Pairing-friendly Hyperelliptic Curves and Weil Restriction

David Mandell Freeman[1]
(joint work with Takakazu Satoh[2])

[1]CWI and Universiteit Leiden, Netherlands
[2]Tokyo Institute of Technology, Japan

Intercity Number Theory Seminar
Eindhoven, Netherlands
18 September 2009

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.

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* (similar).
- 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 $\mathbb{F}_{q^k}^\times$.

More about the embedding degree

- If k is small, pairings can be computed efficiently (via Miller's algorithm).
- 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: abelian varieties with small embedding degree are "special."

The Problem

- Find prime (powers) 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.
- We consider the problem for *abelian surfaces*:
  - Find genus 2 curves whose Jacobians are pairing-friendly.

Why genus 2?

- Want to make q as small as possible for fixed r.
- A g-dimensional Abelian variety $A/\mathbb{F}_q$, the ratio of full group order (in bits) to subgroup order r (in bits) is measured by

$$\rho(A) = \frac{\log_2 q^g}{\log_2 r}, \qquad \text{i.e., } q = r^{\rho/g}.$$

- If $g = 2$ and $\rho \approx 1$ (best possible), then $q \approx \sqrt{r}$ — much smaller than field for an order-r elliptic curve.
- If ρ is small, crypto computations on abelian surfaces could be more efficient than on elliptic curves.

An alternative answer...

Genus 1 is solved*;
genus 3 is too hard†!

*pretty much
†usually

Some genus 2 constructions

Type	Authors	best ρ	notes
product of elliptic curves	(trivial)	**2**	can't get $\rho < 2$
supersingular curves	G'01, RS'02	**1**	must have $k \leq 12$
ordinary curves	FSS'08, F'07,F'08	**4** (8 in general)	
p-rank 1 curves	HMNS'08	**16**	

Best previous non-supersingular genus 2 result

- Jacobian of
$$y^2 = x^5 + ax$$
over $\mathbb{F}_p$, $p \equiv 1$ or $3 \pmod 8$ [KT'08].
- Best $\rho \approx 3$; in general $\rho \approx 4$.
- Construction works for a single $\overline{\mathbb{F}}_p$-isomorphism class of curves.
- Construction is mysterious:
uses explicit formula for $\#\,\mathrm{Jac}(C)(\mathbb{F}_p)$ in terms of the decomposition of p in $\mathbb{Q}(\sqrt{-2})$.

Our results

1. Explain why the [KT'08] construction works.
2. Generalize [KT'08] construction to other genus 2 curves.
3. Produce abelian surfaces with $\rho < 3$.
   - New record: $\rho \approx 2.22$.

Key property of KT curves

If Jacobian of $y^2 = x^5 + ax$ over $\mathbb{F}_p$ is ordinary, then it is

1. Simple over $\mathbb{F}_p$,
2. Isogenous over some extension $\mathbb{F}_{p^d}$ to a product of isomorphic elliptic curves $E \times E$ defined over $\mathbb{F}_p$.

Theorem: Any abelian variety over $\mathbb{F}_p$ with these properties is isogenous to a subvariety of the *Weil restriction* of E from $\mathbb{F}_{p^d}$ to $\mathbb{F}_p$.

Key property of KT curves

If Jacobian of $y^2 = x^5 + ax$ over $\mathbb{F}_p$ is ordinary, then it is

1. Simple over $\mathbb{F}_p$,
2. Isogenous over some extension $\mathbb{F}_{p^d}$ to a product of isomorphic elliptic curves $E \times E$ defined over $\mathbb{F}_p$.

Theorem: Any abelian variety over $\mathbb{F}_p$ with these properties is isogenous to a subvariety of the *Weil restriction* of E from $\mathbb{F}_{p^d}$ to $\mathbb{F}_p$.

What is Weil Restriction?

For L/K finite field ext., *Weil restriction* is a functor

$$\mathrm{Res}_{L/K} : \{\text{varieties over } L\} \to \{\text{varieties over } K\}$$

For an affine variety X:

1. Choose a K-basis $\{\alpha_i\}$ of L;
2. Write each variable x_i over L as variables over K;
3. Separate each equation defining X into $[L : K]$ equations defining $\mathrm{Res}_{L/K}(X)$.

Extend to projective varieties by gluing.

Example of Weil restriction

- $\mathbb{G}_m = Z(xy - 1) \subset \mathbb{A}^2, \quad L/K = \mathbb{Q}(i)/\mathbb{Q}$.
- Write $x = x_1 + ix_2$, $y = y_1 + iy_2$.
- From $(x_1 + ix_2)(y_1 + iy_2) - 1 = 0$ we get

$$\mathrm{Res}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{G}_m) = Z(x_1y_1 - x_2y_2 - 1, x_1y_2 + x_2y_1) \subset \mathbb{A}^4$$

- Some properties:
  1. $\dim \mathrm{Res}_{L/K}(X) = [L : K] \dim X$.
  2. $\mathrm{Res}_{L/K}(X)(K) \cong X(L)$.
  3. $\mathrm{Res}_{L/K}$ of a group variety is a group variety (and (2) is a group isomorphism).

Proof of the theorem (M. Streng)

- Let A be a simple g-dimensional abelian variety over K, and L/K a finite extension.
- Given L-isogeny $\phi : A \to E^g$, functoriality gives K-isogeny

$$\mathrm{Res}_{L/K}(\phi) : \mathrm{Res}_{L/K}(A) \to \mathrm{Res}_{L/K}(E^g) \cong (\mathrm{Res}_{L/K}(E))^g$$

- There is a K-morphism $\chi : A \hookrightarrow \mathrm{Res}_{L/K}(A)$.
  (Choose $\alpha_1 = 1$, and on affine subsets of A set the variables corresponding to all other basis elements α_i of L/K equal to zero.)
- So we have a K-morphism of group varieties

$$\mathrm{Res}_{L/K}(\phi) \circ \chi : A \to (\mathrm{Res}_{L/K}(E))^g,$$

and since A is simple the image must lie in a single factor.

Decomposing the Weil restriction

- Let E be an elliptic curve over $\mathbb{F}_p$, $\pi = Frob_p \in \operatorname{End}(E)$.
- $E(\mathbb{F}_{p^d}) = \ker(\pi^d - 1)$.
- Since $x^d - 1 = \prod_{e|d} \Phi_e(x)$, there is a subgroup of $E(\mathbb{F}_{p^d})$ given by $\ker(\Phi_d(\pi))$.
- Points in this subgroup correspond to $\mathbb{F}_p$-points of a subvariety $V_d \subset \operatorname{Res}_{\mathbb{F}_{p^d}/\mathbb{F}_p}(E)$ of dimension $\varphi(d)$.
- We get a decomposition into *primitive subvarieties*

$$\operatorname{Res}_{\mathbb{F}_{p^d}/\mathbb{F}_p}(E) \sim \bigoplus_{e|d} V_e(E).$$

- If E ordinary and $\pi \notin \mathbb{Q}(\zeta_d)$, then $V_d(E)$ is simple.

The situation at present

For A a simple abelian surface,

$$A \xrightarrow[\mathbb{F}_{p^d}]{\sim} E^2 \quad \Rightarrow \quad A \xrightarrow[\mathbb{F}_p]{} \mathrm{Res}_{\mathbb{F}_{p^d}/\mathbb{F}_p}(E).$$

If $d = 3$ or 4 and $\pi \notin \mathbb{Q}(\zeta_d)$ then

$$A \xrightarrow[\mathbb{F}_p]{\sim} V_d(E) \subset \mathrm{Res}_{\mathbb{F}_{p^d}/\mathbb{F}_p}(E).$$

If $E(\mathbb{F}_{p^d})$ is pairing-friendly with d minimal,

(i.e., $r \mid \#E(\mathbb{F}_{p^d})$ and $r \mid p^k - 1$)

then $V_d(E)(\mathbb{F}_p)$ is pairing-friendly.

Problem: Given such an E, construct C with

$$\mathrm{Jac}(C) \xrightarrow[\mathbb{F}_{p^d}]{\sim} E^2.$$

A generalization of KT curves

Let $C/\mathbb{F}_p$ be the hyperelliptic curve given by

$$y^2 = x^5 + ax^3 + bx.$$

Over $\mathbb{F}_p(b^{1/8})$, C maps to two elliptic curves E, E' defined over $\mathbb{F}_p(\sqrt{b})$.

- E and E' are isomorphic over $\mathbb{F}_p(i)$,
- $\Rightarrow$ Jac(C) is isogenous over $\mathbb{F}_p(b^{1/8}, i)$ to $E \times E$,

Theorem: Suppose $b \in (\mathbb{F}_p^*)^2 \setminus (\mathbb{F}_p^*)^4$, E ordinary, $\pi_E \notin \mathbb{Q}(i)$. Then Jac($C$) is simple and isogenous over $\mathbb{F}_p$ to $V_4(E)$.

- If $c = a/\sqrt{b}$, then $j(E) = \frac{2^6(3c-10)^3}{(c-2)(c+2)^2}$
- Given $j(E)$, we can find equation for C.

A generalization of KT curves

Let $C/\mathbb{F}_p$ be the hyperelliptic curve given by

$$y^2 = x^5 + ax^3 + bx.$$

Over $\mathbb{F}_p(b^{1/8})$, C maps to two elliptic curves E, E' defined over $\mathbb{F}_p(\sqrt{b})$.

- E and E' are isomorphic over $\mathbb{F}_p(i)$,
- $\Rightarrow$ Jac(C) is isogenous over $\mathbb{F}_p(b^{1/8}, i)$ to $E \times E$,

Theorem: Suppose $b \in (\mathbb{F}_p^*)^2 \setminus (\mathbb{F}_p^*)^4$, E ordinary, $\pi_E \notin \mathbb{Q}(i)$. Then Jac($C$) is simple and isogenous over $\mathbb{F}_p$ to $V_4(E)$.

- If $c = a/\sqrt{b}$, then $j(E) = \frac{2^6(3c-10)^3}{(c-2)(c+2)^2}$
- Given $j(E)$, we can find equation for C.

A second family of curves

Analogous results hold for the hyperelliptic curve $C/\mathbb{F}_p$ given by

$$y^2 = x^6 + ax^3 + b.$$

If certain conditions hold, there is an elliptic curve $E/\mathbb{F}_p$ such that $\mathrm{Jac}(C)$ is simple and isogenous over $\mathbb{F}_p$ to $V_3(E)$.

One final problem

- Recall: if $E(\mathbb{F}_{p^d})$ is pairing-friendly with d minimal,
  $\big($ i.e., $r \mid \#E(\mathbb{F}_{p^d})$ and $r \mid p^k - 1$ $\big)$
  then $V_d(E)(\mathbb{F}_p)$ is pairing-friendly.
- Given such an E, with $d = 3$ or 4, we can (often)* construct C such that $\mathrm{Jac}(C) \sim V_d(E)$.
- Question: How to construct such an E?
- Answer: adapt algorithm of Cocks-Pinch.
  - Input: quadratic imaginary field K, integers k and d.
  - Output: Frobenius element $\pi \in \mathcal{O}_K$, subgroup order r.
  - Use *CM method* to find $j(E)$ for E with Frobenius element π (requires K "small").
- We can now construct a pairing-friendly genus 2 curve C!

*Assuming that the equation involving $j(E)$ has a solution in $\mathbb{F}_p$

Best results

- Brezing-Weng modification of Cocks-Pinch algorithm:
  1. Parametrize Frobenius as $\pi(x) \in K[x]$ and subgroup order as $r(x) \in \mathbb{Z}[x]$.
  2. Find x_0 with $p(x_0) = \pi(x_0)\overline{\pi}(x_0)$ and $r(x_0)$ both prime.
  3. Continue construction as before to find a pairing-friendly hyperelliptic cuve $C/\mathbb{F}_{p(x_0)}$.
- For large x_0, $\rho(\mathrm{Jac}(C)) = \dfrac{\log p(x_0)^2}{\log r(x_0)} \approx \dfrac{4 \deg \pi}{\deg r}$.

Best result: $k = 27$, $d = 3$, $K = \mathbb{Q}(i)$, $r(x) = \Phi_{108}(x)$,

$$\pi(x) = \frac{1}{2}\left(-x^{20} + x^{18} + ix^{11} + ix^{9} + x^{2} - 1\right), \quad \rho \approx 20/9 \approx 2.22.$$

Best results

- Brezing-Weng modification of Cocks-Pinch algorithm:
  1. Parametrize Frobenius as $\pi(x) \in K[x]$ and subgroup order as $r(x) \in \mathbb{Z}[x]$.
  2. Find x_0 with $p(x_0) = \pi(x_0)\overline{\pi}(x_0)$ and $r(x_0)$ both prime.
  3. Continue construction as before to find a pairing-friendly hyperelliptic cuve $C/\mathbb{F}_{p(x_0)}$.
- For large x_0, $\rho(\mathrm{Jac}(C)) = \frac{\log p(x_0)^2}{\log r(x_0)} \approx \frac{4 \deg \pi}{\deg r}$.

Best result: $k = 27$, $d = 3$, $K = \mathbb{Q}(i)$, $r(x) = \Phi_{108}(x)$,

$$\pi(x) = \frac{1}{2}\left(-x^{20} + x^{18} + ix^{11} + ix^9 + x^2 - 1\right), \quad \rho \approx 20/9 \approx 2.22.$$

Extra roots of unity cause problems

- On inputs $d = 4$, $K = \mathbb{Q}(\zeta_3)$, algorithm produces $E/\mathbb{F}_p$ with $j(E) = 0$ and $V_4(E)$ pairing-friendly.
- Can always find $C/\mathbb{F}_p$ with $\mathrm{Jac}(C) \sim_{\mathbb{F}_{p^4}} E' \times E'$, $j(E') = 0$, and $\mathrm{Jac}(C)$ simple (so $\mathrm{Jac}(C) \sim_{\mathbb{F}_p} V_4(E')$).
- $\mathit{Frob}_p(E) = \alpha \cdot \mathit{Frob}_p(E')$ for some α with $\alpha^6 = 1$.
- Good case: if $\alpha = \pm 1$ then $\mathrm{Jac}(C) \sim V_4(E') \sim V_4(E)$.
- Bad case: if $\alpha \neq \pm 1$ then $\mathrm{Jac}(C) \sim V_4(E') \sim A$ for some 2-dimensional subvariety $A \subset V_{12}(E)$.

Experimental data

Heuristically, if parameters are "random" then we expect the good case $\alpha = \pm 1$ one third of the time.

- π not parametrized as a polynomial:
  in 1000 trials, **323** curves fall into the good case.
- $\pi(x) = \frac{1}{6}\left((\gamma - 3)x^3 - (\gamma + 3)x^2 - 2\gamma x + 2\gamma\right)$ $[\gamma = \sqrt{-3}]$:
  in 1000 trials, **1000** curves fall into the good case.
- $\pi(x) = \frac{1}{12}\left((\gamma - 1)x^2 + (-2\gamma + 6)x + (6\gamma - 6)\right)$ [Kachisa]:
  in 1000 trials, **0** curves fall into in the good case.

A pairing-friendly curve C produced from the last π would set a record: $\rho(\mathrm{Jac}(C)) \approx 2$.

Experimental data

Heuristically, if parameters are "random" then we expect the good case $\alpha = \pm 1$ one third of the time.

- π not parametrized as a polynomial:
  in 1000 trials, **323** curves fall into the good case.
- $\pi(x) = \frac{1}{6}\left((\gamma - 3)x^3 - (\gamma + 3)x^2 - 2\gamma x + 2\gamma\right)$ $[\gamma = \sqrt{-3}]$:
  in 1000 trials, **1000** curves fall into the good case.
- $\pi(x) = \frac{1}{12}\left((\gamma - 1)x^2 + (-2\gamma + 6)x + (6\gamma - 6)\right)$ [Kachisa]:
  in 1000 trials, **0** curves fall into in the good case.

A pairing-friendly curve C produced from the last π would set a record: $\rho(\mathrm{Jac}(C)) \approx 2$.

Some questions

1. Explain this experimental behavior.
2. If $\mathrm{Jac}(C) \sim A \subset V_{12}(E)$, is $V_4(E)$ isogenous to $\mathrm{Jac}(C')$ for *any* curve $C'/\mathbb{F}_p$?
3. How do we find a curve $C'/\mathbb{F}_p$ with $\mathrm{Jac}(C') \sim V_4(E)$ in this case?

   If $p \equiv 3 \pmod 4$ then $y^2 = x^5 + ax^3 + bx$ splits over $\mathbb{F}_p$ or maps to elliptic curves defined over $\mathbb{F}_{p^2}$ — our method fails!
4. For $E/\mathbb{F}_p$ produced from our algorithm, find $C'/\mathbb{F}_p$ with $\mathrm{Jac}(C') \sim V_4(E)$, or show none exists.

Answers?

Some questions

1. Explain this experimental behavior.
2. If $\mathrm{Jac}(C) \sim A \subset V_{12}(E)$, is $V_4(E)$ isogenous to $\mathrm{Jac}(C')$ for *any* curve $C'/\mathbb{F}_p$?
3. How do we find a curve $C'/\mathbb{F}_p$ with $\mathrm{Jac}(C') \sim V_4(E)$ in this case?

   If $p \equiv 3 \pmod 4$ then $y^2 = x^5 + ax^3 + bx$ splits over $\mathbb{F}_p$ or maps to elliptic curves defined over $\mathbb{F}_{p^2}$ — our method fails!
4. For $E/\mathbb{F}_p$ produced from our algorithm, find $C'/\mathbb{F}_p$ with $\mathrm{Jac}(C') \sim V_4(E)$, or show none exists.

Answers?

Some questions

1. Explain this experimental behavior.
2. If $\mathrm{Jac}(C) \sim A \subset V_{12}(E)$, is $V_4(E)$ isogenous to $\mathrm{Jac}(C')$ for *any* curve $C'/\mathbb{F}_p$?
3. How do we find a curve $C'/\mathbb{F}_p$ with $\mathrm{Jac}(C') \sim V_4(E)$ in this case?

   If $p \equiv 3 \pmod 4$ then $y^2 = x^5 + ax^3 + bx$ splits over $\mathbb{F}_p$ or maps to elliptic curves defined over $\mathbb{F}_{p^2}$ — our method fails!
4. For $E/\mathbb{F}_p$ produced from our algorithm, find $C'/\mathbb{F}_p$ with $\mathrm{Jac}(C') \sim V_4(E)$, or show none exists.

Answers?