Constructing Abelian Varieties for Pairing-Based Cryptography

David Freeman

University of California, Berkeley, USA

University of Washington
26 February 2008

Outline

Outline

What is a pairing?

- Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be finite cyclic groups of the same order.
- A *cryptographic pairing* is a bilinear, nondegenerate map

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

- To be useful in crypto applications, we need:
  1. the pairing to be easy to compute, and
  2. the discrete logarithm problem in $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ to be computationally infeasible.
- Discrete logarithm problem (DLP): Given x, x^a in finite group, compute $a \in \mathbb{Z}/|x|\mathbb{Z}$.

Example: One-round 3-way key exchange (Joux)

- Three players A,B,C want to agree on a shared secret.
- Choose (public) group $\mathbb{G}_1 = \mathbb{G}_2 = \langle g \rangle$ and cryptographic pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.
- A,B,C pick secret integers $a, b, c \in [1, |g|]$.
- A broadcasts g^a, B broadcasts g^b, C broadcasts g^c.
- Shared secret is $e(g, g)^{abc} \in \mathbb{G}_T$:
    - A computes $e(g^b, g^c)^a$,
    - B computes $e(g^a, g^c)^b$,
    - C computes $e(g^a, g^b)^c$.
- If DLP in $\langle g \rangle$ and $\mathbb{G}_T$ are infeasible, then the shared secret can't be recovered from the public information.
    - Can't compute a from g, g^a or $e(g, g), e(g, g^a)$.

Pairings used in cryptography

- Today, pairings used in many cryptographic applications, including *identity-based encryption, digital signatures, private information retrieval, zero knowledge,* and more...
- Groups $\mathbb{G}_1, \mathbb{G}_2$ are groups of points on (principally polarized) abelian varieties $A/\mathbb{F}_q$.
- Pairings e are (variants of) the *Weil pairing*

$$e_{weil,r} : A[r] \times A[r] \to \mu_r$$

or the *Tate* (or *Frey-Rück*) *pairing*

$$e_{tate,r} : A(\mathbb{F}_{q^k})[r] \times A(\mathbb{F}_{q^k})/rA(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^\times/(\mathbb{F}_{q^k}^\times)^r$$

- If r is prime and $\mathbb{F}_{q^k}$ is the smallest field containing μ_r, then $\mathbb{G}_T = \mathbb{F}_{q^k}^\times$ for both pairings.

Embedding degrees

- Let A be an g-dimensional abelian variety over $\mathbb{F}_q$ with $r \mid \#A(\mathbb{F}_q)$, r prime.
  - If keys, signatures, ciphertexts, etc. are elements of $A[r]$, we want q small to save bandwidth.
  - Ideal case: $A(\mathbb{F}_q)$ has prime order ($r \approx q^g$).
- Let k be the smallest integer such that $\mu_r \subset \mathbb{F}_{q^k}^\times$ (equivalently, such that $r \mid q^k - 1$ or $r \mid \Phi_k(q)$).
  - Weil/Tate pairings 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" varieties, $k \sim r$ (Bal.-Kob.).
  - 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 r to construct varieties for various applications.

Outline

Known results: Elliptic curves

- Menezes-Okamoto-Vanstone: Supersingular elliptic curves always have $k \leq 6$; easy to construct.
- Cocks-Pinch, Dupont-Enge-Morain: Construct ordinary elliptic curves with arbitrary k, $q \approx r^2$.
- Barreto-Lynn-Scott, Brezing-Weng: reduce size of q for certain k, but no curves of prime order.
- Miyaji-Nakabayashi-Takano, Barreto-Naehrig: Construct ordinary elliptic curves with $k = 3, 4,$ or 6 (MNT), or $k = 12$ (BN) and prime order $r \approx q$.
- **Our result** *(ANTS-VII)*: Construct ordinary elliptic curves with $k = 10$ and prime order $r \approx q$.

The CM method

- *Complex Multiplication method* (Atkin, Morain) generates elliptic curves with a specified number of points.
- For given square-free $D > 0$, CM method constructs elliptic curve with CM by $\mathbb{Q}(\sqrt{-D})$.
- Running time depends on the class number h_D of $\mathbb{Q}(\sqrt{-D})$.
    - Bottleneck is computing the *Hilbert class polynomial*, a polynomial of degree h_D.
    - Best known algorithms run in (roughly) $O(h_D^2) = O(D)$ (Enge).
- Can be efficiently implemented if h_D not too large.
    - Current record is $h_D = 10^5$ (Enge).

How to generate pairing-friendly curves

- Recall: The *trace* of $E/\mathbb{F}_q$ satisfies $\#E(\mathbb{F}_q) = q + 1 - t$.
- To apply the CM method: Fix D, k. Look for t, r, q (representing trace, order of subgroup, and size of field) satisfying
    1. q, r prime;
    2. $r \mid q + 1 - t$ (formula for number of points);
    3. $r \mid \Phi_k(q)$, where Φ_k is kth cyclotomic polynomial (embedding degree k);
    4. $Dy^2 = 4q - t^2$ for some integer y (“CM equation”).
- For such t, r, q, if h_D is not too large ($\sim 10^5$) we can construct an elliptic curve E over $\mathbb{F}_q$ with an order-r subgroup and embedding degree k.

Generating curves of prime order

- For curves of prime order, have $r = q + 1 - t$.
  - Condition $r \mid \Phi_k(q)$ equivalent to $r \mid \Phi_k(t-1)$.
- Idea of Barreto-Lynn-Scott, others: parametrize t, r, q as polynomials: $t(x), r(x), q(x)$. Construct curves by finding many integer solutions (x, y) to the "CM equaton"

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

- MNT strategy: Fix D, k, choose $t(x)$, let $r(x)$ be an irreducible factor of $\Phi_k(t(x) - 1)$, find solutions (x, y) to CM equation.
- Observation (F.): CM equation will have many solutions only if RHS is quadratic or has a multiple root (Siegel's theorem).

Using the MNT strategy

- Goal: Choose $t(x)$, find factor $r(x)$ of $\Phi_k(t(x)-1)$, such that $f(x) = 4r(x) - (t(x)-2)^2$ is quadratic.
- MNT solution for $k = 3, 4, 6$:
  1. Choose $t(x)$ linear; then $r(x)$ is quadratic, and so is $f(x)$.
  2. Use standard Pell equation algorithms to find solutions (x_0, y_0) to $Dy^2 = f(x)$.
  3. Compute field size $q(x_0)$ and curve order $r(x_0)$.
  4. If no solutions of appropriate size, or $q(x_0)$ or $r(x_0)$ not prime, choose different D and try again.
  5. Use CM method to construct curve equation.

Our solution for $k = 10$

- Goal: Choose $t(x)$, find factor $r(x)$ of $\Phi_{10}(t(x) - 1)$, such that $f(x) = 4r(x) - (t(x) - 2)^2$ is quadratic.
    - All irred. factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid$ degree.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and t^2 cancel out.
    - Smallest possible case: $\deg r = 4$, $\deg t = 2$.
- 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!
- Construct curves via Pell-like equation as in MNT solution.

Choice of Parameters

- Choose t, r, q as follows:

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

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

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

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

$$\begin{aligned} t &= 26990109895270505967027619626089715 3 \\ r &= 18211650803969472064493264347375949776033155743952030750450033782306651 \\ q &= 18211650803969472064493264347375950045934254696657090420726230043203803 \end{aligned}$$

- Use CM method to compute curve equation over $\mathbb{F}_q$:

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

- This curve has r points and embedding degree 10.

Outline

Known Results: Abelian Varieties of Dimension ≥ 2

- Rubin-Silverberg: Classified supersingular abelian varieties of dimension $g \leq 6$.
  - Easy to construct.
  - Always have $k \leq 7.5g$.
- Galbraith-McKee-Valença, Hitt: Showed existence of non-supersingular abelian surfaces ($g = 2$) with small embedding degree, but no construction.
- **Result #1** *(Pairings '07)*:
  Construct ordinary abelian surfaces with arbitrary k.
- **Result #2** (*ANTS-VIII*, with P. Stevenhagen and M. Streng):
  Abstract Result #1 and generalize to arbitrary dimension.

Frobenius Endomorphism and CM fields

- Let A be a g-dimensional ordinary, simple abelian variety over $\mathbb{F}_q$ (q prime).
- $K = \mathrm{End}(A) \otimes \mathbb{Q}$ is a degree-$2g$ number field, called a *CM-field* — an imaginary quadratic extension of a totally real field. (We say A has *CM by K*.)
- The Frobenius endomorphism π of A can be interpreted as an algebraic integer in K.
- $\pi \in \mathcal{O}_K$ is a *q-Weil number*: all embeddings $K \hookrightarrow \mathbb{C}$ have $\pi\overline{\pi} = q$.
- $\#A(\mathbb{F}_q) = \mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$.

Pairing-Friendly Frobenius Elements

- Honda-Tate: (conjugacy classes of) q-Weil numbers π correspond to (isogeny classes of) abelian varieties $A/\mathbb{F}_q$.
- To guarantee that $A/\mathbb{F}_q$ has embedding degree k with respect to a subgroup of order r, we require:

$$\begin{aligned} \mathrm{N}_{K/\mathbb{Q}}(\pi - 1) &\equiv 0 \pmod{r} \\ \Phi_k(\pi\overline{\pi}) &\equiv 0 \pmod{r} \end{aligned}$$

  where Φ_k is the kth cyclotomic polynomial.
- Construction of such π demonstrates *existence* of pairing-friendly abelian varieties.
- Problem: these varieties can only be *constructed* if K is "small."
- Solution: Fix K in advance so that varieties with CM by K can be constructed (more on this later...).

Main Idea: A Modular Approach

- Simple 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:

$$r\mathcal{O}_K = \mathfrak{r}_1 \cdots \mathfrak{r}_g \bar{\mathfrak{r}}_1 \cdots \bar{\mathfrak{r}}_g$$

  with $\mathfrak{r}_i = \sigma^{-i}(\mathfrak{r})$ for some prime $\mathfrak{r}$ over r.
- Given $\xi \in \mathcal{O}_K$, write

$$\xi \equiv \alpha_i \pmod{\mathfrak{r}_i}, \quad \xi \equiv \beta_i \pmod{\bar{\mathfrak{r}}_i}$$

  for $\alpha_i, \beta_i \in \mathbb{F}_r$.
- Define $\pi = \prod_{i=1}^{g} \sigma^i(\xi)$.
- Then $\sigma^i(\xi) \equiv \alpha_i \pmod{\mathfrak{r}}$ and $\sigma^i(\xi) \equiv \beta_i \pmod{\bar{\mathfrak{r}}}$, so we have

$$\pi \equiv \prod_{i=1}^{g} \alpha_i \pmod{\mathfrak{r}}, \qquad \pi \equiv \prod_{i=1}^{g} \beta_i \pmod{\bar{\mathfrak{r}}}.$$

Imposing The Pairing-Friendly Conditions

- We have constructed $\pi \in \mathcal{O}_K$ such that

$$\pi \equiv \prod_{i=1}^{g} \alpha_i \pmod{\mathfrak{r}}, \qquad \overline{\pi} \equiv \prod_{i=1}^{g} \beta_i \pmod{\mathfrak{r}}.$$

- Suppose that
  1. $\zeta = \prod_{i=1}^{g} \alpha_i$ is a kth root of unity in $\mathbb{F}_r^\times$, and
  2. $\prod_{i=1}^{g} \beta_i = 1$ in $\mathbb{F}_r$.
- Then
  1. $\Phi_k(\pi\overline{\pi}) \equiv \Phi_k(\zeta) \equiv 0 \pmod{\mathfrak{r}}$
  2. $\overline{\pi} - 1 \equiv 0 \pmod{\mathfrak{r}}$, so $\mathrm{N}_{K/\mathbb{Q}}(\pi - 1) \equiv 0 \pmod{r}$.
- Conclusion: if $q = \pi\overline{\pi} = \mathrm{N}_{K/\mathbb{Q}}(\xi)$ 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.

Generalizing to Arbitrary CM-Fields

- A *CM-type* of K is a set $\Phi = \{\phi_1, \ldots, \phi_g\}$ of half of the embeddings $K \hookrightarrow \mathbb{C}$, 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

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

- 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 $\pi = \mathrm{N}_\Psi(\xi) \in \mathcal{O}_K$.

The FSS Algorithm

1. Fix primitive CM-type (K, Φ), prime subgroup size r (splits completely in K), embedding degree $k \equiv 1 \pmod{r}$.
2. Compute the reflex type $(\widehat{K}, \Psi)$, let $\widehat{g} = \frac{1}{2} \deg \widehat{K}$.
3. Choose random $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1} \in \mathbb{F}_r^\times$.
4. Choose $\alpha_{\widehat{g}}, \beta_{\widehat{g}} \in \mathbb{F}_r$ such that $\prod_{i=1}^{\widehat{g}} \alpha_i$ is a kth root of unity, and $\prod_{i=1}^{\widehat{g}} \beta_i = 1$.
5. Use Chinese Remainder Theorem to compute $\xi \in \mathcal{O}_{\widehat{K}}$ with residues α_i, β_i modulo factors of $r\mathcal{O}_{\widehat{K}}$.
6. Let $\pi = N_\Psi(\xi)$, $q = \pi\overline{\pi} = \mathrm{N}_{\widehat{K}/\mathbb{Q}}(\xi)$.
7. If q is prime return q and π; otherwise go to (3).

The Output

- Need $g \geq 2$ for algorithm to work.
  - Adaptation for $g = 1$ recovers the Cocks-Pinch algorithm.
- For fixed K, expected running time to output prime q and $\pi \in \mathcal{O}_K$ is (heuristically) polynomial in $\log r$.
- Theorem (FSS): If prime q is unramified in K and $K = \mathbb{Q}(\pi)$ (both of which happen with high probability) then there is an ordinary, simple abelian variety $A/\mathbb{F}_q$ of dimension g that has embedding degree k with respect to a subgroup of order r.
- How do we constuct this A? *CM methods.*

Constructing Abelian Varieties with CM by K

- CM theory: Abelian varieties $A/\mathbb{F}_q$ with CM by K arise as reductions of varieties in characteristic zero with CM by K.
- CM methods: Construct g-dimensional abelian varieties in characteristic zero with CM by K.
  - $g = 1$ (elliptic curves): Compute *Hilbert class polynomials*; roots are j-invariants of elliptic curves E with CM by K.
  - $g = 2$ (abelian surfaces): Compute *Igusa class polynomials*; roots are Igusa invariants of genus 2 curves C whose Jacobians have CM by K.
  - $g = 3$: Methods developed only for fields containing i or ζ_3.
  - Higher dimensions: only a few explicit examples, e.g. Jacobian of $y^2 = x^p + 1$ for prime p.

A small example ($g = 2$)

- Algorithm inputs:
  1. CM-field $K = \mathbb{Q}(\zeta_5)$; CM-type $\Phi = \{\phi_1, \phi_2\}$, where $\phi_n : \zeta_5 \mapsto e^{2\pi i n/5}$.
  2. Embedding degree $k = 10$,
  3. Prime $r = 2011 = \texttt{NextPrime}(2008)$,
- Algorithm outputs:
  1. Prime $q = 2086780871011$,
  2. $\pi = 835578 + 552276\zeta_5 - 845235\zeta_5^2 + 313882\zeta_5^3$.
- CM methods produce curve $C : y^2 = x^5 + 22$ over $\mathbb{F}_q$.
- If $A = \mathrm{Jac}(C)$ is the Jacobian of C, then
  1. $A(\mathbb{F}_q)$ has a subgroup of order r.

$$\#A(\mathbb{F}_q) = 4354647472611861083688755 \equiv 0 \pmod{r}$$

  2. A has embedding degree 10 with respect to r.

Improving the ρ-value

- For abelian varieties 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.)
- Expected ρ-value produced by our algorithm is $2g\widehat{g}$.
  - $\rho = 7.46$ in the example above ($g = \widehat{g} = 2$).
- Major open problem: produce pairing-friendly ordinary abelian varieties with $g \geq 2$ and $\rho \leq 2$.

A New Result

- Used the ideas of FSS algorithm to generalize Brezing-Weng elliptic curve construction to arbitrary dimension.
- Implemented for Galois cyclic CM-fields K.
- Algorithm produces pairing-friendly abelian varieties with $\rho < 2g^2$.

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	$\mathbb{Q}(\sqrt{-2+\sqrt{2}})$

Dimension $g = 3$

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