Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field

Ezekiel J. Kachisa[1], Edward F. Schaefer[2], and Michael Scott[1,⋆]

[1] School of Computing
Dublin City University
Ireland
ekachisa@computing.dcu.ie,
mike@computing.dcu.ie
[2] Department of Mathematics and Computer Science
of Santa Clara University
USA
eschaefer@scu.edu

Abstract. We describe a new method for constructing Brezing-Weng-like pairing-friendly elliptic curves. The new construction uses the minimal polynomials of elements in a cyclotomic field. Using this new construction we present new "record breaking" families of pairing-friendly curves with embedding degrees of $k \in \{16, 18, 36, 40\}$, and some interesting new constructions for the cases $k \in \{8, 32\}$.

1 Introduction

Standard cryptosystems such as the Elliptic Curve Digital Signature Algorithm, Elliptic Curve Diffie-Hellman and ElGamal Elliptic Curve Encryption require randomly generated elliptic curves for their implementation. On the other hand cryptosystems such as short digital signatures, identity-based encryption and one-round three-way key exchange, require so-called pairing-friendly elliptic curves. These curves have special properties which most randomly generated curves will not have. The interest in recent times is to explore various methods of constructing pairing-friendly elliptic curves with prescribed embedding degrees, ideally to make them readily available, more efficient and more secure. Many strategies have been proposed by different researchers to construct such curves ([1, 3, 4, 5, 7, 13]).

Of particular interest to our discussion is the strategy of constructing pairing friendly elliptic curves as proposed by Brezing and Weng [4]. This construction basically uses the Cocks and Pinch idea [5] over polynomials. The interesting point in the Brezing-Weng method is that it reduces the ratio between the bit lengths of the finite field p and the order r of the subgroup with embedding

⋆ These authors acknowledge support from the Science Foundation Ireland under Grant No. 06/MI/006.

S.D. Galbraith and K.G. Paterson (Eds.): Pairing 2008, LNCS 5209, pp. 126–135, 2008.

degree k. This is measured by using a parameter ρ, defined as $\frac{\log p}{\log r}$. For example the Cocks-Pinch method invariably produces curves with $\rho \sim 2$, which is rather inefficient. It is observed that small ρ-values are desirable in speeding up the arithmetic on the curves in the underlying field. Ideally we would prefer $\rho = 1$, which is already achieved by the MNT [13], BN [1] and Freeman [7] constructions, for the cases $k \in \{3, 4, 6, 10, 12\}$.

Let G_1 and G_2 be finite cyclic additive groups of prime order r and G_T be a finite cyclic multiplicative group of order r. A bilinear pairing is a map $e : G_1 \times G_2 \to G_T$ that satisfies the following properties:

1. (bilinear): $e(aP, bQ) = e(P, Q)^{ab}$, for all $P \in G_1$ and $Q \in G_2$ and for all $a, b, \in \mathbb{Z}_r$
2. (non-degenerate): there exists $P \in G_1$ and $Q \in G_2$ such that $e(P, Q) \neq 1$
3. (computable): e can be efficiently computed.

The traditional cryptographic pairings are the Weil and the Tate pairings. In terms of efficiency it is generally accepted that the Tate pairing is superior to the Weil pairing. The algorithm for the calculation of the Tate pairing requires a Miller loop, followed by a final exponentiation. Recently more efficient variants of the Tate pairing have been proposed like the Ate pairing [10], culminating in the recent discovery of the R-ate pairing [11], [9], [18]. These variants achieve their greater efficiency by requiring a much shorter (and thus faster) Miller loop.

Pairings change the elliptic curve discrete logarithm problem (ECDLP) on elliptic curves over a prime field $E(\mathbb{F}_p)$ into the discrete logarithm problem in some extension field $\mathbb{F}_{p^k}$. As such, for the pairing-based cryptosystems to be secure, the ECDLP in $E(\mathbb{F}_p)$ and the DLP in the multiplicative group $\mathbb{F}^*_{p^k}$ must both be computationally infeasible [8]. The parameter k is called the *embedding degree*.

On a non-supersingular elliptic curve while one parameter of the pairing may be a point over the base field $E(\mathbb{F}_p)$, the best that can be done for the second parameter is that it be a point on a twisted curve over an extension field $E(\mathbb{F}_{p^{k/d}})$, where $d \mid k$ and $d = 2$ for the quadratic twist is always possible for even k. The use of even k also enables the useful denominator elimination optimisation for the calculation of the pairing [2], and so this is generally regarded as a good idea. Note that for the optimal R-ate pairing, G_1 must be the group represented in the larger extension field.

The paper is organised as follows: In Section 2 we discuss pairing-friendly elliptic curves. The main contribution of this paper is presented in Sections 3 and 4 where we describe our method and where we give examples of the application of the new method to construct pairing-friendly elliptic curves with various embedding degrees k. We demonstrate the utility of the method by constructing new "record-breaking" families of pairing-friendly elliptic curves of embedding degrees 16, 18, 36 and 40.

2 Pairing-Friendly Elliptic Curves

The *embedding degree* in our context is defined as follows [7].

Definition 1. *Let E be an elliptic curve defined over a prime finite field $\mathbb{F}_p$. Let r be a prime dividing $\#E(\mathbb{F}_p)$. The embedding degree of E with respect to r is the smallest positive integer k such that $r \mid p^k - 1$.*

The definition explains that k is the smallest positive integer such that the extension field $\mathbb{F}_{p^k}$, contains a set of rth roots of unity. The problem is: given k, find a prime p and elliptic curve E, defined over the finite field $\mathbb{F}_p$, such that $\#E(\mathbb{F}_p)$ has a large prime factor r and the curve has embedding degree k with respect to r [7]. In pairing-based cryptography, when curves have small embedding degrees and a large prime-order subgroup they are known as *pairing-friendly elliptic curves*.

The number of points on an elliptic curve, E, is given by $\#E = p+1-t$, where t is the trace of the Frobenius; then by a simple substitution [2] the condition $r|p^k - 1$ is equivalent to

$$(t-1)^k \equiv 1 \bmod r,$$

so $t - 1$ is a k-th root of unity modulo r. Note that it is not sufficient just to find values of r, p and t which satisfy these conditions but it is also necessary to be able to construct the associated elliptic curve. The only known method for doing this is the method of Complex Multiplication (CM). The CM method requires that $4p - t^2$ should be of the form Dy^2, where for practical reasons the discriminant D must be less than about 10^{10}. This is a very restrictive condition, and so pairing-friendly elliptic curves are not so easy to find.

Let us set down some definitions.

Definition 2. *Let $g(x)$ be a polynomial with rational coefficients. Then $g(x)$ represents integers if there exists $x_0 \in \mathbb{Z}$ such that $g(x_0)$ is an integer.*

Definition 3. *Let $g(x)$ be a polynomial of even degree with rational coefficients. Then $g(x)$ represents primes if:*

1. *it is a non-constant irreducible polynomial with a positive leading coefficient*
2. *it represents integers*
3. *there exists $x_1 \in \mathbb{Z}$ and $x_2 \in \mathbb{Z}$, for which $g(x)$ represents integers, such that gcd $(g(x_1), g(x_2)) = 1$.*

Note that if $n \cdot g(x) \in \mathbb{Z}[x]$ then we can verify the second condition by testing n consecutive integer values of x. In addition, if ℓ is a prime greater than the degree of $g(x)$, then we can test the third condition by testing ℓ consecutive integer values of x.

The following definition of pairing-friendly elliptic curves is an adaptation from [8]:

Definition 4. *Let $t(x)$, $r(x)$, and $p(x)$ be polynomials with rational coefficients. For a given positive integer k and square free integer D, the triple $(t(x), r(x), p(x))$ represents a family of elliptic curves with embedding degree k and CM discriminant D if the following conditions are satisfied:*

a. $p(x)$ *represents primes.*
b. $r(x)$ *represents primes.*
c. $t(x)$ *represents integers.*
d. $r(x)$ *divides* $p(x) + 1 - t(x)$.
e. $r(x)$ *divides* $\Phi_k(t(x) - 1)$, *where* Φ_k *is the* k*th cyclotomic polynomial.*
f. $Dy(x)^2 = 4p(x) - t(x)^2$ *has infinitely many integer solutions in* x.

Here the ρ-value for a family of curves is defined as follows:

Definition 5. *Let* $t(x), r(x), p(x) \in \mathbb{Q}[x]$, *and suppose* (t, r, p) *represents a family of elliptic curves with embedding degree* k. *The* ρ*-value of the family represented by* (t, r, p) *is given by* $\rho = lim_{x\to\infty} \frac{\log(p(x))}{\log(r(x))} = \frac{\deg(p(x))}{\deg(r(x))}$.

Note that the value of $p(x)$ is the size of the field while the value of $r(x)$ is the size of the group in which we wish to do our cryptography.

The algorithm for the Brezing-Weng construction is summarised in the following algorithm[8]:

Algorithm 2.4. For a fixed positive integer k and 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 $\frac{\zeta_k - 1}{\sqrt{-D}} \in K$.
5. Let $p(x) \in \mathbb{Q}[x]$ be given by $(t(x)^2 + Dy(x)^2)/4$. If $p(x)$ and $r(x)$ represent primes, then the triple $(t(x), r(x), p(x))$ represents a family of curves with embedding degree k and discriminant D.

Pairing-friendly elliptic curves constructed using this method usually have their ρ-values less than 2 and closer to 1.

The challenging part in the Brezing-Weng construction is finding the polynomial $r(x)$ satisfying the following conditions, the *existence* conditions:

1. $\tilde{r}(x) = e \cdot r(x)$, where $r(x)$ represents primes and $e \in \mathbb{N}$ is a constant
2. $K \cong \mathbb{Q}[x]/\tilde{r}(x)$ contains ζ_k and $\sqrt{-D}$
3. $p(x)$ represents primes and
4. $t(x)$ represents integers.

In many cases the Brezing and Weng method results in curves with discriminant $D = 1$ or $D = 3$. Curves with these discriminants are not only easier to find using the CM method (as clearly D is very small), they also permit very efficient implementations, particularly of the R-ate pairing. For the case $D = 1$ the elliptic curve supports quartic twists ($d = 4$) if $4 \mid k$, and for the case $D = 3$ the curve supports cubic ($d = 3$) and sextic ($d = 6$) twists for $3 \mid k$ and $6 \mid k$ respectively. For example for the R-ate pairing, where $D = 3$ and $k = 12$ [1], it is possible to implement the group G_2 as points on $E(\mathbb{F}_p)$ over the base field and G_1 as points over the sextic twist, that is as points on $E'(\mathbb{F}_{p^{k/6}}) = E'(\mathbb{F}_{p^2})$.

3 The New Construction

We start by making a general, if rather obvious, point about working with polynomials with respect to an irreducible polynomial, rather than with integers with respect to a prime modulus. A power of a field element with respect to a prime modulus, will typically be a number the same size in bits as the modulus. However when working modulo an irreducible polynomial, the power of a field element will be a polynomial of degree *at least one less* than that of the irreducible polynomial. With some extra "luck" it may even be much less than this. Indeed it is exactly this kind of luck which results in Brezing and Weng curves often having a ρ value much less than 2, and closer to 1, (unlike the Cocks-Pinch method). This can also be exploited to reduce the workload of the pairing's final exponentiation [6].

In our construction we use a polynomial other than the cyclotomic polynomial $\Phi_l(x)$ to define the cyclotomic field $\mathbb{Q}(\zeta_l)$. In this construction we look for an element γ of the cyclotomic field $\mathbb{Q}(\zeta_l)$, where l is some multiple of the embedding degree k. Through experiments, we found that choosing γ to be a linear combination of a power basis $\{\zeta_l^i \mid 0 \leq i < \phi(l)\}$ with small integer coefficients, often led to success. So let L be a bound on the absolute size of the integer coefficients and allow a maximum of M non-zero coefficients. If γ is in $\mathbb{Q}(\zeta_l)$ but not in any proper subfield then we find the minimal polynomial of γ in $\mathbb{Q}(\zeta_l)$ which we set as $\tilde{r}(x)$. Otherwise γ gives a minimal polynomial whose degree is less than $\phi(l)$. If $D = 3$, we set $l = \text{lcm}(3, k)$; and if $D = 1$ we set $l = \text{lcm}(4, k)$. Then we proceed by using the Brezing-Weng construction to look for pairing-friendly elliptic curves, with predefined k and D, as follows:

3.1 Outline of Our Algorithm

Search through elements $\sum_{j=0}^{\phi(l)-1} m_i \zeta_l^j$ of $\mathbb{Q}(\zeta_l)$ where $m_i \in [-L, L]$. For each element, $\gamma \in \mathbb{Q}(\zeta_l)$ but not in any proper subfield of $\mathbb{Q}(\zeta_l)$ compute the minimal polynomial of γ and call it $\tilde{r}(x)$. Then for each primitive kth root of unity, ζ_k do:

1. Compute the polynomial $z(x)$ modulo $\tilde{r}(x)$ mapping to ζ_k.
2. Find $t(x) = z(x) + 1$, which maps to $\zeta_k + 1$ in $\mathbb{Q}[x]/\tilde{r}(x)$.
3. Using the algebraic relationship between ζ_k and $\sqrt{-D}$, find a polynomial $s(x)$ representing $\sqrt{-D}$ in $\mathbb{Q}[x]/\tilde{r}(x)$.
4. Compute the polynomial $y(x) = (t(x) - 2)s(x)/(-D)$.
5. Compute the polynomial $p(x) = (t(x)^2 + Dy(x)^2)/4$, and compute ρ. If $p(x)$ represents primes and the ρ-value is better than the best known, then
   (a) Find the smallest positive number $n \in \mathbb{Z}$, such that $n \cdot p(x) \in \mathbb{Z}[x]$.
   (b) Find the residue classes b modulo n such that $p(x) \in \mathbb{Z}$ for $x \equiv b \bmod n$.
   (c) Find the subset of those residue classes for which $t(x) \in \mathbb{Z}$ for $x \equiv b \bmod n$.
   If $\tilde{r}(nx + b) = e \cdot r(x)$ where e is a constant in $\mathbb{N}$ and $r(x)$ represents primes, then output $t(x), \tilde{r}(x), p(x), n, b, e$.

Thus for a given value of $k, (t(nx+b), \tilde{r}(nx+b)/e, p(nx+b))$ represents a family of pairing-friendly elliptic curves. The ρ-value for such a family of curves is then $\rho = \frac{\deg\, p(x)}{\deg\, r(x)}$. The elliptic curves found using this algorithm are pairing friendly by construction, and have an embedding degree of k.

3.2 Searching for New Families of Pairing-Friendly Curves

This algorithm is potentially very time consuming. Our approach is to restrict the search to integer coefficients with a limit L on their absolute size. We observe that smaller coefficients are more likely to lead to usable solutions. But even so the search space can quickly become huge for larger values of l. Therefore we have taken two approaches. The first performs an exhaustive search through all coefficients between $-L$ and $+L$. If this is not practical, the second approach is to limit the number of non-zero coefficients M to perhaps 2, 3 or 4. By trial and error we found that elements of $\mathbb{Q}(\zeta_l)$ of this form often produced good results. The search programs are written in a mixture of NTL [14] and PARI [15]. For comparision purposes a simple NTL program to generate Brezing and Weng families of pairing friendly curves can be found at Mike Scott's website [16].

4 Examples

The following examples demonstrate the construction of new families of pairing-friendly elliptic curves. Most of our examples also improve the existing ρ-values found in the literature. It is easy to verify that $(t(nx+b), \tilde{r}(nx+b)/e, p(nx+b))$ for a particular embedding degree, satisfy the conditions given in Definition 4.

Example 4.1. We start however with the case $k = 8$, where we set no records in terms of ρ, but nevertheless find some interesting new families of pairing friendly curves. For this embedding degree there is a known Brezing and Weng family of curves for $D = 3$ and $l = 24$ [4].

$$\begin{aligned} k &= 8,\ D = 3 \\ t(x) &= x^5 - x + 1 \\ p(x) &= (x^{10} + x^9 + x^8 - x^6 + 2x^5 - x^4 + x^2 - \ 32x + 1)/3 \\ r(x) &= x^8 - x^4 + 1 \\ \rho &= 5/4. \end{aligned}$$

Such a pairing suffers from the fact that we cannot use a higher order twist for G_1, which must therefore be represented by points on $E(\mathbb{F}_{p^4})$.

However for a family of curves with $k = 8$ and $D = 1$ the quartic twist for G_1 would be possible. Using our proposed method for $K \cong \mathbb{Q}(\zeta_8)$ we search through the range in which $m_i \in [-2, 2]$ and $M = 2$. We find that $\zeta_8 - 2\zeta_8^3 \in \mathbb{Q}(\zeta_8)$ has minimal polynomial $\tilde{r}(x) = x^4 - 8x^2 + 25$.

In this field we find that $(2x^3 - 11x)/15$ is a primitive 8^{th} root of unity. So we let $t(x) = (2x^3 - 11x + 15)/15$. With this we get $y(x) = (x^3 + 5x^2 + 2x - 20)/15$

and $p(x) = (x^6+2x^5-3x^4+8x^3-15x^2-82x+125)/180$. When $x \equiv \pm 5 \bmod 30$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)/450$ represent primes. So both of $(t(30x \pm 5), \tilde{r}(30x \pm 5)/450, p(30x \pm 5))$ represent a family of curves with embedding degree 8. In both cases we have

$$\begin{aligned} k &= 8,\ D = 1 \\ t(x) &= (2x^3 - 11x + 15)/15 \\ p(x) &= (x^6 + 2x^5 - 3x^4 + 8x^3 - 15x^2 - 82x + 125)/180 \\ \tilde{r}(x) &= x^4 - 8x^2 + 25 \\ n &= 30,\ b = \pm 5,\ e = 450 \\ \rho &= 3/2. \end{aligned}$$

Here the ρ value is inferior to the previous case, but G_1 can now be represented by points over the smaller extension field $\mathbb{F}_{p^2}$. However this construction does not set any new records as similar families of curves are already reported in [8] Example 6.18, and in [17] and [12].

Interestingly our method finds the BN family of pairing friendly curves [1].

Example 4.2. Fix the embedding degree $k = 12$ and $D = 3$ and set $K \cong \mathbb{Q}(\zeta_{12})$. Searching through $m_i \in [-2, 2]$ and setting $M = 4$, we find $\zeta_{12}^3 - \zeta_{12}^2 + \zeta_{12} + 2 \in \mathbb{Q}(\zeta_{12})$ which has minimal polynomial $\tilde{r}(x) = x^4 - 6x^3 + 18x^2 - 36x + 36$. When $x \equiv 0 \bmod 6$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)/36$ represent primes. So $(t(6x), \tilde{r}(6x)/36, p(6x))$ represent a family of curves with embedding degree 12. In this case we have

$$\begin{aligned} k &= 12,\ D = 3 \\ t(x) &= (x^2 + 6)/6 \\ p(x) &= (x^4 - 6x^3 + 24x^2 - 36x + 36)/36 \\ \tilde{r}(x) &= x^4 - 6x^3 + 18x^2 - 36x + 36 \\ n &= 6,\ b = 0,\ e = 36 \\ \rho &= 1. \end{aligned}$$

Example 4.3. Fix the embedding degree $k = 16$ and $D = 1$ and set $K \cong \mathbb{Q}(\zeta_{16})$. Searching through $m_i \in [-2, 2]$ and $M = 2$, we find $-2\zeta_{16}^5 + \zeta_{16} \in \mathbb{Q}(\zeta_{16})$ which has minimal polynomial $\tilde{r}(x) = x^8 + 48x^4 + 625$. When $x \equiv \pm 25 \bmod 70$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)/61250$ represent primes. So both of $(t(70x \pm 25), \tilde{r}(70x \pm 25)/61250, p(70x \pm 25))$ represent a family of curves with embedding degree 16. In both cases we have

$$\begin{aligned} k &= 16,\ D = 1 \\ t(x) &= (2x^5 + 41x + 35)/35 \\ p(x) &= (x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125)/980 \\ \tilde{r}(x) &= x^8 + 48x^4 + 625 \\ n &= 70,\ b = \pm 25,\ e = 61250 \\ \rho &= 5/4. \end{aligned}$$

This is an improvement over the old record value of $\rho = 11/8$.

Example 4.4. Fix the embedding degree $k = 18$ and $D = 3$ and set $K \cong \mathbb{Q}(\zeta_{18})$. With $m_i \in [-3, 3]$ and $M = 2$ we find $-3\zeta_{18}^5 + \zeta_{18}^2 \in \mathbb{Q}(\zeta_{18})$ has minimal polynomial $\tilde{r}(x) = x^6+37x^3+343$. When $x \equiv 14 \bmod 42$, $t(x)$ represents integers, $p(x)$ and $r(x)/343$ represent primes. So $(t(42x+14), \tilde{r}(42x+14)/343, p(42x+14))$ represents a family of curves with embedding degree 18. We have

$$\begin{aligned} k &= 18,\ D = 3 \\ t(x) &= (x^4 + 16x + 7)/7 \\ p(x) &= (x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401)/21 \\ \tilde{r}(x) &= x^6 + 37x^3 + 343 \\ n &= 42,\ b = 14,\ e = 343 \\ \rho &= 4/3. \end{aligned}$$

This is a significant improvement in ρ over the old record value of $19/12$.

Until now there has not been a good choice of pairing-friendly families of curves which are a good fit for the AES-256 level of security, for larger values of k.

Example 4.5. For the embedding degree $k = 32$, there is a Brezing and Weng family of curves with $\rho = 17/16$, but with $D = 3$, which is the "wrong" discriminant $(3 \nmid k)$ for a simpler form of G_1 [8]. Here we suggest an alternative.

Fix embedding degree $k = 32$ and $D = 1$ and set $K \cong \mathbb{Q}(\zeta_{32})$. Searching through $m_i \in [-3, 3]$ and $M = 2$, we find $-3\zeta_{32} + 2\zeta_{32}^9 \in \mathbb{Q}(\zeta_{32})$ has minimal polynomial $\tilde{r}(x) = x^{16} + 57120x^8 + 815730721$. When $x \equiv \pm 325 \bmod 6214$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)/93190709028482$ represent primes. So both of $(t(6214x \pm 325), \tilde{r}(6214x \pm 325)/93190709028482, p(6214x \pm 325))$ represent a family of curves with embedding degree 32. In both cases we have

$$\begin{aligned} k &= 32,\ D = 1 \\ t(x) &= (-2x^9 - 56403x + 3107)/3107 \\ p(x) &= (x^{18} - 6x^{17} + 13x^{16} + 57120x^{10} - 344632x^9 + 742560x^8 + 815730721x^2 \\ &\quad - 4948305594x + 10604499373)/2970292 \\ \tilde{r}(x) &= x^{16} + 57120x^8 + 815730721 \\ n &= 6214,\ b = \pm 325,\ e = 93190709028482 \\ \rho &= 9/8. \end{aligned}$$

Example 4.6. Fix the embedding degree $k = 36$ and $D = 3$ and set $K \cong \mathbb{Q}(\zeta_{36})$. Searching through $m_i \in [-2, 2]$ with $M = 2$, we find $2\zeta_{36} + \zeta_{36}^7 \in \mathbb{Q}(\zeta_{36})$ has minimal polynomial $\tilde{r}(x) = x^{12} + 683x^6 + 117649$. When for example $x \equiv 287 \bmod 777$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)/161061481$ represent primes.(There are other classes mod 777 that work.) So $(t(777x+287), \tilde{r}(777x+287)/161061481, p(777x + 287))$ represents a family of curves with embedding degree 36. In both cases we have

$$\begin{aligned} k &= 36,\ D = 3 \\ t(x) &= (2x^7 + 757x + 259)/259 \end{aligned}$$

$$\begin{aligned}
p(x) &= (x^{14} - 4x^{13} + 7x^{12} + 683x^8 - 2510x^7 \\
&\quad + 4781x^6 + 117649x^2 - 386569x + 823543)/28749 \\
\tilde{r}(x) &= x^{12} + 683x^6 + 117649 \\
n &= 777,\ b = 287,\ e = 161061481 \\
\rho &= 7/6.
\end{aligned}$$

Again this is an improvement in ρ over the old record value of 17/12.

Example 4.7 Fix the embedding degree $k = 40$ and $D = 1$ and set $K \cong \mathbb{Q}(\zeta_{40})$. Consider $-2\zeta_{40} + \zeta_{40}^{11} \in \mathbb{Q}(\zeta_{40})$. This element has minimal polynomial $\tilde{r}(x) = x^{16} + 8x^{14} + 39x^{12} + 112x^{10} - 79x^8 + 2800x^6 + 24375x^4 + 125000x^2 + 390625$. When for example $x \equiv \pm 1205 \bmod 2370$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)/2437890625$ represent primes. (There are other classes mod 2370 that work.) So both of $(t(2370x \pm 1205), \tilde{r}(2370x \pm 1205)/2437890625, p(2370x \pm 1205))$ represent a family of curves with embedding degree 40. In both cases we have

$$\begin{aligned}
k &= 40,\ D = 1 \\
t(x) &= (2x^{11} + 6469x + 1185)/1185 \\
p(x) &= (x^{22} - 2x^{21} + 5x^{20} + 6232x^{12} - 10568x^{11} + 31160x^{10} \\
&\quad + 9765625x^2 - 13398638x + 48828125)/1123380 \\
\tilde{r}(x) &= x^{16} + 8x^{14} + 39x^{12} + 112x^{10} - 79x^8 \\
&\quad + 2800x^6 + 24375x^4 + 125000x^2 + 390625 \\
n &= 2370,\ b = \pm 1205,\ e = 2437890625 \\
\rho &= 11/8.
\end{aligned}$$

Again this is an improvement in ρ over the old record value of 23/16.

5 Conclusion

We have presented a new method of constructing pairing-friendly elliptic curves. Basically the construction extends ideas from the Brezing-Weng method. The main idea in the construction is to use minimal polynomials of the elements of the cyclotomic field other than the cyclotomic polynomial $\Phi_l(x)$ to define the cyclotomic field $\mathbb{Q}(\zeta_l)$. The potential of the method has been illustrated by constructing new families of pairing-friendly elliptic curves of degrees 8, 16, 18, 32, 36 and 40. In most of these cases the method improves the previously best known ρ-values. Interestingly our method also rediscovers the BN family of "ideal" $\rho = 1$ curves. This holds out the hope that by extending the search space, further families of ideal pairing friendly curves might be found.

Acknowledgement

Thanks are due to Michael Naehrig and David Freeman for useful comments on an early draft of this paper.

References

1. Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer, Heidelberg (2006)
2. Barreto, P.S.L.M., Lynn, B., Kim, H., Scott, M.: Efficient Algorithms for Pairing-Based Cryptosystems. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 354–368. Springer, Heidelberg (2002)
3. Barreto, P.S.L.M., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degree. In: Cimato, S., Galdi, C., Persiano, G. (eds.) SCN 2002. LNCS, vol. 2576, pp. 263–273. Springer, Heidelberg (2002)
4. Brezing, F., Weng, A.: Elliptic curves suitable for pairing based cryptography. Designs Codes and Cryptography 37(1), 133–141 (2005)
5. Cocks, C., Pinch, R.G.E.: Identity-based cryptosystems based on the Weil pairing (unpublished manuscript, 2001)
6. Devegili, A.J., Scott, M., Dahab, R.: Implementing Cryptographic Pairings over Barreto-Naehrig Curves. Cryptography ePrint Archive, Report 2007/390 (2007), http://eprint.iacr.org/2007/390
7. Freeman, D.: Constructing pairing-friendly elliptic curves with embedding Degree 10. In: Hess, F., Pauli, S., Pohst, M. (eds.) ANTS-VII 2006. LNCS, vol. 4076, pp. 452–465. Springer, Heidelberg (2006)
8. Freeman, D., Scott, M., Teske, E.: A Taxonomy of pairing-friendly elliptic curves. Cryptography ePrint Archive, Report 2006/372 (2006), http://eprint.iacr.org/2006/372
9. Hess, F.: Pairing Lattices. Cryptography ePrint Archive, Report 2008/125 (2008), http://eprint.iacr.org/2008/125
10. Hess, F., Smart, N., Vercauteren, F.: The Eta Pairing revisited. IEEE Trans. Information Theory 52, 4595–4602 (2006)
11. Lee, E., Lee, H.S., Park, C.M.: Efficient and Generalized Pairing Computation on Abelian Varieties. Cryptography ePrint Archive, Report 2008/040 (2008), http://eprint.iacr.org/2008/040
12. Matsuda, S., Kanayama, N., Hess, F., Okamoto, E.: Optimised versions of the Ate and Twisted Ate Pairings. Cryptology ePrint Archive, Report 2007/013 (2007), http://eprint.iacr.org/2007/013
13. Miyaji, A., Nakabayashi, M., Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fundamentals E84, 1234–1243 (2001)
14. Shoup, V.: A Library for doing Number Theory (2006), http://www.shoup.net/ntl/
15. PARI-GP, version 2.3.2, Bordeaux (2006), http://pari.math.u-bordeaux.fr/
16. Scott, M.: An NTL program to find Brezing and Weng curves (2007), http://ftp.computing.dcu.ie/pub/crypto/bandw.cpp
17. Tanaka, S., Nakamula, K.: More constructing pairing-friendly elliptic curves for cryptography. Mathematics arXiv Archive, Report 0711.1942 (2007), http://arxiv.org/abs/0711.1942
18. Vercauteren, F.: Optimal Pairings. Cryptography ePrint Archive, Report 2008/096 (2008), http://eprint.iacr.org/2008/096