Constructing Abelian Varieties for Pairing-Based Cryptography

David Freeman

Stanford University, USA

Foundations of Computational Mathematics:
Workshop on Computational Number Theory
24 June 2008

What is pairing-based cryptography?

- "Pairing-based cryptography" refers to protocols that use a nondegenerate, bilinear map

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

  between finite, cyclic groups.
- Need *discrete logarithm problem* (DLP) in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ to be infeasible.
- DLP: Given x, x^a, compute a.

Example: Boneh-Lynn-Shacham signatures

- Setup:
  - Bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.
  - Public $P, Q \in \mathbb{G}_1$.
  - Secret $a \in \mathbb{Z}$ such that $Q = P^a$.
  - Hash function $H : \{0,1\}^* \to \mathbb{G}_2$.
- Signature on message m is $\sigma = H(m)^a$.
- To verify signature: see if $e(Q, H(m)) = e(P, \sigma)$.
  - If signature is correct, then both equal $e(P, H(m))^a$.
  - If DLP is infeasible, then signature cannot be forged.

Useful pairings: Abelian varieties over finite fields

- For certain abelian varieties $A/\mathbb{F}_q$, subgroups of $A(\mathbb{F}_q)$ of prime order r have the necessary properties.
- Pairings are *Weil pairing*

$$e_{weil,r} : A[r] \times A[r] \to \mu_r \subset \mathbb{F}_{q^k}^\times$$

  or *Tate pairing* (more complicated).
- k is the *embedding degree* of A with respect to r.
    - Smallest integer such that $\mu_r \subset \mathbb{F}_{q^k}^\times$ ($\Leftrightarrow q^k \equiv 1 \bmod r$).
- If q, r are large, DLP is infeasible in $A[r]$ and $\mathbb{F}_{q^k}^\times$.
- Pairings can be computed efficiently via Miller's algorithm.

Need to "balance" security on variety and in finite field

- Best DLP algorithm in $A[r]$ is exponential-time.
- Best DLP algorithm in $\mathbb{F}_{q^k}^{\times}$ is subexponential-time.
- For comparable security before and after pairing, need $q^k > r$.
- How much larger depends on desired security level:

Common security levels for elliptic curves

r (bits)	q^k (bits)	Embedding degree k (if $r \approx q$)	Secure until year
160	1024	6	2010
224	2048	10	2030
256	3072	12	2050

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 k 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 r to construct varieties at varying security levels.

"Random" abelian varieties not useful for pairing-based cryptography

- Embedding degree of random $A/\mathbb{F}_q$ with order-r subgroup will be $\approx r$.
- Typical $r \approx 2^{160}$, so pairing on random A can't even be computed.
- Conclusion: pairing-friendly abelian varieties are "special."

Some types of pairing-friendly abelian varieties

- Menezes-Okamoto-Vanstone, Galbraith, Rubin-Silverberg: *supersingular* $A/\mathbb{F}_q$ are always pairing-friendly.
  - If dimension $g \leq 6$ then $k \leq 7.5g$.
  - These k are only acceptable for the lowest security levels.
  - Higher security levels require non-supersingular (usually, *ordinary*) abelian vareities.
- Pairing-friendly ordinary elliptic curves (g = 1) well-studied.
  - Many constructions with small k and $q < r^2$.
  - Can construct elliptic curves with $k \in \{3, 4, 6, 10, 12\}$ and prime order ($q \approx r$).

Higher dimensions: more difficult

- Galbraith-McKee-Valença, Hitt: existence results for non-supersingular pairing-friendly abelian surfaces ($g = 2$)
  - No explicit construction.
- F. '07: explicit construction of ordinary abelian surfaces with arbitrary embedding degree.
- Kawazoe-Takahashi: construct ordinary abelian surfaces over smaller fields, but not absolutely simple.

Algorithms for constructing pairing-friendly A.V.

- Result #1 (ANTS-VIII, with P. Stevenhagen & M. Streng)
  - Method for constructing primes q and ordinary $A/\mathbb{F}_q$ that have a subgroup of order r and prescribed embedding degree k.
  - Works for abitrary k, nearly arbitrary r.
  - Field sizes are large.
    - Best cases: $q \approx r^4$ for $\dim A = 2$, $q \approx r^6$ for $\dim A = 3$.
- Result #2 (Pairing '08)
  - Method for constructing primes q and ordinary $A/\mathbb{F}_q$ that have a subgroup of order r and prescribed embedding degree k.
  - Works for more restricted set of k and r.
  - Field sizes are not as large.
    - Best cases: $q \approx r^2$ for $\dim A = 2$, $q \approx r^4$ for $\dim A = 3$.

Algorithm #1 for constructing pairing-friendly A.V.

- Inputs: embedding degree k, *CM field* K, prime subgroup order r.
- Algorithm constructs a $\pi \in \mathcal{O}_K$ with certain properties modulo r.
- The element π corresponds (in the sense of Honda-Tate theory) to the *Frobenius endomorphism* of an $A/\mathbb{F}_q$ that has embedding degree k with respect to r.
- A can be constructed explicitly using *CM methods*.

Complex multiplication: the basics

- For ordinary, simple, g-dimensional $A/\mathbb{F}_q$, $\mathrm{End}(A) \otimes \mathbb{Q}$ is a *CM field* K of degree $2g$.
  - $K =$ imaginary quadratic extension of totally real field.
- Frobenius endomorphism π is a *q-Weil number* in $\mathcal{O}_K$.
  - All embeddings $K \hookrightarrow \overline{K}$ have $\pi\overline{\pi} = q$.

Properties of Frobenius make $A/\mathbb{F}_q$ pairing-friendly

- Number of points given by $\#A(\mathbb{F}_q) = N_{K/\mathbb{Q}}(\pi - 1)$.
- Embedding degree k is order of $q = \pi\overline{\pi}$ in $(\mathbb{Z}/r\mathbb{Z})^\times$.
- A has embedding degree k with respect to r iff

$$N_{K/\mathbb{Q}}(\pi - 1) \equiv 0 \pmod{r} \tag{1}$$
$$\Phi_k(\pi\overline{\pi}) \equiv 0 \pmod{r} \tag{2}$$

  ($\Phi_k = k$th cyclotomic polynomial).
- Goal: construct a $\pi \in \mathcal{O}_K$ with properties (1) and (2).

Main idea: A modular approach

- Easiest case: K Galois cyclic, degree $2g$, $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$.
- Subgroup order r is a prime that splits completely in K.
- Pick a prime $\mathfrak{r}$ over r in $\mathcal{O}_K$, and write

$$r\mathcal{O}_K = \mathfrak{r} \cdot \mathfrak{r}^{\sigma} \cdots \mathfrak{r}^{\sigma^{g-1}} \cdot \overline{\mathfrak{r}} \cdot \overline{\mathfrak{r}}^{\sigma} \cdots \overline{\mathfrak{r}}^{\sigma^{g-1}}$$

(note $\sigma^g =$ complex conjugation).

Constructing a π with prescribed residues

$$r\mathcal{O}_K = \mathfrak{r} \cdot \mathfrak{r}^{\sigma} \cdots \mathfrak{r}^{\sigma^{g-1}} \cdot \bar{\mathfrak{r}} \cdot \bar{\mathfrak{r}}^{\sigma} \cdots \bar{\mathfrak{r}}^{\sigma^{g-1}}$$

Given $\xi \in \mathcal{O}_K$, write residues of ξ modulo primes over r as

$$(\alpha_1, \alpha_2, \ldots, \alpha_g, \beta_1, \ldots, \beta_g) \in \mathbb{F}_r^{2g}.$$

Then residues of $\xi^{\sigma^{-1}}$ are

$$(\alpha_2, \alpha_3, \ldots, \beta_1, \beta_2, \ldots, \alpha_1) \in \mathbb{F}_r^{2g},$$

and so on for each $\xi^{\sigma^{-i}}$, until residues of $\xi^{\sigma^{g-1}}$ are

$$(\alpha_g, \beta_1, \ldots, \beta_{g-1}, \beta_g, \ldots, \alpha_{g-1}) \in \mathbb{F}_r^{2g}.$$

Define $\pi = \prod_{i=0}^{g-1} \xi^{\sigma^{-i}}$.
Then $\pi \bmod \mathfrak{r} = \prod_{i=1}^{g} \alpha_i \in \mathbb{F}_r$, and $\pi \bmod \bar{\mathfrak{r}} = \prod_{i=1}^{g} \beta_i \in \mathbb{F}_r$.

Imposing the pairing-friendly conditions

- Given $\xi \in \mathcal{O}_K$ with residues α_i, β_i, we construct π with

$$\pi \bmod \mathfrak{r} = \prod_{i=1}^{g} \alpha_i, \quad \pi \bmod \overline{\mathfrak{r}} = \overline{\pi} \bmod \mathfrak{r} = \prod_{i=1}^{g} \beta_i.$$

- Choose α_i, β_i in advance so that
  1. $\prod_{i=1}^{g} \alpha_i = 1$ in $\mathbb{F}_r$,
  2. $\prod_{i=1}^{g} \beta_i$ is a primitive kth root of unity in $\mathbb{F}_r$,

  and construct ξ via Chinese Remainder theorem.
- Then
  1. $\pi \equiv 1 \pmod{\mathfrak{r}}$, so $N_{K/\mathbb{Q}}(\pi - 1) \equiv 0 \pmod{\mathfrak{r}}$,
  2. $\Phi_k(\pi\overline{\pi}) \equiv 0 \pmod{\mathfrak{r}}$.
- Conclusion: if $q = \pi\overline{\pi} = N_{K/\mathbb{Q}}(\xi)$ is prime, then abelian varieties $A/\mathbb{F}_q$ with Frobenius endomorphism π have embedding degree k with respect to a subgroup of order r.

The FSS Algorithm (for K Galois cyclic)

1. Fix CM field K (degree $2g$), prime subgroup size r, embedding degree k.
2. Requirements: r splits completely in K and $k \equiv 1 \pmod{r}$.
3. Choose random $\alpha_1, \ldots, \alpha_{g-1}, \beta_1, \ldots, \beta_{g-1} \in \mathbb{F}_r^\times$.
4. Choose $\alpha_g, \beta_g \in \mathbb{F}_r$ such that $\prod_{i=1}^{g} \alpha_i = 1$, and $\prod_{i=1}^{g} \beta_i$ is a primitive kth root of unity.
5. Use Chinese remainder theorem to construct $\xi \in \mathcal{O}_K$ with residues α_i, β_i modulo primes over r in $\mathcal{O}_K$.
6. Let $\pi = \prod_{i=0}^{g-1} \xi^{\sigma^{-i}}$, $q = \pi\overline{\pi} = N_{K/\mathbb{Q}}(\xi)$.
7. If q is prime return q and π; otherwise go to (3).

Algorithm outputs a pairing-friendly Frobenius element

- For fixed K, expected running time to output prime q and $\pi \in \mathcal{O}_K$ is (heuristically) polynomial in $\log r$.
- Use *CM methods* to construct pairing-friendly abelian variety $A/\mathbb{F}_q$ with Frobenius element π.
  - Methods construct abelian varieties in characteristic zero with prescribed endomorphism ring.
  - Only developed for $g \leq 3$.
  - Only practical when K is "small."
  - For further details, see talks by Kohel and Stevenhagen.

Generalize to arbitrary CM fields using *type norm*

- A *CM type* of K is a set $\Phi = \{\phi_1, \ldots, \phi_g\}$ of half of the embeddings $K \hookrightarrow \overline{K}$, one from each complex conjugate pair.
- The *reflex type* of (K, Φ) is a CM-type $\Psi = \{\psi_1, \ldots, \psi_{\widehat{g}}\}$ of a certain CM-subfield $\widehat{K}$ of the Galois closure of K.
  - $\widehat{K} = K$ if K is Galois; in general $\widehat{g} \gg g$.
- The *type norm* of Ψ is the map

$$N_\Psi : \xi \mapsto \prod_{i=1}^{\widehat{g}} \psi_i(\xi).$$

- Theorem (Shimura): N_Ψ maps $\mathcal{O}_{\widehat{K}}$ to $\mathcal{O}_K$.
- To generalize construction, factor r in $\mathcal{O}_{\widehat{K}}$, construct $\xi \in \mathcal{O}_{\widehat{K}}$ with prescribed residues, and let $\pi = N_\Psi(\xi) \in \mathcal{O}_K$.

Algorithm #2 for constructing pairing-friendly A.V.

- Main idea (Brezing-Weng & others):
  Fix CM field K, embedding degree k;
  parametrize subgroup order r as polynomial $r(x) \in \mathbb{Z}[x]$.
- Algorithm constructs $\pi(x) \in K[x]$ with certain properties modulo $r(x)$.
- For certain $x_0 \in \mathbb{Z}$, $\pi(x_0)$ is Frobenius element of an $A/\mathbb{F}_q$ that has embedding degree k with respect to $r(x_0)$.
- A can be constructed explicitly using CM methods.

How it works (if K Galois cyclic)

- Choose K and $r(x)$ so that $L = \mathbb{Q}(x)/(r(x))$ is a Galois number field containing K and μ_k.
- Pick a factor $s(x)$ of $r(x)$ in $K[x]$, and write

$$r(x) = s(x) \cdot s(x)^{\sigma} \cdots s(x)^{\sigma^{g-1}} \cdot \overline{s(x)} \cdot \overline{s(x)}^{\sigma} \cdots \overline{s(x)}^{\sigma^{g-1}}.$$

  ($\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ acts on $s(x) \in K[x]$ by acting on its coefficients).
- Given $\xi \in K[x]$, write residues of ξ modulo factors of $r(x)$ in $K[x]$ as

$$(\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g) \in L^{2g}.$$

Imposing the pairing-friendly conditions

- Let $\pi(x) = \prod_{i=0}^{g-1} \xi^{\sigma^{-i}}$ (σ acts on coefficients of ξ).
- σ permutes residues of ξ as before, so

$$\pi(x) \bmod s(x) = \prod_{i=1}^{g} \alpha_i, \quad \overline{\pi(x)} \bmod s(x) = \prod_{i=1}^{g} \beta_i.$$

- Choose α_i, β_i in advance so that
  1. $\prod_{i=1}^{g} \alpha_i = 1$ in L,
  2. $\prod_{i=1}^{g} \beta_i$ is a primitive kth root of unity in L,

  and construct ξ via Chinese remainder theorem.
- Then
  1. $\pi(x) - 1 \equiv 0 \pmod{s(x)}$,
     so "$N_{K/\mathbb{Q}}$"$(\pi(x) - 1) \equiv 0 \pmod{s(x)}$;
  2. $\Phi_k(\pi(x)\overline{\pi}(x)) \equiv 0 \pmod{s(x)}$.

Finding an individual variety

- We've constructed $\pi(x) \in K[x]$ that satisfies the pairing-friendly conditions for polynomials.
- To find individual varieties: look for $x_0 \in \mathbb{Z}$ such that
  - $q(x_0) = \pi(x_0)\overline{\pi}(x_0)$ is an integer prime,
  - $r(x_0)$ is (nearly) prime.
- Then $\pi(x_0)$ is the Frobenius endomorphism of an abelian variety $A/\mathbb{F}_q$ that has embedding degree k with respect to a subgroup of order $r(x_0)$.
- Use CM methods to construct A explicitly.
- Adapt method to general CM fields K using *extended type norm*.

Measuring the field size

- To maximize efficiency in applications, want to make q as small as possible for fixed r.
- Ratio of full group order q (in bits) to subgroup order r (in bits) measured by

$$\rho = \frac{\log_2 q^g}{\log_2 r}$$

- Method #1 with Galois K gives $q \approx r^{2g} \Rightarrow \rho \approx 2g^2$.
  - $q = N_{K/\mathbb{Q}}(\xi)$ is a product of $2g$ "randomish" residues mod r.
- Experimental evidence supports this conclusion:
  - $g = 2$, 160-bit r:
    92% of abelian surfaces produced have $7.9 < \rho < 8$.

Method #2 (polynomials) gives smaller field sizes

- $\xi \in K[x]$ constructed via CRT has degree $< \deg r(x)$.
- $\pi(x)$ has degree $< g \deg r(x)$
(since it's a product of g conjugates of ξ).
- If $q = \pi(x_0)\overline{\pi}(x_0)$ and $r = r(x_0)$, then for large x_0

$$\rho \approx \frac{2g \deg \pi(x)}{\deg r(x)} < 2g^2.$$

- If $r(x)$ and residues of ξ are chosen cleverly, can obtain significantly better ρ-values.

Best results for selected k

- Best results when $r(x) = \Phi_k(x)$, $K \subset \mathbb{Q}(\zeta_k)$.

Dimension $g = 2$

k	ρ	CM field
5	4	$\mathbb{Q}(\zeta_5)$
10	6	$\mathbb{Q}(\zeta_5)$
13	6.7	$\mathbb{Q}(\sqrt{-13+2\sqrt{13}})$
16	7	$\mathbb{Q}(\sqrt{-2+\sqrt{2}})$
20	6	$\mathbb{Q}(\zeta_5)$

Dimension $g = 3$

k	ρ	CM field
7	12	$\mathbb{Q}(\zeta_7)$
9	15	$\mathbb{Q}(\zeta_9)$
18	15	$\mathbb{Q}(\zeta_9)$

- Compare with $\rho = 8$ for $g = 2$ and $\rho = 18$ for $g = 3$.
- Ultimate goal: varieties of prime order ($\rho = 1$).
  - Not there yet, but this is a start!