Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10

David Freeman

University of California, Berkeley, USA

ANTS-VII, 2006

Outline

1. Introduction
   - Pairings in Cryptography
   - Embedding Degrees: The Problem and Current Results
2. Constructing Curves with Prescribed Embedding Degree
   - The CM Method: The Basic Construction
   - The CM Method: Generating Families of Curves
3. Curves with Embedding Degree 10
   - The Construction
   - Computational Results

Outline

Pairings in Cryptography

- Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$.
- For any integer r the *Weil pairing* e_r is a bilinear map sending pairs of points with order r to r-th roots of unity in $\overline{\mathbb{F}}_q$:

$$e_r \colon E[r] \times E[r] \to \mu_r.$$

- These pairings can been used in many cryptographic constructions, including:
  - one-round, 3-way key agreement (Joux);
  - short signature schemes (Boneh, Lynn, Shacham);
  - identity-based encryption (Boneh, Franklin);
  - and many others.

Making Pairings Practical

- For pairing-based cryptosystems to be practical and secure, we require:
  - the discrete logarithm in the order-r subgroup of $E(\mathbb{F}_q)$ to be computationally infeasible;
  - the discrete logarithm in μ_r to be computationally infeasible;
  - the pairing to be easily computable (i.e. μ_r lies in a low-degree extension of $\mathbb{F}_q$).
- To optimize applications, we want to choose a curve E so that the two discrete log problems are of about equal difficulty.

Outline

Embedding Degrees

- Let E be an elliptic curve over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = r$.
- Let k be the smallest integer such that $\mu_r \subset \mathbb{F}_{q^k}^\times$ (i.e. $r \mid q^k - 1$).
    - Bal., Kob.: $E[r] \subset E(\mathbb{F}_{q^k})$, so the Weil pairing "embeds" $E(\mathbb{F}_q)$ into $\mathbb{F}_{q^k}^\times$.
    - k is the *embedding degree* of E (with respect to r).
- Note: k is the order of q in $(\mathbb{Z}/r\mathbb{Z})^\times$.
    - For "random" curves, $k \sim r \sim q$.

The Problem

- The problem: find primes q and elliptic curves $E/\mathbb{F}_q$ of prime order r with small embedding degree ($k \leq 30$).
  - Want to be able to control the number of bits of q to construct curves for various applications.
  - Could also look for curves E with nearly prime order – $\#E(\mathbb{F}_q) =$ large prime $r \times$ small cofactor.
- Requirement that $E(\mathbb{F}_q)$ has prime order is what makes the problem difficult.
  - Cocks, Pinch: Constructed E with arbitrary embedding degree k, but largest prime factor of $\#E(\mathbb{F}_q) \sim \sqrt{q}$.

Previous Results

- Menezes, Okamoto, Vanstone, 1993 (MOV): Showed that supersingular elliptic curves always have embedding degree $k \leq 6$.
- Miyaji, Nakabayashi, Takano, 2001 (MNT): Gave complete characterization of ordinary elliptic curves of prime order with embedding degree $k = 3, 4, 6$.
- Barreto, Naehrig, 2005: Constructed a family of elliptic curves of prime order and embedding degree 12.

The Main Result

- D.F., 2006: Constructed elliptic curves of prime order with embedding degree 10.
  - Solves open problem posed by Boneh, Lynn, Shacham, 2001.

Outline

The CM Method of Curve Construction

- Main tool: Complex Multiplication method of curve construction (Atkin, Morain).
  - For given $D > 0$, constructs elliptic curve with CM by $\mathbb{Q}(\sqrt{-D})$.
  - Constructs curves with specified number of points.
  - Running time roughly $O(D)$.
- How it works: Fix D, k. Look for t, n, q (representing trace, number of points, and size of field) satisfying
  1. q, n prime;
  2. $n = q + 1 - t$ (formula for number of points);
  3. n divides $q^k - 1$ (embedding degree k);
  4. $Dy^2 = 4q - t^2$ for some integer y.
- For such t, n, q, if D is not too large ($\sim 10^9$) we can construct an elliptic curve E over $\mathbb{F}_q$ with n points and embedding degree k.

Outline

Observations about the CM Method

- Barreto, Lynn, Scott: The embedding degree condition $n \mid q^k - 1$ can be replaced with $n \mid \Phi_k(t-1)$, where Φ_k is the k-th cyclotomic polynomial.
  - k smallest such that $n \mid q^k - 1$ implies $n \mid \Phi_k(q)$.
  - $q + 1 - t = n$ implies $q = t - 1 \pmod{n}$.
- Barreto, Naehrig: Parametrize t, n, q as polynomials: $t(x), n(x), q(x)$. Construct curves by finding integer solutions to

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

Extending the CM Method

- Combine these observations to get an algorithm for generating families of pairing-friendly curves:
  1. Fix D, k, and choose a polynomial $t(x)$.
  2. Choose $n(x)$ an irreducible factor of $\Phi_k(t(x) - 1)$.
  3. Find integer solutions (x, y) to $Dy^2 = 4n(x) - (t(x) - 2)^2$.
  4. If $q(x)$, $n(x)$ are both prime, construct elliptic curve over $\mathbb{F}_{q(x)}$ with $n(x)$ points.
- Step 3 is the difficult part: if $f(x) = 4n(x) - (t(x) - 2)^2$ has degree ≥ 3, then $Dy^2 = f(x)$ (usually) has only a finite number of integer solutions! (Siegel's Theorem)

Outline

Embedding Degree 10: The Key Observation

- Goal: Choose $t(x)$, choose $n(x)$ an irreducible factor of $\Phi_{10}(t(x)-1)$, such that $4n(x)-(t(x)-2)^2$ is quadratic.
  - $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$ degree 4.
  - All irred. factors of $\Phi_{10}(t(x)-1)$ must have $4 \mid$ degree.
- Key observation: Need to choose $n(x)$, $t(x)$ such that the leading terms of $4n$ and t^2 cancel out.
  - Smallest possible case: $\deg n = 4$, $\deg t = 2$.
- Galbraith, McKee, Valença: Characterized quadratic $t(x)$ such that $\Phi_{10}(t(x)-1)$ factors into two quartics.
- One of these $t(x)$ gives the desired cancellation!

Choice of Parameters

- Choose t, n, q as follows:

$$\begin{aligned} t(x) &= 10x^2 + 5x + 3 \\ n(x) &= 25x^4 + 25x^3 + 15x^2 + 5x + 1 \\ q(x) &= 25x^4 + 25x^3 + 25x^2 + 10x + 3 \end{aligned}$$

- Then $n(x)$ divides $\Phi_{10}(t(x) - 1)$, and

$$f(x) = 4n(x) - (t(x) - 2)^2 = 15x^2 + 10x + 3.$$

Constructing the Curves

- To find curves: set $D' = 15D$, $u = 15x + 5$, complete the square in $Dy^2 = 15x^2 + 10x + 3$ to get

$$u^2 - D'y^2 = -20.$$

- Find integer solutions (u, y) to this Pell-like equation. (Use LMM algorithm.)
- Let $x = (u - 5)/15$. If $q(x)$ and $n(x)$ are prime, there exists an elliptic curve with embedding degree 10!
- If no solutions of appropriate size, or $q(x)$ or $n(x)$ not prime, increase D and try again.

Outline

General Results (Thanks to Mike Scott)

- Searched for curves with $D < 2 \cdot 10^9$, q between 148 and 512 bits.
  - Crypto applications: want $q \sim$ 220-250 bits (discrete log in $E(\mathbb{F}_q)$ about as difficult as discrete log in $\mathbb{F}_{q^{10}}$).
- Found 23 curves of prime order with embedding degree 10.
- Found 101 curves of nearly prime order (large prime $\times$ small cofactor $< 2^{16}$) and embedding degree 10.
- Ability to handle larger D in CM Method would allow us to find more curves.

Example: A 234-bit Curve (Computed by Mike Scott)

- Set $D = 1227652867$.
- Compute solution (x, y) to $Dy^2 = 15x^2 + 10x + 3$.
- Use this value of x to compute

$$
\begin{aligned}
t &= 269901098952705059670276196260897153 \\
n &= 18211650803969472064493264347375949776033155743952030750450033782306651 \\
q &= 18211650803969472064493264347375950045934254696657090420726230043203803
\end{aligned}
$$

- Use CM method to compute curve equation over $\mathbb{F}_q$:
  (Given t, n, q, curve equation took about a week to compute.)

$$y^2 = x^3 - 3x + 15748668094913401184777964473522859086900831274922948973320684995903275.$$

- This curve has n points and embedding degree 10!

Selected References I

- P.S.L.M. Barreto, M. Lynn, M. Scott, “Constructing elliptic curves with prescribed embedding degrees,” *SCN 2002*.
- P.S.L.M. Barreto, M. Naehrig, “Pairing-friendly elliptic curves of prime order,” *SAC 2005*.
- I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography* and *Advances in Elliptic Curve Cryptography*, LMS Lecture Notes, 1999 & 2005.
- S. Galbraith, J. McKee, P. Valença, “Ordinary abelian varieties having small embedding degree,” *Proc. WS Math. Problems and Techniques in Crypto.*, 2005.

Selected References II

- A. Menezes, T. Okamoto, S. Vanstone, ”Reducing elliptic curve logarithms to logarithms in a finite field,” *IEEE Trans. Info. Theory*, 1993.
- A Miyaji, M. Nakabayashi, S. Takano, “Reducing elliptic curve logarithms to logarithms in a finite field,” *IEICE Trans. Fundamaentals*, 2001.
- F. Morain, ”Building cyclic elliptic curves modulo large primes,” *EUROCRYPT 1991*.