Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field

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

[1] School of Computing
Dublin City University
Ireland
[2] Department of Mathematics and Computer Science
Santa Clara University
USA

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

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 while cryptosystems such as short digital signatures, identity-based encryption and one-round three-way key exchange, require 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.
Let G_1 and G_2 be finite cyclic additive groups of prime order r and G_3 be a finite cyclic multiplicative group of prime order r. A bilinear pairing is a map $e : G_1 \text{ x } G_2 \rightarrow G_3$ 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.*

⋆ ekachisa@computing.dcu.ie
⋆⋆ eschaefer@scu.edu
⋆⋆⋆ mike@computing.dcu.ie

The traditional cryptographic pairings are the Weil and the Tate pairings, although recently the η (aka the *twisted Ate* [14]) and Ate pairings have become popular. 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. The η and Ate pairings are more efficient variants of the Tate pairing, which often require only a reduced number of iterations of the Miller loop.
These 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 $E(\mathbb{F}_p)$ of $\mathbb{F}_p$ rational points on E and the DLP in the multiplicative group $\mathbb{F}_{p^k}^*$ must both be hard [10]. The parameter k is called the *embedding degree*.
On a non-supersingular elliptic curve while G_1 may be generated by a point over the base field $E(\mathbb{F}_p)$, points in G_2 may be represented as points 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 [3], and so this is generally regarded as a good idea.

1.1 Organisation of the paper

The paper is organized as follows: In Section 2 we describe some of the constructions in the literature. 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 formally defined as follows [9].

Definition 2.1 *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 $\#E(\mathbb{F}_q)$ has a large prime factor r and the curve has embedding degree k with respect to r [9]. In pairing based cryptography, when curves have small embedding degrees and a large prime order subgroup they are known as *pairing friendly elliptic curves*.

Since $\#E = p + 1 - t$, where t is the trace of the Frobenius, then by a simple substitution [3] this condition 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: 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.

We observe here that whereas the calculation of the Tate pairing requires about $\lg(r-1)$ iterations of the Miller loop using a double-and-add algorithm [8], the Ate pairing requires only $\lg(t-1)$ iterations, and t is commonly much smaller than r as a consequence of the Hasse condition ($t \leq 2\sqrt{p}$). In fact using the generalised Ate pairing [24] it is possible to use a loop with only $\lg((t-1)^c \bmod r)$ iterations for some $0 < c < k$, although on the face of it this might not appear advantageous (but see below). Note that the Ate pairing requires a "reversal of roles" for G_1 and G_2 in the pairing algorithm, with some loss of efficiency. The η pairing does not require this reversal, but requires $\lg((t-1)^{c.(k/d)} \bmod r)$ iterations for the Miller loop, but again on the face of it this is not of much use, certainly for the quadratic twist, as $(t-1)^{k/2} = r - 1 \bmod r$ which is no improvement on the Tate pairing. But again – see below.

Some of the proposed strategies for constructing pairing-friendly elliptic curves are as follows. Miyaji, Nakabayashi and Takano [17] developed the MNT curves. They were also the first to describe a procedure for generating ordinary elliptic curves of low embedding degree. The method used to construct MNT curves was limited to curves of prime order, and to embedding degree $k \leq 6$. Also the curves tended to have a large discriminant D.

Cocks and Pinch [6] presented their general method of constructing curves of arbitrary embedding degree k. In their construction they fixed an embedding degree k, a subgroup size r, and a complex multiplication discriminant D to determine a prime p such that there exists a pairing-friendly elliptic curve E over a finite field. They were able to construct elliptic curves with an arbitrary embedding degree.

Barreto, Lynn and Scott [4] described a simple algrebraic construction for certain pairing friendly families of elliptic curves with low discriminant, for example $D = 3$. These families describe r, p and t as simple polynomials $r(x)$, $p(x)$ and $t(x)$ with integer coefficients. This idea was generalized and extended by the work of Brezing and Weng [5].

Barreto and Naehrig [2], building on earlier work by Galbraith, McKee and Valenca [12], presented a method of constructing elliptic curves of prime order and embedding degree $k = 12$ and $D = 3$. The construction lead to a very efficient implementation of such curves [8].

In addition Freeman [9], presented a general method of constructing families of elliptic curves with prescribed embedding degree and prime order. The method was demonstrated by constructing curves of embedding degree 10.
Of particular interest to our discussion is the strategy of constructing complete cyclotomic families as proposed by Brezing and Weng [5]. This construction basically uses the Cocks and Pinch idea with polynomials.
The interesting point in the Brezing-Weng method is that it reduces the ratio between the bit lengths of the finite field and the order r of the subgroup with embedding 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 curves with small ρ-values are desirable in speeding up the arithmetic on the curves in the underlying field. We would much prefer $\rho \sim 1$, which is already achieved by the MNT, BN and Freeman constructions, for the cases $k \in \{3, 4, 6, 10, 12\}$.
Brezing and Weng define polynomials to represent the parameters p, t, and r. The following definition of pairing-friendly elliptic curves is an adaptation from [10]:

Definition 2.2 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 discriminant D if the following conditions are satisfied:
a. $p(x)$ represents primes.
b. $r(x) = e \cdot \tilde{r}(x)$, where $\tilde{r}(x)$ represents primes and $e \in \mathbb{N}$ is a constant. This was first pointed out in [11].
c. $r(x)$ divides $p(x) + 1 - t(x)$.
d. $r(x)$ divides $\Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial.
e. the equation $Dy(x)^2 = 4p(x) - t(x)^2$ has infinitely many integer solutions in x.

In point (b) we note that it is not necessary that $r(x)$ represent primes as long as $r(x) = e \cdot \tilde{r}(x)$, where $\tilde{r}(x)$ represents primes. A polynomial $g(x)$ of even degree with rational coefficients *represents primes* if $g(x)$

1. is a non-constant polynomial
2. has a positive leading coefficient
3. represents an integer value for some $x \in \mathbb{Z}$ and
4. for some $x_1 \in \mathbb{Z}$ and $x_2 \in \mathbb{Z}$, we have gcd $(g(x_1), g(x_2)) = 1$.
5. is an irreducible polynomial

Furthermore, part (c) of Definition 2.2 ensures that, if $p(x)$ is prime for some value of x, then $r(x) | \#E(\mathbb{F}_{p(x)})$. If $r(x) = p(x) + 1 - t(x)$, for the values of x for which $p(x)$ and $r(x)$ are both prime, then $\#E(\mathbb{F}_p)$ is also prime [10]. The ρ-value for a family of curves is defined as follows [10]:

Definition 2.3 *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 theorem [10]:

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.

The ρ-value for this family is given by the following

$$\rho = \frac{\deg\ p(x)}{\deg\ r(x)}.$$

Pairing-friendly elliptic curves constructed using this method have their ρ-values less than 2. In the ideal situation ρ has a value of 1. It is useful then, to find curves with small ρ-value for various embedding degrees k because different embedding degrees are useful for different applications [10].
The challenging part in the Brezing-Weng construction is finding the polynomial $r(x)$ satisfying the following conditions, the *existence* conditions:

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

In all previous examples, $r(x)$ has been chosen to be a cyclotomic polynomial. 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 η and Ate pairings. 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 where $D = 3$ and $k = 12$ [2], it is possible to implement the group G_1 as points on $E(\mathbb{F}_p)$ over the base field and G_2 as points over the sextic twist, that is as points on $E(\mathbb{F}_p^{k/6}) = E(\mathbb{F}_p^2)$.

The Miller loop control polynomial $m(x)$ is selected as follows [24], [18]:

1. Tate pairing: $m_r(x) = r(x) - 1$

2. Generalised Ate pairing: $m_A(x) = (t(x) - 1)^c \bmod r(x)$
3. Generalised η pairing: $m_\eta(x) = (t(x) - 1)^{c.(k/d)} \bmod r(x)$

For the generalised Ate and η pairings c is chosen so that $m(x)$ is the polynomial of least degree. Note that the η pairing is only a contender when higher order twists are possible, with $d \in (3, 4, 6)$.
Before proceeding we make 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 [8]. And as Naehrig and Barreto [18] point out, it can also result in a shorter than expected Miller loop for both the Ate and η Pairing. To measure the degree of loop reduction possible with respect to the Tate pairing we introduce the parameter ω, where

$$\omega = \frac{\deg\ r(x)}{\deg\ m(x)}$$

3 The new construction

In the new construction we follow the strategy of Brezing and Weng. We fix the embedding degree k and a positive square free integer D. We also set our cyclotomic field to work in as $K \cong \mathbb{Q}(\zeta_l)$, where l is some multiple of the embedding degree k. If $D = 3$, we set $l = \text{lcm}(3, k)$; and if $D = 1$ we set $l = \text{lcm}(4, k)$. Then the following algorithm is followed to look for the families of curves.

Algorithm 3.1

1. Search through elements of $\mathbb{Q}(\zeta_l)$ which are an integer linear combination of a power basis $\{\zeta_l^i \mid 0 \leq i \leq \phi(l) - 1\}$.
2. For each such element, find the minimal polynomial of that element and call it $r(x)$.
3. Search through all primitive kth roots of unity mod $r(x)$.
4. For each primitive kth root of unity ζ_k, find $t(x)$ mapping to $\zeta_k + 1$.
5. Find a polynomial mapping to $\sqrt{-D}$.
6. Find a polynomial $y(x)$ mapping to $\frac{\zeta_k - 1}{\sqrt{-D}}$.
7. Compute ρ. If the ρ-value is sufficiently small then
8. Find $p(x) = (t(x)^2 + Dy(x)^2)/4$.
9. If $p(x)$ is irreducible then
10. Find the best Miller loop polynomial $m(x)$ for the Ate and η pairings (if applicable).

11. Find the smallest positive number $n \in \mathbb{Z}$, such that $n \cdot p(x) \in \mathbb{Z}[x]$.
12. Find the residue classes b modulo n such that $p(x) \in \mathbb{Z}$ for $x \equiv b \bmod n$.
13. Find the subset of those residue classes for which $t(x) \in \mathbb{Z}$ for $x \equiv b \bmod n$.
14. If $r(mx + b) = e\tilde{r}(x)$ where e is a constant and $\tilde{r}(x)$ represents primes, then output $t(x), \tilde{r}(x), p(x), m(x), n, b$.

Thus for a given value of k, $(t(x), \tilde{r}(x), p(x))$ represents a family of pairing-friendly elliptic curves of embedding degree k. The ρ-value for such a family of curves is then $\rho = \frac{\deg\ p(x)}{\deg\ r(x)}$, and $\omega = \frac{\deg\ r(x)}{\deg\ m(x)}$.

4 Searching for new families of pairing-friendly curves

This algorithm is potentially very time consuming, primarily due to step 1. 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 coefficents between $-L$ and $+L$. The second approach is to limit the number of non-zero coefficients, to perhaps 2 or 3. By trial and error we found that elements of $\mathbb{Q}(\zeta_l)$ of this form often produced good results.
Our search programs are written in a mixture of NTL [19] and PARI [20]. For comparision purposes a simple NTL program to generate Brezing and Weng families of pairing friendly curves can be found here [21].

4.1 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. We also compute the parameters for the optimal generalised η or Ate pairing in each case.

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 $l = 24$ [5].

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

Note that not only is $m_A(x)$ for the generalised Ate pairing much smaller than $r(x) - 1$, it is also much smaller than $t(x) - 1$, as would be used for the basic Ate pairing. This is an example of the kind of luck we referred to above – it turns out that $(t(x) - 1)^3 \bmod r(x) \equiv x^3$ which has a degree not only less than $r(x)$, but also less than $t(x)$.

Such a pairing suffers from the fact that we cannot use a higher order twist for G_2, 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_2 would be possible. Using our proposed method we have $l = 8$. Note that $\zeta_8 - 2\zeta_8^3 \in \mathbb{Q}(\zeta_8)$ has minimal polynomial $x^4 - 8x^2 + 25$.

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 $\tilde{r}(x)$ can represent primes. So $(t(x), \tilde{r}(x), p(x))$ represents a family of curves with embedding degree 8. In summary

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

A suitable substitution to meet the existence conditions is $x \leftarrow 5 + 30x$. Here the ρ and ω values are both inferior to the previous case. Observe that the η pairing is now as good as the Ate pairing, and so it is to be preferred as it is more convenient and efficient for implementation [15], and G_2 can 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 [10], example 6.18, and in [22] (although our ω value is an improvement on that reported in [1] and [15]) .

Example 4.2

Fix the embedding degree $k = 16$ and $D = 1$ and set $K \cong \mathbb{Q}(\zeta_{16})$. Now $-2\zeta_{16}^5 + \zeta_{16} \in \mathbb{Q}(\zeta_{16})$ has minimal polynomial $r(x) = x^8 + 48x^4 + 625$. When $x \equiv \pm 25 \bmod 70$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)$ can represent primes. So $(t(x), \tilde{r}(x), p(x))$ represents a family of curves with embedding degree 16.

$$
\begin{aligned}
k &= 16,\ D = 1 \\
t(x) &= (35 + 41x + 2x^5)/35 \\
p(x) &= (3125 + 2398x + 625x^2 + 240x^4 + 152x^5 + 48x^6 + 5x^8 + 2x^9 + x^{10})/980 \\
\tilde{r}(x) &= (625 + 48x^4 + x^8)/61250 \\
m_\eta(x) &= (24 + x^4)/7 \\
\rho &= 5/4,\ \omega = 2
\end{aligned}
$$

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

Example 4.3

Fix the embedding degree $k = 18$ and $D = 3$ and set $K \cong \mathbb{Q}(\zeta_{18})$. Consider $-3\zeta_{18}^5 + \zeta_{18}^2 \in \mathbb{Q}(\zeta_{18})$. This has minimal polynomial $r(x) = x^6 + 37x^3 + 343$. When $x \equiv 14 \bmod 42$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)$ can represent primes. So $(t(x), \tilde{r}(x), p(x))$ represents a family of curves with embedding degree 18.

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

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 family of curves which are a good fit for the AES-256 level of security, for larger values of k.

Example 4.4

For the embedding degree $k = 32$, there is a Brezing and Weng family of curves with $\rho = 17/16$ and $\omega = 32/3$ for the Ate pairing, but with $D = 3$, the "wrong" discriminant ($3 \nmid k$) for a simpler form of G_2 [10]. Here we suggest an alternative.

Fix embedding degree $k = 32$ and $D = 1$ and set $K \cong \mathbb{Q}(\zeta_{32})$. Consider $-3\zeta_{32} + 2\zeta_{32}^9 \in \mathbb{Q}(\zeta_{32})$. This has minimal polynomial $r(x) = x^{16} + 57120x^8 + 815730721$. When $x \equiv \pm 325 \bmod 6214$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)$ can represent primes. So $(t(x), \tilde{r}(x), p(x))$ represents a family of curves with embedding degree 32.

$$
\begin{aligned}
k &= 32,\ D = 1 \\
t(x) &= (3107 - 56403x - 2x^9)/3107 \\
p(x) &= (10604499373 - 4948305594x + 815730721x^2 + 742560x^8 - 344632x^9 \\
&\quad + 57120x^{10} + 13x^{16} - 6x^{17} + x^{18})/2970292 \\
\tilde{r}(x) &= (815730721 + 57120x^8 + x^{16})/93190709028482 \\
m_\eta(x) &= (28560 + x^8)/239 \\
\rho &= 9/8,\ \omega = 2
\end{aligned}
$$

Example 4.5

Fix the embedding degree $k = 36$ and $D = 3$ and set $K \cong \mathbb{Q}(\zeta_{36})$. Consider $2\zeta_{36} + \zeta_{36}^7 \in \mathbb{Q}(\zeta_{36})$. This has minimal polynomial $r(x) = x^{12} + 683x^6 + 117649$. When for example $x \equiv 287 \bmod 777$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)$ can represent primes. So $(t(x), \tilde{r}(x), p(x))$ represents a family of curves with embedding degree 36.

$$
\begin{aligned}
k &= 36,\ D = 3 \\
t(x) &= (259 + 757x + 2x^7)/259 \\
p(x) &= (823543 - 386569x + 117649x^2 + 4781x^6 \\
&\quad - 2510x^7 + 683x^8 + 7x^{12} - 4x^{13} + x^{14})/28749 \\
\tilde{r}(x) &= (117649 + 683x^6 + x^{12})/161061481 \\
m_\eta(x) &= (323 + x^6)/37 \\
\rho &= 7/6,\ \omega = 2
\end{aligned}
$$

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

Example 4.6

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 has minimal polynomial $r(x) = x^{16} + 8x^{14} + 39x^{12} + 112x^{10} - 79x^8 + 2800x^6 + 24375x^4 + 125000x^2 + 390625$. When for example $x \equiv \pm 1205 \bmod 2370$, $t(x)$ represents integers, $p(x)$ and $\tilde{r}(x)$ can represent primes. So $(t(x), \tilde{r}(x), p(x))$ represents a family of curves with embedding degree 40.

$$
\begin{aligned}
k &= 40,\ D = 1 \\
t(x) &= (1185 + 6469x + 2x^{11})/1185 \\
p(x) &= (48828125 - 13398638x + 9765625x^2 + 31160x^{10} - 10568x^{11} \\
&\quad + 6232x^{12} + 5x^{20} - 2x^{21} + x^{22})/1123380 \\
\tilde{r}(x) &= (390625 + 125000x^2 + 24375x^4 + 2800x^6 \\
&\quad - 79x^8 + 112x^{10} + 39x^{12} + 8x^{14} + x^{16})/2437890625 \\
m_\eta(x) &= (3116 + x^{10})/237 \\
\rho &= 11/8,\ \omega = 8/5
\end{aligned}
$$

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

5 Conclusion

We have presented a new algorithm to construct pairing-friendly elliptic curves by using ideas from the Brezing-Weng method. The main idea in the construction is to use a polynomial other than the cyclotomic polynomial $\Phi_l(x)$ to define the cyclotomic field $\mathbb{Q}(\zeta_l)$. The method uses elements of a cyclotomic field other than roots of unity to find an irreducible polynomial $r(x)$. This 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. As pointed out in [15] sometimes the η pairing is to be preferred over the Ate pairing [18]. This is also the case for our curves.

6 Acknowledgement

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

References

1. Antonio, C.A., Tanaka, S. and Nakamula, K., (2007) *Implementing Cryptographic Pairings over Curves of Embedding Degrees 8 and 10.* Cryptology ePrint Archive Report 2007/426, http://eprint.iacr.org/2007/426.
2. Barreto, P.S.L.M., and Naehrig M., (2006) *Pairing-friendly elliptic curves of prime order.* Selected Areas in Cryptography – SAC'2005, Lecture Notes in Computer Science 3897, pp 319–331 Springer-Verlag
3. Barreto P.S.L.M., Lynn, B., Kim H. and Scott, M. (2002) *Efficient Algorithms for Pairing-Based Cryptosystems.* Advances in Cryptology – Crypto'2002, Lecture Notes in Computer Science 2442, pp. 354-368, Springer-Verlag
4. Barreto P.S.L.M., Lynn, B. and Scott, M., (2002) *Constructing elliptic curves with prescribed embedding degree.* Security in Communication Networks -SCN 2002, Lecture Notes in Computer Science 2576, pp. 263–273, Springer-Verlag
5. Brezing F. and Weng A., (2005) *Elliptic curves suitable for pairing based cryptography.*, Designs Codes and Cryptography, Vol. 37, No. 1, pp. 133–141
6. Cocks, C. and Pinch, R. G. E., (2001) *Identity-based cryptosystems based on the Weil pairing.*, Unpublished manuscript.
7. Blake, I., Seroussi, G., and Smart, N., (1994) *Elliptic Curves in Cryptography.* London Mathematical Society, Cambridge: Cambridge University Press.
8. Devegili, A. J., Scott, M. and Dahab R., (2007) *Implementing Cryptographic Pairings over Barreto-Naehrig Curves.* Cryptography ePrint Archive, Report 2007/390, http://eprint.iacr.org/2007/390
9. Freeman, D., (2006) *Constructing pairing-friendly elliptic curves with embedding Degree 10.* In Algorithmic Number Theory Symposium ANTS-VII, Lecture Notes in Computer Science 4096, pp. 452–465. Springer-Verlag

10. Freeman, D., Scott, M. and Teske, E., (2006) *A Taxonomy of pairing-friendly elliptic curves*. Cryptography ePrint Archive, Report 2006/372, http://eprint.iacr.org/2006/372
11. Kachisa, E., (2007) *Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field*, M.Sc. dissertation, Mzuzu University, 2007.
12. Galbraith, S.D, McKee, J. and Valenca, P., (2004) *Ordinary abelian varieties having small embedding degree*. Cryptography ePrint Archive, Report 2004/365, http://eprint.iacr.org/2004/365.
13. Hankerson, D., Menezes, A. and Vanstone, S., (2004) *Guide to elliptic curve cryptography*. New York: Springer-Verlag.
14. Hess, F., Smart, N. and Vercauteren F., (2006) *The Eta Pairing revisited*. IEEE Trans. Information Theory, Vol. 52, pp. 45954602
15. Matsuda, S., Kanayama, N., Hess, F. and Okamoto, E., (2007) *Optimised versions of the Ate and Twisted Ate Pairings*. Cryptology ePrint Archive, Report 2007/013, http://eprint.iacr.org/2007/013
16. Menezes, A., (1993) *Elliptic Curve Public Cryptosystems*. Kluwer Academic Publishers,
17. Miyaji, A., Nakabayashi, M. and Takano, S., (2001) *New explicit conditions of elliptic curve traces for FR-reduction*. IEICE Trans. Fundamentals, E84 pp. 1234 - 1243.
18. Naehrig, M. and Barreto, P.S.L.M., (2007) *On compressible pairings and their computation*. Cryptology ePrint Archive, Report 2007/429, http://eprint.iacr.org/2007/429
19. Shoup, V., (2006) *A Library for doing Number Theory* `http://www.shoup.net/ntl/`.
20. *PARI-GP*, version `2.3.2`, Bordeaux, 2006, `http://pari.math.u-bordeaux.fr/`.
21. Scott M., (2007) *An NTL program to find Brezing and Weng curves* `http://ftp.computing.dcu.ie/pub/crypto/bandw.cpp`
22. Tanaka, S. and Nakamula, K., (2007) *More constructing pairing-friendly elliptic curves for cryptography*. Mathematics arXiv Archive, Report 0711.1942, http://arxiv.org/abs/0711.1942
23. Trappe, W. and Washington, L., (2002). *Introduction to cryptography with coding theory*. New Jersey: Prentice Hall.
24. Zhao, C-A., and Zhang, F. and Huang, J., (2007) *A Note on the Ate Pairing*. Cryptology ePrint Archive, Report 2007/247, http://eprint.iacr.org/2007/247