Constructing Elliptic Curves with Prescribed Embedding Degrees

Paulo S. L. M. Barreto[1]*, Ben Lynn[2], and Michael Scott[3]

[1] Laboratório de Arquitetura e Redes de Computadores (LARC),
Escola Politécnica, Universidade de São Paulo, Brazil.
pbarreto@larc.usp.br
[2] Computer Science Department, Stanford University, USA.
blynn@cs.stanford.edu
[3] School of Computer Applications, Dublin City University
Ballymun, Dublin 9, Ireland.
mscott@indigo.ie

Abstract. Pairing-based cryptosystems depend on the existence of groups where the Decision Diffie-Hellman problem is easy to solve, but the Computational Diffie-Hellman problem is hard. Such is the case of elliptic curve groups whose embedding degree is large enough to maintain a good security level, but small enough for arithmetic operations to be feasible. However, the embedding degree is usually enormous, and the scarce previously known suitable elliptic groups had embedding degree $k \leqslant 6$. In this paper, we examine criteria for curves with larger k that generalize prior work by Miyaji *et al.* based on the properties of cyclotomic polynomials, and propose efficient representations for the underlying algebraic structures.

1 Introduction

A subgroup G of (the group of points of) an elliptic curve $E(\mathbb{F}_q)$ is said to have *embedding degree* or *security multiplier* k if the subgroup order r divides $q^k - 1$, but does not divide $q^i - 1$ for all $0 < i < k$. The Tate pairing [3, 9, 11] (or the Weil pairing [15, 18, 24]) maps the discrete logarithm in G to the discrete logarithm in $\mathbb{F}_{q^k}$, and this is the basis for the Frey-Rück attack [10].

An important open problem in pairing-based cryptography [5, 6, 12, 14, 22, 23, 26, 28] is to build curves containing a subgroup with embedding degree k that is at once big enough to prevent the Frey-Rück attack, but small enough that the Tate pairing is efficiently computable, which in turn means that arithmetic in $\mathbb{F}_{q^k}$ is feasible. The embedding degree is known to be usually enormous [2, 19], and for a long time, the only elliptic curves known to admit subgroups with reasonable k were supersingular curves, particularly over $\mathbb{F}_{3^m}$ where $k = 6$ [18].

Recently, Miyaji, Nakabayashi and Takano [19] showed, using certain properties of the cyclotomic polynomial of order k, how to build non-supersingular

* Co-sponsored by Scopus Tecnologia S. A.

curves over $\mathbb{F}_q$ of prime order with $k = 3, 4, 6$ using the complex multiplication (CM) method [16, 20], as long as certain conditions, which we call the MNT criteria, hold for the field size q, the trace of Frobenius t [24, III.4.6], and the curve order n. However, no technique was known for systematically building curves where $k > 6$ but not enormous.

In this paper we investigate generalizations of the MNT criteria for curves with general embedding degree k, and address the actual construction of such curves. We also discuss representations of the involved fields and groups that lead to efficient implementations of the Tate pairing. Another method for building curves with arbitrary k has been recently proposed by Dupont, Enge and Morain [8].

This paper is organized as follows. Section 2 describes generalizations of the MNT criteria. Section 3 deals with the problem of solving the resulting CM equation to obtain suitable field and curve parameters. Section 4 discusses techniques for efficient implementation of the finite field arithmetic and the Tate pairing. We conclude in section 5.

2 Generalizing the MNT criteria

Any elliptic curve E over $\mathbb{F}_q$ of order n satisfies Hasse's theorem [24, V.1.1], which states that the trace t of the Frobenius endomorphism on E, related to q and n by the equation $n = q + 1 - t$, is restricted to $|t| \leqslant 2\sqrt{q}$.

Given an embedding degree $k > 0$, our goal is to find a prime[4] q, an integer t such that $|t| \leqslant 2\sqrt{q}$, a large prime r satisfying $r \mid q^k - 1$ but $r \nmid q^i - 1$ for all $0 < i < k$, and a curve $E(\mathbb{F}_q)$ whose trace of Frobenius is t and whose order $n = q + 1 - t$ satisfies $r \mid n$, that is, $n = hr$ for some h.

We begin by noticing that $q^u - 1 \equiv (t-1)^u - 1 \pmod{r}$ for all $u > 0$, as it follows by induction from the relation $q = (t - 1) + hr$. Therefore, any suitable r must satisfy $r \mid (t-1)^k - 1$ and $r \nmid (t-1)^i - 1$ for all $0 < i < k$. Let Φ_m be the m-th cyclotomic polynomial [17, definition 2.44]. It is well known [17, theorem 2.45(i)] that $x^u - 1 = \prod_{d|u} \Phi_d(x)$ for any $u > 0$. This leads to the following lemma.

Lemma 1. *Any suitable prime r satisfies $r \mid \Phi_k(t-1)$ and $r \nmid \Phi_i(t-1)$ for all $0 < i < k$.*

Proof. It is necessary that $r \nmid \Phi_i(t-1)$ for all $0 < i < k$, as otherwise $r \mid (t-1)^i - 1$ for some $0 < i < k$. But since r is prime, $r \mid (t-1)^k - 1$ implies $r \mid \Phi_d(t-1)$ for some d dividing k, and the only remaining possibility is $d = k$. Hence, necessarily $r \mid \Phi_k(t-1)$. □

The basic MNT strategy is to choose a trace t of suitable size, finding a prime r in the conditions of the above lemma, computing from t and r a prime of form

[4] Actually, q may be a prime power, but for simplicity we will only refer to the prime case as this is the most relevant in practice.

$q = hr + t - 1$ for some small cofactor[5] h, and finally using the CM method to actually build the desired curve.

2.1 Constraining the parameters

We now derive explicit constraints on the form of t and q, for any h and any k, generalizing the original approach by Miyaji *et al.*

Let ℓ be an integer with $|\ell| > 1$, let r be a prime factor of $\Phi_k(\ell)$, and let d be an integer satisfying $1 \leqslant d \leqslant \deg \Phi_k/2$. Set $n = hr$ for some h, $q = n + \ell^d$, and $t = \ell^d + 1$. It follows from lemma 1 that r satisfies $r \mid \ell^{kd} - 1$, and in general $r \nmid \ell^{id} - 1$ for $0 < i < k$. The restriction $d \leqslant \deg \Phi_k/2$ is imposed to ensure the Hasse bound is satisfied.

Theorem 1. *The choice of parameters proposed above leads to curves containing a subgroup of order r with embedding degree at most k.*

Proof. From the condition $q = hr + \ell^d$ it follows that $q^k - 1 \equiv \ell^{dk} - 1 \pmod r$, by induction on k or considering the binomial expansion of $(hr + \ell^d)^k$. Since $\Phi_k(\ell) \mid \ell^{dk} - 1$ [17, theorem 2.45(i)], the restriction $r \mid \Phi_k(\ell)$ implies $r \mid \ell^{dk} - 1$, that is, $\ell^{dk} - 1 \equiv 0 \pmod r$. Therefore, $q^k - 1 \equiv 0 \pmod r$, that is, $r \mid q^k - 1$. □

An important observation here is that we still must verify that $r \nmid q^i - 1$ for $0 < i < k$, even for such a special case as $r = \Phi_k(\ell)$. Since $\ell^i - 1 = \prod_{u|i} \Phi_u(\ell)$, it is obvious that $\Phi_k(\ell) \nmid \ell^i - 1$, and hence, apparently $r \nmid \ell^i - 1$. However, this reasoning is wrong: the relation $\Phi_k(\ell) \nmid \ell^i - 1$ only holds for the polynomials themselves, not necessarily for some *specific* argument ℓ.

In contrast to the original work by Miyaji *et al.*, the above criteria are not exhaustive, and it is not difficult to find other conditions leading to perfectly valid parameters. For instance, an obvious generalization is $q = n + \Phi_k(\ell)g(\ell) + \ell^d$, for any polynomial $g(\ell)$. This does not help much because in general $\Phi_k(\ell)g(\ell)$ makes the trace t too big to satisfy the Hasse bound, except when the term ℓ^d cancels the term of highest degree in $\Phi_k(\ell)g(\ell)$ and the remaining terms are of suitably low degree (for example, for $k = 9$, by picking an appropriate g, one can obtain $q = n - \ell^3 - 1$). Also, if d is even, k is even, and $k/2$ is odd, it can be verified that setting $t = -\ell^d + 1$ and $q = hr - \ell^d$ is equally possible, that is, $r \mid q^k - 1$ (the restriction to even k such that $k/2$ is odd ensures that $q^{k/2} - 1 \equiv -(\ell^{dk} + 1) \not\equiv 0 \pmod r$). Sometimes, fortuitous solutions barely resembling (but related to) the MNT criteria can be found for particular choices of k. However, for simplicity we will focus on the parameters considered in theorem 1; extending the discussion below to other parameters should not be difficult, and would be hardly necessary in practice.

3 Solving the CM equation

The strategy to build curves given the above criteria seems straightforward: choose ℓ and h, find a prime q and the corresponding trace t according to the

[5] Miyaji *et al.* actually consider only $h = 1$, that is, curves of prime order.

proposed relations, solve for the CM discriminant D (and for V) the CM equation $DV^2 = 4q - t^2$, or equivalently, $DV^2 = 4n - (t-2)^2$, and use the CM method to compute the curve equation coefficients. Since $n = hr$ and $r \mid \Phi_k(\ell)$, we can write $n = m\Phi_k(\ell)$ for some m. Thus, the CM equations for the parameter criteria given in section 2.1 has the form:

$$DV^2 = 4m\Phi_k(\ell) - (\ell^d - 1)^2. \tag{1}$$

Unfortunately, this approach is not practical, because in general the CM discriminant D is too large (comparable to q), and cryptographically significant parameters would have $q \approx 2^{160}$ at least. It is possible to find toy examples using this direct approach, though. For instance, the curve $E : y^2 = x^3 - 3x + 183738738969463$ over $\mathbb{F}_{449018176625659}$ has $4r$ points, where $r = 112254544155601$. The subgroup of order r has embedding degree $k = 12$. This curve satisfies $m = 4$, $r = \Phi_k(\ell)$, $t = \ell + 1$, and $q = 4\Phi_k(\ell) + \ell$ for $\ell = 3255$. The CM equation is $DV^2 = 4q - t^2$ where $D = 13188099$ and $V = 11670$, and the class number is 2940.

Miyaji et al. solve this problem for $k = 3, 4, 6$ by noticing that the CM equation leads, in these cases, to a quadratic Diophantine equation reducible to Pell's equation, whose solution is well known [25]. The case of arbitrary k is much harder, since no general method is known to solve Diophantine equations of degree $\deg(\Phi_k) \geqslant 4$.

However, Tzanakis [27] describes how to solve quartic elliptic Diophantine equations of form

$$V^2 = a\ell^4 + b\ell^3 + c\ell^2 + d\ell + e^2,$$

where $a > 0$ (notice the squared independent term). For $k = 5, 8, 10, 12$, the degree of Φ_k is 4, so that equation 1 has the form $DV^2 = a\ell^4 + b\ell^3 + c\ell^2 + d\ell + f$. If a solution to this equation in small integers is known (as can often be found by exhaustive search), this equation reduces to Tzanakis form by multiplying both sides by D and applying a linear transformation involving the known solution, so that the independent term of the transformed equation is a perfect square.

Unfortunately again, this approach has proven unsuccessful in practice. Using the Magma implementation of Tzanakis method, we were not able to find any cryptographically significant examples of curves with $k = 5, 8, 10, 12$, the only such cases being those where D is too large for traditional CM methods.

We have not tried more recent variants of the CM method like that of [1], so there is still hope that solutions of equation 1 with large D are actually practical. But even if this direct approach remains out of reach, there are successful ways to generate suitable field and curve parameters, as we show next.

3.1 A particular case

Let p be a prime (not to be confused with the finite field size q). We describe how to find algebraic solutions of equation 1 for the special case $D = 3$, $d = 1$, and $k = 3^i 2^j p^s$, for certain exponents i, j, s and prime $p > 3$. In principle, this method enables the ratio m/r to get arbitrarily small for large k if $s = 0$.

The cyclotomic polynomials are known [21] to satisfy the following properties. If v is any prime dividing u, then $\Phi_{uv}(x) = \Phi_u(x^v)/\Phi_u(x)$. On the other hand, if $v \nmid u$, then $\Phi_{uv}(x) = \Phi_u(x^v)$.

Using these properties, it is easy to show by induction that $\Phi_{3^i}(\ell) = \ell^{2 \cdot 3^{i-1}} + \ell^{3^{i-1}} + 1$ and $\Phi_{2^i \cdot 3}(\ell) = \ell^{2^i} - \ell^{2^{i-1}} + 1$ for all $i > 0$. Restrict ℓ so that $\ell \equiv 1 \pmod 3$. Thus, $4\Phi_{3^i}(\ell) - 1 = 3[(2\ell^{3^{i-1}} + 1)/3]^2$ and $4\Phi_{2^i \cdot 3}(\ell) - 3 = [(2\ell^{2^{i-1}} - 1)]^2$. In the first case, multiplying both sides by $(\ell-1)^2$ leads to $4 \cdot (\ell-1)^2 \Phi_{3^i}(\ell) - (\ell-1)^2 = 3[(\ell-1)(2\ell^{3^{i-1}} + 1)/3]^2$, which gives the solution $k = 3^i$, $r = \Phi_{3^i}(\ell)/3$, $t = \ell+1$, $m = (\ell-1)^2$, $V = (\ell-1)(2\ell^{3^{i-1}} + 1)/3$. In the second case, multiplying both sides by $(\ell-1)^2/3$ leads to $4 \cdot [(\ell-1)^2/3]\Phi_{2^i \cdot 3}(\ell) - (\ell-1)^2 = 3[(\ell-1)(2\ell^{2^{i-1}} - 1)/3]^2$, which gives the solution $k = 2^i \cdot 3$, $r = \Phi_{2^i \cdot 3}(\ell)$, $t = \ell + 1$, $m = (\ell - 1)^2/3$, $V = (\ell - 1)(2\ell^{2^{i-1}} - 1)/3$. In both cases, we assume that $q = mr + \ell$ is prime.

Similarly, one can show by induction that, for any prime $p > 3$, $\Phi_{3^i p^j}(\ell) = [(2\ell^{3^{i-1}p^j} + 1)^2 + 3]/[(2\ell^{3^{i-1}p^{j-1}} + 1)^2 + 3]$, for all $i, j > 0$. Multiplying both sides by $12z^2[(2\ell^{3^{i-1}p^{j-1}} + 1)^2 + 3]$ for any z leads to $4 \cdot 3z^2[(2\ell^{3^{i-1}p^{j-1}} + 1)^2 + 3]\Phi_{3^i p^j}(\ell) - (6z)^2 = 3[2z(2\ell^{3^{i-1}p^j} + 1)]^2$. Choosing r to be any large factor of $\Phi_{3^i p^j}(\ell)$, this gives the solution $k = 3^i p^j$, $\ell = 6z + 1$, $n = 3z^2[(2\ell^{3^{i-1}p^{j-1}} + 1)^2 + 3]\Phi_{3^i p^j}(\ell)$, $V = z(2\ell^{3^{i-1}p^j} + 1)$. It is also straightforward (but rather tedious) to show that $\Phi_{3^i 2^j p^s}(\ell) = [(2\ell^{3^{i-1}2^{j-1}p^s} - 1)^2 + 3]/[(2\ell^{3^{i-1}2^{j-1}p^{s-1}} - 1)^2 + 3]$, and hence $4 \cdot 3z^2[(2\ell^{3^{i-1}2^{j-1}p^{s-1}} - 1)^2 + 3]\Phi_{3^i 2^j p^s}(\ell) - (6z)^2 = 3[2z(2\ell^{3^{i-1}2^{j-1}p^s} - 1)]^2$, which gives the solution $k = 3^i 2^j p^s$, $\ell = 6z + 1$, $m = 3z^2[(2\ell^{3^{i-1}2^{j-1}p^{s-1}} - 1)^2 + 3]$, $V = 2z(2\ell^{3^{i-1}2^{j-1}p^s} - 1)$. In all cases, it is necessary to ensure that $q = m\Phi_k(\ell) + \ell$ is prime.

Appendix A contains a detailed example of this method.

It is unclear whether this strategy can be extended to more general k, since the corresponding expressions get very involved. Anyway, this method only produces solutions for $D = 3$, which might have a lower security level, even though no specific vulnerability based on the small D value is known at the time of this writing [4, section VIII.2]. The next method we describe is suitable for much more general D.

3.2 A general method

The general form of the criteria we have been considering is $n = m\Phi_k(\ell)$, $t = \ell^d + 1$, $q = n + t - 1 = m\Phi_k(\ell) + \ell^d$, where $1 \leqslant d \leqslant \deg \Phi_k/2$. Usually one wants m to be small and $\Phi_k(\ell)$ to contain a large prime factor r (the best case is then $\Phi_k(\ell)$ itself being a prime). However, finding actual parameters under these conditions is hard for any k such that $\deg \Phi_k > 2$. Therefore, we relax the restrictions on m, say, by allowing m to be comparable to r. It turns out that obtaining suitable parameters becomes quite easy.

Consider the CM equation $DV^2 = 4m\Phi_k(\ell) - (\ell^d - 1)^2$. We assume that both D and ℓ are chosen and $t \nmid D$; we want to find a solution m (and V) to this equation. For convenience, let $A = 4\Phi_k(\ell)$ and $B = (\ell^d - 1)^2$, so that the equations reads $DV^2 = Am - B$.

Initially, find the smallest positive integer m_0 such that $D \mid Am_0 - B$, that is, $Am_0 - B = z_0 D$ for some z_0. If B is not invertible modulo D (i.e. if B is a multiple of D), then $m_0 = 0$ and $z_0 = B/D^e$ for the largest possible e. If both A and B are invertible modulo D, then $m_0 = B/A \pmod{D}$ and $z_0 = (Am_0 - B)/D$. Finally, if B is invertible modulo D but A is not, there is no solution for this choice of ℓ and D. Therefore, m_0 is never larger than D.

Define:

$$m_i = m_0 + iD,$$
$$z_i = z_0 + iA.$$

Substituting these into the CM equation gives $Dz_i = Am_i - B$. This means that any solution to this equation involves z_i that is a perfect square. Therefore, solve $V^2 = z_0 + iA$ for V and i, and pick up the smallest solution i such that $q = m_i \Phi_k(\ell) + \ell^d$ is a prime. This requires z_0 to be a quadratic residue modulo A. If so, all solutions i_α can be written as $i_\alpha = i_0 + \alpha A$, where $i_0 = (V_0^2 - z_0)/A$ and $V_0 = \sqrt{z_0} \pmod{A}$. A neat strategy to obtain a tight ratio between $\log q$ and $\log r$ is to restrict the search to i_0 alone and vary only ℓ.

Experiments we conducted showed that, in practice, m tends to be close to r. Nevertheless, such solutions are perfectly suitable for most pairing-based cryptosystems, the only exception being the short signature scheme of [6].

Appendix B contains examples of this method.

4 Implementation issues

Since curves with medium-sized embedding degree k can be effectively constructed as described above, the natural question to ask is how to efficiently implement the underlying arithmetic and, particularly, the Tate pairing.

We restrict the discussion to even k. Let $\mathrm{even}(\mathbb{F}_{q^k})$ denote the subset of $\mathbb{F}_{q^k}$ consisting of polynomials whose component monomials are all of even degree, i.e. $\mathrm{even}(\mathbb{F}_{q^k}) = \{u \in \mathbb{F}_{q^k} : u(x) = a_{k-2}x^{k-2} + a_{k-4}x^{k-4} + \cdots + a_0\}$. Similarly, let $\mathrm{odd}(\mathbb{F}_{q^k})$ denote the subset of $\mathbb{F}_{q^k}$ consisting of polynomials whose component monomials are all of odd degree, i.e. $\mathrm{odd}(\mathbb{F}_{q^k}) = \{u \in \mathbb{F}_{q^k} : u(x) = a_{k-1}x^{k-1} + a_{k-3}x^{k-3} + \cdots + a_1 x\}$.

We propose representing $\mathbb{F}_{p^k}$ as $\mathbb{F}_p[x]/R_k(x)$ with a reduction polynomial of form $R_k(x) = x^k + x^2 + \omega$ for some $\omega \in \mathbb{F}_p$. This choice is motivated by the following analysis.

Lemma 2. *If $R(x) = x^k + x^2 + \omega$ is irreducible over $\mathbb{F}_q$, then $r(x) = x^{k/2} + x + \omega$ is irreducible over $\mathbb{F}_q$.*

Proof. By contradiction. If $r(x) = f(x)g(x)$ for some $f, g \in \mathbb{F}_q[x]$, then $R(x) = r(x^2) = f(x^2)g(x^2)$, against the hypothesis that $R(x)$ is irreducible. □

This establishes that the mapping $\psi : \mathbb{F}_q[x]/r(x) \to \mathbb{F}_q[x]/R(x), \psi(f) = F$ such that $F(x) = f(x^2)$, induces an isomorphism between $\mathbb{F}_{q^{k/2}}$ and $\mathrm{even}(\mathbb{F}_{q^k})$.

Notice that this lemma would remain valid if R contained more even-degree monomials, but a trinomial is better suited for efficient implementations. However, it is possible that an irreducible *binomial* $R(x) = x^k + \omega$ exists, in which case it would be an even better choice.

Lemma 3. *Let* $Q = (u, v) \in E(\mathbb{F}_{q^k})$ *where* $E : v^2 = f(u)$*,* $u \in \mathrm{even}(\mathbb{F}_{q^k})$*, and* $f(u)$ *is a quadratic nonresidue. Then* $v \in \mathrm{odd}(\mathbb{F}_{q^k})$*.*

Proof. Notice that $f(u) \in \mathrm{even}(\mathbb{F}_{q^k})$. Let $v(x) = \alpha(x) + x\beta(x)$, where $\alpha, \beta \in \mathrm{even}(\mathbb{F}_{q^k})$. Then $v^2 = (\alpha^2 + \beta^2) + x(2\alpha\beta) \in \mathrm{even}(\mathbb{F}_{q^k})$, so that either $\alpha = 0$ or $\beta = 0$. But $\beta = 0$ would mean that $f(u) = \alpha^2$ is a quadratic residue, against the hypothesis. Therefore, $\alpha = 0$, that is, $v \in \mathrm{odd}(\mathbb{F}_{q^k})$. □

We are now prepared to address the main theorem:

Theorem 2. *Let* $Q = (u, v) \in E(\mathbb{F}_{q^k})$ *where* $E : v^2 = f(u)$*,* $u \in \mathrm{even}(\mathbb{F}_{q^k})$*, and* $f(u)$ *is a quadratic nonresidue. If* $S = (s, t) \in \langle Q \rangle$*, then* $s \in \mathrm{even}(\mathbb{F}_{q^k})$ *and* $t \in \mathrm{odd}(\mathbb{F}_{q^k})$*.*

Proof. This is a consequence of the elliptic addition rules [24, algorithm 2.3]. It is straightforward but tedious to show that the point addition formula and the doubling formula do satisfy the theorem. Thus, we only have to let $S = mQ$, and proceed by induction on m. □

This way, curve points $Q = (u, v) \in E/\mathbb{F}_{p^k}$, where $f(u) \in \mathrm{even}(\mathbb{F}_{q^k})$ is a quadratic nonresidue, are not only suitable for the computation of the Tate pairing $e(P, Q)$ for any $P \in E/\mathbb{F}_p$ (because obviously Q is linearly independent from P); they also have the nice property that the technique of denominator elimination [3, section 5.1] is applicable, thus nearly doubling the performance of Miller's algorithm.

5 Conclusion

We have shown how to effectively solve the problem of constructing elliptic curves with prescribed embedding degree, and suggested ways to efficiently implement the resulting curves, as it is needed by pairing-based cryptosystems.

The possibility of practically constructing curves with arbitrary embedding degree corroborates the need of checking it in conventional cryptosystems to avoid the Frey-Rück attack. On the positive side, a natural subject of further research is whether this can be done for general abelian varieties. We also point out that the problem of generating elliptic curves of prime or near-prime order remains open; such curves are important in certain cryptosystems, like the BLS signature scheme [6].

We are grateful to Steven Galbraith and Frederik Vercauteren for their valuable comments and feedback during the preparation of this work.

References

1. A. Agashe, K. Lauter, R. Venkatesan, "Constructing elliptic curves with a given number of points over a finite field," Cryptology ePrint Archive, Report 2001/096, `http://eprint.iacr.org/2001/096/`.
2. R. Balasubramanian, N. Koblitz, "The improbability that an Elliptic Curve has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm," Journal of Cryptology, Vol. 11, No. 2, 1998, pp. 141–145.
3. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," Cryptology ePrint Archive, Report 2002/008, `http://eprint.iacr.org/2002/008/`.
4. I. Blake, G. Seroussi and N. Smart, "Elliptic Curves in Cryptography," Cambridge University Press, 1999.
5. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Advances in Cryptology – Crypto'2001, Lecture Notes in Computer Science **2139**, pp. 213–229, Springer-Verlag, 2001.
6. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," Asiacrypt'2001, Lecture Notes in Computer Science **2248**, pp. 514–532, Springer-Verlag, 2002.
7. R. Crandall and C. Pomerance, "Prime Numbers: a Computational Perspective," Springer-Verlag, 2001.
8. R. Dupont, A. Enge, F. Morain "Building curves with arbitrary small MOV degree over finite prime fields," Cryptology ePrint Archive, Report 2002/094, available at `http://eprint.iacr.org/2002/094`.
9. G. Frey, M. Müller, and H. Rück, "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems," IEEE Transactions on Information Theory, 45(5), pp. 1717–1719, 1999.
10. 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 (1994), pp. 865–874.
11. S.D. Galbraith, K. Harrison, D. Solera, "Implementing the Tate pairing," Algorithmic Number Theory – ANTS V, 2002, to appear.
12. F. Hess, "Exponent Group Signature Schemes and Efficient Identity Based Signature Schemes Based on Pairings," Cryptology ePrint Archive, Report 2002/012, available at `http://eprint.iacr.org/2002/012/`.
13. IEEE Std 2000–1363, "Standard Specifications for Public Key Cryptography," 2000.
14. A. Joux, "A one-round protocol for tripartite Diffie-Hellman," Algorithm Number Theory Symposium – ANTS IV, Lecture Notes in Computer Science **1838**, pp. 385–394, Springer-Verlag, 2000.
15. A. Joux and K. Nguyen, "Separating Decision Diffie-Hellman from Diffie-Hellman in Cryptographic Groups," Cryptology ePrint Archive, Report 2001/003, `http://eprint.iacr.org/2001/003/`.
16. G.J. Lay, H.G. Zimmer, "Constructing Elliptic Curves with Given Group Order over Large Finite Fields," Algorithmic Number Theory Symposium – ANTS I, Lecture Notes in Computer Science **877** (1994), pp. 250–263.
17. R. Lidl and H. Niederreiter, "Introduction to finite fields and their applications," Cambridge University Press, 1986.
18. A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," IEEE Transactions on Information Theory 39(1993), pp. 1639–1646.

19. A. Miyaji, M. Nakabayashi, and S. Takano, “New explicit conditions of elliptic curve traces for FR-reduction,” IEICE Trans. Fundamentals, Vol. E84 A, no. 5, May 2001.
20. F. Morain, “Building cyclic elliptic curves modulo large primes,” Advances in Cryptology – Eurocrypt’91, Lecture Notes in Computer Science **547** (1991), pp. 328–336.
21. T. Nagell, “Introduction to Number Theory,” 2nd reprint edition, Chelsea Publishing, 2001.
22. K.G. Paterson, “ID-based signatures from pairings on elliptic curves,” Cryptology ePrint Archive, Report 2002/004, available at `http://eprint.iacr.org/2002/004/`.
23. R. Sakai, K. Ohgishi and M. Kasahara, “Cryptosystems based on pairing,” 2000 Symposium on Cryptography and Information Security (SCIS2000), Okinawa, Japan, Jan. 26–28, 2000.
24. J.H. Silverman, “Elliptic curve discrete logarithms and the index calculus,” Workshop on Elliptic Curve Cryptography (ECC’98), September 14–16, 1998.
25. N.P. Smart, “The Algorithmic Resolution of Diophantine Equations,” London Mathematical Society Student Text **41**, Cambridge University Press, 1998.
26. N. Smart, “An Identity Based Authenticated Key Agreement Protocol Based on the Weil Pairing,” Cryptology ePrint Archive, Report 2001/111, available at `http://eprint.iacr.org/2001/111/`.
27. N. Tzanakis, “Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations,” *Acta Arithmetica* **75** (1996), pp. 165–190.
28. E. Verheul, “Self-blindable Credential Certificates from the Weil Pairing,” Advances in Cryptology – Asiacrypt’2001, Lecture Notes in Computer Science **2248** (2002), pp 533–551.

A An example of the closed-form construction

This simple construction implements the method of section 3.1 and quickly yields a curve and a point of large prime order r, with embedding degree $k = 12$.

1. Choose z of an appropriate size at random.
2. Set $w = 3 \cdot z$, $t = w + 2$.
3. Set $r = w^4 + 4w^3 + 5w^2 + 2w + 1$. If r is not prime return to step 1.
4. Set $q = (w^6 + 4w^5 + 5w^4 + 2w^3 + w^2 + 3w + 3)/3$. If q is not prime, return to step 1.
5. Use the CM method to find the curve of the form $y^2 = x^3 + B$ with discriminant $D = 3$ of order $n = q + 1 - t$. Find a point of order r on the curve using the method described in [13, section A11.3].

Note that $n = mr$ and $m = 3z^2$. Rather than using the CM method in step 5, in practice small values of B can be tested to find the correct curve [7].

An example run of this algorithm yields

$$z = 67749197969$$

$$r = 1706481765729006378056715834692510094310238833$$

$$q = 234980175259684736902960831138646770636883178734845136410201584254477$$

$$n = 2349801752596847369029608311386467706368831787348451364081691083153 9$$

Here r is a 151-bit prime, and q is a 224-bit prime. The curve is quickly found as $E : y^2 = x^3 + 4$ over $\mathbb{F}_q$.

B An example of the general construction

Let s be the approximate desired size (in bits) of the subgroup order r, let D be the chosen CM discriminant, and let k be the desired embedding degree. The following procedure implements the general construction method described in section 3.2, and yields a suitable field size q, the subgroup order r, the curve order n (it also indirectly provides the cofactor m, which it seeks to minimize, and the trace of Frobenius t). For simplicity we only consider the case $d = 1$ (cf. section 2.1).

1. Choose $\ell \approx 2^{s/g}$ at random, where $g \equiv \deg(\Phi_k)$.
2. Compute $r \leftarrow \Phi_k(\ell)$, $t \leftarrow \ell + 1$, $A \leftarrow 4r$, and $B \leftarrow (\ell - 1)^2$. Here we could restrict r to be prime (and go back to step 1 if it is not).
3. Check that A is not a perfect square; if it is, choose another ℓ in step 1.
4. Find the smallest m_0 such that $Am_0 - B = z_0 D$ for some z_0, that is:
   (a) if B is not invertible mod D, then $m_0 = 0$ and $z_0 = B/D^e$ for the largest possible e.
   (b) if A and B are both invertible mod D, then $m_0 = B/A \pmod{D}$ and $z_0 = (Am_0 - B)/D$.
   (c) if B is invertible mod D but A is not, there is no solution for this ℓ (hence restart at step 1).
5. Check that z_0 is a quadratic residue mod r; if it is not, choose another ℓ in step 1.
6. Let $V = \sqrt{z_0} \pmod{r}$. If $V^2 - z_0 \neq 0 \pmod{4}$, choose another ℓ in step 1 (this ensures that $V^2 - z_0 = 0 \pmod{A}$).
7. Let $i_0 = (V^2 - z_0)/A$, $m = m_0 + i_0 D$, $n = mr$, and $q = n + t - 1$. If q is not prime, restart with another ℓ at step 1. Otherwise, we have the solution.

An example run of this algorithm for $k = 7$ and $D = 500003$ yields

$$\begin{aligned}
q &= 12507014184746001339698652727369273381429153691361109585242896305246 1\backslash \\
&\quad 410963097505636722876134309 7 \\
r &= 9316148576174318613619119569932653960214872513 1 \\
m &= 1342509094018980683939899818741509350488669517033 2 \\
n &= 12507014184746001339698652727369273381429153691361109585242896305246 1\backslash \\
&\quad 410963097505636722869401349 2 \\
t &= 67329606
\end{aligned}$$

Here r is a 157-bit prime, and q is a 320-bit prime. The curve is quickly found as $E : y^2 = x^3 - 3x + b$ over $\mathbb{F}_q$, where

$$\begin{aligned}
b = {} & 315283565391589690418903185062076693159181569566876474809008162248459\backslash \\
& 2562135264664734043321755 06.
\end{aligned}$$

Another example, this time for $k = 11$ and $D = 500003$:

$$\begin{aligned}
q &= 6457933065634855138129650480350987789632015379681348132364272137169336\backslash \\
&\quad 86883156052523693896455802976765653013549536272470783560105094115 9 \\
r &= 3323772180632929247773347289228681738347763229928181779465948192267 7 \\
m &= 19429529807320017250929519781158178098446838731085667916658667094871 \\
n &= 6457933065634855138129650480350987789632015379681348132364272137169336\backslash \\
&\quad 868831560525236938964558029767656530135495362724707835601045289667 \\
t &= 5651493
\end{aligned}$$

Here r is a 225-bit prime, q is a 448-bit prime, and the curve is $E : y^2 = x^3 + x + b$ over $\mathbb{F}_q$, where

$$\begin{aligned}
b = {} & 1149433909282603066836301091344598051216047703780757772463968059005 05\backslash \\
& 34267578217713248324114121434572733596315614626708485505551511995 5.
\end{aligned}$$