Pairing-Friendly Elliptic Curves of Prime Order

Paulo S. L. M. Barreto[1] and Michael Naehrig[2]

[1] Escola Politécnica, Universidade de São Paulo.
Av. Prof. Luciano Gualberto, tr. 3, n. 158.
BR 05508-900, São Paulo(SP), Brazil.
pbarreto@larc.usp.br
[2] Lehrstuhl für Theoretische Informationstechnik,
Rheinisch-Westfälische Technische Hochschule Aachen.
Sommerfeldstr. 24.
D-52074 Aachen, Germany.
mnaehrig@ti.rwth-aachen.de

Abstract. Previously known techniques to construct pairing-friendly curves of prime or near-prime order are restricted to embedding degree $k \leqslant 6$. More general methods produce curves over $\mathbb{F}_p$ where the bit length of p is often twice as large as that of the order r of the subgroup with embedding degree k; the best published results achieve $\rho \equiv \log(p)/\log(r) \sim 5/4$. In this paper we make the first step towards surpassing these limitations by describing a method to construct elliptic curves of prime order and embedding degree $k = 12$. The new curves lead to very efficient implementation: non-pairing cryptosystem operations only need $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ arithmetic, and pairing values can be compressed to one *sixth* of their length in a way compatible with point reduction techniques. We also discuss the role of large CM discriminants D to minimize ρ; in particular, for embedding degree $k = 2q$ where q is prime we show that the ability to handle $\log(D)/\log(r) \sim (q-3)/(q-1)$ enables building curves with $\rho \sim q/(q-1)$.

Keywords: elliptic curves, pairing-based cryptosystems.

1 Introduction

A non-supersingular elliptic curve over $\mathbb{F}_p$ is called pairing-friendly if it contains a subgroup of order r whose embedding degree k is not too large, which means that computations in the field $\mathbb{F}_{p^k}$ are feasible. The optimal case occurs when the entire curve has prime order and the desired embedding degree.

Pairing-friendly curves of prime or near-prime order are absolutely essential in certain pairing-based schemes like short signatures with longer useful life. For instance, the length of BLS signatures [5] is the size of the base field p; at the 128-bit security level the scheme should be defined on a group of 256-bit order r and be mapped to a finite field of roughly 3072-bit size p^k. In the optimal case, the embedding degree should be $k = 12$. Of course, other systems would benefit as well, since the space requirements for all quantities involved in cryptographic protocols except pairing values would be kept to a minimum (pairing compression techniques [16, 10] would help reducing the bandwidth for pairing values as well).

The pioneering work of Miyaji, Nakabayashi, and Takano [13] describes how to construct elliptic curves of prime order and embedding degree $k \in \{3, 4, 6\}$. Such curves are now dubbed MNT curves, and satisfy $p \sim r$ by the Hasse bound. Extensions of the original MNT construction to curves of near-prime order were investigated by Scott and Barreto [17], and more recently by Galbraith, McKee, and Valença [9][3]. Unfortunately, those methods are restricted to $k \leqslant 6$ and hence only allow for a tradeoff: one has to choose between increasing the base field to a 512-bit prime p (thus doubling the signature size, which ceases to be "short") or contenting oneself with the lower security level of a 1536-bit finite field $\mathbb{F}_{p^6}$.

Let $\rho \equiv \log(p)/\log(r)$ be the ratio between the bit lengths of the finite field and the order of the subgroup with embedding degree k. Several methods have been proposed to construct curves with arbitrary k, including a "folklore" algorithm [4, chapter 9] credited to Cocks and Pinch [7] and related methods due to Barreto, Lynn, and Scott [1] and to Dupont, Enge, and Morain [8]. In general these algorithms only achieve $\rho \sim 2$.

Algebraic methods may produce curves with ρ closer to unity for certain values of k. Such techniques include the families of curves described by Barreto, Lynn, and Scott [3], and by Brezing and Weng [7]. The latter presents the best known results, achieving $\rho \sim 5/4$ for families of curves with $k = 8$ or $k = 24$, and $\rho \sim (k+2)/(k-1)$ for prime k (hence $\rho \leqslant 5/4$ for prime $k \geqslant 13$). Such ratios are already useful under many circumstances. Still, for most embedding degrees the value of ρ is larger than this; for instance, the best published value for $k = 12$ is $\rho \sim 3/2$. Besides, the use of prime k precludes many optimizations that are only possible for even k [2], making the computation of pairings much less efficient.

In spite of all these efforts, constructing pairing-friendly curves with prime order has remained an elusive open problem since it was posed by Boneh *et al.* [5, section 3.5] (see also [6, section 4.5]).

This paper is organised as follows.

Our main contribution, described in section 2, is a surprisingly simple algorithm to construct curves of prime order and embedding degree $k = 12$. The resulting security enhancement is even better than the lower bound of $k = 10$ required by Boneh *et al.*. Using the proposed method, even a 160-bit signature maps to 1920-bit field, where the best algorithms to compute discrete logarithms are worse than Pollard-rho in the elliptic group itself.

We next discuss how to compress the representations of points and pairing values to one sixth of their expected length for the proposed curves in section 3. It turns out that non-pairing operations only need arithmetic over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$,

[3] Interestingly, the latter work also considers the construction of hyperelliptic curves of genus $g = 2$ analogous to MNT elliptic curves, for which the range of embedding degrees is $k \in \{5, 8, 10, 12\}$, but the security ratio k/g is still bound by 6.

and it is possible to compute pairings compressed to one sixth of their length without resorting to full arithmetic on fields larger than $\mathbb{F}_{p^2}$.

Finally, we show in section 4 that the ability to handle large complex multiplication (CM) discriminants may have a positive influence on the minimization of ρ. In particular, for embedding degree $k = 2q$ where q is prime we describe how to build curves with $\rho \sim q/(q-1)$ and $\log(D)/\log(r) \sim (q-3)/(q-1)$. Such discriminants are thus much smaller than expected from random curves with the same embedding degree. We also briefly discuss the possibility of building curves of nearly-prime order over extension fields.

We conclude and summarise our results in section 5.

2 The proposed method for $k = 12$

Theorem 1. *There exists an efficient algorithm to construct elliptic curves of prime order (of nearly arbitrary bitlength) and embedding degree $k = 12$ over a prime field.*

Proof. We follow the strategy of parametrising $p(x)$, $n(x)$ and $t(x)$, and using the property that $n \mid \Phi_k(t-1)$ as in [1]. Since Φ_{12} is quartic and we know from the Hasse bound that $n \sim p \sim t^2$, we must take $t(x)$ to be a quadratic polynomial such that $n(x)$ is a quartic factor of $\Phi_{12}(t-1)$.

Galbraith *et al.* showed [9] that the only quadratic polynomials $u(x)$ such that $\Phi_{12}(u(x))$ splits into two irreducible quartic factors are $u(x) = 2x^2$ and $u(x) = 6x^2$. Setting the trace of the Frobenius to be $t(x) = 6x^2 + 1$, we obtain

$$\Phi_{12}(t(x) - 1) = n(x)n(-x),$$

where $n(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$. From the relation $n = p + 1 - t$ we get the irreducible polynomial $p(x) = n(x) + t(x) - 1 = 36x^4 + 36x^3 + 24x^2 + 6x + 1$. The CM norm equation becomes

$$DV^2 = 4p - t^2 = 3(6x^2 + 4x + 1)^2.$$

Assuming that, for some x_0, both $n = n(x_0)$ and $p = p(x_0)$ evaluate to prime numbers, the CM method for discriminant $D = 3$ [12, 14] produces curves of form $E(\mathbb{F}_p) : y^2 = x^3 + b$, with $b \neq 0$.

Finding b is actually very simple: take the smallest $b \neq 0$ such that $b + 1$ is a quadratic residue mod$p$ and the point $G = (1, \sqrt{b+1} \bmod p)$, which is clearly on the curve[4], satisfies $nG = \infty$. This method is a simplification of the technique described in [11, section A.14.4] and quickly converges to a suitable b.

We see that the bitlength m of the curve order can be easily tailored by a suitable choice of x_0, namely, start with the smallest $x \sim 2^{m/4}$ such that $n(x)$ has bitlength m and increase it until finding some x_0 such that $n(x_0)$ and $p(x_0)$ are prime. □

[4] Since the curve order $n(x)$ is a large prime, there is no point of form $(0, y)$, which would necessarily have order 3.

In summary, we have the following parametrisation, where x may take either positive or negative values:

$$\begin{aligned} t &= 6x^2 + 1, \\ n &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ p &= 36x^4 + 36x^3 + 24x^2 + 6x + 1, \\ DV^2 &= 108x^4 + 144x^3 + 84x^2 + 24x + 3 = 3(6x^2 + 4x + 1)^2. \end{aligned}$$

The choice $u(x) = 2x^2$ as indicated in [9] is not considered, since in this case DV^2 factors as a square free product of irreducible polynomials which in general leads to an enormous CM discriminant D and therefore is not practical. This would also be the case if one took $u(x)$ to be a linear polynomial.

Algorithm 1 shows how the CM method simplifies in our setting. The algorithm takes as input value the desired bitlength of the primes p and n, and returns instances of these primes computed as indicated in the proof of theorem 1, plus a parameter $b \in \mathbb{F}_p$ such that the curve $E(\mathbb{F}_p) : y^2 = x^3 + b$ has order n over the field $\mathbb{F}_p$, and the coordinate y of a sample generator $G = (1, y)$. Appendix A gives a few examples of cryptographic interest. Algorithm 1 tends to produce the smallest p and n of the desired bitlength, but it is straightforward to modify it so that the output parameters meet other simple criteria (for instance, the examples in appendix A were selected to maximize p and n while keeping $b = 3$).

The parametrisation given above may also be deduced in terms of [7]. Choosing a polynomial $u(x)$ such that $\Phi_k(u(x))$ splits may then be interpreted as choosing a suitable number field in the following way. Let $l(x)$ be an irreducible factor of $\Phi_k(u(x))$ and consider the number field

$$K = \mathbb{Q}[x]/(l(x)).$$

As $u(x)$ is a root of Φ_k over K it is a primitive k-th root of unity modulo l. If D is chosen such that $-D$ is a square in K we set $t(x) = u(x)^i + 1 \bmod l(x)$ and $V(x) := (u(x)^i - 1)\sqrt{-D}^{-1} \bmod l(x)$ where $i \in \{1, \ldots, k-1\}$. If $p(x) = (t(x)^2 - DV(x)^2)/4$ is irreducible, one sets $n = p + 1 - t$. We are able to check for the ratio $\deg(p)/\deg(l)$ to be less than a certain given bound. Choosing $u(x) = 6x^2$ and $D = 3$ yields the above parametrisation as well.

Contrary to the case $k = 12$, finding parametrisations when $\varphi(k) > 4$ (but keeping k reasonably small) seems a rather difficult problem. The method suggested in [9] to find quadratic polynomials $u(x)$ such that $\Phi_k(u(x))$ splits, implies finding integer or rational points on an elliptic curve. Increasing $\varphi(k)$ leads to a higher number of indeterminates and also increases the number of equations to deal with. To combine them into a single equation of an elliptic curve may in this case be impossible. The computation of a resultant as suggested in [9] only reduces the number of indeterminates by one and thus in general will not help. One may try to find polynomials $u(x)$ of degree greater than two such that $\Phi_k(u(x))$ splits, but this results in higher degree equations to be solved. We leave it as an open problem the task of buidling curves of prime order and $\varphi(k) > 4$.

Algorithm 1 Constructing a curve of prime order with $k = 12$

INPUT: the approximate desired size m of the curve order (in bits).

OUTPUT: parameters p, n, b, y such that the curve $y^2 = x^3 + b$ has order n over $\mathbb{F}_p$ and the point $G = (1, y)$ is a generator of the curve.

Let $P(x) \equiv 36x^4 + 36x^3 + 24x^2 + 6x + 1$
Compute the smallest $x \approx 2^{m/4}$ such that $\lceil \log_2 P(-x) \rceil = m$.
loop
    $t \leftarrow 6x^2 + 1$
    $p \leftarrow P(-x), \quad n \leftarrow p + 1 - t$
    if p and n are prime **then**
        exit loop
    end if
    $p \leftarrow P(x), \quad n \leftarrow p + 1 - t$
    if p and n are prime **then**
        exit loop
    end if
    $x \leftarrow x + 1.$
end loop
$b \leftarrow 0$
repeat
    repeat
        $b \leftarrow b + 1$
    until $b + 1$ is a quadratic residue mod p
    Compute y such that $y^2 = b + 1 \bmod p$
    $G \leftarrow (1, y)$ on the curve $E : y^2 = x^3 + b$
until $nG = \infty$
return p, n, b, y.

Furthermore, for efficiency reasons in the pairing computation it is desirable to generate curves of prime order n such that n has a low Hamming weight. Constructing such curves for $k = 12$ or $\varphi(k) > 4$ is still a research problem.

3 Six-to-one point and pairing compression

A fascinating possibility suggested by the proposed curves is to enable cryptosystems more efficient than what was attainable with most previously known curves. We now consider two such improvements, namely, point compression and pairing compression, both to about one sixth of the requirements one would expect in naive implementations.

The basic idea for point compression is not only to restrict the first pairing argument to $E(\mathbb{F}_p)$, but also to take the second argument $Q \in E(\mathbb{F}_{p^{12}})$ as the image $\psi(Q')$ of a point on a sextic twist $E'(\mathbb{F}_{p^2})$, where $\psi : E'(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^{12}})$ is an injective group homomorphism. This way one would work only with $E(\mathbb{F}_p)$ and $E'(\mathbb{F}_{p^2})$ for non-pairing operations like key generation, and map from $E'(\mathbb{F}_{p^2})$ to $E(\mathbb{F}_{p^{12}})$ only when actually computing pairing values. As it turns out, it is possible to do better than this, namely, one can work with smaller fields, as we show next.

Lemma 1. *There exists $\xi \in \mathbb{F}_{p^2}^*$ such that $X^6 - \xi$ is irreducible over $\mathbb{F}_{p^2}[X]$ whenever $p \equiv 1 \pmod 6$.*

Proof. Since $p^2 \equiv 1 \pmod 6$, the order of $\mathbb{F}_{p^2} = p^2 - 1$ is a multiple of 6. Thus for any primitive root $a \in \mathbb{F}_{p^2}$, the cube roots of unity are $\{1, \zeta, \zeta^2\}$ where $\zeta \equiv a^{(p^2-1)/3}$. Hence every cube $u^3 \in \mathbb{F}_{p^2}^*$ has three distinct cube roots, namely, $\{u, \zeta u, \zeta^2 u\}$, which means that only one third of the elements of $\mathbb{F}_{p^2}^*$ are cubes. Analogously, only one half of the elements of $\mathbb{F}_{p^2}^*$ are squares. Therefore, there must be some element $\xi \in \mathbb{F}_{p^2}^*$ that is neither a square nor a cube, and hence $X^6 - \xi$ is irreducible over $\mathbb{F}_{p^2}[X]$. □

Any $\xi \in \mathbb{F}_{p^2}^*$ provided by lemma 1 may be used to represent $\mathbb{F}_{p^{12}}$ as $\mathbb{F}_{p^2}[X]/(X^6 - \xi)$ and to define a sextic twist $E'(\mathbb{F}_{p^2}) : y'^2 = x'^3 + b/\xi$. A sensible strategy to obtain ξ without resorting to full $\mathbb{F}_{p^{12}}$ arithmetic is to set $1/\xi = \lambda^2 \mu^3$ where $\lambda \in \mathbb{F}_p$ is a noncube and $\mu \in \mathbb{F}_{p^2}$ is a nonsquare.

Let $z \in \mathbb{F}_{p^{12}}$ be a root of $X^6 - \xi$. The corresponding map $\psi : E'(\mathbb{F}_{p^2}) \to E(\mathbb{F}_{p^{12}})$ is $(x', y') \mapsto (z^2 x', z^3 y')$. Notice that $x = z^2 x' \in \mathbb{F}_{p^6}$ and $y = z^3 y' \in \mathbb{F}_{p^4}$. Also, since any element of $\mathbb{F}_{p^{12}}$ has the form $a_5 z^5 + a_4 z^4 + a_3 z^3 + a_2 z^2 + a_1 z + a_0$ the computation of $\psi(Q')$ does not incur any multiplication overhead, and its rather sparse structure favours efficient implementation of the pairing algorithm.

Alternatively, one may use ξ^5 instead of ξ if the first choice produces a twist E' of wrong order (ξ^2, ξ^3, and ξ^4 give quadratic and cubic twists).

These considerations open the way to compressing pairing values to one sixth of their length in a way that is compatible with point reduction (that is, the technique of keeping only one point coordinate and entirely discarding the other one). Notice that the map $(x', y') \mapsto (z^2x', z^3y')$ produces a point on $E(\mathbb{F}_{p^{12}})$ whose x-coordinate is in $\mathbb{F}_{p^6}$ and whose y-coordinate is in $\mathbb{F}_{p^4}$.

Now suppose that we keep only the y-coordinate of the point $Q' = (x', y')$ on the twist $E'(\mathbb{F}_{p^2}) : y'^2 = x'^3 + b/\xi$ (this is contrary to the conventional choice of keeping only the x-coordinate). There are three points associated to this y-coordinate corresponding to the three cube roots of $y'^2 - b/\xi$. One of the points is Q'. Upon mapping onto $E(\mathbb{F}_{p^{12}})$, it turns out that those points map to *conjugates* over $\mathbb{F}_{p^4}$ (i.e. their images are of form Q, $[p^4]Q$ and $[p^8]Q$) provided Q' is an n-torsion point. This can be seen from the following arguments. Notice that the order of the twist is $\#E'(\mathbb{F}_{p^2}) = (p+1-t)(p-1+t) = n(2p-n)$ and hence there exist n-torsion points. Let ϕ be the p-th power Frobenius endomorphism and $\mathrm{tr}_{\mathbb{F}_{p^6}} : E(\mathbb{F}_{p^{12}}) \to E(\mathbb{F}_{p^6}),\ R \mapsto R + \phi^6(R)$ the trace map over $\mathbb{F}_{p^6}$. An explicit computation leads to the following lemma.

Lemma 2. *Let $Q' = (x', y') \in E'(\mathbb{F}_{p^2})$ and $Q = \psi(Q')$. Then $\mathrm{tr}_{\mathbb{F}_{p^6}}(Q) = Q + \phi^6(Q) = O$.*

The Frobenius endomorphism has two eigenspaces in $E(\mathbb{F}_{p^{12}})[n]$ for the eigenvalues $1, p$. The 1-eigenspace consists of all points in $E(\mathbb{F}_p)$ while the p-Eigenspace is the set of points of trace zero. Therefore we obtain the following lemma which shows that for an n-torsion point whose $\mathbb{F}_{p^6}$-trace is O computing the p-multiple is the same as computing the Frobenius endomorphism.

Lemma 3. *Let $Q \in E(\mathbb{F}_{p^{12}})[n]$. Then $\mathrm{tr}_{\mathbb{F}_{p^6}}(Q) = O$ iff $\phi(Q) = [p]Q$.*

Let $Q = \psi(Q')$ for an n-torsion point Q' on the sextic twist. From lemma 2 we see that we may apply lemma 3 and compute $[p^4]Q = \phi^4(Q) = ((z^2)^{p^4}x', z^3y')$ as well as $[p^8]Q = \phi^8(Q) = ((z^2)^{p^2}x', z^3y')$. The points $Q, [p^4]Q$ and $[p^8]Q$ share the same y-coordinate and therefore have to be the images under ψ of the above mentioned three points corresponding to the given y-coordinate on the twist.

The above shows that the pairing values computed from the three points are also conjugates over $\mathbb{F}_{p^4}$ (i.e. they are of the form e, e^{p^4} and e^{p^8}). Thus, the $\mathbb{F}_{p^4}$-trace of these pairing values is the same for any of the three points. In other words, the choice of the cube root is irrelevant to compute the compressed pairing $\varepsilon(P, Q') \equiv \mathrm{tr}_{\mathbb{F}_{p^4}}(e(P, \psi(Q'))) = e(P, \psi(Q')) + e(P, \psi(Q'))^{p^4} + e(P, \psi(Q'))^{p^8}$, whose length is one third of the length of $e(P, \psi(Q'))$.

One even may go one step further and not only discard the x-coordinate of Q' but also discard one bit of its y-coordinate. This means we do not distinguish between Q' and $-Q'$. With help of the following lemma we can show that pairing compression up to one sixth of the actual pairing length is possible.

Lemma 4. *Let ζ be an n-th root of unity in $\mathbb{F}_{p^{12}}$ and $\mathrm{tr}_{\mathbb{F}_{p^2}} : \mathbb{F}_{p^{12}} \to \mathbb{F}_{p^2}$ the finite field trace over $\mathbb{F}_{p^2}$. Then $\mathrm{tr}_{\mathbb{F}_{p^2}}(\zeta^{-1}) = \mathrm{tr}_{\mathbb{F}_{p^2}}(\zeta)$.*

Proof. Since n divides $\Phi_{12}(t-1)$ it divides $\Phi_{12}(p) = p^4 - p^2 + 1$. So n also divides $p^6 + 1 = (p^2+1)(p^4 - p^2 + 1)$. Therefore since ζ is an n-th root of unity we have $\zeta^{-1} = \zeta^{p^6}$. We now see that $\mathrm{tr}_{\mathbb{F}_{p^2}}(\zeta^{-1}) = \zeta^{-1} + \zeta^{-p^2} + \zeta^{-p^4} + \zeta^{-p^6} + \zeta^{-p^8} + \zeta^{-p^{10}} = \zeta^{p^6} + \zeta^{p^8} + \zeta^{p^{10}} + \zeta + \zeta^{p^2} + \zeta^{p^4} = \mathrm{tr}_{\mathbb{F}_{p^2}}(\zeta)$. □

Note that all pairing values are n-th roots of unity in $\mathbb{F}_{p^{12}}$ and hence $\mathrm{tr}_{\mathbb{F}_{p^2}}(e(P,\psi(Q'))) = \mathrm{tr}_{\mathbb{F}_{p^2}}(e(P,\psi(Q'))^{-1}) = \mathrm{tr}_{\mathbb{F}_{p^2}}(e(P,\psi(-Q')))$. Together with the transitivity of traces using the above condition on $\mathbb{F}_{p^4}$- traces, this yields that the $\mathbb{F}_{p^2}$-traces of the pairing values are equal for all points $(x', \pm y'), (\zeta_3 x', \pm y')$ and $(\zeta_3^2 x', \pm y')$ where $\zeta_3^3 = 1$ in $\mathbb{F}_{p^2}$.

The advantage of this approach is that one can not only work exclusively on $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ for non-pairing operations, but also represent points on $E'(\mathbb{F}_{p^2})$ by the positive or negative of their y-coordinates alone in most protocols, yet obtain a unique compressed pairing value over $\mathbb{F}_{p^2}$. We point out that the compression ratio of $1/6$ is better than what is attainable on any practical supersingular Abelian variety, namely, $8/30$, as shown by Rubin and Silverberg [15].

Laddering techniques as those described in [16] to compute pairings may even make it unnecessary to implement full arithmetic over any field higher than $\mathbb{F}_{p^2}$. Similar effects may be achieved in a torus-based setting as suggested in [10]. If the x-coordinate corresponding to a point in $E'(\mathbb{F}_{p^2})$ with given y-coordinate y' is needed, one may obtain it by simply computing a cube root of $y'^2 - b/\xi$. In appendix B we discuss the computation of cube roots in $\mathbb{F}_{p^2}^*$.

4 Considerations on composite order

Under some circumstances, a reasonably small cofactor may be quite acceptable. For instance, if 256-bit prime fields do not have a substantial impact on bandwidth occupation, the Brezing-Weng family of curves for $k = 8$ and $\rho \sim 5/4$ could provide roughly 200-bit group orders and map the discrete logarithm on the curve to a 2048-bit finite field. Besides, as we already pointed out even values of k are advantageous from the point of view of efficient implementation of the pairing algorithm. It is thus interesting to investigate ways to produce more curves that meet the conditions that k be even and $\rho > 1$ be as small as possible (say, $\rho \leqslant 5/4$).

A naive approach to solving the norm equation $DV^2 = 4h\Phi_k(t-1) - (t-2)^2$, namely, by choosing t and hoping to be able to handle the resulting D, is in general bound to failure since $D \sim t^{\varphi(k)}$, where $\varphi(k)$ is Euler's totient function. For instance, for $k = 2q$ where q is an odd prime we expect to find $D \sim t^{q-1}$.

However, it would be quite simple to obtain curves with $k = 2q$ if we could handle a CM discriminant D as large as t^{q-3}, attaining $\rho \equiv \log(p)/\log(r) \sim q/(q-1)$ as the following reasoning reveals. Let the trace of Frobenius have the form $t = -4u^2 + 2$ for some u (notice that t is negative), and let $x = t - 1$.

Assume that $\Phi_k(x)$ takes a prime value. Then set:

$$\begin{aligned}
h &= -(x-1)/4, \\
r &= \Phi_k(x) \\
&= x^{q-1} - x^{q-2} + x^{q-3} - x^{q-4} + x^{q-5} - \cdots - x + 1 \\
&= x^{q-1} - x^{q-3}(x-1) - x^{q-5}(x-1) - \cdots - x^2(x-1) - (x-1), \\
p &= hr + t - 1, \\
DV^2 &= 4hr - (t-2)^2 \\
&= -(x-1)x^{q-1} + x^{q-3}(x-1)^2 + x^{q-5}(x-1)^2 + \cdots + (x-1)^2 - (x-1)^2 \\
&= -(x-1)x^2[x^{q-3} - (x-1)(x^{q-5} + x^{q-7} + \cdots + 1)].
\end{aligned}$$

By construction, the $-(x-1)x^2$ factor is a square, so D is the square-free part of $z = x^{q-3} - (x-1)(x^{q-5} + x^{q-7} + \cdots + 1)$. Since $p = hr + t - 1$, it is also clear that $\rho \sim q/(q-1)$. For instance, if $k = 10$ (i.e. $\rho \sim 5/4$) we get $z = x^2 - x + 1$, and a simple search produces parameters like these:

$t = -931556989582$: 40 bits

$r = 753074106157227719531468778253698105623799226081$: 160 bits

$p = 175382861816372173247473133505975362972517516867279787545493$: 197 bits

$\rho \sim 1.237425$

$D = 867798424841873127503473$: 80 bits

Another example, now for $k = 14$ (i.e. $\rho \sim 7/6$) where $z = x^4 - x^3 + x^2 - x + 1$:

$t = -82011134$: 27 bits

$r = 304254450525046050085067914513460261078757135361$: 158 bits

$p = 623806328015370575494732907659994082548136453468333889$: 183 bits

$\rho \sim 1.153987$

$D = 45236739484946456935793243535361$: 106 bits

Unfortunately, with currently available CM technology the only case where this construction is tractable occurs for $k = 6$, where we get $D = 1$ but also $\rho \sim 3/2$, much worse than plain MNT curves that attain $\rho \sim 1$.

4.1 Curves over extension fields

Another interesting observation is that, while none of the currently known methods to construct pairing-friendly curves for arbitrary k is able to produce curves over an extension field $\mathbb{F}_{p^m}$, it may be possible to fill this gap if sufficiently large D can be handled. As Galbraith *et al.* point out [9], parametrising $t = 5x^2 + 1$ causes $\Phi_5(t-1)$ to split as $\Phi_5(t-1) = r(x)r(-x)$, where

$r(x) = 25x^4 + 25x^3 + 15x^2 + 5x + 1$. We observe that with cofactor $h = 4$, this gives $hr + t - 1 = (10x^2 + 5x + 2)^2$, a perfect square. This means that finding an odd value $x \in \mathbb{Z}$ such that r and $p = 10x^2 + 5x + 2$ are both prime enables constructing an elliptic curve over a finite field $\mathbb{F}_{p^2}$ with near-prime order $n = 4r$.

The CM equation here has the form $DV^2 = 5(5x^2 \pm 2x + 1)(15x^2 \pm 10x + 3)$. Solving a Pell-like equation can make one but not both of the factors $5x^2 \pm 2x + 1$ or $15x^2 \pm 10x + 3$ to assume the form dy^2 for small d and some y. One might hope that techniques like Hensel lifting could reduce the square-free part of the other factor to $O(x)$, but it is not clear how to harmonise such techniques to solutions of the Pell-like equation. As a consequence, we expect that $D \sim p \sim r^{1/2}$; practical values of p would need $D \sim 2^{100}$ at least.

Nevertheless, such a parametrisation hints that algebraic methods to build ordinary pairing-friendly curves over extension fields might exist for other embedding degrees, and deserved further research.

5 Conclusion

We have presented a very simple algorithm to construct pairing-friendly curves of prime order and embedding degree $k = 12$. This closes (and actually exceeds) the open problem proposed by Boneh *et al.* [5, section 3.5] and enhances the security level of most pairing-based cryptosystems, while also reducing bandwidth occupation (by either points or pairing values) down to 1/6 of the expected requirements; such levels of security and compression are better than what is attainable with any supersingular Abelian variety up to at least genus 6. We leave it as an open problem the task of extending the method for higher values of k.

We have also discussed ways to produce curves of composite order and reasonably small cofactor as long as large discriminants fall within reach of CM methods, and pointed out the possibility of closing yet another problem, namely, building pairing-friendly curves of nearly-prime order over extension fields. Further exploration of such possibilities is left for future research.

6 Acknowledgments

We are grateful to Peter Birkner, Dan Boneh, Steven Galbraith, Florian Heß, Tanja Lange, Ben Lynn, Alfred Menezes, Mike Scott, Fré Vercauteren, and Felipe Voloch for their valuable comments on an earlier version of this work.

References

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

2. 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-Verlag, 2003.
3. P. S. L. M. Barreto, B. Lynn, and M. Scott. Efficient implementation of pairing-based cryptosystems. *Journal of Cryptology*, 17(4):321–334, 2004.
4. I. Blake, G. Seroussi, and N. Smart. *Advances in Elliptic Curve Cryptography*. Number 317 in London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, UK, 2005.
5. 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-Verlag, 2002.
6. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004.
7. F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. Cryptology ePrint Archive, Report 2003/143, 2003. Available from `http://eprint.iacr.org/2003/143`.
8. R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. *Journal of Cryptology*, 18(2):79–89, 2005.
9. S. Galbraith, J. McKee, and P. Valença. Ordinary abelian varieties having small embedding degree. Cryptology ePrint Archive, Report 2004/365, 2004. Available from `http://eprint.iacr.org/2004/365`.
10. R. Granger, D. Page, and M. Stam. On small characteristic algebraic tori in pairing-based cryptography. Cryptology ePrint Archive, Report 2004/132, 2004. Available from `http://eprint.iacr.org/2004/132`.
11. IEEE Computer Society, New York, USA. *IEEE Standard Specifications for Public-Key Cryptography – IEEE Std 1363-2000*, 2000.
12. G.-J. Lay and H. G. Zimmer. Constructing elliptic curves with given group order over large finite fields. In *Algorithmic Number Theory Symposium – ANTS-I*, volume 877 of *Lecture Notes in Computer Science*, pages 250–263. Springer-Verlag, 1994.
13. 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.
14. F. Morain. Building cyclic elliptic curves modulo large primes. In *Advances in Cryptology – Eurocrypt'1991*, volume 547 of *Lecture Notes in Computer Science*, pages 328–336. Springer-Verlag, 1991.
15. K. Rubin and A. Silverberg. Supersingular abelian varieties in cryptology. In *Advances in Cryptology – Crypto'2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 336–353. Springer-Verlag, 2002.
16. 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, Santa Barbara, USA, 2004. Springer-Verlag.
17. M. Scott and P. S. L. M. Barreto. Generating more MNT elliptic curves. *Designs, Codes and Cryptography*, 2005. To appear.

A Some curves of prime order and $k = 12$

All of the following curves satisfy the equation $E(\mathbb{F}_p) : y^2 = x^3 + 3$, with prime order n and trace of the Frobenius t. A sample generator for any of them is

$G = (1, 2)$. In all cases $p \equiv 3 \pmod 4$ and $p \equiv 4 \pmod 9$ (to simplify the computation of square and cube roots), and the bitlengths of p and n are equal. The field $\mathbb{F}_{p^2}$ is represented as $F_p[X]/(X^2+1)$, and i is a root of X^2+1. The sextic twist for all examples has the form $E'(\mathbb{F}_{p^2}) : y'^2 = x'^3 + 3/\xi$, where $1/\xi = \lambda^2\mu^3 = -8+8i$, $\lambda = 2$, and $\mu = 1+i$.

160 bits:

$$
\begin{aligned}
p &= 1461501624496790265145448589920785493717258890819\\
n &= 1461501624496790265145447380994971188499300027613\\
t &= 1208925814305217958863207
\end{aligned}
$$

192 bits:

$$
\begin{aligned}
p &= 6277101719531269400517043710060892862318604713139674509723\\
n &= 6277101719531269400517043709981664699904401744160036556389\\
t &= 79228162414202968979637953335
\end{aligned}
$$

224 bits:

$$
\begin{aligned}
p &= 26959946667149205758383469736921695435015736735261155141423417423923\\
n &= 26959946667149205758383469736921690242718878200571531029749235996909\\
t &= 5192296858534689624111674181427015
\end{aligned}
$$

256 bits:

$$
\begin{aligned}
p &= 1157920892373149368726885612444717420583758783557612051987004095226 29\backslash\\
&\quad 664518163\\
n &= 115792089237314936872688561244471742058035595988840268584488757999429\backslash\\
&\quad 535617037\\
t &= 340282366920936614211651523200128901127
\end{aligned}
$$

B Computing cube roots

Each prime number of form $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$ is congruent to $6x^2 + 6x + 1 \pmod 9$ and hence for all values of $x \in \mathbb{Z}$ it holds that $p(x) \equiv 1 \pmod 9$ or $p(x) \equiv 4 \pmod 9$. In the second case where we get a prime $p \equiv 4 \pmod 9$ computing cube roots modulo p only takes one exponentiation which may be seen from the following.

Let α be a primitive element of $\mathbb{F}_p^*$. The set of all cubes in $\mathbb{F}_p^*$ is exactly $\{\alpha^{3l} \mid l \in \mathbb{Z}\}$. Now let a be a cube in $\mathbb{F}_p^*$. Then $a^{(p-1)/3} \equiv 1 \pmod p$. Therefore we get a simple possibility to compute a cube root r of a by one exponentiation

$$r \equiv a^{(2p+1)/9} \pmod p.$$

Since $(2p+1)/9$ is the inverse to 3 modulo $(p-1)/3$, this clearly gives a cube root of a.

The examples given in appendix A all have $p \equiv 4 \pmod 9$. For recovering the x-coordinate of points on $E'(\mathbb{F}_{p^2})$ given only their y-coordinate as it was indicated in section 3 one needs to compute a cube root in $\mathbb{F}_{p^2}^*$. We consider the case $p \equiv 4 \pmod 9$. Then $p^2 \equiv 7 \pmod 9$. For a cube $a \in \mathbb{F}_{p^2}^*$ it holds $a^{(p^2-1)/3} = 1$ for the same reasons as in the $\mathbb{F}_p$ case. Again the computation of a cube root only takes one exponentiation $r = a^{(p^2+2)/9}$.