HAL
archives-ouvertes.fr

A New Family of Pairing-Friendly elliptic curves

Michael Scott, Aurore Guillevic

▶ To cite this version:

Michael Scott, Aurore Guillevic. A New Family of Pairing-Friendly elliptic curves. International Workshop on the Arithmetic of Finite Fields - WAIFI, Lilya Budaghyan and Tor Helleseth, Jun 2018, Bergen, Norway. pp.43-57, 10.1007/978-3-030-05153-2_2 . hal-01875361

HAL Id: hal-01875361
https://hal.inria.fr/hal-01875361

Submitted on 17 Sep 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A New Family of Pairing-Friendly elliptic curves *

Michael Scott[1] and Aurore Guillevic[2]

[1]MIRACL.com
[2]Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

September 17, 2018

Abstract

There have been recent advances in solving the finite extension field discrete logarithm problem as it arises in the context of pairing-friendly elliptic curves. This has lead to the abandonment of approaches based on supersingular curves of small characteristic, and to the reconsideration of the field sizes required for implementation based on non-supersingular curves of large characteristic. This has resulted in a revision of recommendations for suitable curves, particularly at a higher level of security. Indeed for a security level of 256 bits, the BLS48 curves have been suggested, and demonstrated to be superior to other candidates. These curves have an embedding degree of 48. The well known taxonomy of Freeman, Scott and Teske only considered curves with embedding degrees up to 50. Given some uncertainty around the constants that apply to the best discrete logarithm algorithm, it would seem to be prudent to push a little beyond 50. In this note we announce the discovery of a new family of pairing friendly elliptic curves which includes a new construction for a curve with an embedding degree of 54.

Keywords: Elliptic Curves, Pairing-based Cryptography, Aurifeuillean factorization

1 Introduction

One of great break-throughs in pairing-based cryptography was the discovery of the BN curves [3]. A group size of 256 bits (to match the 128-bit security level) can be supported by an elliptic curve over a field also of 256 bits, and since the embedding degree is 12, the size of the discrete logarithm

*This document is a preprint author's version. Conference version (June 2018) available at `http://www.waifi.org/documents/AcceptedPapers2018/T1-WAIFI_2018_paper_7.pdf`

(DL) problem over the extension field is 3072 bits. Which was a serendipitous direct hit on the size of DL problem believed to correspond to 128-bit security level. The fit was perfect.

Recall that protocols based on bilinear pairings typically consist of operations on three groups, denoted as $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$, and the calculation of the pairing itself, usually denoted as $w = e(P, Q)$, where the pairing takes two elliptic curve point parameters $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$ respectively, and evaluates to an element in the finite extension field $w \in \mathbb{G}_T$. Here $\mathbb{G}_1$ is contained in the elliptic curve $E(\mathbb{F}_p)$, $\mathbb{G}_2$ is contained in $E'(\mathbb{F}_{p^{k/d}})$, and $\mathbb{G}_T$ is contained in the finite extension field $\mathbb{F}_{p^k}$, where k is the embedding degree associated with the pairing-friendly curve, and d is a divisor of k corresponding to a supported twisted curve E'. Note that $\mathbb{G}_2$ points can be manipulated on the smaller twisted curve, and transformed to a point on $E(\mathbb{F}_{p^k})$ only when needed.

The pairing calculation consists of two parts, a Miller loop followed by a final exponentiation. In real-world protocols much of the action takes place in the smallest group $\mathbb{G}_1$, although implementors have tended to concentrate more on the pairing itself. In more complex protocols products of pairings are required, and here a single final exponentiation can be applied to an amalgamation of Miller loops [20].

A BN curve is an example of a parameterised pairing-friendly curve, that is, fixed polynomial formulæ exist for the prime modulus p and the group order r in terms of an integer parameter u, which is chosen such that both p and r are prime. Such parameterised curves have become very popular for many reasons. First the ratio between the group and field size can be as low as one, and secondly multiple optimizations become possible. The most significant of these would be the development of the optimal ate pairing [23], for which the number of iterations of the Miller loop is reduced from the number of bits in r (as required for the original Tate pairing) to the number of bits in u. Since the degrees of the defining polynomial formulæ increase with the embedding degree, rather paradoxically this implies that the number of iterations required in the Miller loop actually tends to decrease as the security level increases. Also a simpler form of final exponentiation applies [21].

However almost immediately after BN curves were introduced, Schirokauer [19] in a paper introducing the Number Field Sieve (NFS), warned us that: "Without discussing the evident difficulty of implementing the NFS for degree 12 fields, we observe that the special form of p may reduce the difficulty of computing logarithms in $\mathbb{F}_{p^{12}}$". In the absence of any concrete evidence to support this concern, the BN curve was nonetheless widely adopted. However Schirokauer's warning has proven to be prescient and the field of pairing-based cryptography has been disrupted by the recent, but not entirely surprising, discovery of a faster algorithm for solving the discrete logarithm problem in the finite extension field that arises when using

DL Algorithm complexity	2^{128}	2^{192}	2^{256}
NFS ($L_{p^k}[1/3, 1.923]$)	3072	7680	15360
(ex)TowerNFS medium ($L_{p^k}[1/3, 1.747]$)	3618	9241	18480
Special(ex)TowerNFS medium ($L_{p^k}[1/3, 1.526]$)	5004	12871	27410

Table 1: Recommended extension field sizes

these types of pairings, see [13, 1, 15].

A pairing-friendly curve can be characterised by the defining triplet $\{\rho, k, d\}$, where ρ is the ratio between the number of bits in p and the number of bits in r. Given a group size of g bits, the field size of $\mathbb{G}_1$ is $f_1 = \rho g$, the extension field size of $\mathbb{G}_T$ is $f_T = \rho k g$, and the field size of $\mathbb{G}_2$ is $f_2 = f_T/d$, where d is from the set of possible twists $\{1, 2, 3, 4, 6\}$, and is usually the maximum from this set that divides k.

When choosing a suitable curve, the starting point is the security level in bits, typically 128, 192 or 256. The group size should ideally be exactly twice this, and the other field sizes are then immediately fixed as shown above by the defining triplet.

For example for 128 bits of security of a BN curve, the defining triplet is $1, 12, 6$, and given $g = 256$, then $f_1 = 256$, $f_T = 3072$, and $f_2 = 512$. For a BLS12 curve (by which we mean a BLS curve with embedding degree of 12, see below), the triplet is $3/2, 12, 6$, and given $g = 256$, then $f_1 = 384$, $f_T = 4608$, and $f_2 = 768$.

The main problem is to satisfy the security requirement for $\mathbb{G}_T$, so that it matches that for $\mathbb{G}_1$. See Table 1. Note that these numbers are rather imprecise as exact analysis is difficult. We have mainly followed the analysis of Barbulescu and Duquesne [1], extrapolating in places, rather than the less conservative estimates of Menezes, Sarkar and Singh [17]. However the estimates they provide depend on certain constants, in which one can have diminishing confidence as the security level increases.

Basically, according to current knowledge, only the NFS and TNFS estimates apply to finite fields of prime extension degree. The exTNFS estimates apply to composite order extensions, and the SexTNFS estimates to parameterised prime, composite order extensions, like the BN curves. It is now clear that BN curves are not quite as perfect as originally thought. As Barbulescu and Duquesne put it: "Variants of NFS where p is parameterized are considered to be the dream situation for an attacker", although they do go on to offer some reassurance that they do not expect any further improvements in the SexTNFS algorithm.

We should say a word about $\mathbb{G}_2$. Since this is of a size an integer multiple of $\mathbb{G}_1$, we can be confident that if $\mathbb{G}_1$ is secure then so is $\mathbb{G}_2$. However in the optimal ate pairing [23], each iteration of the Miller loop typically involves at least a point doubling in $\mathbb{G}_2$. Therefore we would like $\mathbb{G}_2$ to be as small as possible, and therefore the twist d to be as large as possible. The maximum

attainable on an elliptic curve is $d = 6$, and this can only happen if $6|k$. But inevitably as the embedding degree k increases, so must $\mathbb{G}_2$. Ideally we would not want $\mathbb{G}_2$ growing too large, as elliptic curve cryptography over large extension fields will be very slow (and probably best implemented using affine coordinates).

From an implementation point of view the ideal solution is one that keeps f_1 as small as possible, while meeting all of the security constraints. This assumes that the value of ρ is small, that the embedding degree is such that we serendipitously hit the appropriate target in Table 1, and that a sextic twist applies and so the embedding degree is a multiple of 6.

An alternative response might be to revert to the Cocks-Pinch construction [8], avoiding parameterized curves, while continuing to use composite order extensions. It is not difficult to generate such curves for $k = 0 \bmod 6$ such that sextic twists can be supported, although only for $\rho \geq 2$. The idea would be to revert to the original Tate pairing and adopt the lower exTNFS estimates. However this is unlikely to prove competitive in practice.

2 BLS and KSS curves

BLS curves are the original small discriminant parameterised family of families of pairing-friendly elliptic curves [2]. For any positive embedding degree $k = 0 \bmod 6$ (unless $18|k$), they provide simple formulæ from which can be derived pairing friendly curves which support the maximal twist of $d = 6$, and have a relatively small ρ value given by $\rho = (2+k/3)/\varphi(k)$ [10]. Observe that the value of ρ decreases with increasing values of k. Having a range of embedding degrees to choose from makes it easier to hit the optimal values in Table 1 for any security level.

For example Barbulescu and Duquesne [1] have demonstrated that the BLS12 curve is a good fit for the 128-bit level of security, and the BLS24 curve is the best choice for 192 bits of security. In another recent paper Kiyomura et al. [16], reacting to the new understanding, demonstrated that a BLS48 curve is also the best choice of pairing-friendly curve to meet the new estimates for the 256-bit level of security. In this case the security requirement could be met with a group size of 512 bits, a modulus of 576 bits (as $\rho = 9/8$), and a finite field extension size of $48 \cdot 576 = 27648$.

However the BLS curves do not exist for $18|k$, as in these cases the polynomial formula for p is not irreducible, and therefore cannot generate primes [10]. Serendipitously for the cases of $k = 18$ and $k = 36$ there do exist the alternative KSS curves [14], which, as luck would have it, provide curves with the same ρ values as determined by the above formula for the missing BLS curves. However since the taxonomy of Freeman, Scott and Teske does not explore beyond $k = 50$, the situation for $k = 54$ is currently unknown. But if a BLS curve did exist for $k = 54$, then from the formula

given above, it would have a ρ value of 10/9.

3 The new discovery

The new curve was discovered using the KSS method as described in [14]. It was immediately observed that the new curve found with embedding degree 54 is not of the form of a typical KSS curve, where integer solutions exist only in a restricted set of residue classes. Recall that the KSS method also rediscovers the BN curves [3]. It appeared possible that the new family of curves was, like the BN curves, a "sporadic", and not related to any existing family. On the other hand it has a certain symmetry, which suggested that it might be a member of an as-yet undiscovered family of families.

We found that $-\zeta_{54} - \zeta_{54}^{10}$ as a suitable element $\in \mathbb{Q}(\zeta_{54})$, and following the KSS method [14] from there we obtained the solution

$$\begin{aligned} p &= 1 + 3u + 3u^2 + 3^5u^9 + 3^5u^{10} + 3^6u^{10} + 3^6u^{11} + 3^9u^{18} + 3^{10}u^{19} + 3^{10}u^{20} \\ r &= 1 + 3^5u^9 + 3^9u^{18} \\ t &= 1 + 3^5u^{10} \\ c &= 1 + 3u + 3u^2 \end{aligned} \tag{1}$$

where p is the prime modulus, r is the prime order of the pairing-friendly group, t is the trace of the Frobenius, and c is a cofactor. It can be verified that the Complex Multiplication (CM) discriminant is $D = 3$ because $4p - t^2 = 3f^2$, for some polynomial f. This implies that the curve has twists of degree 6 which, as with the BN and BLS curves, facilitates an important optimization. Observe that the prime p can be any of 1, 3, 5 or 7 mod 8 depending on the choice of u. The total number of points on the curve will be $\#E = cr$.

Recall that the embedding degree is the smallest value of k such that $r|(p^k - 1)$ [8]. In this case it is easily confirmed that $k = 54$. The value of $\rho = \deg(p)/\deg(r) = 10/9$, which is close to the ideal value of 1.

4 Aurifeuillean construction of pairing-friendly curves

The method of discovery does not explain the particular form of the new curve, or whether or not it is a member of a larger "family of families". To answer these questions we take a different approach.

The Aurifeuillean factorization of cyclotomic polynomials is a well-known tool used in the Cunningham project[1] [7] to factor large integers of the form

[1] `http://www.cerias.purdue.edu/homes/ssw/cun/index.html`

$b^n \pm 1$, where b is a square-free basis, $b \in \{2, 3, 5, 6, 7, 10, 11, 12\}$. Some of the factors can be obtained with the algebraic factorisation: since $u^n - 1 = \prod_{d|n} \Phi_d(u)$, where Φ_d is the d-th cyclotomic polynomial, then $b^n - 1 = \prod_{d|n} \Phi_d(b)$. For some combinations of bases and powers, more factors can be obtained with the Aurifeuillean factorization of the cyclotomic polynomials [18, 22, 5]:

Lemma 4.1. *Let $k > 1$ be an integer and let $\Phi_k(u)$ denote the k-th cyclotomic polynomial. Let a be a square-free integer and s an integer. Then $\Phi_k(as^2)$ will factor if*

- $a \equiv 1 \pmod 4$ *and* $a \equiv k \pmod{2a}$
- *or* $a \equiv 2, 3 \pmod 4$ *and* $2a \equiv k \pmod{4a}$.

This fact is already known for pairing-friendly curves: it was used to compute the order of the supersingular elliptic curves in characteristic 3 of embedding degree 6 (see for instance [9, Table 1]). Let $E/\mathbb{F}_{3^\ell}$ be a supersingular elliptic curve defined over $\mathbb{F}_{3^\ell}$ for an odd ℓ. If the curve has embedding degree 6, then the order of $E(\mathbb{F}_{3^\ell})$ is a divisor of $\Phi_6(3^\ell)$, where $\Phi_6(u) = u^2 - u + 1$. Assuming that $\ell = 2m + 1$, the Aurifeuillean factorization is $\Phi_6(3u^2) = (3u^2 + 3u + 1)(3u^2 - 3u + 1)$. Replacing u by 3^m so that $3u^2 = 3 \cdot 3^{2m} = 3^\ell$, we get $\Phi_6(3^{2m+1}) = (3^{2m+1} + 3^{m+1} + 1)(3^{2m+1} - 3^{m+1} + 1)$, and $\#E(\mathbb{F}_{3^\ell}) = 3^\ell - 3^{(\ell+1)/2} + 1$. We will apply this tool to find new families of pairing-friendly ordinary curves in large characteristic for $k = 3^j$ and $k = 2 \cdot 3^j$. Moreover this factorization pattern provides a larger framework for pairing-friendly curve construction, and a general point of view for the construction of MNT curves, BN curves and Freeman's curves.

4.1 Aurifeuillean construction

We combine the Brezing-Weng method [6], providing *cyclotomic families*, with Lemma 4.1, to obtain Algorithm 1. The idea is to look for an integer a where $-2k \leq a \leq 2k$, and satisfying Lemma 4.1 so that $\Phi_k(au^2) = r(u)r(-u)$, and we continue as for the Brezing-Weng method, with $r(u)$ a factor of $\Phi_k(au^2)$, and $\zeta_k = au^2$. The number field $K = \mathbb{Q}[u]/(r(u))$ contains a square root of a. When a is positive, we can choose $D = a$, or a multiple of a.

We ran Algorithm 1 for $7 \leq k \leq 100$, and small D ($1 \leq D \leq 100$). We checked that the polynomials $r(x)$ and $p(x)$ can give prime integers (there exist several x_0 such that $p(x_0)$ and $r(x_0)$ are prime at the same time). For $k = 7$ and $k = 35$, $p(x)$ does not represent primes (p is always even for $k = 7$ and $21 \mid p$ for $k = 35$). We obtained new families of pairing-friendly curves of ρ value as good as [10] for $k \in \{9, 15, 21, 30, 33, 39, 42, 45, 51, 54, 57, 66, 69, 75, 78, 81, 87, 90, 93\}$. Each time the best ρ was obtained for $a = 3$ or $a = -3$, and $D = 3$. For $k = 12$

Algorithm 1: Aurifeuillean construction of pairing-friendly curves

Input: embedding degree k, small discriminant D
Output: family (r, t, y, p) of a pairing-friendly elliptic curve of embedding degree k, or $\perp$

$\rho_{\min} \leftarrow 2$
for $a \in \{-2k, \ldots, -3, -2, 2, 3, \ldots, 2k\}$ **do**
  if *IsSquareFree*(a) *and* $((a = 1 \bmod 4$ *and* $k = a \bmod 2a)$ *or* $(a = 2, 3 \bmod 4$ *and* $k = 2a \bmod 4a))$ **then**
    $r(u) =$ an irreducible factor of $\Phi_k(au^2)$, s.t. $\Phi_k(au^2) = r(u)r(-u)$
    $K = \mathbb{Q}(\omega) = \mathbb{Q}[u]/(r(u))$
    if $-D$ *is a square in* K **then**
      $S = 1/\sqrt{-D} \in K$
      write S as a polynomial $s(u)$ s.t. $S = s(\omega)$ in K
      for $e = 1 \ldots k-1$, $\gcd(e, k) = 1$ **do**
        $t(u) = (au^2)^e + 1 \bmod r(u)$
        $y(u) = (t(u) - 2)s(u) \bmod r(u)$
        $p(u) = (t^2(u) + Dy^2(u))/4$
        if $p(u)$ *represents primes (cf. [10, Def. 2.5]) and* $\deg p / \deg r < \rho_{\min}$ **then**
          $\rho_{\min} \leftarrow \deg p / \deg r$
          $F_{\min} \leftarrow (r, t, y, p)$
if $\rho_{\min} = 2$ **then**
  return $\perp$
else
  return $F_{\min}$

and $a = \pm 6$, the output is the BN curve family. As an example, we give the parameters obtained for $k = 15$. The family for $k = 9$ (Example 4.5) falls in our new construction that we present in the next section.

Example 4.2. Aurifeuillean construction for $k = 15$. We obtain a family with $D = 3$, $\deg r(u) = 8$ and $\rho = 4/3$ as in [10]. $\Phi_{15}(-3u^2) = r(u)r(-u)$ where $r(u) = 81u^8 + 81u^7 + 54u^6 + 27u^5 + 9u^4 + 9u^3 + 6u^2 + 3u + 1$. There are two choices for $t(u)$, producing two families with $\rho = 4/3$:

$$\begin{array}{rcl}
t_1(u) & = & 54u^6 + 3u + 1 = (-3u^2)^8 + 1 \bmod r(u) \\
y_1(u) & = & -18u^5 - u - 1 \\
p_1(u) & = & 729u^{12} + 243u^{10} + 81u^7 + 54u^6 + 27u^5 + 3u^2 + 3u + 1 \\
\hline
t_2(u) & = & -27u^6 - 3u + 1 = (-3u^2)^{13} + 1 \bmod r(u) \\
y_2(u) & = & -27u^6 - 18u^5 - u - 1 \\
p_2(u) & = & 729u^{12} + 729u^{11} + 243u^{10} + 81u^7 + 54u^6 + 27u^5 + 3u^2 + 1
\end{array}$$

4.2 Aurifeuillean family for $k = 3^j$

We now explain the generalization of the $k = 54$ family to any $k = 3^j$ using an Aurifeuillean factorization of $\Phi_{3^j}(u)$. We start by the general expression:

$$\Phi_{3^j}(u) = \Phi_3(u^{3^{j-1}}) = u^m + u^{m/2} + 1 \ , \text{ where } m = \varphi(3^j) = 2 \cdot 3^{j-1} \ . \quad (2)$$

If $k = 3^j$, then to obtain an Aurifeuillean factorization, we take $a = -3 \equiv 1 \bmod 4$, we need $k = a \bmod 2a \Leftrightarrow 3^j = 3 \bmod 6$, and indeed this is always the case. The degree of $\Phi_k(u)$ is $m = 2 \cdot 3^{j-1}$, in particular m is even and $m/2$ is odd. We obtain the Aurifeuillean factorization:

$$\begin{array}{rcl}
\Phi_{3^j}(-3u^2) & = & 3^m u^{2m} - 3^{m/2} u^m + 1 \\
& = & (3^{m/2} u^m + 3^{(m+2)/4} u^{m/2} + 1)(3^{m/2} u^m - 3^{(m+2)/4} u^{m/2} + 1) \\
& = & r(u) r(-u)
\end{array}$$

where

$$r(u) = 3^{m/2} u^m + 3^{(m+2)/4} u^{m/2} + 1 \ .$$

We choose $D = 3$, we compute $\sqrt{-3}$ and its inverse modulo $r(u)$:

$$\begin{array}{rcl}
\sqrt{-3} & = & -2 \cdot 3^{(m+2)/4} u^{m/2} - 3 \\
1/\sqrt{-3} & = & -\sqrt{-3}/3 = 2 \cdot 3^{(m-2)/4} u^{m/2} + 1 \ .
\end{array}$$

We know that $-3u^2$ is a primitive k-th root of unity in $K = \mathbb{Q}(u)/(r(u))$. All the $(-3u^2)^e$ for $3 \nmid e$ are primitive k-th roots of unity modulo $r(u)$, i.e., $e \neq 0 \bmod 3$. We have

$$\begin{array}{rcl}
t(u) & = & (-3u^2)^e + 1 \bmod r(u) \\
y(u) & = & (t(u) - 2)/\sqrt{-D} \bmod r(u) \\
& = & ((-3u^2)^e - 1)(2 \cdot 3^{(m-2)/4} u^{m/2} + 1) \bmod r(u) \ .
\end{array}$$

To get $\rho = \deg p / \deg r$ as small as possible, we want to minimize

$$\max(\deg t(u), \deg y(u)) \ .$$

The possible degrees e to get the smallest possible degree of $p(u)$ are listed in Table 2, with the values of $t(u), y(u) \bmod r(u)$, and $p(u)$.

even j			
e	$(m+2)/4$	deg	ρ
$t(u) \bmod r(u)$	$3^{(m+2)/4}u^{m/2+1} + 1$	$m/2+1$	
$y(u) \bmod r(u)$	$-3^{(m+2)/4}u^{m/2+1} - 2 \cdot 3^{(m-2)/4}u^{m/2} - 2u - 1$	$m/2+1$	
$p(u)$	$(3u^2+3u+1)r(u) + t(u) - 1$	$m+2$	$(m+2)/m$
e	$(m+2)/4 + m/2$		
$t(u) \bmod r(u)$	$-2 \cdot 3^{(m+2)/4}u^{m/2+1} - 3u + 1$	$m/2+1$	
$y(u) \bmod r(u)$	$-2 \cdot 3^{(m-2)/4}u^{m/2} + u - 1$	$m/2$	
$p(u)$	$(3u^2+1)r(u) + t(u) - 1$	$m+2$	$(m+2)/m$
e	$(m+2)/4 + m$		
$t(u) \bmod r(u)$	$3^{(m+2)/4}u^{m/2+1} + 3u + 1$	$m/2+1$	
$y(u) \bmod r(u)$	$3^{(m+2)/4}u^{m/2+1} - 2 \cdot 3^{(m-2)/4}u^{m/2} + u - 1$	$m/2+1$	
$p(u)$	$(3u^2-3u+1)r(u) + t(u) - 1$	$m+2$	$(m+2/m)$
even and odd j			
e	1		
$t(u) \bmod r(u)$	$-3u^2 + 1$	2	
$y(u) \bmod r(u)$	$-2 \cdot 3^{(m+2)/4}u^{m/2+2} - 2 \cdot 3^{(m-2)/4}u^{m/2} - 3u^2 - 1$	$m/2+2$	
$p(u)$	$(9u^4+6u^2+1)r(u) + t(u) - 1$	$m+4$	$(m+4)/m$
e	$1 + m/2$		
$t(u) \bmod r(u)$	$-3^{(m+6)/4}u^{m/2+2} - 3u^2 + 1$	$m/2+2$	
$y(u) \bmod r(u)$	$3^{(m+2)/4}u^{m/2+2} - 2 \cdot 3^{(m-2)/4}u^{m/2} + 3u^2 - 1$	$m/2+2$	
$p(u)$	$(9u^4-3u^2+1)r(u) + t(u) - 1$	$m+4$	$(m+4)/m$
e	$1 + m$		
$t(u) \bmod r(u)$	$3^{(m+6)/4}u^{m/2+2} + 2 \cdot 3u^2 + 1$	$m/2+2$	
$y(u) \bmod r(u)$	$3^{(m+2)/4}u^{m/2+2} - 2 \cdot 3^{(m-2)/4}u^{m/2} - 1$	$m/2+2$	
$p(u)$	$(9u^4-3u^2+1)r(u) + t(u) - 1$	$m+4$	$(m+4)/m$

Table 2: For $k = 3^j$, values of e such that $\gcd(e,k) = 1$, $t(u) = (-3u^2)^e + 1 \bmod r(u)$, $p(u)$ is irreducible, and $\deg p(u)$ is minimal. For even j, $\rho = (m+2)/m$. For odd j, $p(u)$ is not irreducible for the first three values $e = (m+2)/4, 3(m-2)/4+2, m+(m+2)/4$, only the last three ones with $\rho = (m+4)/m$ are possible.

4.3 Aurifeuillean family for $k = 2 \cdot 3^j$

We proceed the same way as in Section 4.2. The general expression for $\Phi_{2\cdot 3^j}(u)$ is

$$\Phi_{2\cdot 3^j}(u) = \Phi_{3^j}(-u) = u^m - u^{m/2} + 1 \ , \text{ where } m = \varphi(2 \cdot 3^j) = 2 \cdot 3^{j-1} \ . \quad (3)$$

To obtain an Aurifeuillean factorization of $\Phi_{2\cdot 3^j}(u)$, we choose $a = 3$ (so $a = 3 \bmod 4$) and the condition $k = 2a \pmod{4a} \Leftrightarrow k = 2 \cdot 3^j = 6 \bmod 12$ is always satisfied since $6 \mid k$ but $4 \nmid k$. We obtain

$$\begin{aligned} \Phi_{2\cdot 3^j}(3u^2) &= \Phi_{3^j}(-3u^2) = 3^m u^{2m} - 3^{m/2}u^m + 1 \\ &= r(u)r(-u) \end{aligned}$$

where again

$$r(u) = 3^{m/2}u^m + 3^{(m+2)/4}u^{m/2} + 1 \ .$$

We take $D = 3$, and we know that $3u^2$ is a primitive k-th root (a primitive $2 \cdot 3^j$-th root) of unity in $K = \mathbb{Q}(\omega)$ where ω is a root of $r(u)$. In the same way as previously we obtain Table 3. The polynomial $r(u)$ is the same but the trace differs and the embedding degree of the family is doubled.

	j odd		
e	$(m+2)/4,\ e = 5 \bmod 6$	deg	ρ
$t(u) \bmod r(u)$	$3^{(m+2)/4}u^{m/2+1} + 1$	$m/2+1$	
$y(u) \bmod r(u)$	$-3^{(m+2)/4}u^{m/2+1} - 2 \cdot 3^{(m-2)/4}u^{m/2} - 2u - 1$	$m/2+1$	
$p(u)$	$(3u^2 + 3u + 1)r(u) + t(u) - 1$	$m+2$	$(m+2)/m$
e	$m + (m+2)/4,\ e = 5 \bmod 6$		
$t(u) \bmod r(u)$	$3^{(m+2)/4}u^{m/2+1} + 3u + 1$	$m/2+1$	
$y(u) \bmod r(u)$	$3^{(m+2)/4}u^{m/2+1} - 2 \cdot 3^{(m-2)/4}u^{m/2} + u - 1$	$m/2+1$	
$p(u)$	$(3u^2 - 3u + 1)r(u) + t(u) - 1$	$m+2$	$(m+2)/m$
e	$2m + (m+2)/4,\ e = 5 \bmod 6$		
$t(u) \bmod r(u)$	$-2 \cdot 3^{(m+2)/4}u^{m/2+1} - 3u + 1$	$m/2+1$	
$y(u) \bmod r(u)$	$-2 \cdot 3^{(m-2)/4}u^{m/2} + u - 1$	$m/2$	
$p(u)$	$(3u^2 + 1)r(u) + t(u) - 1$	$m+2$	$(m+2)/m$
	j odd and even		
e	1		
$t(u) \bmod r(u)$	$3u^2 + 1$	2	
$y(u) \bmod r(u)$	$2 \cdot 3^{(m+2)/4}u^{m/2+2} - 2 \cdot 3^{(m-2)/4}u^{m/2} + 3u^2 - 1$	$m/2+2$	
$p(u)$	$(9u^4 - 6u^2 + 1)r(u) + t(u) - 1$	$m+4$	$(m+4)/m$
e	$m+1,\ e = 1 \bmod 6$		
$t(u) \bmod r(u)$	$-3^{(m+6)/4}u^{m/2+2} - 2 \cdot 3u^2 + 1$	$m/2+2$	
$y(u) \bmod r(u)$	$-3^{(m+2)/4}u^{m/2+2} - 2 \cdot 3^{(m-2)/4}u^{m/2} - 1$	$m/2+2$	
$p(u)$	$(9u^4 + 3u^2 + 1)r(u) + t(u) - 1$	$m+4$	$(m+4)/m$
e	$2m+1,\ e = 1 \bmod 6$		
$t(u) \bmod r(u)$	$3^{(m+6)/4}u^{m/2+2} + 3u^2 + 1$	$m/2+2$	
$y(u) \bmod r(u)$	$-3^{(m+2)/4}u^{m/2+2} - 2 \cdot 3^{(m-2)/4}u^{m/2} - 3u^2 - 1$	$m/2+2$	
$p(u)$	$(9u^4 + 3u^2 + 1)r(u) + t(u) - 1$	$m+4$	$(m+4)/m$

Table 3: For $k = 2 \cdot 3^j$, values of e such that $\gcd(e, k) = 1$, $t(u) = (3u^2)^e + 1 \bmod r(u)$, $p(u)$ is irreducible, and $\deg p(u)$ is minimal. For odd j, $\rho = (m+2)/m$. For even j, $p(u)$ is not irreducible for the first three values $e = (m+2)/4, m + (m+2)/4, 2m + (m+2)/4$, only the last three ones with $\rho = (m+4)/m$ are possible.

As speculated in Section 3, the $k = 54$ family found with the KSS method is indeed a member of a larger "family of families".

Construction 4.3. *For $n = 3^j$ and $m = \varphi(n)$, then a pairing-friendly curve with embedding degree of $k = 2n$ if j is odd, and $k = n$ if j is even, with discriminant $D = 3$, and with a ρ value of $(m+2)/m$, can be found as*

$$\begin{aligned} r(u) &= 1 + 3^{(m+2)/4}u^{m/2} + 3^{m/2}u^m \\ t(u) &= 1 - 3u - 2 \cdot 3^{(m+2)/4}u^{1+m/2} \\ c(u) &= 1 + 3u^2 \\ p(u) &= c(u) \cdot r(u) + t(u) - 1 \end{aligned} \tag{4}$$

Construction 4.4. *For $n = 3^j$ and $m = \varphi(n)$, then a pairing-friendly curve with embedding degree of $k = n$ or $k = 2n$, with discriminant $D = 3$, and with a ρ value of $(m + 4)/m$, can be found as*

$$\begin{aligned} r(u) &= 1 + 3^{(m+2)/4}u^{m/2} + 3^{m/2}u^m \\ t(u) &= 1 + 3\epsilon u^2 \\ c(u) &= 9u^4 - 6\epsilon u^2 + 1 \\ p(u) &= c(u) \cdot r(u) + t(u) - 1 \\ \epsilon &= (-1)^{k \bmod 2} \end{aligned} \tag{5}$$

This hypothesis has been tested for all applicable embedding degrees less than 1000. However it is not particularly useful for cases other than $k = 54$. For the embedding degrees that arise from these formulæ which are less than 54 (6 and 9), there already exist curves with the same or better ρ value. The higher values of embedding degree (81, 486) are probably not useful in practice.

4.4 Applications

Our Aurifeuillean constructions 4.3 and 4.4 for $k = 3^j$ and $k = 2 \cdot 3^j$ can be applied when the Brezing–Weng construction and the construction 6.6 of [10] do not provide a satisfying result. The Brezing-Weng fails for $k = 54$ ($p(u)$ is never irreducible) and $k = 90$: p is not irreducible, or does not generate primes. The construction 6.6 of [10] fails for $18 \mid k$ ($k = 18, 36, 54, 72, 90$). We can alternatively use the Aurifeuillean construction when $18 \mid k$ and $8 \nmid k$, that is $k \in \{18, 54, 90\}$. Unfortunately for $k = 18$ the Aurifeuillean construction gives $\rho = 5/3$, larger than $\rho = 4/3$ achieved by [14] (referenced as construction 6.12 in [10]). The construction provides a new family for $k = 54$ with $\rho = 10/9$. For $k = 90$ however, the coefficients of $p(u)$ are very large and such a large embedding degree is unlikely to be used in pairing-based cryptography.

Our family also covers $k = 9$ and as a conclusion we provide our alternative choice for $k = 9$ and $D = 3$.

Example 4.5. Aurifeuillean construction for $k = 9$. $\Phi_9(-3u^2) = r(u)r(-u)$ where $r(u) = 27u^6 + 9u^3 + 1$. Three are three choices for the trace $t(u)$.

With $D = 3$, we obtain $\rho = 4/3$.

$$\begin{array}{rcl}
t_1(u) & = & -18u^4 - 3u + 1 = (-3u^2)^5 + 1 \bmod r(u) \\
y_1(u) & = & -6u^3 + u - 1 \\
p_1(u) & = & 81u^8 + 27u^6 + 27u^5 - 18u^4 + 9u^3 + 3u^2 - 3u + 1 \\
\hline
t_2(u) & = & 9u^4 + 3u + 1 = (-3u^2)^8 + 1 \bmod r(u) \\
y_2(u) & = & 9u^4 - 6u^3 + s - 1 \\
p_2(u) & = & 81u^8 - 81u^7 + 27u^6 + 27u^5 - 18u^4 + 9u^3 + 3u^2 + 1 \\
\hline
t_3(u) & = & 9u^4 + 1 = (-3u^2)^2 + 1 \bmod r(u) \\
y_3(u) & = & -9u^4 - 6u^3 - 2u - 1 \\
p_3(u) & = & 81u^8 + 81u^7 + 27u^6 + 27u^5 + 36u^4 + 9u^3 + 3u^2 + 3u + 1
\end{array}$$

MNT curves as Aurifeuillean curves for $k = 3$. The MNT construction provides three families of curves of embedding degree 3, 4 and 6 respectively. The curve for $k = 3$ can be obtained with the Aurifeuillean factorization of $\Phi_3(u)$, and the two curves for $k = 4, 6$ with the cyclotomic construction. We start with $\Phi_3(-3u^2) = (3u^2 + 3u + 1)(3u^2 - 3u + 1) = r(u)r(-u)$. The two choices for the trace are $-3u^2 + 1 \bmod r(u) = -3u + 2 = t_1$ and $(-3u^2)^2 + 1 \bmod r(u) = 3u - 1 = t_2$. Since $t_1 = t_2(-u+1)$, we continue with $t = 3u - 1$, and compute $p(u) = r(u) + t(u) - 1 = 3u^2 - 1$. We obtain the first MNT curve (see Table 4.4), with the change of variable $l = 2u$ (indeed, $p = 3u^2 - 1$ is always even for odd u, so the MNT family takes $l = 2u$). The CM equation is $4p - t^2 = 3u^2 + 6u - 5$, and requires to solve a Pell equation as in the original paper. The MNT curve families for $k = 4$ and $k = 6$ do not correspond to the Aurifeuillean construction, but to a cyclotomic construction ($r(u) = \Phi_k(u)$). The two Aurifeuillean constructions (without choosing $-D$ as a square in $\mathbb{Q}(\zeta_k)$) for $k = 4, 6$ produce supersingular curves of characteristic 2 and 3 respectively. We summarise this in Table 4.4.

k		MNT	cyclotomic	Aurifeuillean
3	$t(u)$	$-1 \pm 6l$	$u+1, -u$ $(\zeta_3 = u, -u-1)$	$-3u+2, 3u-1$
	$r(u)$	$12l^2 \mp 6l + 1$	$\Phi_3(u) = u^2 + u + 1$	$3u^2 - 3u + 1$, $\Phi_3(-3u^2) = r(u)r(-u)$
	$p(u)$	$12l^2 - 1$	$(u+1)^2, u^2$	$3u^2 - 6u + 2$, $3u^2 - 1$
	Dy^2	$12l^2 \pm 12l - 5$	$3(u+1)^2, 3u^2$	$3u^2 - 12u + 4$, $3u^2 + 6u - 5$
			supersingular, $q = p^2$	MNT with $l = 2u$
4	$t(u)$	$-l$, $l+1$	$\pm u + 1$ $(\zeta_4 = \pm u)$	$2u, -2(u-1)$
	$r(u)$	$l^2 + 2l + 2$, $l^2 + 1$	$\Phi_4(u) = u^2 + 1$	$2u^2 - 2u + 1$, $\Phi_4(\pm 2u^2) = r(u)r(-u)$
	$p(u)$	$l^2 + l + 1$	$u^2 \pm u + 1$	$2u^2, 2(u-1)^2$
	Dy^2	$3l^2 + 4l + 4$	$3u^2 \pm 2u + 3$	$4u^2, 4(u-1)^2$
			MNT with $l = u, u-1$	supersingular, $q = 2^\ell$
6	$t(u)$	$1 \pm 2l$	$u+1, -u+2$ $(\zeta_6 = u, -u+1)$	$3u, -3(u-1)$
	$r(u)$	$4l^2 \mp 2l + 1$	$\Phi_6(u) = u^2 - u + 1$	$3u^2 - 3u + 1$, $\Phi_6(3u^2) = r(u)r(-u)$
	$p(u)$	$4l^2 + 1$	$u^2 + 1, u^2 - 2u + 2$	$3u^2, 3(u-1)^2$
	Dy^2	$12l^2 - 4l + 3$	$3u^2 - 2u + 3, 3u^2 - 4u + 4$	$3u^2, 3(u-1)^2$
			MNT with $l = 2u$	supersingular, $q = 3^\ell$

Table 4: Correspondence between MNT families, cyclotomic construction and Aurifeuillean factorization

Galbraith, McKee and Valença factorisation patterns. Galbraith, McKee and Valença already investigated the strategy of finding $q(l)$ such that $\Phi_k(q(l))$ splits into two quadratic factors for $k = 3, 4, 6$ or two quartic factors for $k = 5, 8, 10, 12$ in [11]. They obtained Aurifeuillean factorisation patterns for $k = 3, 4, 5, 6, 10, 12$. Their work allowed Freeman to obtain $k = 10$ curves and Barreto and Naehrig to obtain $k = 12$ curves, both with $\rho = 1$.

4.5 Further investigations

Granville and Pleasants [12] investigated the possibility that there are other identities still to be discovered. Wagstaff [24] used the Cunningham tables to try unsuccessfully to discover new identities. His results tend to confirm the theoretical results of [12] that under reasonable definitions, Schinzel found the last Aurifeuillean-like factorizations.

It seems very unlikely that a new mysterious pairing-friendly family as the Barreto-Naehrig curves with $\rho = 1$ will be discovered with similar techniques: we ran Algorithm 1 for $k \leq 100$ without success.

New discoveries are still possible, but will more probably arise with large computer search for factorization of $\Phi_k(g(u))$ for polynomials $g(u)$ of degree strictly larger than 2, as for $k = 8$.

5 An example construction

An actual curve can be generated using the seed value $u = C404042_{16}$, which has a low Hamming weight of 6. Then the curve

$$y^2 = x^3 + 12$$

is a pairing-friendly elliptic curve with a group order r of 512 bits, and a modulus p of 569 bits. Given the embedding degree of 54, the finite extension field is of size 30726 bits, comfortably, but not excessively, above the size recommended for an overall security equivalent to 256 bits (from table 1). The embedding degree $k = 54$ is obviously of the desirable form $k = 2^i 3^j$, which simplifies implementation [16].

To derive an optimal pairing, following [23] we find the shortest vector in a lattice and observe that $u + up^9 + p^{10} = 0 \bmod r$. Then an optimal ate pairing is defined as

$$t(Q, P) = (f_{u,Q}^{p^9+1}(P).l_{p^9uQ+p^{10}Q,uQ}(P).l_{p^{10}Q,p^9uQ}(P))^{(p^{54}-1)/r}$$

The Miller loop (of just 28 iterations, given the bit length of u) provides $f_{u,Q}(P)$ and the value of uQ, after which two line function evaluations, some cheap applications of the Frobenius operator, and a final exponentiation complete the calculation.

Implementation will require the construction of a tower of extensions. Since $\mathbb{G}_2$ is over $E'(\mathbb{F}_{p^9})$ it would make sense to use a 1-3-9-18-54 towering, similar to that recommended for the $k = 18$ case [4]. It is apparent from the defining equation that $p = 1 \bmod 3$. It is also clear that u must be even to generate primes. So we make the substitution $u = 2v$ and from there it is straightforward if tedious to coerce Fermat's identity $p = a^2 + 3b^2$ where

$$\begin{aligned} a &= 1 + 3v + 2^8 3^5 v^9 + 2^{10} 3^5 v^{10} \\ b &= v + 2^8 3^4 v^9 \end{aligned} \tag{6}$$

As demonstrated by Benger and Scott [4] this implies by Euler's conjecture that $x^{54} - 2$ is irreducible over $\mathbb{F}_p$ as long as $3 \nmid b$, which is equivalent to the simple condition that $3 \nmid u$.

6 Conclusion

We present a new family of pairing friendly curves with an embedding degree of $k = 54$, which fills a gap that might be useful in the event of a deeper understanding emerging of the true difficulty of the discrete logarithm problem as it applies to high-security pairing-based cryptography. Motivated by this discovery we place it into a wider context, and identify it as just one member of a larger family of curves. The $k = 54$ solution may have been previously overlooked as the limit of practical interest was at one time conservatively estimated as being 50 [10]. We also strived to find a solution for the next "missing" case of $k = 72$ (by which we mean an embedding degree which is a multiple of six, and which is not covered by the BLS construction) but failed despite an extensive computer search. Nevertheless clearly the KSS method is a powerful tool for discovering families of pairing-friendly curves.

References

[1] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. *Journal of Cryptology*, Jan 2018. `https://doi.org/10.1007/s00145-018-9280-5`, `http://eprint.iacr.org/2017/334`.

[2] 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 *LNCS*, pages 263–273. Springer-Verlag, 2002. `https://eprint.iacr.org/2002/088`.

[3] P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptography – SAC'2005*, volume 3897 of *LNCS*, pages 319–331, Kingston, 2006. Springer-Verlag. `https://eprint.iacr.org/2005/133`.

[4] N. Benger and M. Scott. Constructing tower extensions of finite fields for implementation of pairing-based cryptography. In *WAIFI 2010*, volume 6087 of *LNCS*, pages 180–195. Springer-Verlag, 2010. https://eprint.iacr.org/2009/556.

[5] Richard P. Brent. On computing factors of cyclotomic polynomials. *Math. Comp.*, 61(203):131–149, 1993. https://doi.org/10.2307/2152941.

[6] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptography*, 37(1):133–141, 2005. https://eprint.iacr.org/2003/143.

[7] John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*, volume 22 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, second edition, 1988. https://homes.cerias.purdue.edu/~ssw/cun/.

[8] N. El Mrabet and M. Joye, editors. *Guide to Pairing-Based Cryptography*. Chapman and Hall/CRC, 2016. https://www.crcpress.com/Guide-to-Pairing-Based-Cryptography/El-Mrabet-Joye/p/book/9781498729505.

[9] Nicolas Estibals. Compact hardware for computing the Tate pairing over 128-bit-security supersingular curves. In Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors, *Pairing 2010*, volume 6487 of *LNCS*, pages 397–416, Yamanaka Hot Spring, Japan, 2010. Springer. https://eprint.iacr.org/2010/371.

[10] D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology*, 23(2):224–280, 2010. http://eprint.iacr.org/2006/372.

[11] S.D. Galbraith, J.F. McKee, and P.C. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields and Their Applications*, 13(4):800 – 814, 2007. https://eprint.iacr.org/2004/365.

[12] Andrew Granville and Peter Pleasants. Aurifeuillian factorization. *Math. Comp.*, 75(253):497–508, 2006. https://doi.org/10.1090/S0025-5718-05-01766-7.

[13] Antoine Joux and Cécile Pierrot. The special number field sieve in $\mathbb{F}_{p^n}$ - application to pairing-friendly constructions. In Zhenfu Cao and Fangguo Zhang, editors, *Pairing 2013*, volume 8365 of *LNCS*, pages 45–61, Beijing, China, 2013. Springer. https://eprint.iacr.org/2013/582.

[14] E. Kachisa, E.F. Schaefer, and M. Scott. Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. In *Pairing 2008*, volume 5209 of *LNCS*, pages 126–135. Springer-Verlag, 2008. https://eprint.iacr.org/2007/452.

[15] T. Kim and R. Barbulescu. The extended tower number field sieve: A new complexity for the medium prime case. In *Crypto 2016*, volume 9814 of *LNCS*, pages 543–571. Springer-Verlag, 2016. https://eprint.iacr.org/2015/1027.

[16] Y. Kiyomura, A. Inoue, Y. Kawahara, M. Yasuda, T. Takagi, and T. Kobayashi. Secure and efficient pairing at 256-bit security level. In *ACNS 2017*, volume 10355 of *LNCS*, pages 59–79. Springer-Verlag, 2017.

[17] A. Menezes, P. Sarkar, and S. Singh. Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography. In *Mycrypt 2016*, volume 10311 of *LNCS*, pages 83–108. Springer-Verlag, 2016. https://eprint.iacr.org/2016/1102.

[18] A. Schinzel. On primitive prime factors of $a^n - b^n$. *Proc. Cambridge Philos. Soc.*, 58(4):555–562, 1962. https://doi.org/10.1017/S0305004100040561.

[19] Oliver Schirokauer. The number field sieve for integers of low weight. *Mathematics of Computation*, 79(269):583–602, January 2010. https://doi.org/10.1090/S0025-5718-09-02198-X, http://eprint.iacr.org/2006/107.

[20] M. Scott. On the efficient implementation of pairing-based protocols. In *IMACC 2011*, volume 7089 of *LNCS*, pages 296–308. Springer-Verlag, 2011. https://eprint.iacr.org/2011/334.

[21] M. Scott, N. Benger, M. Charlemagne, and L. Dominguez Perez. On the final exponentiation for calculating pairings on ordinary elliptic curves. In *Pairing 2009*, volume 5671 of *LNCS*, pages 78–88. Springer-Verlag, 2009. https://eprint.iacr.org/2008/490.

[22] Peter Stevenhagen. On Aurifeuillian factorizations. *Nederl. Akad. Wetensch. Indag. Math.*, 49(4):451–468, 1987. https://doi.org/10.1016/1385-7258(87)90009-6.

[23] F. Vercauteren. Optimal pairings. *IEEE Transactions of Information Theory*, 56:455–461, 2009. https://eprint.iacr.org/2008/096.

[24] Samuel S Wagstaff, Jr. The search for Aurifeuillian-like factorizations. *Journal of Integers*, 12A(6):1449–1461, 2012. https://homes.cerias.purdue.edu/~ssw/cun/mine.pdf.