Pairing-Friendly Elliptic Curves of Prime Order

Paulo S. L. M. Barreto[1] Michael Naehrig[2]

[1]University of São Paulo
pbarreto@larc.usp.br

[2]RWTH Aachen University
mnaehrig@ti.rwth-aachen.de

SAC 2005

Outline

- Constructing pairing-friendly curves (review)
  - prime order, but restricted to $k \leq 6$
  - general k, but $\rho = {}^{\log p}/_{\log r} \approx 2$
  - selected values of $k > 6$, best result $\rho \approx \frac{5}{4}$
- New method: curves of prime order and $k = 12$
  - construction
  - twisted pairings
  - point and pairing compression

Pairing-Friendly Curves

- An elliptic curve is *pairing-friendly* if it contains a subgroup of (large) prime order r such that
  - $r \mid p^k - 1$,
  - $r \nmid p^i - 1$ for $0 < i < k$,

  where k is
  - small enough that arithmetic on $\mathbb{F}_{p^k}$ is feasible,
  - large enough that the DLP on $\mathbb{F}_{p^k}^*$ is about as intractable as the ECDLP on $E(\mathbb{F}_p)[r]$.

Pairing-Friendly Curves

- An elliptic curve is *pairing-friendly* if it contains a subgroup of (large) prime order r such that
  - $r \mid p^k - 1$,
  - $r \nmid p^i - 1$ for $0 < i < k$,

  where k is
  - small enough that arithmetic on $\mathbb{F}_{p^k}$ is feasible,
  - large enough that the DLP on $\mathbb{F}_{p^k}^*$ is about as intractable as the ECDLP on $E(\mathbb{F}_p)[r]$.

- Unfortunately, k is usually too large (special construction needed).

Complex Multiplication (CM)

- The goal:
  Find p, n ($p > 3$ prime) and $a, b \in \mathbb{F}_p$ s.t.
  the elliptic curve $E : y^2 = x^3 + ax + b$
  has order $\#E(\mathbb{F}_p) = n$
  (and trace of the Frobenius $t = p + 1 - n$).

- Prerequisite:
  The CM norm equation $DV^2 = 4p - t^2$ must be satisfied with moderate CM discriminant D.

Some Constructions

- Miyaji-Nakabayashi-Takano (2001)
  use the fact that $n \mid \Phi_k(p)$ to parametrise p, n and t,
  for $k \in \{3, 4, 6\}$ the CM norm equation reduces to a
  Pell equation $DV^2 = 4n(u) - (t(u) - 2)^2$.
- Restriction: unable to handle larger k
  (norm equation at least quartic).

Some Constructions

- Miyaji-Nakabayashi-Takano (2001)
  use the fact that $n \mid \Phi_k(p)$ to parametrise p, n and t, for $k \in \{3, 4, 6\}$ the CM norm equation reduces to a Pell equation $DV^2 = 4n(u) - (t(u) - 2)^2$.
- Restriction: unable to handle larger k
  (norm equation at least quartic).

- Cocks-Pinch (2002)
  unpublished algorithm based on the property that
  $r \mid n = p + 1 - t$ and $r \mid p^k - 1$.
  $\Rightarrow t - 1$ is a primitive k-th root of unity mod r.
- Restriction: usually $\rho = {}^{\log p}/_{\log r} \approx 2$.

Algebraic Constructions

- Barreto-Lynn-Scott (2002), Brezing-Weng (2003)
- For certain values of k and D there exist closed-form parametrisations for families of curves with known equations.
  (e.g. $k = 2^i 3^j$ and $D = 3$, or $k = 2^i 7^j$ and $D = 7$)

Algebraic Constructions

- Barreto-Lynn-Scott (2002), Brezing-Weng (2003)
- For certain values of k and D there exist closed-form parametrisations for families of curves with known equations.
  (e.g. $k = 2^i 3^j$ and $D = 3$, or $k = 2^i 7^j$ and $D = 7$)
- Advantages: ρ closer to 1.
  (best case: $\rho = \frac{5}{4}$ for $k = 8$ and $D = 3$)

Algebraic Constructions

- Barreto-Lynn-Scott (2002), Brezing-Weng (2003)
- For certain values of k and D there exist closed-form parametrisations for families of curves with known equations.
  (e.g. $k = 2^i 3^j$ and $D = 3$, or $k = 2^i 7^j$ and $D = 7$)
- Advantages: ρ closer to 1.
  (best case: $\rho = \frac{5}{4}$ for $k = 8$ and $D = 3$)
- Limitations: solutions known only for small D and curve order always composite (ρ still 'large').

The Problem

- Boneh-Lynn-Shacham (2001)
  - Original challenge: how to build pairing-friendly curves with $k > 6$?
  - Modified challenge: how to build pairing-friendly curves of prime order with $k > 6$?
- Suggested lower bound: $k = 10$

Extending the MNT Approach

- Galbraith-McKee-Valença (2004) start from the property $n \mid \Phi_k(p)$ and parametrise $p(u)$ such that
$$\Phi_k(p(u)) = n_1(u)n_2(u).$$

Extending the MNT Approach

- Galbraith-McKee-Valença (2004) start from the property $n \mid \Phi_k(p)$ and parametrise $p(u)$ such that
$$\Phi_k(p(u)) = n_1(u)n_2(u).$$
- Leads to conditions on quadratic $p(u)$ s.t. the factors of $\Phi_k(p(u))$ are quartic for $k \in \{5, 8, 10, 12\}$.

Extending the MNT Approach

- Galbraith-McKee-Valença (2004)
  start from the property $n \mid \Phi_k(p)$ and parametrise $p(u)$ such that
  $$\Phi_k(p(u)) = n_1(u)n_2(u).$$
- Leads to conditions on quadratic $p(u)$ s.t. the factors of $\Phi_k(p(u))$ are quartic for $k \in \{5, 8, 10, 12\}$.
- Result: families of genus 2 curves similar to MNT elliptic curves.

Extending the MNT Approach

- NB: $p(u)$ must be a prime (or prime power).
- Some conditions cannot lead to solutions:
  for $k = 12$ the parametrisation $p(u) = 6u^2$ will never produce a prime power.

Extending the MNT Approach

- NB: $p(u)$ must be a prime (or prime power).
- Some conditions cannot lead to solutions: for $k = 12$ the parametrisation $p(u) = 6u^2$ will never produce a prime power.
- How about changing the strategy?

New Strategy

- Start from $n \mid \Phi_k(t(u) - 1)$ and parametrise $t(u)$ s.t. $\Phi_k(t(u) - 1)$ splits into quartic factors $n_1(u)n_2(u)$.
- The only restriction on $t(u)$ is the Hasse bound. Since $n(u)$ is quartic, $t(u)$ must be at most quadratic for $k \in \{5, 8, 10, 12\}$.

New Strategy

- Start from $n \mid \Phi_k(t(u) - 1)$ and parametrise $t(u)$ s.t. $\Phi_k(t(u) - 1)$ splits into quartic factors $n_1(u)n_2(u)$.
- The only restriction on $t(u)$ is the Hasse bound. Since $n(u)$ is quartic, $t(u)$ must be at most quadratic for $k \in \{5, 8, 10, 12\}$.
- Most conditions do not lead to a favourable factorisation of the norm equation

$$DV^2 = 4n(u) - (t(u) - 2)^2.$$

New Curves

- The condition $t(u) = 6u^2 + 1$ does lead to a favourable factorisation for $k = 12$.

$$\Phi_k(t(u) - 1) = n(u)n(-u).$$

- Parameters:

$$\begin{aligned} n(u) &= 36u^4 + 36u^3 + 18u^2 + 6u + 1 \\ p(u) &= 36u^4 + 36u^3 + 24u^2 + 6u + 1 \\ DV^2 &= 4p - t^2 = 3(6u^2 + 4u + 1)^2 \end{aligned}$$

NB: $u \in \mathbb{Z} \setminus \{0\}$ (positive or negative values).

New Curves

- Since $D = 3$, the curve equation has the form

$$E(\mathbb{F}_p) : y^2 = x^3 + b,$$

  with $b > 0$ adjusted to attain the right order. (A simple sequential search quickly finds a suitable b.)

- NB: the method always produces $p \equiv 1 \pmod 3$ (no supersingular curves).

Twisted Pairings

- There exists a sextic twist $E'(\mathbb{F}_{p^2})$ and an injective group homomorphism

$$\psi : E'(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^{12}}).$$

Twisted Pairings

- There exists a sextic twist $E'(\mathbb{F}_{p^2})$ and an injective group homomorphism

$$\psi : E'(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^{12}}).$$

- Define a twisted pairing

$$\hat{e} : E(\mathbb{F}_p) \times E'(\mathbb{F}_{p^2}) \longrightarrow \mathbb{F}_{p^{12}}, \quad \hat{e}(P, Q) = e(P, \psi(Q)).$$

Twisted Pairings

- There exists a sextic twist $E'(\mathbb{F}_{p^2})$ and an injective group homomorphism

$$\psi : E'(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^{12}}).$$

- Define a twisted pairing

$$\hat{e} : E(\mathbb{F}_p) \times E'(\mathbb{F}_{p^2}) \longrightarrow \mathbb{F}_{p^{12}}, \quad \hat{e}(P, Q) = e(P, \psi(Q)).$$

- The field arithmetic needed for non-pairing operations is restricted to $\mathbb{F}_{p^2}$ instead of $\mathbb{F}_{p^{k/2}}$.
- The homomorphism is only needed when actually computing pairings.

Compressed Pairings

- Pairing compression is possible with ratio $\frac{1}{3}$ in a way that naturally integrates with point compression.
- Instead of reducing a point $(x', y') \in E'(\mathbb{F}_{p^2})$ to its x-coordinate, discard it and keep only the y-coordinate. Recovering (x', y') creates ambiguity between three possible values of x'.

Compressed Pairings

- Pairing compression is possible with ratio $\frac{1}{3}$ in a way that naturally integrates with point compression.
- Instead of reducing a point $(x', y') \in E'(\mathbb{F}_{p^2})$ to its x-coordinate, discard it and keep only the y-coordinate. Recovering (x', y') creates ambiguity between three possible values of x'.

- The three points that share the same y-coordinate are conjugates, as are the pairing values computed on them (provided the points are n-torsion points).
- The trace of all three pairing values is the same $\mathbb{F}_{p^4}$ value.

Point Compression

- Discard one more bit of y', i.e. do not distinguish between y' and $-y'$.
- Keep only the information to represent an equivalence class $\{(x', \pm y'), (\zeta_3 x', \pm y'), (\zeta_3^2 x', \pm y')\}$.

Point Compression

- Discard one more bit of y', i.e. do not distinguish between y' and $-y'$.
- Keep only the information to represent an equivalence class $\{(x', \pm y'), (\zeta_3 x', \pm y'), (\zeta_3^2 x', \pm y')\}$.

- The $\mathbb{F}_{p^2}$-traces of the pairing values of all six points in the class are equal.
- Obtain a unique compressed pairing value over $\mathbb{F}_{p^2}$.

Point Compression

- Discard one more bit of y', i.e. do not distinguish between y' and $-y'$.
- Keep only the information to represent an equivalence class $\{(x', \pm y'), (\zeta_3 x', \pm y'), (\zeta_3^2 x', \pm y')\}$.

- The $\mathbb{F}_{p^2}$-traces of the pairing values of all six points in the class are equal.
- Obtain a unique compressed pairing value over $\mathbb{F}_{p^2}$.

- Represent points in $E'(\mathbb{F}_{p^2})$ with less than $\log(p^2)$ bits.
- Pairing compression with ratio $\frac{1}{6}$ may be possible.

Work in Progress

- Reduce the loop length similar to the η_T pairing.
  Use a space-time tradeoff, see Scott (2005).
  Simplify the final powering.

Work in Progress

- Reduce the loop length similar to the η_T pairing. Use a space-time tradeoff, see Scott (2005). Simplify the final powering.

- Security assessment of certain features, e.g. sparse curve orders correspond to sparse field sizes - attacks may be possible, but their relevance is uncertain.

More Open Problems

- How to build pairing-friendly curves of genus $g \in \{1, 2, 3, 4\}$ and prime order for $k/g < 32$ and $\varphi(k) > 4$ over a field $\mathbb{F}_{p^m}$?
- Are there any real security problems with small D? Can we handle really large D?
- Lots of other problems …

Thank you!