zeta_l), \quad \mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\zeta_l), \quad \text{if } D \equiv 1 \pmod{4} \\ \sqrt{-D} \in \mathbb{Q}(\zeta_l), \quad \mathbb{Q}(\sqrt{-D}) \subset \mathbb{Q}(\zeta_l), \quad \text{if } D \equiv 3 \pmod{4} \end{aligned}$$

2. If  $4 \mid l$  and  $D \mid l$ , but  $2 \nmid D$  then  $\sqrt{D}, \sqrt{-D} \in \mathbb{Q}(\zeta_l)$  and  $\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{-D}) \subset \mathbb{Q}(\zeta_l)$ .
3. If  $8 \mid l$  and  $D \mid l$ , then  $\sqrt{D}, \sqrt{-D} \in \mathbb{Q}(\zeta_l)$  and  $\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{-D}) \subset \mathbb{Q}(\zeta_l)$ .

**Proof.** See [15], Lemma 2.3.  $\square$

Additionally, the representation of  $\sqrt{-D}$  in a cyclotomic field is based on the following facts. Let  $q$  be an odd prime,  $\zeta_q$  a primitive  $q$ th root of unity and  $\mathbb{Q}(\zeta_q)$  the  $q$ th cyclotomic field. Then:

**Table 2**  
Cyclotomic Complete families at 128-bit security level.

| $k$ | $l$ | $\text{degr}$ | $D$ | $i$ | $\rho(p, t, r)$ | $x_0$                      | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|---------------|-----|-----|-----------------|----------------------------|------------|--------------------|
| 7   | 7   | 6             | 7   | 3   | 1.6667          | $\{1, 4\} \bmod 7$         | 2987       | 137                |
| 7   | 21  | 12            | 3   | 3   | 1.6667          | $1 \bmod 3$                | 2987       | 137                |
| 7   | 28  | 12            | 1   | 16  | 1.5000          | $1 \bmod 2$                | 2688       | 131                |
| 10  | 20  | 8             | 1   | 2   | 1.7500          | $1 \bmod 2$                | 4480       | 129                |
| 10  | 20  | 8             | 5   | 18  | 1.7500          | $\{0, 4, 6\} \bmod 10$     | 4480       | 129                |
| 10  | 30  | 8             | 15  | 3   | 1.7500          | $\{1, 3, 6, 13\} \bmod 15$ | 4480       | 129                |
| 10  | 40  | 16            | 2   | 36  | 1.8750          | $0 \bmod 4$                | 4800       | 133                |
| 11  | 33  | 20            | 3   | 12  | 1.2000          | $1 \bmod 3$                | 3379       | 144                |
| 11  | 33  | 20            | 3   | 24  | 1.3000          | $\{1, 2\} \bmod 3$         | 3661       | 149                |
| 12  | 12  | 4             | 3   | 1   | 1.5000          | $1 \bmod 3$                | 4608       | 130                |
| 12  | 24  | 8             | 2   | 2   | 1.7500          | $1 \bmod 2$                | 5376       | 139                |

$$\prod_{i=1}^{(q-1)/2} (\zeta_q^i - \zeta_q^{-i}) = \begin{cases} \sqrt{q}, & \text{if } q \equiv 1 \pmod{4} \\ \sqrt{-q}, & \text{if } q \equiv 3 \pmod{4} \end{cases}$$

whereas  $\sqrt{2} = \zeta_4 \zeta_8(1 + \zeta_4)$  and  $\sqrt{-2} = \zeta_8(1 + \zeta_4)$ .

For every output of Algorithm 2, we need to make sure that the polynomials  $p(x), t(x)$  and  $r(x)$  have integer coefficients, or in other words they produce integer values. If this is true, then there exist  $a, b \in \mathbb{Z}$ , such that  $p(x) \in \mathbb{Z}$ , for every  $x \equiv b \pmod{a}$ . In order to generate suitable elliptic curve parameters  $p, t$  and  $r$ , we are searching for some  $x_0 \equiv b \pmod{a}$ , such that  $p(x_0)$  and  $r(x_0)$  are both primes, where  $r(x_0)$  has a desired size  $S_r$ . By the construction of the family  $(p(x), t(x), r(x))$ ,

**Algorithm 3** Finding suitable parameters using complete families.

**Input:** A complete family  $(p(x), t(x), r(x))$  and a desired bit size  $S_r$ .

**Output:** A prime  $p$ , a (nearly) prime  $r$  and a Frobenius trace  $t$ .

- 1: Find  $a, b \in \mathbb{Z}$ , so that  $p(x) \in \mathbb{Z}$ , for every  $x \equiv b \pmod{a}$ .
- 2: Search for  $x_0 \equiv b \pmod{a}$ , such that  $r(x_0) = nr$  for some prime  $r$  and  $n \geq 1$ .
- 3: Set  $p = p(x_0)$ ,  $r = r(x_0)/n$  and  $t = t(x_0)$ .
- 4: If  $\log r \approx S_r$  and  $p$  is prime, return  $(p, t, r)$  and  $D$ .

since it has a certain  $\rho$ -value, the size of  $p(x_0)$  will be around  $\rho(p, t, r)S_r$ . As stated in many papers we can relax this condition and allow  $r(x_0)$  to contain a small factor  $n \geq 1$ . In this case  $r = r(x_0)/n$  must be a large prime. This process is described in Algorithm 3. We emphasize on the fact that the search for suitable parameters described this algorithm is affected by the degree of the polynomials  $r(x), p(x)$  and particularly, as  $\text{degr}$  grows,  $\text{deg } p$  grows as well and it is harder to find suitable candidates  $x_0$  for both polynomials. Algorithm 3 is also affected by the size of the coefficients of these polynomials and more precisely, we need to keep the coefficients of  $r(x)$  and  $p(x)$  rather small. This is a reason why in most papers,  $r(x)$  is set as the  $l$ th cyclotomic polynomial (such polynomials have coefficients  $\pm 1$  and 0). Consequently, we require polynomials with relatively small degree and coefficients, depending on the security level we are working in.

3.1. Recommendations of complete families

We present our recommendations of complete families aiming at security levels of 128, 192 and 256 bits. For the rest of this paper, by security level, we mean the size of the corresponding key that is used for symmetric cryptography, such as in AES encryption scheme. Recall that our basic concern is not to find the families with the smallest  $\rho$ -values but we are rather interested in families with  $\rho$ -values such that the DLP in the  $r$ -order subgroups  $\mathbb{G}_1, \mathbb{G}_2$  of  $E(\mathbb{F}_{p^k})$  and in the extension field  $\mathbb{F}_{p^k}$  have approximately the same difficulty. Therefore we also introduce complete families with  $\rho(p, t, r) = 2$ . Most of the families presented here derive from the following setup:

$$r(x) = \Phi_l(x), \quad u(x) = x, \quad t(x) \equiv [u(x)^i + 1] \pmod{r(x)},$$

for some  $i = 1, \dots, \varphi(l) - 1$ , where  $u(x)$  is a primitive  $l$ th root of unity in  $\mathbb{Q}[x]/(r(x))$ . We will often refer to such families as *cyclotomic*. The asymptotic complexity of the DLP in the finite extension  $\mathbb{F}_{p^k}$  is measured by the  $L$ -notation given in Equation (1) (ignoring the constant  $o(1)$ ) for  $\ell = 1/3$ ,  $c = 1.923$ , when  $k$  is prime and  $c = 1.526$ , when  $k$  is composite, according to the improvements of the TNFS method for composite degree extension fields [9,11,4].

3.1.1. 128-bit security level

In Table 2 we give our recommendations for complete families that are likely to achieve a 128-bit security level in the source groups  $\mathbb{G}_1, \mathbb{G}_2$  of a pairing and in the extension field  $\mathbb{F}_{p^k}$ . In this case the prime  $r$  is around 256-bit long. On the other hand the asymptotic complexity of the DLP in  $\mathbb{F}_{p^k}$  implies that  $k \log p \approx 2530$  when  $k$  is prime and  $k \log p \approx 4352$  when  $k$  is composite. We observe that the best balance in Table 2 for a composite embedding degree is achieved by the



**Table 3**  
Cyclotomic Complete families at 128-bit security level with lifts  $t_1, y_1 \in \mathbb{Q}$  and  $\rho = 2$ .

| $k$ | $l$ | $\text{deg } r$ | $D$ | $i$ | $t_1$ | $y_1$ | $x_0$                  | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|-----------------|-----|-----|-------|-------|------------------------|------------|--------------------|
| 5   | 15  | 8               | 3   | 3   | 1     | 1     | $\{0, 2\} \bmod 3$     | 2560       | 128                |
| 5   | 20  | 8               | 1   | 12  | 1     | 0     | $0 \bmod 2$            | 2560       | 128                |
| 5   | 20  | 8               | 5   | 4   | 1     | 0     | $\{0, 2, 8\} \bmod 10$ | 2560       | 128                |
| 8   | 8   | 4               | 1   | 1   | 1     | 0     | $0 \bmod 2$            | 4096       | 124                |
| 8   | 8   | 4               | 2   | 3   | 1     | 0     | $1 \bmod 2$            | 4096       | 124                |
| 8   | 24  | 8               | 3   | 9   | 1     | -1    | $1 \bmod 3$            | 4096       | 124                |
| 9   | 9   | 6               | 3   | 5   | 1     | 1     | $2 \bmod 3$            | 4608       | 130                |
| 9   | 36  | 12              | 1   | 4   | 1     | 0     | $0 \bmod 2$            | 4608       | 130                |
| 9   | 72  | 24              | 2   | 8   | 1     | 0     | $0 \bmod 2$            | 4608       | 130                |

pairs  $(k, \rho) = (10, 1.75)$  and  $(12, 1.5)$ . In the first case, for a prime  $r$  around 256-bits, the size of the extension field  $\mathbb{F}_{p^{10}}$  is around 4480-bits, while for  $k = 12$ , we get an extension field around 4608-bits. For  $k = 10$ , there are three families with  $\rho(p, t, r) = 1.75$  in Table 2, with CM discriminants  $D \equiv 1, 5$  and 15. In Example 5 we describe how to extract the complete family for  $k = 10$ ,  $D = 5$  and  $\rho(p, t, r) = 1.75$  using Table 2.

**Example 5.** By Table 2, we set the number field  $K = \mathbb{Q}(\zeta_{20})$ . Thus we take  $r(x)$  as the 20th cyclotomic polynomial:

$$r(x) = \Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1 \quad \text{with} \quad \text{deg } r = 8$$

and  $u(x) = x$  is a primitive 20th root of unity in  $\mathbb{Q}[x]/\langle r(x) \rangle$ . By Lemma 4, the representation of  $\sqrt{-5}$  in  $K = \mathbb{Q}(\zeta_{20})$  is given by  $\sqrt{-5}\zeta_4(\zeta_5 - \zeta_5^4)(\zeta_5^2 - \zeta_5^3)$  and in  $\mathbb{Q}[x]/\langle r(x) \rangle$  by the polynomial:

$$z(x) \equiv \left[ u(x)^5 \left( u(x)^4 - u(x)^{16} \right) \left( u(x)^8 - u(x)^{12} \right) \right] \bmod r(x) \equiv \left( -2x^7 + x^5 - 2x^3 \right) \bmod r(x).$$

For  $i = 18$  in Algorithm 2 we obtain:

$$t(x) \equiv \left( -x^6 + x^4 - x^2 + 2 \right) \bmod r(x) \quad \text{and} \quad y(x) \equiv \frac{1}{5} \left( -2x^7 + 3x^5 - 3x^3 + 2x \right) \bmod r(x).$$

The field polynomial  $p(x)$  is calculated by the relation:

$$p(x) = \frac{1}{4} \left[ t(x)^2 + 5y(x)^2 \right] = \frac{1}{20} \left( 4x^{14} - 7x^{12} + 11x^{10} - 11x^8 - 9x^6 + 13x^4 - 16x^2 + 20 \right).$$

The polynomial  $p(x)$  is integer-valued when evaluated at integers satisfying  $x \equiv \{0, 4, 6\} \bmod 10$ . We conclude that the polynomial triple  $(p(x), t(x), r(x))$  represents a complete family of elliptic curves with embedding degree  $k = 10$ , CM discriminant  $D = 5$  and  $\rho$ -value:

$$\rho(p, t, r) = \frac{\text{deg } p}{\text{deg } r} = \frac{7}{4} = 1.7500.$$

All examples of Table 2, as well as in all tables of this section are obtained in the same way.  $\square$

The remaining examples of complete families in Table 2 also provide an acceptable balance between the security level in the source groups  $\mathbb{G}_1, \mathbb{G}_2$  and  $\mathbb{F}_{p^k}$ , but with a slightly larger extension field. An optimal balance in the prime embedding degree case is achieved by families with  $k = 5$  and  $\rho(p, t, r) = 2$ . We can obtain such families by applying Algorithm 2 and considering constant lifts  $t_1, y_1 \in \mathbb{Q}$  for the polynomials  $t(x)$  and  $y(x)$ , as stated in Remark 3. Examples of complete families with embedding degrees 5, 8 and 9, aiming at a security level of 128-bits in the extension field are presented in Table 3. This are the first examples of families in the literature with  $\rho(p, t, r) = 2$ . Note that when  $k = 5$ , and  $\log r = 256$ , the extension field  $\mathbb{F}_{p^5}$  is approximately 2560-bits, which is not very large, although  $\rho = 2$  is far from the ideal case. On the other hand, for the case  $k = 8$ , the best examples so far had  $\rho(p, t, r) = 1.5$  resulting in extension fields of size around 3072-bits. We argue that the optimal case for  $k = 8$  should be revised and use families with  $\rho(p, t, r) = 2$  yielding extension fields around 4096-bits. Finally, we can also reach an extension field with 128-bit security level by choosing  $k = 9$  and  $\rho(p, t, r) = 2$ , where  $9 \log q \approx 4608$ . These facts justify our earlier claim, that finding families with the smallest  $\rho$ -value should not be our main concern at this point.

### 3.1.2. 192-bit security level

Our recommendations for complete families that achieve a 192-bit security level in the three pairing groups  $\mathbb{G}_1, \mathbb{G}_2$  and  $\mathbb{G}_T$  are presented in Table 4. Clearly there is a larger variety of available families to choose from in this case. The size of the prime  $r$  dividing the order of the curve is now 384-bits. The asymptotic complexity of the DLP in the extension field  $\mathbb{F}_{p^k}$  implies that for the prime embedding degree case we must have  $k \log p \approx 6670$ , while in the composite case we

**Table 4**  
Cyclotomic Complete families at 192-bit security level.

| $k$ | $l$ | $\text{degr}$ | $D$ | $i$ | $\rho(p, t, r)$ | $x_0$               | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|---------------|-----|-----|-----------------|---------------------|------------|--------------------|
| 11  | 11  | 10            | 11  | 1   | 1.8000          | {1, 4, 8, 9} mod 11 | 7603       | 202                |
| 11  | 11  | 10            | 11  | 8   | 1.6000          | 1 mod 11            | 6758       | 193                |
| 11  | 33  | 20            | 3   | 6   | 1.7000          | {1, 2} mod 3        | 7181       | 197                |
| 11  | 33  | 20            | 3   | 18  | 1.8000          | 1 mod 3             | 7603       | 202                |
| 11  | 33  | 20            | 3   | 27  | 1.6000          | 1 mod 3             | 6758       | 193                |
| 11  | 44  | 20            | 1   | 28  | 1.7000          | 1 mod 2             | 7181       | 197                |
| 13  | 39  | 24            | 3   | 3   | 1.3333          | 1 mod 3             | 6656       | 191                |
| 13  | 39  | 24            | 3   | 18  | 1.5000          | 1 mod 3             | 7488       | 201                |
| 13  | 39  | 24            | 3   | 30  | 1.4167          | {1, 2} mod 3        | 7072       | 196                |
| 13  | 52  | 24            | 1   | 30  | 1.4167          | 1 mod 2             | 7072       | 196                |
| 16  | 16  | 8             | 2   | 1   | 1.7500          | 1 mod 2             | 10752      | 185                |
| 18  | 72  | 24            | 2   | 4   | 1.5833          | 1 mod 2             | 10944      | 186                |
| 20  | 20  | 8             | 1   | 1   | 1.5000          | 1 mod 2             | 11520      | 190                |
| 20  | 60  | 16            | 3   | 3   | 1.6250          | {1, 2} mod 3        | 12480      | 196                |
| 21  | 21  | 12            | 3   | 1   | 1.3333          | 1 mod 3             | 10752      | 185                |
| 21  | 21  | 12            | 3   | 2   | 1.5000          | {1, 2} mod 3        | 12096      | 194                |
| 22  | 44  | 20            | 1   | 2   | 1.3000          | 1 mod 2             | 10982      | 187                |
| 22  | 44  | 20            | 1   | 26  | 1.5000          | 1 mod 2             | 12672      | 198                |
| 22  | 66  | 20            | 3   | 3   | 1.4000          | 1 mod 3             | 11827      | 192                |
| 24  | 24  | 8             | 3   | 1   | 1.2500          | 1 mod 3             | 11520      | 190                |
| 26  | 78  | 24            | 3   | 27  | 1.1667          | 1 mod 3             | 11648      | 191                |
| 27  | 27  | 18            | 3   | 1   | 1.1111          | 1 mod 3             | 11520      | 190                |

**Table 5**  
Cyclotomic Complete families at 192-bit security level with lifts  $t_1, y_1 \in \mathbb{Q}$  and  $\rho = 2$ .

| $k$ | $l$ | $\text{degr}$ | $D$ | $i$ | $t_1$ | $y_1$ | $x_0$            | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|---------------|-----|-----|-------|-------|------------------|------------|--------------------|
| 15  | 15  | 8             | 3   | 4   | 1     | 1     | 0 mod 3          | 11520      | 190                |
| 15  | 15  | 8             | 15  | 7   | 1     | 1     | {11, 14} mod 15  | 11520      | 190                |
| 15  | 60  | 16            | 1   | 4   | 1     | 0     | 0 mod 2          | 11520      | 190                |
| 15  | 60  | 16            | 5   | 4   | 1     | 0     | {0, 4, 6} mod 10 | 11520      | 190                |
| 16  | 16  | 8             | 2   | 1   | 1     | 1     | 1 mod 2          | 12288      | 195                |
| 16  | 16  | 8             | 1   | 1   | 1     | 0     | 0 mod 2          | 12288      | 195                |
| 16  | 48  | 16            | 3   | 33  | 1     | 1     | 1 mod 3          | 12288      | 195                |

have  $k \log p \approx 11670$ . The best balance when  $k$  is prime can be obtained by the pairs  $(k, \rho) = (11, 1.6)$  and  $(13, 1.3333)$ . In the first case,  $p^{11}$  is 6758-bit long and we present two such families in Table 4 with CM discriminant  $D = 3$  and 11. In the second case,  $p^{13}$  has a size around 6656-bits and there is one family for CM discriminant  $D = 3$  in Table 4. For composite embedding degrees there are even more optimal families, for example  $(k, \rho) = (20, 1.5)$ ,  $(22, 1.4)$ ,  $(26, 1.1667)$ . These examples provide an extension field of size 11500 to 11900-bits, with security level around 192-bits, according to the asymptotic complexity given by Equation (1). The rest of the families in Table 4 also provide a nicely balanced security level in all pairing-groups. An optimal balance for composite embedding degrees can be also achieved with complete families having  $\rho(p, t, r) = 2$ . For families with this property, we need to take constant lifts  $t_1, y_1 \in \mathbb{Q}$ , in order to reach an 192-bit security level in the extension field  $\mathbb{F}_{p^k}$ . We present such examples in Table 5, for  $k = 15, 16$ .

### 3.1.3. 256-bit security level

For a 256-bit security level, the extension field  $\mathbb{F}_{p^k}$  gets even larger. Today's requirements indicate that the optimal security level is around 128-bits corresponding to an AES symmetric key. Larger security levels, such as 192 and 256-bits, are for future reference. Additionally, the prime  $r$  that represents the order of the three pairing groups  $\mathbb{G}_1, \mathbb{G}_2$  and  $\mathbb{G}_T$  has now a size of 512-bits. Complete families at this security level should generate extension fields  $\mathbb{F}_{p^k}$  around 13500-bits in the prime case and 23900-bits in the composite case. We give a list of optimal complete families in Table 6. The best balance in the prime case is achieved by the pairs  $(k, \rho) = (17, 1.5625)$ ,  $(19, 1.3889)$  and  $(23, 1.1364)$ . On the other hand, for composite embedding degrees we get the best balance by the families with  $(k, \rho) = (28, 1.6667)$ ,  $(34, 1.3750)$ . Finally, in Table 7 we demonstrate complete families with embedding degrees  $k = 13$  and 24 and  $\rho(p, t, r) = 2$ . These are suitable for generating the desired extension fields, where the DLP is resistant to the new variants of the TNFS attacks.

### 3.1.4. Non-cyclotomic families

More complete families can be constructed by choosing the polynomial  $r(x)$  to be other than a cyclotomic polynomial, with respect to condition (2) of Definition 1. We refer to this type of complete families as *non-cyclotomic*. Such examples appear in [10,16], which however need to be updated as the proposed families were produced in the pre-TNFS period. The difficult part when constructing non-cyclotomic families is the choice of the polynomial  $r(x)$  and the primitive  $k$ th root of unity  $u(x) \in \mathbb{Q}[x]/(r(x))$ . Strategies for determining such polynomials can be found in [6,10,12,13,16]. However the problem



**Table 6**  
Cyclotomic Complete families at 256-bit security level.

| $k$ | $l$ | $\text{deg } r$ | $D$ | $i$ | $\rho(p, t, r)$ | $x_0$        | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|-----------------|-----|-----|-----------------|--------------|------------|--------------------|
| 17  | 51  | 32              | 3   | 24  | 1.5000          | 1 mod 3      | 13056      | 252                |
| 17  | 51  | 32              | 3   | 42  | 1.5625          | {1, 2} mod 3 | 13600      | 256                |
| 17  | 68  | 32              | 1   | 8   | 1.5625          | 1 mod 2      | 13600      | 256                |
| 19  | 57  | 36              | 3   | 6   | 1.3889          | {1, 2} mod 3 | 13511      | 256                |
| 19  | 57  | 36              | 3   | 24  | 1.3333          | 1 mod 3      | 12971      | 252                |
| 19  | 76  | 36              | 1   | 44  | 1.3889          | 1 mod 2      | 13511      | 256                |
| 23  | 69  | 44              | 3   | 3   | 1.1818          | 1 mod 3      | 13916      | 259                |
| 23  | 69  | 44              | 3   | 48  | 1.1364          | {1, 2} mod 3 | 13382      | 255                |
| 23  | 92  | 44              | 1   | 48  | 1.1364          | 1 mod 2      | 13382      | 255                |
| 25  | 75  | 40              | 3   | 12  | 1.8500          | {1, 2} mod 3 | 23680      | 255                |
| 25  | 100 | 40              | 1   | 12  | 1.8500          | 1 mod 2      | 23680      | 255                |
| 26  | 78  | 24              | 3   | 9   | 1.8333          | 1 mod 3      | 24405      | 258                |
| 26  | 104 | 48              | 2   | 4   | 1.7917          | 1 mod 2      | 23851      | 255                |
| 26  | 104 | 48              | 2   | 44  | 1.8333          | 1 mod 2      | 24405      | 258                |
| 27  | 27  | 18              | 3   | 7   | 1.7778          | 1 mod 3      | 24576      | 258                |
| 27  | 108 | 36              | 1   | 4   | 1.7222          | 1 mod 2      | 23808      | 255                |
| 28  | 28  | 12              | 1   | 3   | 1.6667          | 1 mod 2      | 23893      | 256                |
| 30  | 30  | 8               | 3   | 1   | 1.5000          | 1 mod 3      | 23040      | 252                |
| 30  | 60  | 16              | 5   | 34  | 1.6250          | 5 mod 10     | 24960      | 260                |
| 33  | 33  | 20              | 3   | 14  | 1.4000          | 1 mod 3      | 23654      | 255                |
| 34  | 68  | 32              | 1   | 6   | 1.4375          | 1 mod 2      | 25024      | 260                |
| 34  | 102 | 32              | 3   | 39  | 1.3750          | 1 mod 3      | 23936      | 256                |
| 39  | 39  | 24              | 3   | 1   | 1.1667          | 1 mod 3      | 23296      | 253                |
| 39  | 39  | 24              | 3   | 2   | 1.2500          | {1, 2} mod 3 | 24960      | 260                |

**Table 7**  
Cyclotomic Complete families at 256-bit security level with lifts  $t_1, y_1 \in \mathbb{Q}$  and  $\rho = 2$ .

| $k$ | $l$ | $\text{deg } r$ | $D$ | $i$ | $t_1$ | $y_1$ | $x_0$                           | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|-----------------|-----|-----|-------|-------|---------------------------------|------------|--------------------|
| 13  | 39  | 24              | 3   | 12  | 1     | 1     | 0 mod 3                         | 13312      | 254                |
| 13  | 52  | 24              | 1   | 4   | 1     | 0     | 0 mod 2                         | 13312      | 254                |
| 13  | 52  | 24              | 13  | 4   | 1     | 0     | {0, 2, 4, 8, 18, 22, 24} mod 26 | 13312      | 254                |
| 24  | 24  | 8               | 1   | 1   | 1     | 0     | 0 mod 2                         | 24576      | 258                |
| 24  | 24  | 8               | 2   | 1   | 1     | 0     | 0 mod 4                         | 24576      | 258                |
| 24  | 24  | 8               | 3   | 17  | 1     | 1     | 1 mod 3                         | 24576      | 258                |
| 24  | 24  | 8               | 6   | 7   | 1     | 0     | 2 mod 12                        | 24576      | 258                |

is that the coefficients of the polynomials  $r(x)$  and  $p(x)$  might get very large affecting the process of generating suitable curve parameters.

The most famous non-cyclotomic complete family is due to Barreto and Naehrig’s *BN-family*. It has embedding degree  $k = 12$ , CM discriminant  $D = 3$  and  $\rho(p, t, r) = 1$  and it is represented by the polynomials:

$$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1, \quad t(x) = 6x^2 + 1, \quad p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1,$$

where  $u(x) = 6x^2$  is a primitive 12th root of unity in  $\mathbb{Q}[x]/\langle r(x) \rangle$ . This example was ideal for a security level of 128-bits in the pre-TNFS period, since it produces elliptic curve parameters with  $\rho = 1$ . More precisely, for a 256-bit prime  $r$ , it produces an extension field of 3072-bit. Due to the recent improvements of the TNFS method, the security level in  $\mathbb{F}_{p^{12}}$  only reaches 110-bits. Therefore we need to consider larger extensions fields and particularly of size  $12 \log p \approx 4608$  leading to families with  $\rho(p, t, r) = 1.5$  (see for example our recommendation in Table 2). The next example is produced by Barreto and Naehrig’s setup.

**Example 6.** For  $l = k = 12$  and  $D = 3$ , set:

$$\begin{aligned} r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1 \\ u(x) = 6x^2 &\implies t(x) \equiv [u(x)^7 + 1] \pmod{r(x)} = -6x^2 + 1 \\ p(x) &= 1728x^6 + 2160x^5 + 1548x^4 + 756x^3 + 240x^2 + 54x + 7 \end{aligned}$$

The  $\rho(p, t, r) = 1.5$  and all polynomials have integer coefficients.  $\square$

Kachisa et al. [10] presented several examples on non-cyclotomic families, that need to be updated. We give alternatives to these examples, based on the polynomials  $r(x)$  and  $u(x)$  presented in [10].

**Example 7.** For  $l = k = 16$ ,  $D = 1$  and set:

$$r(x) = x^8 + 48x^4 + 625$$

$$u(x) = (-2x^7 + 29x^3)/875 \implies t(x) \equiv [u(x)^3 + 1] \pmod{r(x)} = (-2x^7 + 29x^3 + 1)/875$$

$$p(x) = (x^{14} - 22x^{11} + 48x^{10} + 125x^8 - 1112x^7 + 625x^6 + 6000x^4 - 12938x^3 + 78125)/24500$$

Then  $\rho(p, t, r) = 1.75$  and all polynomials are integer-valued when  $x \equiv \{25, 45\} \pmod{70}$ .  $\square$

This family is suitable for producing extension fields of size  $16 \log p = 10752$ -bits, providing a security level of 185-bits, for primes  $r$  around 384-bits. The polynomials  $r(x)$  and  $u(x)$  were used in [10] to construct a complete family with  $\rho(p, t, r) = 1.25$ , which does not fall into any of the three security levels we consider.

### 3.2. Numerical examples

In Table 8 we give a list of numerical examples obtained by selected complete families presented in this section, for security levels of 128, 192 and 256-bits. Recall that in order to generate suitable elliptic curve parameters, given a complete family of pairing-friendly elliptic curves, we apply Algorithm 3. The column “ $x_0$ ” refers to the integer input for the polynomials  $p(x)$ ,  $t(x)$  and  $r(x)$ . The column “ $n$ ” on the other hand denotes the possible cofactor contained in  $r(x_0)$ , in which case by Algorithm 3 we set  $r = r(x_0)/n$ . As stated earlier, this factor  $n$  might be helpful in some cases as it further increases the size of the extension field. In the final column we measure the security level provided by the constructed extension field, using Equation (1) and ignoring the constant  $o(1)$ .

For instance, recall the complete family  $(p(x), t(x), r(x))$  with  $k = 10$  and  $D = 5$  presented in Example 5. In order to obtain integer triples, these polynomials must be evaluated at some  $x_0$ , such that  $x_0 \equiv \{0, 4, 6\} \pmod{10}$ . If we set  $x_0 = 4658060020 \equiv 0 \pmod{10}$ , we obtain the following parameters:

$$r(x_0) = 22163617251415031266325075694218605110560054976974123945895535 \\ 4678221533759601$$

$$p(x_0) = 45279447453335595936920178688640432706575155450889283537011469 \\ 50122092141266824754981156165939483994764135169768897393282580 \\ 43201383681$$

$$t(x_0) = -10214814427560271006181812182933762983830315056204066240398$$

with  $\rho = 1.7461$ . Additionally, the prime  $r(x_0)$  is 256-bits and the extension field  $\mathbb{F}_{p^{10}}$  has size 4470-bits, corresponding to a security level of 129-bits, according to Equation (1). Therefore, these parameters are ideal for a 128-bit security level. The rest of the examples in Table 8 are obtained by the families of this section in the same way.

Recall also that the search for suitable  $x_0$  is affected by both the degree of the polynomial  $r(x)$ , as well as by the size of its leading coefficient. In particular, this search is performed by choosing at random  $x_0 \in \mathbb{Z}$  such that:

$$\text{degr} \cdot \log x_0 + \log(\text{lc}(r)) \approx \text{security level}, \quad (4)$$

where  $\text{lc}(r)$  is the leading coefficient of  $r(x)$ . Note that when  $r(x) = \Phi_l(x)$  in cyclotomic families, then  $\log(\text{lc}(r)) = 0$ . The security level in the  $r$ -order subgroups  $\mathbb{G}_1, \mathbb{G}_2$  is taken as  $\log r/2$ . In Equation (4) it is clear that  $\text{degr}$  affects the search and thus, it should not be too large. For example, for a 128-bit security level we have considered families with  $\text{degr} \leq 24$ . For 192-bit security level our families have  $\text{degr} \leq 24$  and for 256-bit security level we set the restriction  $\text{degr} \leq 48$ . On the other hand, the security level in the extension field  $\mathbb{F}_{p^k}$  is measured by the  $L$ -notation of Equation (1), namely  $L_{p^k}[1/3, c]$ , where  $c = 1.923$  when  $k$  is prime and  $c = 1.526$  when  $k$  is composite. In general we want  $L_{p^k}[1/3, c] \approx \log r/2$ . Table 8 is just an instance of a few numerical examples. There are a lot of different triples  $(p, t, r)$  that can be produced by applying the techniques described in this section. Furthermore, we emphasize on the fact that the easiest way to generate pairing-friendly elliptic curve parameters is to use complete families, rather than the other two types of Definition 2.

## 4. CVD families revised

By Definition 2, the CM polynomial  $f(x) = 4q(x) - t(x)^2$  is equal to the product of some linear term  $g(x) = cx + d$  times a perfect square  $y(x)^2$ . As stated in Section 2 we can always apply on  $g(x)$  a linear transformation  $x \rightarrow (x - d)/c$  in order to obtain  $g(x) = x$ . The difference in the case of CVD families is that the CM discriminant is not constant and predefined as in complete families, but it is represented by the linear term  $g(x) = x$ . Thus for a fixed embedding degree  $k$  we need to find a number field  $K$  containing both the primitive  $k$ th roots of unity and the element  $\sqrt{-x}$ .

According to Dryła [3], we can apply a modified version of the Brezing-Weng method, introduced in Algorithm 2, for the case of CVD families. This modified version is presented in Algorithm 4. We set  $K = \mathbb{Q}(\zeta_l)$  and  $r(x) = \Phi_l(x)$ , for some  $l > 0$ , with  $k | l$  and then search for a polynomial  $z(x) \in \mathbb{Q}[x]/\langle r(x) \rangle$ , such that  $-z(x)^2 \equiv x \pmod{r(x)}$ . This search is easy

**Table 8**  
Numerical examples of pairing-friendly parameters from selected complete families.

| Source    | $k$ | $D$ | $x_0$                                   | $n$ | $\log r$ | $k \log p$ | $\rho$ | $L_{p^k}[1/3, c]$ |
|-----------|-----|-----|---|-----|----------|------------|--------|-------------------|
| Table 3   | 5   | 3   | $4467952995 \equiv 0 \pmod 3$           | 1   | 256      | 2560       | 2.0000 | 128               |
| Table 3   | 5   | 5   | $4339430220 \equiv 0 \pmod{10}$         | 1   | 256      | 2550       | 1.9922 | 128               |
| Table 3   | 5   | 1   | $5335509292 \equiv 0 \pmod 2$           | 5   | 256      | 2575       | 2.0117 | 129               |
| Table 2   | 7   | 1   | $2713075 \equiv 1 \pmod 2$              | 1   | 256      | 2674       | 1.4922 | 131               |
| Table 3   | 8   | 1   | $68654621113518002124 \equiv 0 \pmod 2$ | 113 | 256      | 4200       | 2.0508 | 125               |
| Table 3   | 8   | 2   | $60985336081474503491 \equiv 1 \pmod 2$ | 82  | 256      | 4184       | 2.0430 | 125               |
| Table 3   | 8   | 3   | $8318694697 \equiv 1 \pmod 3$           | 193 | 256      | 4216       | 2.0586 | 126               |
| Table 2   | 10  | 1   | $4327482431 \equiv 1 \pmod 2$           | 1   | 256      | 4460       | 1.7422 | 129               |
| Table 2   | 10  | 5   | $4658060020 \equiv 0 \pmod{10}$         | 1   | 256      | 4470       | 1.7461 | 129               |
| Table 2   | 10  | 15  | $4506234361 \equiv 1 \pmod{15}$         | 1   | 256      | 4470       | 1.7461 | 129               |
| Table 2   | 12  | 3   | $19476673796408493595 \equiv 1 \pmod 3$ | 1   | 256      | 4584       | 1.4922 | 130               |
| Example 6 | 12  | 3   | $7968144943122361485$                   | 1   | 256      | 4644       | 1.5117 | 131               |
| Table 4   | 11  | 3   | $609856 \equiv 1 \pmod 3$               | 1   | 384      | 6743       | 1.5964 | 192               |
| Table 4   | 13  | 3   | $66427 \equiv 1 \pmod 3$                | 1   | 384      | 6643       | 1.3307 | 191               |
| Table 5   | 15  | 3   | $663228522589779 \equiv 0 \pmod 3$      | 751 | 384      | 11805      | 2.0495 | 192               |
| Table 4   | 21  | 3   | $4371055696 \equiv 1 \pmod 3$           | 1   | 384      | 12054      | 1.4948 | 194               |
| Table 4   | 22  | 3   | $602956 \equiv 1 \pmod 3$               | 1   | 384      | 11792      | 1.3958 | 192               |
| Table 4   | 26  | 3   | $66211 \equiv 1 \pmod 3$                | 1   | 384      | 11596      | 1.1615 | 191               |
| Table 7   | 13  | 13  | $3188926 \equiv 0 \pmod{26}$            | 1   | 512      | 13455      | 2.0215 | 255               |
| Table 7   | 24  | 2   | $19228544116597719574 \equiv 2 \pmod 4$ | 1   | 512      | 24576      | 2.0000 | 258               |
| Table 6   | 26  | 3   | $2710936 \equiv 1 \pmod 3$              | 1   | 512      | 24388      | 1.8320 | 258               |
| Table 6   | 27  | 3   | $389679094 \equiv 1 \pmod 3$            | 1   | 512      | 24597      | 1.7793 | 258               |
| Table 6   | 28  | 1   | $7238566404315 \equiv 1 \pmod 2$        | 1   | 512      | 23856      | 1.6641 | 255               |
| Table 6   | 39  | 3   | $3305782 \equiv 1 \pmod 3$              | 157 | 512      | 23556      | 1.1797 | 254               |

when  $r(x)$  is the  $l$ th cyclotomic polynomial (see for example [3]). However if we set  $r(x)$  as any irreducible polynomial in  $\mathbb{Q}[x]$ , satisfying condition (2) of Definition 1, the search is harder, especially as  $\deg r$  grows. A few such examples are also presented in [3]) (see also [12,13], for additional examples). Once  $z(x)$  is determined, then we proceed according to

**Algorithm 4** The Brezing-Weng method for CVD families of pairing-friendly elliptic curves.

**Input:** An embedding degree  $k$ .

**Output:** A CVD family  $(p(x), t(x), r(x))$  with embedding degree  $k$ .

- 1: Set  $K = \mathbb{Q}(\zeta_l)$ , where  $k \mid l$  and  $r(x) = \Phi_l(x)$ , so that  $K \cong \mathbb{Q}[x]/(r(x))$ .
- 2: Find a polynomial  $z(x) \in K$ , such that  $-z(x)^2 \equiv x \pmod{r(x)}$ .
- 3: Let  $u(x)$  be the polynomial mapping to  $\zeta_l$  in  $\mathbb{Q}[x]/(r(x))$ .
- 4: For every  $i = 1, \dots, \varphi(l) - 1$ , such that  $l/\gcd(i, l) = k$  set:

$$t(x) \equiv [u(x)^i + 1] \pmod{r(x)} \quad \text{and} \quad y(x) \equiv [(u(x)^i - 1)z(x)^{-1}] \pmod{r(x)}. \tag{5}$$

- 5: Compute  $p(x)$  by the relation  $4p(x) = t(x)^2 + xy(x)^2$ .
- 6: If  $p(x)$  represents primes, return  $(p(x), t(x), r(x))$ .

Algorithm 2. The only thing that changes is the construction of the field polynomial in Equation (5). The families produced by Algorithm 4 have generally  $\rho$ -values:

$$\rho(p, t, r) = \frac{\deg p}{\deg r} = \frac{\max\{2 \deg t, 2 \deg y + 1\}}{\deg r} \leq \frac{2\varphi(l) - 1}{\varphi(l)} < 2.$$

By Remark 3, if we wish to obtain a CVD family with  $\rho(p, t, r) = 2$  we need to consider constant lifts  $t_1, y_1 \in \mathbb{Q}$  for the polynomials  $t(x)$  and  $y(x)$  respectively in step (3) of Algorithm 4.

As in complete families, the outputs of Algorithm 4 are potential CVD families, since we need to make sure that the constructed polynomials are integer-valued. Thus we need to search for  $a, b \in \mathbb{Z}$ , such that  $p(x) \in \mathbb{Z}$ , for every  $x \equiv b \pmod a$ .

**Algorithm 5** Finding suitable parameters using CVD families.

**Input:** A CVD family  $(p(x), t(x), r(x))$  and a desired bit size  $S_r$ .

**Output:** A prime  $p$ , a (nearly) prime  $r$  and a Frobenius trace  $t$ .

- 1: Find  $a, b \in \mathbb{Z}$ , so that  $p(x) \in \mathbb{Z}$ , for every  $x \equiv b \pmod a$ .
- 2: Search for  $x_0 \in \mathbb{Z}$  of the form  $x_0 = Dy^2$ , with  $x_0 \equiv b \pmod a$ , such that  $r(x_0) = nr$  for some prime  $r$  and  $n \geq 1$ .
- 3: Set  $p = p(x_0)$ ,  $r = r(x_0)/n$  and  $t = t(x_0)$ .
- 4: If  $\log r \approx S_r$  and  $p$  is prime, return  $(p, t, r)$  and  $D$ .

Then, in order to generate pairing-friendly parameters using this type of families, we are searching for  $x_0 \in \mathbb{Z}$ , such that  $p(x_0)$  is prime and  $r(x_0)$  is nearly prime, i.e. it contains a small factor  $n \geq 1$ . An additional condition in this case is that  $g(x_0)$

**Table 9**  
Cyclotomic CVD families at 128-bit security level.

| $k$ | $l$ | $\text{deg } r$ | $i$ | $\rho(p, t, r)$ | $x_0$   | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|-----------------|-----|-----------------|---------|------------|--------------------|
| 7   | 14  | 6               | 8   | 1.5000          | 1 mod 2 | 2688       | 131                |
| 9   | 18  | 6               | 10  | 1.8333          | 1 mod 2 | 4224       | 126                |
| 10  | 10  | 4               | 1   | 1.7500          | 1 mod 2 | 4480       | 129                |
| 11  | 22  | 10              | 6   | 1.2000          | 1 mod 2 | 3379       | 144                |
| 14  | 14  | 6               | 1   | 1.5000          | 1 mod 2 | 5376       | 139                |

must be equal to the product of some square-free  $D > 0$  times a perfect square  $y^2$ . We can perform this search by setting  $x_0 = Dy^2$  and vary  $D, y$  until we hit a valid pair  $(D, y)$ , for which  $g(x_0) = Dy^2$ . This procedure is described in Algorithm 5 (see also Paragraph 4.2 for generating suitable elliptic curve parameters using CVD families). Once again this process is affected by the degree of the polynomial  $r(x)$ , as well as the size of its coefficients (especially the leading coefficient).

In general, CVD families are a nice choice for applications that require large and flexible CM discriminants. Although there is no particular attack on elliptic curves with small discriminants, in [4] it is recommended to use curves with large  $D$ . However we emphasize on the fact that the values for  $D$  to be tested must be relatively small (e.g.  $D < 10^{10}$ ), in order to apply the CM method for constructing elliptic curves efficiently. Another option for flexible CM discriminants is to use sparse families (see for example [3,6,8]), but in this case the procedure of generating suitable parameters is slightly more complicated.

4.1. Recommendations of CVD families

We now present our recommendations of CVD families at the usual security levels of 128, 192 and 256-bits. As stated in the case of complete families, our basic concern is to introduce CVD families with  $\rho$ -values such that the DLP in the  $r$ -order subgroups  $\mathbb{G}_1, \mathbb{G}_2$  of  $E(\mathbb{F}_{p^k})$  and in the extension field  $\mathbb{F}_{p^k}$  have approximately the same difficulty. Therefore we also introduce CVD families with  $\rho(p, t, r) = 2$ , that have not been considered before. The proposed CVD families are mainly cyclotomic families obtained by the following setup:

$$r(x) = \Phi_l(x), \quad u(x) = x, \quad t(x) \equiv [u(x)^i + 1] \pmod{r(x)}, \quad z(x) = x^{\frac{l/2+1}{2}}, \tag{6}$$

for  $i = 1, \dots, \varphi(l) - 1$ , where  $u(x)$  and  $z(x)$  represent the primitive  $l$ th root of unity and the element  $\sqrt{-x}$  in  $\mathbb{Q}[x]/\langle r(x) \rangle$  respectively. In addition, by the choice of  $z(x)$  in Equation (6), we get that  $l$  must be an even, positive integer. This setup was first considered by Dryło [3], however his families are aiming for the smallest  $\rho$ -values for each embedding degree. In addition we also introduce a few non-cyclotomic CVD families for embedding degrees that do not appear in the cyclotomic case. For every proposed family we measure the asymptotic complexity of the DLP in the finite extension  $\mathbb{F}_{p^k}$  by using the  $L$ -notation of Equation (1), for  $l = 1/3, c = 1.923$ , when  $k$  is prime and  $c = 1.526$ , when  $k$  is composite. This follows from the recent improvements of the TNFS methods for composite degree extension fields [9,11,4].

4.1.1. 128-bit security level

Examples of cyclotomic CVD families for a 128-bit security are presented in Table 9. Recall that in this case the prime  $r = \#\mathbb{G}_1 = \#\mathbb{G}_2$  is 256-bits, while the extension field must be  $k \log p \approx 2530$ , when  $k$  is prime and  $k \log p \approx 4352$ , when  $k$  is composite. The best examples in this case are achieved by the pairs  $(k, \rho) = (7, 1.5)$  and  $(10, 1.75)$ . In the first case the extension field  $\mathbb{F}_{p^k}$  is 2688-bits, while in the second case, it is 4480-bits. The rest of the examples produce a slightly larger extension field, but still close to the optimal balance. We describe how the first CVD family of Table 9 is obtained in the following example.

**Example 8.** We set the number field  $K = \mathbb{Q}(\zeta_{14})$ . Hence the polynomial  $r(x)$  is the  $l$ th cyclotomic polynomial:

$$r(x) = \Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 \quad \text{with} \quad \text{deg } r = 6$$

and  $u(x) = x$  is a primitive 14th root of unity in  $\mathbb{Q}[x]/\langle r(x) \rangle$ . By Equations (6), we set  $z(x) = x^4$  so that

$$z(x)^2 = x^8 \equiv -x \pmod{r(x)} \implies z(x) \equiv \sqrt{-x} \pmod{r(x)}.$$

For  $i = 8$  in Algorithm 4 we obtain:

$$t(x) \equiv (-x + 1) \pmod{r(x)} \quad \text{and} \quad y(x) \equiv (x^4 + x^3) \pmod{r(x)}.$$

Since  $\text{gcd}(i, l) = 2$ , we get that  $k = 7$ , by step (4) of Algorithm 4. For the field polynomial  $p(x)$  we use the relation:

$$p(x) = \frac{1}{4} [t(x)^2 + xy(x)^2] = \frac{1}{4} (x^9 + 2x^8 + x^7 + x^2 - 2x + 1)$$

**Table 10**  
Cyclotomic CVD families at 128-bit security level with lifts  $t_1, y_1 \in \mathbb{Q}$  and  $\rho = 2$ .

| $k$ | $l$ | $\text{deg } r$ | $i$ | $t_1$ | $y_1$ | $x_0$   | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|-----------------|-----|-------|-------|---------|------------|--------------------|
| 5   | 10  | 4               | 6   | 1     | 0     | 0 mod 2 | 2560       | 128                |
| 9   | 18  | 6               | 4   | 1     | 0     | 0 mod 2 | 4608       | 130                |

**Table 11**  
Cyclotomic CVD families at 192-bit security level.

| $k$ | $l$ | $\text{deg } r$ | $i$ | $\rho(p, t, r)$ | $x_0$   | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|-----------------|-----|-----------------|---------|------------|--------------------|
| 11  | 22  | 10              | 2   | 1.5000          | 1 mod 2 | 6336       | 188                |
| 11  | 22  | 10              | 8   | 1.6000          | 1 mod 2 | 6758       | 193                |
| 11  | 22  | 10              | 14  | 1.7000          | 1 mod 2 | 7181       | 197                |
| 13  | 26  | 12              | 2   | 1.4167          | 1 mod 2 | 7072       | 196                |
| 13  | 26  | 12              | 8   | 1.3333          | 1 mod 2 | 6656       | 191                |
| 18  | 18  | 6               | 5   | 1.6667          | 1 mod 2 | 11520      | 190                |
| 22  | 22  | 10              | 1   | 1.3000          | 1 mod 2 | 10982      | 187                |
| 22  | 22  | 10              | 7   | 1.4000          | 1 mod 2 | 11827      | 192                |
| 22  | 22  | 10              | 13  | 1.5000          | 1 mod 2 | 12672      | 198                |
| 25  | 50  | 20              | 26  | 1.3500          | 1 mod 2 | 12960      | 200                |
| 26  | 26  | 12              | 7   | 1.1667          | 1 mod 2 | 11648      | 191                |

**Table 12**  
Cyclotomic CVD families at 192-bit security level with lifts  $t_1, y_1 \in \mathbb{Q}$  and  $\rho = 2$ .

| $k$ | $l$ | $\text{deg } r$ | $i$ | $t_1$ | $y_1$ | $x_0$   | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|-----------------|-----|-------|-------|---------|------------|--------------------|
| 15  | 30  | 8               | 4   | 3     | 0     | 0 mod 2 | 11520      | 190                |

and it is integer valued for every integer  $x \equiv 1 \pmod 2$ . We then conclude that the polynomial triple  $(p(x), t(x), r(x))$  represents a CVD polynomial family of pairing-friendly elliptic curves with embedding degree  $k = 7$  and  $\rho$ -value:

$$\rho(p, t, r) = \frac{\text{deg } p}{\text{deg } r} = \frac{3}{2} = 1.5000.$$

All examples in Table 9, as well as all examples in the tables to follow are obtained in an analogous way.  $\square$

As we did in Section 3, we also introduce several CVD families with  $\rho(p, t, r) = 2$ . Such families can be obtained by applying Algorithm 4 and considering constant lifts  $t_1, y_1 \in \mathbb{Q}$  for the polynomials  $t(x)$  and  $y(x)$ . CVD families with this  $\rho$ -value have not considered before, however we argue that they are likely to offer a nicely balanced security level in the three pairing groups. We give two such examples in Table 10 for embedding degrees 5 and 9, which produce an extension field  $\mathbb{F}_{p^k}$  of 2560-bits in the first case and 4608-bits in the second case. Although  $\rho = 2$  in these families, the corresponding extension fields are not so large that we cannot handle. Both in complete and CVD families we see that the potentially ideal families are limited when working at an 128-bit security level. However, each family is likely to produce a large number of pairing-friendly elliptic curves, when evaluated at appropriate integers. More families can be found when working at higher security levels, such as 192 or 256-bits as we will see in the next paragraphs.

#### 4.1.2. 192-bit security level

Our examples for the case of CVD families that produce an optimal security level in the three pairing groups  $\mathbb{G}_1, \mathbb{G}_2$  and  $\mathbb{G}_T$  are listed in Table 11. For an 192-bit security level recall that the prime  $r$  has a size of 384-bits and the extension field  $\mathbb{F}_{p^k}$  should be around 6670-bits for prime embedding degrees and 11670-bits for composite values of  $k$ , in order for the DLP to be resistant against TNFS attacks. The best balance in the prime case is obtained by the pairs  $(k, \rho) = (11, 1.6)$  and  $(13, 1.3333)$  and for the composite case by the pairs  $(k, \rho) = (22, 1.4)$  and  $(26, 1.1667)$ . The remaining examples in Table 11 also achieve a security level in the extension field close to 192 bits. We also introduce an example for  $k = 15$  with  $\rho(p, t, r) = 2$ , which is obtained by taking constant lifts  $t_1, y_1 \in \mathbb{Q}$  for the polynomials  $t(x)$  and  $y(x)$ . The extension field  $\mathbb{F}_{p^k}$  in this case has size around 11520-bits, providing a security level of 190-bits (see Table 12).

#### 4.1.3. 256-bit security level

For a 256-bit security level, the prime  $r$  must be 512-bit large and the extension field must be 13500-bits for prime and 23780-bits for composite embedding degrees. The best possible balance for the security level in the three pairing groups is obtained by the pairs  $(k, \rho) = (17, 1.5625)$ ,  $(19, 1.3889)$  and  $(23, 1.1364)$  in the prime case. For composite embedding degrees we have an optimal balance by the pairs  $(k, \rho) = (25, 1.8500)$ ,  $(27, 1.7222)$ ,  $(34, 1.3750)$  and  $(38, 1.2222)$ . The rest of the examples in Table 13 also achieve a security level around 256-bits. It is also possible to get a nicely balanced security level by considering the family of Table 14, for  $k = 13$ , with  $\rho(p, t, r) = 2$ .

**Table 13**  
Cyclotomic CVD families at 256-bit security level.

| $k$ | $l$ | $\text{deg } r$ | $i$ | $\rho(p, t, r)$ | $x_0$   | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|-----------------|-----|-----------------|---------|------------|--------------------|
| 17  | 34  | 16              | 4   | 1.5625          | 1 mod 2 | 13600      | 256                |
| 17  | 34  | 16              | 12  | 1.5000          | 1 mod 2 | 13056      | 252                |
| 19  | 38  | 18              | 12  | 1.3333          | 1 mod 2 | 12971      | 252                |
| 19  | 38  | 18              | 22  | 1.3889          | 1 mod 2 | 13511      | 256                |
| 23  | 46  | 22              | 24  | 1.1364          | 1 mod 2 | 13382      | 255                |
| 25  | 50  | 24              | 6   | 1.8500          | 1 mod 2 | 23680      | 255                |
| 26  | 26  | 12              | 11  | 1.8333          | 1 mod 2 | 24405      | 258                |
| 26  | 26  | 12              | 17  | 1.7500          | 1 mod 2 | 23296      | 253                |
| 27  | 54  | 18              | 2   | 1.7222          | 1 mod 2 | 23808      | 255                |
| 27  | 54  | 18              | 16  | 1.7778          | 1 mod 2 | 24576      | 258                |
| 34  | 34  | 16              | 11  | 1.3750          | 1 mod 2 | 23936      | 256                |
| 38  | 38  | 18              | 11  | 1.2222          | 1 mod 2 | 23780      | 255                |
| 38  | 38  | 18              | 21  | 1.2778          | 1 mod 2 | 24860      | 260                |

**Table 14**  
Cyclotomic CVD families at 256-bit security level with lifts  $t_1, y_1 \in \mathbb{Q}$  and  $\rho = 2$ .

| $k$ | $l$ | $\text{deg } r$ | $i$ | $t_1$ | $y_1$ | $x_0$   | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|-----------------|-----|-------|-------|---------|------------|--------------------|
| 13  | 26  | 12              | 2   | 3     | 0     | 0 mod 2 | 13312      | 254                |

**Table 15**  
Non-cyclotomic CVD families at 128, 192 and 256-bit security.

| $k$ | $l$ | $r(x)$          | $\text{deg } r$ | $t(x)$        | $z(x)$   | $\rho(p, t, r)$ | $x_0$   | $k \log p$ | $L_{p^k}[\ell, c]$ |
|-----|-----|-----------------|-----------------|---------------|--|-----------------|---------|------------|--------------------|
| 12  | 12  | $\Phi_{12}(2x)$ | 4               | $2x + 1$      | $4x^3 + 2x^2 - x$                                      | 1.7500          | 3 mod 4 | 5376       | 139                |
| 14  | 28  | $\Phi_{28}(2x)$ | 12              | $(2x)^2 + 1$  | $1024x^{11} + 8x^4$                                    | 1.4167          | 3 mod 4 | 5077       | 136                |
| 28  | 28  | $\Phi_{28}(2x)$ | 12              | $-(2x)^9 + 1$ | $1024x^{11} + 8x^4$                                    | 1.7500          | 3 mod 4 | 25088      | 261                |
| 30  | 30  | $\Phi_{30}(5x)$ | 8               | $-(5x)^2 + 1$ | $(5x)^7 + 2(5x)^6 + (5x)^5 - (5x)^4 - (5x)^3 - 5x + 1$ | 1.6250          | 1 mod 2 | 24960      | 260                |

4.1.4. Non-cyclotomic families

An alternative approach is to choose the polynomial  $r(x)$  to be a non-cyclotomic polynomial, satisfying condition (2) of Definition 1, in which case we construct non-cyclotomic CVD families. This setup allows us to obtain examples of families for embedding degrees that we could not find using the cyclotomic setup of Equation (6). As stated when we were discussing complete families, it is sometimes hard to determine a primitive  $k$ th root of unity in  $\mathbb{Q}[x]/\langle r(x) \rangle$ . In general, what we have to do is to find a polynomial  $u(x) \in \mathbb{Q}[x]$ , such that  $\Phi_k(u(x)) = 0 \pmod{r(x)}$ . Methods that produce such polynomials  $r(x)$  and  $u(x)$  can be found in [6,10,12,13,16]. In addition, for CVD families it is also hard to find a polynomial  $z(x) \equiv \sqrt{-x} \pmod{r(x)}$ . A general procedure to do this, is to set  $z(x) \in \mathbb{Q}[x]/\langle r(x) \rangle$  to be of the form:

$$z(x) = z_{\text{deg } r} x^{\text{deg } r} + z_{\text{deg } r - 1} x^{\text{deg } r - 1} + \dots + z_1 x + z_0$$

and then search for coefficients  $z_i$ , such that  $z(x)^2 \equiv -x \pmod{r(x)}$ , via an exhaustive search. Clearly this is a very time consuming process, especially when the degree of the polynomial  $r(x)$  is large (e.g.  $\text{deg } r > 4$ ).

One trick to avoid the above process is to set  $r(x) = \Phi_l(ax)$  and  $u(x) = ax$ , for some  $a \in \mathbb{Z}$  and some  $l \in \mathbb{Z}_{>0}$ , such that  $k \mid l$ , but still we need to determine a suitable polynomial  $z(x)$ . Such examples are given in Table 15. The family for  $k = 30$  was first introduced in [3]. For  $k = 28$ , Dryło presented a CVD family for the same  $r(x)$  as in Table 15, but with  $\rho(p, t, r) = 1.5$ . For a 512-bit prime, this family produces an extension field of size 21504-bits, which is more than 2000-bits smaller than the optimal size for a 256-bit security level. Using Dryło’s setup, we introduce a CVD family with  $k = 28$  and  $\rho(p, t, r) = 1.75$ . With this choice we obtain extension fields of size 25088-bits, which corresponds to a security level of 261-bits according to the new TNFS attacks for composite embedding degrees. Furthermore, with this setup we also constructed a family with  $k = 14$  and  $\rho(p, t, r) = 1.4167$ , which could not be obtained by the cyclotomic setup of Equations (6).

In [3], Dryło presented a non-cyclotomic CVD family with embedding degree 8 and  $\rho(p, t, r) = 1.5$ . This family produces an extension field of 3072-bits, when  $\log r = 256$ , which might have been optimal before the improvements of the TNFS method for composite  $k$ . Today, such extension fields reach a security level of 110-bits. Using Dryło’s polynomials  $r(x)$  and  $u(x)$ , we present our recommendation of a CVD family for  $k = 8$  and  $\rho(p, t, r) = 2$ , in the following example.

**Example 9.** For  $l = k = 8$  we take Dryło’s polynomials [3]:

$$u(x) = \frac{1}{12}(-x^3 + 5x^2 - 16x + 2), \quad r(x) = x^4 - 4x^3 + 8x^2 + 8x + 4, \quad z(x) = \frac{1}{4}(-x^2 + 2x - 2),$$



**Table 16**  
Numerical examples of pairing-friendly parameters from selected CVD families.

| Source    | $k$ | $D$     | $x_0$                                   | $n$ | $\log r$ | $k \log p$ | $\rho$ | $L_{p^k}[1/3, c]$ |
|-----------|-----|---------|---|-----|----------|------------|--------|-------------------|
| Table 10  | 5   | 8871207 | $D \cdot 1511472^2 \equiv 0 \pmod 2$    | 1   | 256      | 2555       | 1.9961 | 128               |
| Table 9   | 7   | 9160269 | $D \cdot 903^2 \equiv 1 \pmod 2$        | 1   | 256      | 2674       | 1.4922 | 131               |
| Example 9 | 8   | 814127  | $D \cdot 6727283^2 \equiv 23 \pmod{24}$ | 9   | 256      | 4136       | 2.0195 | 125               |
| Table 9   | 9   | 908587  | $D \cdot 2903^2 \equiv 1 \pmod 2$       | 1   | 256      | 4212       | 1.8281 | 126               |
| Table 10  | 9   | 4330077 | $D \cdot 1302^2 \equiv 0 \pmod 2$       | 1   | 256      | 4590       | 1.9922 | 130               |
| Table 9   | 10  | 3281749 | $D \cdot 2575675^2 \equiv 1 \pmod 2$    | 1   | 256      | 4470       | 1.7461 | 129               |
| Table 15  | 12  | 4725179 | $D \cdot 1517443^2 \equiv 3 \pmod 4$    | 1   | 256      | 5352       | 1.7422 | 139               |
| Table 15  | 14  | 1350211 | $D \equiv 3 \pmod 4$                    | 1   | 256      | 5040       | 1.4063 | 135               |
| Table 11  | 11  | 1040779 | $D \cdot 611^2 \equiv 1 \pmod 2$        | 1   | 384      | 6743       | 1.5964 | 192               |
| Table 11  | 13  | 179     | $D \cdot 4959^2 \equiv 1 \pmod 2$       | 1   | 384      | 6630       | 1.3281 | 191               |
| Table 12  | 15  | 876018  | $D \cdot 18341^2 \equiv 0 \pmod 2$      | 1   | 384      | 11550      | 2.0052 | 190               |
| Table 12  | 18  | 2331871 | $D \cdot 2949767^2 \equiv 1 \pmod 2$    | 1   | 384      | 11502      | 1.6641 | 190               |
| Table 12  | 22  | 87847   | $D \cdot 2051^2 \equiv 1 \pmod 2$       | 1   | 384      | 11770      | 1.3932 | 192               |
| Table 12  | 25  | 87847   | $D \equiv 1 \pmod 2$                    | 1   | 384      | 12925      | 1.3464 | 199               |
| Table 12  | 26  | 8281427 | $D \cdot 23^2 \equiv 1 \pmod 2$         | 1   | 384      | 11596      | 1.1615 | 191               |
| Table 14  | 13  | 5013326 | $D \cdot 1203^2 \equiv 0 \pmod 2$       | 1   | 512      | 13338      | 2.0039 | 254               |
| Table 13  | 17  | 1971089 | $D \cdot 47^2 \equiv 1 \pmod 2$         | 1   | 512      | 13566      | 1.5586 | 256               |
| Table 13  | 19  | 2166897 | $D \cdot 13^2 \equiv 1 \pmod 2$         | 1   | 512      | 13471      | 1.3848 | 255               |
| Table 13  | 23  | 16403   | $D \cdot 25^2 \equiv 1 \pmod 2$         | 1   | 512      | 13340      | 1.1328 | 254               |
| Table 13  | 25  | 307795  | $D \cdot 13^2 \equiv 1 \pmod 2$         | 1   | 512      | 23650      | 1.8477 | 254               |
| Table 13  | 26  | 2385911 | $D \cdot 1735^2 \equiv 1 \pmod 2$       | 1   | 512      | 24362      | 1.8301 | 258               |
| Table 13  | 27  | 2703    | $D \cdot 371^2 \equiv 1 \pmod 2$        | 1   | 512      | 23760      | 1.7188 | 255               |
| Table 15  | 28  | 2143411 | $D \cdot 1291^2 \equiv 1 \pmod 2$       | 1   | 512      | 25060      | 1.7480 | 260               |
| Table 15  | 30  | 4895545 | $D \cdot 902873^2 \equiv 1 \pmod 2$     | 1   | 512      | 24870      | 1.6191 | 259               |
| Table 13  | 34  | 3628579 | $D \cdot 35^2 \equiv 1 \pmod 2$         | 1   | 512      | 23902      | 1.3730 | 255               |
| Table 13  | 38  | 2193243 | $D \cdot 13^2 \equiv 1 \pmod 2$         | 1   | 512      | 23712      | 1.2188 | 254               |

so that  $z(x)^2 \equiv -x \pmod{r(x)}$ . Set:

$$t(x) = -r(x) + u(x), \quad y(x) \equiv [(u(x) - 1)z(x)^{-1}] \pmod{r(x)}, \quad 4q(x) = t(x)^2 + xy(x)^2.$$

We obtain a CVD family with embedding degree 8 and  $\rho(q, t, r) = 2$ , which is integer-valued when  $x \equiv 23 \pmod{24}$ .  $\square$

In Example 9 we actually take a lift  $t_1 = -1$  for the trace polynomial  $t(x)$ , so that the resulting field polynomial has  $\deg p = 2 \deg r$ . With this CVD family, the extension fields  $\mathbb{F}_{p^8}$  have size around 4096-bits resulting in an 124-bit security level. These are just a few examples of non-cyclotomic CVD families, but we argue that a lot more can be found by choosing the right polynomials  $r(x), u(x)$  and  $z(x)$ .

#### 4.2. Numerical examples

We give our numerical examples obtained by the CVD families of this section in Table 16, for 128, 192 and 256-bit security level. The parameters we constructed are generated by applying Algorithm 5. The column “ $x_0$ ” refers to the integer input for the polynomials  $p(x), t(x)$  and  $r(x)$ . Recall that an additional constraint in the case of CVD families is that the integer  $x_0$  must be of the form  $x_0 = Dy^2$ , for some relatively small, positive and square-free  $D$  and some  $y \in \mathbb{Z}$ . This  $D$ , hidden in  $x_0$  is the CM discriminant and by relatively small, we mean  $D < 10^{10}$  in order to ensure the efficiency of the CM method for constructing elliptic curves. The column “ $n$ ” refers to the relaxed condition that  $r(x_0)$  might contain a small cofactor  $n$ , which increases the probability of finding pairing-friendly elliptic curve triples. In this case we set the prime  $r = r(x_0)/n$ . In the final column, we calculate the complexity of the DLP in the extension field  $\mathbb{F}_{p^k}$ , using Equation (1), for  $\ell = 1/3$  and ignoring the constant  $o(1)$ . For prime  $k$  we set  $c = 1.923$  and for composite  $k$ , we set  $c = 1.526$ , according to the new variants of the TNFS attacks [9,11,4].

For example we demonstrate how the values in Table 16 are obtained, by explaining the first line. Recall the CVD family  $(p(x), t(x), r(x))$  with embedding degree 5 and  $\rho(p, t, r) = 2$ , presented in Table 10. We evaluate this family at

$$x_0 = 8871207 \cdot 1511472^2 \equiv 0 \pmod 2,$$

thus the CM discriminant is  $D = 8871207$  and  $y = 1511472$ . The corresponding polynomials extract the following values:

$$r(x_0) = 16870645622941276613526765048486665176998090384315424123446880583$$

$$6830177009921$$

**Table 17**  
Recommended complete and CVD families at an 128, 192 and 256-bit security level.

| Security level: 128-bits |        |            | Security level: 192-bits |        |            | Security level: 256-bits |        |            |
|--------------------------|--------|------------|--------------------------|--------|------------|--------------------------|--------|------------|
| $k$                      | $\rho$ | $k \log p$ | $k$                      | $\rho$ | $k \log p$ | $k$                      | $\rho$ | $k \log p$ |
| 5                        | 2.0000 | 2560       | 11                       | 1.6000 | 6758       | 13                       | 2.0000 | 13312      |
| 7                        | 1.5000 | 2688       | 13                       | 1.3333 | 6656       | 17                       | 1.5625 | 13600      |
| 8                        | 2.0000 | 4096       | 15                       | 2.0000 | 11520      | 19                       | 1.3889 | 13511      |
| 9                        | 2.0000 | 4608       | 18                       | 1.6667 | 11520      | 24                       | 2.0000 | 24576      |
| 10                       | 1.7500 | 4480       | 21                       | 1.5000 | 12096      | 25                       | 1.8500 | 23680      |
| 12                       | 1.5000 | 4608       | 22                       | 1.4000 | 11827      | 26                       | 1.8333 | 24405      |
| 14                       | 1.4167 | 5077       | 24                       | 1.2500 | 11520      | 27                       | 1.7222 | 23808      |
|                          |        |            | 26                       | 1.1667 | 11648      | 28                       | 1.7500 | 25088      |
|                          |        |            |                          |        | 30         | 1.6250                   | 24960  |            |
|                          |        |            |                          |        | 33         | 1.4000                   | 23654  |            |
|                          |        |            |                          |        | 34         | 1.3750                   | 23936  |            |
|                          |        |            |                          |        | 38         | 1.2222                   | 23780  |            |
|                          |        |            |                          |        | 39         | 1.2500                   | 24960  |            |

$$p(x_0) = 71154670933716913814275569191462866732338754674253388144787542905 \\ 65870927012305049095317570533504848265231612212043863267520197109 \\ 556649950433990502597121$$

$$t(x_0) = 16870645622941276613526765048486665176998090384315424123444853914 \\ 2109041541634$$

with  $\rho = 1.9961$ . The prime  $r$  is 256-bits and the extension field  $\mathbb{F}_{p^5}$  is 2555-bits corresponding to 128-bit security level, according to Equation (1), for  $\ell = 1/3$  and  $c = 1.923$ . The rest of the examples in Table 16 are obtained in the same way.

Recall that the search for suitable integers  $x_0$  is affected by the degree of the polynomial  $r(x)$  and by the size of its leading coefficient, where in the case of CVD families,  $x_0 = Dy^2$ . In the examples of Table 16 we have considered CM discriminants  $D < 10^7$ , however we could also allow it to be slightly larger. Our search is then performed by a random choice of  $D$  up to  $10^7$  and a random choice of  $y \in \mathbb{Z}$ , such that

$$\text{deg } r(\log D + 2 \log y) + \log(\text{lc}(r)) \approx \text{security level}, \quad (7)$$

where  $\text{lc}(r)$  is the leading coefficient of  $r(x)$  (note that  $\text{lc}(r) = 0$ , when  $r(x) = \Phi_l(x)$ ). Then we set  $x_0 = Dy^2$ . In some case, in order to reach a desired security level, we need  $y = 1$ , so that  $x_0 = D$ . This happens when the degree of the polynomial  $r(x)$  is large. For CVD families at an 128-bit security level we have considered polynomials  $r(x)$  with  $\text{deg } r \leq 10$ , for 192-bit security level we have  $\text{deg } r \leq 20$  and for 256-bit security level,  $\text{deg } r \leq 24$ .

**Remark 10.** As stated earlier in this section, a useful advantage of CVD families is that they allow us to obtain more flexible CM discriminants than the case of complete families, where  $D$  is fixed and relatively small. Throughout the tables in Sections 3 and 4, we see that for many embedding degrees, complete and CVD families have the same  $\rho$ -value. The advantage of the CVD families we presented is that the degree of the polynomial  $r(x)$  is half the degree of the corresponding polynomial  $r(x)$  for complete families. This allows us to better handle the sizes of the extracted elliptic curve parameters.  $\square$

## 5. Conclusion

Since the recent improvements on variants of the TNFS methods [9,11,4] there has been much speculation on whether pairings can be indeed used for robust cryptographic applications. Especially for extension fields of composite degree these TNFS attacks have a major effect causing the necessity to update the criteria for selecting elliptic curve parameters of composite embedding degree for pairing-based implementations.

Motivated by this necessity, we presented a survey of families of pairing-friendly elliptic curves with composite embedding degrees, which are likely to generate elliptic curve parameters resistant to the improved TNFS attacks. As stated throughout this paper, our main concern is not to search for families with the smallest  $\rho$ -values, but for families that produce an equally balanced security level in the three pairing groups  $\mathbb{G}_1, \mathbb{G}_2 \subseteq E(\mathbb{F}_{p^k})$  and  $\mathbb{G}_T \subseteq \mathbb{F}_{p^k}^*$ . Therefore, we also introduce families with prime embedding degrees, which have not been considered before due to a larger  $\rho$ -value. Additionally, in this paper we are studying to types of polynomial families. These are complete families (see Section 3), where the CM discriminant is a constant square-free positive value  $D$  and complete with variable discriminant (see Section 4), where the CM discriminant is represented by a linear term  $x$ . We argue that all proposed families are suitable for producing a balanced security level of 128, 192 and 256-bits in the three pairing groups. Our recommendations are summarized in Table 17.

The three columns correspond to the three security levels of 128, 192 and 256-bits. In each column we record the embedding degree  $k$  and the  $\rho$ -value  $\rho(p, t, r)$  achieved by a complete or CVD family (or both) presented in Sections 3 and 4. For each family we calculate the extension field size by  $k \log p$ , where  $\log p = \rho \log r$  and  $\log r$  is twice the security level. We can then calculate the asymptotic complexity of the DLP in the extension field  $\mathbb{F}_{p^k}$ , by Equation (1), i.e.  $L_{p^k}[1/3, c]$ , where  $c = 1.923$  when  $k$  is prime and  $c = 1.526$  when  $k$  is composite. Particularly in Table 17, we present the families (complete or CVD) that produce the closest balance in the three pairing groups.

### Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

### References

- [1] P.S.L.M. Barreto, M. Naehrig, Pairing-friendly elliptic curves of prime order, in: International Workshop on Selected Areas in Cryptography–SAC'05, Springer, Berlin, Heidelberg, 2005, pp. 319–331.
- [2] F. Brezing, A. Weng, Elliptic curves suitable for pairing based cryptography, *Des. Codes Cryptogr.* 37 (1) (2005) 133–141.
- [3] R. Drylo, On constructing families of pairing-friendly elliptic curves with variable discriminant, in: International Conference on Cryptology in India–INDOCRYPT'11, Springer, Berlin, Heidelberg, 2011, pp. 310–319.
- [4] N. El Mrabet, M. Joye, *Guide to Pairing-Based Cryptography*, CRC Press, 2017.
- [5] G. Fotiadis, E. Konstantinou, On the efficient generation of generalized MNT elliptic curves, in: T. Muntean, D. Poulakis, R. Rolland (Eds.), International Conference on Algebraic Informatics–CAI'13, Springer, Berlin, Heidelberg, 2013, pp. 147–159.
- [6] G. Fotiadis, E. Konstantinou, More sparse families of pairing-friendly elliptic curves, in: International Conference on Cryptology and Network Security–CANS'14, Springer International Publishing, 2014, pp. 384–399.
- [7] D. Freeman, Constructing pairing-friendly elliptic curves with embedding degree 10, in: F. Hess, S. Pauli, M. Pohst (Eds.), International Algorithmic Number Theory Symposium–ANTS-VII'06, Springer, Berlin, Heidelberg, 2006, pp. 452–465.
- [8] D. Freeman, M. Scott, E. Teske, A taxonomy of pairing-friendly elliptic curves, *J. Cryptol.* 23 (2) (2010) 224–280.
- [9] J. Jeong, T. Kim, Extended Tower Number Field Sieve With Application to Finite Fields of Arbitrary Composite Extension Degree, 2016, IACR Cryptology ePrint Archive.
- [10] E.J. Kachisa, E.F. Schaefer, M. Scott, Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field, in: International Conference on Pairing-Based Cryptography–Pairing'08, Springer, Berlin, Heidelberg, 2008, pp. 126–135.
- [11] T. Kim, R. Barbulescu, Extended tower number field sieve: a new complexity for the medium prime case, in: Advances in Cryptology–CRYPTO'16, Springer, Berlin, Heidelberg, 2016, pp. 543–571.
- [12] H.-S. Lee, C.-M. Park, Generating pairing-friendly curves with the CM equation of degree 1, in: International Conference on Pairing-Based Cryptography–Pairing'09, Springer, Berlin, Heidelberg, 2009, pp. 66–77.
- [13] H.-S. Lee, C.-M. Park, Constructing pairing-friendly curves with variable CM discriminant, *Bull. Korean Math. Soc.* 49 (1) (2012) 75–88.
- [14] A. Miyaji, M. Nakabayashi, S. Takano, New explicit conditions of elliptic curve traces for FR-reduction, *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* 84 (5) (2001) 1234–1243.
- [15] A. Murphy, N. Fitzpatrick, *Elliptic Curves for Pairing Applications*, IACR Cryptology ePrint Archive, Citeseer, 2005, pp. 1–15.
- [16] S. Tanaka, K. Nakamura, Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials, in: International Conference on Pairing-Based Cryptography–Pairing'08, Springer, Berlin, Heidelberg, 2008, pp. 136–145.