Endomorphism rings of genus 2 jacobians

Sorina Ionica

Ecole Normale Supérieure and Inria, France

ECC 2012
Cryptographic motivation

We need an abelian variety of small dimension (i.e. 1,2) defined over $\mathbb{F}_q$ s.t. $\# A(\mathbb{F}_q)$ is divisible by a large prime number.

For pairing based cryptography, use the complex multiplication method to generate curves with prescribed number of points. → needs precomputing the class polynomials.
Let $J$ be a (simple) abelian surface over $\mathbb{C}$.

$\text{End}(J)$ is an order of a (primitive) quartic CM field $K$ (totally imaginary quadratic extension of a totally real number field).

The class polynomials $H_1, H_2, H_3 \in \mathbb{Q}[X]$ parametrize the invariants of all abelian varieties $A/\mathbb{C}$ with $\text{End}(A) \cong \mathcal{O}_K$.

Assume $p$ is a "good" prime

$$H_i(X) = \prod_{\text{End}(A) \cong \mathcal{O}_K} (X - j_i(A))$$

$$\#J(\mathbb{F}_p) = N_{K/\mathbb{Q}}(\pi - 1),$$ where $\pi$ is the Frobenius endomorphism.
Eisenträger, Freeman, Lauter, Bröker, Gruenewald, Robert:

- Select a "good" prime $p$.
- For each abelian surface $J$ in the $p^3$ isomorphism classes
  - Check if $J$ is in the right isogeny class.
  - Check if $\text{End}(J) \cong \mathcal{O}_K$.
- Reconstruct $H_i \mod p$ from jacobians with maximal endomorphism ring

Compute class polynomials modulo small "good" primes and use the CRT to reconstruct $H_1, H_2, H_3$. 
Eisenträger, Freeman, Lauter, Bröker, Gruenewald, Robert:

- Select a “good” prime $p$.
- For each abelian surface $J$ in the $p^3$ isomorphism classes.
  - Check if $J$ is in the right isogeny class.
  - Check if $\text{End}(J) \simeq \mathcal{O}_K$.
  - Generate jacobians with CM by $\mathcal{O}_K$ by computing horizontal isogenies* from $J$.
- Reconstruct $H_i \mod p$ from jacobians with maximal endomorphism ring

*An isogeny $I : J_1 \to J_2$ is horizontal iff $\text{End } J_1 \simeq \text{End } J_2$. 
I.-Joux 2010: algorithms for horizontal isogeny and endomorphism ring computation in genus 1 by using the Tate pairing

F. Morain: “je suis sûr qu’il y a quelque chose à dire sur les matrices du Frobenius. De toute façon, tout est dans le Frobenius!”

meaning

“It’s all about the Frobenius!”

Claim: Indeed, but from a computational point of view, using pairings is faster in many cases.

\[ \text{End}(J) \otimes \mathbb{Z}_\ell \rightarrow \text{End}_{\mathbb{F}_q}(T_\ell(J)) \text{ bijectively} \]
Let $K$ be a quartic CM field and assume that $K = \mathbb{Q}(\eta)$ with

$$
\eta = i \sqrt{a + b^{-1} + \frac{\sqrt{d}}{2}} \text{ for } d \equiv 1 \mod 1
$$

$$
\eta = i \sqrt{a + b \sqrt{d}} \text{ for } d \equiv 2, 3 \mod 4
$$

Assume real multiplication $\mathcal{O}_{K_0}$ has class number 1.

Let $J$ be a jacobian of a genus 2 curve defined over $\mathbb{F}_q$.

$J$ is ordinary, i.e. $\text{End}(J)$ is an order of $K$.

$$
\mathbb{Z}[\pi, \bar{\pi}] \subset \text{End}(J) \subset \mathcal{O}_K
$$
Eisenträger and Lauter’s algorithm (2005), Freeman-Lauter (2008)

Idea: If $\alpha : J \rightarrow J$ is an endomorphism, then $\frac{\alpha}{n}$ is an endomorphism iff $J[n] \subset \text{Ker} \; \alpha$.

Check if an order $O$ is contained in $\text{End}(J)$:

- Write down a basis for the order $O$: $\gamma_i = \frac{\alpha_i}{n_i}$, with $\alpha_i \in \mathbb{Z}[\pi]$.
- Check if $\gamma_i \in \text{End}(J)$ by checking if $\alpha_i$ is zero on $J[n_i]$.

Since $n_i | [O_K : \mathbb{Z}[\pi, \bar{\pi}]]$ we end up working over large extension fields!
The smallest extension field $\mathbb{F}_{q^r}$ s.t. $J[\ell] \subset J(\mathbb{F}_{q^r})$ has degree $r$ at most $\ell^4$.

If $J[\ell^2] \not\subset J(\mathbb{F}_{q^r})$, then $J[\ell^2] \subset J(\mathbb{F}_{q^{r\ell}})$

$$J[\ell^3] \subset J(\mathbb{F}_{q^{r\ell^2}})$$

... 

Bottleneck: group structure computation $\implies \ell$ is small
Computing the endomorphism ring

- For small $\ell$, use Eisenträger-Lauter

- If $\ell$ is larger, use Bisson’s algorithm (2012)
  - *smooth* relations in the class group of the order $\mathcal{O}$
  - corresponding *smooth* horizontal isogeny chains

$$O((\exp \sqrt{\log q \log \log q})^{2\sqrt{3}+o(1)})$$

under GRH and other heuristic assumptions
Let $\theta \in \mathcal{O}$. We define

$$v_{\ell,\mathcal{O}}(\theta) := \max_{a \in \mathbb{Z}} \{ m|\theta + a \in \ell m \mathcal{O} \}$$

How do we compute this?

Consider a $\mathbb{Z}$-basis $1, \delta, \gamma, \eta$ for $\mathcal{O}$:

Write $\theta = a_1 + a_2 \delta + a_3 \gamma + a_4 \eta$. Then

$$v_{\ell,\mathcal{O}}(\theta) := v_{\ell}(\gcd(a_2, a_3, a_4)).$$
Checking locally maximal orders at $\ell$

In general, $v_{\ell,\mathcal{O}}(\theta) \leq v_{\ell,\mathcal{O}_K}(\theta)$

Take $\mathcal{O}_K = [1, \omega]$ and $\eta = i\sqrt{a + b\omega}$, with $(b, \ell) = 1$. Then $\theta = a_1 + a_2\omega + (a_3 + a_4\omega)\eta$, $a_i \in \mathbb{Z}$.

**Lemma** *

Let $\mathcal{O}$ be an order such that $\theta \in \mathcal{O}$ and $[\mathcal{O}_K : \mathcal{O}]$ is divisible by a power of $\ell$. If $\max(v_{\ell}(\frac{a_3 - a_4}{\ell}), v_{\ell}(\frac{\ell(a_3 - a_4)}{\ell^2})) < \min(v_{\ell}(a_3), v_{\ell}(a_4))$ then $v_{\ell,\mathcal{O}}(\theta) < v_{\ell,\mathcal{O}_K}(\theta)$.

Let $v_{\ell}(\pi) = v_{\ell,\text{End}(J)}(\pi)$.

A simple criterion: check if $v_{\ell}(\pi) = v_{\ell,\mathcal{O}_K}(\pi)$. 

Checking locally maximal orders at $\ell$

How do we compute $v_\ell(\pi)$?

**Proposition**

$v_\ell(\pi)$ is the largest integer $m$ such that the Frobenius action on $T_\ell(J)$ is a multiple of the identity up to precision $m$.

The matrix of the Frobenius is of the form

$$
\begin{pmatrix}
\lambda & 0 & 0 & 0 \\
0 & \lambda & 0 & 0 \\
0 & 0 & \lambda & 0 \\
0 & 0 & 0 & \lambda
\end{pmatrix}
\mod \ell^k, k \leq m
$$

We could compute the action of the Frobenius on $J[\ell], J[\ell^2] \ldots$

This means working over large extension fields very quickly, so **NO!**
How do we compute $v_\ell(\pi)$?

2006 Schmoyer: bring pairings into play!
Let $A$ be an abelian variety defined over a field $K$. $A[m]$ is the $m$-torsion and $\hat{A}[m] \simeq \text{Hom}(A[m], \mu_m)$.

**Weil pairing**

$$e_m : A[m] \times \hat{A}[m] \to \mu_m$$
is a bilinear, non-degenerate map.

If $A$ is a principally polarized variety

$$e_m : A[m] \times A[m] \to \mu_m$$
$$(P, Q) \to e_m(P, Q).$$
The Tate pairing

We denote by $G_K = \text{Gal}(\bar{K}/K)$ the Galois group.

Consider $0 \to A[m] \to A(\bar{K}) \xrightarrow{m} A(\bar{K}) \to 0$.

Take Galois cohomology and get connecting morphism

$$\delta : A(K)/mA(K) = H^0(G_K, A)/mH^0(G_K, A) \to H^1(G_K, A[m])$$

$$P \to F_P,$$

where we take $\bar{P}$ such that $m\bar{P} = P$ and define

$$F_P(\sigma) : G_K \to A(\bar{K})[m]$$

$$\sigma \to \sigma \cdot \bar{P} - \bar{P}.$$
The Tate pairing

We get the map

\[ A(K)/mA(K) \times \hat{A}[m](K) \rightarrow H^1(G_K, \mu_m) \]
\[ (P, Q) \rightarrow [\sigma \mapsto e_m(F_P(\sigma), Q)] \]

bilinear, non-degenerate
The Tate pairing

We get the map

\[
A(K)/mA(K) \times A[m](K) \rightarrow H^1(G_K, \mu_m) \\
(P, Q) \rightarrow [\sigma \mapsto e_m(F_P(\sigma), Q)]
\]

bilinear, non-degenerate
The Tate pairing

For a principally polarized abelian variety over a finite field $\mathbb{F}_q$ s.t. $\mu_m \subset \mathbb{F}_q$

$$H^1(G_{\mathbb{F}_q}, \mu_m) \cong H^1(Gal(\mathbb{F}_{q^m}/\mathbb{F}_q), \mu_m) \cong \mu_m$$

We take $\bar{P} \in A(\bar{F}_q)$ such that $m\bar{P} = P$ and define

**The Tate pairing**

$$A(\mathbb{F}_q)/mA(\mathbb{F}_q) \times A[m](\mathbb{F}_q) \to \mu_m$$

$$(P, Q) \to e_m(\pi(\bar{P}) - \bar{P}, Q)$$
Assume there is $n \geq 1$ is s.t. $J[\ell^n] \subseteq J[\mathbb{F}_q]$ and $J[\ell^{n+1}] \not\subseteq J[\mathbb{F}_q]$, $\ell > 2$ prime (or $\pi - 1$ is divisible exactly by $\ell^n$)

Let $\mathcal{W}$ be the set of subgroups $G$ of rank 2 in $J[\ell^n]$ which are maximal isotropic with respect to the Weil pairing.

$$k_{\ell,J} := \max_{G \in \mathcal{W}} \{ k | \exists P, Q \in G \text{ s.t. } T_{\ell^n}(P, Q) \in \mu_{\ell^k} \setminus \mu_{\ell^{k-1}} \}$$
One pairing, two formulae

\[ A(\mathbb{F}_q)/\ell^n A(\mathbb{F}_q) \times A[\ell^n](\mathbb{F}_q) \to \mu_{\ell^n} \]

Tate

\[(P, Q) \to e_{\ell^n}(\pi(\bar{P}) - \bar{P}, Q)\]

with \(\ell^n\bar{P} = P\) and \(\bar{P} \notin J(\mathbb{F}_q)\)
One pairing, two formulae

\[ A(\mathbb{F}_q) / \ell^n A(\mathbb{F}_q) \times A[\ell^n](\mathbb{F}_q) \to \mu_{\ell^n} \]

Tate

\[(P, Q) \to e_{\ell^n}(\pi(\bar{P}) - \bar{P}, Q)\]

with \(\ell^n\bar{P} = P\) and \(\bar{P} \notin J(\mathbb{F}_q)\)

Lichtenbaum

\[(P, Q) \to (f_P, \ell^n(Q + R)/f_P, \ell^n(R))^{\frac{q-1}{\ell^n}}\]

with \(f_P, \ell^n\) s.t. \(\text{div}(f_P, \ell^n) \sim \ell^n(P)\)

\[\iff\]

compute in \(O(n \log \ell + \log q)\) op. in \(\mathbb{F}_q\).
One pairing, two formulae

\[ A(\mathbb{F}_q)/\ell^n A(\mathbb{F}_q) \times A[\ell^n](\mathbb{F}_q) \to \mu_{\ell^n} \]

Tate

\[(P, Q) \to e_{\ell^n}(\pi(\bar{P}) - \bar{P}, Q)\]

with \(\ell^n \bar{P} = P\) and \(\bar{P} \notin J(\mathbb{F}_q)\)

compute the Frobenius action up to precision \(\geq n\).

Lichtenbaum

\[(P, Q) \to (f_{P,\ell^n}(Q + R)/f_{P,\ell^n}(R))^{q-1\ell^n}\]

with \(f_{P,\ell^n}\) s.t. \(\text{div}(f_{P,\ell^n}) \sim \ell^n(P)\)

\(\Leftarrow\)

compute in \(O(n \log \ell + \log q)\) op. in \(\mathbb{F}_q\).
Computing $v_\ell(\pi)$

**Theorem**
Suppose $\pi - 1$ is exactly divisible by $\ell^n$ and $0 < v_{\ell, \mathcal{O}_K}(\pi) < 2n$. Then $v_\ell(\pi) = 2n - k_{\ell,J}$.

**Proof**: Galois cohomology + linear algebra

**Corollary**
If $0 < v_{\ell, \mathcal{O}_K}(\pi) < 2n$ and under the conditions of Lemma $\ast$, then $\text{End}(J)$ is a locally maximal order at $\ell$ iff $k_{\ell,J} = 2n - v_{\ell, \mathcal{O}_K}(\pi)$. 
We need to get $k_{\ell,J} = \max_{G \in \mathcal{W}} \{ k \mid T_{\ell n} : G \times G \to \mu_{\ell k} \text{ surjective} \}$.

There are $O(\ell^3)$ subgroups in $\mathcal{W}$!

In practice, compute a symplectic basis $\{Q_1, Q_{-1}, Q_2, Q_{-2}\}$.

Get $k_{\ell,J} = \max_{j \neq -i} \{ k \mid T_{\ell n}(Q_i, Q_j) \text{ is a } \ell^k\text{-th primitive root of unity} \}$
If the $J[\ell]$ is not defined over $\mathbb{F}_q$, switch to $\mathbb{F}_{q^r}$, $r \leq \ell^4 - 1$.

Compute largest integer $n$ s.t. $J[\ell^n] \subset J(\mathbb{F}_{q^r})$.

Compute a symplectic basis $\{Q_1, Q_{-1}, Q_2, Q_{-2}\}$.

Compute $k_{\ell,J} = \max_{i \neq -j} \{k \mid T^{\ell n}(Q_i, Q_j) \text{ is a } \ell^k \text{-th primitive root of unity}\}$

If $v_{\ell,O_K}(\pi^r) = 2n - k_{\ell,J}$ return true.
Denote by $\mathbb{F}_{q^r}$ the smallest extension field such that $J[\ell] \subset J[\mathbb{F}_{q^r}]$.

Let $n \geq 1$ be the largest integer such that $J[\ell^n] \subset J(\mathbb{F}_q)$ and $u = v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]).

Let $M(r)$ is the cost of a multiplication in $F_{q^r}$.

<table>
<thead>
<tr>
<th>Freeman-Lauter</th>
<th>This work</th>
</tr>
</thead>
<tbody>
<tr>
<td>$O((r\ell^{u-n} + \ell^{2u})M(r\ell^{u-n}) \log q)$ (worst case)</td>
<td>$O(M(r)(r \log q + \ell^{2n} + n \log \ell))$</td>
</tr>
</tbody>
</table>

Heuristically, if $u$ is large, we would expect $u > n$. 
Consider $y^2 = 27x^6 + 869x^5 + 364x^4 + 407x^3 + 518x^2 + 47x + 806$ over $\mathbb{F}_{1009}$.

The index is $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]] = 3^4$. The 3-torsion is defined over $\mathbb{F}_{1009^2}$.

$$\pi^2 = 8626 - 234 \frac{1+\sqrt{109}}{2} + (-33 + 27 \frac{1+\sqrt{109}}{2}) \sqrt{702} - 13 \frac{1+\sqrt{109}}{2} \implies v_{\ell, \mathcal{O}_K}(\pi^2) = 1.$$ 

It took less then 2 seconds on a AMD Phenom II X2 B55 (3 GHz) to compute $k_{\ell, J} = 1$ and decide that $\text{End}(J)$ is locally maximal at $\ell$.

The Freeman-Lauter algorithm runs over $\mathbb{F}_{1009^6}$ and returns the same result in 60 sec.
Select a "good" prime $p$.

For each abelian surface $J$ in the $p^3$ isomorphism classes

- Check if $J$ is in the right isogeny class.
- Check if $\text{End}(J) \cong \mathcal{O}_K$.
- Generate jacobians with CM by $\mathcal{O}_K$ by computing horizontal isogenies from $J$.

Reconstruct $H_i \mod p$ from jacobians with maximal endomorphism ring

Compute class polynomials modulo small "good" primes and use the CRT to reconstruct $H_1, H_2, H_3$. 
An $\ell$-isogeny is an isogeny whose kernel is a subgroup of $J[\ell]$ maximal isotropic with respect to the Weil pairing.

An $\ell$-isogeny $I : J_1 \to J_2$ is horizontal iff $\text{End } J_1 \simeq \text{End } J_2$.

Given by the action of the Shimura class group

$$\{(a, \alpha) | a \text{ is a fractional } \mathcal{O}_K\text{-ideal with } \bar{a}a = (\alpha) \text{ with } \alpha \in K_0 \text{ totally positive}\}/K^*$$

Let $\ell$ coprime to discriminant of $\mathbb{Z}[\pi, \bar{\pi}]$. Then the kernel of $I_a$ is a subgroup invariated by $\pi$.

$$\mathcal{O}(M(r)(r \log q + \ell^{2n}))$$
Let $J$ be a jacobian whose endomorphism ring is locally maximal at $\ell$.

Assume $\pi - 1$ is exactly divisible by $\ell^n$ and let $G$ be a subgroup in $\mathcal{W}$.

The Tate pairing is non-degenerate on $G \times G$ if

$$T_{\ell^n} : G \times G \to \mu_{\ell^k, J}$$

is surjective. We say it is degenerate otherwise.
Computing horizontal isogenies

Let $G_1$ be a maximal isotropic subgroup of $J[\ell]$. Consider $G \in \mathcal{W}$ such that $\ell^{n-1} G = G_1$.

**Theorem**

- If the isogeny of kernel $G_1$ is horizontal, then the Tate pairing is degenerate on $G \times G$.
- Under the conditions from Lemma *, if the Tate pairing is degenerate on $G \times G$, then the isogeny is horizontal.

$$O(M(r)(r \log q + \ell^{2n} + n \log \ell))$$
An example

We consider the jacobian of the hyperelliptic curve

\[ y^2 = 5x^5 + 4x^4 + 98x^2 + 7x + 2, \text{ over } \mathbb{F}_{127}. \]

\( \text{End}(J) \) is maximal at 5 and \([\text{End}J : \mathbb{Z}[\pi, \bar{\pi}]] = 50.\)

The decomposition \((5) = a\bar{a} \text{ in } \mathcal{O}_K\) gives two horizontal isogenies.

The 5-torsion is defined over \(\mathbb{F}_{127}(t) := \mathbb{F}_{127^8}.\)

With MAGMA, we computed the Mumford coordinates of the generators of kernels:

\[
\begin{align*}
(x^2 + (74t^7 + 25t^6 + 6t^5 + 110t^4 + 96t^3 + 75t^2 + 29t + 20)x + 39t^7 + 62t^6 + 77t^5 + 47t^4 + 9t^3 + 62t^2 + 97t + 15, & \quad (116t^7 + 61t^6 + 13t^5 + 38t^4 + 70t^3 + 109t^2 + 62t + 71)x + 98t^7 + 77t^6 + 17t^5 + 76t^4 + 81t^3 + 5t^2 + 36t + 33), \\
(x^2 + (66t^7 + 89t^6 + 50t^5 + 124t^4 + 91t^3 + 102t^2 + 100t + 52)x + 119t^7 + 14t^6 + 126t^5 + 42t^4 + 42t^3 + 85t^2 + 12t + 77, & \quad (92t^7 + 90t^6 + 94t^5 + 57t^4 + 59t^3 + 24t^2 + 72t + 11)x + 103t^7 + 16t^6 + 7t^5 + 111t^4 + 95t^3 + 79t^2 + 45t + 34)
\end{align*}
\]
There are $\ell^3 + \ell^2 + \ell + 1$ $\ell$-isogenies. Experimentally, we observed:

<table>
<thead>
<tr>
<th>$\ell$</th>
<th>$#\ell$-Isogenies</th>
<th>$#Kernels$ with deg. pairing</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>40</td>
<td>4, 7, 8</td>
</tr>
<tr>
<td>5</td>
<td>156</td>
<td>6, 8, 12</td>
</tr>
<tr>
<td>7</td>
<td>400</td>
<td>8, 14, 16</td>
</tr>
<tr>
<td>11</td>
<td>1464</td>
<td>12, 22, 24</td>
</tr>
</tbody>
</table>

It seems that at most $O(\ell)$ subgroups in $\mathcal{W}$ have degenerate Tate pairing.
In genus 1, the $\ell$-adic valuation of the Frobenius fully characterizes the endomorphism ring.

I.-Joux, Pairing the volcano
http://arxiv.org/abs/1110.3602

In genus 2, we need a stronger invariant. Work in progress with Emmanuel Thomé.

Thanks to: Ben Smith, David Gruenewald, John Boxall, François Morain.