A Generalized Brezing-Weng Algorithm for Constructing Pairing-Friendly Ordinary Abelian Varieties

David Freeman

Stanford University, USA

Pairing 2008
1 September 2008

Pairings for cryptography

- Groups used in pairing-based crypto consist of points of prime order r on *abelian varieties* $A/\mathbb{F}_q$.
    - Elliptic curves are 1-dimensional abelian varieties.
- Pairings are (variants of) *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 r, q^k are large, *discrete log problem* (DLP) is infeasible in $A[r]$ and $\mathbb{F}_{q^k}^\times$.
- If k is small, pairings can be computed efficiently (Miller).

Pairing-friendly abelian varieties: first attempts

- Random abelian varieties
  - 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.
- *Supersingular* abelian varieties
  - Embedding degree in dimension $g \leq 6$ is $k \leq 7.5g$ (Rubin-Silverberg).
  - These k are only acceptable for the lowest security levels.
- Conclusion: need to develop specific constructions of non-supersingular (usually, *ordinary*) abelian vareities.

The Problem

- Find primes q and ordinary 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.
- Want $\rho = \log(q^g)/\log r$ close to 1 to maximize efficiency in implementations.

Our contribution

- We give a method for constructing primes q and ordinary $A/\mathbb{F}_q$ that have prescribed embedding degree k.

	arbitrary k, large ρ	many k, smaller ρ
elliptic curves	Cocks-Pinch	Brezing-Weng
higher dimensions	F.-Stevenhagen-Streng	*This work*

- Kawazoe-Takahashi (next talk) give another approach to filling in the lower-right corner (dimension 2 only).
- Uses techniques of F.-Stevenhagen-Streng to generalize Brezing-Weng method to arbitrary dimension.

Algorithm for constructing pairing-friendly A.V.

- Inputs: embedding degree k, *CM field* K
- *FSS idea*:
  Construct a $\pi \in \mathcal{O}_K$ with certain properties modulo r.
- *Brezing-Weng idea*:
  Parametrize subgroup order r as polynomial $r(x) \in \mathbb{Z}[x]$.
- *Combine ideas*:
  Obtain $\pi(x) \in K[x]$ with FSS properties modulo $r(x)$.
- For certain $x_0 \in \mathbb{Z}$, $\pi(x_0)$ 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 $r(x_0)$.
- 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 $2g$.
  - $K =$ totally 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

$$\begin{aligned} N_{K/\mathbb{Q}}(\pi - 1) &\equiv 0 \pmod{r} \quad (1) \\ \Phi_k(\pi\overline{\pi}) &\equiv 0 \pmod{r} \quad (2) \end{aligned}$$

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

The Brezing-Weng Algorithm

Construct pairing-friendly elliptic curves via the following algorithm:

1. Choose embedding degree k, CM field $K = \mathbb{Q}(\sqrt{-D})$.
2. Choose irreducible $r(x) \in \mathbb{Z}[x]$ such that $L = \mathbb{Q}[x]/(r(x))$ contains K and ζ_k.
3. Compute $t(x)$ mapping to $\zeta_k + 1$ in L.
4. Compute $y(x)$ mapping to $(\zeta_k - 1)/\sqrt{-D}$ in L.
5. Set $q(x) \leftarrow \frac{1}{4}(t(x)^2 + Dy(x)^2)$.

Theorem: If $q(x_0)$ is a prime integer for some x_0, there is an elliptic curve over $\mathbb{F}_{q(x_0)}$ with an order-$r(x_0)$ subgroup and embedding degree k.

Rethinking the Brezing-Weng algorithm

- BW: $t(x) \equiv \zeta_k + 1$ and $y(x) \equiv (\zeta_k - 1)/\sqrt{-D} \bmod r(x)$.
- Let $\mathfrak{r}(x)$ be a factor of $r(x)$ in $K[x]$.
- Let $\pi(x) = \frac{1}{2}(t(x) + y(x)\sqrt{-D})$. Then
  1. $\pi(x) \equiv \zeta_k \bmod \mathfrak{r}(x)$,
  2. $\overline{\pi}(x) \equiv 1 \bmod \mathfrak{r}(x)$.
- This implies that

$$N_{K[x]/\mathbb{Q}[x]}(\pi(x) - 1) \equiv 0 \bmod r(x) \tag{3}$$
$$\Phi_k(\pi(x)\overline{\pi}(x)) \equiv 0 \bmod r(x) \tag{4}$$

so when we plug in any integer x, the pairing-friendly conditions (1) and (2) hold.

Main idea: A modular approach

- Easiest case: K Galois cyclic, degree $2g$, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$.
- If $L = \mathbb{Q}[x]/(r(x))$ is Galois and contains K, then $r(x)$ factors into $2g$ irreducibles in $K[x]$.
- Pick a factor $\mathfrak{r}(x)$ of $r(x)$ in $K[x]$, and write

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

  - σ acts on a polynomial by acting on its coefficients.
  - $\sigma^g =$ complex conjugation.

Constructing a $\pi(x)$ with prescribed residues

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

Given $\xi(x) \in K[x]$, write residues of ξ modulo factors of $r(x)$ in $K[x]$ as

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

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

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

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

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

Define $\pi(x) = \prod_{i=0}^{g-1} \xi(x)^{\sigma^{-i}}$.
Then $\pi(x) \bmod \mathfrak{r}(x) = \prod_{i=1}^{g} \alpha_i$, $\pi(x) \bmod \overline{\mathfrak{r}(x)} = \prod_{i=1}^{g} \beta_i \in L$.

Imposing the pairing-friendly conditions

- Given $\xi(x) \in K[x]$ with residues α_i, β_i, construct $\pi(x)$ with

$$\begin{aligned} \pi(x) \bmod \mathfrak{r}(x) &= \textstyle\prod_{i=1}^{g} \alpha_i, \\ \pi(x) \bmod \overline{\mathfrak{r}(x)} &= \overline{\pi}(x) \bmod \mathfrak{r}(x) = \textstyle\prod_{i=1}^{g} \beta_i. \end{aligned}$$

- 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 $\xi(x)$ via Chinese Remainder theorem.
- Then
  1. $\pi(x) \equiv 1 \bmod \mathfrak{r}(x)$, so
     $N_{K[x]/\mathbb{Q}[x]}(\pi(x) - 1) \equiv 0 \bmod \mathfrak{r}(x)$,
  2. $\Phi_k(\pi(x)\overline{\pi}(x)) \equiv 0 \bmod \mathfrak{r}(x)$.

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.
  - Methods construct abelian varieties in characteristic zero with prescribed endomorphism ring.
  - Only developed for $g \leq 3$.
  - Only practical when K is "small."

Expected ρ-value is $< 2g^2$

- $\xi(x) \in K[x]$ 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

$$\rho = \frac{\log(q(x_0)^g)}{\log(r(x_0))} \approx \frac{2g \deg \pi(x)}{\deg r(x)} < 2g^2.$$

- Compare with FSS algorithm: expect $\rho \approx 2g^2$.
- If $r(x)$ and residues of $\xi(x)$ 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 FSS: $\rho = 8$ for $g = 2$ and $\rho = 18$ for $g = 3$.
- Ultimate goal: varieties of prime order ($\rho \approx 1$).
  - Not there yet, but this is a start!