Constructing Pairing-Friendly Elliptic Curves for Cryptography

David Freeman

University of California, Berkeley, USA

2nd KIAS-KMS Summer Workshop on Cryptography

Seoul, Korea
30 June 2007

Outline

1. Recent Developments
   - Varying the CM Discriminant
   - Curves of Composite Order
   - Hyperelliptic Curves

Outline

1. Recent Developments
   - Varying the CM Discriminant
   - Curves of Composite Order
   - Hyperelliptic Curves

Small CM Discriminants

- Constructing pairing-friendly curves requires solving an equation of the form $Dy^2 = 4p - t^2$.
- D is the *CM discriminant*; if $D < 10^{10}$, then we can construct a curve with the desired properties.
- Most constructions of families of pairing-friendly curves fix $D = 1, 2,$ or 3.
- Curves with small CM discriminant often have extra structure (e.g., extra automorphisms) that might be used to aid a future attack on the discrete log problem.
  - No such attack currently known, but we want to think ahead!
- For maximum security, want to construct families with variable CM discriminant D.
  - No international standard, but German Information Security Agency requires that class number of $\mathbb{Q}(\sqrt{-D})$ be > 200.

Varying the CM Discriminant

- Recall: complete families of curves constructed by finding $t(x), r(x), p(x)$ satisfying certain conditions.
  - Also $y(x)$ in CM equation $Dy^2 = 4p - t^2$.
- Theorem (F.-Scott-Teske):
  - Suppose $t(x), r(x), p(x)$ give a family of pairing-friendly elliptic curves with embedding degree k and CM discriminant D.
  - Suppose $t(x), r(x), p(x)$ are even polynomials and the corresponding $y(x)$ is an odd polynomial.
  - Subsituting $x^2 \mapsto ax^2$ for any a gives a family with embedding degree k, CM discriminant aD, and the same ρ-value.
- Given a family that satisfies the conditions of the theorem, we can construct curves with nearly arbitrary square-free CM discriminant.

Families Allowing Variable CM Discriminant

- Brezing-Weng families with embedding degree k and $2k$, k odd.
  - $\rho = (k+2)/\varphi(k)$, or $(k+2)/(k-1)$ for prime k.
- F.-Scott-Teske families with embedding degree k ($k \equiv 3 \mod 4$) or $2k$ ($k \equiv 1 \mod 4$).
  - $\rho = (k+1)/\varphi(k)$, or $(k+1)/(k-1)$ for prime k.
- F.-Scott-Teske families with $3 \mid k$, $8 \nmid k$, $k \geq 18$.
  - ρ often close to 2; only even CM discriminants.
- Scott-Barreto families.
  - Doesn't make use of Theorem; D a parameter in the construction.
- Conclusion: variable discriminant families exist for every k with $\gcd(k, 24) \in \{1, 2, 3, 6, 12\}$.

Outline

1. Recent Developments
   - Varying the CM Discriminant
   - Curves of Composite Order
   - Hyperelliptic Curves

Composite-Order Subgroups

- Many recent protocols require curves to be pairing-friendly with respect to a subgroup of composite order $r = r_1 r_2$ that is infeasible to factor (e.g., r is an RSA modulus).
- Security of protocols relies on factoring, not discrete log problem.
- Factoring an integer of size r takes roughly the same amount of time as discrete log in a finite field of size r.
- Conclude: for maximum efficiency, want to minimize $\rho \cdot k =$ ratio of field size to subgroup size.

Pairing-Friendly Curves of Composite Order

- Want to minimize $\rho \cdot k$; theoretical minimum is 2.
- Two options with $\rho \cdot k = 2$:
  - Supersingular curves over prime fields (Boneh-Goh-Nissim): $k = 2$, $\rho = 1$.
  - Cocks-Pinch method with Chinese Remainder Theorem (Rubin-Silverberg): $k = 1$, $\rho = 2$.
- Supersingular curves have slight advantage due to implementation improvements for even k.

Outline

1. Recent Developments
   - Varying the CM Discriminant
   - Curves of Composite Order
   - Hyperelliptic Curves

Hyperelliptic Curves

- A hyperelliptic curve C of genus g is given by $y^2 = f(x)$, where $\deg f = 2g + 1$.
  - Elliptic curves have genus 1.
- There is no group law on C, but there is a group law on the *Jacobian* of C, $\mathrm{Jac}(C)$.
  - $\mathrm{Jac}(C)$ is a g-dimensional abelian variety.
  - Can think of $\mathrm{Jac}(C)$ as g-tuples of points on C.
  - Efficient group law algorithm given by Cantor.
- The Weil and Tate pairings exist on $\mathrm{Jac}(C)$ and have the same properties as on elliptic curves.
- Thus we can search for *pairing-friendly hyperelliptic curves*, whose Jacobians have large prime-order subgroup and small embedding degree.

Supersingular Abelian Varieties

- $\mathrm{Jac}(C)$ is *supersingular* if there is a map from $\mathrm{Jac}(C)$ to a product of supersingular elliptic curves.
- Rubin-Silverberg: showed all curves C with supersingular Jacobians are pairing-friendly.
  - Gave upper bound on k for all g.
  - Gave sharp bound on k for $g \leq 6$.
- Cardona-Nart: gave explicit formulas for embedding degree when C has genus 2.
- Possible embedding degrees (and thus security levels) always limited.
  - For more flexibility, must use non-supersingular varieties.

Non-supersingular Abelian Varieties

- Results only exist for $g = 2$ (abelian surfaces).
- Galbraith-McKee-Valença: Showed existence of abelian surfaces A over prime fields with $k = 5, 10$.
- Hitt: Showed existence of abelian surfaces A in characteristic 2 with various $k < 50$.
- Neither technique gives explicit construction of a pairing-friendly curve C.
- F.: Constructed pairing-friendly curves C over prime fields whose Jacobians have arbitrary k and subgroup size r.
  - Adapts Cocks-Pinch method for elliptic curves.
  - Jac(C) has $\rho \approx 8$ (quite poor!)
- Open problem: construct non-supersingular pairing-friendly abelian surfaces with $\rho \leq 2$.

For Further Information

- See survey article by F.-Scott-Teske, "A Taxonomy of Pairing-Friendly Elliptic Curves"
- Available at `http://eprint.iacr.org/2006/372`.