Pairing-Friendly Elliptic Curves Resistant to TNFS Attacks [⋆]

Georgios Fotiadis and Elisavet Konstantinou

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

Abstract. The recent progress on the tower number field sieve (TNFS) method reduce the complexity of the discrete logarithm problem (DLP) in finite extensions $\mathbb{F}_{q^k}$ of composite degree and this has a major impact on the selection of pairing-friendly elliptic curve parameters. In this paper we revise the criteria for selecting pairing-friendly elliptic curves in order to surpass the TNFS attacks in finite extensions of composite embedding degree. We also update the criteria for selecting suitable elliptic curves of prime embedding degree in order to meet today's security requirements.

Keywords: Pairings, elliptic curves, pairing-friendly parameters, embedding degree, TNFS attacks.

1 Introduction

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve over a prime field $\mathbb{F}_q$, with Frobenius trace $t = q+1-\#E(\mathbb{F}_q)$, where $E(\mathbb{F}_q)$ is the group of $\mathbb{F}_q$-rational points for which $\#E(\mathbb{F}_q) \approx q$. Let $E[r]$ be the group of r-torsion points on $E/\mathbb{F}_q$, for some $r \in \mathbb{Z}_{>0}$, i.e. all points on the curve whose order is finite and equal to r. By $D > 0$ we denote the *CM discriminant* of the elliptic curve $E/\mathbb{F}_q$. This is the square-free integer satisfying the *CM equation* $Dy^2 = 4q - t^2$, for some $y \in \mathbb{Z}$.

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

1. The order of $E/\mathbb{F}_q$ is $\#E(\mathbb{F}_q) = hr$, for some small cofactor $h \geq 1$ and a large prime r.
2. The ρ-value defined as $\rho = \log q / \log r$ must be close to 1, so that $\log r \approx \log q$.
3. The prime r must be large enough, so that the DLP in $\mathbb{G}_1, \mathbb{G}_2$ is computationally hard.
4. The embedding degree k must be large enough, so that the DLP in the extension field $\mathbb{F}_{q^k}$ (and hence in $\mathbb{G}_\mathrm{T}$) is approximately as hard as in $\mathbb{G}_1, \mathbb{G}_2$.
5. The embedding degree k must be small enough for efficient operations in $\mathbb{G}_\mathrm{T}$.
6. The sizes of r and q^k should provide a security level of 128, 256, or 512 bits, corresponding to an AES key used for symmetric cryptography.

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

A survey of methods for constructing pairing-friendly elliptic curves can be found in [6]. However the smallest ρ-values are achieved by the Brezing-Weng method [2]. In this case the curve parameters q, t, r are represented as polynomial families $q(x), t(x), r(x) \in \mathbb{Q}[x]$ respectively (see Section 2 for the precise definition). Then pairing-friendly parameters are obtained by evaluating these polynomials

[⋆] Presented at the 7th International Conference on Algebraic Informatics – CAI'2017, in June 25-28, 2017 in Kalamata, Greece.

at some $x_0 \in \mathbb{Z}$, such that $q(x_0)$ and $r(x_0)$ are both primes and $4q(x_0) - t(x_0)^2 = Dy^2$, for some square-free $D > 0$ and some $y \in \mathbb{Z}$. Taking the above conditions into account, Freeman et al. [6] suggested that pairing-friendly parameters should be chosen as in Table 1.

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

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

The complexity of the DLP in $\mathbb{G}_1$, $\mathbb{G}_2$ is $O(\sqrt{r})$ and it is achieved by Pollard's rho algorithm. In practice this means that for a n bit symmetric key, we need a curve whose order contains a prime of size $2n$, i.e. twice the security level. On the other hand, the complexity of the DLP in a finite extension $\mathbb{F}_{q^k}$ depends on the choice of the embedding degree k and the characteristic of the extension field. In particular recall the usual L-notation given by the formula:

$$L_N\left[\ell, c\right] := \exp\left[(c + o(1))(\ln N)^{\ell}(\ln\ln N)^{1-\ell}\right], \quad \text{with } N = q^k, \tag{1.1}$$

for some real constants $\ell \in [0, 1]$ and $c > 0$. In general for a finite field extension, the NFS attack applies with complexity $L_N[1/3, 1.923]$. This complexity is still true for extensions of prime degree. When k is composite and q has a special form (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 (SexTNFS) algorithms [7, 9] 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. The most important consequence is that the extension field should be taken larger than before. This means that 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 (1.1), an extension field of this size reaches a security level of 110 bits. To achieve an extension field with 128 bit security level, one should choose q^{12} around 4608 bits. Since $\rho \approx 1$ in BN curves, this would result to $\log r \approx 384$ and hence a mismatch between the security level in $\mathbb{G}_1$, $\mathbb{G}_2$ and in $\mathbb{G}_{\mathrm{T}}$.

In this paper we revise the criteria for selecting polynomial families $(q(x), t(x), r(x))$ considering the impact of the TNFS variants. For composite embedding degrees we propose the use of families that are likely to produce a balanced security level between $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_{\mathrm{T}}$ 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 ρ-value. All families presented in this paper can provide a security level of 128, 256 and 512 bits. We produce numerical examples of cryptographic value obtained by our recommended families where the asymptotic complexity of the DLP in the finite extensions $\mathbb{F}_{q^k}$ is measured by using Equation (1.1) and ignoring the constant $o(1)$.

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 suggestions on the selection of 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. Finally, we conclude this paper in Section 5, summarizing our recommendations for selecting suitable pairing-friendly parameters.

2 Constructing Pairing-Friendly Elliptic Curves

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

Definition 1 (Freeman et al. [6]) A polynomial triple $(q(x), t(x), r(x))$ *parameterizes a family of pairing-friendly elliptic curves with embedding degree k and CM discriminant D* if:

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

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

The ρ-value of a polynomial family is defined as $\rho(q, t, r) = \deg q / \deg r$. Condition 3 of Definition 1 implies that the order of the curve has a polynomial representation $\#E(\mathbb{F}_{q(x)}) = h(x)r(x)$, where $h(x) \in \mathbb{Q}[x]$ is the cofactor and $t(x) - 1$ is a primitive k^{th} root of unity modulo $r(x)$. There are three types of families depending on the form of the polynomial $f(x) = 4q(x) - t(x)^2$.

Definition 2 (Dryło [3]) A polynomial family $(q(x), t(x), r(x))$ is:

1. *complete*, if $f(x) = Dy(x)^2$, 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 some linear $g(x) \in \mathbb{Q}[x]$,
3. *sparse*, if $g(x)$ is quadratic, non-square, with positive leading coefficient.

Examples of complete families can be found in [1, 2, 6, 8, 12, 13]. CVD families are studied in [3, 6, 10, 11] and finally, a few examples of sparse families are presented in [3, 5, 6]. In this paper we focus on complete and CVD polynomial families. This is because such families are easier to find and also the generation of pairing-friendly parameters is simpler than in the case of sparse families.

2.1 The Brezing-Weng Method

The most commonly used method for constructing pairing-friendly polynomial families is due to Brezing and Weng [2]. This method was initially applied for complete families and was later modified by Dryło [3], for the other two types of Definition 2. The number field K in Algorithm 1 is usually chosen as the l^{th} cyclotomic field $\mathbb{Q}(\zeta_l)$, for some $l > 0$, such that $k \mid l$ and $\sqrt{-D} \in \mathbb{Q}(\zeta_l)$. Then $r(x)$ is the l^{th} cyclotomic polynomial $\Phi_l(x)$ and thus $K \cong \mathbb{Q}[x]/\langle r(x) \rangle$. A more detailed description of the Brezing-Weng algorithm for complete families is given in Section 3.

In [3] (Algorithm 5, p. 312), Dryło generalized 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

Algorithm 1 The Brezing-Weng method [2].

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

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 term $g(x) = cx + d \in \mathbb{Q}[x]$. However, we can always apply the linear transformation $x \to (x - d)/c$ so that $g(x) = x$. We give a full analysis on how to construct CVD families via the Brezing and Weng method in Section 4. Sparse families can also be constructed by modifying the Brezing-Weng method (see [3]), however we do not consider this type of families here. For such examples we refer to [3, 5, 6]

In any case we need the polynomials $q(x), t(x)$ and $r(x)$ to be integer-valued. This condition can be tested by examining whether there exists a linear transformation $x \to (az + b)$ such that $q(az + b), t(az + b)$ and $r(az + b)$ have integer coefficients. When $(q(x), t(x), r(x))$ is a complete family, we can generate suitable pairing-friendly parameters by searching for some $x_0 \in \mathbb{Z}$, such that $q(x_0)$ and $r(x_0)$ are both primes of a desired size (see Section 3 for details). On the other hand, when $(q(x), t(x), r(x))$ 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 $q(x_0)$, $r(x_0)$ are both primes of a desired size (see Section 4 for the precise algorithm).

2.2 Our Contribution

Numerous examples can be found in the literature for both complete and CVD families of pairing-friendly elliptic curves. These examples were aiming for ρ-values as close to 1 as possible. However this condition may not be ideal any more for composite k, due to the improvements of the TNFS method [7, 9] for extension fields of composite degree. In this paper we present a revision of the criteria for selecting pairing-friendly polynomial families for prime and composite embedding degrees in the range $5 \leq k \leq 39$. More precisely, our contribution is summarized as follows.

1. **Composite k:** We propose complete and CVD families for various composite k that are suitable for generating parameters resistant to the TNFS attacks presented in [7, 9]. These families have larger ρ-values compared to previous results, in order to enlarge the extension field size $k \log q$ and hence increase the complexity of the DLP in $\mathbb{G}_{\mathrm{T}}$.
2. **Prime k:** We recommend complete and CVD families that have not been considered before due to a larger ρ-value than other families. We argue that our proposals are ideal for generating pairing-friendly parameters at a high and balanced security level in $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_{\mathrm{T}}$.
3. **Numerical Examples:** For each of the recommended families we provide numerical examples of pairing-friendly parameters achieving a security level of 128, 256, or 512 bits. For extension fields of composite embedding degree we give an asymptotic complexity of $L_N[1/3, 1.526]$ group operations achieved by the SexTNFS method. Since the TNFS variants do not apply for prime degree extension fields, we generated parameters by following Table 1. Then the complexity of the DLP in $\mathbb{F}_{q^k}$ is computed by $L_N[1/3, 1.923]$, where $N = q^k$.

We argue that at present, finding families with the smallest ρ-value is not the main concern. The families we use must have ρ-values such that the DLP in the extension field is resistant to various NFS attacks and approximately as hard as in the r-order subgroups $\mathbb{G}_1, \mathbb{G}_2$ of $E(\mathbb{F}_q)$. To this end our recommendations consist of families of pairing-friendly elliptic curves with $\rho(q,t,r) \leq 2$.

3 Complete Families Revised

We give a more detailed description of the Brezing-Weng algorithm for constructing complete families of pairing-friendly elliptic curves. By the discussion in Section 2, in order to apply the Brezing-Weng method, we need to fix a number field K containing the primitive k^{th} roots of unity, for some $k > 0$ and the element $\sqrt{-D}$, for some square-free positive CM discriminant. By [12] 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 embedding degree k and a CM discriminant D we can fix the number field K as $\mathbb{Q}(\zeta_l)$, where $l = \operatorname{lcm}(k,m)$. In this case we can set $r(x) = \Phi_l(x)$, where $\deg r = \varphi(l)$. In our examples we have considered only cases where $r(x) = \Phi_l(x)$. However the polynomial $r(x)$ can be chosen as any irreducible polynomial with positive leading coefficient (see for example [1, 8, 13]). We get the modified Brezing-Weng method presented in Algorithm 2. The complete families obtained by this algorithm have ρ-values less than 2 and particularly:

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

```
Input: An embedding degree $k$ and a square-free $D > 0$, such that $\sqrt{-D} \in \mathbb{Q}(\zeta_m)$, for some $m > 0$.
Output: A complete family with embedding degree $k$ and discriminant $D$.
Set $K = \mathbb{Q}(\zeta_l)$, where $l = \operatorname{lcm}(k,m)$ and $r(x) = \Phi_l(x)$, so that $K \cong \mathbb{Q}[x]/\langle r(x) \rangle$.
Let $u(x)$ and $z(x)$ be the polynomials mapping to $\zeta_l$ and $\sqrt{-D}$ respectively in $\mathbb{Q}[x]/\langle r(x) \rangle$.
For every $i = 1, ..., \varphi(l) - 1$, such that $l/\gcd(i,l) = k$ set:
    $t(x) \equiv \left[u(x)^i + 1\right] \bmod r(x), \quad y(x) \equiv \left[\left(u(x)^i - 1\right) z(x)^{-1}\right] \bmod r(x).$   (3.1)
Compute $q(x)$ by the relation $4q(x) = t(x)^2 + Dy(x)^2$.
If $q(x)$ represents primes, return $(q(x), t(x), r(x))$.
```

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

Remark 1 In Algorithm 2, $t(x)$ and $y(x)$ are taken in $\mathbb{Q}[x]/\langle r(x) \rangle$ and so $\deg t, \deg y \leq \varphi(l) - 1$. Alternatively, we can choose lifts of these polynomials in $\mathbb{Q}[x]$ (see [2, 3]). Then by Equation (3.1):

$$t(x) = \alpha(x) r(x) + \left[u(x)^i + 1\right] \bmod r(x), \quad y(x) = \beta(x) r(x) + \left[\left(u(x)^i - 1\right) z(x)^{-1}\right] \bmod r(x),$$

for some $\alpha(x), \beta(x) \in \mathbb{Q}[x]$. For example to achieve $\rho(q,t,r) = 2$ these lifts must be constant. □

The conditions for the element $\sqrt{-D}$ to lie in $\mathbb{Q}(\zeta_l)$ are given in the next lemma. This is taken from Murphy and Fitzpatrick [12].

Lemma 1 Let ζ_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:

- If $D \equiv 1 \bmod 4$, we have $\sqrt{D} \in \mathbb{Q}(\zeta_l)$ and $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\zeta_l)$.
- If $D \equiv 3 \bmod 4$, we have $\sqrt{-D} \in \mathbb{Q}(\zeta_l)$ and $\mathbb{Q}(\sqrt{-D}) \subset \mathbb{Q}(\zeta_l)$.

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 [12], Lemma 2.3. □

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

$$\prod_{i=1}^{(p-1)/2} \left(\zeta_p^i - \zeta_p^{-i}\right) = \begin{cases} \sqrt{p}, & \text{if} \quad p \equiv 1 \bmod 4 \\ \sqrt{-p}, & \text{if} \quad p \equiv 3 \bmod 4 \end{cases}$$

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

Algorithm 3 Finding suitable parameters using complete families.

```
Input: A complete family $(q(x), t(x), r(x))$ and a desired bit size $S_r$.
Output: A prime $q$, a (nearly) prime $r$ and a Frobenius trace $t$.
1: Find $a, b \in \mathbb{Z}$, so that $q(x) \in \mathbb{Z}$, for every $x \equiv b \bmod a$.
2: Search for $x_0 \equiv b \bmod a$, such that $r(x_0) = nr$, for some prime $r$ and $n \geq 1$.
3: Set $q = q(x_0)$, $r = r(x_0)/n$ and $t = t(x_0)$.
4: If $\log r \approx S_r$ and $q$ is prime, return $(q, t, r)$.
```

For every output of Algorithm 2, we need to make sure that the polynomials $q(x), t(x)$ and $r(x)$ have integer coefficients. If this is true, then there exist $a, b \in \mathbb{Z}$, such that $q(x) \in \mathbb{Z}$, for every $x \equiv b \bmod a$. In order to generate suitable elliptic curve parameters q, t and r, we are searching for some $x_0 \equiv b \bmod a$, such that $q(x_0)$ and $r(x_0)$ are both primes of a desired size. 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 also need to point out that the search for suitable parameters is affected by the degree of the polynomial $r(x)$ and as $\deg r$ grows it is harder to find suitable candidates x_0.

3.1 Examples for 128, 192 and 256 bit Security Level

In Tables 2–4 we present examples of complete families with $\rho(q, t, r) < 2$ produced by Algorithm 2 aiming at a security level of 128, 192 and 256 bits respectively. Recall that our basic concern is not to find the families with the smallest ρ-values. We are interested in families with ρ-values such that the DLP in r-order subgroups $\mathbb{G}_1, \mathbb{G}_2$ of $E(\mathbb{F}_q)$ and in the extension field $\mathbb{F}_{q^k}$ have approximately the same difficulty. Therefore we also introduce complete families with $\rho(q, t, r) = 2$ in Table 5. All complete families presented in this section derive from the following setup:

$$r(x) = \Phi_l(x), \quad u(x) = x, \quad t(x) \equiv \left[u(x)^i + 1\right] \bmod r(x),$$

for some $i = 1, \ldots, \varphi(l) - 1$, where $u(x)$ is a primitive l^{th} root of unity in $\mathbb{Q}[x]/\langle r(x)\rangle$. In the case where $\rho(q, t, r) = 2$ we are taking some constant lifts $\alpha(x), \beta(x) \in \mathbb{Q}$ for the polynomials $t(x)$ and $y(x)$ respectively. The asymptotic complexity of the DLP in the finite extension $\mathbb{F}_{q^k}$ is measured by the usual L-notation given in Equation (1.1). In particular, for prime embedding degree, the complexity of $\mathbb{F}_{q^k}$ is given by $L_{q^k}[1/3, 1.923]$, while when k is composite, according to the improvements of the TNFS method we have $L_{q^k}[1/3, 1.526]$.

In Table 2 we give our recommendations for complete families families that are likely to achieve an 128 bit security level in $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{F}_{q^k}$. In this case the prime r must be approximately 256 bit long. On the other hand the asymptotic complexity of the DLP in $\mathbb{F}_{q^k}$ implies that $k \log q \approx 2530$ when k is prime and $k \log q \approx 4352$ when k is composite. In Table 2 we observe that the best balance is achieved by the pairs $(k, \rho) = (10, 1.75)$ and $(12, 1.5)$. The remaining examples also achieve an acceptable balance but with a slightly larger extension field. Another optimal balance in the prime case can be achieved by families with $k = 5$ and $\rho(q, t, r) = 2$, where $5 \log q \approx 2550$. On the other hand, for the composite case, we can reach an extension field with 128 bit security level by choosing $k = 9$ and $\rho(q, t, r) = 2$, where $9 \log q \approx 4608$. For $k = 8$ the best ρ-values in the literature have $\rho(q, t, r) = 1.5$, which corresponds to extension fields of size approximately 3072 bits. We argue that the optimal case for $k = 8$ should be revised and use families with $\rho(q, t, r) = 2$. This will give us extension fields around 4096 bits. By Remark 1 we can construct complete families with $\rho(q, t, r) = 2$ by taking constant lifts of $t(x)$ and $y(x)$ in $\mathbb{Q}[x]$. Such examples appear in Table 5 for embedding degrees 5, 8, 9 and a security level of 128 bits.

Table 2. Complete families at 128 bit security level with $r(x) = \Phi_l(x)$ and $t(x) \equiv (x^i + 1) \bmod r(x)$.

k	l	D	i	$\rho(q,t,r)$	x_0	k	l	D	i	$\rho(q,t,r)$	x_0	k	l	D	i	$\rho(q,t,r)$	x_0
7	7	7	3	1.6667	$\{1,4\} \bmod 7$	10	30	15	3	1.7500	$\{1,3,6,13\} \bmod 15$	11	33	3	24	1.3000	$\{1,2\} \bmod 3$
	21	3	3	1.6667	$1 \bmod 3$		40	2	36	1.8750	$\{0,4\} \bmod 4$	12	12	3	1	1.5000	$1 \bmod 3$
10	20	5	18	1.7500	$\{0,4,6,10\} \bmod 10$	11	33	3	12	1.2000	$1 \bmod 3$		24	2	2	1.7500	$1 \bmod 2$

Recommendations of complete families for 192 bit security level are presented in Table 3. In this case the elliptic curve order must contain a prime r of size 384 bits. The prime embedding degree case corresponds to $k \log q \approx 6670$, while for composite k we have $k \log q \approx 11670$. The best balance for the first case is achieved by the entries $(k, \rho) = (11, 1.6)$ and $(13, 1.3333)$. For the composite case, the best balance is obtained by the pairs $(k, \rho) = (21, 1.5)$ and $(24, 1.25)$. For composite embedding degrees, we can also obtain a nice balance by considering complete families with $k = 15$ and $\rho(q, t, r) = 2$, where $15 \log q \approx 11520$. Additionally, one could also choose families with embedding degree 16 and $\rho(q, t, r) = 2$, where the extension field is $16 \log q \approx 12288$. Such examples are presented in Table 5 and require constant lifts of the polynomials $t(x)$ and $y(x)$.

Table 3. Complete families at 192 bit security level with $r(x) = \Phi_l(x)$ and $t(x) \equiv (x^i + 1) \bmod r(x)$.

k	l	D	i	$\rho(q,t,r)$	x_0	k	l	D	i	$\rho(q,t,r)$	x_0	k	l	D	i	$\rho(q,t,r)$	x_0
11	11	11	1	1.8000	$1 \bmod 11$	13	39	3	3	1.3333	$1 \bmod 3$	21	21	3	2	1.5000	$\{1,2\} \bmod 3$
11	11	11	6	1.7000	$\{1,2\} \bmod 3$				6	1.5833					10	1.6667	$1 \bmod 3$
			18	1.8000	$1 \bmod 3$				18	1.5000		21	21	7	5	1.6667	$\{2,4\} \bmod 7$
			27	1.6000					30	1.4167	$\{1,2\} \bmod 3$	24	24	2	1	1.5000	$1 \bmod 4$
			30	1.9000	$\{1,2\} \bmod 3$	16	16	2	1	1.7500	$1 \bmod 2$	24	24	3	1	1.2500	$1 \bmod 3$

For a security level of 256 bits we recommend the complete families of Table 4. For prime embedding degrees the optimal case is to use extension fields of size approximately 13500 bits, while for composite degree extension fields we should have $k \log q \approx 23780$. In the composite k case the best families are given by the pairs $(k, \rho) = (33, 1.4)$ and $(39, 1.167)$. For prime k we do not have any examples in Table 4. However an 256 bit security level in $\mathbb{F}_{q^k}$ can be achieved by selecting complete families with $k = 13$ and $\rho(q, t, r) = 2$. This case generates extension fields with $13 \log q \approx 13312$ bits. Two complete families for $D = 3, 13$ are given in Table 5. On the other hand, for the composite case we could choose $k = 24$ and $\rho(q, t, r) = 2$, for which $24 \log q \approx 24576$ bits. Examples appear in Table 5, for $D = 2, 3$.

Table 4. Complete families at 256 bit security level with $r(x) = \Phi_l(x)$ and $t(x) \equiv (x^i + 1) \bmod r(x)$.

k	l	D	i	$\rho(q,t,r)$	x_0	k	l	D	i	$\rho(q,t,r)$	x_0	k	l	D	i	$\rho(q,t,r)$	x_0
27	27	3	7	1.7778	1 mod 3	30	30	3	1	1.5000	1 mod 3	32	32	2	1	1.6250	1 mod 2
28	28	7	1	1.5000	1 mod 7	33	33	3	14	1.4000	1 mod 3	39	39	3	1	1.1670	1 mod 3
			3	1.8333	$\{1,2,4\}$ mod 7				26	1.5000	$\{1,2\}$ mod 3				2	1.2500	$\{1,2\}$ mod 3

Table 5. Complete families at 128, 192 and 512 bit security level with lifts of $t(x)$ and $y(x)$.

k	l	D	i	$\alpha(x)$	$\beta(x)$	$\rho(q,t,r)$	x_0	Security Level
5	15	3	3	1	1	2.0000	$\{0,2,3\}$ mod 3	128
5	20	5	4	1	0	2.0000	$\{0,2,8,10\}$ mod 10	
8	8	2	3	1	0	2.0000	1 mod 2	
8	24	3	9	1	-1	2.0000	1 mod 3	
9	9	3	5	1	1	2.0000	2 mod 3	
15	15	3	4	1	1	2.0000	$\{0,3\}$ mod 3	192
15	15	15	7	1	1	2.0000	$\{11,14\}$ mod 15	
15	60	5	4	1	0	2.0000	$\{0,4,6,10\}$ mod 10	
16	16	2	1	1	0	2.0000	$\{0,1,2\}$ mod 2	
16	48	3	9	1	1	2.0000	2 mod 3	
13	39	3	12	1	1	2.0000	$\{0,3\}$ mod 3	256
13	52	13	4	1	0	2.0000	$\{0,2,4,8,18,22,24,26\}$ mod 26	
24	24	3	6	1	1	2.0000	2 mod 3	
24	24	2	7	1	1	2.0000	2 mod 4	

More of complete families can be constructed by choosing the polynomial $r(x)$ to be other than the l^{th} cyclotomic polynomial. For such examples, see [8, 13], which however need to be updated, as the proposed families were produced in the pre-TNFS period. We only give one example of non-cyclotomic families here. Recall that for $k = 12$ Barreto and Naehrig [1] proposed a complete family for $D = 3$ and $\rho(q, t, r) = 1$. In particular the BN family is:

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

and $u(x) = 6x^2$ is a primitive 12^{th} root of unity in $\mathbb{Q}[x]/\langle r(x) \rangle$. This example was ideal in the pre-TNFS period, since for a 256 bit prime r, it produces an extension field of 3072 bit. Due to the recent improvements of the TNFS method, we need to consider extensions fields with $12 \log q \approx 4608$ and so $\rho(q,t,r) = 1.5$. The next example is produced by Barreto and Naehrig's setup.

Example 1 For $l = k = 12$ and $D = 3$, set

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

Then $\rho(q,t,r) = 1.5$ and all polynomials have integer coefficients. □

Table 6. Numerical examples of pairing-friendly parameters from complete families.

Family	k	D	x_0	n	$\log r$	$k \log q$	ρ	$L_{q^k}[1/3, c]$
Table 5	5	5	$4339430220 \equiv 0 \bmod 10$	1	256	2550	1.9922	128
	5	3	$4467952995 \equiv 0 \bmod 3$	1	256	2560	2.0000	128
Table 2	7	7	$10179463309681 \equiv 1 \bmod 7$	7	256	3003	1.6758	137
	7	3	$2714125 \equiv 1 \bmod 3$	1	256	2975	1.6602	136
Table 5	8	2	$6098533608147450349 1 \equiv 1 \bmod 2$	82	256	4184	2.0430	125
	8	3	$4296478348 \equiv 1 \bmod 3$	1	256	4096	2.0000	124
	8	3	$7562084023 \equiv 1 \bmod 3$	73	256	4200	2.0508	125
	9	3	$7567161105890 \equiv 2 \bmod 3$	1	256	4617	2.0039	130
Table 2	10	5	$4658060020 \equiv 0 \bmod 10$	1	256	4470	1.7461	128
	10	15	$4506234361 \equiv 1 \bmod 15$	1	256	4470	1.7461	128
	11	3	$9328 \equiv 1 \bmod 3$	463	254	3454	1.2362	145
	12	3	$19476673796408493595 \equiv 1 \bmod 3$	1	256	4584	1.4922	130
Exam. 1	12	3	7968144943122361485	1	256	4644	1.5117	130
Table 3	11	3	$621071 \equiv 2 \bmod 3$	1	384	7172	1.6979	197
	11	3	$609856 \equiv 1 \bmod 3$	1	384	6743	1.5964	192
	13	3	$66427 \equiv 1 \bmod 3$	1	384	6643	1.3307	191
	13	3	$65771 \equiv 2 \bmod 3$	1	384	7046	1.4115	195
Table 5	15	3	$663228522589779 \equiv 0 \bmod 3$	751	384	11805	2.0495	192
	15	15	$281474976719246 \equiv 11 \bmod 15$	1	384	11550	2.0052	190
	15	5	$17399844 \equiv 4 \bmod 10$	1	384	11505	1.9974	190
	16	2	$297221152944808 \equiv 0 \bmod 2$	1	384	12272	1.9974	195
	16	3	$17003435 \equiv 2 \bmod 3$	1	384	12288	2.0000	195
Table 3	21	3	$4371055696 \equiv 1 \bmod 3$	1	384	12054	1.4948	193
	24	3	$524070931301332 \equiv 1 \bmod 3$	73	384	11688	1.2682	191
Table 5	13	3	$3176547 \equiv 0 \bmod 3$	1	512	13468	2.0234	255
	13	13	$3188926 \equiv 0 \bmod 26$	1	512	13455	2.0215	255
	24	3	$18858059538137430449 \equiv 2 \bmod 3$	1	512	24576	2.0000	258
	24	2	$19228544116597719574 \equiv 2 \bmod 4$	1	512	24576	2.0000	258
Table 4	27	3	$389679094 \equiv 1 \bmod 3$	1	512	24597	1.7793	258
	28	3	$7094524748557 \equiv 1 \bmod 7$	1	512	26208	1.8281	265
	30	3	$36738675093168908494 \equiv 1 \bmod 3$	151	512	23340	1.5195	253
	33	3	$52489264 \equiv 1 \bmod 3$	1	512	23628	1.3984	254
	39	3	$3305782 \equiv 1 \bmod 3$	157	512	23556	1.1797	254

Applying Algorithm 3 to our complete families we produced some numerical examples for security levels of 128, 192 and 256 bits. These are presented in Table 6. The x_0 denotes the integer input for the polynomials $q(x), t(x)$ and $r(x)$. The search for suitable x_0 is performed by taking random $x_0 \in \mathbb{Z}$ for which $\deg r \cdot \log x_0 + \log(\mathrm{lc}(r))$ is approximately equal to the desired security level, where $\mathrm{lc}(r)$ is the leading coefficient of $r(x)$. Note that if $r(x) = \Phi_l(x)$, then $\log(\mathrm{lc}(r)) = 0$. We considered primes $q = q(x_0)$ and $r = r(x_0)/n$, for some relatively small $n \geq 1$. This factor $n > 1$ might be helpful in some cases as it further increases the size of the extension field. The security level in the r-order subgroups $\mathbb{G}_1, \mathbb{G}_2$ is taken as $\log r/2$. On the other hand, the security level in the extension field $\mathbb{F}_{q^k}$ is measured by the L-notation of Equation (1.1), namely $L_{q^k}[1/3, c]$, where $c = 1.923$ when k is prime and $c = 1.526$ when k is composite. In general we want $L_{q^k}[1/3, c] \approx \log r/2$.

4 CVD Families Revised

By Definition 2, the 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 earlier, we can apply a linear transformation $x \to (x - d)/c$ in order to obtain $g(x) = x$. The difference in the case of CVD families is that the CM discriminant 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 the primitive k^{th} roots of unity and the element $\sqrt{-x}$. We set $K = \mathbb{Q}(\zeta_l)$ and $r(x) = \Phi_l(x)$, for some $l > 0$, with $k \mid l$ and then search for a polynomial $z(x) \in K$ such that $-z(x)^2 \equiv x \bmod r(x)$. This search is easy when $r(x)$ is the l^{th} cyclotomic polynomial (see for example [3]). However if we set $r(x)$ as any irreducible polynomial in $\mathbb{Q}[x]$ the search is harder, especially as $\deg r$ grows. We then conclude to Algorithm 4 which is a modified version of the Brezing-Weng method for constructing CVD polynomial families of pairing-friendly elliptic curves. The families produced by this algorithm have generally ρ-values:

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

```
Input: An embedding degree $k$.
Output: A CVD family with embedding degree $k$.
1: Set $K = \mathbb{Q}(\zeta_l)$, where $k \mid l$ and $r(x) = \Phi_l(x)$, so that $K \cong \mathbb{Q}[x]/\langle r(x) \rangle$.
2: Find a polynomial $z(x) \in K$, such that $-z(x)^2 \equiv x \bmod r(x)$.
3: Let $u(x)$ be the polynomial mapping to $\zeta_l$ in $K$.
4: For every $i = 1, ..., \varphi(l) - 1$, such that $l/\gcd(i, l) = k$ set:
       $t(x) \equiv \left[u(x)^i + 1\right] \bmod r(x), \quad y(x) \equiv \left[\left(u(x)^i - 1\right) z(x)^{-1}\right] \bmod r(x).$   (4.1)
5: Compute $q(x)$ by the relation $4q(x) = t(x)^2 + xy(x)^2$.
6: If $q(x)$ represents primes, return $(q(x), t(x), r(x))$.
```

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

By Remark 1 another option for the fourth step of the algorithm is to consider lifts $\alpha(x), \beta(x) \in \mathbb{Q}[x]$ of the polynomials $t(x)$ and $y(x)$.

The outputs of Algorithm 4 are potential CVD families. As in the case of complete families, 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 $q(x) \in \mathbb{Z}$, for every $x \equiv b \bmod a$. In order to generate pairing-friendly parameters

Algorithm 5 Finding suitable parameters using CVD families.

```
Input: A CVD family $(q(x), t(x), r(x))$ and a desired bit size $S_r$.
Output: A prime $q$, a (nearly) prime $r$ and a Frobenius trace $t$.
1: Find $a, b \in \mathbb{Z}$, so that $q(x) \in \mathbb{Z}$, for every $x \equiv b \bmod a$.
2: Search for $x_0 \in \mathbb{Z}$ of the form $x_0 = Dy^2$, with $x_0 \equiv b \bmod a$, such that $r(x_0) = nr$ for some prime $r$ and $n \geq 1$.
3: Set $q = q(x_0)$, $r = r(x_0)/n$ and $t = t(x_0)$.
4: If $\log r \approx S_r$ and $q$ is prime, return $(q, t, r)$ and $D$.
```

using this type of families, we are searching for $x_0 \in \mathbb{Z}$, such that $q(x_0)$ 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 $g(x_0)$ 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. Once again this process is affected as $\deg r$ grows.

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. $D < 10^7$), in order construct the elliptic curve efficiently. Another option for constructing elliptic curves with flexible CM discriminants is to use sparse families (see for example [3, 5, 6]), but in this case the procedure of generating suitable parameters is a little more complicated.

4.1 Examples for 128, 192 and 256 bit Security Level

In Tables 7–9 we give examples of CVD families produced by Algorithm 4, with $\rho(q, t, r) < 2$. Additionally, in Table 10 we present CVD families with $\rho(q, t, r) \approx 2$, which are obtained by considering constant lifts for the polynomials $t(x)$ and $y(x)$. In all families of Tables 7–10 we have taken $l = 2l'$, for some odd $l' > 0$ and $k = l'$ or $k = 2l'$. Furthermore we set:

$$r(x) = \Phi_l(x), \quad u(x) = x, \quad t(x) \equiv \left(u(x)^i + 1\right) \bmod r(x), \quad z(x) = x^{\frac{l/2+1}{2}},$$

for $i = 1, \ldots, \varphi(l) - 1$, where $u(x)$ and $z(x)$ represent a primitive l^{th} root of unity and the element $\sqrt{-x}$ respectively in $K = \mathbb{Q}[x]/\langle r(x) \rangle$. This setup was first considered by Dryło in [3], however his examples are aiming for the families with the smallest ρ-value for each embedding degree. Here we recommend more CVD families with ρ-values achieving a nice balance between the security level of an r-order subgroup of $E(\mathbb{F}_q)$ and the extension field $\mathbb{F}_{q^k}$. In addition, our recommendations intend to produce extension fields $\mathbb{F}_{q^k}$ such that the DLP is resistant against the improved TNFS attacks. These recommendations do not necessarily coincide with the smallest ρ-values.

In Table 7 we gather the recommended CVD families for an 128 bit security level. Recall from Section 3 that in this case $\log r = 256$ bits and we are looking for extension fields where $k \log q \approx 2530$ for prime embedding degrees and $k \log q \approx 4352$ for the composite case. Note that for $k = 10$, the smallest ρ-value obtained by Algorithm 4 is $\rho(q, t, r) = 1.5$. Such a family produces extension fields with size $10 \log q \approx 3840$ bits. The complexity of the DLP in this extension field is $L_{q^{10}}[1/3, 1.526] \approx 120$, which is slightly small for an 128 bit security level. Our recommendation in this case is the family with $k = 10$ and $\rho(q, t, r) = 1.75$ which produces extension fields of $10 \log q \approx 4480$ bits with DLP complexity $L_{q^{10}}[1/3, 1.526] \approx 128$.

For an 192 bit security level our recommendations of CVD families are summarized in Table 8. For prime embedding degrees the extension field must satisfy $k \log q \approx 6670$ and in the composite

Table 7. CVD families at 128 bit security level with $r(x) = \Phi_l(x)$, $z(x) = x^{\frac{l/2+1}{2}}$ and $t(x) \equiv (x^i + 1) \bmod r(x)$.

k	l	i	$\rho(q,t,r)$	x_0	k	l	i	$\rho(q,t,r)$	x_0	k	l	i	$\rho(q,t,r)$	x_0
7	14	4	1.3333	1 mod 2	9	18	10	1.8333	1 mod 2	11	22	6	1.2000	1 mod 2
		8	1.5000		10	10	1	1.7500	1 mod 2	14	14	1	1.5000	1 mod 2

case $k \log q \approx 11670$. Additionally, the prime r must be chosen such that $\log r = 384$ bits. The best balance for prime k is obtained by the families with $(k, \rho) = (11, 1.6)$ and $(13, 1.333)$. Although there exist families with $\rho(q,t,r) < 1.6$ for $k = 11$, they do not reach the security level of 192 bits in the extension field. For composite embedding degrees we have even more options. For a security level of 256 bits our proposals for CVD families are presented in Table 9. Recall that in this case the prime r is around 512 bits. The extension field should be of size around 13500 bit for prime k and approximately 23780 bits when k is composite.

Table 8. CVD families at 192 bit security level with $r(x) = \Phi_l(x)$, $z(x) = x^{\frac{l/2+1}{2}}$ and $t(x) \equiv (x^i + 1) \bmod r(x)$.

k	l	i	$\rho(q,t,r)$	x_0	k	l	i	$\rho(q,t,r)$	x_0	k	l	i	$\rho(q,t,r)$	x_0
11	22	8	1.6000	1 mod 2	17	34	18	1.1875	1 mod 2	25	50	14	1.4000	1 mod 2
		14	1.7000		18	18	1	1.8333	1 mod 2			26	1.3500	
13	26	2	1.4167	1 mod 2			5	1.6667		26	26	1	1.2500	1 mod 2
		8	1.3333		22	22	7	1.4000	1 mod 2			7	1.1667	
		16	1.5833				13	1.5000		34	34	9	1.1250	1 mod 2

Table 9. CVD families at 256 bit security level with $r(x) = \Phi_l(x)$, $z(x) = x^{\frac{l/2+1}{2}}$ and $t(x) \equiv (x^i + 1) \bmod r(x)$.

k	l	i	$\rho(q,t,r)$	x_0	k	l	i	$\rho(q,t,r)$	x_0	k	l	i	$\rho(q,t,r)$	x_0
17	34	4	1.5625	1 mod 2	25	50	6	1.8500	1 mod 2	27	54	2	1.7222	1 mod 2
		12	1.5000				18	1.8000				16	1.7778	
19	38	4	1.5000	1 mod 2			32	1.9500		34	34	3	1.4375	1 mod 2
		14	1.5556		26	26	5	1.9167	1 mod 2			11	1.3750	
		22	1.3889				11	1.8333		38	38	11	1.2222	1 mod 2
23	46	24	1.1364	1 mod 2			17	1.7500				21	1.2778	

In Table 10 we give some examples of CVD families with $\rho(q,t,r) \approx 2$. These examples are constructed by considering constant lifts $\alpha(x)$ and $\beta(x)$ for $t(x)$ and $y(x)$ respectively. In particular, a constant lift $\alpha(x) \in \mathbb{Q}$ only for $t(x)$ will result is families with ρ-value equal to 2. On the other hand if we consider a constant lift $\beta(x) \in \mathbb{Q}$ for $y(x)$ as well, we will get $\rho(q,t,r) = 2 + 1/\varphi(l)$. For the later case we give an example for $k = 13$, with $\rho(q,t,r) = 2.0833$.

Alternatively, as mentioned also in the case of complete families, we can choose $r(x)$ as any irreducible polynomial, other than $\Phi_l(x)$. Here we give only one example for $k = 8$ (see also [3]). Such choices are likely to produce more examples for embedding degrees where the above setup fails to generate suitable families. However in this case it is sometimes hard to determine suitable

Table 10. CVD families at 128, 192 and 512 bit security level with lifts of $t(x)$ and $y(x)$.

k	l	i	$\alpha(x)$	$\beta(x)$	$\rho(q,t,r)$	x_0	Security Level
5	10	6	1	0	2.0000	$\{0,2\}$ mod 2	128
9	18	4	1	0	2.0000	$\{0,2\}$ mod 2	
15	30	4	3	0	2.0000	$\{0,2\}$ mod 2	192
13	26	2	3	0	2.0000	$\{0,2\}$ mod 2	256
13	26	6	1	1	2.0833	$\{0,2\}$ mod 2	

Table 11. Non-cyclotomic CVD families at 128, 192 and 512 bit security level.

k	l	$r(x)$	$t(x)$	$z(x)$	$\rho(q,t,r)$	x_0	Security Level
12	12	$\Phi_{12}(2x)$	$2x+1$	$4x^3+2x^2-x$	1.7500	3 mod 4	128
14	28	$\Phi_{28}(2x)$	$(2x)^2+1$	$1024x^{11}+8x^4$	1.4167	3 mod 4	
28			$-(2x)^9+1$		1.7500	3 mod 4	256
30	30	$\Phi_{30}(5x)$	$-(5x)^2+1$	$(5x)^7+2(5x)^6+(5x)^5-(5x)^4-(5x)^3-5x+1$	1.6250	1 mod 2	

polynomials $z(x)$, such that $z(x)^2 \equiv -x \bmod r(x)$. The general way to do this is to set $z(x) \in \mathbb{Q}[x]/\langle r(x)\rangle$ to be in its general form:

$$z(x) = z_{\varphi(l)-1}x^{\varphi(l)-1} + \cdots + z_1x + z_0$$

and search for coefficients z_i, such that $z(x)^2 \equiv -x \bmod r(x)$. In Table 11 we give some examples of CVD families with $\rho(q,t,r) < 2$, where $r(x) = \Phi_l(ax)$ and $u(x) = ax$, for some $a \in \mathbb{Z}$. For $k = 30$, this family was first introduced in [3]. For $k = 28$, Dryło presented a CVD family for $r(x)$ as in Table 11 with $\rho(q,t,r) = 1.5$. Our family in this case has $\rho(q,t,r) = 1.75$ and produces extension fields of size $28\log q \approx 25088$ bits. This corresponds to a security level around 261 bits. Below we give an example where $r(x)$ is not the l^{th} cyclotomic polynomial, for $k = 8$ and $\rho(q,t,r) = 2$. This family is obtained by taking a constant lift for the trace polynomial. Additionally, the polynomials $r(x)$ and $z(x)$ are taken from Dryło [3] who presented a CVD family for the same embedding degree, but with $\rho(q,t,r) = 1.5$.

Example 2 For $l = k = 8$ we take Dryło's polynomials [3]:

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

so that $z(x)^2 \equiv -x \bmod r(x)$. Set the following polynomials:

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

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

In Table 12 we give some numerical results of pairing-friendly parameters obtained by the CVD families of this section. Our results are aiming at 128, 192 and 256 bit security levels and various values of D up to 10^7. The entries for x_0 denote the input for the polynomials $q(x), t(x)$ and $r(x)$. These are obtained by Algorithm 5 in the following way. We are selecting random square-free values for D up to 10^7 and for each D we are searching for random $y \in \mathbb{Z}$, such that

$$\deg r\,[\log D + 2\log y] + \log(\mathrm{lc}(r))$$

is approximately equal to the desired security level. Then we set $x_0 = Dy^2$. In Table 12 we have recorded the first such examples that came up. In some cases, in order to reach a desired security level, we need $y = 1$, so that $x_0 = D$. This happens in families where $\deg r$ is large. Furthermore, as in the case of complete families, we are looking for x_0, such that $q = q(x_0)$ and $r = r(x_0)/n$ are both primes, for some small factor $n \geq 1$. In almost every example of Table 12 this small factor is equal to 1. The complexity of the DLP in the r-order subgroups of $E(\mathbb{F}_q)$ is $\log r/2$ and in the extension field $\mathbb{F}_{q^k}$ is $L_{q^k}[1/3, c]$, where $c = 1.923$ for prime k and $c = 1.526$ for composite embedding degrees, according to the new results regarding the TNFS attacks.

Table 12. Numerical examples of pairing-friendly parameters from CVD families.

Family	k	D	x_0	n	$\log r$	$k \log q$	ρ	$L_{q^k}[1/3, c]$
Table 10	5	8871207	$D \cdot 1511472^2 \equiv 0 \bmod 2$	1	256	2555	1.9961	128
Table 7	7	9160269	$D \cdot 903^2 \equiv 1 \bmod 2$	1	256	2674	1.4922	130
Exam. 2	8	814127	$D \cdot 6727283^2 \equiv 23 \bmod 24$	9	256	4136	2.0195	124
Table 7	9	908587	$D \cdot 2903^2 \equiv 1 \bmod 2$	1	256	4212	1.8281	125
Table 10	9	4330077	$D \cdot 1302^2 \equiv 0 \bmod 2$	1	256	4590	1.9922	130
Table 7	10	3281749	$D \cdot 2575675^2 \equiv 1 \bmod 2$	1	256	4470	1.7461	128
	11	9647	$D \cdot 73^2 \equiv 1 \bmod 2$	1	256	3355	1.1914	143
Table 11	12	4725179	$D \cdot 1517443^2 \equiv 3 \bmod 4$	1	256	5352	1.7422	138
Table 7	14	2358697	$D \cdot 1757^2 \equiv 1 \bmod 2$	1	256	5348	1.4922	138
Table 11	14	1350211	$D \equiv 3 \bmod 4$	1	256	5040	1.4063	135
Table 8	11	1040779	$D \cdot 611^2 \equiv 1 \bmod 2$	1	384	6743	1.5964	192
	13	179	$D \cdot 4959^2 \equiv 1 \bmod 2$	1	384	6630	1.3281	191
Table 10	15	876018	$D \cdot 18341^2 \equiv 0 \bmod 2$	1	384	11550	2.0052	190
Table 8	17	13841	$D \cdot 35^2 \equiv 1 \bmod 2$	1	384	7718	1.1823	203
	18	2331871	$D \cdot 2949767^2 \equiv 1 \bmod 2$	1	384	11502	1.6641	190
	22	87847	$D \cdot 2051^2 \equiv 1 \bmod 2$	1	384	11770	1.3932	191
	25	614161	$D \equiv 1 \bmod 2$	1	384	12925	1.3464	199
	26	8281427	$D \cdot 23^2 \equiv 1 \bmod 2$	1	384	11596	1.1615	190
	34	4895	$D \cdot 59^2 \equiv 1 \bmod 2$	1	384	14620	1.1198	209
Table 10	13	711401	$D \cdot 3136^2 \equiv 0 \bmod 2$	1	512	13832	2.0781	258
Table 9	17	1971089	$D \cdot 47^2 \equiv 1 \bmod 2$	1	512	13566	1.5586	256
	19	2166897	$D \cdot 13^2 \equiv 1 \bmod 2$	1	512	13471	1.3848	255
	23	16403	$D \cdot 25^2 \equiv 1 \bmod 2$	1	512	13340	1.1328	254
	25	307795	$D \cdot 13^2 \equiv 1 \bmod 2$	1	512	23650	1.8477	254
	26	2385911	$D \cdot 1735^2 \equiv 1 \bmod 2$	1	512	24362	1.8301	257
	27	2703	$D \cdot 371^2 \equiv 1 \bmod 2$	1	512	23760	1.7188	254
Table 11	28	2143411	$D \cdot 1291^2 \equiv 1 \bmod 2$	1	512	25060	1.7480	260
	30	4895545	$D \cdot 902873^2 \equiv 1 \bmod 2$	1	512	24870	1.6191	259
Table 9	34	3628579	$D \cdot 35^2 \equiv 1 \bmod 2$	1	512	23902	1.3730	255
	38	2193243	$D \cdot 13^2 \equiv 1 \bmod 2$	1	512	23712	1.2188	254

5 Conclusion

Since the improvements on the TNFS method [7, 9], there has been much discussion on whether pairings can be indeed used for robust cryptographic applications. Especially for composite embedding degrees k, these TNFS variants have a major effect. Consequently it is necessary to update the criteria for selecting elliptic curve parameters for pairing-based implementations.

In this paper we presented families of pairing-friendly elliptic curves with composite embedding degree that are suitable for producing parameters resistant to the TNFS attacks. Additionally for prime embedding degrees we proposed families which can provide a nice balance between the security level of the r-order subgroups $\mathbb{G}_1, \mathbb{G}_2$ of $E(\mathbb{F}_q)$ and the security level of $\mathbb{F}_{q^k}$. Some of the recommended families were not considered before, due to a larger ρ-value. However we argue that at present, larger ρ-values can be advantageous, especially for composite k, since a larger ρ implies a larger extension field and hence an increase of the complexity of the DLP in $\mathbb{F}_{q^k}$.

Table 13. Recommended (complete or CVD) families at 128, 192 and 256 bit security level.

Security Level: 128 bits				Security Level: 192 bits				Security Level: 256 bits			
k	ρ	$k \log q$	$L_{q^k}[1/3, c]$	k	ρ	$k \log q$	$L_{q^k}[1/3, c]$	k	ρ	$k \log q$	$L_{q^k}[1/3, c]$
5	2.0000	2560	128	11	1.6000	6758	192	13	2.0000	13312	254
7	1.5000	2688	131	13	1.3333	6656	191	17	1.5625	13600	256
8	2.0000	4096	124	15	2.0000	11520	190	19	1.3889	13511	255
9	1.8333	4224	125	16	2.0000	12288	195	23	1.1364	13382	254
9	2.0000	4608	130	17	1.1875	7752	203	24	2.0000	24576	258
10	1.7500	4480	128	18	1.6667	11520	190	25	1.8500	23680	254
11	1.2000	3379	144	21	1.5000	12096	194	26	1.8333	24405	257
12	1.5000	4608	130	22	1.4000	11827	192	27	1.7222	23808	255
14	1.4167	5077	135	24	1.2500	11520	190	28	1.7500	25088	260
14	1.5000	5376	139	25	1.3500	12960	199	30	1.6250	24960	260
				26	1.1667	11648	191	33	1.4000	23654	254
								34	1.3750	23936	255
								38	1.2222	23780	255
								39	1.2500	24960	260

Our recommendations are summarized in Table 13. 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 ρ-value $\rho(q, t, r)$ achieved by a complete or CVD family (or both) presented in Sections 3 and 4. For each family we also calculate the extension field size by $k \log q$, where $\log q = \rho \log r$ and $\log r$ is twice the security level. In addition we give the asymptotic complexity of the DLP in the extension field $\mathbb{F}_{q^k}$, which is measured by the usual L-notation $L_{q^k}[1/3, c]$, where $c = 1.923$ when k is prime and $c = 1.526$ when k is composite. Finally we have presented extended numerical results of pairing-friendly parameters obtained by our recommended families, with a balanced security level for both composite and prime embedding degrees.

References

1. P. S. L. M. Barreto and M. Naehrig. Pairing-Friendly Elliptic Curves of Prime Order. In *International Workshop on Selected Areas in Cryptography*–SAC'05, pages 319–331. Springer, Berlin, Heidelberg, 2005.
2. F. Brezing and A. Weng. Elliptic Curves Suitable for Pairing Based Cryptography. *Designs, Codes and Cryptography*, 37(1):133–141, 2005.
3. R. Dryło. On Constructing Families of Pairing-Friendly Elliptic Curves with Variable Discriminant. In *International Conference on Cryptology in India*–INDOCRYPT'11, pages 310–319. Springer, Berlin, Heidelberg, 2011.

4. N. El Mrabet and M. Joye. *Guide to Pairing-Based Cryptography.* CRC Press, 2017.
5. G. Fotiadis and E. Konstantinou. More Sparse Families of Pairing-Friendly Elliptic Curves. In *International Conference on Cryptology and Network Security*–CANS'14, pages 384–399. Springer International Publishing, 2014.
6. D. Freeman, M. Scott, and E. Teske. A Taxonomy of Pairing-Friendly Elliptic Curves. *Journal of Cryptology*, 23(2):224–280, 2010.
7. J. Jeong and T. Kim. Extended Tower Number Field Sieve With Application to Finite Fields of Arbitrary Composite Extension Degree. IACR Cryptology ePrint Archive, 2016.
8. E. J. Kachisa, E. F. Schaefer, and M. Scott. Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field. In *International Conference on Pairing-Based Cryptography*–Pairing'08, pages 126–135. Springer, Berlin, Heidelberg, 2008.
9. T. Kim and R. Barbulescu. Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case. In *Advances in Cryptology*–CRYPTO'16, pages 543–571. Springer, Berlin, Heidelberg, 2016.
10. H.-S. Lee and C.-M. Park. Generating Pairing-Friendly Curves With the CM Equation of Degree 1. In *International Conference on Pairing-Based Cryptography*–Pairing'09, pages 66–77. Springer, Berlin, Heidelberg, 2009.
11. H.-S. Lee and C.-M. Park. Constructing Pairing-Friendly Curves With Variable CM Discriminant. *Bulletin of the Korean Mathematical Society*, 49(1):75–88, 2012.
12. A. Murphy and N. Fitzpatrick. Elliptic Curves for Pairing Applications. In *IACR Cryptology ePrint Archive*, pages 1–15. Citeseer, 2005.
13. S. Tanaka and K. Nakamula. Constructing Pairing-Friendly Elliptic Curves Using Factorization of Cyclotomic Polynomials. In *International Conference on Pairing-Based Cryptography*–Pairing'08, pages 136–145. Springer, Berlin, Heidelberg, 2008.