A New Family of Pairing-Friendly Elliptic Curves

Michael Scott and Aurore Guillevic

MIRACL.com
Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

WAIFI 2018, Bergen, Norway, June 14–16

Pairings in cryptography

$(\mathbb{G}_1, +), (\mathbb{G}_2, +), (\mathbb{G}_T, \cdot)$ three cyclic groups of large prime order r
A *pairing* is a map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

1. bilinear: $e(P_1 + P_2,\ Q) = e(P_1, Q) \cdot e(P_2, Q)$,
   $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$
2. non-degenerate: $e(G_1, G_2) \neq 1$ for $\langle G_1 \rangle = \mathbb{G}_1$, $\langle G_2 \rangle = \mathbb{G}_2$
3. efficiently computable.

Mostly used in practice:

$$e([a]P, [b]Q) = e([b]P, [a]Q) = e(P, Q)^{ab}$$

Many applications in asymmetric cryptography.

Pairing-Friendly Curves – PFCs

$$\text{ordinary curve } E/\mathbb{F}_p : y^2 = x^3 + ax + b$$

- $r \mid \#E(\mathbb{F}_p) = p + 1 - t$, $\mathbb{G}_1 = E(\mathbb{F}_p)[r]$ (points of order r)
- $r | p^k - 1$, for some reasonably small integer "embedding degree" k
- $\mathbb{G}_2 \subset E(\mathbb{F}_{p^k})[r]$, $\mathbb{G}_T = \{x \in \mathbb{F}^*_{p^k} : \ x^r = 1\}$
- E as secure and efficient as for ECC.
- DL problem hard in $E(\mathbb{F}_p)$ and in $\mathbb{F}_{p^k}$
- Hasse bound: $\#E(\mathbb{F}_p) = p + 1 - t$, $|t| \leq 2\sqrt{p}$
- Parameter size efficiency: ratio $\rho = \log_2 p / \log_2 r \geq 1$ small, ideally $\rho = 1$.
- E with *sextic twists* for efficient pairings ($\Rightarrow 6|k$ and a CM discriminant of $D = 3$ ($j(E) = 0$, $E/\mathbb{F}_p : y^2 = x^3 + b$))
- $k = 2^i 3^j$ for efficient implementation of $\mathbb{F}_{p^k}$ arithmetic

The candidates

- Candidate curves and curve families are described in the Freeman, Scott, Teske taxonomy paper [FST10]
- Non-parameterised Cocks-Pinch curves, easy to find for any k, but $\rho = 2$
- Parameterised curves, where p and r have a simple polynomial description
- For example MNT curves [MNT01], $p = x^2 + 1$, $r = x^2 - x + 1$, $k = 6$, $\rho = 1$ Pell equation and CM method needed
- But very rare, $D \neq 3$, lacks a fortuitous match between size of r and size of p^k for ECC and DL security resp.
- Most popular PFCs are small discriminant parameterised families ([BN06], [BLS02], [KSS08])

BN curves

- Embedding degree of $k = 12$, ρ=1.
- For 128-bit security, an r of 256 bits as required for ECC security matches p^k of 3072 bits as (apparently) required for DL security!
- A match made in heaven!
- That 3072-bit value derives from extensive historical analysis of RSA security, and the assumption that finite field DL problem is if anything harder.
- But murmurings from the background – surely the parameterised form of p might make the DL problem easier (Schirokauer [Sch06])? First weakness found by Joux–Pierrot [JP13].
- And anyhow how about 192 and 256-bit security. Here BN curves are not such a good match.
- Maybe BLS or KSS curves might be a better fit for these.

New DL results

- Schirokauer was right! Kim and Barbulescu [KB16] attack, analysed by Menezes–Sarkar–Singh [MSS16], Barbulescu and Duquesne [BD18]
- However low discriminant parameterised families are still optimal. We just need to revise upwards the size of p^k

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

Table: Recommended extension field sizes (rough estimate)
$L_{p^k} = \exp(c(\log p^k)(\log\log p^k)^{2/3})$

Practicality and performances of TNFS, SNFS and STNFS depends on k and the PFC family.

The response

- Recently Kiyomura et al. [KIK+17] considered 256-bit security and, responding to our new understanding, suggested that a $k = 48$ BLS curve might be optimal.
- The FST taxonomy only considered embedding degrees up to $k = 50$!
- Might be appropriate to go back and have another look...
- BLS are a family of families of PFCs, which supports for example the implementation-friendly values of $k = 12, 24, 48..$, but not $k = 18, 36$
- The ρ value is $(k + 6)/k$
- KSS curves are "sporadics" which happily fill in the gaps for $k = 18, 36$, and feature the same ρ formula.
- but maybe we should look at the next one up, $k = 54$?

The Discovery

- A new discovery is one of the most pleasing outcomes of research
- but its often more accident than design
- We re-ran our old KSS discovery code for values of $k > 50$
- and out popped a new solution for $k = 54$ almost immediately. At first we ignored it, hoping to find a BN-like solution with $\rho = 1$
- It didn't look like a typical KSS curve, for example KSS k=18
- $p = (x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401)/21$

A new family of PFCs

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

What exactly have we got here?

- Its pretty!
- The ρ value is $10/9$, which is again $(k+6)/k$
- But it doesn't have the look and feel of a typical KSS curve
- But then again the KSS method also finds the BN curves.
- Is it a sporadic family of curves, or a member of a larger family of families?

A similar pattern: supersingular curves over $GF(3^\ell)$

Pairings in 2001–2014: ℓ odd,

$$E/\mathbb{F}_{3^\ell} : y^2 = x^3 - x + b,\ \ b = \pm 1$$

$\#E(\mathbb{F}_{3^\ell}) = p + 1 - t$ where $p = 3^\ell,\ t = \pm 3^{(\ell+1)/2}$
Embedding degree: smallest k s.t. $r \mid \Phi_k(p)$

- $t = -3^{(\ell+1)/2}, \#E(\mathbb{F}_{3^\ell}) = (3^\ell + 3^{(\ell+1)/2} + 1)$, $\#E(\mathbb{F}_{3^\ell}) \mid \Phi_3(p),\ k = 3$
- $t = 3^{(\ell+1)/2},\ \#E(\mathbb{F}_{3^\ell}) = (3^\ell - 3^{(\ell+1)/2} + 1)$, $\#E(\mathbb{F}_{3^\ell}) \mid \Phi_6(p),\ k = 6$

Factorisation pattern

$$\Phi_3(-3u^2) = \Phi_6(3u^2) = (3u^2 + 3u + 1)(3u^2 - 3u + 1)$$

- $p = 3^{2m+1} = 3u^2,\ r = 3u^2 + 3u + 1,\ t = 3u$

Factorisation patterns in pairing-friendly curves

Galbraith, McKee and Valença patterns [GMV07]:

- $\Phi_{12}(6u^2) = r(u)r(-u)$, $r(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1$
  $\to$ Barreto–Naehrig curves
- $\Phi_{12}(2u^2) = r(u)r(-u)$, $r(u) = 4u^4 + 4u^3 + 2u^2 + 2u + 1$
- $\Phi_5(5u^2) = \Phi_{10}(-5u^2) = r(u)r(-u)$,
  $r(u) = 25u^4 + 25u^3 + 15u^2 + 5u + 1$
  $\to$ Freeman curves

Cunningham project[1]

Aim: factor large integers $b^n \pm 1$, where $b \in \{2, 3, 5, 6, 7, 10, 11, 12\}$

- algebraic factorisation: $b^n - 1 = \prod_{d|n} \Phi_d(b)$
- Aurifeuillean factorisation for matching b, n

Aurifeuillean factorisation Aurifeuille, Schinzel, Brent, Stevenhagen

$k > 1$ integer, $\Phi_k(u)$ k-th cyclotomic polynomial. Let a be a square-free integer and u an integer. Then $\Phi_k(au^2)$ will factor if

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

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

Brezing-Weng construction [BW05]

Input: Embedding degree k, square-free $D > 0$ s.t. $-D$ square in $\mathbb{Q}(\zeta_k)$

$r(u) \leftarrow \Phi_k(u)$

$s(u) \leftarrow \sqrt{-D} \bmod r(u)$, i.e. $1/s^2(u) = -D \bmod r(u)$

for e *in* $1, \ldots, k-1$, $\gcd(e,k) = 1$ **do**

  $t(u) = u^e + 1 \bmod r(u)$

  $y(u) = (t(u) - 2)/s(u) \bmod r(u)$

  $p(u) = (t^2(u) + Dy^2(u))/4$

  if $p(u)$ *represents primes and leading coeff*$(r) > 0$ **then**

    return k, D, r, t, y, p

  end

end

Issues:

- very small choice of D
- $p(u)$ not irreducible, or never takes prime integer values

Aurifeuillean pairing-friendly curves

Modification of Brezing-Weng construction:
Look for $a \in \{-2k, -2k-1, ..., 2k\}$ s.t. $\Phi_k(au^2) = r(u)r(-u)$ has Aurifeuillean factorisation, continue with $r(u)$ and $t(u) = (au^2)^e + 1 \bmod r(u)$, $\gcd(e, k) = 1$.

Example: $k = 9$

$\Phi_9(-3u^2) = r(u)r(-u)$ where $r(u) = 27u^6 + 9u^3 + 1$
Take $D = 3$: three families:
$t = (-3u^2)^2 + 1,\ (-3u^2)^5 + 1,\ (-3u^2)^8 + 1 \bmod r(u)$

$$\begin{aligned} t_1(u) &= -18u^4 - 3u + 1 = (-3u^2)^5 + 1 \bmod r(u) \\ y_1(u) &= -6u^3 + u - 1 \\ p_1(u) &= 81u^8 + 27u^6 + 27u^5 - 18u^4 + 9u^3 + 3u^2 - 3u + 1 \end{aligned}$$

And $\rho = \deg p / \deg r = 4/3$ as good as former construction.

Our construction for $k = 2 \cdot 3^j$

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

Take $a = 3$:

$$\Phi_{2\cdot 3^j}(3u^2) = \Phi_{3^j}(-3u^2) = r(u)r(-u)$$

where $r(u) = 3^{m/2}u^m + 3^{(m+2)/4}u^{m/2} + 1$.
Take $D = 3$: $1\sqrt{-3} = 2 \cdot 3^{(m-2)/4}u^{m/2} + 1 \bmod r(u)$.
Continue Brezing-Weng with r, D

$$\rightarrow \text{minimise } \max(\deg t(u), \deg y(u)).$$

Odd j:
$e \in \{(m+2)/4,\ m + (m+2)/4,\ 2m + (m+2)/4\}$
$\rho = (m+2)/m = (k+6)/k$

Any j:
$e \in \{1,\ 1+m,\ 1+2m\}$
$\rho = (m+4)/m = (k+12)/k$

And so for k=54...

$$\Phi_{54}(3u^2) = (1 + 3^5u^9 + 3^9u^{18})(1 - 3^5u^9 + 3^9u^{18})$$

- Choose $r(u) = 1 + 3^5u^9 + 3^9u^{18}$
- $D = 3$
- $m = 2k/3 = 18$
- $e = (m + 2)/4 = 5$
- So $t(u) = 1 + (3u^2)^5 = 1 + 3^5u^{10}$
- $y(u) = 3^5u^{10} + 2.3^4.u^9 + 2u + 1$
- $p(u) = (t(u)^2 + 3y(u)^2)/4 = 1 + 3u + 3u^2 + 3^5u^9 + 3^5u^{10} + 3^6u^{10} + 3^6u^{11} + 3^9u^{18} + 3^{10}u^{19} + 3^{10}u^{20}$
- $\rho = (k + 6)/k = 10/9$

Conclusion

- Mystery solved!
- So our new discovery was indeed just one member of a family of families of PFCs
- New families with competitive ρ for $k \in \{9, 15, 21, 30, 33, 39, 42, 45, 51, 54, 57, 66, 69, 75, 78, 81, 87, 90, 93\}$
- Not applicable for $8 \mid k$ (no Aurifeuillean factorisation)
- The new $k = 54$ case could be of future use for 256-bit security (maybe better than BLS-48?)
- Nice alternate construction for $k = 9$

References I

Razvan Barbulescu and Sylvain Duquesne.
Updating key size estimations for pairings.
Journal of Cryptology, Jan 2018.

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.

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. Springer-Verlag, 2006.

References II

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.

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.

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.

References III

Andrew Granville and Peter Pleasants.

Aurifeuillian factorization.

Math. Comp., 75(253):497–508, 2006.

https://doi.org/10.1090/S0025-5718-05-01766-7.

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-Based Cryptography - Pairing 2013 - 6th International Conference, Beijing, China, November 22-24, 2013, Revised Selected Papers*, volume 8365 of *LNCS*, pages 45–61. Springer, 2013.

https://eprint.iacr.org/2013/582.

References IV

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.

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.

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.

References V

N. El Mrabet and M. Joye, editors.
Guide to Pairing-Based Cryptography.
Chapman and Hall/CRC, 2016.

A. Miyaji, M. Nakabayashi, and S. Takano.
New explicit conditions of elliptic curve traces for FR-reduction.
IEICE Transactions on Fundamentals, E84-A(5):1234–1243, 2001.

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.

References VI

O. Schirokauer.
The number field sieve for integers of low weight.
Cryptography ePrint Archive, Report 2006/107, 2006.
http://eprint.iacr.org/2006/107.