On Pairing-Friendly Elliptic Curves

Edlyn Teske
University of Waterloo

Toronto, 14 May 2009

Reference:

David Freeman, Michael Scott and Edlyn Teske,
A taxonomy of pairing-friendly elliptic curves.

52 pages, 2006-2009.

Cryptology ePrint Archive: Report 2006/372
(continuously updated)
To appear in Journal of Cryptology

Contents of the “taxonomy paper”:

- Description of all constructions of pairing-friendly curves known to date (May 2009), and a coherent framework for them.

- Several new constructions with improved ρ-values for certain embedding degrees.

- Construction to obtain families with good ρ-value (< 2) and variable CM discriminant.

- Recommendation of curves for various security levels and performance requirements.

This talk:

a (strict) subset of the above.

As this is a “retrospective meeting” ....

......let's look at a few major achievements over 2.5 years.........

October 30, 2006......

........the first day of

“Computational challenges arising in algorithmic number theory and cryptography”

here at the Fields Institute:

$2\frac{1}{2}$ years later.....

......April 25, 2009:

On Pairing-Friendly Elliptic Curves

Edlyn Teske
University of Waterloo

Toronto, 14 May 2009

Pairing-friendly:
An elliptic curve E/F_q with small *embedding degree* and large prime-order subgroup.

Embedding degree:
Let $E/\mathbb{F}_q$ and assume $r|\#E(\mathbb{F}_q)$,
where $\gcd(r,q)=1$.
The *embedding degree of* E *with respect to* r is

- the smallest $k \in \mathbb{N}$ such that $\mathbb{F}_{q^k}$ contains all r-th roots of unity;

- the smallest $k \in \mathbb{N}$ such that $r|(q^k-1)$.

Embedding degree – Comments

- If $E/\mathbb{F}_q$ has embedding degree k with respect to r, then
$$E[r] \subseteq E(\mathbb{F}_{q^k}).$$

- Weil pairing:
$$e_r : E[r] \times E[r] \to \mu_r \subseteq \mathbb{F}_{q^k}^* \ .$$

- If $E/\mathbb{F}_q$ is supersingular
($\#E(\mathbb{F}_q) = q + 1 - t$ with $\gcd(q, t) > 1$):
Then $1 \leq k \leq 6$.

  (Frey-Rück attack,
Menezes-Okamoto-Vanstone attack).

Why?

- The Weil and Tate pairings are building blocks for a host of exciting public-key protocols, such as
  - short signatures,
  - ID-based cryptography,
  - group signatures,
  - certificateless cryptography,
  - ....
- k needs to be small so that pairings are efficiently computable.
  Recall: A pairing maps into $\mathbb{F}_{q^k}$, where q has 160 or more bits.

Small embedding degrees are rare!

- We need $\mu_r \subset \mathbb{F}_{q^k}$.
- For a random curve, expect $k \approx r$.

Balasubramanian and Koblitz (1998):

For a random curve $E/\mathbb{F}_q$ (q a prime),
having a prime number r of points,
the probability that r divides $q^k - 1$ for some

$$k \leq \log^2 q$$

is **vanishingly small**.

Illustration:
q 160-bit prime $\Longrightarrow \log^2 q \approx 12300$.
$k \leq 12300$ with probability less than 10^{-28}.

We'd like $k \leq 50$.
But we may allow $\#E(\mathbb{F}_q)$ to be composite.

Definition: pairing-friendly [FST]

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. We say that E is *pairing-friendly* if

1. there is a prime $r \geq \sqrt{q}$ dividing $\#E(\mathbb{F}_q)$, and

2. the embedding degree of E with respect to r is less than $(\log_2 r)/8$.

Pairing-friendly − Comments:

1. $r|\#E(\mathbb{F}_q)$ where $r > \sqrt{q}$:

   Curves with small embedding degree with respect to r are abundant if $r < \sqrt{q}$ and quite rare if $r > \sqrt{q}$ [Luca-Shparlinski, 2006].

   Define: $\rho = \dfrac{\log q}{\log r}$.

   So $1 - \varepsilon \leq \rho \leq 2$ for pairing-friendly curves.

2. $\mu_r \subseteq \mathbb{F}^*_{q^k}$ with $k < \dfrac{\log_2 r}{8}$:

   Embedding degrees of practical interest in pairing-based applications depend on the desired security level. The bound $(\log_2 r)/8$ is chosen to *roughly* reflect the bounds on k given on the next slide.

Bit sizes of curve parameters and corresponding embedding degrees for commonly desired levels of security.

Security level (in bits)	Subgroup size r (in bits)	Extension field size q^k (in bits)	Embedding degree k	
			$\rho \approx 1$	$\rho \approx 2$
80	160	960 − 1280	6 − 8	3 − 4
112	224	2200 − 3600	10 − 16	5 − 8
128	256	3000 − 5000	12 − 20	6 − 10
192	384	8000 − 10000	20 − 26	10 − 13
256	512	14000 − 18000	28 − 36	14 − 18

(Matching the security levels of SKIPJACK, Triple-DES, AES-Small, AES-Medium, and AES-Large, respectively.)

Complex Multiplication (CM) Method

Assume q is prime.

Input: $\mathbb{F}_q$, $N = q + 1 - t$ $\qquad (|t| \leq 2\sqrt{q})$,

$D > 0$ such that **(CM norm equation)**

$$4q - t^2 = Dy^2$$

where D squarefree (*CM discriminant*).

Output: $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = N$

(and End(E) $\cong$ order in $\mathbb{Q}(\sqrt{-D})$).

Necessary:

D relatively small, e.g. $D < 10^{12} \approx 2^{40}$.
(Very unlikely for 160-bit q and "random" t.)

Theorem:

An elliptic curve over $\mathbb{F}_q$ of embedding degree k, with a subgroup of prime order r and with trace t can be constructed if and only if

(1) q is prime or a prime power.

(2) r is prime.

(3) r divides $q + 1 - t$.

(4) r divides $q^k - 1$, and
r does not divide $q^i - 1$ for $1 \leq i < k$.

(5) $4q - t^2 = Dy^2$ for some sufficiently small positive integer D and some integer y.

If r does not divide k, then condition (4) is equivalent with

(4') r divides $\Phi_k(t - 1)$.

Families of pairing-friendly curves: [FST]
We say the triple

$$(r(x), t(x), q(x)) \in \mathbb{Q}[x]$$

is a **family** of pairing-friendly elliptic curves (with embedding degree k and discriminant D) if

1. $q(x) = p(x)^d$, and $p(x)$ *represents primes*.

2. $r(x)$ is non-constant, irreducible, and integer-valued, and has positive leading coefficient.

3. $r(x)$ divides $q(x) + 1 - t(x)$.

4. $r(x)$ divides $\Phi_k(t(x) - 1)$.

5. $4q(x) - t(x)^2 = Dy^2$ has **infinitely many** integer solutions (x, y).

The ρ-value of a family

Recall: $\rho = \dfrac{\log q}{\log r}$.

For a family:

$$\rho(r,t,q) = \lim_{x\to\infty} \frac{\log q(x)}{\log r(x)} = \frac{\deg q(x)}{\deg r(x)}.$$

Example of a family:
Barreto-Nährig curves [BN2005]

$(r(x), t(x), q(x))$ where

$$\begin{aligned} r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ t(x) &= 6x^2 + 1, \\ q(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1. \end{aligned}$$

A family of curves with embedding degree $k = 12$ and ρ-value 1.

BN curves have CM discriminant 3.

In fact:

$$4q(x) - t^2(x) = 3y^2(x)$$

where $y(x) = 6x^2 + 4x + 1$.

The BN family is a **complete** family.

A family (r, t, q) is **complete** if there is some

$$y(x) \in \mathbb{Q}[x]$$

such that

$$4q(x) - t(x)^2 = Dy(x)^2.$$

Otherwise, we say that the family is **sparse**:
The CM equation only has solutions for some set of (x, y) (that grows exponentially).

Example of a sparse family: MNT curves
(Miyaji, Nakabayashi and Takano, 2001).
Case $k = 6$:
$(r(x), t(x), q(x))$ where

$$\begin{aligned} r(x) &= 4x^2 \mp 2x + 1, \\ t(x) &= 1 \pm 2x, \\ q(x) &= 4x^2 + 1. \end{aligned}$$

Solving the CM equation $4q(x) - t(x)^2 = Dy^2$ can be shown equivalent to solving the "MNT equation"

$$X^2 - 3DY^2 = -8,$$

a generalized Pell equation.

Back to complete families

A complete family (r, t, q) with k, D is **cyclotomic** if

- $r(x) = \Phi_l(x)$ for some $l = sk$, and
- and $\sqrt{-D} \in K := \mathbb{Q}[x]/(r(x))$.

(Brezing-Weng 2005; Barreto-Lynn-Scott 2002)

A complete family (r, t, q) with k, D is **sporadic** if

- $K = \mathbb{Q}[x]/(r(x))$ is a (perhaps trivial) extension of a cyclotomic field,

- $r(x)$ is not a cyclotomic polynomial,

- $\sqrt{-D} \in K$.

Example: Barreto-Nährig curves form a sporadic family: $\Phi_{12}(6x^2) = r(x)r(-x)$.

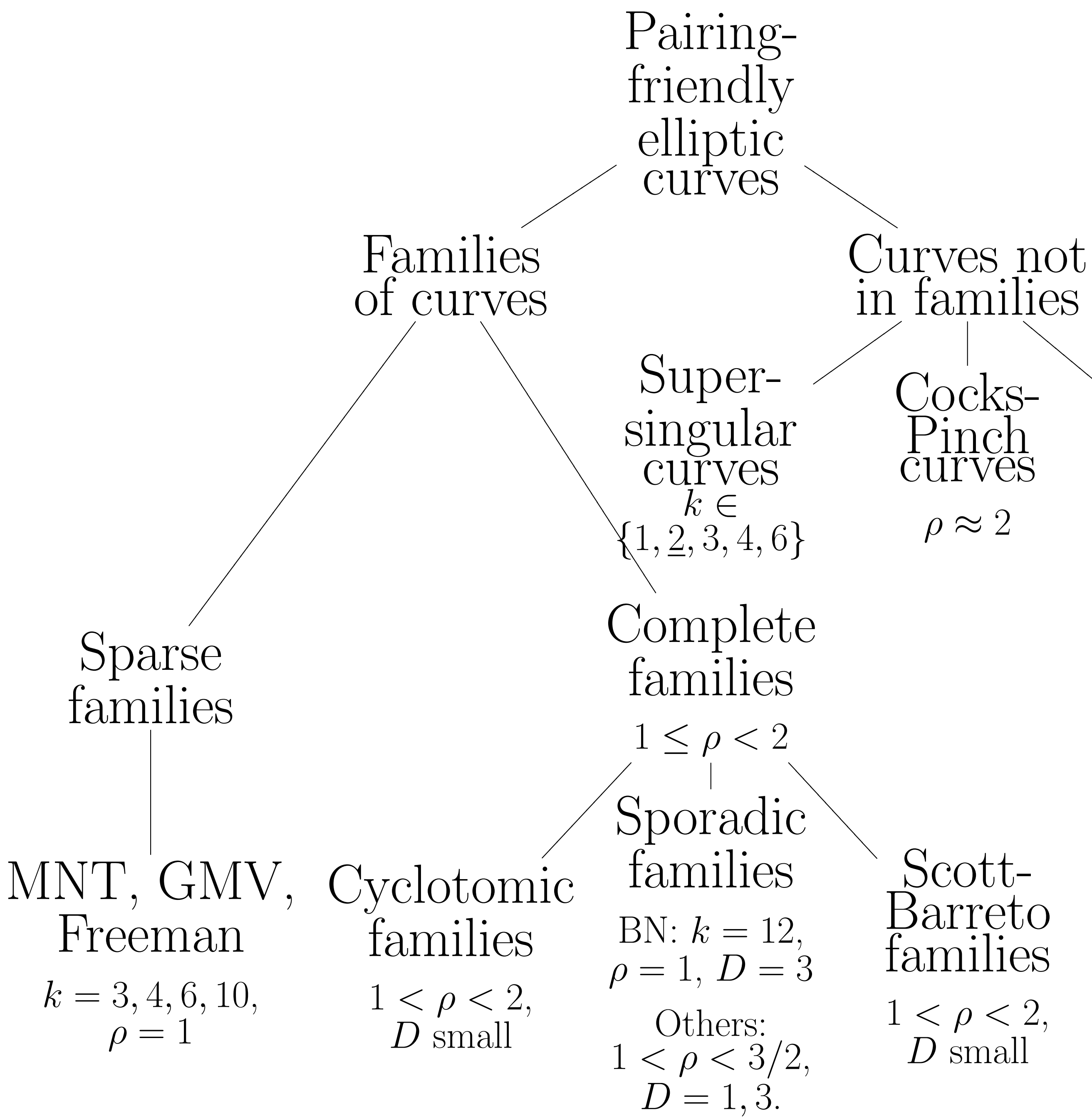
(Also: Kachisa-Schaefer-Scott 2008)

We speak of a **Scott-Barreto** family if

- $K = \mathbb{Q}[x]/(r(x))$ is an extension of a cyclotomic field,

- $\sqrt{-D} \notin K$.

Classification of pairing-friendly elliptic curves



Cocks-Pinch curves (manuscript, 2001):

- Fix $k \geq 1$ and squarefree $D > 0$.

- Let r be a prime with $k | (r-1)$ and $\left(\frac{-D}{r}\right) = 1$.

  Let ζ_k be a primitive kth root of unity in $(\mathbb{Z}/r\mathbb{Z})^*$.

  So, $\sqrt{-D}, \zeta_k \in (\mathbb{Z}/r\mathbb{Z})^*$.

- Let $t' = \zeta_k + 1$, let $y' = \frac{\zeta_k - 1}{\sqrt{-D}}$ mod r.

- Let $0 < t, y \leq r$ such that
  $t \equiv t' \pmod{r}$ and $y \equiv y' \pmod{r}$.

- Let $q = \frac{1}{4}(t^2 + Dy^2)$.

- If q is an integer and prime, use CM method to construct curve $E/\mathbb{F}_q$ with $q + 1 - t$ points.

Cock-Pinch method – Discussion

- Works for all embedding degrees k.

- Relative freedom to choose r and D.

- Recall: $t = \zeta_k + 1 \bmod r$ and $y = \frac{\zeta_k - 1}{\sqrt{(-D)}} \bmod r$

  so $t, y \approx r$ and $q = \frac{1}{4}(t^2 + Dy^2) \approx r^2$.

  $\Longrightarrow \rho = \dfrac{\log q}{\log r} \approx 2.$

- CP is the **method of choice** if $\rho \approx 2$ is acceptable.

The CP construction has been generalized

- to produce complete (cyclotomic) families of curves with $\rho < 2$ [Brezing-Weng, 2005].

- to produce pairing-friendly abelian varieties of arbitrary dimension $g \geq 2$ [Freeman, 2007; Freeman-Stevenhagen-Streng, 2008].

Example of a cyclotomic family
– Brezing-Weng construction.

Let $k = 5$. Let

$$r(x) = \Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1,$$

and $K = Q[x]/(\Phi_{20}(x))$. Then $\zeta_5, \sqrt{-1} \in K$.
So let's work with $D = 1$.
In K, ζ_5 represents as $-x^2$, so (use $t = \zeta_k + 1$)

$$t(x) = -x^2 + 1.$$

In K, $\sqrt{-1}$ represents as x^5, so
(use $y = \frac{\zeta_k - 1}{\sqrt{-D}} = -(\zeta_k - 1)\sqrt{-D}$)

$$y(x) = x^7 + x^5,$$

and (use $q = \frac{1}{4}(t^2 + Dy^2)$)

$$q(x) = \frac{1}{4}(x^{14} + 2x^{12} + x^{10} + x^4 - 2x^2 + 1),$$

irreducible.

(r, t, q) is a complete family of elliptic curves of embedding degree $k = 5$, with CM discriminant $D = 1$, and with ρ-value $14/8 = 1.75$.

The issue of small discriminants......

- Barreto-Naehrig curves ($k = 12$, $\rho = 1$) have discriminant $D = 3$.

- For complete families, $D = 1, 3$ are the most common working choices.

Some people love such small D.....:

- $D = 3 \Longrightarrow E/\mathbb{F}_q$ has sextic twist $\longrightarrow$ great for implementing pairings if k is divisible by 6. (Evaluate pairing in $\mathbb{F}_{q^{k/6}}$ rather than $\mathbb{F}_{q^k}$).

.....but others may not like small D:

- Speed-up for Pollard's rho method for curves with $D = 1, 3$ (making use of automorphism groups of order 4,6 (respectively)
  [Duursma-Gaudry-Morain,1999].
  $\longrightarrow$ decrease in security by a few bits.
  By a few bits only. But: A warning sign?!

Koblitz (2002): *Good and bad uses of elliptic curves in cryptography*:

> "All parameters for a cryptosystem must always be chosen with the maximal possible degree of randomness, because any extra structure or deviation from randomness might some day be used to attack the system."

Pairing-friendly curves with variable discriminant

Theorem: [FST]

Let (r, t, q) be a family of elliptic curves with embedding degree k and discriminant D.

Let $K = \mathbb{Q}[x]/(r(x))$.
Let $y(x) \mapsto (\zeta_k - 1)/\sqrt{-D}$ in K.

Suppose r, t, and q are even polynomials, and y is an odd polynomial.

Define $r' \in \mathbb{Z}[x]$ and $t', q', y' \in Q[x]$ such that

$$r(x) = r'(x^2), \qquad t(x) = t'(x^2), \qquad q(x) = q'(x^2),$$
$$y(x) = x \cdot y'(x^2).$$

Let $\alpha \in \mathbb{N}$ such that

- αD is squarefree
- $r'(\alpha x^2)$ is irreducible
- $y'(\alpha x^2) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$
- $q'(\alpha x^2)$ irreducible

Theorem: [FST]

Let (r, t, q) be a family of elliptic curves with embedding degree k and discriminant D.

Let $K = \mathbb{Q}[x]/(r(x))$.
Let $y(x) \mapsto (\zeta_k - 1)/\sqrt{-D}$ in K.

Suppose r, t, and q are even polynomials, and y is an odd polynomial.

Define $r' \in \mathbb{Z}[x]$ and $t', q' \in Q[x]$ such that

$$r(x) = r'(x^2), \qquad t(x) = t'(x^2), \qquad q(x) = q'(x^2),$$
$$y(x) = x \cdot y'(x^2).$$

Let $\alpha \in \mathbb{N}$ such that

- αD is squarefree
- $r'(\alpha x^2)$ is irreducible
- $y'(\alpha x^2) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$
- $q'(\alpha x^2)$ irreducible

Then $(r'(\alpha x^2), t'(\alpha x^2), q'(\alpha x^2))$ is a complete family of elliptic curves with embedding degree k and discriminant αD, and the same ρ-value as the family (r, t, q).

Example: Our cyclotomic family with $k = 5$:

$r(x) = \Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1,$
$t(x) = -x^2 + 1,$
$q(x) = \frac{1}{4}(x^{14} + 2x^{12} + x^{10} + x^4 - 2x^2 + 1),$
$y(x) = x^7 + x^5.$

For any **odd** integer α, define
$r'(\alpha x^2) = \alpha^4 x^8 - \alpha^3 x^6 + \alpha^2 x^4 - \alpha x^2 + 1,$
$t'(\alpha x^2) = -\alpha x^2 + 1,$
$q'(\alpha x^2) =$
$\quad \frac{1}{4}(\alpha^7 x^{14} + 2\alpha^6 x^{12} + \alpha^5 x^{10} + \alpha^2 x^4 - 2\alpha x^2 + 1).$

Then $(r'(\alpha x^2), t'(\alpha x^2), q'(\alpha x^2))$ is a complete family with $k = 5$ and $D = \alpha$, and $\rho = 1.75$.

Hm......

So, $r'(\alpha x^2) = \Phi_{10}(\alpha x^2)$.

We have seen in the case of BN curves, that $\Phi_{12}(6x^2)$ is reducible.....

So, how can we be sure that $r'(\alpha x^2)$ and $q'(\alpha x^2)$ are irreducible?

Theorem: [FST]

Let $k \in \mathbb{N}$, let α be a squarefree integer that does not divide k. Then $\Phi_k(\alpha x^2)$ is irreducible.

More generally:

Theorem: [FST]

Let $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ be irreducible. Let α be a square-free integer that does not divide $a_0 a_d$ disc(f). Then $f(\alpha x^2)$ is irreducible.

Our example:

$r_\alpha(x) = \Phi_{10}(\alpha x^2)$ is irreducible if α is squarefree and does not divide 10.

Further, let

$f(x) = 4q'(x) = x^7 + 2x^6 + x^5 + x^2 - 2x + 1.$

Then disc(f) $= -9477104 = -2^4 \cdot 7 \cdot 13 \cdot 23 \cdot 283.$

So $q'(\alpha x^2)$ is irreducible if α is squarefree and does not divide 592319.

(Recall: We needed α to be odd as well.)

Remarks on variable discriminants:

- The variable-discriminant construction does not apply to BN curves.
  For example,
  $$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$
  is not an even polynomial.

- The construction works for all k with $\gcd(k, 24) \in \{1, 2, 3, 6, 12\}$.

  That is, $k \not\equiv 0 \pmod 4$ or k divisible by 3 but not divisible by 8.

  It also works for $k = 28, 44$ but not for $k = 20$.

- Given a complete family $(r'(\alpha x^2), t'(\alpha x^2), q'(\alpha x^2))$, find explicit pairing-friendly curves:
  - choose $\alpha < 10^{10}$ and vary x of the right size until $r'(\alpha x^2)$ and $q'(\alpha x^2)$ are both prime.
  - **or:** choose x and vary α of the right size ...... [Comuta-Kawazoe-Takahashi, 2007]

Conclusion

- We presented a complete classification of pairing-friendly elliptic curves,
  with several explicit examples.

- We presented a construction to obtain complete families of pairing-friendly curves of variable discriminant.

- We did NOT cover implementation considerations such as:
  twists and compression, extension field arithmetic, low Hamming weight.
  See e.g. Michael Scott's *Pairing 2007* paper "Implementing cryptographic pairings"

- We did NOT cover our recommendations, on which construction to use for a given embedding degree.
  See Tables 8.1 and 8.2 of our paper "A taxonomy of pairing-friendly elliptic curves".