Explicit isogenies and the Discrete Logarithm Problem in genus three

Benjamin Smith

INRIA Saclay–Île-de-France Laboratoire d'informatique de l'école polytechnique (LIX)

EUROCRYPT 2008 : Istanbul, April 2008

We work over \mathbb{F}_q , with $\gcd(q, 6) = 1$

Discrete Logarithm Problems

Recall the Elliptic Curve Discrete Logarithm Problem:

Given an elliptic curve $E: y^2 = F(x)$ over \mathbb{F}_q and P and Q in $E(\mathbb{F}_q)$ such that Q = [m]P, compute m.

We will consider the analogous problem where E is replaced by the Jacobian J_X of a curve of genus 3.

A brief look at Jacobians of genus 3 curves

Suppose X is an algebraic curve of genus 3. Its **Jacobian**, J_X , is a 3-dimensional algebraic group associated to X.

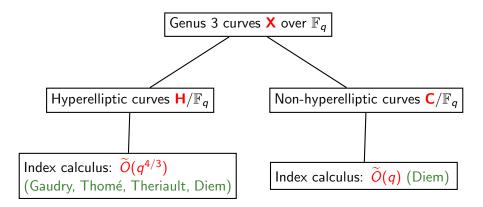
Points of J_X correspond to **divisor classes** on X (elements of $Pic^0(X)$); that is, equivalence classes of formal sums of points on X.

 $\# J_X(\mathbb{F}_q) = O(q^3)$, so Pollard rho / BSGS solves DLP instances in $J_X(\mathbb{F}_q)$ in $\widetilde{O}(q^{3/2})$ group operations.

We can do better using **index calculus** algorithms, which use the geometry of X.

Dichotomy of genus 3 curves and their DLPs

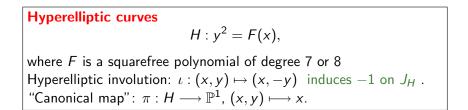
Curves of genus 3 fall into two geometric classes.



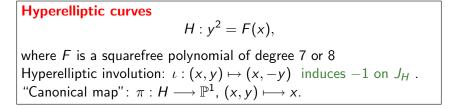
Too much mathematics already? Official alternative entertainment at

http://tinyurl.com/2g9mqh

Geometry of genus 3 curves



Geometry of genus 3 curves



Non-hyperelliptic curves

$$C: F(x_0, x_1, x_2) = 0,$$

where F is a homogeneous polynomial of degree 4 Canonical map: embedding $C \hookrightarrow \mathbb{P}^2$ (Nonsingular plane quartic).

We can compute canonical maps in polynomial time.

Smith (LIX)

Isogenies and the DLP

Hyperelliptic and non-hyperelliptic curves have different geometries.

H cannot be isomorphic to C $\implies J_H$ cannot be isomorphic to J_C (as PPAVs)

...so we can't translate index calculus algorithms between J_C and J_H .

Isogenies and the DLP

Hyperelliptic and non-hyperelliptic curves have different geometries.

H cannot be isomorphic to C $\implies J_H$ cannot be isomorphic to J_C (as PPAVs)

...so we can't translate index calculus algorithms between J_C and J_H .

We **can** have homomorphisms $\phi : J_H \longrightarrow J_C$, which we could use to translate DLPs from J_H to J_C :

$$Q = [m]P \implies \phi(Q) = [m]\phi(P).$$

DLP-based crypto uses absolutely simple Jacobians \implies all useful homomorphisms are **isogenies** (surjective, finite kernel).

Smith (LIX)

Aim: explicit isogenies from hyperelliptic to non-hyperelliptic Jacobians. **Problem**: a priori, we don't know of any useful isogenies... BUT:

Quotients of J_H by maximal Weil-isotropic subgroups give isogenies to 3-dimensional PPAVs.

Aim: explicit isogenies from hyperelliptic to non-hyperelliptic Jacobians. **Problem**: a priori, we don't know of any useful isogenies... BUT:

Quotients of J_H by maximal Weil-isotropic subgroups give isogenies to 3-dimensional PPAVs.

+

Oort and Ueno: every 3-dimensional PPAV over \mathbb{F}_q is isomorphic $/\mathbb{F}_{q^2}$ to the Jacobian of a genus 3 curve.

Aim: explicit isogenies from hyperelliptic to non-hyperelliptic Jacobians. **Problem**: a priori, we don't know of any useful isogenies... BUT:

Quotients of J_H by maximal Weil-isotropic subgroups give isogenies to 3-dimensional PPAVs.

+

Oort and Ueno: every 3-dimensional PPAV over \mathbb{F}_q is isomorphic $/\mathbb{F}_{q^2}$ to the Jacobian of a genus 3 curve.

quotients of J_H by maximal Weil-isotropic subgroups give isogenies to Jacobians of other genus 3 curves.

For an isogeny $\phi: J_H \to J_X$ to be useful to us,

(1) X must be isomorphic to a non-hyperelliptic C:

For an isogeny $\phi: J_H \to J_X$ to be useful to us,

(1) X must be isomorphic to a non-hyperelliptic C:

The isomorphism classes of genus 3 Jacobians form a 6-dimensional moduli space, with the hyperelliptic Jacobians forming a 5-dimensional subspace. ...so we expect $X \cong C$ with overwhelming probability.

For an isogeny $\phi: J_H \to J_X$ to be useful to us,

(1) X must be isomorphic to a non-hyperelliptic C:

The isomorphism classes of genus 3 Jacobians form a 6-dimensional moduli space, with the hyperelliptic Jacobians forming a 5-dimensional subspace. ...so we expect $X \cong C$ with overwhelming probability.

(2) the isogeny must be defined over \mathbb{F}_q :

For an isogeny $\phi: J_H \to J_X$ to be useful to us,

(1) X must be isomorphic to a non-hyperelliptic C:

The isomorphism classes of genus 3 Jacobians form a 6-dimensional moduli space, with the hyperelliptic Jacobians forming a 5-dimensional subspace. ...so we expect $X \cong C$ with overwhelming probability.

(2) the isogeny must be defined over \mathbb{F}_q :

If $\phi: J_H \to J_C$ is defined over \mathbb{F}_{q^d} , then $\phi(J_H(\mathbb{F}_q)) \subset J_C(\mathbb{F}_{q^d})$, where Diem's algorithm works in time $\widetilde{O}(q^d)$; we need d < 4/3.

Minimum requirement: ker ϕ defined over \mathbb{F}_q (Frobenius-stable) (note: ker ϕ need not be contained in $J_H(\mathbb{F}_q)$)

The big problem

We can try to construct useful isogenies by computing quotients by (Frobenius-stable, maximal Weil-isotropic) subgroups.

Problem: lack of explicit constructions for genus 3 isogenies: For most choices of kernel subgroup, no explicit construction of the quotient isogeny is known.

We will give a solution to a special case (with kernel $\cong (\mathbb{Z}/2\mathbb{Z})^3$) that turns out to be useful for a large proportion of genus 3 Jacobians.

Computing explicit isogenies

The Weierstrass points of $H: y^2 = \widetilde{F}(x, z)$ are the eight points W_1, \ldots, W_8 of $H(\overline{\mathbb{F}_q})$ where $y(W_i) = 0$.

The divisor classes $[W_1 - W_2]$, $[W_3 - W_4]$, $[W_5 - W_6]$, and $[W_7 - W_8]$ generate a subgroup $S \cong (\mathbb{Z}/2\mathbb{Z})^3$ of J_H (depends on the ordering of the W_i).

We call such subgroups tractable subgroups.

We have derived explicit formulae for isogenies with tractable kernels.

Trigonal maps

Suppose we are given H and $S = \langle [W_i - W_{i+1}] : i \in \{1, 3, 5, 7\} \rangle$.

Let $g: \mathbb{P}^1 \to \mathbb{P}^1$ be a 3-to-1 (trigonal) map such that

 $g(\pi(W_i)) = g(\pi(W_{i+1}))$ for each $[W_i - W_{i+1}] \in S$.

Trigonal maps

Suppose we are given H and $S = \langle [W_i - W_{i+1}] : i \in \{1, 3, 5, 7\} \rangle$.

Let $g: \mathbb{P}^1 \to \mathbb{P}^1$ be a 3-to-1 (trigonal) map such that

$$g(\pi(W_i))=g(\pi(W_{i+1}))$$
 for each $[W_i-W_{i+1}]\in S.$

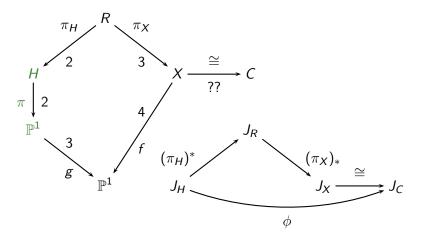
Given a tractable subgroup S/\mathbb{F}_q , we compute g using basic linear algebra. This requires solving a quadratic equation over \mathbb{F}_q $\implies 50\%$ chance that g is **not** defined over \mathbb{F}_q (since only half of the elements of \mathbb{F}_q are squares).

(Later: explicit descent *should* allow us to avoid this problem.)

The trigonal construction

Recillas' **trigonal construction**, applied to $\pi : H \to \mathbb{P}^1$ and $g : \mathbb{P}^1 \to \mathbb{P}^1$, yields a curve X of genus 3 and a 4-to-1 map $f : X \to \mathbb{P}^1$.

Donagi and Livné: there is an isogeny $\phi : J_H \to J_X$ with kernel S.



If Q is a point on \mathbb{P}^1 , then

$$(g \circ \pi)^{-1}(Q) = \{P_1, P_2, P_3, \iota(P_1), \iota(P_2), \iota(P_3)\} \subset H$$
$$f^{-1}(Q) = \left\{ \begin{array}{l} Q_1 \leftrightarrow \{P_1 + P_2 + P_3, \ \iota(P_1) + \iota(P_2) + \iota(P_3)\}, \\ Q_2 \leftrightarrow \{P_1 + \iota(P_2) + \iota(P_3), \ \iota(P_1) + P_2 + P_3\}, \\ Q_3 \leftrightarrow \{\iota(P_1) + P_2 + \iota(P_3), \ P_1 + \iota(P_2) + P_3\}, \\ Q_4 \leftrightarrow \{\iota(P_1) + \iota(P_2) + P_3, \ P_1 + P_2 + \iota(P_3)\} \end{array} \right\} \subset X$$

If Q is a point on \mathbb{P}^1 , then

$$(g \circ \pi)^{-1}(Q) = \{P_1, P_2, P_3, \iota(P_1), \iota(P_2), \iota(P_3)\} \subset H$$
$$f^{-1}(Q) = \begin{cases} Q_1 \leftrightarrow \{P_1 + P_2 + P_3, \iota(P_1) + \iota(P_2) + \iota(P_3)\}, \\ Q_2 \leftrightarrow \{P_1 + \iota(P_2) + \iota(P_3), \iota(P_1) + P_2 + P_3\}, \\ Q_3 \leftrightarrow \{\iota(P_1) + P_2 + \iota(P_3), P_1 + \iota(P_2) + P_3\}, \\ Q_4 \leftrightarrow \{\iota(P_1) + \iota(P_2) + P_3, P_1 + P_2 + \iota(P_3)\} \end{cases} \subset X$$

Mumford representation: triples correspond to ideals

$$P_1 + P_2 + P_3 \longleftrightarrow (a(x), y - b(x))$$

a monic, deg *a* = 3, deg *b* = 2, *b*² \equiv *F* mod *a*
 $a(x(P_i)) = 0, \ b(x(P_i)) = y(P_i)$

An affine model for X

Mumford representation: pairs of triples correspond to pairs of ideals

$$\{P_1 + P_2 + P_3, \iota(P_1) + \iota(P_2) + \iota(P_3)\} \longleftrightarrow (a(x), y \pm b(x))$$

— ie X parametrizes the coefficients of a and b^2 .

An affine model for X

Mumford representation: pairs of triples correspond to pairs of ideals

$$\{P_1 + P_2 + P_3, \iota(P_1) + \iota(P_2) + \iota(P_3)\} \longleftrightarrow (a(x), y \pm b(x))$$

— ie X parametrizes the coefficients of a and b^2 .

- If g is defined by $g: x \mapsto t = N(x)/D(x)$, then take a(x) = N(x) tD(x).
- 2 Let the coefficients of b^2 be variables, then expand $b^2 \equiv F \mod a$ to get defining equations for an affine model of X.
- **③** The map $f : X \to \mathbb{P}^1$ is projection onto the *t*-coordinate.

An affine model for X

Mumford representation: pairs of triples correspond to pairs of ideals

$$\{P_1 + P_2 + P_3, \iota(P_1) + \iota(P_2) + \iota(P_3)\} \longleftrightarrow (a(x), y \pm b(x))$$

— ie X parametrizes the coefficients of a and b^2 .

- If g is defined by $g : x \mapsto t = N(x)/D(x)$, then take a(x) = N(x) tD(x).
- 2 Let the coefficients of b^2 be variables, then expand $b^2 \equiv F \mod a$ to get defining equations for an affine model of X.
- **③** The map $f: X \to \mathbb{P}^1$ is projection onto the *t*-coordinate.

If g is defined over \mathbb{F}_q , then so is our model of X. If not, *in theory* we can use descent to find a model for X over \mathbb{F}_q .

The isogeny

Given X, f, and g, we compute the relative product $H \times_{\mathbb{P}^1} X$. After solving a quadratic equation — with 50% chance of success — $H \times_{\mathbb{P}^1} X$ splits into two isomorphic curves, R and R' (correspondences).

Take R; we have natural projections $\pi_H^R : R \to H$ and $\pi_X^R : R \to X$. We have an isogeny $\phi = (\pi_X^R)_* \circ (\pi_H^R)^*$; in terms of divisor classes,

$$\phi: \left[\sum_{i} n_{i} P_{i}\right] \longmapsto \left[\sum_{i} n_{i} \sum_{Q \in (\pi_{H}^{R})^{-1}(P_{i})} \pi_{X}^{R}(Q)\right]$$

Using R' instead gives us $-\phi$. essential square root — descent cannot fix this.

Rationality

Recall requirement (2):

Our isogenies are only useful if they are defined over \mathbb{F}_q .

We therefore need

- An \mathbb{F}_q -rational kernel subgroup S
- **2** A model for X over \mathbb{F}_q
 - \longrightarrow probability 1/2 for a given S over \mathbb{F}_q
 - or 1 with explicit descent on X
- The correspondence R to be defined over \mathbb{F}_q \longrightarrow probability 1/2 for a given S, g, X over \mathbb{F}_q
- \implies probability 1/4 (or 1/2) for each tractable $S\subset J_H$ defined over $\mathbb{F}_q.$

Rationality

Recall requirement (2):

Our isogenies are only useful if they are defined over \mathbb{F}_q .

We therefore need

- An \mathbb{F}_q -rational kernel subgroup S
- **2** A model for X over \mathbb{F}_q
 - \longrightarrow probability 1/2 for a given S over \mathbb{F}_q
 - or 1 with explicit descent on X
- The correspondence R to be defined over \mathbb{F}_q \longrightarrow probability 1/2 for a given S, g, X over \mathbb{F}_q
- \implies probability 1/4 (or 1/2) for each tractable $S\subset J_H$ defined over $\mathbb{F}_q.$

Question: how many tractable subgroups S over \mathbb{F}_q ?

How many kernel subgroups are there?

 $H: y^2 = \widetilde{F}(x, z): \widetilde{F}$ homogeneous, squarefree, deg $\widetilde{F} = 8$. S(H) := set of \mathbb{F}_q -rational tractable subgroups of J_H .

Degrees of k-irreducible factors of \widetilde{F}	$\#\mathcal{S}(H)$
(8), (6, 2), (6, 1, 1), (4, 2, 1, 1)	1
(4, 4)	5
(4, 2, 2), (4, 1, 1, 1, 1), (3, 3, 2), (3, 3, 1, 1)	3
(2, 2, 2, 1, 1)	7
(2, 2, 1, 1, 1, 1)	9
(2, 1, 1, 1, 1, 1, 1)	15
(2,2,2,2)	25
(1, 1, 1, 1, 1, 1, 1, 1)	105
Other	0

"Security" of genus 3 hyperelliptic Jacobians depends significantly on the factorization of the hyperelliptic polynomial F.

How often do we have a rational isogeny?

Summing over probabilities of factorization types, we find that for a randomly chosen $H: y^2 = F(x)$, there is an expectation of

 $\sim 18.57\%$

that our methods will produce an isogeny $J_H \to J_C$ over \mathbb{F}_q .

How often do we have a rational isogeny?

Summing over probabilities of factorization types, we find that for a randomly chosen $H: y^2 = F(x)$, there is an expectation of

 $\sim 18.57\%$

that our methods will produce an isogeny $J_H \to J_C$ over \mathbb{F}_q .

If we can use descent to account for the square root in computing g, we obtain an even better expectation:

 $\sim 31.13\%$

• Our approach is independent of the size of the DLP subgroup.

- Our approach is independent of the size of the DLP subgroup.
- **②** These constructions are *very* fast (and also polynomial-time).

- Our approach is independent of the size of the DLP subgroup.
- In the second transformed and the second transformation of transformati
- With constructions for more general isogenies (eg with kernels ≅ (Z/3Z)³, (Z/5Z)³, etc...), more hyperelliptic curves will be vulnerable to O(q) index calculus (including curves in characteristics 2 and 3).

- Our approach is independent of the size of the DLP subgroup.
- In the second transformed and the second transformation of transformati
- With constructions for more general isogenies (eg with kernels ≅ (Z/3Z)³, (Z/5Z)³, etc...), more hyperelliptic curves will be vulnerable to O(q) index calculus (including curves in characteristics 2 and 3).
- This approach is not generally applicable in lower genus (low probability of isogeny mapping to a weak curve...)

- Our approach is independent of the size of the DLP subgroup.
- In the second terms are very fast (and also polynomial-time).
- With constructions for more general isogenies (eg with kernels ≅ (Z/3Z)³, (Z/5Z)³, etc...), more hyperelliptic curves will be vulnerable to O(q) index calculus (including curves in characteristics 2 and 3).
- This approach is not generally applicable in lower genus (low probability of isogeny mapping to a weak curve...)
- ...and probably will not work in higher genus either (negligible probability of isogeny mapping to any Jacobian)

Thanks

Thanks: to Roger Oyono and Christophe Ritzenthaler