Constructing Pairing-Friendly Ordinary Genus 2 Curves

David Freeman

University of California, Berkeley, USA

Crypto 2007 Rump Session
21 August 2007

(Result originally presented at Pairing 2007, Tokyo, Japan)

The Problem

- All pairings proposed for cryptography make use of abelian varieties (e.g., elliptic curves) over finite fields.
  - e.g., Weil pairing on order-r points of $A/\mathbb{F}_q$:

$$e\colon A[r] \times A[r] \to \mathbb{F}_{q^k}^{\times}.$$

- k is the *embedding degree* of A (with respect to r).
- If r is large, random A will have embedding degree too large to be practical.
- 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.

The Problem

- All pairings proposed for cryptography make use of abelian varieties (e.g., elliptic curves) over finite fields.
  - e.g., Weil pairing on order-r points of $A/\mathbb{F}_q$:

$$e\colon A[r] \times A[r] \longrightarrow \mathbb{F}_{q^k}^{\times}.$$

- k is the *embedding degree* of A (with respect to r).
- If r is large, random A will have embedding degree too large to be practical.
- 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.

The Problem

- All pairings proposed for cryptography make use of abelian varieties (e.g., elliptic curves) over finite fields.
  - e.g., Weil pairing on order-r points of $A/\mathbb{F}_q$:

$$e\colon A[r] \times A[r] \longrightarrow \mathbb{F}_{q^k}^{\times}.$$

- k is the *embedding degree* of A (with respect to r).
- If r is large, random A will have embedding degree too large to be practical.
- 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.

The Problem

- All pairings proposed for cryptography make use of abelian varieties (e.g., elliptic curves) over finite fields.
  - e.g., Weil pairing on order-r points of $A/\mathbb{F}_q$:

$$e\colon A[r] \times A[r] \longrightarrow \mathbb{F}_{q^k}^{\times}.$$

- k is the *embedding degree* of A (with respect to r).
- If r is large, random A will have embedding degree too large to be practical.
- 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.

The Problem

- All pairings proposed for cryptography make use of abelian varieties (e.g., elliptic curves) over finite fields.
  - e.g., Weil pairing on order-r points of $A/\mathbb{F}_q$:

$$e\colon A[r] \times A[r] \longrightarrow \mathbb{F}_{q^k}^{\times}.$$

- k is the *embedding degree* of A (with respect to r).
- If r is large, random A will have embedding degree too large to be practical.
- 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.

The Problem

- All pairings proposed for cryptography make use of abelian varieties (e.g., elliptic curves) over finite fields.
  - e.g., Weil pairing on order-r points of $A/\mathbb{F}_q$:

$$e\colon A[r] \times A[r] \longrightarrow \mathbb{F}_{q^k}^{\times}.$$

- k is the *embedding degree* of A (with respect to r).
- If r is large, random A will have embedding degree too large to be practical.
- 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.

The Problem

- All pairings proposed for cryptography make use of abelian varieties (e.g., elliptic curves) over finite fields.
  - e.g., Weil pairing on order-r points of $A/\mathbb{F}_q$:

$$e\colon A[r] \times A[r] \longrightarrow \mathbb{F}_{q^k}^{\times}.$$

- k is the *embedding degree* of A (with respect to r).
- If r is large, random A will have embedding degree too large to be practical.
- 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.

The CM Method for Abelian Surfaces

- Number of points on an ordinary abelian surface $A/\mathbb{F}_q$ (Jacobian of genus 2 curve) can be related to a "quartic CM field" $\mathbb{Q}(\sqrt{-a+b\sqrt{d}})$, $a, b, d > 0$:

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

  for some $s, t, u, v, w \in \mathbb{Z}$.

- Describing this relationship explicitly is one of our primary contributions.

The CM Method for Abelian Surfaces

- Number of points on an ordinary abelian surface $A/\mathbb{F}_q$ (Jacobian of genus 2 curve) can be related to a "quartic CM field" $\mathbb{Q}(\sqrt{-a+b\sqrt{d}})$, $a, b, d > 0$:

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

  for some $s, t, u, v, w \in \mathbb{Z}$.
- Describing this relationship explicitly is one of our primary contributions.

The Algorithm (modeled on Cocks-Pinch)

1. Fix prime subgroup size r, embedding degree k, and CM field $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$.
2. Find a solution mod r to a system of 5 equations in 6 variables q, s, t, u, v, w:
   - 1 equation to guarantee a subgroup of order r;
   - 1 equation to guarantee embedding degree k;
   - 3 "CM equations" from previous slide.
3. Lift the solution to $\mathbb{Z}$ such that q is prime.
4. Use "Igusa class polynomials" for K to construct the equation for $A/\mathbb{F}_q$.
   - Can only do this if K is small.

The Algorithm (modeled on Cocks-Pinch)

1. Fix prime subgroup size r, embedding degree k, and CM field $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$.
2. Find a solution mod r to a system of 5 equations in 6 variables q, s, t, u, v, w:
   - 1 equation to guarantee a subgroup of order r;
   - 1 equation to guarantee embedding degree k;
   - 3 "CM equations" from previous slide.
3. Lift the solution to $\mathbb{Z}$ such that q is prime.
4. Use "Igusa class polynomials" for K to construct the equation for $A/\mathbb{F}_q$.
   - Can only do this if K is small.

The Algorithm (modeled on Cocks-Pinch)

1. Fix prime subgroup size r, embedding degree k, and CM field $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$.
2. Find a solution mod r to a system of 5 equations in 6 variables q, s, t, u, v, w:
   - 1 equation to guarantee a subgroup of order r;
   - 1 equation to guarantee embedding degree k;
   - 3 "CM equations" from previous slide.
3. Lift the solution to $\mathbb{Z}$ such that q is prime.
4. Use "Igusa class polynomials" for K to construct the equation for $A/\mathbb{F}_q$.
   - Can only do this if K is small.

The Algorithm (modeled on Cocks-Pinch)

1. Fix prime subgroup size r, embedding degree k, and CM field $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$.
2. Find a solution mod r to a system of 5 equations in 6 variables q, s, t, u, v, w:
   - 1 equation to guarantee a subgroup of order r;
   - 1 equation to guarantee embedding degree k;
   - 3 "CM equations" from previous slide.
3. Lift the solution to $\mathbb{Z}$ such that q is prime.
4. Use "Igusa class polynomials" for K to construct the equation for $A/\mathbb{F}_q$.
   - Can only do this if K is small.

The Algorithm (modeled on Cocks-Pinch)

1. Fix prime subgroup size r, embedding degree k, and CM field $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$.
2. Find a solution mod r to a system of 5 equations in 6 variables q, s, t, u, v, w:
   - 1 equation to guarantee a subgroup of order r;
   - 1 equation to guarantee embedding degree k;
   - 3 “CM equations” from previous slide.
3. Lift the solution to $\mathbb{Z}$ such that q is prime.
4. Use “Igusa class polynomials” for K to construct the equation for $A/\mathbb{F}_q$.
   - Can only do this if K is small.

The Algorithm (modeled on Cocks-Pinch)

1. Fix prime subgroup size r, embedding degree k, and CM field $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$.
2. Find a solution mod r to a system of 5 equations in 6 variables q, s, t, u, v, w:
   - 1 equation to guarantee a subgroup of order r;
   - 1 equation to guarantee embedding degree k;
   - 3 “CM equations” from previous slide.
3. Lift the solution to $\mathbb{Z}$ such that q is prime.
4. Use “Igusa class polynomials” for K to construct the equation for $A/\mathbb{F}_q$.
   - Can only do this if K is small.

The Algorithm (modeled on Cocks-Pinch)

1. Fix prime subgroup size r, embedding degree k, and CM field $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$.
2. Find a solution mod r to a system of 5 equations in 6 variables q, s, t, u, v, w:
   - 1 equation to guarantee a subgroup of order r;
   - 1 equation to guarantee embedding degree k;
   - 3 “CM equations” from previous slide.
3. Lift the solution to $\mathbb{Z}$ such that q is prime.
4. Use “Igusa class polynomials” for K to construct the equation for $A/\mathbb{F}_q$.
   - Can only do this if K is small.

The Algorithm (modeled on Cocks-Pinch)

1. Fix prime subgroup size r, embedding degree k, and CM field $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$.
2. Find a solution mod r to a system of 5 equations in 6 variables q, s, t, u, v, w:
   - 1 equation to guarantee a subgroup of order r;
   - 1 equation to guarantee embedding degree k;
   - 3 “CM equations” from previous slide.
3. Lift the solution to $\mathbb{Z}$ such that q is prime.
4. Use “Igusa class polynomials” for K to construct the equation for $A/\mathbb{F}_q$.
   - Can only do this if K is small.

Results

- First explicit construction of ordinary abelian surfaces over finite fields with prescribed embedding degree.
  - Previously: only supersingular surfaces (Rubin-Silverberg) and existence results for ordinary surfaces (Galbraith-McKee-Valença, Hitt).
- Algorithm gives $q \sim r^4$.
  - Ideally $q \sim \sqrt{r}$.
  - Improve by generalizing Miyaji-Nakabayashi-Takano or Brezing-Weng methods?
- Algorithm can be modified to produce bilinear groups of composite order (Boneh-Goh-Nissim).

Results

- First explicit construction of ordinary abelian surfaces over finite fields with prescribed embedding degree.
  - Previously: only supersingular surfaces (Rubin-Silverberg) and existence results for ordinary surfaces (Galbraith-McKee-Valença, Hitt).
- Algorithm gives $q \sim r^4$.
  - Ideally $q \sim \sqrt{r}$.
  - Improve by generalizing Miyaji-Nakabayashi-Takano or Brezing-Weng methods?
- Algorithm can be modified to produce bilinear groups of composite order (Boneh-Goh-Nissim).

Results

- First explicit construction of ordinary abelian surfaces over finite fields with prescribed embedding degree.
  - Previously: only supersingular surfaces (Rubin-Silverberg) and existence results for ordinary surfaces (Galbraith-McKee-Valença, Hitt).
- Algorithm gives $q \sim r^4$.
  - Ideally $q \sim \sqrt{r}$.
  - Improve by generalizing Miyaji-Nakabayashi-Takano or Brezing-Weng methods?
- Algorithm can be modified to produce bilinear groups of composite order (Boneh-Goh-Nissim).

Results

- First explicit construction of ordinary abelian surfaces over finite fields with prescribed embedding degree.
  - Previously: only supersingular surfaces (Rubin-Silverberg) and existence results for ordinary surfaces (Galbraith-McKee-Valença, Hitt).
- Algorithm gives $q \sim r^4$.
  - Ideally $q \sim \sqrt{r}$.
  - Improve by generalizing Miyaji-Nakabayashi-Takano or Brezing-Weng methods?
- Algorithm can be modified to produce bilinear groups of composite order (Boneh-Goh-Nissim).

Results

- First explicit construction of ordinary abelian surfaces over finite fields with prescribed embedding degree.
  - Previously: only supersingular surfaces (Rubin-Silverberg) and existence results for ordinary surfaces (Galbraith-McKee-Valença, Hitt).
- Algorithm gives $q \sim r^4$.
  - Ideally $q \sim \sqrt{r}$.
  - Improve by generalizing Miyaji-Nakabayashi-Takano or Brezing-Weng methods?
- Algorithm can be modified to produce bilinear groups of composite order (Boneh-Goh-Nissim).

Results

- First explicit construction of ordinary abelian surfaces over finite fields with prescribed embedding degree.
  - Previously: only supersingular surfaces (Rubin-Silverberg) and existence results for ordinary surfaces (Galbraith-McKee-Valença, Hitt).
- Algorithm gives $q \sim r^4$.
  - Ideally $q \sim \sqrt{r}$.
  - Improve by generalizing Miyaji-Nakabayashi-Takano or Brezing-Weng methods?
- Algorithm can be modified to produce bilinear groups of composite order (Boneh-Goh-Nissim).

For More Information

To learn more about this construction, you could:

- Read the full paper (IACR eprint 2007/057);
- See my web page (`http://math.berkeley.edu/~dfreeman`);
- Hire me as a postdoc for 2008-09.

For More Information

To learn more about this construction, you could:

- Read the full paper (IACR eprint 2007/057);
- See my web page (`http://math.berkeley.edu/~dfreeman`);
- Hire me as a postdoc for 2008-09.

For More Information

To learn more about this construction, you could:

- Read the full paper (IACR eprint 2007/057);
- See my web page (`http://math.berkeley.edu/~dfreeman`);
- Hire me as a postdoc for 2008-09.