A TAXONOMY OF PAIRING-FRIENDLY ELLIPTIC CURVES

DAVID FREEMAN[1], MICHAEL SCOTT[2], AND EDLYN TESKE[3]

[1] University of California, Berkeley
dfreeman@math.berkeley.edu

[2] Dublin City University
mike@computing.dcu.ie

[3] University of Waterloo
eteske@math.uwaterloo.ca

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 currently existing in the literature. We also include new constructions of pairing-friendly elliptic 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.

Keywords. Elliptic curves, pairing-based cryptosystems, embedding degree, Tate pairing, Ate pairing, efficient implementation.

1. Introduction

There has been much interest over the past few years in cryptographic schemes based on pairings on elliptic curves. In a flurry of recent research results, many new and novel protocols have been suggested, including one-round three-way key exchange [35], identity-based encryption [64, 9], identity-based signatures [14, 59], and short signature schemes [11]. 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 [4] and the recently discovered Ate pairing [34]. All of the proposed pairings take as input points on an elliptic curve E defined over a finite field $\mathbb{F}_q$ and give as output an element of an extension field $\mathbb{F}_{q^k}$. For the system 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 [61, 56], 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., [55]) 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 is the degree k of the extension field required by the pairing; and the parameter $\rho = \log q / \log r$, which measures the 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 Section 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) [42, 57]. 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 1.1 our own view of the matter, distilled from material taken from various authoritative sources, in particular [29] and [42]. 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.

TABLE 1.1. 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

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, 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 $\rho \cdot k = 8$.

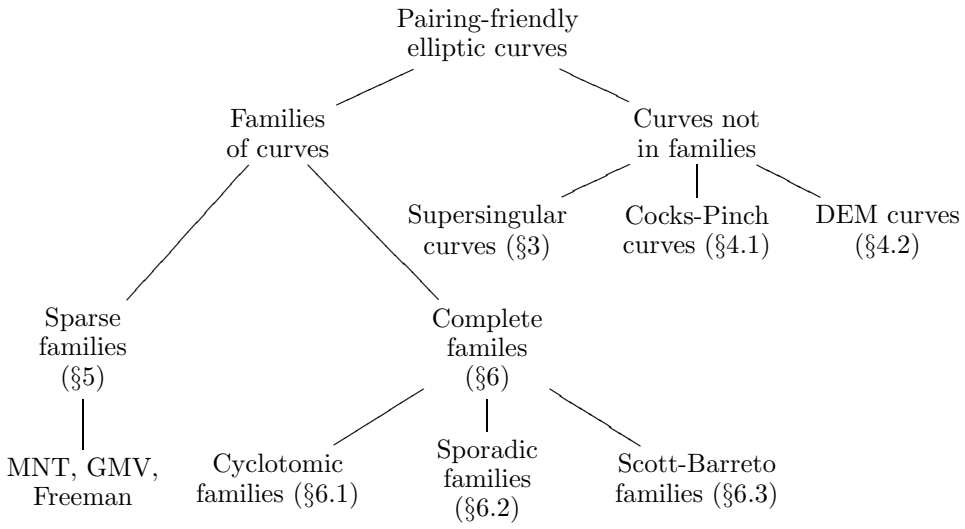
In general, curves with small ρ-values are desirable in order to speed up arithmetic on the elliptic curve. For example, an elliptic curve with a 160-bit subgroup and $\rho = 1$ is defined over a 160-bit field, while a curve with a 160-bit subgroup and $\rho = 2$ is defined over a 320-bit field, and 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 protocols [67]. Therefore $k = 2$ (marked with an asterisk) has been included in Table 1.1 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 1.2.

The designers of the first pairing-based protocols proposed the use of supersingular elliptic curves [9]. However, such curves are limited to embedding degree $k = 2$ for prime fields and $k \leq 6$ in general [49], 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 and an integer n, and constructs an elliptic curve over $\mathbb{F}_q$ with n points [1]. In Section 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.

TABLE 1.2. Classification of pairing-friendly elliptic curves



The highest-level distinction we make in our framework is between methods that construct individual curves and those that construct families of curves. The former type are methods that give integers q and n such that there is an elliptic curve E over $\mathbb{F}_q$ with n points and embedding degree k. The latter type are methods that give polynomials $q(x)$ and $n(x)$ such that if $q(x)$ is prime for some value of x, there is an elliptic curve E over $\mathbb{F}_{q(x)}$ with $n(x)$ points and embedding degree k. Families of curves have the advantage that the sizes of the finite field and the prime-order subgroup can be varied simply by specifying x.

Supersingular curves, which we discuss in Section 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 [17] and that of Dupont, Enge, and Morain [22]. In Section 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 Section 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, i.e. 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 Section 5, are primarily based on the ideas of Miyaji, Nakabayashi, and Takano [52]. These families give most of the known constructions

of curves of prime order, but are limited to embedding degrees $k \leq 10$. Complete families, discussed in Section 6, exist for arbitrary k but usually give curves with $\rho > 1$. All of the constructions of complete families can be viewed as choosing a number field $K \cong \mathbb{Q}[x]/(f(x))$ and computing polynomials in $\mathbb{Q}[x]$ that map to certain elements of K. We can then further classify the complete families according to the properties of the number field K. We briefly list the families and the corresponding type of number field.

- Cyclotomic families (§6.1): K is a cyclotomic field. Constructions given in [5, 12, 37].
- "Sporadic" families (§6.2): K is an extension of a cyclotomic field, and K contains $\sqrt{-D}$ for some small D. Constructions given in [7], new examples in §6.2.
- Scott-Barreto families (§6.3): K is an extension of a cyclotomic field, and K contains no $\sqrt{-D}$ for any small D. Constructions given in [69].

1.3. **New constructions.** In addition to classifying construction methods, in Section 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 such families will be most useful in practice.

In Section 6.1, we use the method of Brezing and Weng to demonstrate families of pairing-friendly elliptic curves with $\rho < 2$ for every embedding degree k 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 2.6).

In Sections 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 Section 6.1.

Our most significant contribution with regard to new constructions is Theorem 6.23. The constructions of Sections 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*. But some users might 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 6.23, which, given a family of curves with fixed discriminant, 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 6.23 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 Section 6.4 we use Theorem 6.23 to give examples of variable-discriminant families for any embedding degree k satisfying $\gcd(k, 24) \in \{1, 2, 3, 6, 12\}$. In particular, Constructions 6.25 and 6.28 combine Theorem 6.23 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. Furthermore, the families with $k \equiv 10 \pmod{24}$ have ρ-value smaller than any other known complete family, with fixed (in advance) or variable discriminant.

1.4. **Recommendations.** The body of this paper gathers in one place for the first time all known constructions of pairing-friendly elliptic curves. In Section 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 8.2. For each embedding degree k, $1 \leq k \leq 50$, the table gives two options: a family of curves with CM discriminant 1, 2, or 3, and a 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.

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

Section 8.4 discusses curves that are optimal for the Ate pairing, and gives a list of constructions from Section 6 from which to choose for this purpose.

Finally, Section 8.5 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 [10], are used in a number of recent protocols and are an active subject of research.

1.5. **Acknowledgments.** The authors thank Paulo Barreto, Florian Hess, Ezekiel Kachisa, Ben Lynn, Michael Naehrig, Edward Schaefer, Igor Shparlinski, Alice Silverberg, and Frederik Vercauteren for helpful discussions and feedback on earlier versions of this paper. The first author is supported by a National Defense Science and Engineering Graduate Fellowship. The third author is grateful to the Centrum voor Wiskunde en Informatica (CWI, Amsterdam) for its hospitality in 2006-07.

2. How to generate pairing-friendly curves

We assume the reader is familiar with elliptic curves and finite fields; for a good exposition of the former, see Silverman's book [70], and for the latter, see the book of Lidl and Niederreiter [43]. 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. For any integer r, we let $E[r]$ denote the group of all r-torsion points of E (defined over an algebraic closure of K), and by $E(K)[r]$ the group of r-torsion points of E that are defined over K.

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 $|t| \leq 2\sqrt{q}$ [70, 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 [70, Theorem V.3.1].) If the ring of endomorphisms of E, denoted $\mathrm{End}(E)$, is strictly larger than $\mathbb{Z}$, then we say E has

complex multiplication or E is a *CM curve*. All elliptic curves over finite fields are CM curves, with $\mathrm{End}(E) \otimes \mathbb{Q}$ 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 [49] and Frey and Rück [27], 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, the Weil pairing is a map

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

where $\overline{K}$ is an algebraic closure of K and μ_r is the group of rth roots of unity in $\overline{K}$ [70, §III.8]. If L is the smallest extension of K containing the rth roots of unity, the Weil pairing "embeds" the discrete logarithm in $E[r]$ into the multiplicative group of L, and we call the degree of the extension $[L : K]$ 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. The *embedding degree of E with respect to r* is the degree of the smallest extension field L/K containing the rth roots of unity μ_r.

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 multiplicative order of q modulo r.

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

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 [44] 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 [60], 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 [45], 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 1.1.

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 [49], 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 $\mathbb{F}_q$.

An 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) r divides $q + 1 - t$.
(4) r divides $q^k - 1$, and $r \nmid q^i - 1$ for $1 \leq i < k$.
(5) $4q - t^2 = Dy^2$ 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 (5) implies that $t \leq 2\sqrt{q}$, and thus there exists an elliptic curve E defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$ (cf. [73]). Conditions (2) and (3) combine to tell us that $E(\mathbb{F}_q)$ has a subgroup of prime order r. By Remark 2.2, condition (4) 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 elliptic curve $E/\mathbb{F}_q$ with embedding degree k and an order-r subgroup. The requirement

that D be sufficiently small in condition (5) 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, originally 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 roughly $O(h_{\mathcal{O}})^{2+\epsilon}$, where $h_{\mathcal{O}}$ is the class number of the order $\mathcal{O}$ [13, 24]. Given current computational power, the method can construct curves when $h_{\mathcal{O}} \leq 10^5$ [24]. In practice we almost always take $\mathcal{O}$ to be the ring of integers in $\mathbb{Q}(\sqrt{-D})$; in this case the class number $h_{\mathcal{O}}$ grows roughly as $O(\sqrt{D})$, and we see that "sufficiently small" in condition (5) can be taken to be $D < 10^{10}$.

The equation in condition (5) is called the *CM equation*. If we use condition (3) 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 [43]. 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 all $\ell < k$. 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 phi 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 $r \nmid k$. 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 [48, Lemma 6.3]. 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 (4) necessary to construct a pairing-friendly curve with the following:

(4) 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 parametrizing t, r, q as polynomials has been used by several different authors in their constructions, including Miyaji, Nakabayashi, and Takano [52]; Barreto, Lynn, and Scott [5]; Scott and Barreto [69]; and Brezing and Weng [12]. 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 [41, p. 323]) says that a non-constant $f(x)$ takes an infinite number of prime values if and only if f has positive leading coefficient, f is irreducible, and $\gcd(\{f(x) : x \in \mathbb{Z}\}) = 1$.

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

(1) $f(x)$ is non-constant.
(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) $\gcd(\{f(x) : x, f(x) \in \mathbb{Z}\}) = 1$.

For future reference, we note that if there is some x such that $f(x) = \pm 1$, then conditions (4) and (5) are both satisfied. We are now prepared to define families of pairing-friendly curves.

Definition 2.6. Let $t(x)$, $r(x)$, and $q(x)$ be polynomials with rational coefficients.

(i) For a given positive integer k and positive square-free integer D, the triple (t, r, q) *represents 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) $r(x) = c \cdot \tilde{r}(x)$ for some constant $c \in \mathbb{N}$ and $\tilde{r}(x)$ that represents primes.
  (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).

(ii) We say that a family (t, r, q) is *complete* if for any integer x there is some y that satisfies the equation $Dy^2 = 4q(x) - t(x)^2$; otherwise we say that the family is *sparse*.

(iii) We say that (t, r, q) represents a *potential* family of curves if conditions (2)–(5) of (i) are satisfied; in this case $q(x)$ may or may not represent primes.

Part (i) of Definition 2.6 is designed so that if (t, r, q) represents a family of curves with embedding degree k, and (x_0, y_0) is a solution to the equation of condition (5) such that $p(x_0)$ and $\tilde{r}(x_0)$ are prime, then there exists an elliptic curve $E/\mathbb{F}_{q(x_0)}$ with a subgroup of prime order $\tilde{r}(x_0)$ and embedding degree k. If $D < 10^{10}$ then E can be constructed via the CM method. In practice we will usually have $d = 1$ in condition (1), so $q(x)$ will represent primes and the curves we construct will be defined over prime fields.

Condition (3) of Definition 2.6 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 2.7.

(i) Let $E/\mathbb{F}_q$ be an elliptic curve, and suppose 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 (t, r, q) represents a family of elliptic curves with embedding degree k. The *ρ-value of the family represented by* (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 (t, r, q) represents curves of prime order, then $\deg r = \deg q$ and $\rho = 1$; 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.

The most common pairing used in applications is the Tate pairing, which can in general be computed faster than the Weil pairing [32]. Recently, a new pairing called the Ate pairing has been proposed [34], which in some cases can be computed even more quickly than the Tate pairing. The computation of the Ate pairing executes a loop on the bits of $t - 1$, so this pairing is most efficient when the value of t is small with respect to the size of the prime-order subgroup. We incorporate this property into our next definition. (See Section 7.6 for further discussion of the Ate pairing.)

Definition 2.8.

(i) Let $E/\mathbb{F}_q$ be an elliptic curve with trace $t \neq 0$, and suppose E has a subgroup of order r. The *ω-value of E (with respect to r)* is

$$\omega(E) = \frac{\log r}{\log |t|}.$$

(ii) Let $t(x), r(x), q(x) \in \mathbb{Q}[x]$, and suppose (t, r, q) represents a family of elliptic curves with embedding degree k. If $t(x) \neq 0$, the *ω-value of the family represented by (t, r, q)*, denoted $\omega(t, r, q)$, is

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

The Hasse bound $|t| \leq 2\sqrt{q}$ implies that $\rho(t, r, q)\omega(t, r, q) \geq 2$, so families of pairing-friendly curves will have $\omega \geq 1$. (For individual pairing-friendly curves, $\omega(E) \geq 1 - \frac{\log 2}{\log |t|}$.) On the other hand, the following proposition gives an upper bound for $\omega(t, r, q)$ in most cases.

Proposition 2.9. *Suppose (t, r, q) represents a family of elliptic curves with embedding degree $k \geq 3$. Then $\omega(t, r, q) \leq \varphi(k)$.*

Proof. By Proposition 2.4, E has embedding degree k if and only if $\Phi_k(t(x)-1) \equiv 0 \mod r(x)$, i.e. $t(x) - 1$ is a primitive kth root of unity in $K \cong \mathbb{Q}[x]/(r(x))$. Thus either $\Phi_k(t(x) - 1)$ is identically zero or $\deg \Phi_k(t(x) - 1) \geq \deg r(x)$. If $\deg t(x) = 0$ then $t(x) - 1$ is a primitive kth root of unity contained in $\mathbb{Q}$, contradicting the assumption $k \geq 3$. Thus $t(x)$ is a polynomial of degree at least 1, and we see that $\Phi_k(t(x) - 1)$ is not identically zero. We then have

$$\deg \Phi_k(t(x) - 1) = \varphi(k) \cdot \deg t(x) \geq \deg r(x).$$

Dividing both sides of the inequality by $\deg t(x)$, we conclude that $\omega \leq \varphi(k)$. □

Remark 2.10. One can show that for individual curves E with embedding degree $k \geq 3$, we have $\omega(E) \leq \varphi(k)(1 + \varepsilon)$ with $\varepsilon \to 0$ as $r \to \infty$.

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

Proposition 2.11. *Suppose (t, r, q) represents 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.*

   In the first case, we also have $\omega(t, r, q) \leq 1$.
(2) *If $k = 2$, then $\rho(t, r, q) \geq 2$ and $\omega(t, r, q) \leq 1$.*

Proof. Since $r(x)$ divides $\Phi_k(t(x) - 1)$ and $\deg \Phi_k = 1$, if $\Phi_k(t(x) - 1) \neq 0$ then we must have $\deg t(x) \geq \deg r(x)$. Thus $\omega(t, r, q) \leq 1$, and 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 supersingular, 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 (1b) 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 2.12. For $k = 1$, the hypothesis (1b) is necessary to show that families with trace 2 have ρ-values at least 2. However, for any individual trace 2 curve $E/\mathbb{F}_q$ with an order-r subgroup, we have $Dy^2 = 4\#E(\mathbb{F}_q)$, so if r is square-free and prime to D then $r^2 \mid \#E(\mathbb{F}_q)$, so $\rho(E)$ will be at least $2 - \frac{2\log 2}{\log r}$. One can then use the same reasoning as in the proof of Proposition 2.11 to show that any other ordinary curve with $k = 1$ or 2 has $|t| \approx r$, so by the Hasse bound $\rho \approx 2$.

More precisely, suppose $E/\mathbb{F}_q$ has embedding degree $k \leq 2$ with respect to r, and let D be the CM discriminant of E. If either

(1) $k = 1$, r is square-free, and $\gcd(r, D) = 1$, or
(2) $k = 2$, E is ordinary, and q and r are prime,

then one can show that $\rho(E) \geq 2(1 - \varepsilon)$, with $\varepsilon \to 0$ as $r \to \infty$.

We also note that while the ω-values of trace 2 curves are large, the Ate pairing is degenerate on such curves, so the large ω-values are of no practical use.

3. Supersingular curves

Recall that the 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 $\gcd(t, q) > 1$. 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 $q \geq 5$. By the Hasse bound, group orders of supersingular curves are of the form $q + 1 - t$ with $t^2 \in \{0, q, 2q, 3q, 4q\}$. Menezes [47] has characterized prime-order supersingular curves with embedding degrees $k = 3, 4, 6$. For fields of characteristic two and three, representatives for each $\mathbb{F}_q$-isomorphism class of supersingular curves have been determined by Menezes and Vanstone [50] and Morain [53], respectively.

The only known general method to construct supersingular curves is using 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 primes $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$ respectively. These two curves will suffice for most applications; a complete algorithm for constructing a supersingular curve over any given prime field is described in Section 3.2.

As supersingular curves with $k \neq 2$ 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 two or three and fields of the form $\mathbb{F}_{p^2}$ for large p; we give data for characteristic three fields only if no constructions for characteristic two 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 [19], the fields $\mathbb{F}_q$ must be larger when $q = 2^s$ or 3^s than when $q = p$ or p^2.

Remark 3.1. Supersingular curves are widely perceived as "weak" curves, and thus as not desirable for cryptographic applications. However, as Koblitz and Menezes [39] argue, "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, as opposed to ordinary curves with embedding degree $k > 1$, supersingular curves have the added advantage that they have distortion maps (in the sense of Verheul [72]), which is a desirable feature in some pairing-based applications. See Section 7.2 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. Then we can write $q - 1 = (\sqrt{q} + 1)(\sqrt{q} - 1)$, so $r \mid q - 1$ if $r \mid (\sqrt{q} + 1)$ or $r \mid (\sqrt{q} - 1)$. For a supersingular curve with $k = 1$ over $\mathbb{F}_q$, this requires $\#E(\mathbb{F}_q) = q \pm 2\sqrt{q} + 1$, that is, $t = \pm 2\sqrt{q}$ [8], and we see that 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 $(x + i\sqrt{q'})(x - i\sqrt{q'})$. The Weil conjectures [70, 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 will see in Section 3.2 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 for $E/\mathbb{F}_q$ 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. Furthermore, if for some reason we want our curve to have $q + 2\sqrt{q} + 1$ points, we may simply take a quadratic twist (over $\mathbb{F}_q$) of the curve with $q - 2\sqrt{q} + 1$ points.

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 $\rho(E') = \rho_0/2$.

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 size and 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 [70, §5.4]. Specifically, 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 [50].

Construction of supersingular curves in characteristic greater than 3 makes use of the following theorem:

Theorem 3.2 ([40, Theorem 13.12])**.** *Let L be a number field, and E/L be an elliptic curve with complex multiplication. Suppose* $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-D})$*. Let $\mathfrak{p} \mid p$ be a prime of L where E has good reduction. Then the reduction of $E \mod \mathfrak{p}$ 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 even h such that $q = hr - 1$ is prime, then we have the following algorithm (combining the constructions of Koblitz and Menezes [39, §7] and Bröker [13, §3.4]) for constructing a curve over $\mathbb{F}_q$ with embedding degree 2 with respect to r.

(1) If $q \equiv 3 \pmod 4$, return $y^2 = x^3 + ax$ for any $a \in \mathbb{F}_q^\times$.

(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 $c \in \mathbb{F}_q^\times$.

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 Section 7.5 for details.) In particular, Boheh, Goh, and Nissim [10] 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 CM discriminant 1 and 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 [39] give explicit determinations of the distortion maps in both cases.

3.3. **Embedding degree $k = 3$.** A supersingular curve over $\mathbb{F}_q$ of prime order has embedding degree $k = 3$ if and only if $q = p^s$ with s even, and $t = \pm\sqrt{q}$ [52]. In characteristic $p > 3$, the only such curves are those of the form

$$y^2 = x^3 + \gamma,$$

where γ is a non-cube in $\mathbb{F}_q^\times$ [53]. 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. We find the corresponding result for the curves with $t = p$ and $p = 3x + 1$.

We can recast these results in our language of "families" (Definition 2.6). Let

$$\begin{aligned} t(x) &= \pm 3x + 1, \\ r(x) &= 9x^2 \pm 3x + 1, \\ q(x) &= (3x \pm 1)^2. \end{aligned}$$

Since $4q(x) - t(x)^2 = 3(3x \pm 1)^2$, the triple (t, r, q) represents a family of elliptic curves with embedding degree 3 and discriminant 3. The ρ-value for this family is 1; in particular, if $r(x)$ and $3x \pm 1$ are prime then we may construct a curve over $\mathbb{F}_{q(x)}$ with embedding degree 3 and prime order.

Since arithmetic in $\mathbb{F}_{p^2}$ for suitably chosen p can be as fast as arithmetic in $\mathbb{F}_{p'}$ with $p' \approx p^2$, this is 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 [21] give sample families and curves for this set-up.

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

$$y^2 + \gamma^j y = x^3 + \alpha$$

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 [50].

3.4. **Embedding degree $k = 4$.** Supersingular curves with embedding degree $k = 4$ only exist over finite fields of characteristic two. Then necessarily, $q = 2^s$ with s odd, and $t = \pm\sqrt{2q}$ [52]. The only possible such curves are ([50])

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

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.

3.5. **Embedding degree $k = 6$.** To obtain a supersingular curve with embedding degree $k = 6$, we need to work over a characteristic three finite field. For prime-order curves, this implies $q = 3^s$ with s odd, and $t = \pm\sqrt{3q}$ [52]. The only possible such curves are ([53])

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

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.

Harrison, Page and Smart [33] 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 ordinary pairing-friendly 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 2.6, but we will see in Section 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 [17], Cocks and Pinch gave a procedure for constructing pairing-friendly curves with arbitrary embedding degree k. The Cocks-Pinch method fixes a subgroup size r and a CM discriminant D and computes t such that the CM equation must be satisfied.

Theorem 4.1 ([17])**.** *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 be the unique lift of t' to $(0,r]$, and let y be the unique lift of y' to $(0,r]$. 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 $D < 10^{10}$ 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 $4(q+1-t) \equiv 0 \mod r$. Lastly, the choice of t ensures that $\Phi_k(t-1) \equiv 0 \mod r$.

We observe that there is no reason to believe *a priori* that t or y 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. However, these curves are easy to generate, and in particular we can take r to be (nearly) arbitrary, so r can have low Hamming weight or other desirable features.

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 Section 6.

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 Section 7.1.

Remark 4.3. Rubin and Silverberg [63] 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 [22] is to compute t and r simultaneously using resultants.

Theorem 4.4 ([22])**.** *Fix a positive integer k, and execute the following steps.*

(1) *Compute the resultant*
$$R(a) = \mathrm{Res}_x(\Phi_k(x-1), a+(x-2)^2).$$
(2) *Choose a such that $a = Dy^2$ with D small, and let r be the largest prime factor of $R(a)$.*
(3) *Compute $g(x) = \gcd(\Phi_k(x-1), a+(x-2)^2)$ in $(\mathbb{Z}/r\mathbb{Z})[x]$, and let t' be a root of the polynomial g.*
(4) *Let t be the unique lift of t' to $(0,r]$. 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.

The key idea of the Dupont-Enge-Morain method is to use the following property of resultants: if $\mathrm{Res}_x(f(x), g(x)) = 0$, then $f(x)$ and $g(x)$ have a common factor

for some value of x. If we consider $\Phi_k(x-1)$ and $a+(x-2)^2$ to be polynomials in the two variables a, x, then the resultant R is a single-variable polynomial in a of degree $\varphi(k)$. If we fix a and take r to be some prime factor of $R(a)$, then $R(a) \equiv 0 \pmod{r}$, and thus there is some integer t such that $\Phi_k(t-1)$ and $a+(t-2)^2$ have a common factor modulo r. This factor can be found by computing the greatest common divisor of the polynomials in $(\mathbb{Z}/r\mathbb{Z})[t]$. Thus the values of t and r computed 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 $q+1-t \equiv 0 \mod r$.

We observe that 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.

Like the Cocks-Pinch method, the Dupont-Enge-Morain method is effective for computing curves for 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 factor of a value of the polynomial $R(a)$. Since r must be of cryptographic size, it will usually only be computationally feasible to find such an r if the remaining factors of $R(a)$ are small, so in general r will be roughly the size of $R(a)$. Since $R(a)$ has degree $\varphi(k)$ and is irreducible (because it is the resultant of two irreducible polynomials), the factors r we find will grow roughly like $a^{\varphi(k)}$. 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

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

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 [52] 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 equation (5.1) is quadratic, 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 2.6.

Freeman [25] 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 equation (5.1) and $f(x)$ is square-free, then the equation 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 2.6. On the other hand, if $\deg f(x) \geq 3$, then condition (5) of Definition 2.6 can never be satisfied ([25, Proposition 2.10]). Indeed, in this case the curve defined by equation (5.1) has genus $g \geq 1$, and by Siegel's theorem

(see [70, Theorem IX.4.3] and [20, §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 [7], which we describe from a different viewpoint in Section 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 ([25, 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 [52] were the first authors to propose ordinary pairing-friendly curves, for embedding degrees $k = 3$, 4, and 6. In fact, ordinary curves of prime order with embedding degrees 3, 4, or 6 have been fully characterized as follows:

Theorem 5.2 ([52])**.** *Let q be a prime and $E/\mathbb{F}_q$ be an ordinary elliptic curve such that $r = \#E(\mathbb{F}_q)$ is prime. Let $t = q + 1 - r$.*

1. *Assume $q > 64$. 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. *Assume $q > 36$. 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. *Assume $q > 64$. 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.

Remark 5.3. It is easy to show (see [38]) that if both r and q are primes greater than 64 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 [46] or Robertson [62]. Such a solution may or may not exist. If a solution exists, then for $j \in \mathbb{Z}$ define (X_j, Y_j) through

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

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 $D \equiv 19 \pmod{24}$ [52], and if $k = 4, 6$, necessarily $D \equiv 3 \pmod 8$ and $D \not\equiv 5 \pmod{10}$. Also, 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 2.6. In fact, Luca and Shparlinski [45] give a heuristic argument that for any upper bound $\overline{D}$, there exist only a finite number of MNT curves with discriminant $D \leq \overline{D}$, 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, [57] and [68]).

5.2. **Extensions of the MNT strategy.** The MNT strategy has been extended by Scott and Barreto [69], and by Galbraith, McKee and Valença [28], by allowing a small constant-size cofactor h.

Starting out with (5.1), Scott and Barreto [69] 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 for 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 [28] give a complete characterization of curves with embedding degree $3, 4$ and 6 with cofactors $2 \leq h \leq 5$. 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 parametrizations for t are linear in x, and all resulting parametrizations 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 equation (5.1) is quadratic. However, Freeman [25] 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 [28]. 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,

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

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. Here, the search can be sped up by using that necessarily, $D \equiv 43$ or $67 \pmod{120}$.

6. Complete families of pairing-friendly curves

Once again, we start out with the CM equation

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

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 a perfect square, and thus the equation is satisfied for any x. These constructions thus give complete families of curves in the sense of Definition 2.6.

There are two principal strategies for constructing complete families, one due to Scott and Barreto [69] and the other due originally to Barreto, Lynn, and Scott [5], and in its fullest generality to Brezing and Weng [12]. Both start in the same way: fix an embedding degree k, choose a polynomial $r(x)$ 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

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

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 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 $q(x)$ and $r(x)$ represent primes, then (t, r, q) represents 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 a multiple of k, in which case the polynomial $r(x)$ is 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 [54] for more details. We call families constructed in this manner "cyclotomic families," and we discuss some of the most efficient constructions in Section 6.1 below.

We may achieve even better success by choosing K to be an extension of a cyclotomic field. To create such an extension, we make the substitution $x \mapsto u(x)$ for some polynomial u. 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. Since factorizations of $\Phi_\ell(u(x))$ are rare, we will call families of curves obtained by this technique "sporadic" families; they are discussed in Section 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 [7], who used this method to construct curves of prime order with embedding degree 12 (Example 6.16 below).

6.1. **Cyclotomic families.** Barreto, Lynn, and Scott [5], and independently, Brezing and Weng [12], both observed that if we apply the Cocks-Pinch method but parametrize t, r, q as polynomials, then we can improve on this value of ρ. Brezing and Weng stated the construction in greatest generality; their theorem is below.

Theorem 6.1 ([12])**.** *Fix a positive integer k and a positive square-free integer D. Execute the following steps.*

1. *Choose a number field K containing $\sqrt{-D}$ and a primitive kth root of unity ζ_k.*
2. *Find an irreducible (but not necessarily monic) polynomial $r(x) \in \mathbb{Z}[x]$ such that $\mathbb{Q}[x]/(r(x)) \cong K$.*
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* $y(x) \equiv (2 - t(x))s(x)/D \pmod{r(x)}$*.)*
(5) *Let* $q(x) \in \mathbb{Q}[x]$ *be given by* $(t(x)^2 + Dy(x)^2)/4$*.*

If $q(x)$ *and* $r(x)$ *represent primes, then the triple* $(t(x), r(x), q(x))$ *represents a family of curves with embedding degree* k *and discriminant* D*.*

The ρ-value for this family is

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

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 will now examine in detail some constructions for certain sets of k.

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 [12] set $r(x)$ to be a cyclotomic polynomial $\Phi_\ell(x)$ for some ℓ that is a multiple 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 Definition 2.5 and thus represents primes. 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 ([12])**.** Let k be odd, and let $r(x) = \Phi_{4k}(x)$, so $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{4k})$. We choose $\zeta_k \mapsto -x^2$ (so $t(x) = 1 - x^2$) and $\sqrt{-1} \mapsto x^k$. The Brezing-Weng method (Theorem 6.1) then gives

$$\begin{aligned} q(x) &= \frac{1}{4}((-x^2 + 1)^2 + (x^2 + 1)^2 x^{2k}) \\ &= \frac{1}{4}\left(x^{2k+4} + 2x^{2k+2} + x^{2k} + x^4 - 2x^2 + 1\right). \end{aligned} \tag{6.2}$$

Since $q(1) = 1$, if q is irreducible then it represents primes. Computations with PARI [58] show that $q(x)$ is irreducible for odd $k < 200$, and we conjecture that $q(x)$ is irreducible for all odd k. We conclude that for odd $k < 200$ (and conjecturally for all odd k), (t, r, q) represents a complete family of curves with embedding degree k and discriminant 1. The ρ-value for this family is $\deg q / \deg \Phi_{4k} = (k + 2)/\varphi(k)$.

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. Changing the sign of ζ_k in Construction 6.2 gives

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

Then (t, r, q) represents a potential family of pairing-friendly elliptic curves with embedding degree $2k$ and discriminant 1. If x is odd, then $q(x)$ is an integer. Since $q(x)$ is the reverse of the polynomial given in (6.2), $q(x)$ is irreducible if and only if (6.2) is. Thus (t, r, q) represents a family of curves for odd $k < 200$, and we conjecture for all k. The ρ-value for this family is $(k+2)/\varphi(k)$; in terms of the embedding degree $k' = 2k$ the ρ-value is $(k'/2 + 2)/\varphi(k')$.

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

Construction 6.4. Let k be odd. Using $\zeta_{4k} \mapsto x$ in Construction 6.2 gives

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

Then (t, r, q) represents a potential family of pairing-friendly elliptic curves with embedding degree $4k$ and discriminant 1. Since $q(1) = 1$, if q is irreducible then it represents primes. Computations with PARI [58] show that $q(x)$ is irreducible for odd $k < 200$, and we conjecture that $q(x)$ is irreducible for all odd k. Thus (t, r, q) represents a family of curves for odd $k < 200$, and we conjecture for all k. The ρ-value for this family is $(k+1)/\varphi(k)$; in terms of the embedding degree $k' = 4k$ the ρ-value is $(k'/4 + 1)/\varphi(k')$.

Remark 6.5. For any odd k, the families of Constructions 6.2, 6.3, and 6.4 have ω-values $\varphi(k)$, $\varphi(2k)$, and $\varphi(4k)$, respectively. By Proposition 2.9 these are the maximum possible ω-values.

Example 6.6 ([12])**.** For $k = 10$, Brezing and Weng achieve a better ρ-value than Construction 6.3. We set $r(x) = \Phi_{20}(x)$, so $\mathbb{Q}[x]/(r(x))$ contains ζ_{10} and $\sqrt{-1}$. Choosing $\zeta_{10} \mapsto -x^6 + x^4 - x^2 + 1$ and $y(x) = x^5 - x^3$ gives

$$\begin{aligned} t(x) &= -x^6 + x^4 - x^2 + 2 \\ q(x) &= \frac{1}{4}(x^{12} - x^{10} + x^8 - 5x^6 + 5x^4 - 4x^2 + 4) \end{aligned}$$

Since $q(x)$ is irreducible and $q(0) = 1$, the triple (t, r, q) represents a family of pairing-friendly elliptic curves with embedding degree 10 and discriminant 1. The ρ-value for this family is $3/2$.

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 [12] for certain values of k; we consider the construction for all k, and discover families in all cases where k is not divisible by 18.

Construction 6.7. Let k be any positive integer, let $\ell = \operatorname{lcm}(6, k)$, and let $r(x) = \Phi_\ell(x)$. 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 use the relation $x^{\ell/3} = x^{\ell/6} - 1 \mod r(x)$ to minimize the degree of $y(x) = (\zeta_k - 1)/\sqrt{-3}$. 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 $\ell/6$. 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 $\gcd(a, k) = 1$. The exact choice depends on the congruence class of x modulo 6:

- $k \equiv 1 \pmod 6$, $\ell = 6k$: 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 $\zeta_k \mapsto -x^{2k+1} \equiv -x^{k+1} + x \mod r(x)$.
- $k \equiv 2 \pmod 6$, $\ell = 3k$: We have $k + 1 \equiv 3 \pmod 6$, so we choose $\zeta_k \mapsto x^{k+1} \equiv x^{k/2+1} - x \mod r(x)$.
- $k \equiv 3 \pmod 6$, $\ell = 2k$: 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 $\zeta_k \mapsto -x^{2k/3+1} \equiv -x^{k/3+1} + x \mod r(x)$.
- $k \equiv 4 \pmod 6$, $\ell = 3k$: Choose $\zeta_k \mapsto x^3$.
- $k \equiv 5 \pmod 6$, $\ell = 6k$: We have $k + 1 \equiv 0 \pmod 6$, so we choose $\zeta_k \mapsto x^{k+1}$.
- $k \equiv 0 \pmod 6$, $\ell = k$: Choose $\zeta_k \mapsto x$.

If $z(x)$ is the polynomial mapped to by ζ_k, we compute $y(x)$ by taking $\frac{1}{3}z(x)(1 - 2x^{\ell/6})$ and adding $\pm 2xr(x)$ to cancel out the leading term if $k \pmod 6 \in \{1, 2, 3, 5\}$. We note that for small values of k the resulting $t(x)$ and $y(x)$ are not completely reduced modulo $r(x)$; however, we find that further reduction leads to a $q(x)$ that does not represent primes. Our choices for ζ_k and $y(x)$ give the following formulas for $q(x)$, which are valid for all positive k:

- $k \equiv 1 \pmod 6$: $q(x) = \frac{1}{3}(x + 1)^2(x^{2k} - x^k + 1) - x^{2k+1}$.
- $k \equiv 2 \pmod 6$: $q(x) = \frac{1}{3}(x - 1)^2(x^k - x^{k/2} + 1) + x^{k+1}$.
- $k \equiv 3 \pmod 6$: $q(x) = \frac{1}{3}(x + 1)^2(x^{2k/3} - x^{k/3} + 1) - x^{2k/3+1}$.
- $k \equiv 4 \pmod 6$: $q(x) = \frac{1}{3}(x^3 - 1)^2(x^k - x^{k/2} + 1) + x^3$.
- $k \equiv 5 \pmod 6$: $q(x) = \frac{1}{3}(x^2 - x + 1)(x^{2k} - x^k + 1) + x^{k+1}$.
- $k \equiv 0 \pmod 6$: $q(x) = \frac{1}{3}(x - 1)^2(x^{k/3} - x^{k/6} + 1) + x$.

We see that we have $\deg q = \ell/3 + 2$ in all cases except $k \equiv 4 \pmod 6$, in which case $\deg q = \ell/3 + 6$. Thus for any k, we have constructed a potential family of pairing-friendly curves with embedding degree k and discriminant 3. The ρ-values of these families are $\rho = (\ell/3 + 6)/\varphi(\ell)$ if $k \equiv 4 \pmod 6$, and $(\ell/3 + 2)/\varphi(\ell)$ otherwise.

It remains to consider whether $q(x)$ represents primes. We can check conditions (4) and (5) of Definition 2.5 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 PARI [58] indicate that the appropriate $q(x)$ is irreducible for all $k < 300$, except when k is divisible by 18. We conjecture that these polynomials are irreducible for all k not divisible by 18.

Remark 6.8. Note that if $k \equiv 0$ or $4 \pmod 6$, then the ω-value of the family constructed is $\varphi(k)$, which by Proposition 2.9 is the maximum possible value. Furthermore, curves with k a multiple of 6 and $D = 3$ can take advantage of sextic

twists to speed up computation of the Ate pairing [7]. Thus the families of curves in Construction 6.7 with $k \equiv 6$ or $12 \pmod{18}$ are ideal for implementation of the Ate pairing.

Remark 6.9. The construction given for $k \equiv 4 \pmod 6$ carries over identically to $k \equiv 2 \pmod 6$, giving a family with maximum ω-value in this case as well.

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 [54] give an example of the construction for $k = 24$; we describe the construction for any k divisible by 3.

Construction 6.10. Let k be a positive integer divisible by 3. We work in the field $\mathbb{Q}(\zeta_k, \zeta_8)$, defined as $K \cong \mathbb{Q}[x]/(\Phi_\ell(x))$, where $\ell = \operatorname{lcm}(8, k)$. In this field, we have $\zeta_k \mapsto x^{\ell/k}$ (so $t(x) = x^{\ell/k} + 1$), and $\sqrt{-2} = \zeta_8 + \zeta_8^3 \mapsto x^{\ell/8} + x^{3\ell/8}$. We set $y(x) \mapsto (\zeta_k - 1)/\sqrt{-2}$ and compute the reduction of $y(x)$ modulo $\Phi_\ell(x)$. Since k is a multiple of 3, we can use the relation $x^{\ell/3} = x^{\ell/6} - 1$ to compute $y(x)$ modulo $\Phi_\ell(x)$ explicitly, for we have

$$\begin{aligned} \frac{\zeta_k - 1}{\sqrt{-2}} &\mapsto \frac{1}{2}(1 - x^{\ell/k})(x^{3\ell/8} + x^{\ell/8}) \\ &\equiv \frac{1}{2}(1 - x^{\ell/k})(x^{5\ell/24} + x^{\ell/8} - x^{\ell/24}) \mod \Phi_\ell(x). \end{aligned}$$

We set $y(x)$ equal to this last polynomial. If $\frac{\ell}{k} + \frac{5\ell}{24} < \varphi(\ell)$ (a condition which holds whenever $3 \mid k$, $k \geq 18$, and k has at most two prime factors greater than 3), then $y(x)$ is the minimal-degree representative of $(\zeta_k - 1)/\sqrt{-2}$ modulo $\Phi_\ell(x)$, and we may set

$$q(x) = \frac{1}{8}\left(2(x^{\ell/k} + 1)^2 + (1 - x^{\ell/k})^2(x^{5\ell/24} + x^{\ell/8} - x^{\ell/24})^2\right).$$

The degree of q is thus $\left(\frac{2\ell}{k} + \frac{5\ell}{12}\right)$. We observe that $q(1) = 1$ for any k; computations with PARI show that $q(x)$ is irreducible when $3 \mid k$ and $k < 200$, and we conjecture that $q(x)$ is irreducible for all such k. Thus for these values of k, $(x^{\ell/k} + 1, \Phi_\ell(x), q(x))$ represents a family of curves with embedding degree k. 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.

Remark 6.11. For any k not divisible by 8, the families of Construction 6.10 have ω-value $k\varphi(\ell)/\ell$, which is equal to $\varphi(k)$ if k is even and $\varphi(k)/2$ if k is odd. Thus by Proposition 2.9, for even k Construction 6.10 achieves the maximum possible ω-value.

Construction 6.10, 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 6.7, the expressions for $q(x)$ when k is not divisible by 3 or when $\frac{\ell}{k} + \frac{5\ell}{24} \geq \varphi(\ell)$ become too complicated to enumerate explicitly in general. Furthermore, in some cases the construction may not give a family of curves; 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 6.1.

Lastly, the following Brezing-Weng-type construction is due to Kachisa [37]. The key idea of the construction is to use a polynomial other than the cyclotomic polynomial $\Phi_k(x)$ to define the cyclotomic field $\mathbb{Q}(\zeta_k)$.

TABLE 6.1. Families with $k \in \{15, 28, 44\}$ and $D = 2$.

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

Construction 6.12. Let k be any positive integer. Let $\ell = \mathrm{lcm}(3, k)$, $\ell = \mathrm{lcm}(4, k)$, or $\ell = \mathrm{lcm}(8, k)$, depending on whether we are going to use $D = 3$, 1, or 2, respectively. Let ζ_ℓ be a primitive ℓth root of unity. We represent $\mathbb{Q}(\zeta_\ell)$ as $\mathbb{Q}[z]/(\Phi_\ell(z))$, so $\zeta_\ell \mapsto z$. Let $\beta = \sum_{i=0}^{\varphi(\ell)-1} \alpha_i z^i$ for some small integer coefficients α_i, and let $r(x) \in \mathbb{Z}[x]$ be the minimal polynomial of β. We work in the field $\mathbb{Q}(\beta)$, defined as $K \cong \mathbb{Q}[x]/(r(x))$. In general we find that $\mathbb{Q}(\beta) \cong \mathbb{Q}(\zeta_k)$, so we can choose a kth root of unity modulo $r(x)$ and determine $t(x)$ and $q(x)$ along the lines of Theorem 6.1.

Which coefficients α_i 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 we find 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: Kachisa has used Construction 6.12 to produce the following two examples for $k = 16, 18$.

Example 6.13 ([37])**.** Let $k = \ell = 16$. We set $\beta = -2z^5 + z^2$, which has minimal polynomial

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

In $\mathbb{Q}[x]/(r(x))$, we use $\zeta_{16} \mapsto \frac{1}{35}(2x^5 + 41x)$, so

$$t(x) = \frac{1}{35}\left(2x^5 + 41x + 35\right).$$

We use $\sqrt{-1} \mapsto -\frac{1}{7}(x^4 + 24)$. We get $y(x) = -\frac{1}{35}(x^5 + 5x^4 + 38x + 120)$ and

$$q(x) = \frac{1}{980}\left(x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125\right).$$

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 (mod 70). In addition, $\gcd(\{q(\pm 25 + 70n) : n \in \mathbb{Z}\}) = 1$, so q represents primes. Lastly, $r(25 + 70n) = 61250\tilde{r}(n)$, where $\tilde{r}(n)$ represents primes. So (t, r, q) represents a family of curves with embedding degree 16. The ρ-value of this family is 5/4.

Example 6.14 ([37])**.** Let $k = \ell = 18$. We set $\beta = -3z^5 + z^2$, which has minimal polynomial

$$r(x) = x^6 + 37x^3 + 343.$$

In $\mathbb{Q}[x]/(r(x))$, we use $\zeta_{18} \mapsto \frac{1}{7}(x^4 + 16x)$, so

$$t(x) = \frac{1}{7}\left(x^4 + 16x + 7\right),$$

and $\sqrt{-3} \mapsto -2x^3 - 37$. Then $y(x) = -\frac{1}{21}\left(5x^4 + 14x^3 + 94x + 259\right)$ and

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

The polynomial $q(x)$ is irreducible. Now, both $q(x)$ and $t(x)$ are integers if and only if $x \equiv 7$ or $14 \pmod{21}$. Moreover, $\gcd(\{q(\pm 7 + 21n) : n \in \mathbb{Z}\}) = 1$, so q represents primes. However, if $x \equiv 7 \pmod{21}$ then $3 \mid q(x)$, and if $x \equiv 35 \pmod{42}$ then $4 \mid q(x)$, so $q(x)$ can never be prime for those x-values. We thus restrict ourselves to $x \equiv 14 \pmod{42}$. We have $r(14 + 42n) = 343\tilde{r}(n)$, where $\tilde{r}(n)$ represents primes. So (t, r, q) represents a family of curves with embedding degree 18. The ρ-value of this family is $4/3$.

Remark 6.15. The ω-values for the two families above are low: we have $\omega = 8/5$ in Example 6.13, and $\omega = 3/2$ in Example 6.14. On the other hand, the $k = 16$ curves have quartic twists and the $k = 18$ curves have sextic twists, which can be used to speed up computation (see Section 7.3).

6.2. **Sporadic families of Brezing-Weng curves.** Brezing and Weng only consider cyclotomic fields for their constructions, but in some cases extensions of cyclotomic fields may turn out to be even more effective. Such extensions are constructed by substituting $x \mapsto u(x)$ in the cyclotomic polynomial $\Phi_\ell(x)$, where $u(x)$ is some polynomial. 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 substituting $x \mapsto u(x)$ in t, r, and q. However, if $\Phi_\ell(u(x))$ factors, we may gain some advantage.

Galbraith, McKee and Valença [28] 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, parametrized be 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 the extension of $\mathbb{Q}(\zeta_5)$, and thus our prospects of using Theorem 6.1 to construct a complete family using such a factorization appear dim.

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 6.16 (Barreto-Naehrig curves [7])**.** Galbraith, McKee and Valença discovered that if $u(x) = 6x^2$, then $\Phi_{12}(u(x)) = r(x)r(-x)$, where $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$. If we set $K = \mathbb{Q}[x]/(r(x))$, then $\zeta_{12} \mapsto 6x^2$ in K, and using $\sqrt{-3} = 2\zeta_{12}^2 - 1$ we compute $y(x) = 6x^2 + 4x + 1$ and $q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$. 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.

Viewing the Barreto-Naehrig construction in this way allows us to extend the construction to the other quadratic $u(x)$ for which $\Phi_{12}(u(x))$ factors.

Example 6.17. 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. However, if we look at $\zeta_4 \mapsto u(x)^3 \bmod r(x)$, we find

$$\begin{aligned} t(x) &= -4x^3, \\ q(x) &= \frac{1}{3}\left(16x^6 + 8x^4 + 4x^3 + 4x^2 + 4x + 1\right), \end{aligned}$$

which gives a family of curves with $k = 4$, $D = 3$, and $\rho = 3/2$.

A computer search for further factorizations of $\Phi_k(u(x))$ for various values of k and degrees of u found the following example.

Example 6.18. Let $k = 8$. If $u(x) = 9x^3 + 3x^2 + 2x + 1$, 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 $\sqrt{-1} = \zeta_8^2 \mapsto -18x^3 - 15x^2 - 10x - 4 \bmod r(x)$. Applying Theorem 6.1, we compute

$$\begin{aligned} t(x) &= -9x^3 - 3x^2 - 2x \\ q(x) &= \frac{1}{4}(81x^6 + 54x^5 + 45x^4 + 12x^3 + 13x^2 + 6x + 1). \end{aligned}$$

Since $q(1) = 53$ and $q(-1) = 17$ are distinct primes, $q(x)$ represents primes. We conclude that (t, r, q) represents a family of curves with embedding degree 8. The ρ-value for this family is $3/2$, which is worse than $\rho = 5/4$ given by Construction 6.7. However, curves with $D = 1$ have an automorphism of order 4, and since k is a multiple of 4 we may take advantage of this "quartic twist" 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 Section 7.3).

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

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

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 6.7 for $k = 12$, which has $\rho = 3/2$, but they are clearly inferior to the ideal Barreto and Naehrig construction (Example 6.16). However, the result does indicate that more useful solutions may well exist.

6.3. **Scott-Barreto families.** To employ the strategy of Scott and Barreto [69], 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

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

take the form of a linear factor times a perfect square. Below we give some examples of this method that achieve ρ-values less than 2 with (nearly) arbitrary D; these examples were found by fixing k and executing a computer search through the space of possible $t(x)$ and $h(x)$.

Example 6.19. Let $k = 4$. Take $t(x) = x + 1$, $r(x) = \Phi_4(x) = x^2 + 1$, $h(x) = (x + 13)/25$; then the CM equation becomes

$$\begin{aligned} Dy^2 &= \frac{4}{25}(x + 13)(x^2 + 1) - (x - 1)^2 \\ &= \frac{1}{25}(4x + 3)(x + 3)^2. \end{aligned}$$

If we substitute $x = (Dz^2 - 3)/4$, the right hand side becomes D times a square, and we find

$$q(x) = \frac{1}{25}\left(x^3 + 13x^2 + 26x + 13\right).$$

The ρ-value for this family is $3/2$. We observe that $q(x)$ is an integer if and only if $x \equiv 2 \pmod 5$, and since $x = (Dz^2 - 3)/4$ we conclude that $D \equiv 11$ or $19 \pmod{20}$.

Example 6.20. Let $k = 6$. Take $t(x) = -4x^2 + 4x + 2$, $r(x) = \Phi_6(t(x) - 1) = 16x^4 - 32x^3 + 12x^2 + 4x + 1$, $h(x) = x/4$. Then the CM equation becomes

$$Dy^2 = x(4x^2 - 6x + 1)^2.$$

If we substitute $x = Dz^2$, the right hand side becomes D times a square, and we find

$$q(x) = 4x^5 - 8x^4 + 3x^3 - 3x^2 + \frac{17}{4}x + 1.$$

The ρ-value for this family is $5/4$.

Setting $D = 3$ in this family would be ideal in terms of performance, for such curves have sextic twists [7] that would allow both inputs to the pairing to be given over $\mathbb{F}_q$. Unfortunately, the polynomial $r(3z^2)$ factors into two degree-four polynomials in z, so $r(3z^2)$ can never be prime. However, the construction does produce curves with $\rho \approx 5/4$ for most other values of D.

Example 6.21. The Scott-Barreto method also works well for the cases $k = 1$ and $k = 2$. For the case $k = 2$ (cf. [69]), we take $t(x) = x + 1$, $r(x) = \Phi_2(x) = x + 1$, $h(x) = (x - 1)/4$. Then the CM equation becomes

$$Dy^2 = 2(x - 1).$$

If we substitute $x = 1 + Dz^2/2$, the right hand side becomes D times a square, and we find

$$q(x) = \frac{1}{4}(x^2 + 4x - 1).$$

However if instead we consider the case $k = 1$ with $r(x) = \Phi_1(x) = x - 1$ and select $h(x) = (x + 1)/4$, with the other parameters as before, we get exactly the same family! In fact it is perfectly possible (but often overlooked) that one elliptic curve might support multiple embedding degrees. If points are chosen of an order which divides $x - 1$ then the embedding degree is 1. If points are chosen of an order which divides $x + 1$, then the embedding degree is 2. This property might be useful – imagine an application where one standardized elliptic curve can be quickly "upgraded" to a higher security level by simply switching to a group of points with a higher embedding degree. In either case the family has ρ-value 2, which by Proposition 2.11 is the smallest ρ-value we can expect for $k = 1$ or 2.

Example 6.22 (The Koblitz-Menezes family for $k = 1$)**.** Koblitz and Menezes [39, Sect. 6] propose the following complete family (t, r, q) representing ordinary elliptic curves with embedding degree 1:

$$\begin{aligned} t(x) &= 2, \\ r(x) &= x, \\ q(x) &= Dl^2x^2 + 1, \end{aligned}$$

where l is any even integer. The ρ-value of this family is 2. This construction may be viewed as an example of the Scott-Barreto construction with $h(x) = Dl^2$. Koblitz and Menezes give two explicit elliptic curves with $D = 1$, with equations $y^2 = x^3 - x$ if $4 \mid lx$ 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 Section 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., [35, 36]), this condition is in fact not necessary [65]. 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, most $k = 1$ curves constructed via the CM method do have all r-torsion points defined over the base field; Freeman [26, Proposition 2.6] has given a set of conditions that guarantees this property.

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 Section 7.3), the extra structure may be used to aid a future (as yet unknown) discrete logarithm attack. Thus for maximum security, we seek curves with variable square-free discriminant D. We restrict our attention to the square-free part of D because all elliptic curves over $\mathbb{F}_q$ whose CM discriminants have the same square-free part are isogenous (with the isogeny defined over $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$ in most cases).

We now show that if the polynomials constructed by the Brezing-Weng method (Theorem 6.1) 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.

Theorem 6.23. *Suppose (t, r, q) represents a potential family of elliptic curves with embedding degree k and discriminant D. Let $K \cong \mathbb{Q}[x]/(r(x))$, and let $y(x) \mapsto (\zeta_k - 1)/\sqrt{-D}$ in K as in Theorem 6.1. Suppose t, r, and q are even polynomials and y is an odd polynomial. Define r', q' to be the polynomials such that $r(x) = r'(x^2)$ and $q(x) = q'(x^2)$. Then for any integer α such that $r'(\alpha x^2)$ represents primes, there exists a potential family of curves with embedding degree k, discriminant αD, and ρ-value equal to $\rho(t, r, q)$.*

Proof. We begin by defining polynomials t', y' such that $t(x) = t'(x^2)$ and $y(x) = x \cdot y'(x^2)$. Let σ be a root of $r(x)$, so $K = \mathbb{Q}(\sigma)$. Let $\tau = \sigma/\sqrt{\alpha}$, so τ is a root of $r'(\alpha x^2)$. If $r'(\alpha x^2)$ is irreducible, we may define L to be the number field $\mathbb{Q}(\tau) \cong \mathbb{Q}[x]/(r'(\alpha x^2))$. Then any element of K that can be expressed as an even polynomial $g(\sigma^2)$ is also an element of L. In particular, since $t(x)$ is even and $t'(\sigma^2) - 1 = \zeta_k$ in K, we have $\zeta_k = t'(\alpha\tau^2) - 1$ in L.

Now let β be the element $y'(\sigma^2) \in K$; then $\beta = y'(\alpha\tau^2)$ in L. From the definition of $y(x)$ we have $-Dy(\sigma)^2 = -D\sigma^2 y'(\sigma^2)^2 = (\zeta_k - 1)^2$ in K, so

$$-D\sigma^2 y'(\alpha\tau^2)^2 = (\zeta_k - 1)^2$$

in L. Substituting $\sigma^2 = \alpha\tau^2$ gives

$$-D\alpha\tau^2 y'(\alpha\tau^2)^2 = (\zeta_k - 1)^2,$$

so we conclude that

$$\tau y'(\alpha\tau^2) = \frac{\zeta_k - 1}{\sqrt{-\alpha D}}$$

in L.

A straightforward computation shows that

$$q'(\alpha x^2) = \frac{1}{4}\left(t'(\alpha x^2)^2 + \alpha D(x y'(\alpha x^2))^2\right).$$

Since $r'(\alpha x^2)$ represents primes by hypothesis, by Theorem 6.1, the triple

$$(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$$

represents a potential family of curves with embedding degree k and discriminant αD. The ρ-value for this family is $2 \deg q' / 2 \deg r' = \deg q / \deg r$. □

Theorem 6.23 tells us that if t, r, q are even polynomials and $\sqrt{-D} \mod r(x)$ is an odd polynomial, then the substitution $x^2 \mapsto \alpha x^2$ usually gives a potential family of curves with discriminant αD. In practice, if $r(x)$ represents primes then $r'(\alpha x^2)$ nearly always represents primes, and the difficult part in obtaining true families is ensuring that $q'(\alpha x^2)$ represents primes. This observation motivates the following definition.

Definition 6.24. Let $t'(x)$, $r'(x)$, $q'(x)$ be polynomials with rational coefficients. We say that (t', r', q') represents a *meta-family* of pairing-friendly curves with embedding degree k if the following two conditions are satisfied:

(1) For any positive integer α, the triple $(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$ represents a potential family of pairing-friendly elliptic curves with embedding degree k (Definition 2.6).
(2) There is some integer α such that $q'(\alpha x^2)$ represents primes (Definition 2.5).

Our first application of Theorem 6.23 is to the following construction, which improves on Construction 6.2 for certain odd values of k.

Construction 6.25. Let k be odd, $D = 1$, and $K = \mathbb{Q}[x]/(\Phi_{4k}(x))$. If we take $\zeta_k \mapsto (-1)^{(k+1)/2} x^{k+1}$, so $t(x) = 1 + (-1)^{(k+1)/2} x^{k+1}$, then using $\sqrt{-1} \mapsto x^k$ we have

$$\frac{\zeta_k - 1}{\sqrt{-1}} \mapsto (1 - (-1)^{(k+1)/2} x^{k+1}) x^k \equiv (-1)^{(k+1)/2} x + x^k \mod \Phi_{4k}(x)$$

(since $x^{2k} \equiv -1 \mod \Phi_{4k}(x)$). We may then compute

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

Then $(t(x), \Phi_{4k}(x), q(x))$ represents a complete potential family of curves with embedding degree k and discriminant 1. The ρ-value for this family is $\deg q / \deg \Phi_{4k} = (k+1)/\varphi(k)$.

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 have a family of curves. We conjecture that $q(x)$ is irreducible whenever $k \equiv 3 \pmod 4$, and computations show that the conjecture holds for $k < 200$. 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 6.25 are even polynomials and $\sqrt{-1}$ is an odd polynomial, so we may apply Theorem 6.23 to make the substitution $x^2 \mapsto \alpha x^2$ in t, r, q. After making this substitution, we may find that the new $q(x)$ does indeed represent primes and thus we get a true family of curves. However, to get even a potential family, we must first show that $r(x)$ represents primes. We will first need an algebraic lemma.

Lemma 6.26. *Let $K = \mathbb{Q}(\theta)$ be a number field, and let $r(x)$ be the minimal polynomial of θ. Then for any $\alpha \in K$, $r(\alpha x^2)$ is irreducible if and only if $\alpha\theta$ is not a square in K.*

Proof. The proof follows exactly the proof of [28, Lemma 1]. We observe that the argument holds regardless of whether K is Galois. □

Proposition 6.27. *Let k be odd, and let α be an integer not dividing k. Then $\Phi_k(\alpha x^2)$ represents primes.*

Proof. Since ζ_k is a square in $\mathbb{Q}(\zeta_k)$, by Lemma 6.26 $\Phi_k(\alpha x^2)$ is irreducible if and only if α is not a square in $\mathbb{Q}(\zeta_k)$; a sufficient condition for this to occur is $\alpha \nmid k$. Finally $\Phi_k(0) = 1$ regardless of α. □

Proposition 6.27 and Theorem 6.23 combine to tell us that Construction 6.25 leads to potential families of curves with discriminant α for (nearly) arbitrary $\alpha \nmid k$, and 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. If $k \equiv 1 \pmod 4$ then $q_\alpha(x)$ always factors, but for $k \equiv 3 \pmod 4$ $q_\alpha(x)$ is likely to be irreducible. We then observe that $q_{-1}(1) = 1$, so (t', r', q') represents a meta-family of pairing-friendly elliptic curves.

Other than by checking each value of α and k individually, we have no way of showing that even some subset of this meta-family has $q_\alpha(x)$ representing primes. However, if $\alpha \equiv 3 \pmod 4$ and x is odd, $q_\alpha(x)$ is an odd integer, so q_α may represent primes. In practice it appears that, for various k and α both congruent to 3 (mod 4), $q_\alpha(x)$ 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 if k is odd then $\zeta_{2k} = -\zeta_k$ to derive an analogous construction for embedding degrees that are twice an odd number.

Construction 6.28. Let k be odd. Changing the sign of ζ_k in Construction 6.25 gives

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

Then (t, r, q) represents 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 $(k'/2+1)/\varphi(k')$. □

If $k \equiv 3 \pmod 4$ then $q(x)$ has a factor of $(x^2-1)^2$, and if $k \equiv 1 \pmod 4$ then $q(x)$ takes integer values when x is odd, and these values are always even. Substituting $x^2 \mapsto \alpha x^2$, we get

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

We have $q_{-1}(x)$ irreducible for all $k < 200$ with $k \equiv 1 \pmod 4$, and $q_{-1}(1) = 1$, so (t', r', q') represents a meta-family of pairing-friendly curves. As in Construction 6.25, $q_\alpha(x)$ is even for $\alpha \equiv 1 \pmod 4$, so we must choose $\alpha \equiv 3 \pmod 4$ 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 6.23. We make the substitution $x^2 \mapsto \alpha x^2$, where α is odd, and since $q'(1) = 1$ in both cases, we get a meta-family of pairing-friendly curves. The discriminant of a curve in the meta-family is α.

We also note that Construction 6.10 satisfies the conditions of Theorem 6.23 when k is not divisible by 8. If k is not divisible by 4 we may choose any odd α; if k is divisible by 4 we must choose $\alpha \equiv 1 \pmod 4$. Since $D = 2$ in Construction 6.10, the discriminant of a curve in the resulting meta-family can be any square-free positive integer congruent to 2 mod 4 (if $4 \nmid k$) or 2 mod 8 (if $4 \mid k$). We can do the same for the cases presented in Table 6.1; an analysis shows that we can take any α for $k = 15$ and $\alpha \equiv 3 \pmod 4$ for $k = 28$ and 44.

Summary: Algorithm for generating variable-discriminant families. By combining the substitution $x^2 \mapsto \alpha x^2$ from Theorem 6.23 (for some appropriate α) with one of the basic constructions 6.2, 6.3, 6.10, 6.25 or 6.28, 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 8.2 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 6.10, if $3 \mid k$.
   - Construction 6.25, if $k \equiv 3 \pmod 4$.
   - Construction 6.28, if $k \equiv 2 \pmod 8$.
(3) Use the selected basic construction to compute polynomials $t(x)$, $r(x)$, $q(x)$ that represent 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 $\alpha \nmid k$ such that after the substitution $x^2 \mapsto \alpha x^2$, the resulting polynomials $r'(\alpha x^2)$ and $q'(\alpha x^2)$ represent primes. This condition requires α to have the following form:
   - α odd for Constructions 6.2, 6.3, and 6.10 with $4 \nmid k$.
   - $\alpha \equiv 1 \pmod 4$ for Construction 6.10 with $4 \mid k$.
   - $\alpha \equiv 3 \pmod 4$ for Constructions 6.25 and 6.28.
(6) Let $D = 2\alpha$ if Construction 6.10 was used, and let $D = \alpha$ otherwise.

Then $(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$ represents 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 $D < 10^{10}$, the equation for this curve can be computed by the CM method.

7. Implementation considerations

There are many factors to take into account when choosing an elliptic curve for pairing-based cryptography. 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.

For an extensive survey of implementation considerations, see Scott's recent paper [67]. Page, Smart and Vercauteren [57] give a detailed comparison of MNT curves (Section 5.1) with supersingular curves (Section 3).

7.1. **Balancing security.** When choosing an elliptic curve for pairing applications, one usually begins by fixing in advance a minimum bit size b_1 for the prime-order subgroup of the elliptic curve and a minimum bit size b_2 for the finite field in which the discrete logarithm must be infeasible. To achieve these minimum 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 require twice as much storage space and base field operations take roughly twice 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 (Section 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 pairing 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 [30, 72]. For the $k = 1$ case, see Charles' paper [15] for a thorough discussion, and Section 6.3 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 [16].

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 [70, Chapter X]. If q is a power of 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 [6] 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. Barreto and Naehrig [7] 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 [34, §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 Tate pairing can be computed in $\mathbb{F}_{p^{k/d}}$ instead of $\mathbb{F}_{p^k}$, with the loss of $\lceil \log_2 d \rceil$ bits of information. This "compression" technique was introduced for quadratic twists by Scott and Barreto [68] and extended to sextic twists by Barreto and Naehrig [7]; similar ideas apply to quartic and cubic twists. This technique could reduce the time needed to compute the pairing by a factor of d or more.

A twist of degree k on a curve with embedding degree k would be ideal for implementation, as it would allow all of the pairing computation to be done in 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 order r 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 [34, 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 [71, 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 family of ordinary curves 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 2.11). Such families do exist: see for example Construction 6.4 for $k = 4$, $D = 1$, or Construction 6.7 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 [39, §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 [7, §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 [51] 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 (Section 3.2) and Cocks-Pinch curves (Section 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 Section 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 [66]. Thus q will have to be slightly larger to achieve the same level of security, counteracting somewhat the performance boost for field operations.

7.6. **The Ate pairing.** While the Tate pairing is computed by iterating on the bits of the subgroup order r, the Ate pairing is computed by iterating on the bits of $t-1$, where t is the trace [34]. Thus if $\omega = \log r / \log |t|$ is large, the computation of the Ate pairing for a given pair of inputs (P, Q) may be much faster than the corresponding Tate pairing computation. As a consequence, if we are looking for curves for use with the Ate pairing, we should choose curves with large ω-values.

In most pairing applications, the second input point Q is the same for all pairing evaluations, and only the first input point P varies. If the pairing used is the Tate pairing, P is usually a point on $E(\mathbb{F}_q)$ and Q is defined over an extension field $\mathbb{F}_{q^k}$. The Ate pairing switches the roles of P and Q, making the variable point P the one that is defined over the extension field. Thus it is more important when using the Ate pairing that the curve have extra twists that allow P to be mapped into a small subfield; see Section 7.3 for a discussion of twists.

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 on the elliptic curve $E/\mathbb{F}_q$ and in the finite field $\mathbb{F}_{q^k}$. 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 family of curves $(t(x), r(x), q(x))$, to compute parameters for a specific curve one then must loop through x of the appropriate size until one is found that gives prime values for $q(x)$ and $r(x)$. If the degrees of these polynomials are too large relative to the desired security levels, finding such an x may be difficult. The following proposition makes this idea more precise.

Proposition 8.1. *Let $g(x)$ be a polynomial of degree d. Then heuristically the expected number of x such that $g(x)$ is a $(b+1)$-bit prime number is approximately $\frac{2^{b/d}}{bd}$.*

Proof. 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 $x^d \in [2^b, 2^{b+1})$. Taking dth roots gives $x \in [2^{b/d}, 2^{(b+1)/d})$, so the number of such x is $2^{b/d}(2^{1/d} - 1)$. Using

$2^{1/d} = e^{\log(2)/d}$, the Taylor series for e^x gives $2^{1/d} - 1 \approx \log(2)/d$, so the number of 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 prime is roughly $\frac{2^{b/d}}{bd}$. □

The consequence of this 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 8.1 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.

TABLE 8.1. 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

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 6.7 with $k = 32$; these polynomials have degree 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 8.2. If we can apply Theorem 6.23 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 [18], who independently demonstrated examples of this approach; their construction is equivalent to applying Theorem 6.23 to our Constructions 6.3 and 6.28 and fixing $x = 1$. The restriction that the square-free part of α be less than 10^{10} will not in general pose a problem, since even with $x = 1$ we may still find values of r with as many as $16 \cdot \deg r(x)$ bits. Thus

for constructions using Theorem 6.23, 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 (Section 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 $D < 10^{10}$), 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 8.2 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 8.2 gives the best ρ-value achieved by two different constructions.

The first construction listed is the one that yields the best ρ-value when the CM discriminant D is 1, 2, 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

$$\begin{array}{lll} E_1: & y^2 = x^3 + ax & (D = 1), \\ E_2: & y^2 = x^3 - 30a^2x + 56a^3 & (D = 2), \\ E_3: & y^2 = x^3 + a & (D = 3) \end{array}$$

for any $a \in \mathbb{F}_q^\times$. Furthermore, curves with small CM discriminant have low-degree endomorphisms which may be used to speed up elliptic curve arithmetic [31], and curves with CM discriminant 1 or 3 have twists that can speed up pairing computation for certain embedding degrees k (Section 7.3). The table shows that in a large majority of cases, the optimal ρ-value is achieved by Construction 6.7; 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 [23]. 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 Section 6 is combined with the substitution $x^2 \mapsto \alpha x^2$ (Theorem 6.23) to construct curves with variable D; see the algorithm on page 34 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.

Explanation of symbols in Table 8.2.

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

TABLE 8.2. Best ρ-values for families of curves with $k \leq 50$. See Page 40 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	6.7	2.000	any	1	6.21, 6.22
2	any$^{\#}$	1,3	–	§3.2	any$^{\#}$	3 mod 4	–	§3.2
3	**1.000**$^{\#}$	3	2	§3.3	**1.000**	some	2	§5.1-5.2
4	1.500	3	4	6.17	**1.000**	some	2	§5.1-5.2
5	1.500	3	8	6.7	1.750	any odd	8	6.2+
6	1.250	1	4	6.20	**1.000**	some	2	§5.1-5.2
7	1.333†	3	12	6.7, 6.25+	1.333†	3 mod 4	12	6.25+
8	1.250	3	8	6.7	–	–	–	–
9	1.333	3	6	6.7	1.833	any odd	12	6.2+
10	1.500	1,3	8	6.6, 6.28+	**1.000**	some	4	§5.3
11	1.200†	3	20	6.7, 6.25+	1.200†	3 mod 4	20	6.25+
12	**1.000**	3	4	6.16	1.750	2 mod 8	8	6.10+
13	1.167†	3	24	6.7	1.250	any odd	24	6.2+
14	1.333†	3	12	6.7	1.500	any odd	12	6.3+
15	1.500	3	8	6.7	1.750	any even	32	6.10*+
16	1.250	1	10	6.13	–	–	–	–
17	1.125†	3	32	6.7	1.188	any odd	32	6.2+
18	1.333	3	8	6.14	1.583	2 mod 4	24	6.10+
19	1.111†	3	36	6.7	1.111†	3 mod 4	36	6.25+
20	1.375	3	16	6.7	–	–	–	–
21	1.333	3	12	6.7	1.792	2 mod 4	48	6.10+
22	1.300†	1	20	6.3	1.300†	any odd	20	6.3+
23	*1.091*†	3	*44*	*6.7, 6.25+*	1.091†	3 mod 4	44	6.25+
24	1.250	3	8	6.7	–	–	–	–
25	1.300†	3	40	6.7	1.350	any odd	40	6.2+
26	1.167†	3	24	6.7, 6.28+	1.167†	3 mod 4	24	6.28+
27	1.111	3	18	6.7	1.472	2 mod 4	72	6.10+
28	1.333†	1	24	6.4	1.917	6 mod 8	24	6.10*+
29	*1.071*†	3	*56*	*6.7*	1.107	any odd	56	6.2+
30	1.500	3	8	6.7	1.813	2 mod 4	32	6.10+
31	*1.067*†	3	*60*	*6.7, 6.25+*	1.067†	3 mod 4	60	6.25+
32	1.063†	3	32	6.7	–	–	–	–
33	1.200	3	20	6.7	1.575	2 mod 4	80	6.10+
34	1.125†	3	32	6.28+	1.125†	3 mod 4	32	6.28+
35	*1.500*†	3	*48*	*6.7, 6.25+*	1.500†	3 mod 4	48	6.25+
36	1.417†	2	24	6.10	1.417†	2 mod 8	24	6.10+
37	*1.056*†	3	*72*	*6.7*	1.083	any odd	72	6.2+
38	1.111†	3	36	6.7	1.167	any odd	36	6.3 +
39	1.167	3	24	6.7	*1.521*	*2 mod 4*	*96*	*6.10+*
40	1.438†	3	32	6.7	–	–	–	–
41	*1.050*†	3	*80*	*6.7*	1.075	any odd	80	6.2+
42	1.333	3	12	6.7	1.625	2 mod 4	48	6.10+
43	*1.048*†	3	*84*	*6.7, 6.25+*	*1.048*†	*3 mod 4*	*84*	*6.25+*
44	1.150†	3	40	6.7	1.750	6 mod 8	40	6.10*+
45	1.333	3	24	6.7	*1.729*	*2 mod 4*	*96*	*6.10+*
46	*1.136*†	3	*44*	*6.25+*	1.136†	any odd	44	6.3+
47	*1.043*†	3	*92*	*6.7*	*1.043*†	*3 mod 4*	*92*	*6.25+*
48	1.125	3	16	6.7	–	–	–	–
49	*1.190*†	3	*84*	*6.7*	*1.214*	*any odd*	*84*	*6.2+*
50	1.300†	3	40	6.7, 6.28+	1.300†	3 mod 4	40	6.28+

$\deg r \leq 40$, and for variable-discriminant curves we require $\deg r \leq 80$; see Proposition 8.1, Remark 8.2, and the discussion in between. 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 [12], 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 Section 3.2). Depending on the residue class of $q \pmod{12}$ we can construct curves with $D = 1$, $D = 3$, or $D \equiv 3 \pmod 4$ with $(\frac{-D}{q}) = -1$ (see the algorithm on page 14). 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 Scott-Barreto curves of Example 6.21.
- $k = 3$, small D: We recommend a supersingular curve over $\mathbb{F}_{p^2}$; see Section 3.3. If a curve over a prime field is required, Construction 6.7 gives a family with ρ-value 2.

\+ A construction marked with a + indicates that the given basic construction is combined with the substitution $x^2 \mapsto \alpha x^2$ (Theorem 6.23) to construct families with the given discriminant; see the algorithm on page 34 for details.

* For $k = 15$, 28, or 44 and variable D, we use the same technique as in Construction 6.10, 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 6.1.

– 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 Section 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 (Section 7.3), and constructing extension fields in towers defined by simple polynomials (Section 7.4). Table 8.3 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 8.3 lists the family with highest-order twists; if more than one such construction exists, we choose the one with smallest ρ-value. For $k = 36$ we offer two possibilities: a complete family with quartic twists and $\rho = 5/3$, and Cocks-Pinch curves with sextic twists and $\rho \approx 2$; which option is faster will depend on the specific implementation. We also recommend Cocks-Pinch curves for $k = 32$ because we know of no construction with $k = 32$, $D = 1$, and $\rho < 2$.

We note that with the exception of $k = 8, 12, 16, 18$, all of the families in this list (excluding Cocks-Pinch curves) have maximum ω-value and are thus optimal for the Ate pairing (see Section 7.6). 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.

TABLE 8.3. Families with efficient arithmetic.

k	ρ	D	Twist order	Construction
3	1.000	3	3	§3.3
4	2.000	1	4	6.4
6	2.000	3	6	6.7
8	1.500	1	4	6.18
9	1.333	3	3	6.7
12	1.000	3	6	6.16
16	1.250	1	4	6.13
18	1.333	3	6	6.14
24	1.250	3	6	6.7
27	1.111	3	3	6.7
32	≈ 2	1	4	4.1
36	1.667	1	4	6.4
36	≈ 2	3	6	4.1
48	1.125	3	6	6.7

8.4. **Our recommendations – Ate-friendly curves.** If a pairing-friendly elliptic curve E has ω-value greater than 1, the number of iterations required to compute the Ate pairing is less than the number required for the Tate pairing, so in this case the Ate pairing may be more efficient to compute. Proposition 2.9 tells us that a curve with embedding degree k can have ω-value at most $\varphi(k)$; curves with $\omega = \varphi(k)$ will thus maximize performance for the Ate pairing. In Section 6 we have seen complete families of curves with $\omega = \varphi(k)$ for all values of k not divisible by 72, namely:

- Construction 6.2, if k is odd. The CM discriminant is 1, and one can apply Theorem 6.23 to extend to all odd CM discriminants.
- Construction 6.3, if k is twice an odd number. The CM discriminant is 1, and one can apply Theorem 6.23 to extend to all odd CM discriminants.
- Construction 6.4, if k is four times an odd number. The CM discriminant is 1.
- Construction 6.7, if k is even and not divisible by 18 (using Remark 6.9 if $k \equiv 2 \pmod 6$). The CM discriminant is 3.
- Construction 6.10, if $\gcd(k, 24) \in \{6, 12\}$. The CM discriminant is 2, and one can apply Theorem 6.23 to extend to all CM discriminants $D \equiv 2$

(mod 8) if k is divisible by 12, and all discriminants $D \equiv 2 \pmod 4$ otherwise.

The curves obtained through constructions from this list are thus optimal for the Ate pairing. All of the usual performance considerations discussed in Section 7 will apply; for optimal performance, a curve with small ρ-value, $D = 3$, and k a multiple of 6 should be chosen. Construction 6.7 produces such curves for k not divisible by 18.

8.5. **Our recommendations – Curves of composite order.** Several recently proposed protocols require curves having 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 (Section 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 2.12 and the discussion of Section 3.1, the smallest possible ρ-value for 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 (Section 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 Examples 6.21 and 6.22) 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 Sections 7.3 and 7.4, while the $k = 1$ curves cannot.

References

[1] A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61:29–68, 1993.

[2] D. Bailey and C. Paar. Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. *Journal of Cryptology*, 14:153–176, 2001.

[3] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *Journal of Cryptology*, 11:141–145, 1998.

[4] P.S.L.M. Barreto, S. Galbraith, C. O'hEigeartaigh, and M. Scott. Efficient pairing computation on supersingular abelian varieties. To appear in *Designs, Codes and Cryptography.* Preprint version available at: `http://eprint.iacr.org/2004/375`.

[5] P.S.L.M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In *Proceedings of SCN 2002 – Security in Communication Networks*, volume 2576 of *Lecture Notes in Computer Science*, pages 263–273. Springer, 2002.

[6] P.S.L.M. Barreto, B. Lynn, and M. Scott. On the selection of pairing-friendly groups. In *Selected Areas in Cryptography – SAC'2003*, volume 3006 of *Lecture Notes in Computer Science*, pages 17–25. Springer, 2003.

[7] P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *Proceedings of SAC 2005 – Workshop on Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer, 2006.

[8] I. F. Blake, G. Seroussi, and N. P. Smart, editors. *Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2005.

[9] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003.

[10] D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-DNF formulas on ciphertexts. *Proceedings of TCC 05*, volume 3378 of *Lecture Notes in Computer Science*, pages 325–341. Springer, 2005.

[11] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In *Advances in Cryptology – Asiacrypt'2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer, 2002.

[12] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Designs, Codes and Cryptography*, 37:133–141, 2005.

[13] 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`.

[14] J. C. Cha and J. H. Cheon. An identity-based signature from gap Diffie-Hellman groups. In *Public-Key Cryptography – PKC 2003*, volume 2567 of *Lecture Notes in Computer Science*, pages 18-30. Springer, 2003.

[15] 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/`.

[16] L. Chen, Z. Cheng, and N. P. Smart. Identity-based key agreement protocols from pairings. Cryptology ePrint Archive Report 2006/199. Available at: `http://eprint.iacr.org/2006/199/`.

[17] C. Cocks and R. G. E. Pinch. Identity-based cryptosystems based on the Weil pairing. Unpublished manuscript, 2001.

[18] A. Comuta, M. Kawazoe, and T. Takahashi. How to construct pairing-friendly curves for the embedding degree $k = 2n$, n is an odd prime. Cryptology ePrint Archive Report 2006/427. Available at: `http://eprint.iacr.org/2006/427`.

[19] D. Coppersmith. Fast evaluation of logarithms in fields of characteristic two. *IEEE Transactions on Information Theory*, 30:587–594, 1984.

[20] G. Cornell and J. Silverman, eds. *Arithmetic Geometry*. Springer, New York, 1986.

[21] P. Duan, S. Cui, and 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/`.

[22] R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. *Journal of Cryptology*, 18:79–89, 2005.

[23] I. Duursma, P. Gaudry, and F. Morain. Speeding up the discrete log computation on curves with automorphisms. In *Advances in Cryptology – Asiacrypt 1999*, volume 1716 of *Lecture Notes in Computer Science*, pages 103–121. Springer, 1999.

[24] A. Enge. The complexity of class polynomial computation via floating point approximations. arXiv e-print report cs.CC/0601104. Available at: `http://fr.arxiv.org/abs/cs.CC/0601104`.

[25] D. Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. In *Algorithmic Number Theory Symposium ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 452-465. Springer, 2006.

[26] D. Freeman. Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians. Cryptology ePrint Archive Report 2007/057. Available at: `http://eprint.iacr.org/2007/057/`.

[27] G. Frey and H. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62:865–874, 1994.

[28] S. Galbraith, J. McKee, and P. Valença. Ordinary abelian varieties having small embedding degree. To appear in *Finite Fields and Applications*.

[29] S. Galbraith, K. Paterson, and N. Smart. Pairings for cryptographers. Cryptology ePrint Archive Report 2006/165. Available at: http://eprint.iacr.org/2006/165/.
[30] S. Galbraith and V. Rotger. Easy decision Diffie-Hellman groups. *LMS Journal of Computation and Mathematics*, 7:201–218, 2004.
[31] R. Gallant, R. J. Lambert, and S. A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In *Advances in Cryptology – Crypto 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 190–200. Springer, 2001.
[32] R. Granger, D. Page, and N. Smart. High security pairing-based cryptography revisited. In *Algorithmic Number Theory Symposium ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 480–494. Springer, 2006.
[33] K. Harrison, D. Page, and N. P. Smart. Software implementation of finite fields of characteristic three, for use in pairing-based cryptosystems. *LMS Journal of Computation and Mathematics*, 5:181–193, 2002.
[34] F. Hess, N. Smart, and F. Vercauteren. The Eta pairing revisited. Cryptology ePrint Archive Report 2006/110. Available at: http://eprint.iacr.org/2006/110/.
[35] A. Joux. A one round protocol for tripartite Diffie-Hellman. In *Algorithmic Number Theory Symposium ANTS-IV*, volume 1838 of *Lecture Notes in Computer Science*, pages 385-393. Springer, 2000. Full version: *Journal of Cryptology*, 17:263-276, 2004.
[36] A. Joux and K. Nguyen. Separating decision Diffie-Hellman from computational Diffie-Hellman in cryptographic groups. *Journal of Cryptology*, 16:239-247, 2003.
[37] E. Kachisa. Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. M.Sc. dissertation, Mzuzu University, 2007.
[38] 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.
[39] N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. In *Proceedings of Cryptography and Coding: 10th IMA International Conference*, volume 3796 of *Lecture Notes in Computer Science*, pages 13–36. Springer, 2005.
[40] S. Lang. *Elliptic functions*. Springer, 1987.
[41] S. Lang. Algebra, revised 3rd edition. Springer, 2002.
[42] A. K. Lenstra. Unbelievable security: Matching AES security using public key systems. In *Advances in Cryptology – Asiacrypt 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 67–86. Springer, 2001.
[43] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1997.
[44] F. Luca, D. Mireles, and I. Shparlinski. MOV attack in various subgroups on elliptic curves. *Illinois J. Math.*, 48:1041–1052, 2004.
[45] F. Luca and I. Shparlinski. Elliptic curves with low embedding degree. *Journal of Cryptology*, 19:553–562, 2006.
[46] K. Matthews. The diophantine equation $x^2 - Dy^2 = N$, $D > 1$, in integers. *Expositiones Mathematicae*, 18:323–331, 2000.
[47] A. Menezes. *Elliptic curve public key cryptosystems* Kluwer Academic Publishers, 1993.
[48] 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.
[49] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39:1639–1646, 1993.
[50] A. Menezes and S. Vanstone. Isomorphism classes of elliptic curves over finite fields of characteristic 2. *Utilitas Mathematica*, 38:135–153, 1990.
[51] V. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17:235–261, 2004.
[52] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals*, E84-A(5):1234–1243, 2001.
[53] F. Morain. Classes d'isomorphismes des courbes elliptiques supersingulières en caracteristique ≥ 3. *Utilitas Mathematica*, 52:241–253, 1997.
[54] A. Murphy and N. Fitzpatrick. Elliptic curves for pairing applications. Cryptology ePrint Archive Report 2005/302. Available at: http://eprint.iacr.org/2005/302.
[55] A. M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In *Advances in Cryptology – Eurocrypt 1984*, volume 209 of *Lecture Notes in Computer Science*, pages 224–314, Springer, 1985.

[56] P. C. van Oorschot and M. J. Wiener. Parallel collision search with cryptanalytic applications. *Journal of Cryptology*, 12:1–18, 1999.
[57] D. Page, N. P. Smart, and F. Vercauteren. A comparison of MNT curves and supersingular curves. Cryptology ePrint Archive Report 2004/165. Available at: `http://eprint.iacr.org/2004/165`.
[58] PARI/GP Computer Algebra System. Available at: `http://pari.math.u-bordeaux.fr`.
[59] K. G. Paterson. ID-based signatures from pairings on elliptic curves. *Electronics Letters*, 38:1025–1026, 2002.
[60] S. Pohlig and M. Hellman. An improved algorithm for computing discrete logarithms over $GF(p)$ and its cryptographic significance. *IEEE Trans. Information Theory* **24**, pp. 106–110 (1978).
[61] J. M. Pollard. Monte Carlo Methods for Index Computation (mod p). *Mathematics of Computation*, 32:918–924, 1978.
[62] J. Robertson. Solving the generalized Pell equation. Unpublished manuscript, 2004. Available at: `http://hometown.aol.com/jpr2718/pell.pdf`.
[63] K. Rubin and A. Silverberg. Finding composite order ordinary elliptic curves using the Cocks-Pinch method. In preparation.
[64] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *2000 Symposium on Cryptography and Information Security – SCIS 2000*, Okinawa, Japan, 2000.
[65] 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*, volume 13 of *Lecture Notes Ser. Comput.*, pages 1–12. World Scientific Publishing, 2005.
[66] O. Schirokauer. The number field sieve for integers of low weight. Cryptology ePrint Archive Report 2006/107. Available at: `http://eprint.iacr.org/2006/107/`.
[67] M. Scott. Implementing cryptographic pairings. Preprint, 2006. Available at: `ftp://ftp.computing.dcu.ie/pub/resources/crypto/pairings.pdf`.
[68] M. Scott and P.S.L.M. Barreto. Compressed pairings. In *Advances in Cryptology – Crypto 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 140–156. Springer, 2004.
[69] M. Scott and P.S.L.M. Barreto. Generating more MNT elliptic curves. *Designs, Codes and Cryptography*, 38:209–217, 2006.
[70] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.
[71] J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones math.*, 2:134–144, 1966.
[72] E. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *Journal of Cryptology*, 17:277–296, 2004.
[73] W. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. Ecole Norm. Sup.*, 2:521–560, 1969.