Constructing Pairing-Friendly Genus 2 Curves with Ordinary Jacobians

David Freeman

University of California, Berkeley, USA

First International Conference on Pairing-Based Cryptography

Tokyo, Japan
3 July 2007

Outline

1. Pairings on Abelian Varieties
   - Pairings in Cryptography
   - Pairing-Friendly Abelian Varieties
2. The Genus 2 CM Method
   - Complex Multiplication
   - Constructing Curves from Igusa Invariants
3. Constructing Pairing-Friendly Genus 2 Curves
   - Constraints on the parameters
   - The Algorithm
   - Extending the Algorithm

Outline

1. Pairings on Abelian Varieties
   - Pairings in Cryptography
   - Pairing-Friendly Abelian Varieties
2. The Genus 2 CM Method
   - Complex Multiplication
   - Constructing Curves from Igusa Invariants
3. Constructing Pairing-Friendly Genus 2 Curves
   - Constraints on the parameters
   - The Algorithm
   - Extending the Algorithm

Pairings on Abelian Varieties

- Let A be a abelian variety defined over a finite field $\mathbb{F}_q$.
  - e.g., elliptic curve, or Jacobian of a hyperelliptic curve.
- For any integer r the *Weil pairing* e_r is a bilinear map sending pairs of points of order r to r-th roots of unity in $\overline{\mathbb{F}}_q$:

$$e_r : A[r] \times A[r] \to \mu_r.$$

- The *Tate pairing* is analogous.
- These pairings have been used in many cryptographic constructions, described in this conference and elsewhere.

Making Pairings Practical

- For pairing-based cryptosystems to be practical and secure, we require:
  1. the discrete logarithm in the order-r subgroup of $A(\mathbb{F}_q)$ to be computationally infeasible;
  2. the discrete logarithm in μ_r to be computationally infeasible;
  3. 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 so that the two discrete log problems are of about equal difficulty.
- The *embedding degree* quantifies this concept.

Embedding Degrees

- Let r be a prime number.
- Let A be an abelian variety over $\mathbb{F}_q$ with $r \mid \#A(\mathbb{F}_q)$.
- Let k be the smallest integer such that $\mu_r \subset \mathbb{F}_{q^k}^\times$ (i.e., such that $r \mid q^k - 1$).
  - The Weil pairing can be used to embed $A(\mathbb{F}_q)[r]$ into $\mathbb{F}_{q^k}^\times$.
  - k is the *embedding degree* of A (with respect to r).
- Equivalently, k is the order of q in $(\mathbb{Z}/r\mathbb{Z})^\times$.
  - For "random" curves, $k \sim r$.
  - If r is large ($\sim 2^{160}$), random A will have embedding degree too large to be practical.

The Problem

- The problem: find primes q and abelian varieties $A/\mathbb{F}_q$ having
  1. a subgroup of large prime order r, and
  2. prescribed (small) embedding degree with respect to r.
     - In practice, want $r > 2^{160}$ and $k \leq 50$.
- We call such varieties "pairing-friendly."
- Want to be able to control the number of bits of q to construct varieties for various applications.

Previous Results

- Pairing-friendly elliptic curves well-studied. (See survey article by F.-Scott-Teske.)
- Two-dimensional abelian varieties (abelian surfaces) are more mysterious.
  - Can be described as Jacobians of genus 2 curves.
- Rubin-Silverberg: supersingular abelian surfaces have $k \leq 12$.
  - Description made more explicit by Cardona-Nart.
  - Supersingular abelian surfaces easy to construct.
- Galbraith-McKee-Valença, Hitt: Demonstrated existence of non-supersingular abelian surfaces with small embedding degree.
  - Unable to construct surfaces explicitly.

The Main Result: Our Algorithm

- Input: a prime r and an embedding degree k.
  - e.g., $r = 2011 = \texttt{NextPrime}(2007)$, $k = 10$.
- Output: a prime q and a genus 2 curve C over $\mathbb{F}_q$.
  - e.g., $q = 27185091709621$, $C : y^2 = x^5 + 18$.
- If $A = \text{Jac}(C) = \text{Pic}^0(C)$ is the Jacobian of C, then
  1. A is ordinary.
     - In this case, equivalent to $q \equiv 1 \pmod 5$.
  2. $A(F_q)$ has a subgroup of order r.

     $$\#A(\mathbb{F}_q) = 739028832225496605008350416 \equiv 0 \pmod r$$
  3. A has embedding degree k with respect to r.
     - $q^{10} \equiv 1 \pmod r$

Outline

1. Pairings on Abelian Varieties
   - Pairings in Cryptography
   - Pairing-Friendly Abelian Varieties
2. The Genus 2 CM Method
   - Complex Multiplication
   - Constructing Curves from Igusa Invariants
3. Constructing Pairing-Friendly Genus 2 Curves
   - Constraints on the parameters
   - The Algorithm
   - Extending the Algorithm

Frobenius Endomorphism and CM fields

- Let A be an abelian surface over $\mathbb{F}_q$.
- The Frobenius endomorphism of A is a root of a polynomial

$$h(x) = x^4 - sx^3 + tx^2 - sqx + q^2$$

  (the "characteristic polynomial of Frobenius").
- A is ordinary $\Leftrightarrow \gcd(t, q) = 1$.
- If $h(x)$ is irreducible, $K = \mathbb{Q}[x]/(h(x))$ is a degree-4 number field, called a *CM field*. (We say A has *CM by K*.)
- Any such K can be written as

$$K = \mathbb{Q}\left(\sqrt{-a + b\sqrt{d}}\right),$$

  for some $a, b, d > 0$ with $a^2 - b^2 d > 0$.

From Frobenius to Genus 2 Curve

- Pairing-friendly property of A is determined by properties of $h(x)$ modulo r.
- Problem: given an $h(x)$ with pairing-friendly properties, construct an abelian surface A with characteristic polynomial of Frobenius $h(x)$.
- Equivalently: construct a genus 2 curve C whose Jacobian has CM by $K = \mathbb{Q}[x]/(h(x))$.
- Solution: Igusa invariants and Igusa class polynomials.

Genus 2 Invariant Theory

- Igusa invariants: triple of numbers (j_1, j_2, j_3) that classify a genus 2 curve C up to isomorphism.
  - Analogous to j-invariant of elliptic curve.
- Igusa class polynomials for K: polynomials $H_1, H_2, H_3 \in \mathbb{Q}[x]$ whose roots are the Igusa invariants of genus 2 curves (over $\mathbb{C}$) whose Jacobians have CM by K.
  - Analogous to Hilbert class polynomial for elliptic curve.
- Fact: Igusa invariants of curves over $\mathbb{F}_q$ whose Jacobians have CM by K are roots mod q of Igusa class polynomials for K.

Constructing Genus 2 Curves

- To construct curve $C/\mathbb{F}_q$ whose Jacobian has CM by K: compute Igusa class polynomials for K, take triples of roots mod q as Igusa invariants for C.
  - Mestre: algorithm to construct C from its Igusa invariants.
- Major obstacle: Igusa class polynomials can only be computed for very small CM fields K.
- Solution: Fix K in advance, construct $h(x)$ such that $K \cong \mathbb{Q}[x]/h(x)$.

Outline

1. Pairings on Abelian Varieties
   - Pairings in Cryptography
   - Pairing-Friendly Abelian Varieties
2. The Genus 2 CM Method
   - Complex Multiplication
   - Constructing Curves from Igusa Invariants
3. Constructing Pairing-Friendly Genus 2 Curves
   - Constraints on the parameters
   - The Algorithm
   - Extending the Algorithm

Determining the CM Field

- Given $K = \mathbb{Q}\left(\sqrt{-a + b\sqrt{d}}\right)$, want to compute $h(x) = x^4 - sx^3 + tx^2 - sqx + q^2$ with $K \cong \mathbb{Q}[x]/(h(x))$.
- The field $\mathbb{Q}[x]/(h(x))$ is isomorphic to $\mathbb{Q}(\eta)$, where

$$\eta = \sqrt{\left(\frac{s^2}{2} - t - 2q\right) + s\sqrt{\frac{s^2}{4} - t + 2q}}.$$

  (Apply the quadratic formula twice.)
- To guarantee $\mathbb{Q}(\eta) = K$, set

$$\begin{aligned} -a &= \frac{s^2}{2} - t - 2q \\ b &= s \\ d &= \frac{s^2}{4} - t + 2q \end{aligned}$$

Adding Degrees of Freedom

- Problem: once we impose conditions on s, t, q to make A pairing-friendly, we don't have enough degrees of freedom to find a solution.
- Solution: use the isomorphism

$$\mathbb{Q}\left(\sqrt{-a+b\sqrt{d}}\right) \cong \mathbb{Q}\left(\sqrt{(u+v\sqrt{d})^2(-aw^2+b\sqrt{dw^4})}\right).$$

- Now we have

$$\begin{aligned} \frac{s^2}{2} - t - 2q &= -w^2(au^2 + adv^2 + 2bduv) &(1)\\ s &= bu^2 + bdv^2 + 2auv &(2)\\ \frac{s^2}{4} - t + 2q &= dw^4. &(3) \end{aligned}$$

with 6 degrees of freedom (q, s, t, u, v, w).

Making *A* Pairing-Friendly

- To guarantee that A has embedding degree k with respect to a subgroup of order r, we require:

$$q^2 - s(q+1) + t + 1 \equiv 0 \pmod{r} \quad (4)$$

$$\Phi_k(q) \equiv 0 \pmod{r} \quad (5)$$

  where Φ_k is the kth cyclotomic polynomial.
- (1)-(5) give 5 equations in 6 variables.
- We find solutions mod r to all 5, and choose different lifts to integers until the value of q is prime.

The Algorithm

1. Fix prime subgroup size r, embedding degree k, and CM field $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$.
2. Fix $v' \in \mathbb{F}_r$, and find solutions $q', s', t', u', w' \in \mathbb{F}_r$ to equations (1)-(5).
   - If no solutions, choose different v'.
3. Let $u_0, v_0, w_0 \in \mathbb{Z}$ be representatives for u', v', w' in $[0, r)$.
4. Choose small integers i_1, i_2, i_3, let $u = u_0 + i_1 r$, $v = v_0 + i_2 r$, $w = w_0 + i_3 r$.
5. Solve equations (1)-(3) in integers for q, s, t.
   - If no integer solutions or if q not prime, choose different i_1, i_2, i_3.
6. Return q and $h(x) = x^4 - sx^3 + tx^2 - sqx + q^2$.

The Final Result

- Given q and $h(x)$ output by the algorithm, can use Igusa class polynomials to construct curve $C/\mathbb{F}_q$ whose Jacobian has characteristic polynomial of Frobenius $h(x)$.
- Theorem: $\text{Jac}(C)$ has embedding degree k with respect to r.

Extending the Algorithm

- Group of r-torsion points on an abelian surface A is $\cong (\mathbb{Z}/r\mathbb{Z})^4$.
- Our algorithm gives A with
  - one dimension of r-torsion defined over $\mathbb{F}_q$,
  - one dimension of r-torsion defined over $\mathbb{F}_{q^k}$,
  - other two dimensions uncontrolled.
- Future applications may require 3 or 4 linearly independent points with small embedding degree.
- Modify algorithm: add one more constraint on q, s, t; produce A with 4 dimensions of r-torsion defined over $\mathbb{F}_{q^k}$.

Composite-Order Groups

- Algorithm can also be modified to produce A that is pairing-friendly with respect to composite-order $r = r_1 r_2$.
  - See Dan Boneh's talk yesterday.
- Solve equations (1)-(5) modulo r_1 and r_2 independently; combine via Chinese remainder theorem.

Improving the ρ-value

- For abelian variety A of dimension g over $\mathbb{F}_q$, define a parameter

$$\rho = \frac{\log q^g}{\log r}.$$

- Since $\#A \approx q^g$, ρ measures ratio of pairing-friendly subgroup size to entire group size (in bits).
  - Want ρ small for maximum efficiency. (Minimum is 1.)
- Our algorithm produces ρ-values around 8.
  - $\rho = 8.13$ in the example above.
- Major open problem: produce pairing-friendly ordinary abelian surfaces with $\rho \leq 2$.
  - Find genus 2 analogues of Miyaji-Nakabayashi-Takano or Brezing-Weng methods.