J. Cryptol. (2010) 23: 224–280
DOI: 10.1007/s00145-009-9048-z

Journal of
CRYPTOLOGY

A Taxonomy of Pairing-Friendly Elliptic Curves

David Freeman
CWI and Universiteit Leiden, Science Park 123, 1098 XG Amsterdam, The Netherlands
freeman@cwi.nl

Michael Scott
School of Computer Applications, Dublin City University, Ballymun, Dublin 9, Ireland
mike@computing.dcu.ie

Edlyn Teske
Dept. of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada
eteske@math.uwaterloo.ca

Communicated by Dan Boneh

Received 8 March 2007 and revised 25 May 2009
Online publication 18 June 2009

Abstract. Elliptic curves with small embedding degree and large prime-order subgroup are key ingredients for implementing pairing-based cryptographic systems. Such "pairing-friendly" curves are rare and thus require specific constructions. In this paper we give a single coherent framework that encompasses all of the constructions of pairing-friendly elliptic curves currently existing in the literature. We also include new constructions of pairing-friendly curves that improve on the previously known constructions for certain embedding degrees. Finally, for all embedding degrees up to 50, we provide recommendations as to which pairing-friendly curves to choose to best satisfy a variety of performance and security requirements.

Key words. Elliptic curves, Pairing-based cryptosystems, Embedding degree, Efficient implementation.

1. Introduction

There has been much interest in recent years in cryptographic schemes based on pairings on elliptic curves. In a flurry of research results, many new and novel protocols have been suggested, including one-round three-way key exchange [44], identity-based encryption [12,75], identity-based signatures [19,70], and short signature schemes [13]. Some of these protocols have already been deployed in the marketplace, and developers are eager to deploy many others.

However, whereas standard elliptic curve cryptosystems such as ElGamal encryption or ECDSA can be implemented using randomly generated elliptic curves, the elliptic curves required to implement pairing-based systems must have certain properties that

randomly generated elliptic curves are unlikely to have. To this end it is important that it should be easy to find such "pairing-friendly" elliptic curves for all kinds of applications and all desired levels of security.

Our contribution in this paper is threefold:

- To gather all of the existing constructions of pairing-friendly elliptic curves into a single coherent framework;
- To describe several new constructions of pairing-friendly elliptic curves that improve on existing constructions for certain embedding degrees;
- To recommend curves to use for a variety of security levels and performance requirements.

1.1. *Pairings and Embedding Degrees*

The most common pairings used in applications are the Tate and Weil pairings on elliptic curves over finite fields; other proposed pairings include the Eta pairing [8], the Ate pairing [42], and their generalizations [41]. Given an elliptic curve E defined over a finite field $\mathbb{F}_q$, all of these pairings take as inputs points on E that are defined over $\mathbb{F}_q$ or over an extension field $\mathbb{F}_{q^k}$ and give as output an element of $\mathbb{F}_{q^k}^{\times}$. For a pairing-based cryptosystem to be secure, the discrete logarithm problems in the group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on E and in the multiplicative group $\mathbb{F}_{q^k}^{\times}$ must both be computationally infeasible. The best known discrete logarithm algorithm on elliptic curves is the parallelized Pollard rho algorithm [72,86], which has running time $O(\sqrt{r})$ where r is the size of largest prime-order subgroup of $E(\mathbb{F}_q)$. On the other hand, the best algorithm for discrete logarithm computation in finite fields is the index calculus attack (e.g., [68]) which has running time subexponential in the field size. Thus to achieve the same level of security in both groups, the size q^k of the extension field must be significantly larger than r. The ratio of these sizes is measured by two parameters: the *embedding degree*, which in most cases[1] is the degree k of the extension field that the pairing maps into; and the parameter $\rho = \log q / \log r$, which measures the base field size relative to the size of the prime-order subgroup on the curve. We will call an elliptic curve with a small embedding degree and a large prime-order subgroup *pairing-friendly*. (For precise definitions of all of these terms, see Sect. 2.)

There has been much speculation about the exact sizes of r and q^k required to match standard sizes of keys for symmetric encryption, using, for example, the Advanced Encryption Standard (AES) [54,69]. The problem is complicated by the fact that the effectiveness of index calculus attacks is not yet fully understood, especially over extension fields. We outline in Table 1 our own view of the matter, distilled from material taken from various authoritative sources, in particular [37] and [54]. The listed bit sizes are those matching the security levels of the SKIPJACK, Triple-DES, AES-Small, AES-Medium, and AES-Large symmetric key encryption schemes.

As we can see from the table, to achieve varied levels of security it is necessary to construct curves with varying embedding degree. We give two different ranges for the embedding degree because the ratio of the extension field size q^k to the subgroup size r depends not only on the embedding degree k but also on the parameter ρ; specifically,

[1] See the discussion after Remark 2.2.

Table 1. Bit sizes of curve parameters and corresponding embedding degrees to obtain commonly desired levels of security.

Security level (in bits)	Subgroup size r (in bits)	Extension field size q^k (in bits)	Embedding degree k	
			$\rho \approx 1$	$\rho \approx 2$
80	160	960–1280	6–8	2*, 3–4
112	224	2200–3600	10–16	5–8
128	256	3000–5000	12–20	6–10
192	384	8000–10000	20–26	10–13
256	512	14000–18000	28–36	14–18

we have $\log q^k / \log r = \rho \cdot k$. Thus, for example, if we wish to set up a system with a 160-bit elliptic curve subgroup and a 1280-bit extension field, we could use a curve with embedding degree 8 and $\rho = 1$ (though we currently know of no such curves), a curve with embedding degree 4 and $\rho = 2$, or anything in between with $\rho \cdot k = 8$.

In general, curves with small ρ-values are desirable in order to speed up arithmetic on the elliptic curve. For example, an elliptic curve with a 160-bit subgroup and $\rho = 1$ is defined over a 160-bit field, while a curve with a 160-bit subgroup and $\rho = 2$ is defined over a 320-bit field, and the group operation can be computed much more quickly on the first curve. On the other hand, though, at times a larger ρ-value is acceptable for the sake of fast pairing evaluation. For example, at a security level of 80 bits, using a 512-bit q, a 160-bit r, and $k = 2$ represents an efficient setup for some choices of curves and protocol; see [78] for a detailed explanation. Therefore $k = 2$ (marked with an asterisk) has been included in Table 1 at the 80-bit security level.

1.2. *Our Framework*

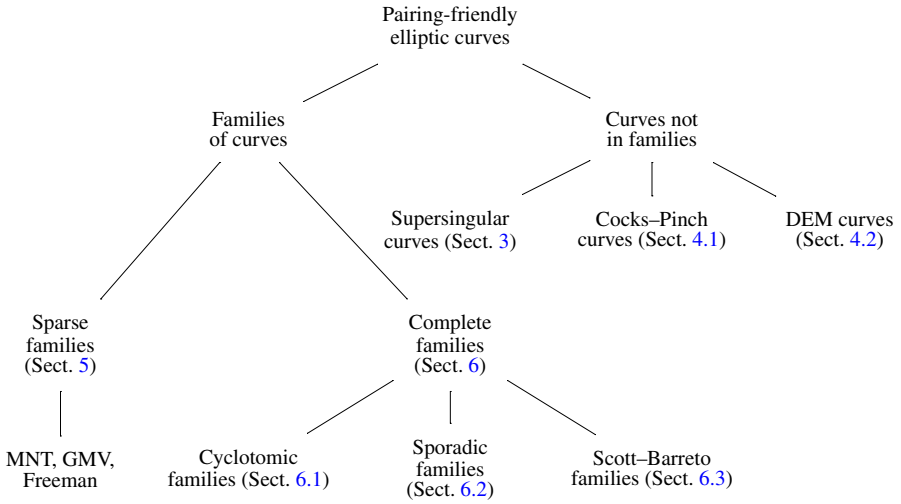
A primary contribution of this paper is to give a classification of the known methods for constructing pairing-friendly elliptic curves. A diagram outlining this classification is given in Table 2.

The designers of the first pairing-based protocols proposed the use of supersingular elliptic curves [12]. However, such curves are limited to embedding degree $k = 2$ for prime fields and $k \leq 6$ in general [62], so for higher embedding degrees, we must turn to ordinary curves.

There are a large number of constructions of ordinary elliptic curves with prescribed embedding degree. All of these constructions are based on the *complex multiplication (CM) method* of curve construction, and all construct curves over prime fields. The CM algorithm takes as input a prime power q (which in our applications will always be prime) and an integer n, and constructs an elliptic curve over $\mathbb{F}_q$ with n points [1]. In Sect. 2 we will give a list of conditions for a given k such that if q and n satisfy these conditions, then the algorithm will terminate in a reasonable amount of time and the curve constructed will have embedding degree k.

The highest-level distinction we make in our framework is between methods that construct individual curves and those that construct parametric *families* of curves. The former type are methods that give integers q and r such that there is an elliptic curve E over $\mathbb{F}_q$ with a subgroup of order r and embedding degree k with respect to r. The latter type are methods that give polynomials $q(x)$ and $r(x)$ such that if $q(x_0)$ is a prime

Table 2. Classification of pairing-friendly elliptic curves.



power for some value of x_0, there is an elliptic curve E over $\mathbb{F}_{q(x_0)}$ with a subgroup of order $r(x_0)$ and embedding degree k with respect to $r(x_0)$. (In practice the prime power $q(x_0)$ is always prime.) Parametric families have the advantage that the sizes of the finite field and the prime-order subgroup can be varied simply by specifying x_0.

Supersingular curves, which we discuss in Sect. 3, do not fall into families. There are also two constructions in the literature that produce ordinary elliptic curves with small embedding degree that are not given in terms of families: the method of Cocks and Pinch [22] and that of Dupont, Enge, and Morain [27]. In Sect. 4 we describe these two methods and discuss their merits and drawbacks.

The remaining constructions of ordinary elliptic curves with small embedding degree fall into the category of families of curves. Here we make another distinction. The construction of such curves depends on our being able to find integers x, y satisfying an equation of the form

$$Dy^2 = 4q(x) - t(x)^2$$

for some fixed positive integer D and polynomials $q(x)$ and $t(x)$. The parameter D is the *CM discriminant* (often called simply the "discriminant"), which we will define formally in Sect. 2. In some cases, this equation will only have solutions for some set of (x, y) that grows exponentially; we call such families *sparse*. In others, this equation may be satisfied for any x, and in fact we can write y as a polynomial in x, and the equation gives an equality of polynomials; we call such families *complete*.

Sparse families, discussed in Sect. 5, are primarily based on the ideas of Miyaji, Nakabayashi, and Takano [64]. These families give most of the known constructions of curves of prime order but are currently limited to embedding degrees $k \leq 10$. Complete families, discussed in Sect. 6, exist for arbitrary k but usually lead to curves with $\rho > 1$.

All of the constructions of complete families can be viewed as choosing a polynomial $r(x)$ parameterizing the pairing-friendly subgroup size and computing polynomials in $\mathbb{Q}[x]$ that map to certain elements of the number field $K = \mathbb{Q}[x]/(r(x))$. We can then further classify the complete families according to the properties of the number field K. We briefly list here the families and the corresponding type of number field.

- Cyclotomic families (Sect. 6.1): K is a cyclotomic field, r is a cyclotomic polynomial, and K contains $\sqrt{-D}$ for some small D. Constructions appear in [5,17].
- "Sporadic" families (Sect. 6.2): K is a (perhaps trivial) extension of a cyclotomic field, r is not a cyclotomic polynomial, and K contains $\sqrt{-D}$ for some small D. Constructions appear in [4,47]; we give new examples in Sect. 6.2.
- Scott–Barreto families (Sect. 6.3): K is an extension of a cyclotomic field, and K contains no $\sqrt{-D}$ for any small D. Constructions appear in [81].

1.3. *New Constructions*

In addition to classifying construction methods, in Sect. 6 we give several new constructions of pairing-friendly elliptic curves. Our focus throughout is to construct families with minimal ρ-value, as we believe that such families will be most useful in practice.

In Sect. 6.1 we use the method of Brezing and Weng to demonstrate families of pairing-friendly elliptic curves with $\rho \leq 2$ for every embedding degree $k \leq 1000$ that is not divisible by 72. Examples of these constructions have previously appeared in the literature for specific values of k, but the families have not been described in the general terms that we use, and even the examples that do appear have not all been shown to satisfy the criteria necessary to produce valid parameters for constructing pairing-friendly curves (our Definition 2.7). We conjecture that our constructions extend to all k not divisible by 72; these conjectures are mainly of theoretical interest, as we do not expect that curves with $k > 1000$ will be necessary in practice in the foreseeable future.

In Sects. 6.2 and 6.3 we give a few more examples of new complete families of curves for certain small values of k. Most of these families have ρ-values smaller than those achieved by any construction in Sect. 6.1.

Our most significant contribution with regard to new constructions is Theorem 6.19. The constructions of Sects. 6.1 and 6.2 have in common that we first fix a (small) square-free CM discriminant and then compute the corresponding complete family of curves, all with the same discriminant. We refer to such constructions as *basic constructions*. However, to ensure maximum security, some users may desire a greater degree of randomness in cryptosystem parameters. Such users will prefer more flexibility with regard to the CM discriminant, in particular to be able to have variable discriminants within a family of curves. This is achieved through Theorem 6.19, which, given a parametric family of curves with fixed discriminant that satisfies certain conditions, allows us to build a family of curves with variable square-free CM discriminant and the same ρ-value. Thus, combining a basic construction with Theorem 6.19 yields a general method for constructing families of curves with variable CM discriminant and $\rho < 2$. Previous constructions with variable discriminant required either $\rho \geq 2$ or $k \leq 6$.

In Sect. 6.4 we use Theorem 6.19 to give examples of variable-discriminant parametric families for any embedding degree k satisfying $\gcd(k, 24) \in \{1, 2, 3, 6, 12\}$. In particular, Constructions 6.20 and 6.24 combine Theorem 6.19 with the method of Brezing

and Weng to give new families of curves for $k \equiv 3 \pmod 4$ and $k \equiv 2 \pmod 8$, respectively. When k is not divisible by 3, these families have ρ-value smaller than that of any other known variable-discriminant complete family with the same embedding degree. Furthermore, the families with $k \equiv 10 \pmod{24}$ and $k \geq 34$ have ρ-value smaller than any other known complete family with the same embedding degree, with either fixed (in advance) or variable discriminant. Table 5 lists the variable-discriminant family with smallest ρ-value for each $k \leq 50$.

1.4. *Recommendations*

The body of this paper gathers in one place for the first time all known methods for constructing pairing-friendly elliptic curves. In Sect. 8 we distill this information into recommendations for users wishing to implement pairing-based protocols. As requirements for security and performance will vary from system to system, we provide several different recommendations among which users will choose according to their needs.

Section 8.1 discusses our recommendations for the case where minimizing ρ is not necessary; in general we recommend the Cocks–Pinch method (Theorem 4.1).

Section 8.2 considers the case where we wish to minimize ρ. We summarize our recommendations in Table 5. For each embedding degree k, $1 \leq k \leq 50$, the table gives two options: a parametric family of curves with CM discriminant 1 or 3, and a parametric family of curves with variable CM discriminant, both of which minimize ρ in their respective category. In general, we recommend the former to users for whom performance is paramount, and the latter to users who are suspicious of curves with small CM discriminant.

Our families are described in terms of polynomials whose values give the field size and subgroup size for the pairing-friendly curve, and the ρ-value of a family is defined in terms of these polynomials. In each case we have checked that our families can be used to produce explicit curves and that the ρ-values of these curves are very close to the ρ-value of the family.

Section 8.3 considers the case where we wish to take advantage of certain techniques for speeding up pairing evaluation. These techniques, discussed in Sect. 7, offer the greatest improvement when the embedding degree is of the form $k = 2^i 3^j$. Table 6 gives a recommended family of curves for each such embedding degree less than 50.

Finally, Sect. 8.4 discusses curves with subgroups whose orders are composite numbers that are presumed to be infeasible to factor. Such curves, first proposed for use by Boneh, Goh, and Nissim [14], are used in a number of recent protocols and are an active subject of research.

2. How to Generate Pairing-Friendly Curves

We assume that the reader is familiar with elliptic curves and finite fields; for a good exposition of the former, see Silverman's book [82], and for the latter, see the book of Lidl and Niederreiter [55]. We begin by fixing some notation related to elliptic curves. Let E be an elliptic curve defined over a field K; we may also use E/K (read "E over K") to denote such a curve. We denote by $E(K)$ the group of K-rational points of E and by $\#E(K)$ the order of this group when it is finite. For any integer r, we let $E[r]$ denote the group of all r-torsion points of E (defined over an algebraic closure $\overline{K}$ of K) and by $E(K)[r]$ the group of r-torsion points of E that are defined over K.

For any prime power q, we let $\mathbb{F}_q$ denote the field of q elements. If E is an elliptic curve over $\mathbb{F}_q$, we define the *trace* of $E/\mathbb{F}_q$ to be $t = q + 1 - \#E(\mathbb{F}_q)$. A theorem of Hasse (the "Hasse bound") says that $|t| \leq 2\sqrt{q}$ [82, Theorem V.1.1]. If $\gcd(t, q) = 1$, the elliptic curve E is said to be *ordinary*; otherwise E is *supersingular*. (For a multitude of equivalent definitions of supersingularity, see [82, Theorem V.3.1].)

Let E/K be an elliptic curve. If the ring of $\overline{K}$-endomorphisms of E, denoted $\mathrm{End}(E)$, is strictly larger than $\mathbb{Z}$, then we say that E has *complex multiplication* or that E is a *CM curve*. All elliptic curves over finite fields are CM curves, with $\mathrm{End}(E) \otimes \mathbb{Q}$ isomorphic to either a quadratic imaginary field (if E is ordinary) or a quaternion algebra (if E is supersingular). If $E/\mathbb{F}_q$ is ordinary, we define the *complex multiplication discriminant* (or *CM discriminant*) of E to be the square-free part D of the nonnegative integer $4q - t^2$. (Other authors may define the CM discriminant to be negative, or to be the discriminant of the quadratic imaginary field $\mathbb{Q}(\sqrt{-D})$.) With this definition, we have $\mathrm{End}(E) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{-D})$. By abuse of notation, we may extend this definition to supersingular curves $E/\mathbb{F}_q$, but in this case D has no relation to $\mathrm{End}(E)$.

The original application of pairings to cryptography, due to Menezes, Okamoto, and Vanstone [62] and Frey and Rück [34], was the use of the Weil or Tate pairing (respectively) to reduce the discrete logarithm problem in the group of points on an elliptic curve to a discrete logarithm problem in the multiplicative group of a finite field. As these pairings are bilinear and nondegenerate, they can be used to "embed" a subgroup of an elliptic curve into a subgroup of the multiplicative group of a finite field.

It is well known from the theory of elliptic curves that if E is an elliptic curve defined over a field K and r is an integer prime to $\mathrm{char}\, K$, the Weil pairing is a nondegenerate bilinear map

$$e_r : E[r] \times E[r] \to \mu_r \subset \overline{K},$$

where μ_r is the group of rth roots of unity in $\overline{K}$ [82, Sect. III.8]. If the group $E(K)[r]$ is cyclic, the nondegeneracy of the pairing allows us to "embed" $E(K)[r]$ into the multiplicative group of the extension field $K(\mu_r)$. We call the degree of this extension the "embedding degree" of E.

Definition 2.1. Let E be an elliptic curve defined over a field K, and suppose E has a K-rational point of order r with $\gcd(r, \mathrm{char}\, K) = 1$. The *embedding degree of E with respect to r* is the extension degree $[K(\mu_r) : K]$.

Remark 2.2. If K is a finite field $\mathbb{F}_q$ and $r \mid \#E(\mathbb{F}_q)$ is relatively prime to q, the following three conditions are equivalent:

(1) E has embedding degree k with respect to r.
(2) k is the smallest integer such that r divides $q^k - 1$.
(3) k is the order of q in $(\mathbb{Z}/r\mathbb{Z})^\times$.

We often ignore r when stating the embedding degree, as it is usually clear from the context.

Hitt [43] observed that when $q = p^m$, the Weil and Tate pairings take values in the field $F = \mathbb{F}_p(\mu_r)$. The field F is called the *minimum embedding field* of E with respect

to r. If q is not prime, then F may be a proper subfield of $\mathbb{F}_{q^k}$. Since the security of a pairing-based cryptosystem depends on the difficulty of the discrete logarithm in $F^\times$, in these cases one must be careful to choose parameters so that F is sufficiently large. On the other hand, since most of the curves we consider are defined over prime fields, we may safely ignore this result for the bulk of our discussion. We will however take this observation into account when discussing supersingular curves defined over non-prime fields (Sect. 3).

For constructive applications of pairings, the embedding degree of E needs to be small enough so that the pairing is easy to compute but large enough so that the discrete logarithm in $\mathbb{F}_{q^k}^\times$ is computationally infeasible. Balasubramanian and Koblitz [3] showed that for a random elliptic curve E over a random field $\mathbb{F}_q$ and a prime $r \approx q$, the probability that E has embedding degree less than $\log^2 q$ with respect to r is vanishingly small, and in general the embedding degree can be expected to be around r. Luca, Mireles, and Shparlinski [57] have obtained similar results for fixed values of q. These results imply that if r and q are both of size around 2^{160} (the smallest values currently acceptable for security in implementations), pairings on a random curve take values in a field of around 2^{160} bits, so the computation is completely hopeless.

To avoid the Pohlig–Hellman attack [71], the points on $E(\mathbb{F}_q)$ used in cryptographic protocols should have prime order. Our problem is thus to find elliptic curves that have large prime-order subgroups and small embedding degrees. Such curves are commonly referred to as "pairing-friendly," but this term has never been formally defined. We make the notion precise in the following definition.

Definition 2.3. Suppose E is an elliptic curve defined over a finite field $\mathbb{F}_q$. We say that E is *pairing-friendly* if the following two conditions hold:

(1) there is a prime $r \geq \sqrt{q}$ dividing $\#E(\mathbb{F}_q)$, and
(2) the embedding degree of E with respect to r is less than $\log_2(r)/8$.

In this definition, the bound on the subgroup size r is based on the result, due to Luca and Shparlinski [56], that curves having small embedding degree with respect to r are abundant if $r < \sqrt{q}$ and quite rare if $r > \sqrt{q}$. The bound on the embedding degree is based on the rationale that embedding degrees of practical interest in pairing-based applications depend on the desired security level, of which r is a clear measure. In particular, the bound $\log_2(r)/8$ is chosen to *roughly* reflect the bounds on k given in Table 1.

Recently a number of pairing-based protocols have been proposed that require elliptic curves $E/\mathbb{F}_q$ that have small embedding degree with respect to a large composite number r of known factorization, such as an RSA modulus. By analogy with Definition 2.3, we will say that such an E is pairing-friendly if $r > \sqrt{q}$ and the embedding degree of E with respect to r is less than $\log_2(r)/8$.

Since supersingular elliptic curves have embedding degree 2 over prime fields $\mathbb{F}_p$ with $p \geq 5$ and have embedding degree at most 6 in any case [62], a supersingular curve is always pairing-friendly if it has a large prime-order subgroup. Section 3 discusses supersingular curves in more detail.

If we want to vary the embedding degree to achieve higher security levels, we must construct pairing-friendly ordinary elliptic curves. This turns out to be a difficult task.

There are a number of methods in the literature for constructing such curves, all of which follow essentially the same high-level structure:

(1) Fix k and compute integers t, r, q such that there is an elliptic curve $E/\mathbb{F}_q$ that has trace t, a subgroup of prime order r, and embedding degree k.
(2) Use the *complex multiplication method* to find the equation of the curve E over $\mathbb{F}_q$.

The difficult part of such algorithms is finding t, r, q as in Step (1) while ensuring that Step (2) remains feasible.

An ordinary elliptic curve with these properties can be constructed if and only if the following conditions hold:

(1) q is prime or a prime power.
(2) r is prime.
(3) t is relatively prime to q.
(4) r divides $q + 1 - t$.
(5) r divides $q^k - 1$, and $r \nmid q^i - 1$ for $1 \leq i < k$.
(6) $4q - t^2 = Dy^2$ for some sufficiently small positive integer D and some integer y.

Condition (1) ensures that there is a finite field with q elements. Since the proportion of prime powers to primes is virtually zero, we will in general take q to be a prime number. Condition (6) implies that $t \leq 2\sqrt{q}$; together with condition (3), this implies that there exists an ordinary elliptic curve E defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$ (cf. [88, Theorem 4.1]). Conditions (2) and (4) combine to tell us that $E(\mathbb{F}_q)$ has a subgroup of prime order r. By Remark 2.2, condition (5) is equivalent to E having embedding degree k with respect to r.

We now know that if such t, r, q can be constructed, then there exists an ordinary elliptic curve $E/\mathbb{F}_q$ with embedding degree k and an order-r subgroup. The requirement that D be sufficiently small in condition (6) is necessary for us to be able to find the equation of such a curve. The method we use is the *complex multiplication (CM) method* of curve construction, due originally to Atkin and Morain [1]. The CM method, which was devised for use in primality testing, constructs a curve with endomorphism ring isomorphic to a given order $\mathcal{O}$ in a quadratic imaginary field $\mathbb{Q}(\sqrt{-D})$ and can be used to construct a curve with a specified number of points. The complexity of the method is $O(|D_{\mathcal{O}}|^{1+\epsilon})$, where $D_{\mathcal{O}}$ is the discriminant of the order $\mathcal{O}$ [18,29]. Given current computational power, the method can construct curves over finite fields when $|D_{\mathcal{O}}| \leq 10^{12}$ [83]. In practice we can always take $\mathcal{O}$ to be the ring of integers in $\mathbb{Q}(\sqrt{-D})$, in which case $|D_{\mathcal{O}}| = D$ or $4D$ and D is the CM discriminant of the resulting curve. Thus we see that "sufficiently small" in condition (6) can be taken to be $D < 10^{12}$.

The equation in condition (6) is called the *CM equation*. If we use condition (4) to write $q + 1 - t = hr$ for some h, then the CM equation is equivalent to

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

We call h the *cofactor* of the pairing-friendly curve.

Constructions of pairing-friendly curves make substantial use of the theory of cyclotomic polynomials and cyclotomic fields. We recall a few basic facts here; for a deeper

discussion, see Lidl and Niederreiter's book [55]. For every positive integer k, we let ζ_k denote a primitive kth root of unity in $\overline{\mathbb{Q}}$, i.e., an algebraic number such that $(\zeta_k)^k = 1$ and $(\zeta_k)^\ell \neq 1$ for any positive $\ell < k$. The minimal polynomial of ζ_k is known as the *kth cyclotomic polynomial* and is denoted $\Phi_k(x)$. These polynomials have integer coefficients and can be defined recursively by setting $\Phi_1(x) = x - 1$ and using the formula

$$x^k - 1 = \prod_{d|k} \Phi_d(x) \tag{2.2}$$

for $k > 1$. The degree of $\Phi_k(x)$ is denoted $\varphi(k)$ and is also called *Euler's totient function*; it gives the number of positive integers less than or equal to k that are relatively prime to k.

The following observation is crucial for the construction of prime-order curves with embedding degree k.

Proposition 2.4. *Let k be a positive integer, $E/\mathbb{F}_q$ an elliptic curve with $\#E(\mathbb{F}_q) = hr$ where r is prime, and let t be the trace of $E/\mathbb{F}_q$. Assume that $r \nmid kq$. Then $E/\mathbb{F}_q$ has embedding degree k with respect to r if and only if $\Phi_k(q) \equiv 0 \pmod{r}$, or, equivalently, if and only if $\Phi_k(t-1) \equiv 0 \pmod{r}$.*

Proof. Let us first assume that E has embedding degree k with respect to r. Then $r \mid q^k - 1$ but $r \nmid q^i - 1$ for any $1 \leq i < k$. By (2.2) and since r is prime, this means $r \mid \Phi_k(q)$. Now, since $q + 1 - t = hr$, $q \equiv t - 1 \pmod{r}$, so $r \mid \Phi_k(t-1)$.

Conversely, if $r \mid \Phi_k(t-1)$, then $r \mid \Phi_k(q)$ and thus $r \mid q^k - 1$; this means that $E/\mathbb{F}_q$ has embedding degree at most k. It remains to show that $r \nmid q^i - 1$ for any $1 \leq i < k$. We follow Menezes' proof [60, Lemma 6.2]. Let $f(x) = x^k - 1$ and $\mathbb{F} = \mathbb{Z}/r\mathbb{Z}$. Then $\mathbb{F}$ is a field. Since $r \nmid k$, we have $\gcd(f(x), f'(x)) = 1$ in $\mathbb{F}[x]$. Thus, f has only single roots in $\mathbb{F}$. Using (2.2) and the fact that q is a root of $\Phi_k(x)$ over $\mathbb{F}$, we obtain $\Phi_d(q) \not\equiv 0 \pmod{r}$ for any $d \mid k$, $1 \leq d < k$. Therefore, $r \nmid q^d - 1$ for any $d \mid k$, $1 \leq d < k$. Finally, we note that $r \nmid q^i - 1$ for any positive i that does not divide k, since in this case we would have $r \mid q^{\gcd(i,k)} - 1$. □

Proposition 2.4 tells us that we can replace condition (5) necessary to construct a pairing-friendly curve with the following:

(5′) r divides $\Phi_k(t-1)$.

2.1. *Families of Pairing-Friendly Curves*

For applications, we would like to be able to construct curves of specified bit size. To this end, we describe "families" of pairing-friendly curves for which the curve parameters t, r, q are given as polynomials $t(x), r(x), q(x)$ in terms of a parameter x. The idea of parameterizing t, r, q as polynomials has been used by several different authors in their constructions, including Miyaji, Nakabayashi, and Takano [64]; Barreto, Lynn, and Scott [5]; Scott and Barreto [81]; and Brezing and Weng [17]. Our definition of a family of pairing-friendly curves is a formalization of ideas implicit in these works. The definition provides a concise description of many existing constructions and gives us a framework that we can use to discover previously unknown pairing-friendly curves.

Since the values of $q(x)$ and $r(x)$ will be the sizes of a field and a group in which we wish to do cryptography, respectively, the polynomials we construct will need to have the property that for many values of x, $q(x)$ is a prime power (which in general we will take to be a prime), and $r(x)$ is prime or a small cofactor times a prime. However, one drawback to the description of q and r as polynomials is that very little is known about prime values of polynomials. For example, it is not even known that $x^2 + 1$ takes an infinite number of prime values. Thus when describing the polynomials that we wish to take prime values, we must impose conditions that make it likely that they will do so.

Our definition is motivated by the following fact: if $f(x) \in \mathbb{Z}[x]$, then a famous conjecture of Buniakowski and Schinzel (see [53, p. 323]) asserts that a nonconstant $f(x)$ takes an infinite number of prime values if and only if f has positive leading coefficient, f is irreducible, and $\gcd(\{f(x) : x \in \mathbb{Z}\}) = 1$. Furthermore, a conjecture of Bateman and Horn [9] vastly generalizes the prime number theorem to give the expected density of such prime values. For our purposes, we must also consider polynomials with rational coefficients; our definition incorporates the natural generalization of these conjectures to such polynomials.

Definition 2.5. Let $f(x)$ be a polynomial with rational coefficients. We say that f *represents primes* if the following conditions are satisfied:

(1) $f(x)$ is nonconstant.
(2) $f(x)$ has positive leading coefficient.
(3) $f(x)$ is irreducible.
(4) $f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$ (equivalently, for an infinite number of $x \in \mathbb{Z}$).
(5) $\gcd(\{f(x) : x, f(x) \in \mathbb{Z}\}) = 1$.

Clearly each of the conditions of Definition 2.5 is necessary for f to take an infinite number of prime values; their sufficiency is conjectural. We note that testing whether a polynomial $f(x)$ represents primes is a finite calculation: condition (4) can be tested by computing $f(x)$ for all integers $x \in [0, N)$ for some N such that $N \cdot f(x) \in \mathbb{Z}[x]$, while condition (5) can be tested by computing some $f(n) \in \mathbb{Z}$ and determining whether $f(x)$ is identically zero mod p for all primes p dividing $f(n)$. In addition, if either $f(x) = \pm 1$ for some x or $f(x)$ takes two distinct prime values, then conditions (4) and (5) are both satisfied.

We need one more definition before we can define families of pairing-friendly curves.

Definition 2.6. A polynomial $f(x) \in \mathbb{Q}[x]$ is *integer-valued* if $f(x) \in \mathbb{Z}$ for every $x \in \mathbb{Z}$.

For example, $f(x) = \frac{1}{2}(x^2 + x + 2)$ is integer-valued and represents primes.

Definition 2.7. Let $t(x)$, $r(x)$, and $q(x)$ be nonzero polynomials with rational coefficients.

(i) For a given positive integer k and positive square-free integer D, the triple (t, r, q) *parameterizes a family of elliptic curves with embedding degree k and discriminant D* if the following conditions are satisfied:

(1) $q(x) = p(x)^d$ for some $d \geq 1$ and $p(x)$ that represents primes.
(2) $r(x)$ is nonconstant, irreducible, and integer-valued and has positive leading coefficient.
(3) $r(x)$ divides $q(x) + 1 - t(x)$.
(4) $r(x)$ divides $\Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial.
(5) The equation $Dy^2 = 4q(x) - t(x)^2$ has infinitely many integer solutions (x, y).

If these conditions are satisfied, we often refer to the triple (t, r, q) as a *family*.

(ii) For (t, r, q) as in (i), if x_0 is an integer and E is an elliptic curve over $\mathbb{F}_{q(x_0)}$ with trace $t(x_0)$, then we say E is a *curve in the family* (t, r, q).
(iii) We say that a family (t, r, q) is *ordinary* if $\gcd(t(x), q(x)) = 1$.
(iv) We say that a family (t, r, q) is *complete* if there is some $y(x) \in \mathbb{Q}[x]$ such that $Dy(x)^2 = 4q(x) - t(x)^2$; otherwise we say that the family is *sparse*.
(v) We say that (t, r, q) parameterizes a *potential* family of curves if conditions (2)–(5) of (i) are satisfied; in this case $p(x)$ may or may not represent primes.

Part (i) of Definition 2.7 is designed so that if (t, r, q) parameterizes a family of curves with embedding degree k, and (x_0, y_0) is a solution to the equation of condition (5) such that $t(x_0)$ is an integer and $p(x_0)$ is an integer prime, then there exists an elliptic curve $E/\mathbb{F}_{q(x_0)}$ with a subgroup of order $r(x_0)$ and embedding degree k. If $D < 10^{12}$, then E can be constructed via the CM method. All of the ordinary families we describe below have $d = 1$ in condition (1), so $q(x)$ will represent primes and the curves we construct will be defined over prime fields. However, we do allow $d > 1$ in order to fit the supersingular curves of Sect. 3.3 into this framework as well as to accommodate any future constructions over non-prime fields.

We note that it may happen that a triple (t, r, q) satisfying Definition 2.7(i) does not lead to any explicit examples of elliptic curves; for example, if $t(x)$ is never an integer simultaneously with $q(x)$. However, all of the families we present in this paper have been shown to produce explicit examples of pairing-friendly elliptic curves for certain values of x.

In addition to finding an x_0 such that $q(x_0)$ is prime, for cryptographic applications, we also need $r(x_0)$ to be prime or very nearly prime. The conditions (2) on $r(x)$ suggest that this will often be the case. Assuming that the Bateman–Horn conjecture is true, by fixing a y_0 and choosing values of x_0 near y_0, the expected time needed to find an x_0 with the necessary properties grows linearly in $\deg q$ and $\deg r$ and quadratically in $\log y_0$; see [32, Algorithm 4.1 and Proposition 4.2] for details.

Condition (3) of Definition 2.7(i) ensures that for a given value of x for which $q(x)$ is prime, $r(x)$ divides $\#E(\mathbb{F}_{q(x)})$. If in fact $r(x) = q(x) + 1 - t(x)$, then for values of x for which $r(x)$ and $q(x)$ are both prime, $\#E(\mathbb{F}_q)$ will be prime. This is the ideal case, but it is difficult to achieve in practice. We therefore define a parameter ρ that represents how close to this ideal a given curve or family of curves is. This parameter expresses the ratio of the size q of the field to the size r of the prime-order subgroup of $E(\mathbb{F}_q)$.

Definition 2.8.

(i) Let $E/\mathbb{F}_q$ be an elliptic curve, and suppose that E has a subgroup of order r. The *ρ-value of E (with respect to r)* is

$$\rho(E) = \frac{\log q}{\log r}.$$

(ii) Let $t(x), r(x), q(x) \in \mathbb{Q}[x]$, and suppose that (t, r, q) parameterizes a family (or potential family) of elliptic curves with embedding degree k. The *ρ-value of* (t, r, q), denoted $\rho(t, r, q)$, is

$$\rho(t, r, q) = \lim_{x \to \infty} \frac{\log q(x)}{\log r(x)} = \frac{\deg q(x)}{\deg r(x)}.$$

By Definition 2.3, pairing-friendly curves have $\rho(E) \leq 2$. On the other hand, the Hasse bound $|\#E(\mathbb{F}_q) - q + 1| \leq 2\sqrt{q}$ implies that $\rho(t, r, q)$ is always at least 1. (For individual curves, $\rho(E) \geq 1 - \frac{2\log 2}{\log r}$.) If there are curves in the family (t, r, q) whose order is prime, then $\deg r = \deg q$ and $\rho(t, r, q) = 1$; this is the "ideal" case. Note, however, that the converse may not be true: if $\rho(t, r, q) = 1$, then we may find that for any curve E in this family, $\#E(\mathbb{F}_q) = hr(x)$ where h is a constant-size cofactor. (For examples of such families, see [36, Sect. 3].)

We conclude this section by demonstrating some properties of ρ for ordinary elliptic curves with embedding degree 1 or 2.

Proposition 2.9. *Suppose that (t, r, q) parameterizes a family of ordinary elliptic curves with embedding degree $k \leq 2$ and discriminant D.*

(1) *If $k = 1$, then $\rho(t, r, q) \geq 2$ if either of the following conditions holds*:
   (a) $\deg t(x) \geq 1$, *or*
   (b) *there are an infinite number of integer solutions (x, y) to the CM equation (2.1) for which $r(x)$ is square free and relatively prime to D.*

(2) *If $k = 2$, then $\rho(t, r, q) \geq 2$.*

Proof. Since $r(x)$ divides $\Phi_k(t(x) - 1)$ and $\deg \Phi_k = 1$ for $k = 1$ or 2, if $\Phi_k(t(x) - 1) \neq 0$, then we must have $\deg t(x) \geq \deg r(x)$. Thus by the Hasse bound $\rho(t, r, q) \geq 2$. It remains to consider the cases $k = 1, t(x) = 2$ and $k = 2, t(x) = 0$. If $t(x) = 0$, then the family of curves is not ordinary, a contradiction. Now suppose $k = 1$ and $t(x) = 2$; then the CM equation (2.1) becomes $Dy^2 = 4h(x)r(x)$. The hypothesis (b) implies that there are an infinite number of x for which $h(x) \geq r(x)$, and therefore $\deg h(x) \geq \deg r(x)$. Since $\deg q(x) = \deg h(x) + \deg r(x)$, we conclude that $\rho \geq 2$. □

Remark 2.10. Let $E/\mathbb{F}_q$ be an ordinary elliptic curve that has embedding degree $k \leq 2$ with respect to r, and let D be the CM discriminant of E. Using the same reasoning as in the proof of Proposition 2.9, one can show that if either

(1) $k = 1$, r is square free, and $\gcd(r, D) = 1$, or
(2) $k = 2$ and r is prime,

then $\rho(E) \geq 2(1 - \varepsilon)$ with $\varepsilon \to 0$ as $r \to \infty$.

3. Supersingular Curves

Recall that an elliptic curve $E/\mathbb{F}_q$ (where $q = p^s$ for some prime p and $s \in \mathbb{N}$) with $\#E(\mathbb{F}_q) = q + 1 - t$ is *supersingular* if and only if $\gcd(t, q) > 1$. Waterhouse [88, Theorem 4.1] showed that group orders of supersingular elliptic curves are of the form $q + 1 - t$ with $t^2 \in \{0, q, 2q, 3q, 4q\}$. It follows directly from this result that supersingular curves have embedding degrees $k \in \{1, 2, 3, 4, 6\}$, and furthermore $k = 2$ is the only possible embedding degree over prime fields $\mathbb{F}_q$ with $q \geq 5$ [62]. Menezes [59] has characterized prime-order supersingular curves with embedding degrees $k = 3, 4, 6$. For fields of characteristic 2 and 3, representatives for each $\mathbb{F}_q$-isomorphism class of supersingular curves have been determined by Menezes and Vanstone [61] and Morain [65], respectively.

The only known general method to construct supersingular curves is reduction of CM curves in characteristic zero. In particular, the CM curves $y^2 = x^3 + ax$ and $y^2 = x^3 + b$ defined over $\mathbb{Q}$ reduce to supersingular curves over $\mathbb{F}_p$ for all odd primes $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$, respectively. These two curves will suffice for most applications; Algorithm 3.3 gives an explicit procedure for constructing a supersingular curve over any given prime field.

As supersingular curves with embedding degree $k \neq 2$ cannot be defined over prime fields, in this section we consider non-prime fields a well as prime fields. For efficiency reasons, we restrict ourselves to non-prime fields of characteristic 2 or 3 and fields of the form $\mathbb{F}_{p^2}$ for large primes p; we give data for characteristic 3 fields only if no constructions for characteristic 2 fields or for prime fields exist. (Note, however, that due to Coppersmith's index calculus method for discrete logarithm computation in finite fields of small characteristic [24], the fields $\mathbb{F}_q$ must be larger when $q = 2^s$ or 3^s than when $q = p$ or p^2.) When discussing non-prime fields we must take into account the work of Hitt [43] and consider how the minimal embedding field $\mathbb{F}_{p^{k'}}$ (i.e., the field in which the Weil and Tate pairings take their values) compares to the field $\mathbb{F}_{q^k}$ determined by the embedding degree.

Remark 3.1. Due to the perception of the Menezes–Okamoto–Vanstone and Frey–Rück reductions [34,62] as "attacks," supersingular curves are widely believed to be "weak" curves and thus not desirable for cryptographic applications. However, Koblitz and Menezes argue [51]:

> There is no known reason why a nonsupersingular curve with small embedding degree k would have any security advantage over a supersingular curve with the same embedding degree.

On the other hand, in contrast to ordinary curves with embedding degree $k > 1$, supersingular curves have the added advantage that they have distortion maps (in the sense of Verheul [87]), which is a desirable feature in some pairing-based applications. See Sect. 7.2 or [21] for further details.

3.1. *Embedding Degree* $k = 1$

Supersingular curves with embedding degree $k = 1$ exist only over finite fields $\mathbb{F}_q$ where $q = p^s$ with s even [62]. In this case we must have $t = \pm 2\sqrt{q}$, and thus $\#E(\mathbb{F}_q) =$

$q \pm 2\sqrt{q} + 1$. Since the subgroup order r must divide both $\#E(\mathbb{F}_q)$ and $\Phi_k(1) = q - 1$, we see that r is a factor of $\gcd(\#E(\mathbb{F}_q), q - 1) = \sqrt{q} \pm 1$, and therefore such curves must have $\rho \geq 2$.

To construct supersingular curves with embedding degree 1, we let $q' = \sqrt{q}$ and let $E/\mathbb{F}_{q'}$ be a curve with trace zero, i.e., $\#E(\mathbb{F}_{q'}) = q' + 1$. Then the characteristic polynomial of the q'-power Frobenius endomorphism is $x^2 + q'$, which factors as $(x + i\sqrt{q'})(x - i\sqrt{q'})$, where $i = \sqrt{-1}$. The Weil conjectures [82, Theorem V.2.2] then tell us that the characteristic polynomial of the q-power Frobenius map is $(x + q')^2$, so $\#E(\mathbb{F}_q) = (q' + 1)^2 = q + 2\sqrt{q} + 1$. Thus even though $E/\mathbb{F}_{q'}$ has embedding degree 2, if we consider E as a curve over $\mathbb{F}_q$, then E has embedding degree 1 with respect to r. We note that if q' is prime, then $\mathbb{F}_q$ is also the minimal embedding field for E with respect to r.

We will see in Algorithm 3.3 below how to construct a trace-zero curve over $\mathbb{F}_{q'}$ with an order-r subgroup for arbitrary r. Since we may take $\log q'/\log r$ arbitrarily close to 1 for such curves, the ρ-value of $E/\mathbb{F}_q$ with embedding degree 1 can be made arbitrarily close to 2, and we see from the discussion above that this is the best possible ρ-value. We conclude that in any case where a supersingular curve $E/\mathbb{F}_q$ with $k = 1$ and $\rho(E) = \rho_0$ is desired, we may obtain an entirely equivalent setup by choosing a supersingular curve $E'/\mathbb{F}_{\sqrt{q}}$ with $k = 2$ and $\rho(E') = \rho_0/2$.

As a side note, if we let E' be a quadratic twist (over $\mathbb{F}_q$) of the curve with $q + 2\sqrt{q} + 1$ points, then $\#E'(\mathbb{F}_q) = q - 2\sqrt{q} + 1$. This curve also has embedding degree 1 over $\mathbb{F}_q$, but in fact since $\#E'(\mathbb{F}_q) = (p - 1)^2$, the minimal embedding field is $\mathbb{F}_p$. Thus the twisted curve can be thought of as having "embedding degree 1/2": the curve is defined over $\mathbb{F}_q$, but the Weil and Tate pairings take values in a field half the size of $\mathbb{F}_q$.

3.2. *Embedding Degree $k = 2$*

The case of embedding degree 2 offers the most flexibility; in fact, we can construct curves over prime fields with arbitrary subgroup order r and arbitrary ρ-value. For embedding degree $k = 2$, we require $r \mid q + 1$. This is certainly the case if $t = 0$, and such supersingular curves can be defined over both prime and non-prime fields.

In fields of characteristic 2 or 3, there is only one supersingular curve up to $\overline{\mathbb{F}}_q$-isomorphism, namely, the curve with j-invariant zero [82, Sect. 5.4]. Explicitly, in fields $\mathbb{F}_q$ of characteristic 2, the trace-zero supersingular curves over $\mathbb{F}_q$ are

$$E/\mathbb{F}_q : y^2 + y = x^3 + \delta x$$

if $q = 2^s$ with s even, where $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_4}\, \delta \neq 0$, and

$$E/\mathbb{F}_q : y^2 + y = x^3$$

if $q = 2^s$ with s odd [61]. If either $\rho < 3(1 - 1/\log_2 r)$ or s is prime and $r > 3$, then $\mathbb{F}_{q^2}$ is also the minimal embedding field for E with respect to r [10, Proposition 3.5].

Construction of supersingular curves over prime fields of characteristic greater than 3 makes use of the following theorem:

Theorem 3.2 [52, Theorem 13.12]. *Let L be a number field, and E/L be an elliptic curve with complex multiplication. Suppose* $\mathrm{End}_L(E) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-D})$. *Let $\mathfrak{p} \mid p$ be a prime of L where E has good reduction. Then the reduction of $E \bmod \mathfrak{p}$ is supersingular if and only if $\mathfrak{p}$ does not split in $\mathbb{Q}(\sqrt{-D})$, i.e., $(\frac{-D}{p}) \neq 1$.*

Given a subgroup size r, if we choose any h such that $q = hr - 1$ is prime, then we have the following algorithm (combining the constructions of Koblitz and Menezes [51, Sect. 7] and Bröker [18, Sect. 3.4]) for constructing a curve over $\mathbb{F}_q$ with embedding degree 2 with respect to r.

Algorithm 3.3. Input: a prime $q \geq 5$. Output: a supersingular elliptic curve $E/\mathbb{F}_q$.

(1) If $q \equiv 3 \pmod 4$, return $y^2 = x^3 + ax$ for any $a \in \mathbb{F}_q^\times$ with $-a \notin (\mathbb{F}_q^\times)^2$.
(2) If $q \equiv 5 \pmod 6$, return $y^2 = x^3 + b$ for any $b \in \mathbb{F}_q^\times$.
(3) If $q \equiv 1 \pmod{12}$, do the following:
   (a) Let D be the smallest prime such that $D \equiv 3 \pmod 4$ and $(\frac{-D}{q}) = -1$.
   (b) Compute the Hilbert class polynomial H_D of $\mathbb{Q}(\sqrt{-D})$.
   (c) Compute a root $j \in \mathbb{F}_q$ of $H_D \pmod q$.
   (d) Let $m = j/(1728 - j)$, and return $y^2 = x^3 + 3mc^2x + 2mc^3$ for any $c \in \mathbb{F}_q^\times$.

Assuming the Generalized Riemann Hypothesis, the running time of the algorithm is $O((\log p)^{3+\epsilon})$ for any $\epsilon > 0$ [18, Theorem 3.8]. The requirement in Step (1) that $-a$ be a nonsquare in $\mathbb{F}_q^\times$ guarantees that $E[2] \not\subset E(\mathbb{F}_q)$, so E has embedding degree 2 with respect to the subgroup of order 2 [62, Lemma 2]. The condition $D \equiv 3 \pmod 4$ in Step (a) guarantees that the Hilbert class polynomial H_D has a root in $\mathbb{F}_q$ [18, Sect. 3.4].

Note that this construction allows us to choose r and h almost completely arbitrarily, so we may make our choices so that r and q have low Hamming weight or some other special form. (However, we may want to avoid q with low Hamming weight; see Sect. 7.5 for details.) In particular, Boneh, Goh, and Nissim [14] observe that we may choose r to be a large composite number such as an RSA modulus. Furthermore, by fixing any $\rho_0 \geq 1$ and choosing $h \approx r^{\rho_0 - 1}$, we may ensure that the curve constructed has ρ-value very close to ρ_0.

We see from Theorem 3.2 that the popular supersingular curves $y^2 = x^3 + ax$ and $y^2 = x^3 + b$ are simply special cases of the general construction method, for the two equations define CM curves over $\mathbb{Q}$ with endomorphism rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta_3]$, respectively. However, these two cases have the additional nice property that the distortion maps are easy to compute, as both curves have automorphisms defined over $\mathbb{F}_{q^2}$. Koblitz and Menezes [51] give explicit determinations of the distortion maps in both cases.

3.3. *Embedding Degree $k = 3$*

A supersingular curve over $\mathbb{F}_q$ has embedding degree $k = 3$ with respect to a subgroup of prime order $r > 3$ if and only if $q = p^s$ with s even, and $t = \pm\sqrt{q}$ [64]. In characteristic $p > 3$, the only such curves are those of the form

$$E/\mathbb{F}_q : y^2 = x^3 + \gamma,$$

where γ is a non-cube in $\mathbb{F}_q^\times$ [65]. If we specialize to the case $q = p^2$ where $p \equiv 2 \pmod 3$ is a large prime, then we have $\#E(\mathbb{F}_{p^2}) = p^2 \pm p + 1$. If the sign of the middle term is positive (i.e., $t = -p$), then for certain $p = 3x - 1$, we may find curves of prime order, since $r(x) = (3x-1)^2 + (3x-1) + 1$ represents primes in the sense of Definition 2.5. In the case where $t = p$ we find that $\#E(\mathbb{F}_q)$ must be a multiple of 3 but can be equal to 3 times a prime.

We can recast these results in our language of "families" (Definition 2.7). Depending on the sign of t, we have one of

$$\begin{aligned} t(x) &= -3x + 1, \qquad r(x) = 9x^2 - 3x + 1, \qquad q(x) = (3x-1)^2; \\ t(x) &= 3x - 1, \qquad r(x) = 9x^2 - 9x + 3, \qquad q(x) = (3x-1)^2. \end{aligned} \tag{3.1}$$

Since $4q(x) - t(x)^2 = 3(3x-1)^2$, the triple (t, r, q) parameterizes a family of elliptic curves with embedding degree 3 and discriminant 3. The ρ-value of this family is 1. In particular, if $r(x_0)$ and $3x_0 - 1$ are prime for some $x_0 \in \mathbb{Z}$, then we may construct a curve over $\mathbb{F}_{q(x_0)}$ with embedding degree 3 and prime order. Since $\#E(\mathbb{F}_{p^2})$ is equal to $\Phi_6(p)$ if $t > 0$ and $\Phi_3(p)$ if $t < 0$, we see that the minimal embedding field is $\mathbb{F}_{p^6} = \mathbb{F}_{q^3}$ in the first case and $\mathbb{F}_{p^3} = \mathbb{F}_{q^{3/2}}$ in the second case.

Since arithmetic in $\mathbb{F}_{p^2}$ for suitably chosen p can be as fast as arithmetic in $\mathbb{F}_{p'}$ with $p' \approx p^2$, the families (3.1) give a good method for generating useful curves with embedding degree 3 and small ρ-value. Note that particularly fast $\mathbb{F}_{p^2}$ arithmetic results when optimal extension fields [2] are used; Duan, Cui, and Chan [26] give sample families and curves for this set-up.

If $q = 2^s$, then curves with embedding degree 3 are of the form

$$E/\mathbb{F}_q : y^2 + \gamma^j y = x^3 + \alpha,$$

where $j \in \{1, 2\}$, γ is a non-cube in $\mathbb{F}_q^\times$, and either $\alpha = 0$ or $\alpha \in \mathbb{F}_q$ such that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \gamma^{-2j}\alpha = 1$ for $j \in \{1, 2\}$. If $\alpha = 0$, we have $t = \sqrt{q}$ if and only if $4 \nmid s$ and $t = -\sqrt{q}$ otherwise. If $\alpha \neq 0$, we have $t = \sqrt{q}$ if and only if $4 \mid s$ and $t = -\sqrt{q}$ otherwise [61].

If $t = \sqrt{q}$ and $\rho < 10/3(1 - 1/\log_2 r)$, then the minimal embedding field of E with respect to r is $\mathbb{F}_{q^3}$, while if $t = -\sqrt{q}$ and $\rho < 4/3$, then the minimal embedding field is $\mathbb{F}_{q^{3/2}}$ [10, Proposition 3.8].

3.4. *Embedding Degree* $k = 4$

Supersingular curves that have embedding degree $k = 4$ with respect to a subgroup of prime order $r > 2$ only exist over finite fields of characteristic 2. Then necessarily, $q = 2^s$ with s odd, and $t = \pm\sqrt{2q}$ [64]. The only possible such curves are ([61])

$$E/\mathbb{F}_q : y^2 + y = x^3 + x \quad \text{and} \quad E/\mathbb{F}_q : y^2 + y = x^3 + x + 1.$$

For the first curve, $t = \sqrt{2q}$ if and only if $s \equiv \pm 3 \pmod 8$ and $t = -\sqrt{2q}$ otherwise, while for the second curve, $t = \sqrt{2q}$ if and only if $s \equiv \pm 1 \pmod 8$ and $t = -\sqrt{2q}$ otherwise. If either $\rho < 3/2(1 - 1/\log_2 r)$ or s is prime and $r > 5$, then $\mathbb{F}_{q^4}$ is also the minimal embedding field for E with respect to r [10, Proposition 3.2].

3.5. *Embedding Degree $k = 6$*

Supersingular curves that have embedding degree $k = 6$ with respect to a subgroup of prime order $r > 3$ only exist over finite fields of characteristic 3. Then necessarily, $q = 3^s$ with $s > 1$ and odd, and $t = \pm\sqrt{3q}$ [64]. The only possible such curves are ([65])

$$E/\mathbb{F}_q : y^2 = x^3 - x + \delta \quad \text{and} \quad E/\mathbb{F}_q : y^2 = x^3 - x - \delta,$$

where $\delta \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}\delta = 1$ (for example, $\delta = 1$ if $s \equiv 1 \pmod 3$). For the first curve, $t = \sqrt{3q}$ if and only if $4 \nmid s - 1$ and $t = -\sqrt{3q}$ otherwise, while for the second curve, $t = \sqrt{3q}$ if and only if $4 \mid s - 1$ and $t = -\sqrt{3q}$ otherwise.

If either $\rho < 5/3(1 - 1/\log_2 r)$ or s is prime and $r > 7$, then $\mathbb{F}_{q^6}$ is also the minimal embedding field for E with respect to r [10, Proposition 3.3]. Harrison, Page, and Smart [40] give specific choices of prime extension degrees s for which supersingular curves over $\mathbb{F}_{3^s}$ of almost-prime group order and embedding degree $k = 6$ exist.

4. Generating Ordinary Curves with Arbitrary Embedding Degree

We begin our survey of methods for constructing pairing-friendly ordinary elliptic curves with the two most general methods in the literature, the Cocks–Pinch method and the Dupont–Enge–Morain method. Both methods can be used to construct curves with arbitrary embedding degree; however, both methods produce curves with $\rho \approx 2$, which may not be suitable for certain applications. Neither method produces families of curves in the sense of Definition 2.7, but we will see in Sect. 6 that the Cocks–Pinch method does generalize to produce families with $\rho < 2$. Furthermore, the Cocks–Pinch method has the advantage that it can produce curves with prime-order subgroups of nearly arbitrary size. The subgroups of Dupont–Enge–Morain curves, on the other hand, must have an order r that is the value of a certain polynomial, which results in the value of r being more difficult to specify precisely.

4.1. *The Cocks–Pinch Method*

In an unpublished manuscript [22], Cocks and Pinch gave a procedure for constructing pairing-friendly curves with arbitrary embedding degree k. The Cocks–Pinch method is important not only because it is the most flexible algorithm for constructing ordinary pairing-friendly curves, but also because it can be generalized to produce families of curves with $\rho < 2$; see Sect. 6. In addition, the method can be generalized to produce pairing-friendly abelian varieties of arbitrary dimension $g \geq 2$ [31,33].

The Cocks–Pinch method works by first fixing a subgroup size r and a CM discriminant D and then computing a trace t and prime q such that the CM equation must be satisfied.

Theorem 4.1 [22]. *Fix a positive integer k and a positive square-free integer D. Execute the following steps.*

(1) *Let r be a prime such that $k \mid r - 1$ and $(\frac{-D}{r}) = 1$.*

(2) *Let z be a kth root of unity in $(\mathbb{Z}/r\mathbb{Z})^\times$. (Such a z exists because $k \mid r-1$.) Let $t' = z+1$.*
(3) *Let $y' = (t'-2)/\sqrt{-D} \pmod r$.*
(4) *Let $t \in \mathbb{Z}$ be congruent to $t \bmod r$, and let $y \in \mathbb{Z}$ be congruent to $y' \bmod r$. Let $q = (t^2 + Dy^2)/4$.*

If q is an integer and prime, then there exists an elliptic curve E over $\mathbb{F}_q$ with an order-r subgroup and embedding degree k. If $D < 10^{12}$, then E can be constructed via the CM method.

The key feature of this algorithm is that y is constructed such that $Dy^2 + (t-2)^2$ is divisible by r. With q chosen such that the CM equation $4q - t^2 = Dy^2$ is satisfied, this yields $4(q+1-t) \equiv 0 \bmod r$. Lastly, the choice of t ensures that $\Phi_k(t-1) \equiv 0 \bmod r$.

We observe that there is no reason to believe *a priori* that t or y can be chosen to be much smaller than r, and thus in general $q \approx r^2$. We conclude that the curves produced by this method tend to have ρ-values around 2. However, these curves are easy to generate, and in particular we can take r to be any prime congruent to 1 mod k, so r can have low Hamming weight or other desirable features.

Remark 4.2. In Step (4) we could in fact choose t and y to be *any* integers congruent to t' and y' modulo r. In particular, if we wish to generate a curve with a given ρ-value $\rho_0 \geq 2$, we could add to t and y an integer divisible by r and of size roughly $r^{\rho_0/2}$. For a discussion of situations where curves with $\rho > 2$ might be useful, see Sect. 7.1.

Remark 4.3. Rubin and Silverberg [74] have observed that the Cocks–Pinch method can be used to construct curves with embedding degree k with respect to r when r is a large composite number, such as an RSA modulus. As in the case where r is prime, these curves have ρ-value around 2.

4.2. *The Dupont–Enge–Morain Method*

Whereas the Cocks–Pinch method fixes an r and then computes t and q such that the CM equation is satisfied, the approach of Dupont, Enge, and Morain [27] is to compute t and r simultaneously using resultants. The theory of resultants is discussed in [53, Sect. IV.8].

Theorem 4.4 [27]. *Fix a positive integer k and execute the following steps.*

(1) *Compute the resultant*

$$R(a) = \mathrm{Res}_x\left(\Phi_k(x-1), a + (x-2)^2\right) \in \mathbb{Z}[a].$$

(2) *Choose $a \in \mathbb{Z}$ such that $R(a)$ is prime and set $r = R(a)$.*
(3) *Compute $g(x) = \gcd(\Phi_k(x-1), a + (x-2)^2)$ in $\mathbb{F}_r[x]$ and let $t' \in \mathbb{F}_r$ be a root of the polynomial g.*
(4) *Let $t \in \mathbb{Z}$ be congruent to $t' \bmod r$. Let $q = (t^2 + a)/4$.*

If q is an integer and prime, then there exists an elliptic curve over $\mathbb{F}_q$ with an order-r subgroup and embedding degree k. If $a = Dy^2$ with $D < 10^{12}$, then E can be constructed via the CM method.

The key idea of the Dupont–Enge–Morain method is to use the following property of resultants [53, Corollary IV.8.4]: if $f(x)$ and $g(x)$ are polynomials over a field K, then $\mathrm{Res}_x(f(x), g(x)) = 0$ if and only if $f(x)$ and $g(x)$ have a common root in $\overline{K}$. When we consider $\Phi_k(x-1)$ and $a + (x-2)^2$ as polynomials in the two variables a, x, the resultant R is a single-variable polynomial in a of degree $\varphi(k)$. If we choose a such that $r = R(a)$ is prime, then $R(a) \equiv 0 \pmod{r}$, and thus $\Phi_k(x-1)$ and $a + (x-2)^2$ have a common factor $g(x)$ when considered as polynomials mod r, i.e., in $\mathbb{F}_r[x]$. We will show in Lemma 4.5 below that $r \equiv 1 \pmod{k}$, which implies that $\Phi_k(x)$ splits into distinct linear factors in $\mathbb{F}_r(x)$. Since $g(x) \mid \Phi_k(x)$, the polynomial $g(x)$ has a root $t' \in \mathbb{F}_r$. The values of t and r computed thus satisfy $r \mid \Phi_k(t-1)$ and $r \mid Dy^2 + (t-2)^2$. By construction of q, the CM equation holds, which then yields $q + 1 - t \equiv 0 \pmod{r}$.

As in the Cocks–Pinch construction, there is no reason to believe *a priori* that t is much smaller than r, and thus in general $q \approx r^2$. We conclude that the curves produced by this method tend to have ρ values around 2.

The following lemma suggests that it should be easy to find values of a such that $R(a)$ in Step (2) is prime; see also the discussion preceding Definition 2.5.

Lemma 4.5. *Fix a positive integer k, and let $R(a) \in \mathbb{Z}[a]$ be defined as in Theorem 4.4 above. Then $R(a)$ represents primes (in the sense of Definition 2.5). Furthermore, if $R(a)$ is an odd prime for some $a \in \mathbb{Z}$, then $R(a) \equiv 1 \pmod{k}$.*

Proof. Since both polynomials input to the resultant are monic and have integer coefficients, $R(a)$ is also monic with integer coefficients. If $k \leq 2$, we are done since any monic linear polynomial represents primes. We may thus assume that $k \geq 3$.

Let $\zeta_k \in \overline{\mathbb{Q}}$ be a root of $\Phi_k(x)$, and let $K = \mathbb{Q}(\zeta_k)$. The properties of resultants (see [53, Proposition IV.8.3]) then imply that

$$R(a) = \mathrm{Norm}_{K/\mathbb{Q}}\big(a + (\zeta_k - 1)^2\big). \tag{4.1}$$

If $R(a)$ is reducible, then the root $-(\zeta_k - 1)^2$ of $R(a)$ must lie in a proper subfield of K and thus be fixed under the Galois conjugation $\zeta_k \mapsto \zeta_k^e$ for some $e \not\equiv 1 \pmod{k}$. In this case we must then have $\zeta_k + \zeta_k^e = 2$, which cannot happen for $k \geq 3$. Thus $R(a)$ is irreducible.

From (4.1) we see that $R(0) = \mathrm{Norm}_{K/\mathbb{Q}}(1 - \zeta_k)^2 = \Phi_k(1)^2$. By well-known properties of cyclotomic polynomials (see [53, Sect. VI.3]) we have that if $k = p^m$ is a prime power, then $\Phi_k(1) = p$, and otherwise $\Phi_k(1) = 1$. If k is not a prime power then this implies that $\gcd(\{R(a) : a \in \mathbb{Z}\}) = 1$. If $k = p^m$ is a prime power, then to draw the same conclusion we must show that $p \nmid R(a)$ for some $a \in \mathbb{Z}$.

Let $k = p^m$. Then the prime p is totally ramified in $K = \mathbb{Q}(\zeta_k)$, with a unique prime factor $\mathfrak{p}$ satisfying $\sigma(\mathfrak{p}) = \mathfrak{p}$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Furthermore, in the residue field $\mathbb{F}_p$ the cyclotomic polynomial $\Phi_k(x)$ has a single root 1 with multiplicity $\varphi(k)$. It follows that $\sigma(a + (\zeta_k - 1)^2) \equiv a \pmod{\mathfrak{p}}$ for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, and therefore $R(a) \equiv$

$a^{\varphi(k)} \equiv 1 \pmod{p}$ whenever $\gcd(a, p) = 1$. We conclude that $\gcd(\{R(a) : a \in \mathbb{Z}\}) = 1$ if k is a prime power.

We have now shown that $R(a)$ represents primes in the sense of Definition 2.5. If $r = R(a)$ is prime for some a, then the element $a + (\zeta_k - 1)^2 \in K$ has prime norm r, and it follows that r splits completely into principal ideals in K. Since the primes splitting completely in $K = \mathbb{Q}(\zeta_k)$ are exactly those congruent to 1 mod k, this completes the proof. □

Like the Cocks–Pinch method, the Dupont–Enge–Morain method is effective for computing curves with arbitrary embedding degree k. However, whereas in the former method we could choose the subgroup size r nearly arbitrarily, in this method r is a value of the polynomial $R(a)$. Since $R(a)$ has degree $\varphi(k)$, the primes r we find will grow roughly like $a^{\varphi(k)}$. One can also take r to be any prime factor of $R(a)$ congruent to 1 mod k, but such r will still be roughly the size of $R(a)$ since it will only be feasible to compute an r of cryptographic size if the remaining factors of $R(a)$ are small. Thus the possible subgroup orders r are more restricted in the Dupont–Enge–Morain method than in the Cocks–Pinch method. This is the only significant difference between the two methods, and thus we recommend using the Cocks–Pinch method for applications where a curve with arbitrary embedding degree and $\rho \approx 2$ is desired.

5. Sparse Families of Pairing-Friendly Curves

Recall that to construct families of pairing-friendly curves, we search for polynomials $t(x), r(x), q(x)$ that satisfy certain divisibility conditions modulo $r(x)$ and for which the CM equation

$$Dy^2 = 4q(x) - t(x)^2 = 4h(x)r(x) - \big(t(x) - 2\big)^2 \tag{5.1}$$

has infinitely many solutions (x, y). Here, $h(x)$ is the "cofactor" satisfying

$$h(x)r(x) = q(x) + 1 - t(x).$$

If we are searching for curves of prime order, then we set $h(x) = 1$. Miyaji, Nakabayashi, and Takano [64] were the first to construct ordinary elliptic curves of prime order with prescribed embedding degree. Their construction relies on the fact that if the right-hand side of (5.1) is a quadratic polynomial, then we can make a substitution to transform the equation into a generalized Pell equation. Such equations often have an infinite number of solutions, in which case we obtain a family of curves in the sense of Definition 2.7.

Freeman [30] placed this result in a more general context by observing that if $f(x) = 4q(x) - t(x)^2$ is the right-hand side of (5.1) and $f(x)$ is square free, then (5.1) defines a smooth affine plane curve of genus $g = \lfloor \frac{\deg f - 1}{2} \rfloor$. If $f(x)$ is quadratic, then $g = 0$, and genus-zero curves have either no integral points or an infinite number of integral points. In the latter case we obtain a family (t, r, q) in the sense of Definition 2.7. On the other hand, if $\deg f(x) \geq 3$, then condition (5) of Definition 2.7 can never be satisfied ([30, Proposition 2.10]). Indeed, in this case the curve defined by (5.1) has genus $g \geq 1$,

and by Siegel's theorem (see [82, Theorem IX.4.3] and [25, Sect. I.2]) such curves have only a finite number of integral points.

The case that $f(x)$ contains a square factor is a very rare and lucky case. (However, it can occur; see the Barreto–Naehrig construction [4], which we describe from a different viewpoint in Sect. 6.2.) As for the case that $f(x)$ is quadratic (and square free), Freeman argues that this can only naturally occur if $k = 3$, 4, or 6. Specifically, we have the following theorem:

Theorem 5.1 [30, Lemma 5.1]. *Let $k \in \mathbb{N}$, let $t(x) \in \mathbb{Z}[x]$, and let $r(x) \in \mathbb{Z}[x]$ be an irreducible factor of $\Phi_k(t(x) - 1)$. Then $\varphi(k) \mid \deg r(x)$.*

Thus, as $\deg q(x) \geq \deg r(x)$, if $\varphi(k) \geq 4$, then $4q(x) - t(x)^2$ typically is square free and has degree at least 4. A quadratic right-hand side of the CM equation can be obtained only if the high-order terms of $4q(x)$ and $t(x)^2$ cancel out. The only case where this has been achieved so far is for embedding degree $k = 10$; for any other embedding degree, finding suitable $(t(x), r(x), q(x))$ remains an open problem.

5.1. *MNT Curves*

Miyaji, Nakabayashi, and Takano [64] were the first authors to propose ordinary pairing-friendly curves, doing so for embedding degrees $k = 3$, 4, and 6. In fact, they fully characterize ordinary curves of prime order with embedding degrees 3, 4, or 6 as follows:

Theorem 5.2 [64]. *Let q be a prime, and let $E/\mathbb{F}_q$ be an ordinary elliptic curve such that $r = \#E(\mathbb{F}_q)$ is prime. Let $t = q + 1 - r$.*

(1) *E has embedding degree $k = 3$ if and only if there exists $x \in \mathbb{Z}$ such that $t = -1 \pm 6x$ and $q = 12x^2 - 1$.*
(2) *E has embedding degree $k = 4$ if and only if there exists $x \in \mathbb{Z}$ such that $t = -x$ or $t = x + 1$, and $q = x^2 + x + 1$.*
(3) *E has embedding degree $k = 6$ if and only if there exists $x \in \mathbb{Z}$ such that $t = 1 \pm 2x$ and $q = 4x^2 + 1$.*

In all three cases, the proof (of the "only if" part) of Theorem 5.2 starts out with the condition $r \mid \Phi_k(q)$ and exploits the primality of the group order. All of the proofs are entirely elementary. Miyaji et al. prove the theorem for $q > 64$; the remaining cases can be demonstrated via a brute-force search.

Remark 5.3. Karabina and Teske [48,49] show that if r and q are both primes greater than 3, then there is an elliptic curve $E/\mathbb{F}_q$ with embedding degree 6, discriminant D, and $\#E(\mathbb{F}_q) = r$ if and only if there is an elliptic curve $E'/\mathbb{F}_r$ with embedding degree 4, discriminant D, and $\#E'(\mathbb{F}_r) = q$.

In all three cases of Theorem 5.2, the CM equation $Dy^2 = 4q(x) - t(x)^2$ defines a curve of genus zero, with the right-hand side being quadratic in x. In each case, by a linear change of variables, the CM equation can be transformed into a generalized Pell equation of the form $X^2 - SDY^2 = M$. Specifically,

(1) for $k = 3$, setting $X = 6x \pm 3$ yields $X^2 - 3Dy^2 = 24$,
(2) for $k = 4$, setting $X = 3x + 2$ (if $t = -x$) or $X = 3x + 1$ (if $t = x + 1$) yields $X^2 - 3Dy^2 = -8$, and
(3) for $k = 6$, setting $X = 6x \mp 1$ yields $X^2 - 3Dy^2 = -8$.

(The signs in (1) and (3) are to match those in Theorem 5.2.)

The general strategy to find integer solutions to the generalized Pell equation $X^2 - SDY^2 = M$ is to first find the minimal positive integer solution (U, V) (that is, $U > 0$, $V > 0$, and V minimal) to the Pell equation $U^2 - SDV^2 = 1$, by computing the simple continued fraction expansion of $\sqrt{SD}$. Then find a so-called fundamental solution (X_0, Y_0) to $X^2 - SDY^2 = M$, for example, using one of the techniques described by Matthews [58] or Robertson [73]. Such a solution may or may not exist. If a solution exists, then for $j \in \mathbb{Z}$, define (X_j, Y_j) by

$$X_j + Y_j\sqrt{SD} = (U + V\sqrt{SD})^j \cdot (X_0 + Y_0\sqrt{SD}). \tag{5.2}$$

This yields an infinite sequence of solutions to $X^2 - SDY^2 = M$.

Now, the *MNT strategy* to generate ordinary elliptic curves of prime order with embedding degree $k = 3$, 4, or 6 is the following: repeatedly select small discriminants D and compute solutions (X_j, Y_j) as in (5.2) (with $S = 3$, and $M = 24$ or $M = -8$) until the corresponding $q = q(x)$ and $r = q(x) + 1 - t(x)$ are primes of the desired bit length. Then there exists an elliptic curve over $\mathbb{F}_q$ with r points and embedding degree 3, 4, or 6, respectively, which can be constructed via the CM method.

The search for MNT curves can be sped up slightly by noting that if $k = 3$, it is necessary that $D \equiv 19 \pmod{24}$ [64], and if $k = 4, 6$, necessarily $D \equiv 3 \pmod 8$ and $D \not\equiv 5 \pmod{10}$. Also, in all three cases, M must be a quadratic residue modulo $3D$.

The major downside of MNT curves is that the consecutive solutions (X_j, Y_j) of the generalized Pell equation grow exponentially, so that only very few x-values work, and we obtain a sparse family in the sense of Definition 2.7. In fact, Luca and Shparlinski [56] give a heuristic argument that for any upper bound $\overline{D}$, there exist only a finite number of MNT curves with discriminant $D \le \overline{D}$, with no bound on the field size! On the other hand, specific sample curves of cryptographic interest have been found, such as MNT curves of 160-bit, 192-bit, or 256-bit prime order (see, for example, [69] and [80]).

5.2. *Extensions of the MNT Strategy*

The MNT strategy has been extended by Scott and Barreto [81] and by Galbraith, McKee, and Valença [36], by allowing a small constant-size cofactor h.

Starting out with (5.1), Scott and Barreto [81] fix small integers h and d and substitute $r = \Phi_k(t-1)/d$ and $t = x + 1$, to obtain the equation

$$Dy^2 = 4h\frac{\Phi_k(x)}{d} - (x-1)^2. \tag{5.3}$$

As the right-hand side is quadratic in x for $k = 3$, 4, or 6, just as with MNT curves, we can transform (5.3) into a generalized Pell equation by an appropriate linear substitution

of x. Subsequently, the MNT strategy can be applied to find curves with embedding degrees $k = 3, 4$, or 6 of almost-prime order.

Galbraith, McKee, and Valença [36] give a complete characterization of curves with embedding degree 3, 4, and 6 with cofactors $2 \le h \le 5$. This is achieved by mimicking the Miyaji–Nakabayashi–Takano proof of Theorem 5.2 but substituting hr for $\#E(\mathbb{F}_q)$, followed by an explicit (but tedious) analysis for $h = 2, 3, 4, 5$. Just as in the prime-order case, all resulting parameterizations for t are linear in x, and all resulting parameterizations for q are quadratic in x, so that the resulting CM equations $Dy^2 = 4q(x) - t(x)^2$ are quadratic in x and allow for a transformation into generalized Pell equations.

Given the nature of the solutions of Pell equations, we once again obtain sparse families.

5.3. *Freeman's Family for $k = 10$*

As discussed above, if $\varphi(k) > 2$, it is extremely unlikely that the right-hand side of (5.1) is quadratic. However, Freeman [30] discovered one example where this does occur for $k = 10$. The construction uses the following factorization of $\Phi_{10}(u(x))$, discovered by Galbraith, McKee, and Valença [36]. Let $u(x) = 10x^2 + 5x + 2$; then

$$\Phi_{10}(u(x)) = (25x^4 + 25x^3 + 15x^2 + 5x + 1)(400x^4 + 400x^3 + 240x^2 + 60x + 11).$$

Using this factorization, Freeman observed that if we take $r(x)$ to be the first factor, $t(x) = u(x) + 1$, and $q(x) = r(x) + t(x) - 1$, that is,

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

the two highest-order terms of the polynomial $f(x) = 4q(x) - t(x)^2$ cancel out, which results in the quadratic CM equation $Dy^2 = 15x^2 + 10x + 3$. Via the substitution $X = 15x + 5$, this CM equation is equivalent to the generalized Pell equation $X^2 - 15Dy^2 = -20$. For any D for which the latter equation possesses an integer solution, this yields a sparse family (t, r, q) with embedding degree 10, which can be computed by mimicking the MNT strategy. In this case the search can be sped up by using the fact that any D leading to a solution must satisfy $D \equiv 43$ or $67 \pmod{120}$.

6. Complete Families of Pairing-Friendly Curves

Once again, we start out with the CM equation

$$Dy^2 = 4q(x) - t(x)^2 = 4h(x)r(x) - \big(t(x) - 2\big)^2 \tag{6.1}$$

and search for polynomials $t(x), r(x), q(x)$ that satisfy certain divisibility conditions and for which the CM equation has infinitely many solutions (x, y). The constructions in this section work by choosing the parameters $D, t(x), r(x), q(x)$ such that the right-hand side of the CM equation is always D times the square of a polynomial $y(x)$. These constructions thus give complete families of curves in the sense of Definition 2.7.

There are two principal strategies for constructing complete families, one due to Scott and Barreto [81] and the other due originally to Barreto, Lynn, and Scott [5], and in its fullest generality to Brezing and Weng [17]. Both start in the same way: fix an embedding degree k, choose an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ such that $K \cong \mathbb{Q}[x]/(r(x))$ is a number field containing the kth roots of unity, and then choose $t(x)$ to be a polynomial mapping to $1 + \zeta_k$, where ζ_k is a primitive kth root of unity in K.

At this point the two strategies diverge. Brezing and Weng use the fact that if K contains a square root of $-D$, then since $r(x) = 0$ in K, we can factor the CM equation (6.1) in K as

$$\left(t(x) - 2 + y\sqrt{-D}\right)\left(t(x) - 2 - y\sqrt{-D}\right) \equiv 0 \bmod r(x).$$

Since $t(x) \mapsto \zeta_k + 1 \in K$, it now becomes clear that if we choose $y(x)$ to be a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in K, then the CM equation is automatically satisfied for any x.

If we do not know that K contains an element of the form $\sqrt{-D}$ for some small D, then we may apply the Scott–Barreto strategy. This strategy is to take the $t(x)$ and $r(x)$ from above and search (usually via computer) for cofactors $h(x)$ that make the right-hand side of the CM equation (6.1) either a perfect square or a linear factor times a perfect square. The CM equation then becomes

$$Dy^2 = (ax + b)g(x)^2.$$

If $a = 0$, then we take $D = b$ and $y = g(x)$. If $a > 0$, we may choose any D and make the substitution $x \mapsto \frac{Dz^2 - b}{a}$. If we then set $y = zg(x)$, the CM equation is automatically satisfied for any z.

In both cases, we finish by constructing $q(x)$ as

$$q(x) = \frac{1}{4}\left(t(x)^2 + Dy(x)^2\right).$$

If $q(x)$ represents primes and $r(x)$ has positive leading coefficient, then (t, r, q) parameterizes a complete family of pairing-friendly curves.

The success of either strategy depends heavily on the choice of number field K. The obvious choice is to set K to be a cyclotomic field $\mathbb{Q}(\zeta_\ell)$ for some ℓ that is a multiple of k and define $r(x)$ to be the ℓth cyclotomic polynomial $\Phi_\ell(x)$. Then K contains the kth roots of unity. Furthermore, it is a standard result of the theory of cyclotomic fields that K contains $\sqrt{-1}$ if $4 \mid \ell$, K contains $\sqrt{-2}$ if $8 \mid \ell$, and K contains $\sqrt{(\frac{-1}{p})p}$ for any odd prime p dividing ℓ. Thus, for any k and D, we can use a cyclotomic field in the Brezing–Weng construction; see Murphy and Fitzpatrick's work [66] for more details. We call families constructed in this manner "cyclotomic families," and we discuss some of the most efficient constructions (i.e., those with smallest ρ-value) in Sect. 6.1 below.

We may achieve even better success by choosing K to be a (perhaps trivial) extension of a cyclotomic field, with $r(x)$ not a cyclotomic polynomial. There are two ways of creating such an extension. The first is to evaluate the cyclotomic polynomial Φ_ℓ at some polynomial $u(x)$. If $\Phi_\ell(u(x))$ is irreducible, we have gained nothing, but if $\Phi_\ell(u(x))$

factors as $r_1(x)r_2(x)$ with r_1 irreducible, then we may set $K = \mathbb{Q}[x]/(r_1(x))$. Then K is a field containing the ℓth roots of unity, and $u(x)$ maps to an ℓth root of unity in K. If we know that $\sqrt{-D} \in \mathbb{Q}(\zeta_\ell)$, then $\sqrt{-D} \in K$ as well, and we may use the Brezing–Weng construction; otherwise we may apply the Scott–Barreto construction.

The second method, due to Kachisa, Schaefer, and Scott [47], is to find a non-cyclotomic polynomial $r(x)$ such that $K = \mathbb{Q}[x]/(r(x))$ is isomorphic to the cyclotomic field $\mathbb{Q}(\zeta_\ell)$. Such a polynomial $r(x)$ can be computed as the minimal polynomial of a randomly chosen element of $\mathbb{Q}(\zeta_\ell)$. Given this $r(x)$, we can find a polynomial $z(x)$ mapping to ζ_ℓ in K and proceed as in the Brezing–Weng method.

Since nontrivial factorizations of $\Phi_\ell(u(x))$ are rare for random $u(x)$ and, furthermore, the $q(x)$ produced by the Kachisa–Schaefer–Scott technique do not usually represent primes, we will call families of curves obtained by either of these techniques "sporadic" families; they are discussed in Sect. 6.2 below. Although such families are rare, they may have better ρ-values than curves constructed using a cyclotomic field. This was most spectacularly demonstrated by Barreto and Naehrig [4], who used the first method to construct curves of prime order with embedding degree 12 (Example 6.8 below).

We have checked that all of the families we describe in this section can be used to produce explicit examples of pairing-friendly elliptic curves and have confirmed that for parameters of cryptographic size, the ρ-value of a curve is very close to the ρ-value of its family. As listing examples of curves is beyond the scope of this paper, we either refer the reader to the original papers describing the constructions or suggest trying various values of x until a value is found such that $q(x)$ is a prime of the desired size.

6.1. *Cyclotomic Families*

Barreto, Lynn, and Scott [5] and (independently) Brezing and Weng [17] both observed that if we apply the Cocks–Pinch method but parameterize t, r, q as polynomials, then we can improve on the ρ-value of 2 produced by the Cocks–Pinch method. Brezing and Weng stated the construction in greatest generality; their theorem is below. An alternative interpretation of the construction can be found in the paper of Freeman [32], which generalizes the method to produce higher-dimensional abelian varieties.

Theorem 6.1 [17]. *Fix a positive integer k and a positive square-free integer D. Execute the following steps.*

(1) *Find an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ with positive leading coefficient such that $K = \mathbb{Q}[x]/(r(x))$ is a number field containing $\sqrt{-D}$ and the cyclotomic field $\mathbb{Q}(\zeta_k)$.*
(2) *Choose a primitive kth root of unity $\zeta_k \in K$.*
(3) *Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta_k + 1$ in K.*
(4) *Let $y(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in K. (So, if $\sqrt{-D} \mapsto s(x)$, then $y(x) \equiv (2 - t(x))s(x)/D \bmod r(x)$.)*
(5) *Let $q(x) \in \mathbb{Q}[x]$ be given by $(t(x)^2 + Dy(x)^2)/4$.*

Suppose that $q(x)$ represents primes and $y(x_0) \in \mathbb{Z}$ for some $x_0 \in \mathbb{Z}$. Then the triple $(t(x), r(x), q(x))$ parameterizes a complete family of elliptic curves with embedding

degree k and discriminant D. The ρ-value of this family is

$$\rho(t,r,q) = \frac{2\max\{\deg t(x), \deg y(x)\}}{\deg r(x)}. \tag{6.2}$$

Since we can always choose $t(x)$ and $y(x)$ to have degree strictly less than $r(x)$, we see that this method can produce families with ρ-values strictly less than 2. In general, we expect the smallest possible degree for $t(x)$ and $y(x)$ to be $\deg(r)-1$, so ρ will not be much less than 2. However, for certain clever choices of the number field K, we may construct polynomials t and y with smaller degree, thus improving the ρ-value.

We now examine in detail some constructions that make use of Theorem 6.1. Here and in the following examples, for $\alpha \in K$ and $f(x) \in \mathbb{Q}[x]$, we use the notation $\alpha \mapsto f(x)$ to mean that $f(x)$ represents α in $K = \mathbb{Q}[x]/(r(x))$.

Barreto, Lynn, and Scott [5] gave the first construction along the lines of Theorem 6.1. They construct families by taking the polynomial $r(x)$ defining the number field K to be the kth cyclotomic polynomial, choosing $\zeta_k \mapsto x$ in K (so $t(x) = 1+x$) and using the fact that if k is divisible by 3, then $\sqrt{-3} \in K$. Brezing and Weng [17] give a more general construction by setting $r(x)$ to be a cyclotomic polynomial $\Phi_\ell(x)$ for some multiple ℓ of the desired embedding degree k and choosing various representatives for ζ_k in $\mathbb{Q}[x]/(r(x))$. The discriminants D in these constructions are often taken to be 1 or 3, and any cyclotomic polynomial satisfies condition (2) of Definition 2.7(i). The tricky part of most of these constructions is ensuring that the resulting $q(x)$ represents primes.

We begin with a construction given by Brezing and Weng, who state the construction for prime embedding degrees k; we observe that the construction extends readily to all odd k. We choose K to be a cyclotomic field containing a fourth root of unity $\sqrt{-1}$, so we may choose $D = 1$.

Construction 6.2 [17]. Let k be odd, $k < 1000$. Let

$$\begin{aligned} r(x) &= \Phi_{4k}(x), \\ t(x) &= -x^2 + 1, \\ q(x) &= \frac{1}{4}\left(x^{2k+4} + 2x^{2k+2} + x^{2k} + x^4 - 2x^2 + 1\right). \end{aligned} \tag{6.3}$$

Then (t,r,q) parameterizes a complete family of pairing-friendly elliptic curves with embedding degree k and discriminant 1. The ρ-value of this family is $(k+2)/\varphi(k)$.

Proof. We apply Theorem 6.1 with $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{4k})$, which contains $\mathbb{Q}(\zeta_k)$ and $\sqrt{-1}$. We choose $\zeta_k \mapsto -x^2$ and $\sqrt{-1} \mapsto x^k$. Then $y(x) = (x^2+1)x^k$, giving $q(x) = \frac{1}{4}((-x^2+1)^2 + (x^2+1)^2x^{2k})$, which simplifies to (6.3). Now, $q(x)$ is an integer whenever x is odd, and $q(1) = 1$. Thus if q is irreducible, then it represents primes. Computations with Magma [15] show that $q(x)$ is irreducible for all odd $k < 1000$. (This pattern of irreducibility motivates us to conjecture that $q(x)$ is indeed irreducible for all odd k.) Lastly, $y(x) \in \mathbb{Z}$ for all $x \in \mathbb{Z}$. The claimed ρ-value follows from (6.2) as $\deg r = 2\varphi(k)$ and $\deg t < \deg y = k+2$. □

We next observe that if k is odd, then $\zeta_{2k} = -\zeta_k$. Thus if we change the sign of the polynomials representing ζ_k in Construction 6.2, the same construction can be used to create families with embedding degree $2k$ and the same ρ-values.

Construction 6.3. Let k be odd, $k < 1000$. Let

$$\begin{aligned} r(x) &= \Phi_{4k}(x), \\ t(x) &= x^2 + 1, \\ q(x) &= \frac{1}{4}\big(x^{2k+4} - 2x^{2k+2} + x^{2k} + x^4 + 2x^2 + 1\big). \end{aligned}$$

Then (t, r, q) parameterizes a complete family of pairing-friendly elliptic curves with embedding degree $k' = 2k$ and discriminant 1. The ρ-value of this family is $(k'/2 + 2)/\varphi(k')$.

Proof. Again, we invoke Theorem 6.1, choosing $r(x)$ as in Construction 6.2, $\sqrt{-1} \mapsto x^k$, and $\zeta_{2k} \mapsto x^2$. We obtain $t(x)$ as stated and $y(x) = (-x^2 + 1)x^k$, giving the stated $q(x)$. Since $q(x)$ is the reverse polynomial of (6.3), we have $q(1) = 1$ and $q(x) \in \mathbb{Z}$ for all odd x. Further, $q(x)$ is irreducible if and only if (6.3) is, that is, certainly for all $k < 1000$ and conjecturally for all odd k. Just as in Construction 6.2, the ρ-value of this family is $(k + 2)/\varphi(k)$. □

With the same setup, using $\zeta_{4k} = \sqrt{\zeta_{2k}}$ gives the following construction.

Construction 6.4. Let k be odd, $k < 1000$. Let

$$\begin{aligned} r(x) &= \Phi_{4k}(x), \\ t(x) &= x + 1, \\ q(x) &= \frac{1}{4}\big(x^{2k+2} - 2x^{2k+1} + x^{2k} + x^2 + 2x + 1\big). \end{aligned}$$

Then (t, r, q) parameterizes a complete family of pairing-friendly elliptic curves with embedding degree $k' = 4k$ and discriminant 1. The ρ-value of this family is $(k'/2 + 2)/\varphi(k')$.

Proof. We use Theorem 6.1 with $r(x)$ as in the previous constructions, $\sqrt{-1} \mapsto x^k$, and $\zeta_{4k} \mapsto x$. Then $y(x) = (-x + 1)x^k$, from which we obtain $q(x)$ as stated. Since $q(1) = 1$, if q is irreducible, then it represents primes. Computations with Magma [15] show that $q(x)$ is irreducible for odd $k < 1000$ (and we conjecture once again that $q(x)$ is irreducible for all odd k). From (6.2) we obtain the ρ-value of this family as $(k + 1)/\varphi(k)$. □

For $k = 10$, Brezing and Weng achieve a better ρ-value than Construction 6.3.

Example 6.5 [17]. Let

$$\begin{aligned} r(x) &= \Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1, \\ t(x) &= -x^6 + x^4 - x^2 + 2, \\ q(x) &= \frac{1}{4}\left(x^{12} - x^{10} + x^8 - 5x^6 + 5x^4 - 4x^2 + 4\right). \end{aligned}$$

Then (t, r, q) parameterizes a complete family of pairing-friendly elliptic curves with embedding degree 10 and discriminant 1. The ρ-value of this family is $3/2$.

Proof. The field $K = \mathbb{Q}[x]/(r(x))$ contains ζ_{10} and $\sqrt{-1}$. We choose $\sqrt{-1} \mapsto x^5$ and $\zeta_{10} \mapsto -x^6 + x^4 - x^2 + 1$ and use Theorem 6.1. Then $\zeta_{10} + 1 \mapsto t(x)$, and $y(x) = x^5 - x^3$, giving $q(x)$ as stated. Since $q(x)$ is irreducible and $q(0) = 1$, it represents primes. □

We now consider families constructed by choosing K to be a cyclotomic field containing a cube root of unity. Such fields contain $\sqrt{-3}$, so we may choose $D = 3$. Some constructions of this form have been given by Barreto, Lynn, and Scott [5] and Brezing and Weng [17] for certain values of k; we consider the construction for all k and discover (potential) families in all cases where k is not divisible by 18.

Construction 6.6. Let k be a positive integer with $k \leq 1000$ and $18 \nmid k$.

- If $k \equiv 1 \pmod 6$, let

$$\begin{aligned} r(x) &= \Phi_{6k}(x), \\ t(x) &= -x^{k+1} + x + 1, \\ q(x) &= \frac{1}{3}(x+1)^2\left(x^{2k} - x^k + 1\right) - x^{2k+1}. \end{aligned}$$

- If $k \equiv 2 \pmod 6$, let

$$\begin{aligned} r(x) &= \Phi_{3k}(x), \\ t(x) &= x^{k/2+1} - x + 1, \\ q(x) &= \frac{1}{3}(x-1)^2\left(x^k - x^{k/2} + 1\right) + x^{k+1}. \end{aligned}$$

- If $k \equiv 3 \pmod 6$, let

$$\begin{aligned} r(x) &= \Phi_{2k}(x), \\ t(x) &= -x^{k/3+1} + x + 1, \\ q(x) &= \frac{1}{3}(x+1)^2\left(x^{2k/3} - x^{k/3} + 1\right) - x^{2k/3+1}. \end{aligned}$$

- If $k \equiv 4 \pmod 6$, let

$$\begin{aligned} r(x) &= \Phi_{3k}(x), \\ t(x) &= x^3 + 1, \\ q(x) &= \frac{1}{3}\left(x^3 - 1\right)^2\left(x^k - x^{k/2} + 1\right) + x^3. \end{aligned}$$

- If $k \equiv 5 \pmod 6$, let

$$\begin{aligned} r(x) &= \Phi_{6k}(x), \\ t(x) &= x^{k+1} + 1, \\ q(x) &= \frac{1}{3}\left(x^2 - x + 1\right)\left(x^{2k} - x^k + 1\right) + x^{k+1}. \end{aligned}$$

- If $k \equiv 0 \pmod 6$, let

$$\begin{aligned} r(x) &= \Phi_k(x), \\ t(x) &= x + 1, \\ q(x) &= \frac{1}{3}(x-1)^2\left(x^{k/3} - x^{k/6} + 1\right) + x. \end{aligned}$$

Then (t, r, q) parameterizes a complete family of pairing-friendly curves with embedding degree k and discriminant 3.

Let $\ell = \operatorname{lcm}(6, k)$. Then the ρ-value of any such family is $\rho = (\ell/3 + 6)/\varphi(\ell)$ if $k \equiv 4 \pmod 6$ and $(\ell/3 + 2)/\varphi(\ell)$ otherwise. In particular, we have $\rho \leq 2$ for all $k \leq 1000$ except for $k = 4$ and $\rho < 2$ for all $5 \leq k \leq 1000$ except for $k = 6$ and 10.

Proof. We use Theorem 6.1 with $r(x) = \Phi_\ell(x)$, where $\ell = \operatorname{lcm}(k, 6)$. That is, we work in the field $\mathbb{Q}(\zeta_k, \zeta_6)$ defined as $K \cong \mathbb{Q}[x]/(\Phi_\ell(x))$. In this field we have $\sqrt{-3} \mapsto 2x^{\ell/6} - 1$. Our goal is to find a polynomial $y(x)$ of small degree such that $(\zeta_k - 1)/\sqrt{-3} \mapsto y(x)$. The degree of $y(x)$ depends on our choice of polynomial $z(x)$ with $\zeta_k \mapsto z(x)$ The obvious choice is $\zeta_k \mapsto x^{\ell/k}$; however, in many cases we can do better by choosing $\zeta_k \mapsto x^a$ with a only slightly larger than $\ell/6$ and reducing modulo $\Phi_\ell(x)$ to obtain $z(x)$. Since x is a primitive ℓth root of unity, for x^a to be a primitive kth root of unity, we need a to be a multiple of ℓ/k and relatively prime to k. The specific choices for $\zeta_k \mapsto z(x)$ are given below.

For a given $z(x)$, we let $t(x) = z(x) + 1$, and we compute $y(x)$ by taking $\frac{1}{3}(z(x) - 1)(1 - 2x^{\ell/6})$ and adding $\pm\frac{2}{3}x\Phi_6(x^{\ell/k})$ (a polynomial divisible by $r(x)$) to cancel out the leading term if $k \pmod 6 \in \{1, 2, 3, 5\}$. Specifically,

- If $k \equiv 1 \pmod 6$, then $\ell = 6k$. Since $2k + 1 \equiv 3 \pmod 6$, x^{2k+1} is a primitive $2k$th root of unity. Since k is odd, $-x^{2k+1}$ is a primitive kth root of unity. Thus we choose $\zeta_k \mapsto -x^{2k+1} \equiv -x^{k+1} + x \bmod r(x)$, which gives $t(x)$ as stated, and $y(x) = \frac{1}{3}(-x^{k+1} + 2x^k - x - 1)$.

- If $k \equiv 2 \pmod 6$, then $\ell = 3k$. We have $k+1 \equiv 3 \pmod 6$, so we choose $\zeta_k \mapsto x^{k+1} \equiv x^{k/2+1} - x \bmod r(x)$. This gives $t(x)$ as stated, and $y(x) = \frac{1}{3}(x^{k/2+1} + 2x^{k/2} + x - 1)$.
- If $k \equiv 3 \pmod 6$, then $\ell = 2k$. Since $x^{2k/3}$ is a cube root of unity and $3 \mid k$, we need to multiply $x^{2k/3}$ by a primitive kth root of unity. Since k is odd and x is a $2k$th root of unity, $-x$ is a kth root of unity. Thus we choose $\zeta_k \mapsto -x^{2k/3+1} \equiv -x^{k/3+1} + x \bmod r(x)$. Again, this gives $t(x)$ as stated, and $y(x) = \frac{1}{3}(-x^{k/3+1} + 2x^{k/3} - x - 1)$.
- If $k \equiv 4 \pmod 6$, then $\ell = 3k$. Choose $\zeta_k \mapsto x^3 = z(x)$. Then $y(x) = \frac{1}{3}(-2x^{k/2+3} + 2x^{k/2} + x^3 - 1)$.
- If $k \equiv 5 \pmod 6$, then $\ell = 6k$. We have $k+1 \equiv 0 \pmod 6$, so we choose $\zeta_k \mapsto x^{k+1} = z(x)$. Then $y(x) = \frac{1}{3}(-x^{k+1} + 2x^k + 2x - 1)$.
- If $k \equiv 0 \pmod 6$, then $\ell = k$. Choose $\zeta_k \mapsto x = z(x)$. Then $y(x) = \frac{1}{3}(-2x^{k/6+1} + 2x^{k/6} + x - 1)$.

By computing $q(x) = \frac{1}{4}(t(x)^2 + 3y(x)^2)$ one can immediately verify that from these $t(x)$ and $y(x)$ we obtain the polynomials $q(x)$ as stated, Note that for small values of k, some of the resulting $t(x)$ and $y(x)$ are not completely reduced modulo $r(x)$; in these cases we find that further reduction leads to a $q(x)$ that does not represent primes.

It remains to consider whether $q(x)$ represents primes. We can check conditions (4) and (5) of Definition 2.5(i) simultaneously: If k is even, then $q(1) = 1$, if $k \equiv 1$ or $3 \pmod 6$, then $q(-1) = 1$, and if $k \equiv 5 \pmod 6$, then $q(-1) = 4$ and $q(2)$ is an odd integer. Finally, computations with Magma [15] indicate that the appropriate $q(x)$ is irreducible for all $k \leq 1000$, except when k is divisible by 18. (This pattern of irreducibility motivates us to conjecture that the appropriate $q(x)$ is irreducible for all k not divisible by 18.)

As for the ρ-value, note that we have $\deg q = \ell/3 + 2$ in all cases except $k \equiv 4 \pmod 6$, in which case $\deg q = \ell/3 + 6$. □

Next, we consider families obtained by choosing K to be a cyclotomic field containing an eighth root of unity. Such fields contain $\sqrt{-2}$, so we may choose $D = 2$. Murphy and Fitzpatrick [66] give an example of the construction for $k = 24$; we describe the construction for any k divisible by 3.

Construction 6.7. Let k be a positive integer with $k < 1000$ and $3 \mid k$. Let $\ell = \operatorname{lcm}(8, k)$ and

$$\begin{aligned} r(x) &= \Phi_\ell(x), \\ t(x) &= x^{\ell/k} + 1, \\ q(x) &= \frac{1}{8}\left(2\left(x^{\ell/k}+1\right)^2 + \left(1 - x^{\ell/k}\right)^2\left(x^{5\ell/24} + x^{\ell/8} - x^{\ell/24}\right)^2\right). \end{aligned}$$

Then (t, r, q) parameterizes a complete family of curves with embedding degree k and discriminant 2. The ρ-value of this family is $(\frac{5k}{6}+4)/\varphi(k)$ if k is odd and $(\frac{5k}{12}+2)/\varphi(k)$ if k is even. (These ρ-values are less than 2 for all $k \leq 1000$ except for $k = 3$, 6, or 15.)

Table 3. Families with $k \in \{15, 28, 44\}$ and $D = 2$.

k	ℓ	$t(x), r(x), q(x)$	ρ
15	120	$t(x) = x^{28} + x^{24} - x^{16} - x^{12} - x^8 + 1$ $r(x) = \Phi_{120}(x)$ $q(x) = \frac{1}{8}(2x^{56} + 4x^{52} + x^{50} + 2x^{48} + 2x^{46} - 4x^{44} + x^{42} - 6x^{40} - 4x^{36} - x^{30} + 12x^{28} - 2x^{26} + 14x^{24} - x^{22} + 2x^{20} - 10x^{16} - 10x^{12} + x^{10} - 8x^8 + 2x^6 + x^2 + 8)$	7/4
28	56	$t(x) = -x^2$ $r(x) = \Phi_{56}(x)$ $q(x) = \frac{1}{8}(2(x^2-1)^2 + x^{14}(x^2+1)^2(x^{14}+1)^2)$	23/12
44	88	$t(x) = -x^2$ $r(x) = \Phi_{88}(x)$ $q(x) = \frac{1}{8}(2(x^2-1)^2 + x^{22}(x^2+1)^2(x^{22}+1)^2)$	7/4

Proof. We apply Theorem 6.1, working in the field $K = \mathbb{Q}[x]/(\Phi_\ell(x))$, which is isomorphic to $\mathbb{Q}(\zeta_k, \zeta_8)$. In this field, we have $\zeta_k \mapsto x^{\ell/k}$, and $\sqrt{-2} = \zeta_8 + \zeta_8^3 \mapsto x^{\ell/8} + x^{3\ell/8}$. We wish to compute $y(x)$ such that $(\zeta_k - 1)/\sqrt{-2} \mapsto y(x)$. Explicitly, we have

$$\frac{\zeta_k - 1}{\sqrt{-2}} \mapsto \frac{1}{2}\bigl(1 - x^{\ell/k}\bigr)\bigl(x^{3\ell/8} + x^{\ell/8}\bigr). \tag{6.4}$$

Since k is a multiple of 3, we can use the relation $x^{\ell/3} \equiv x^{\ell/6} - 1 \bmod \Phi_\ell(x)$ to reduce the right-hand side of (6.4) further, obtaining

$$y(x) = \frac{1}{2}\bigl(1 - x^{\ell/k}\bigr)\bigl(x^{5\ell/24} + x^{\ell/8} - x^{\ell/24}\bigr).$$

Choosing $t(x) = x^{\ell/k} + 1$ gives $q(x)$ as stated. Note that unless $k = 3, 6$, or 15, we have $\frac{\ell}{k} + \frac{5\ell}{24} < \varphi(\ell)$, and thus $y(x)$ is indeed the minimal-degree representative of $(\zeta_k - 1)/\sqrt{-2}$ modulo $\Phi_\ell(x)$ (see also below for the case $k = 15$).

To establish that $q(x)$ represents primes, we first observe that $q(1) = 1$ for any k. Computations with Magma [15] then show that $q(x)$ is irreducible whenever $3 \mid k$ and $k < 1000$. (This pattern of irreducibility motivates us to conjecture that $q(x)$ is irreducible for all k divisible by 3.) As for the ρ-value, it suffices to note that $\deg q(x) = (\frac{2\ell}{k} + \frac{5\ell}{12})$, and $\deg r(x) = \varphi(k)\ell/(2k)$ if k is odd and $\deg r(x) = \varphi(k)\ell/k$ if k is even. □

Construction 6.7, while stated only for k divisible by 3, can be carried out for any positive integer k, setting $y(x)$ to be the minimal-degree representative for $(\zeta_k - 1)/\sqrt{-2}$ in K. However, unlike the case of Construction 6.6, the expressions for $q(x)$ when k is not divisible by 3 become too complicated to enumerate explicitly in general. Furthermore, in some cases the construction may not give a family in the sense of Definition 2.7; for example, if $k = 20$, the $q(x)$ given by the construction never takes integer values. Potential families for a few selected values of k are given in Table 3; here we include the case $k = 15$ with $y(x)$ completely reduced modulo $\Phi_{120}(x)$.

6.2. *Sporadic Families of Brezing–Weng Curves*

Brezing and Weng only consider cyclotomic polynomials $r(x)$ for their constructions, but in some cases using non-cyclotomic polynomials $r(x)$ that define (perhaps trivial) extensions of cyclotomic fields may turn out to be even more effective. One method for constructing such extensions is to evaluate the cyclotomic polynomial $\Phi_\ell(x)$ at some polynomial $u(x)$. If $\Phi_\ell(u(x))$ is irreducible, as is usually the case, going to the extension field will give us no advantage, as we will just be evaluating t, r, and q at $u(x)$. However, if $\Phi_\ell(u(x))$ factors, we may gain some advantage.

Galbraith, McKee, and Valença [36] have analyzed the factorizations of $\Phi_\ell(u(x))$ when u is quadratic and Φ_ℓ has degree 4. For $\ell = 8$, there are no quadratic u such that $\Phi_8(u(x))$ factors. For $\ell = 5, 10$, there is a one-dimensional family of such u, parameterized by the rational points of a rank-one elliptic curve over $\mathbb{Q}$. However, since $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_{10})$ has no quadratic imaginary subfields, we do not expect to find $\sqrt{-D}$ in an extension of $\mathbb{Q}(\zeta_5)$.

Finally, for $\ell = 12$, there are two such $u(x)$. Barreto and Naehrig constructed pairing-friendly curves of prime order using one such factorization.

Example 6.8 (Barreto–Naehrig curves [4]). Let

$$\begin{aligned} r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ t(x) &= 6x^2 + 1, \\ q(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1. \end{aligned}$$

Then (t, r, q) parameterizes a complete family of curves with embedding degree $k = 12$, discriminant 3, and ρ-value 1.

Proof. Galbraith, McKee, and Valença discovered that if $u(x) = 6x^2$, and $r(x)$ is as stated above, then $\Phi_{12}(u(x)) = r(x)r(-x)$. If $K = \mathbb{Q}[x]/(r(x))$, then $\zeta_{12} \mapsto 6x^2$ in K, giving $t(x)$ as stated above. Using $\sqrt{-3} = 2\zeta_{12}^2 - 1$, we compute $y(x) = 6x^2 + 4x + 1$, giving $q(x)$ as stated. It is immediately verified that $q(x)$ represents primes. □

Note that since $q(x)$ and $r(x)$ have the same degree *and* leading coefficient, $r(x)$ is actually the number of points on the elliptic curve to be constructed. Thus if $q(x)$ and $r(x)$ are both prime for some value of x, then the elliptic curve constructed will have prime order. In addition, this family has the added benefit that curves with $D = 3$ have twists of degree 6, and since k is divisible by 6, we may take advantage of these twists to map points in $E(\mathbb{F}_{q^{12}})$ to points defined over $\mathbb{F}_{p^2}$, which allow for much faster group operations. (See Sect. 7.3 for further details).

Barreto and Naehrig present their construction as an MNT-type family (see Sect. 5) in which the right-hand side of the CM equation happens to be a constant times a perfect square polynomial. However, viewing the construction as we do in Example 6.8 suggests that we can extend the construction to the other quadratic $u(x)$ for which $\Phi_{12}(u(x))$ factors. Namely, if $u(x) = 2x^2$, then $\Phi_{12}(u(x)) = r(x)r(-x)$ with $r(x) = 4x^4 + 4x^3 + 2x^2 + 2x + 1$. Again we have $\zeta_{12} \mapsto u(x)$ and $\sqrt{-3} = 2\zeta_{12}^2 - 1$. The construction of $q(x)$ for embedding degree 12 again gives a degree-four polynomial, but this polynomial never takes integer values. Instead, let us look at $\zeta_4 \mapsto u(x)^3 \bmod r(x)$.

Example 6.9. Let

$$t(x) = -4x^3,$$
$$r(x) = 4x^4 + 4x^3 + 2x^2 + 2x + 1,$$
$$q(x) = \frac{1}{3}\big(16x^6 + 8x^4 + 4x^3 + 4x^2 + 4x + 1\big).$$

Then (t, r, q) parameterizes a complete family of curves with embedding degree $k = 4$ and discriminant 3. The ρ-value of this family is $3/2$.

Proof. If $u(x) = 2x^2$ and $r(x)$ is as above, then $\Phi_{12}(u(x)) = r(x)r(-x)$. Now $\zeta_4 \mapsto u(x)^3 \bmod r(x)$, that is, $\zeta_4 \mapsto -4x^3 - 1$, so let $t(x) = -4x^3$. Using $\sqrt{-3} \mapsto 8y^3 + 4y^2 + 4y + 3$, we compute $y(x) = \frac{1}{3}(4y^3 + 4y + 2)$, giving $q(x)$ as stated. Since $q(x)$ is irreducible and $q(-1) = 7$ and $q(2) = 403$ are relatively prime, $q(x)$ represents primes. □

A computer search for further factorizations of $\Phi_k(u(x))$ for various values of k and degrees of u found the following example for $k = 8$; Tanaka and Nakamula [84] have given similar constructions using the same idea.

Example 6.10. Let $k = 8$. Let

$$r(x) = 9x^4 + 12x^3 + 8x^2 + 4x + 1,$$
$$t(x) = -9x^3 - 3x^2 - 2x,$$
$$q(x) = \frac{1}{4}\big(81x^6 + 54x^5 + 45x^4 + 12x^3 + 13x^2 + 6x + 1\big).$$

Then (t, r, q) parameterizes a complete family of curves with embedding degree $k = 8$ and discriminant 1. The ρ-value is $3/2$.

Proof. Let $u(x) = 9x^3 + 3x^2 + 2x + 1$. Then $\Phi_8(u(x))$ has an irreducible factor $r(x) = 9x^4 + 12x^3 + 8x^2 + 4x + 1$. Setting $D = 1$, in the field $K = \mathbb{Q}[x]/(r(x))$ we choose $\zeta_8 \mapsto -u(x)$ and $\sqrt{-1} = \zeta_8^2 \mapsto -18x^3 - 15x^2 - 10x - 4 \bmod r(x)$. From this we compute $t(x)$ as stated and $y(x) = -3x - 1$. Applying Theorem 6.1, we obtain $q(x)$ as stated. Since $q(x)$ is irreducible and $q(1) = 53$ and $q(-1) = 17$ are distinct primes, $q(x)$ represents primes. □

Note that the ρ-value of this family is worse than the ρ-value $5/4$ given by Construction 6.6. However, curves with $D = 1$ have a twists of degree 4, and since k is a multiple of 4, we may take advantage of these twists to map points $P \in E(\mathbb{F}_{q^8})$ down to the field $\mathbb{F}_{q^2}$, thus speeding up the pairing computation. (See Sect. 7.3 for further details.)

Our search also found the following factorization: If $u(x) = x^5 + 2x^4 + 2x^3 + 2x^2 + 1$, then $\Phi_{12}(u(x)) = r_1(x)r_2(x)$, where

$$\begin{aligned} r_1(x) &= x^8 + 4x^7 + 7x^6 + 8x^5 + 6x^4 + 4x^3 + 4x^2 + 2x + 1, \\ r_2(x) &= x^{12} + 4x^{11} + 9x^{10} + 16x^9 + 19x^8 + 20x^7 + 17x^6 + 10x^5 \\ &\quad + 10x^4 + 4x^2 - 2x + 1. \end{aligned}$$

Each of these leads to a complete family of pairing friendly curves with $D = 3$, the former with $\rho = 5/4$ and the latter with $\rho = 7/6$. These are both superior to Construction 6.6 for $k = 12$, which has $\rho = 3/2$, but they are clearly inferior to the ideal Barreto and Naehrig construction (Example 6.8). However, the result does indicate that more useful solutions may well exist.

Kachisa, Schaefer, and Scott [47], building on the work of Kachisa [46], give a different strategy for constructing non-cyclotomic polynomials that define a cyclotomic field. Their strategy is to choose elements $\beta \in \mathbb{Q}(\zeta_\ell)$ that can be written as an integer linear combination of a power basis with small coefficients, and let $r(x)$ be the minimal polynomial of β. Since most elements of $\mathbb{Q}(\zeta_\ell)$ do not lie in a proper subfield, in most cases we have $\mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$. We can then proceed as in the Brezing–Weng method.

Which β and which kth root of unity modulo $r(x)$ to choose are determined by computer search; the resulting polynomial $q(x)$ should have a degree low enough such that we obtain an attractive ρ-value. In practice one finds that most polynomials $q(x)$ generated by the construction have large denominators, so it is rare for these polynomials to take integer values. Yet favorable polynomials do exist, as the following examples show. We give full details for the first example and give the polynomials t, r, q and the relevant congruence classes of x for the others; full details can be found in [47].

Example 6.11 [47]. Let $k = \ell = 16$. Let

$$\begin{aligned} t(x) &= \frac{1}{35}\left(2x^5 + 41x + 35\right), \\ r(x) &= x^8 + 48x^4 + 625, \\ q(x) &= \frac{1}{980}\left(x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125\right). \end{aligned}$$

Then (t, r, q) parameterizes a complete family of curves with embedding degree 16 and discriminant 1. The ρ-value of this family is $5/4$.

Proof. We set $\beta = -2\zeta_{16}^5 + \zeta_{16} \in \mathbb{Q}(\zeta_{16})$, which has minimal polynomial $r(x)$. We apply Theorem 6.1, working in the field $K = \mathbb{Q}(\zeta_{16})$ defined as $\mathbb{Q}[x]/(r(x))$. We use $\zeta_{16} \mapsto \frac{1}{35}(2x^5 + 41x)$ in K, giving $t(x)$ as stated. Now we use $\sqrt{-1} \mapsto -\frac{1}{7}(x^4 + 24)$, from which we get $y(x) = -\frac{1}{35}(x^5 + 5x^4 + 38x + 120)$ and $q(x)$ as stated. The polynomial $q(x)$ is irreducible. We find that both $q(x)$ and $t(x)$ are integers if and only if $x \equiv 25$ or $45 \pmod{70}$. In addition, $\gcd(\{q(\pm 25 + 70n) : n \in \mathbb{Z}\}) = 1$, so $q(x)$ represents primes. □

Example 6.12 [47]. Let $k = \ell = 18$, $D = 3$. We set

$$t(x) = \frac{1}{7}\left(x^4 + 16x + 7\right),$$
$$r(x) = x^6 + 37x^3 + 343,$$
$$q(x) = \frac{1}{21}\left(x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401\right).$$

We find that $q(x)$ can take prime values for $x \equiv 14 \pmod{42}$. The ρ-value of this family is $4/3$.

Example 6.13 [47]. Let $k = \ell = 32$, $D = 1$. We set

$$t(x) = \frac{1}{3107}\left(-2x^9 - 56403x + 3107\right),$$
$$r(x) = x^{16} + 57120x^8 + 815730721,$$
$$q(x) = \frac{1}{2970292}\left(x^{18} - 6x^{17} + 13x^{16} + 57120x^{10} - 344632x^9 + 742560x^8 + 815730721x^2 - 4948305594x + 10604499373\right).$$

We find that $q(x)$ can take prime values for $x \equiv \pm 325 \pmod{6214}$. The ρ-value of this family is $9/8$.

Example 6.14 [47]. Let $k = \ell = 36$, $D = 3$. We set

$$t(x) = \frac{1}{259}\left(259 + 757x + 2x^7\right),$$
$$r(x) = x^{12} + 683x^6 + 117649,$$
$$q(x) = \frac{1}{28749}\left(x^{14} - 4x^{13} + 7x^{12} + 683x^8 - 2510x^7 + 4781x^6 + 117649x^2 - 386569x + 823543\right).$$

We find that $q(x)$ can take prime values for $x \equiv \pm 49 \pmod{259}$. The ρ-value of this family is $7/6$.

Example 6.15 [47]. Let $k = \ell = 40$, $D = 1$. We set

$$t(x) = \frac{1}{1185}\left(2x^{11} + 6469x + 1185\right),$$
$$r(x) = x^{16} + 8x^{14} + 39x^{12} + 112x^{10} - 79x^8 + 2800x^6 + 24375x^4 + 125000x^2 + 390625,$$
$$q(x) = \frac{1}{1123380}\left(x^{22} - 2x^{21} + 5x^{20} + 6232x^{12} - 10568x^{11} + 31160x^{10} + 9765625x^2 - 13398638x + 48828125\right).$$

We find that $q(x)$ can take prime values for $x \equiv \pm 20 \pmod{1185}$. The ρ-value of this family is $11/8$.

6.3. *Scott–Barreto Families*

To employ the strategy of Scott and Barreto [81], we again take K to be an extension of a cyclotomic field, but this time we do not assume that K contains an element $\sqrt{-D}$. If we choose $t(x)$ to be any polynomial and $r(x)$ to be an irreducible factor of $\Phi_k(t(x)-1)$, then $\mathbb{Q}[x]/(r(x))$ defines an extension of a cyclotomic field. We then search for an $h(x)$ that makes the right-hand side of the CM equation

$$Dy^2 = 4h(x)r(x) - \big(t(x)-2\big)^2 \tag{6.5}$$

take the form of a linear factor times a perfect square. Once such an $h(x)$ is found, we can set x to be the linear function of Dz^2 that makes the right-hand side of (6.5) D times a square polynomial in z.

Below we give an example of this method that achieves ρ-values less than 2 with (nearly) arbitrary D; this example was found by fixing k and executing a computer search through the space of possible $t(x)$ and $h(x)$.

Example 6.16. Let $k = 6$. Let

$$\begin{aligned} t(x) &= -4x^2 + 4x + 2, \\ r(x) &= 16x^4 - 32x^3 + 12x^2 + 4x + 1, \\ q(x) &= 4x^5 - 8x^4 + 3x^3 - 3x^2 + \frac{17}{4}x + 1. \end{aligned}$$

Let D be a square-free positive integer not dividing $2 \cdot 3 \cdot 5 \cdot 911$. Then the triple $(t(Dz^2), r(Dz^2), q(Dz^2))$ parameterizes a complete family of curves with embedding degree 6 and discriminant D. The ρ-value of this family is $5/4$.

Proof. Note that $r(x) = \Phi_6(t(x)-1)$. Now let $h(x) = x/4$, which gives $q(x) = h(x)r(x) + t(x) - 1$. Under the substitution $x = Dz^2$, the CM equation (6.5) becomes

$$Dy^2 = x\big(4x^2 - 6x + 1\big)^2 = Dz^2\big(4D^2z^4 - 6Dz^2 + 1\big)^2.$$

Since $4q(x)$ and $r(x)$ are irreducible in $\mathbb{Z}[x]$, it follows from Proposition 6.22 below that $r(Dz^2)$ is irreducible when D does not divide $16 \operatorname{disc} r(x) = 2^{20}3^3$, and $q(Dz^2)$ is irreducible when D does not divide $64 \operatorname{disc} 4q(x) = 2^{22}5^3911$. Finally, since $q(0) = 1$ for any value of D, we conclude that $q(Dz^2)$ represents primes whenever $D \nmid 2 \cdot 5 \cdot 911$. □

We conclude this section with a construction, due to Koblitz and Menezes, that may be viewed as an example of the Scott–Barreto construction with $h(x) = Dl^2$ for any square-free D and even l.

Example 6.17 [51, Sect. 6]. Let l be an even integer, and let D be a positive square-free integer. Define (t, r, q) by:

$$t(x) = 2,$$
$$r(x) = x,$$
$$q(x) = Dl^2x^2 + 1.$$

Then (t, r, q) parameterizes a complete family of elliptic curves with embedding degree 1 and discriminant D. The ρ-value of this family is 2.

Proof. It is clear that $r(x)$ is irreducible and $q(x)$ represents primes for any positive l and D. Furthermore, $r(x)$ divides both $q(x) + 1 - t(x) = Dl^2x^2$ and $\Phi_1(t(x) - 1) = 0$. □

Koblitz and Menezes give two explicit elliptic curves with $D = 1$, with equations $y^2 = x^3 - x$ if $lx \equiv 0 \pmod 4$ and $y^2 = x^3 - 4x$ if $lx \equiv 2 \pmod 4$. Both of these curves have the special feature that $E(\mathbb{F}_q) \cong \mathbb{Z}/(lx)\mathbb{Z} \times \mathbb{Z}/(lx)\mathbb{Z}$. Curves in this family are equipped with distortion maps; see Sect. 7.2 for a more detailed discussion. The advantage of this construction is the great freedom in the choice of x and l, which allows us to choose r and q of low Hamming weight or some other special form.

There is some disagreement in the literature as to whether or not elliptic curves with embedding degree 1 and only a single cyclic subgroup of order r are suitable for pairing-based cryptography. While it is commonly believed that $E(\mathbb{F}_q)[r]$ must be isomorphic to $(\mathbb{Z}/r\mathbb{Z})^2$ in order to guarantee a nontrivial Tate pairing (see, e.g., [44,45]), this condition is in fact not necessary [76]. The confusion may result from the fact that on curves with $k > 1$, all r-torsion points are defined over $\mathbb{F}_{q^k}$ [3, Lemma 2]. In practice, however, $k = 1$ curves constructed via the CM method do have all r-torsion points defined over the base field. Specifically, we have the following:

Proposition 6.18. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve that has embedding degree 1 with respect to a prime r. Suppose that E has CM discriminant D. Let $\mathcal{O}$ be the ring of integers in $\mathbb{Q}(\sqrt{-D})$, and let C be the conductor $[\mathcal{O} : \mathrm{End}(E)]$. If $r \nmid 2CD$, then $E[r] \subset E(\mathbb{F}_q)$.*

Proof. Since E has embedding degree 1 with respect to r, we have $q \equiv 1 \pmod r$ and $t \equiv 2 \pmod r$. The fact that E has CM discriminant D means that we can write $4q - t^2 = Dy^2$, and since r is prime to D, it follows that $y \equiv 0 \pmod r$. If $\pi \in \mathcal{O}$ is the Frobenius endomorphism of E, then $\pi = \frac{1}{2}(t \pm y\sqrt{-D})$. Since r is odd, we can write $\pi - 1 = \alpha r$ for some $\alpha \in \mathcal{O}$. The conductor C necessarily divides $[\mathcal{O} : \mathbb{Z}[\pi]]$, which is equal to y if $D \equiv 3 \pmod 4$ and $y/2$ otherwise. Since $r \nmid C$, we see that C also divides $[\mathcal{O} : \mathbb{Z}[\alpha]] = y/r$ or $y/2r$, respectively. It follows that $\mathbb{Z}[\alpha] \subset \mathrm{End}(E)$, and therefore α corresponds to an endomorphism of E. We conclude that $E[r] \subset E[\alpha r] = E[\pi - 1] = E(\mathbb{F}_q)$. □

6.4. *More Discriminants in Cyclotomic Families*

The examples given by Brezing and Weng and others assume that the CM discriminant D is fixed in advance, so that all curves are constructed with the same D. In particular, most of the examples given by Brezing and Weng and all of those given by Barreto, Lynn, and Scott require that $D = 3$. Curves with $D = 3$ have the unusual property of having an automorphism group of order 6, and while such curves are favorable for implementation purposes (see Sect. 7.3), the extra structure may be used to aid a future (as yet unknown) discrete logarithm attack. This is an example of the "hard-line" position on security articulated by Koblitz [50]:

> All parameters for a cryptosystem must always be chosen with the maximal possible degree of randomness, because any extra structure or deviation from randomness might some day be used to attack the system.

Users taking this viewpoint will want families of pairing-friendly elliptic curves with variable CM discriminant D.

Note that since D is square-free by definition, elliptic curves with different CM discriminants are necessarily in different isogeny classes. Constructing elliptic curves in the same isogeny class with different endomorphism rings provides no additional security, since the discrete logarithm problems on a pair of such curves can be reduced to each other in less time than it takes to construct the curves themselves via the CM method [16].

We now show that if the polynomials (t, r, q) that parameterize a complete family of elliptic curves have a certain form, we may obtain families with (nearly) arbitrary discriminant. In particular, this allows us to make D a parameter input at the time of curve construction rather than at the time the polynomials t, r, q are computed.

Recall that a triple (t, r, q) *parameterizes a potential family of elliptic curves* if it satisfies conditions (2)–(5) of Definition 2.7(i).

Theorem 6.19. *Suppose that (t, r, q) parameterizes a complete potential family of elliptic curves with embedding degree k and discriminant D. Let $y(x)$ be as in Definition 2.7*(iv)*. Suppose that t, r, and q are even polynomials and y is an odd polynomial. Define t', r', q', y' to be polynomials such that*

$$t(x) = t'\left(x^2\right), \qquad r(x) = r'\left(x^2\right), \qquad q(x) = q'\left(x^2\right), \qquad y(x) = x \cdot y'\left(x^2\right).$$

Let α be a positive integer such that

(a) *αD is square-free,*
(b) *$r'(\alpha x^2)$ is irreducible, and*
(c) *$y'(\alpha x^2)$ is an integer for some integer x.*

Then the triple $(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$ parameterizes a complete potential family of elliptic curves with embedding degree k, discriminant αD, and ρ-value equal to $\rho(t, r, q)$.

Proof. For any integer $\alpha > 0$ satisfying conditions (a)–(c), we must verify conditions (2)–(5) of Definition 2.7(i) for the triple $(t'(\alpha x^2),\ r'(\alpha x^2), q'(\alpha x^2))$. If $r'(\alpha x^2)$ is irre-

ducible, then condition (2) on $r'(\alpha x^2)$ follows from the same condition on $r(x)$. Conditions (3) and (4) are identities on the polynomials t, r, q, so they still hold when we evaluate at $\sqrt{\alpha}x$. Finally, evaluating the CM equation (6.1) at $\sqrt{\alpha}x$ gives the identity

$$4q'\big(\alpha x^2\big) - t'\big(\alpha x^2\big)^2 = D \cdot \alpha x^2 \cdot y'\big(\alpha x^2\big)^2.$$

Since $y'(\alpha x^2)$ is an integer for some x, it is an integer for infinitely many x, and condition (5) follows.

To prove the last statement, we observe that

$$\rho\big(t'\big(\alpha x^2\big), r'\big(\alpha x^2\big), q'\big(\alpha x^2\big)\big) = \frac{2\deg q'}{2\deg r'} = \frac{\deg q}{\deg r} = \rho(t, r, q). \qquad \square$$

It follows from Theorem 6.19 that if t, r, q are even polynomials and $\sqrt{-D} \bmod r(x)$ is an odd polynomial, then the substitution $x^2 \mapsto \alpha x^2$ may give potential family of curves with discriminant αD. The difficult part in obtaining a family in the sense of Definition 2.7(i) is ensuring that $q'(\alpha x^2)$ represents primes; in particular, we often find that $\gcd\{q(x) : x, q(x) \in \mathbb{Z}\} > 1$.

Our first application of Theorem 6.19 is to the following construction, which improves on Construction 6.2 for certain odd values of k.

Construction 6.20. Let k be odd. Let

$$\begin{aligned} t(x) &= 1 + (-1)^{(k+1)/2} x^{k+1}, \\ r(x) &= \Phi_{4k}(x), \\ q(x) &= \frac{1}{4}\big(x^{2k+2} + x^{2k} + 4(-1)^{(k+1)/2} x^{k+1} + x^2 + 1\big). \end{aligned} \tag{6.6}$$

Then (t, r, q) parameterizes a complete potential family of pairing-friendly elliptic curves with embedding degree k and discriminant 1. The ρ-value of this family is $(k+1)/\varphi(k)$.

Proof. We apply Theorem 6.1 with $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_k, \sqrt{-1})$. We choose $\zeta_k \mapsto (-1)^{(k+1)/2} x^{k+1}$ and $\sqrt{-1} \mapsto x^k$. Then

$$\frac{\zeta_k - 1}{\sqrt{-1}} \mapsto \big(1 - (-1)^{(k+1)/2} x^{k+1}\big) x^k \equiv (-1)^{(k+1)/2} x + x^k \bmod r(x),$$

so we can choose $y(x) = (-1)^{(k+1)/2} x + x^k$. We may then compute

$$q(x) = \frac{1}{4}\Big(\big((-1)^{(k+1)/2} x^{(k+1)} + 1\big)^2 + \big((-1)^{(k+1)/2} x + x^k\big)^2\Big),$$

which simplifies to (6.6). The ρ-value of $(k+1)/\varphi(k)$ follows from $\deg q = 2k+2$ and $\deg r = 2\varphi(k)$. $\square$

When $k \equiv 1 \pmod 4$ (i.e., when the middle term of $q(x)$ is negative), $q(x)$ has a factor $(x^2 - 1)^2$, and thus we do not obtain a family of curves in the sense of Definition 2.7(i).

On the other hand, computations with Magma [15] show that $q(x)$ is irreducible for all $k < 1000$ with $k \equiv 3 \pmod 4$, and based on this evidence, we conjecture that $q(x)$ is irreducible for all $k \equiv 3 \pmod 4$. In addition, $q(x)$ is an integer whenever x is odd. Unfortunately, we find that $q(x)$ is always even when x is odd, so q fails condition (5) of Definition 2.5 and thus does not represent primes.

But all is not lost! We note that t, r, q of Construction 6.20 are even polynomials and $y(x)$ is an odd polynomial, so for certain values of α, we may apply Theorem 6.19 to make the substitution $x^2 \mapsto \alpha x^2$ in t, r, q. We will use the following algebraic results to show that in most cases the new triple $(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$ parameterizes a family of curves.

Lemma 6.21. *Let $L = \mathbb{Q}(\theta)$ be a number field, and let $f(x)$ be the minimal polynomial of θ. Then for any $\alpha \in L$, $f(\alpha x^2)$ is irreducible if and only if $\alpha\theta$ is not a square in L.*

Proof. The proof follows exactly the proof of [36, Lemma 1]. We observe that the argument holds regardless of whether L is Galois. □

Proposition 6.22. *Let $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ be irreducible. Let α be a square-free integer that does not divide $a_0 a_d \operatorname{disc} f$. Then $f(\alpha x^2)$ is irreducible.*

Proof. Let θ be a root of $f(x)$ in $\overline{\mathbb{Q}}$, and let $L = \mathbb{Q}(\theta)$. If $f(\alpha x^2)$ is reducible, then by Lemma 6.21 the element $\alpha\theta$ is a square in L, and therefore the fractional ideal $(\alpha\theta)$ is a square. Thus to prove the statement, it suffices to show that there is some prime $\mathfrak{p} \subset \mathcal{O}_L$ that divides the integral ideal (α) exactly and has exponent zero in the fractional ideal decomposition

$$(\theta) = \prod \mathfrak{p}_i^{e_i}. \tag{6.7}$$

Now observe that any prime $\mathfrak{p}_i$ with nonzero exponent e_i in (6.7) must lie over a prime p with nonzero valuation in $|\mathrm{Norm}_{L/\mathbb{Q}}\theta| = |a_0/a_d|$. The hypothesis $\alpha \nmid a_0 a_d \operatorname{disc} f$ thus implies that there is some rational prime $p \mid \alpha$ that is unramified in L and whose factors in L appear with exponent zero in (6.7). Since p is unramified and α is square free, any prime $\mathfrak{p}$ lying over p must divide (α) exactly, which completes the proof. □

Corollary 6.23. *Let k be a positive integer, and let α be a square-free integer with $\alpha \nmid k$. Then $\Phi_k(\alpha x^2)$ is irreducible.*

Proof. We apply Proposition 6.22 with $f(x) = \Phi_k(x)$, using the fact that any prime dividing $\operatorname{disc} \Phi_k$ also divides k. For $k = 1$ or 2, the result follows directly from the square-free property of α. □

We now return to the task of applying Theorem 6.19 to Construction 6.20. Since k is odd, the $r(x)$ of Construction 6.20 is equal to $\Phi_{4k}(x) = \Phi_k(-x^2)$. It thus follows from Corollary 6.23 that (in the notation of Theorem 6.19) $r'(\alpha x^2) = \Phi_k(-\alpha x^2)$ is irreducible for any square-free $\alpha \nmid k$, so condition (b) of Theorem 6.19 is satisfied for such α. Furthermore, condition (c) is clearly satisfied since $y(x) = x^k + (-1)^{(k+1)/2} x$

has integer coefficients. Thus by Theorem 6.19, the substitution $x^2 \mapsto \alpha x^2$ gives a potential family of curves with discriminant α for any positive square-free $\alpha \nmid k$.

To obtain a family of curves in the sense of Definition 2.7(i), it remains only to check that the new q, which we denote as

$$q_\alpha(x) = \frac{1}{4}\left(\alpha^{k+1}x^{2k+2} + \alpha^k x^{2k} + 4(-\alpha)^{(k+1)/2}x^{k+1} + \alpha x^2 + 1\right),$$

represents primes. Since $4q_1(\sqrt{x})$ is a monic polynomial with constant term 1, it defines a number field $L = \mathbb{Q}(\theta)$ with θ a unit in $\mathcal{O}_L$. By Proposition 6.22 and the fact that $\operatorname{disc} f(x^2) = (\operatorname{disc} f(x))^2$, we conclude that if $k \equiv 3 \pmod 4$ and $k < 1000$, then for any square-free α not dividing $\operatorname{disc} q(x)$, the polynomial $q_\alpha(x)$ is irreducible. Other than by checking each value of α and k individually, we have no way of showing that $\gcd(\{q_\alpha(x) : x, q_\alpha(x) \in \mathbb{Z}\}) = 1$. In practice it appears that, for various k and square-free α both congruent to 3 (mod 4), this condition does hold and therefore $q_\alpha(x)$ does indeed represent primes, but we cannot prove this result.

As in the derivation of Construction 6.3 from Construction 6.2, we may use the fact that $\zeta_{2k} = -\zeta_k$ when k is odd to derive an analogous construction for embedding degrees that are twice an odd number.

Construction 6.24. Let k be odd. Let

$$\begin{aligned} t(x) &= 1 - (-1)^{(k+1)/2}x^{k+1}, \\ r(x) &= \Phi_{4k}(x), \\ q(x) &= \frac{1}{4}\left(x^{2k+2} + x^{2k} - 4(-1)^{(k+1)/2}x^{k+1} + x^2 + 1\right). \end{aligned}$$

Then (t, r, q) parameterizes a potential family of pairing-friendly elliptic curves with embedding degree $2k$, discriminant 1, and ρ-value $(k+1)/\varphi(k)$. In terms of the embedding degree $k' = 2k$, the ρ-value is thus $(k'/2+1)/\varphi(k')$.

Proof. With $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{2k}, \sqrt{-1})$, we choose $\zeta_{2k} \mapsto -(-1)^{(k+1)/2}x^{k+1}$. The rest of the proof is identical to that of Construction 6.20. □

Computations with Magma [15] show that $q(x)$ is irreducible for all $k < 1000$ with $k \equiv 1 \pmod 4$, and based on this evidence, we conjecture that $q(x)$ is irreducible for all $k \equiv 1 \pmod 4$.

Substituting $x^2 \mapsto \alpha x^2$, we get

$$q_\alpha(x) = \frac{1}{4}\left(\alpha^{k+1}x^{2k+2} + \alpha^k x^{2k} - 4(-\alpha)^{(k+1)/2}x^{k+1} + \alpha x^2 + 1\right).$$

As in Construction 6.20, $q_\alpha(x)$ is never an integer for even α, and $q_\alpha(x)$ is even for $\alpha \equiv 1 \pmod 4$. Thus we must choose $k \equiv 1 \pmod 4$ and $\alpha \equiv 3 \pmod 4$ if we want $q_\alpha(x)$ to represent primes.

To conclude this section, we note that Constructions 6.2 and 6.3 satisfy the conditions of Theorem 6.19 for any square-free $\alpha \nmid k$. We make the substitution $x^2 \mapsto \alpha x^2$, where

α is an odd square-free integer not dividing the embedding degree k. In both cases we have k odd and $r(x) = \Phi_{4k}(x) = \Phi_k(-x^2)$, so $r'(\alpha x^2)$ is irreducible by Corollary 6.23. Furthermore by Proposition 6.22 $q'(\alpha x^2)$ is irreducible whenever $q(x)$ is irreducible and $\alpha \nmid \operatorname{disc} q$. If $q'(\alpha x^2)$ represents primes then Theorem 6.19 gives a family of pairing-friendly curves with discriminant α.

We also note that Construction 6.7 satisfies the conditions of Theorem 6.19 when k is not divisible by 8. Since $r(x) = \Phi_\ell(x) = \Phi_{\ell/2}(x^2)$ for some ℓ divisible by 8, Corollary 6.23 implies that $r'(\alpha x^2)$ is irreducible for all square-free α not dividing k. Furthermore by Proposition 6.22 $q'(\alpha x^2)$ is irreducible whenever $q(x)$ is irreducible and $\alpha \nmid \operatorname{disc} q$. Since $D = 2$ in Construction 6.7, if $q'(\alpha x^2)$ represents primes, then Theorem 6.19 gives a family of pairing-friendly curves with discriminant 2α. If $q'(\alpha x^2)$ represents primes, then α must be odd; if k is divisible by 4, then we must have $\alpha \equiv 1 \pmod 4$.

We can also apply Theorem 6.19 to the cases presented in Table 3; we leave the details to the reader.

Summary: Algorithm for Generating Variable-Discriminant Families

By combining the substitution $x^2 \mapsto \alpha x^2$ from Theorem 6.19 (for some appropriate α) with one of the basic constructions 6.2, 6.3, 6.7, 6.20, or 6.24, we can generate a family of pairing-friendly curves with variable discriminant D for any k satisfying $\gcd(k, 24) \in \{1, 2, 3, 6, 12\}$. We conclude this section with step-by-step instructions for this procedure.

(1) Select an embedding degree k with $\gcd(k, 24) \in \{1, 2, 3, 6, 12\}$.
(2) Select a basic construction from the following list. (Some values of k may offer more than one possibility; see Table 5 for the construction that minimizes ρ for each $k \leq 50$.)

- Construction 6.2 if k is odd.
- Construction 6.3 if $k \equiv 2 \pmod 4$.
- Construction 6.7 if $3 \mid k$.
- Construction 6.20 if $k \equiv 3 \pmod 4$.
- Construction 6.24 if $k \equiv 2 \pmod 8$.

(3) Use the selected basic construction to compute a triple (t, r, q) that parameterizes a family of elliptic curves with embedding degree k.
(4) Let t', r', q' be polynomials such that $t(x) = t'(x^2)$, $r(x) = r'(x^2)$, and $q(x) = q'(x^2)$.
(5) Select a square-free positive integer $\alpha \nmid k \operatorname{disc} q$ such that after the substitution $x^2 \mapsto \alpha x^2$, the resulting polynomial $q'(\alpha x^2)$ represents primes. (In each case, $r'(\alpha x^2)$ is irreducible by Corollary 6.23, and $q'(\alpha x^2)$ is irreducible by Proposition 6.22.) This condition requires α to have the following form:

- α odd for Constructions 6.2, 6.3, and 6.7 with $4 \nmid k$.
- $\alpha \equiv 1 \pmod 4$ for Construction 6.7 with $4 \mid k$.
- $\alpha \equiv 3 \pmod 4$ for Constructions 6.20 and 6.24.

(6) Let $D = 2\alpha$ if Construction 6.7 was used, and let $D = \alpha$ otherwise.

Then $(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$ parameterizes a family of elliptic curves with embedding degree k and discriminant D. In particular, for values of α and x such that $q'(\alpha x^2)$ is prime, there is an elliptic curve over $\mathbb{F}_{q'(\alpha x^2)}$ with a subgroup of order $r'(\alpha x^2)$ and embedding degree k. If $D < 10^{12}$, the equation for this curve can be computed by the CM method.

Note that the Cocks–Pinch method (Theorem 4.1) can be used to generate elliptic curves with arbitrary CM discriminant for any embedding degree k. However, the ρ-values of such curves will always be around 2. The advantage of the procedure outlined above is that we can vary the CM discriminant *and* obtain ρ-values strictly less than 2 for many values of k.

7. Implementation Considerations

There are many factors to take into account when choosing an elliptic curve for use in a pairing-based cryptosystem. To discuss each factor in detail would take us too far afield; rather, our goal in this section is to mention the pertinent issues and refer the reader to the literature for more detail.

Scott [79] has conducted an extensive survey of implementation considerations for pairing-friendly elliptic curves. In addition, Page, Smart, and Vercauteren [69] give a detailed comparison of MNT curves (Sect. 5.1) with supersingular curves (Sect. 3).

7.1. *Balancing Security*

When choosing an elliptic curve for pairing applications, one usually begins by fixing in advance a desired bit size b_1 for the prime-order subgroup of the elliptic curve and a desired bit size b_2 for the finite field in which the discrete logarithm must be infeasible. To achieve these bit sizes exactly one must have $b_2/b_1 = \rho \cdot k$. This relation may allow a number of choices for curves with the desired security levels. In general, a smaller ρ is desirable to minimize bandwidth requirements and the time necessary to perform elliptic curve arithmetic. For example, a curve with $k = 4$ and $\rho = 2$ over a 320-bit field provides the same security levels as a (hypothetical) curve with $k = 8$ and $\rho = 1$ over a 160-bit field; however, points on the former curve generally require twice as much storage space and base field operations take roughly four times as much time.

While in general choosing minimal ρ for the same security levels will optimize performance, there are other factors that may affect performance, most notably twists (Sect. 7.3 below). A (hypothetical) curve with $k = 6$ and $\rho = 4/3$ over a 214-bit field $\mathbb{F}_q$ would provide the same security as the curves in the previous example, but if the curve had a sextic twist, the group operations could be computed in $\mathbb{F}_q$ instead of $\mathbb{F}_{q^k}$. Whether this would be faster than the $k = 8$, $\rho = 1$ curve would likely depend on the specific implementation.

Furthermore, there is no reason that the subgroup and field sizes need to be exactly the minimum necessary for desired security, and unbalancing one of the parameters may in fact improve performance. To continue with our example, a curve with $k = 6$ and $\rho = 2$ over a 320-bit field overshoots our desired security level for discrete log in the finite field, but such a curve may be advantageous if it has a sextic twist. (And such curves do in fact exist!) In general, if $\rho \cdot k > b_2/b_1$, then the finite field will be larger

than required, and if $\rho \cdot k < b_2/b_1$, then the elliptic curve subgroup will be larger than required. We also note that curves with $\rho > 2$ could be chosen to balance $\rho \cdot k$ with b_2/b_1, though such curves would in general have inefficient group operations.

7.2. *Distortion Maps*

Most pairings used in cryptography have the property that they are degenerate when the inputs (P, Q) are linearly dependent. On the other hand, many protocols require that the two inputs to the pairing be from the same cyclic group $\langle P \rangle$. One way of getting around this conflict is to use a *distortion map*, which is an efficiently computable endomorphism ϕ such that $\phi(P) \notin \langle P \rangle$. A distortion map exists for a curve E with embedding degree $k > 1$ if and only if E is supersingular [35,87]. For the $k = 1$ case, see Charles' paper [20] for a thorough discussion and Sect. 6.3 above for an example.

On ordinary elliptic curves there are other means of getting around the problem of the degeneracy of pairings on linearly dependent points, and ordinary elliptic curves can be used in almost all pairing-based protocols. However, the proofs of security for some of these protocols rest on the existence of distortion maps, and thus for such protocols, one must choose supersingular curves if "provable security" is desired. For a thorough discussion of security assumptions and a categorization of the different types of groups used in pairings, see the paper of Chen, Cheng, and Smart [21].

7.3. *Twists and Compression*

A *twist* of $E/\mathbb{F}_q$ is an elliptic curve $E'/\mathbb{F}_q$ that is isomorphic to E over $\overline{\mathbb{F}}_q$. The minimal d for which E and E' are isomorphic over $\mathbb{F}_{q^d}$ is the *degree* of the twist. All elliptic curves have quadratic (i.e., degree 2) twists. The only curves with higher-order twists are those with CM discriminant 1 (defined by equations of the form $y^2 = x^3 + ax$), which have quartic twists, and those with CM discriminant 3 (defined by equations of the form $y^2 = x^3 + b$), which have cubic and sextic twists. (For a more theoretical description of twisting, see [82, Chap. X]. Over fields of characteristic 2 or 3, the situation is slightly more complicated, but the degree of a twist must still divide 6.)

In general, the points input into a pairing on a curve of embedding degree k take the form $P \in E(\mathbb{F}_q)$, $Q \in E(\mathbb{F}_{q^k})$. However, Barreto, Lynn, and Scott [7] use the quadratic twist to show that when k is even, one can take Q to be a point on $E'(\mathbb{F}_{q^{k/2}})$, where E' is a quadratic twist of E. In fact we usually prefer k to be even as this facilitates the "denominator elimination" optimization of Barreto, Kim, Lynn, and Scott [6]. Barreto and Naehrig [4] extend this idea to curves with sextic twists and embedding degree k divisible by 6, showing that Q can be taken to be a point on $E'(\mathbb{F}_{q^{k/6}})$, where E' is a sextic twist of E. Hess, Smart, and Vercauteren [42, Sect. 5] unify these ideas in a general framework that also takes into account cubic and quartic twists.

On any curve with embedding degree k that has a degree-d twist with $d \mid k$, the output of the Tate pairing can be given as an element of $\mathbb{F}_{q^{k/d}}$ instead of $\mathbb{F}_{q^k}$, with the loss of $\lceil \log_2 d \rceil$ bits of information. This "compression" technique was introduced for quadratic twists by Scott and Barreto [80] and extended to sextic twists by Barreto and Naehrig [4]; similar ideas apply to quartic and cubic twists. While these techniques apply only to the output of the pairing, Naehrig, Barreto, and Schwabe [67] give methods for executing the entire pairing computation over a proper subfield of $\mathbb{F}_{q^k}$.

A twist of degree k on a curve with embedding degree k would be ideal for implementation, as it would allow all curve points and pairing values to be given over the base field $\mathbb{F}_q$. Unfortunately, such a curve must either be supersingular or have ρ-value nearly 2. The precise formulation of this statement and its proof were presented to us by Frederik Vercauteren.

Proposition 7.1. *Let E be an elliptic curve over $\mathbb{F}_q$ with a subgroup of prime order $r > 3$ and embedding degree $k > 1$ with respect to r. If E has a twist $E'/\mathbb{F}_q$ of degree k and $r > 4\sqrt{q}$, then E is supersingular.*

Proof. By [42, Theorem 3] there is a unique degree-k twist of E such that r divides $\#E'(\mathbb{F}_q)$. We take E' to be this twist. The hypothesis $r > 4\sqrt{q}$ implies that there is at most one multiple of r in the Hasse interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$, and since $\#E(\mathbb{F}_q)$ and $\#E'(\mathbb{F}_q)$ must both be in this interval by Hasse's theorem, we conclude that $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$. By Tate's theorem [85, Theorem 1] there is an isogeny $\psi : E \to E'$ defined over $\mathbb{F}_q$.

The hypothesis that E' is a twist of E of degree $k > 1$ tells us that E and E' are isomorphic over an extension field of $\mathbb{F}_q$ but are not isomorphic over $\mathbb{F}_q$. Composing this isomorphism with the isogeny ψ gives an endomorphism ϕ of E that is not defined over $\mathbb{F}_q$. Since ϕ is not defined over $\mathbb{F}_q$, it does not commute with the Frobenius endomorphism of E. We conclude that $\mathrm{End}(E)$ is noncommutative, and therefore E must be supersingular. □

As an immediate corollary, if E is an ordinary elliptic curve with embedding degree $k > 1$ and a degree-k twist, then $r \leq 4\sqrt{q}$, so $\rho(E) \geq 2 - \frac{4 \log 2}{\log r}$. In particular, any ordinary family with one of the of the following combinations of embedding degree and discriminant must have ρ-value at least 2: embedding degree 6 and discriminant 3; embedding degree 4 and discriminant 1; or embedding degree 2 and any discriminant (cf. Proposition 2.9). Such families do exist: see, for example, Construction 6.4 for $k = 4$, $D = 1$, or Construction 6.6 for $k = 6$, $D = 3$.

7.4. *Extension Field Arithmetic*

Arithmetic in the extension field $\mathbb{F}_{q^k}$ can be implemented very efficiently if this field can be built up as a "tower" of extension fields,

$$\mathbb{F}_q \subset \mathbb{F}_{q^{d_1}} \subset \mathbb{F}_{q^{d_2}} \subset \cdots \subset \mathbb{F}_{q^k},$$

where the ith extension field $\mathbb{F}_{q^{d_i}}$ is obtained by adjoining a root of a polynomial $x^{d_i/d_{i-1}} + \beta_i$ for some $\beta_i \in \mathbb{F}_{q^{d_{i-1}}}$ that are "small" in the sense that they can be represented using very few bits. This property is likely to apply if $k = 2^a 3^b$ for some a, b, so pairings may be computed more quickly on curves with embedding degree of this form.

Koblitz and Menezes [51, Sect. 5] show that if $k = 2^a 3^b$ and $q \equiv 1 \pmod{12}$, then $\mathbb{F}_{q^k}$ can be built in one step by adjoining a root of $x^k + \beta$ for some (not necessarily small) $\beta \in \mathbb{F}_q$. Barreto and Naehrig [4, Sect. 3] give a construction for $k = 12$ consisting of adjoining a square root followed by a sixth root.

7.5. *Low Hamming Weight*

The standard Miller algorithm for computing pairings [63] works by a double-and-add iteration on the bits of the prime subgroup order r. The "add" part of the computation is executed for each bit of r that is set to 1, so the pairing computation may be executed more quickly if r has low Hamming weight. The constructions of supersingular curves (Sect. 3.2) and Cocks–Pinch curves (Sect. 4.1) allow for r to be chosen arbitrarily, so a prime of low Hamming weight can be chosen. If r is given by a polynomial $r(x)$ such as those in the constructions of Sect. 6.1, then choosing x of low Hamming weight will often give low Hamming weight r as well. In general, the degree of control over the Hamming weight depends roughly on the degree of the polynomial $r(x)$, and this control is much greater for complete families of curves than for sparse ones.

If the field size q is a prime of low Hamming weight, then field operations can be computed more quickly. However, for such q, the discrete logarithm problem in $\mathbb{F}_q^\times$ becomes somewhat easier due to the better performance of the Number Field Sieve in this case [77]. Thus q will have to be slightly larger to achieve the same level of security, counteracting somewhat the performance boost for field operations.

8. Conclusion: Your One-Stop Shop for Pairing-Friendly Curves

The selection of a pairing-friendly elliptic curve for a given application depends on many factors. The most important are the desired security levels in the elliptic curve group $E(\mathbb{F}_q)$ and in the multiplicative group $\mathbb{F}_{q^k}^\times$. However the choice of a curve may also be influenced by the choice of pairing used, the need for speed in the pairing computation, the level of precision necessary in the bit sizes, and doubts about the security level of curves with "special" properties, such as supersingular curves, curves with extra automorphisms, curves defined over very small fields (e.g., Koblitz curves), or curves with extremely small CM discriminant. Thus in our quest to fulfill the title of this section, we present several different options for choice of curves.

To implement pairing-friendly curves in real life, depending on the security level desired, an administrator will choose (minimum) bit sizes desired for the prime-order subgroup of the elliptic curve and of the extension field, and select a construction method from our recommendations below. If the construction produces a sparse family of curves, then to find explicit parameters one uses the MNT method as described in Sect. 5. If the construction produces a complete family of curves $(t(x), r(x), q(x))$, to compute parameters for a specific curve one then must loop through inputs x of the appropriate size until an x_0 is found such that $q(x_0)$ is a prime integer, $t(x_0)$ is an integer, and $r(x_0)$ is prime or has a large prime factor. If the degrees of these polynomials are too large relative to the desired security levels, finding such an x_0 may be difficult.

Specifically, let $g(x)$ be a polynomial of degree d. We approximate $g(x)$ as x^d and compute the number of $(b+1)$-bit numbers produced by $g(x)$. This is the number of x such that $x^d \in [2^b, 2^{b+1})$, which is $2^{b/d}(2^{1/d} - 1)$. Since $2^{1/d} - 1 \approx \log(2)/d$, the number of such x is roughly $2^{b/d}\log(2)/d$. Finally, by the prime number theorem, the probability that a number of size around 2^b is prime is approximately $1/(b\log 2)$. Thus the expected number of x such that $g(x)$ is a $(b+1)$-bit prime number is approximately $\frac{2^{b/d}}{bd}$.

Table 4. Maximum degree of $r(x)$ for various security levels.

Security level (bits)	$r(x)$ (bits)	$\max \deg r(x)$
80	160	10
112	224	12
128	256	16
192	384	20
256	512	24

The consequence of this heuristic result is that if we are using a family to generate pairing-friendly curves and wish to specify precisely the field and subgroup sizes, the degrees of the polynomials $r(x)$ and $q(x)$ cannot be too large. For example, if we were trying to generate curves having a 512-bit subgroup with $r(x)$ of degree 32, we would expect to find only about four 512-bit prime values of $r(x)$. The requirement that $q(x)$ is prime imposes even stricter conditions; if $q(x)$ has degree ρd, then only around $1/\rho b$ of the x that give prime values for r will also give prime values for q.

Table 4 gives the maximum recommended values of $\deg r$ for various security levels if strict control of the field and subgroup sizes is desired. For each bit size $b+1$ of $r(x)$, we compute d such that $2^{b/d}/(b^2 d \log 2) = 1$ and recommend $\max \deg r(x)$ slightly larger than this d.

If one is willing to be flexible about the bit sizes of the curve parameters, then one may be able to increase x indefinitely until prime $q(x)$ and $r(x)$ are found, and in lucky cases the first instance where this occurs will be near the desired bit size. For example, let $q(x)$ and $r(x)$ be the polynomials given by Construction 6.6 with $k = 32$; these polynomials have degrees 34 and 32, respectively. If we are looking for a 512-bit prime-order subgroup to match the security level of 256-bit AES, choosing $x = 66100$ makes $q(x)$ a 543-bit prime and $r(x)$ a 513-bit prime, which is very close to our specified bit size.

Even so, if $\deg r(x) > 40$, we expect to find very few prime values even of $r(x)$ alone that are as large as 512 bits. Therefore, we cannot recommend any families of curves with $\deg r(x)$ so high.

Remark 8.1. If we can apply Theorem 6.19 to vary the CM discriminant as well as x, then we will be able to generate more prime values of $q(x)$ and $r(x)$. In particular, since the degrees of $q'(\alpha x^2)$ and $r'(\alpha x^2)$ in α are half the degrees in x, if we fix x and vary the square-free part of the parameter α, we can expect to find more prime values than if we fix α and vary x. This idea first appears in the paper of Comuta, Kawazoe, and Takahashi [23], who independently demonstrated examples of this approach; their construction is equivalent to applying Theorem 6.19 to our Constructions 6.3 and 6.24 and fixing $x = 1$. The restriction that the square-free part of α be (roughly) less than 10^{12} will not in general pose a problem, since even with $x = 1$ we may still find values of r with as many as $20 \cdot \deg r(x)$ bits. Thus for constructions using Theorem 6.19, it is perfectly acceptable to take $\deg r(x)$ as large as 80.

8.1. *Our Recommendations: Curves with $\rho \approx 2$*

If minimizing ρ is not desired, we recommend the Cocks–Pinch method (Sect. 4.1). This method has several advantages: it works for any embedding degree k, it works for any

CM discriminant D (within the limits of the CM method, roughly $D < 10^{12}$), and the size r of the prime-order subgroup $E(\mathbb{F}_q)$ is chosen in advance. The only disadvantage is that ρ is around 2, so the number of bits needed to specify a point on E will be about twice the minimum number of bits needed to obtain a given level of security.

8.2. *Our Recommendations: Curves with $\rho < 2$*

In this section we assume that the user wishes to minimize the parameter ρ, for example, to save bandwidth in applications. Table 5 gives the best known values of ρ for families of curves with embedding degree $k \leq 50$. These values of k should cover all desired security levels for the foreseeable future.

For each embedding degree k, Table 5 gives the best ρ-value achieved by two different constructions.

The first construction listed is the one that yields the smallest ρ-value when the CM discriminant D is 1 or 3. The curve equations for these values of D are particularly easy to compute; if q is prime to 6, the curves over $\mathbb{F}_q$ are given by

$$E_1 : y^2 = x^3 + ax \quad (D = 1),$$
$$E_3 : y^2 = x^3 + b \quad (D = 3).$$

By choosing a random point on $E(\mathbb{F}_q)$ and multiplying by the expected curve order $q + 1 - t$, one can quickly determine the residue class of $a \bmod (\mathbb{F}_q^\times)^4$ (if $D = 1$) or $b \bmod (\mathbb{F}_q^\times)^6$ (if $D = 3$) that gives the desired twist of E.

Curves with $D = 1$ or 3 have both low-degree endomorphisms and twists; the former may be used to speed up elliptic curve arithmetic [38], while the latter can speed up pairing computation for certain embedding degrees k (see Sect. 7.3). The table shows that in a large majority of cases, the optimal ρ-value is achieved by Construction 6.6; other constructions do better for some small k, $k \equiv 4 \pmod 6$, and k divisible by 18.

However, there are known methods to improve the efficiency of Pollard's rho algorithm on curves with $D = 1$ or 3 [28]. These methods lead to a decrease in security of only a few bits, but some users may take their existence as a warning that curves with small CM discriminant are in some sense special and should be avoided. Therefore, we also indicate the optimal ρ-values for families with variable CM discriminant, the allowed discriminants D, and the constructions which produce these ρ-values. Here, whenever we indicate (in the last column) a construction of the form 6.x+, this means that the corresponding basic construction from Sect. 6 is combined with the substitution $x^2 \mapsto \alpha x^2$ (Theorem 6.19) to construct curves with variable D; see the algorithm on p. 266 for details. Note that to date we know of no variable-discriminant construction when $k = 20$ or when k is a multiple of 8; in these cases a family with $D \leq 3$ or a Cocks–Pinch curve must be used.

We have checked that all of the families listed in Table 5 can be used to produce explicit examples of pairing-friendly elliptic curves and have confirmed that for parameters of cryptographic size, the ρ-value of a curve is very close to the ρ-value of its family.

All families in the table except for one lead to curves over prime fields, and the minimum embedding field is $\mathbb{F}_{q^k}$ for such curves. The lone exception is the supersingular

Table 5. Best ρ-values for families of curves with $k \leq 50$.
See Page 274 for explanations of the symbols and fonts.

	fixed $D \leq 3$				variable D			
k	ρ	D	$\deg r(x)$	Constr.	ρ	D	$\deg r(x)$	Constr.
1	2.000	3	2	6.6	2.000	any	1	6.17
2	any$^{\#}$	1,3	–	Sect. 3.2	any$^{\#}$	3 mod 4	–	Sect. 3.2
3	**1.000**$^{\#}$	3	2	Sect. 3.3	**1.000**	some	2	Sect. 5.1-5.2
4	1.500	3	4	6.9	**1.000**	some	2	Sect. 5.1-5.2
5	1.500	3	8	6.6	1.750	any odd	8	6.2+
6	1.250	1	4	6.16	**1.000**	some	2	Sect. 5.1-5.2
7	1.333†	3	12	6.6, 6.20+	1.333†	3 mod 4	12	6.20+
8	1.250	3	8	6.6	–	–	–	–
9	1.333	3	6	6.6	1.833	any odd	12	6.2+
10	1.500	1,3	8	6.5, 6.24+	**1.000**	some	4	Sect. 5.3
11	1.200†	3	20	6.6, 6.20+	1.200†	3 mod 4	20	6.20+
12	**1.000**	3	4	6.8	1.750	2 mod 8	8	6.7+
13	1.167†	3	24	6.6	1.250	any odd	24	6.2+
14	1.333†	3	12	6.6	1.500	any odd	12	6.3+
15	1.500	3	8	6.6	1.750	any even	32	6.7*+
16	1.250	1	8	6.11	–	–	–	–
17	1.125†	3	32	6.6	1.188	any odd	32	6.2+
18	1.333	3	6	6.12	1.583	2 mod 4	24	6.7+
19	1.111†	3	36	6.6	1.111†	3 mod 4	36	6.20+
20	1.375	3	16	6.6	–	–	–	–
21	1.333	3	12	6.6	1.792	2 mod 4	48	6.7+
22	1.300†	1	20	6.3	1.300†	any odd	20	6.3+
23	*1.091*†	3	*44*	*6.6, 6.20*+	1.091†	3 mod 4	44	6.20+
24	1.250	3	8	6.6	–	–	–	–
25	1.300†	3	40	6.6	1.350	any odd	40	6.2+
26	1.167†	3	24	6.6, 6.24+	1.167†	3 mod 4	24	6.24+
27	1.111	3	18	6.6	1.472	2 mod 4	72	6.7+
28	1.333†	1	12	6.4	1.917	6 mod 8	24	6.7*+
29	*1.071*†	3	*56*	*6.6*	1.107	any odd	56	6.2+
30	1.500	3	8	6.6	1.813	2 mod 4	32	6.7+
31	*1.067*†	3	*60*	*6.6, 6.20*+	1.067†	3 mod 4	60	6.20+
32	1.063†	3	32	6.6	–	–	–	–
33	1.200	3	20	6.6	1.575	2 mod 4	80	6.7+
34	1.125†	3	32	6.24+	1.125†	3 mod 4	32	6.24+
35	*1.500*†	3	*48*	*6.6, 6.20*+	1.500†	3 mod 4	48	6.20+
36	1.167	3	12	6.14	1.417†	2 mod 8	24	6.7+
37	*1.056*†	3	*72*	*6.6*	1.083	any odd	72	6.2+
38	1.111†	3	36	6.6	1.167	any odd	36	6.3 +
39	1.167	3	24	6.6	*1.521*	*2 mod 4*	*96*	*6.7*+
40	1.375	1	16	6.15	–	–	–	–
41	*1.050*†	3	*80*	*6.6*	1.075	any odd	80	6.2+
42	1.333	3	12	6.6	1.625	2 mod 4	48	6.7+
43	*1.048*†	3	*84*	*6.6, 6.20*+	*1.048*†	*3 mod 4*	*84*	*6.20*+
44	1.150†	3	40	6.6	1.750	6 mod 8	40	6.7*+

Table 5. (*continued*)

	fixed $D \leq 3$				variable D			
k	ρ	D	$\deg r(x)$	Constr.	ρ	D	$\deg r(x)$	Constr.
45	1.333	3	24	6.6	*1.729*	*2 mod 4*	*96*	*6.7*+
46	*1.136*†	1	*44*	*6.3*	1.136†	any odd	44	6.3+
47	*1.043*†	3	*92*	*6.6*	*1.043*†	*3 mod 4*	*92*	*6.20*+
48	1.125	3	16	6.6	–	–	–	–
49	*1.190*†	3	*84*	*6.6*	*1.214*	*any odd*	*84*	*6.2*+
50	1.300†	3	40	6.6, 6.24+	1.300†	3 mod 4	40	6.24+

family with $k = 3$. The minimum embedding field for a curve in this family is either $\mathbb{F}_{q^3}$ or $\mathbb{F}_{q^{3/2}}$; see Sect. 3.3 for details.

Explanation of Symbols in Table 5

bold Entries in bold in the table indicate that curves of prime order can be constructed with the given embedding degree.

italic Entries in italic indicate that while the ρ-value achieved for the given family may be optimal, the degrees of the polynomials involved are too high to make the construction practical. For fixed-discriminant curves, we require $\deg r \leq 40$, and for variable-discriminant curves, we require $\deg r \leq 80$; see Remark 8.1 and the preceding discussion. In cases where $\deg r(x)$ is too large, if one is not willing to allow for very little control over the bit sizes of r and q, the Cocks–Pinch method should be used to achieve the desired embedding degree and discriminant, constructing a curve with $\rho \approx 2$.

† A ρ-value marked with a † is smaller than any ρ-value previously reported. In particular, for $k \in \{7, 11, 13, 14, 17, 19\}$, we achieve ρ-values smaller than those reported by Brezing and Weng [17], who state that their ρ-values are "probably optimal."

To achieve the ρ-values marked with a #, we recommend supersingular curves.

- $k = 2$: For both the small D and the variable D cases, arbitrary ρ-values can be easily achieved with supersingular curves (see Sect. 3.2). Depending on the residue class of q (mod 12), we can construct curves with $D = 1$, $D = 3$, or $D \equiv 3 \pmod 4$ with $(\frac{-D}{q}) = -1$ (see Algorithm 3.3). As discussed in Remark 3.1, we have no hesitation recommending supersingular curves over ordinary curves with the same embedding degree.
  For those who believe that supersingular curves must be avoided, we recommend the Cocks–Pinch construction.
- $k = 3$, small D: We recommend a supersingular curve over $\mathbb{F}_{p^2}$; see Sect. 3.3. The minimal embedding field (i.e., the field in which the Weil and Tate pairings take values) will be $\mathbb{F}_{p^6} = \mathbb{F}_{q^3}$ if $t = p$ and $\mathbb{F}_{p^3} = \mathbb{F}_{q^{3/2}}$ if $t = -p$. Since the minimal embedding field—and not the embedding degree—determines discrete log security in the finite field [43], users should be careful to choose curve parameters giving the desired security level.
  If a curve over a prime field is required, Construction 6.6 gives a family with ρ-value 2.

Table 6. Families with efficient arithmetic.

k	ρ	D	Twist order	Construction
3	1.000	3	3	Sect. 3.3
4	2.000	1	4	6.4
6	2.000	3	6	6.6
8	1.500	1	4	6.10
9	1.333	3	3	6.6
12	1.000	3	6	6.8
16	1.250	1	4	6.11
18	1.333	3	6	6.12
24	1.250	3	6	6.6
27	1.111	3	3	6.6
32	1.125	1	4	6.13
36	1.167	3	6	6.14
48	1.125	3	6	6.6

+ A construction marked with a + indicates that the given basic construction is combined with the substitution $x^2 \mapsto \alpha x^2$ (Theorem 6.19) to construct families with the given discriminant; see the algorithm on page 266 for details.
* For $k = 15$, 28, or 44 and variable D, we use the same technique as in Construction 6.7, the only difference being that $y(x) \mapsto (\zeta_k - 1)/\sqrt{-2}$ reduces further modulo $r(x)$. The polynomials for the basic constructions are given in Table 3.
– Entries missing from the table for a given embedding degree k indicate that there is no known family of curves of the given type (i.e., small D or variable D) for that particular k. In these cases the Cocks–Pinch method should be used to achieve the desired embedding degree and discriminant, constructing a curve with $\rho \approx 2$.

8.3. *Our Recommendations: Curves with Efficient Arithmetic*

In Sect. 7 we saw two general techniques for speeding up pairing computations that depend on the embedding degree k: using twists to define elliptic curve points and pairing values over smaller extension fields (Sect. 7.3), and constructing extension fields in towers defined by simple polynomials (Sect. 7.4). Table 6 recommends curves that can take advantage of both of these techniques. The embedding degrees we consider are of the form $k = 2^a 3^b$, as this choice allows for the construction of extension fields in towers. If k is divisible by 4, then curves with CM discriminant 1 have twists that can be used to work over $\mathbb{F}_{q^{k/4}}$ instead of $\mathbb{F}_{q^k}$. If k is divisible by 3, then curves with CM discriminant 3 have twists that can be used to work over $\mathbb{F}_{q^{k/3}}$ (if k is odd) or $\mathbb{F}_{q^{k/6}}$ (if k is even).

For each $k = 2^a 3^b$ less than 50, Table 6 lists the family with highest-order twists; if more than one such construction exists, we choose the one with smallest ρ-value. The entries for $k = 3, 4, 6$ reflect the result of Proposition 7.1: curves with embedding degree k and a degree-k twist must either have $\rho \geq 2$ or be supersingular.

8.4. *Our Recommendations: Curves of Composite Order*

Several recently proposed protocols require curves that have small embedding degree with respect to a composite number r that is presumed to be infeasible to factor, such as

an RSA modulus. Currently, the only effective means of generating such curves are to construct supersingular curves over prime fields (Sect. 3.2) or to use the Cocks–Pinch method (see Remark 4.3).

For pairing-based cryptosystems using elliptic curves of composite order to be secure, three problems must be infeasible: the discrete logarithm on the elliptic curve $E(\mathbb{F}_q)$, the discrete logarithm in the finite field $\mathbb{F}_{q^k}^{\times}$, and factorization of the curve order $\#E(\mathbb{F}_q)$. Since there exist subexponential-time factorization algorithms but only exponential-time elliptic curve discrete log algorithms, the size of the elliptic curve group will be determined by the security level desired for the factoring problem. In particular, since factorization of a large composite number r takes roughly the same amount of time as the discrete logarithm in a finite field of size around r (as both algorithms use the Number Field Sieve), the parameters should ideally be chosen so that $\#E(\mathbb{F}_q) \approx q^k$.

We thus deduce that pairing-friendly curves of composite order should have ρ-values and embedding degrees chosen to minimize $\rho \cdot k$. By Remark 2.10 and the discussion of Sect. 3.1, we see that the smallest possible ρ-value of a curve of cryptographic size with embedding degree 1 and small CM discriminant is very close to 2. On the other hand, supersingular curves over prime fields (Sect. 3.2) have embedding degree 2 and can have ρ-values very close to 1 for any specified group order r.

We conclude that $k = 1$ ordinary curves (such as those given in Example 6.17) and $k = 2$ supersingular curves both provide the minimum possible value for $\rho \cdot k$ and are thus optimal for protocols requiring composite-order subgroups. For implementations, we recommend the supersingular option, as these curves can take advantage of the computational speedups of Sects. 7.3 and 7.4, while the $k = 1$ curves cannot.

Acknowledgements

The authors thank Paulo Barreto, Brian Conrad, Florian Hess, Ezekiel Kachisa, Ben Lynn, François Morain, Michael Naehrig, Edward Schaefer, Igor Shparlinski, Alice Silverberg, Marco Streng, Frederik Vercauteren, and the anonymous referees for helpful discussions and feedback on earlier versions of this paper. The work of the first author has been supported by a National Defense Science and Engineering Graduate Fellowship, a National Science Foundation Mathematical Sciences Postdoctoral Research Fellowship, a National Science Foundation International Research Fellowship, and the Office of Multidisciplinary Activities in the NSF Directorate for Mathematical and Physical Sciences. The second author acknowledges support from the Science Foundation Ireland under grant No. 06/MI/006. The third author is grateful to the Centrum voor Wiskunde en Informatica (CWI, Amsterdam) for its hospitality in 2006–08.

References

[1] A.O.L. Atkin, F. Morain, Elliptic curves and primality proving. *Math. Comput.* **61**, 29–68 (1993)
[2] D. Bailey, C. Paar, Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. *J. Cryptol.* **14**, 153–176 (2001)

[3] R. Balasubramanian, N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm. *J. Cryptol.* **11**, 141–145 (1998)
[4] P.S.L.M. Barreto, M. Naehrig, Pairing-friendly elliptic curves of prime order, in *Selected Areas in Cryptography—SAC 2005*. Lecture Notes in Computer Science, vol. 3897 (Springer, Berlin, 2006), pp. 319–331
[5] P.S.L.M. Barreto, B. Lynn, M. Scott, Constructing elliptic curves with prescribed embedding degrees, in *Security in Communication Networks—SCN 2002*. Lecture Notes in Computer Science, vol. 2576 (Springer, Berlin, 2002), pp. 263–273
[6] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, M. Scott, Efficient algorithms for pairing-based cryptosystems, in *Advances in Cryptology—Crypto 2002*. Lecture Notes in Computer Science, vol. 2442 (Springer, Berlin, 2002), pp. 354–368
[7] P.S.L.M. Barreto, B. Lynn, M. Scott, On the selection of pairing-friendly groups, in *Selected Areas in Cryptography—SAC 2003*. Lecture Notes in Computer Science, vol. 3006 (Springer, Berlin, 2003), pp. 17–25
[8] P.S.L.M. Barreto, S. Galbraith, C. O'hEigeartaigh, M. Scott, Efficient pairing computation on supersingular abelian varieties. *Des. Codes Cryptogr.* **42**, 239–271 (2007)
[9] P. Bateman, R. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comput.* **16**, 363–367 (1962)
[10] N. Benger, M. Charlemagne, D. Freeman, On the security of pairing-friendly abelian varieties over non-prime fields, in *Pairing-Based Cryptography—Pairing 2009*, to appear. Preprint available at: http://eprint.iacr.org/2008/417/
[11] I.F. Blake, G. Seroussi, N.P. Smart (eds.), *Advances in Elliptic Curve Cryptography* (Cambridge University Press, Cambridge, 2005)
[12] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in *Advances in Cryptology—Crypto 2001*. Lecture Notes in Computer Science, vol. 2139 (Springer, Berlin, 2001), pp. 213–229. Full version: *SIAM J. Comput.* **32**(3), 586–615 (2003)
[13] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, in *Advances in Cryptology—Asiacrypt 2001*. Lecture Notes in Computer Science, vol. 2248 (Springer, Berlin, 2002), pp. 514–532. Full version: *J. Cryptol.* **17**, 297–319 (2004)
[14] D. Boneh, E.-J. Goh, K. Nissim, Evaluating 2-DNF formulas on ciphertexts, in *Theory of Cryptography Conference—TCC 2005*. Lecture Notes in Computer Science, vol. 3378 (Springer, Berlin, 2005), pp. 325–341
[15] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. *J. Symb. Comput.* **24**(3–4), 235–265 (1997)
[16] A. Bostan, F. Morain, B. Salvy, É. Schost, Fast algorithms for computing isogenies between elliptic curves. *Math. Comput.* **77**, 1755–1778 (2008)
[17] F. Brezing, A. Weng, Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptogr.* **37**, 133–141 (2005)
[18] R. Bröker, Constructing elliptic curves of prescribed order. Ph.D. thesis, Dept. of Mathematics, Leiden University, 2006. Available at: http://www.math.leidenuniv.nl/~reinier/thesis.pdf
[19] J.C. Cha, J.H. Cheon, An identity-based signature from gap Diffie–Hellman groups, in *Public-Key Cryptography—PKC 2003*. Lecture Notes in Computer Science, vol. 2567 (Springer, Berlin, 2003), pp. 18–30
[20] D. Charles, On the existence of distortion maps on ordinary elliptic curves, Cryptology ePrint Archive Report 2006/128. Available at: http://eprint.iacr.org/2006/128/
[21] L. Chen, Z. Cheng, N. Smart, Identity-based key agreement protocols from pairings. *Int. J. Inf. Secur.* **6**, 213–241 (2007)
[22] C. Cocks, R.G.E. Pinch, Identity-based cryptosystems based on the Weil pairing. Unpublished manuscript, 2001
[23] A. Comuta, M. Kawazoe, T. Takahashi, Pairing-friendly elliptic curves with small security loss by Cheon's algorithm, in *Information Security and Cryptography—ICISC 2007*. Lecture Notes in Computer Science, vol. 4817 (Springer, Berlin, 2007), pp. 297–308
[24] D. Coppersmith, Fast evaluation of logarithms in fields of characteristic two. *IEEE Trans. Inf. Theory* **30**, 587–594 (1984)
[25] G. Cornell, J. Silverman (eds.), *Arithmetic Geometry* (Springer, New York, 1986)

[26] P. Duan, S. Cui, C.W. Chan, Effective polynomial families for generating more pairing-friendly elliptic curves, Cryptology ePrint Archive Report 2005/236. Available at: http://eprint.iacr.org/2005/236/
[27] R. Dupont, A. Enge, F. Morain, Building curves with arbitrary small MOV degree over finite prime fields. *J. Cryptol.* **18**, 79–89 (2005)
[28] I. Duursma, P. Gaudry, F. Morain, Speeding up the discrete log computation on curves with automorphisms, in *Advances in Cryptology—Asiacrypt 1999*. Lecture Notes in Computer Science, vol. 1716 (Springer, Berlin, 1999), pp. 103–121
[29] A. Enge, The complexity of class polynomial computation via floating point approximations. *Math. Comput.* **78**, 1089–1107 (2009)
[30] D. Freeman, Constructing pairing-friendly elliptic curves with embedding degree 10, in *Algorithmic Number Theory Symposium—ANTS-VII*. Lecture Notes in Computer Science, vol. 4076 (Springer, Berlin, 2006), pp. 452–465
[31] D. Freeman, Constructing pairing-friendly genus 2 curves with ordinary Jacobians, in *Pairing-Based Cryptography—Pairing 2007*. Lecture Notes in Computer Science, vol. 4575 (Springer, Berlin, 2007), pp. 152–176
[32] D. Freeman, A generalized Brezing–Weng method for constructing pairing-friendly ordinary abelian varieties, in *Pairing-Based Cryptography—Pairing 2008*. Lecture Notes in Computer Science, vol. 5209 (Springer, Berlin, 2008), pp. 146–163
[33] D. Freeman, P. Stevenhagen, M. Streng, Abelian varieties with prescribed embedding degree, in *Algorithmic Number Theory Symposium—ANTS-VIII*. Lecture Notes in Computer Science, vol. 5011 (Springer, Berlin, 2008), pp. 60–73
[34] G. Frey, H. Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comput.* **62**, 865–874 (1994)
[35] S. Galbraith, V. Rotger, Easy decision Diffie–Hellman groups. *LMS J. Comput. Math.* **7**, 201–218 (2004)
[36] S. Galbraith, J. McKee, P. Valença, Ordinary abelian varieties having small embedding degree. *Finite Fields Appl.* **13**, 800–814 (2007)
[37] S. Galbraith, K. Paterson, N. Smart, Pairings for cryptographers. *Discrete Appl. Math.* **15**, 3113–3121 (2008)
[38] R. Gallant, R.J. Lambert, S.A. Vanstone, Faster point multiplication on elliptic curves with efficient endomorphisms, in *Advances in Cryptology—Crypto 2001*. Lecture Notes in Computer Science, vol. 2139 (Springer, Berlin, 2001), pp. 190–200
[39] R. Granger, D. Page, N. Smart, High security pairing-based cryptography revisited, in *Algorithmic Number Theory Symposium ANTS-VII*. Lecture Notes in Computer Science, vol. 4076 (Springer, Berlin, 2006), pp. 480–494
[40] K. Harrison, D. Page, N.P. Smart, Software implementation of finite fields of characteristic three, for use in pairing-based cryptosystems. *LMS J. Comput. Math.* **5**, 181–193 (2002)
[41] F. Hess, Pairing lattices, in *Pairing-Based Cryptography—Pairing 2008*. Lecture Notes in Computer Science, vol. 5209 (Springer, Berlin, 2008), pp. 18–38
[42] F. Hess, N. Smart, F. Vercauteren, The Eta pairing revisited. *IEEE Trans. Inf. Theory* **52**, 4595–4602 (2006)
[43] L. Hitt, On the minimal embedding field, in *Pairing-Based Cryptography—Pairing 2007*. Lecture Notes in Computer Science, vol. 4575 (Springer, Berlin, 2007), pp. 294–301
[44] A. Joux, A one round protocol for tripartite Diffie–Hellman, in *Algorithmic Number Theory Symposium—ANTS-IV*. Lecture Notes in Computer Science, vol. 1838 (Springer, Berlin, 2000), pp. 385–393. Full version: *J. Cryptol.* **17**, 263–276 (2004)
[45] A. Joux, K. Nguyen, Separating decision Diffie–Hellman from computational Diffie–Hellman in cryptographic groups. *J. Cryptol.* **16**, 239–247 (2003)
[46] E. Kachisa, Constructing Brezing–Weng pairing friendly elliptic curves using elements in the cyclotomic field. M.Sc. dissertation, Mzuzu University, 2007
[47] E. Kachisa, E. Schaefer, M. Scott, Constructing Brezing–Weng pairing friendly elliptic curves using elements in the cyclotomic field, in *Pairing-Based Cryptography—Pairing 2008*. Lecture Notes in Computer Science, vol. 5209 (Springer, Berlin, 2008), pp. 126–135
[48] K. Karabina, On prime-order elliptic curves with embedding degrees 3, 4 and 6. M.Math. thesis, Univ. of Waterloo, Dept. of Combinatorics and Optimization, 2006

[49] K. Karabina, E. Teske, On prime-order elliptic curves with embedding degrees 3, 4 and 6, in *Algorithmic Number Theory Symposium—ANTS-VIII*. Lecture Notes in Computer Science, vol. 5011 (Springer, Berlin, 2008), pp. 102–117
[50] N. Koblitz, Good and bad uses of elliptic curves in cryptography. *Mosc. Math. J.* **2**, 693–715 (2002) 805–806
[51] N. Koblitz, A. Menezes, Pairing-based cryptography at high security levels, in *Proceedings of Cryptography and Coding: 10th IMA International Conference*. Lecture Notes in Computer Science, vol. 3796 (Springer, Berlin, 2005), pp. 13–36
[52] S. Lang, *Elliptic Functions* (Springer, Berlin, 1987)
[53] S. Lang, *Algebra*, revised 3rd edn. (Springer, Berlin, 2002)
[54] A.K. Lenstra, Unbelievable security: Matching AES security using public key systems, in *Advances in Cryptology—Asiacrypt 2001*. Lecture Notes in Computer Science, vol. 2248 (Springer, Berlin, 2001), pp. 67–86
[55] R. Lidl, H. Niederreiter, *Finite Fields* (Cambridge University Press, Cambridge, 1997)
[56] F. Luca, I. Shparlinski, Elliptic curves with low embedding degree. *J. Cryptol.* **19**, 553–562 (2006)
[57] F. Luca, D. Mireles, I. Shparlinski, MOV attack in various subgroups on elliptic curves. *Ill. J. Math.* **48**, 1041–1052 (2004)
[58] K. Matthews, The Diophantine equation $x^2 - Dy^2 = N$, $D > 0$. *Expo. Math.* **18**, 323–331 (2000)
[59] A. Menezes, *Elliptic Curve Public Key Cryptosystems* (Kluwer Academic, Dordrecht, 1993)
[60] A. Menezes, An introduction to pairing-based cryptography. Notes from lectures given in Santander, Spain, 2005. Available at: http://www.cacr.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf
[61] A. Menezes, S. Vanstone, Isomorphism classes of elliptic curves over finite fields of characteristic 2. *Util. Math.* **38**, 135–153 (1990)
[62] A. Menezes, T. Okamoto, S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inf. Theory* **39**, 1639–1646 (1993)
[63] V. Miller, The Weil pairing, and its efficient calculation. *J. Cryptol.* **17**, 235–261 (2004)
[64] A. Miyaji, M. Nakabayashi, S. Takano, New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans. Fundam.* **E84-A**(5), 1234–1243 (2001)
[65] F. Morain, Classes d'isomorphismes des courbes elliptiques supersingulières en caracteristique ≥ 3. *Util. Math.* **52**, 241–253 (1997)
[66] A. Murphy, N. Fitzpatrick, Elliptic curves for pairing applications, Cryptology ePrint Archive Report 2005/302. Available at: http://eprint.iacr.org/2005/302
[67] M. Naehrig, P.S.L.M. Barreto, P. Schwabe, On compressible pairings and their computation, in *Progress in Cryptology—Africacrypt 2008*. Lecture Notes in Computer Science, vol. 5023 (Springer, Berlin, 2008), pp. 371–388
[68] A. Odlyzko, Discrete logarithms in finite fields and their cryptographic significance, in *Advances in Cryptology—Eurocrypt 1984*. Lecture Notes in Computer Science, vol. 209 (Springer, Berlin, 1985), pp. 224–314
[69] D. Page, N. Smart, F. Vercauteren, A comparison of MNT curves and supersingular curves. *Appl. Algebra Eng., Commun. Comput.* **17**, 379–392 (2006)
[70] K. Paterson, ID-based signatures from pairings on elliptic curves. *Electron. Lett.* **38**, 1025–1026 (2002)
[71] S. Pohlig, M. Hellman, An improved algorithm for computing discrete logarithms over $GF(p)$ and its cryptographic significance. *IEEE Trans. Inf. Theory* **24**, 106–110 (1978)
[72] J. Pollard, Monte Carlo methods for index computation (mod p). *Math. Comput.* **32**, 918–924 (1978)
[73] J. Robertson, Solving the generalized Pell equation $x^2 - Dy^2 = N$. Unpublished manuscript, 2004. Available at: http://hometown.aol.com/jpr2718/pell.pdf
[74] K. Rubin, A. Silverberg, Finding composite order ordinary elliptic curves using the Cocks–Pinch method, in preparation
[75] R. Sakai, K. Ohgishi, M. Kasahara, Cryptosystems based on pairings, in *2000 Symposium on Cryptography and Information Security—SCIS 2000*, Okinawa, Japan, 2000
[76] E. Schaefer, A new proof for the non-degeneracy of the Frey–Rück pairing and a connection to isogenies over the base field, in *Computational Aspects of Algebraic Curves*. Lecture Notes Ser. Comput., vol. 13 (World Scientific, Singapore, 2005), pp. 1–12
[77] O. Schirokauer, The number field sieve for integers of low weight. *Math. Comput.* to appear. Preprint available at: http://eprint.iacr.org/2006/107/

[78] M. Scott, Computing the Tate pairing, in *Topics in Cryptology—CT-RSA 2005*. Lecture Notes in Computer Science, vol. 3376 (Springer, Berlin, 2005), pp. 293–304
[79] M. Scott, Implementing cryptographic pairings, in *Pairing-Based Cryptography—Pairing 2007*. Lecture Notes in Computer Science, vol. 4575 (Springer, Berlin, 2007), pp. 177–196
[80] M. Scott, P.S.L.M. Barreto, Compressed pairings, in *Advances in Cryptology—Crypto 2004*. Lecture Notes in Computer Science, vol. 3152 (Springer, Berlin, 2004), pp. 140–156
[81] M. Scott, P.S.L.M. Barreto, Generating more MNT elliptic curves. *Des. Codes Cryptogr.* **38**, 209–217 (2006)
[82] J. Silverman, *The Arithmetic of Elliptic Curves* (Springer, Berlin, 1986)
[83] A. Sutherland, Computing Hilbert class polynomials with the Chinese remainder theorem. Preprint, 2009. Available at http://arxiv.org/abs/0903.2785
[84] S. Tanaka, K. Nakamula, Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials, in *Pairing-Based Cryptography—Pairing 2008*. Lecture Notes in Computer Science, vol. 5209 (Springer, Berlin, 2008), pp. 136–145
[85] J. Tate, Endomorphisms of abelian varieties over finite fields. *Invent. Math.* **2**, 134–144 (1966)
[86] P.C. van Oorschot, M.J. Wiener, Parallel collision search with cryptanalytic applications. *J. Cryptol.* **12**, 1–18 (1999)
[87] E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *J. Cryptol.* **17**, 277–296 (2004)
[88] W. Waterhouse, Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (IV)* **2**, 521–560 (1969)