Abelian varieties, theta functions and cryptography

Damien Robert\textsuperscript{1}

\textsuperscript{1}LFANT Team, IMB & Inria Bordeaux Sud-Ouest

10/02/2011 (Luminy)
Outline

1. Public-key cryptography
2. Abelian varieties, Arithmetic and Pairings
3. Isogenies
A brief history of public-key cryptography

- Secret-key cryptography: Vigenère (1553), One time pad (1917), AES (NIST, 2001).

- Public-key cryptography:
  - Diffie–Hellman key exchange (1976).
  - ElGamal: exponentiation/discrete logarithm in $G = \mathbb{F}_q^*$.

  $\Rightarrow$ Encryption, Signature (+Pseudo Random Number Generator, Zero Knowledge).

## RSA versus (H)ECC

<table>
<thead>
<tr>
<th>Security (bits level)</th>
<th>RSA</th>
<th>ECC</th>
</tr>
</thead>
<tbody>
<tr>
<td>72</td>
<td>1008</td>
<td>144</td>
</tr>
<tr>
<td>80</td>
<td>1248</td>
<td>160</td>
</tr>
<tr>
<td>96</td>
<td>1776</td>
<td>192</td>
</tr>
<tr>
<td>112</td>
<td>2432</td>
<td>224</td>
</tr>
<tr>
<td>128</td>
<td>3248</td>
<td>256</td>
</tr>
<tr>
<td>256</td>
<td>15424</td>
<td>512</td>
</tr>
</tbody>
</table>

Key length comparison between RSA and ECC

- Factorisation of a 768-bit RSA modulus [KAF+10].
- Currently: attempt to attack a 130-bit Koblitz elliptic curve.
**Definition (DLP)**

Let \( G = \langle g \rangle \) be a cyclic group of prime order. Let \( x \in \mathbb{N} \) and \( h = g^x \). The discrete logarithm \( \log_g(h) \) is \( x \).

- Exponentiation: \( O(\log p) \). DLP: \( \tilde{O}(\sqrt{p}) \) (in a generic group).
- \( G = \mathbb{F}_p^* \): sub-exponential attacks.

\( \Rightarrow \) Find secure groups with efficient law, compact representation.

**Protocol [Diffie–Hellman Key Exchange]**

Alice sends \( g^a \), Bob sends \( g^b \), the common key is

\[
g^{ab} = (g^b)^a = (g^a)^b.
\]
Pairing-based cryptography

Definition

A **pairing** is a bilinear application \( e : G_1 \times G_1 \rightarrow G_2 \).

- Identity-based cryptography [BF03].
- Short signature [BLS04].
- One way tripartite Diffie–Hellman [Jou04].
- Self-blindable credential certificates [Ver01].
- Attribute based cryptography [SW05].
- Broadcast encryption [GPSW06].

Tripartite Diffie–Hellman

Alice sends \( g^a \), Bob sends \( g^b \), Charlie sends \( g^c \). The common key is

\[
e(g, g)^{abc} = e(g^b, g^c)^a = e(g^c, g^a)^b = e(g^a, g^b)^c \in G_2.
\]
Abelian varieties

Definition

An Abelian variety is a complete connected group variety over a base field $k$.

- Abelian variety = points on a projective space (locus of homogeneous polynomials) + an abelian group law given by rational functions.

$\Rightarrow$ Use $G = A(k)$ with $k = \mathbb{F}_q$ for the DLP.

Pairings on abelian varieties

The Weil and Tate pairings on abelian varieties are the only known examples of cryptographic pairings.

$$e_W : A[\ell] \times A[\ell] \rightarrow \mu_\ell \subset \mathbb{F}_{q^k}^*.$$
**Elliptic curves**

**Definition (car $k \neq 2, 3$)**

$E : y^2 = x^3 + ax + b$.  $4a^3 + 27b^2 \neq 0$.

- An elliptic curve is a plane curve of genus 1.
- Elliptic curves = Abelian varieties of dimension 1.

$$P + Q = -R = (x_R, -y_R)$$

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

$$x_R = \lambda^2 - x_P - x_Q$$

$$y_R = y_P + \lambda(x_R - x_P)$$
Jacobian of hyperelliptic curves

\[ C : y^2 = f(x), \text{ hyperelliptic curve of genus } g. \quad (\deg f = 2g + 1) \]

- Divisor: formal sum \( D = \sum n_i P_i \), \( P_i \in C(k) \).
  \[ \deg D = \sum n_i. \]

- Principal divisor: \( \sum_{P \in C(k)} \nu_P(f).P; \quad f \in \overline{k}(C). \)

Jacobian of \( C = \) Divisors of degree 0 modulo principal divisors + Galois action = Abelian variety of dimension \( g \).

- Divisor class \( D \Rightarrow \text{unique} \) representative (Riemann–Roch):
  \[ D = \sum_{i=1}^{k} (P_i - P_\infty) \quad k \leq g, \quad \text{symmetric } P_i \neq P_j \]

- Mumford coordinates: \( D = (u, v) \Rightarrow u = \prod (x - x_i), \quad v(x_i) = y_i. \)

- Cantor algorithm: addition law.
Example of the addition law in genus 2

\[ D = P_1 + P_2 - 2\infty \]
\[ D' = Q_1 + Q_2 - 2\infty \]
Example of the addition law in genus 2

\[ D = P_1 + P_2 - 2\infty \]
\[ D' = Q_1 + Q_2 - 2\infty \]
Example of the addition law in genus 2

\[ D = P_1 + P_2 - 2\infty \]
\[ D' = Q_1 + Q_2 - 2\infty \]
\[ D + D' = R_1 + R_2 - 2\infty \]
### Security of abelian varieties

<table>
<thead>
<tr>
<th>$g$</th>
<th># points</th>
<th>DLP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$</td>
<td>$O(q)$</td>
<td>$\tilde{O}(q^{1/2})$</td>
</tr>
<tr>
<td>$2$</td>
<td>$O(q^2)$</td>
<td>$\tilde{O}(q)$</td>
</tr>
<tr>
<td>$3$</td>
<td>$O(q^3)$</td>
<td>$\tilde{O}(q^{4/3})$ (Jacobian of hyperelliptic curve)</td>
</tr>
<tr>
<td>$g$</td>
<td>$O(q^g)$</td>
<td>$\tilde{O}(q^{2-2/g})$</td>
</tr>
<tr>
<td>$g &gt; \log(q)$</td>
<td>$O(q^g)$</td>
<td>$L_{1/2}(q^g) = \exp(O(1)\log(x)^{1/2}\log\log(x)^{1/2})$</td>
</tr>
</tbody>
</table>

**Security of the DLP**

- Weak curves (MOV attack, Weil descent, anomalous curves).

  $\Rightarrow$ Public-key cryptography with the DLP: Elliptic curves, Jacobian of hyperelliptic curves of genus 2.

  $\Rightarrow$ Pairing-based cryptography: Abelian varieties of dimension $g \leq 4$. 
## Security of abelian varieties

<table>
<thead>
<tr>
<th>$g$</th>
<th># points</th>
<th>DLP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$O(q)$</td>
<td>$\tilde{O}(q^{1/2})$</td>
</tr>
<tr>
<td>2</td>
<td>$O(q^2)$</td>
<td>$\tilde{O}(q)$</td>
</tr>
<tr>
<td>3</td>
<td>$O(q^3)$</td>
<td>$\tilde{O}(q^{4/3})$ (Jacobian of hyperelliptic curve)</td>
</tr>
<tr>
<td>$g$</td>
<td>$O(q^g)$</td>
<td>$\tilde{O}(q^{2-2/g})$ (Jacobian of non hyperelliptic curve)</td>
</tr>
<tr>
<td>$g &gt; \log(q)$</td>
<td>$O(q^g)$</td>
<td>$L_{1/2}(q^g) = \exp(O(1)\log(x)^{1/2}\log\log(x)^{1/2})$</td>
</tr>
</tbody>
</table>

### Security of the DLP

- Weak curves (MOV attack, Weil descent, anomalous curves).

⇒ **Public-key cryptography** with the DLP: Elliptic curves, Jacobian of hyperelliptic curves of genus 2.

⇒ **Pairing-based cryptography**: Abelian varieties of dimension $g \leq 4$. 
Complex abelian varieties

- Abelian variety over \( \mathbb{C} \): \( A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g) \), where \( \Omega \in \mathcal{H}_g(\mathbb{C}) \) the Siegel upper half space.
- The theta functions with characteristic give a lot of analytic (quasi periodic) functions on \( \mathbb{C}^g \).

\[
\vartheta \left[ \begin{array}{c} a \\ b \end{array} \right] (z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i t (n+a)\Omega(n+a)+2\pi i t(n+a)(z+b)} \quad a, b \in \mathbb{Q}^g
\]

Quasi-periodicity:

\[
\vartheta \left[ \begin{array}{c} a \\ b \end{array} \right] (z + m_1\Omega + m_2, \Omega) = e^{2\pi i (t \cdot a \cdot m_2 - t \cdot b \cdot m_1) - \pi i t m_1 \Omega m_1 - 2\pi i t m_1 \cdot z} \vartheta \left[ \begin{array}{c} a \\ b \end{array} \right] (z, \Omega).
\]

- Projective coordinates:

\[
A \longrightarrow \mathbb{P}^{n^g-1}
\]

\[
z \longmapsto (\tilde{\vartheta}_i(z))_{i \in Z(\overline{n})}
\]

where \( Z(\overline{n}) = \mathbb{Z}^g / n\mathbb{Z}^g \) and \( \tilde{\vartheta}_i = \vartheta \left[ \begin{array}{c} 0 \\ \overline{i/n} \end{array} \right] (., \overline{\Omega/n}) \).
Theta functions of level $n$

- Translation by a point of $n$-torsion:

$$\vartheta_i(z + \frac{m_1}{n} \Omega + \frac{m_2}{n}) = e^{-\frac{2\pi i}{n} t \cdot m_1} \vartheta_{i+m_2}(z).$$

- $(\vartheta_i)_{i \in \mathbb{Z}(\overline{n})}$: basis of the theta functions of level $n$


- $(\vartheta_i)_{i \in \mathbb{Z}(\overline{n})} = \begin{cases} 
  \text{coordinates system} & n \geq 3 \\
  \text{coordinates on the Kummer variety } A/\pm 1 & n = 2
\end{cases}$

- Theta null point: $\vartheta_i(0)_{i \in \mathbb{Z}(\overline{n})} = \text{modular invariant.}$
The differential addition law \((k = \mathbb{C})\)

\[
\left( \sum_{t \in \mathbb{Z}(2)} \chi(t) \vartheta_{i+t}(x + y) \vartheta_{j+t}(x - y) \right) \cdot \left( \sum_{t \in \mathbb{Z}(2)} \chi(t) \vartheta_{k+t}(0) \vartheta_{l+t}(0) \right) =
\left( \sum_{t \in \mathbb{Z}(2)} \chi(t) \vartheta_{-i+t}(y) \vartheta_{j'+t}(y) \right) \cdot \left( \sum_{t \in \mathbb{Z}(2)} \chi(t) \vartheta_{k'+t}(x) \vartheta_{l'+t}(x) \right).
\]

where \(\chi \in \hat{\mathbb{Z}}(2), i, j, k, l \in \mathbb{Z}(n)\)

\((i', j', k', l') = A(i, j, k, l)\)

\[
A = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}
\]
### Arithmetic with low level theta functions (car k ≠ 2)

<table>
<thead>
<tr>
<th></th>
<th>Mumford [Lan05]</th>
<th>Level 2 [Gau07]</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Doubling</strong></td>
<td>$34M + 7S$</td>
<td>$7M + 12S + 9m_0$</td>
<td>$49M + 36S + 27m_0$</td>
</tr>
<tr>
<td><strong>Mixed Addition</strong></td>
<td>$37M + 6S$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Multiplication cost in genus 2 (one step).**

<table>
<thead>
<tr>
<th></th>
<th>Montgomery</th>
<th>Level 2</th>
<th>Jacobians</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Doubling</strong></td>
<td>$5M + 4S + 1m_0$</td>
<td>$3M + 6S + 3m_0$</td>
<td>$3M + 5S$</td>
</tr>
<tr>
<td><strong>Mixed Addition</strong></td>
<td>$7M + 6S + 1m_0$</td>
<td>$7M + 6S + 1m_0$</td>
<td>$9M + 10S + 5$</td>
</tr>
</tbody>
</table>

**Multiplication cost in genus 1 (one step).**
Arithmetic with high level theta functions \cite{LR10a}

- **Algorithms** for
  - Additions and differential additions in level 4.
  - Computing $P \pm Q$ in level 2 (need one square root). \cite{LR10b}
  - Fast differential multiplication.

- **Compressing coordinates** $O(1)$:
  - Level $2n$ theta null point $\Rightarrow 1 + g(g + 1)/2$ level 2 theta null points.
  - Level $2n$ $\Rightarrow 1 + g$ level 2 theta functions.

- **Decompression**: $n^g$ differential additions.
The Weil and Tate pairing with theta coordinates [LR10b]

$P$ and $Q$ points of $\ell$-torsion.

\[
\begin{align*}
0_A & \quad P & \quad 2P & \quad \ldots & \quad \ell P = \lambda^0_P 0_A \\
Q & \quad P \oplus Q & \quad 2P + Q & \quad \ldots & \quad \ell P + Q = \lambda^1_P Q \\
2Q & \quad P + 2Q & \quad & \quad \ldots & \quad \ldots \\
\ell Q = \lambda^0_Q 0_A & \quad P + \ell Q = \lambda^1_Q P
\end{align*}
\]

- $e_{W,\ell}(P, Q) = \frac{\lambda^1_P \lambda^0_Q}{\lambda^0_P \lambda^1_Q}$.

  If $P = \Omega x_1 + x_2$ and $Q = \Omega y_1 + y_2$, then $e_{W,\ell}(P, Q) = e^{-2\pi i\ell (t x_1 \cdot y_2 - t y_1 \cdot x_2)}$.

- $e_{T,\ell}(P, Q) = \frac{\lambda^1_P}{\lambda^0_P}$. 
Isogenies

Definition

A (separable) isogeny is a finite surjective (separable) morphism between two Abelian varieties.

- Isogenies = Rational map + group morphism + finite kernel.
- Isogenies $\iff$ Finite subgroups.

$(f : A \to B) \mapsto \text{Ker } f$

$(A \to A/H) \mapsto H$

Example: Multiplication by $\ell$ ($\Rightarrow \ell$-torsion), Frobenius (non separable).
Cryptographic usage of isogenies

- Transfer the DLP from one Abelian variety to another.
- Point counting algorithms ($\ell$-adic or $p$-adic) ⇒ Verify a curve is secure.
- Compute the class field polynomials (CM-method) ⇒ Construct a secure curve.
- Compute the modular polynomials ⇒ Compute isogenies.
- Determine $\text{End}(A)$ ⇒ CRT method for class field polynomials.
Vélu’s formula

Theorem

Let $E : y^2 = f(x)$ be an elliptic curve and $G \subset E(k)$ a finite subgroup. Then $E/G$ is given by $Y^2 = g(X)$ where

$$X(P) = x(P) + \sum_{Q \in G \setminus \{0_E\}} (x(P + Q) - x(Q))$$

$$Y(P) = y(P) + \sum_{Q \in G \setminus \{0_E\}} (y(P + Q) - y(Q)).$$

- Uses the fact that $x$ and $y$ are characterised in $k(E)$ by

$$v_0(x) = -2 \quad v_P(x) \geq 0 \quad \text{if} \ P \neq 0_E$$

$$v_0(y) = -3 \quad v_P(y) \geq 0 \quad \text{if} \ P \neq 0_E$$

$$y^2 / x^3(0_E) = 1$$

- No such characterisation in genus $g \geq 2$ for Mumford coordinates.
The isogeny theorem

**Theorem**

- Let $\varphi : \mathbb{Z}(\bar{n}) \to \mathbb{Z}(\ell \bar{n}), x \mapsto \ell \cdot x$ be the canonical embedding.
  - Let $K = A_2[\ell] \subset A_2[\ell \bar{n}]$.

- Let $(\vartheta^A_i)_{i \in \mathbb{Z}(\ell \bar{n})}$ be the theta functions of level $\ell \bar{n}$ on $A = \mathbb{C}g / (\mathbb{Z}g + \Omega \mathbb{Z}g)$.

- Let $(\vartheta^B_i)_{i \in \mathbb{Z}(n)}$ be the theta functions of level $n$ of $B = A/K = \mathbb{C}g / (\mathbb{Z}g + \frac{\Omega}{\ell} \mathbb{Z}g)$.

- We have:
  
  $$(\vartheta^B_i(x))_{i \in \mathbb{Z}(\bar{n})} = (\vartheta^A_{\varphi(i)}(x))_{i \in \mathbb{Z}(\bar{n})}$$

**Example**

$\pi : (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}) \mapsto (x_0, x_3, x_6, x_9)$ is a 3-isogeny between elliptic curves.
An example with $g = 1$, $n = 2$, $\ell = 3$

\[ z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n \xrightarrow{[\ell]} \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n \]

\[ \pi \]

\[ z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g), \text{ level } n \]
An example with $g = 1$, $n = 2$, $\ell = 3$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \xrightarrow{[\ell]} \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n$$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n$$
An example with $g = 1$, $n = 2$, $\ell = 3$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n \xrightarrow{[\ell]} \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n$$

$$\pi$$

$$\hat{\pi}$$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega \mathbb{Z}^g), \text{ level } n$$
An example with $g = 1$, $n = 2$, $\ell = 3$

$$z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n \quad \xrightarrow{[\ell]} \quad \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n$$

$$\pi$$

$$z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g), \text{ level } n$$
An example with $g = 1$, $n = 2$, $\ell = 3$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n \xrightarrow{[\ell]} \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n$$

$$\pi$$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega \mathbb{Z}^g), \text{ level } n$$

\[
\begin{align*}
1 & \quad \quad \Omega & \quad 3\Omega \\
R_0 & \times & \times & \times \\
& \times & \times & \times \\
R_1 & \times & \times & \times \\
R_2 & \times & \times & \times \\
y & \times & \times & \times
\end{align*}
\]
An example with $g = 1$, $n = 2$, $\ell = 3$

\[ z \in \mathbb{C}^g / ( \mathbb{Z}^g + \ell \Omega \mathbb{Z}^g ), \text{ level } \ell n \]

\[ \pi \]

\[ \hat{\pi} \]

\[ z \in \mathbb{C}^g / ( \mathbb{Z}^g + \Omega \mathbb{Z}^g ), \text{ level } n \]
An example with $g = 1$, $n = 2$, $\ell = 3$

\[
z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n \quad \xrightarrow{[\ell]} \quad \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n
\]

$\pi$  \quad  $\hat{\pi}$

$z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g), \text{ level } n$
Theorem (Koizumi–Kempf)

Let $F$ be a matrix of rank $r$ such that $^t FF = \ell \text{Id}_r$. Let $X \in (\mathbb{C}g)_r$ and $Y = F(X) \in (\mathbb{C}g)_r$. Let $j \in (\mathbb{Q}g)_r$ and $i = F(j)$. Then we have

$$\vartheta \begin{bmatrix} 0 \\ i_1 \\ \vdots \\ i_r \end{bmatrix} \left( Y_1, \frac{\Omega}{n} \right) \cdots \vartheta \begin{bmatrix} 0 \\ i_r \end{bmatrix} \left( Y_r, \frac{\Omega}{n} \right) =$$

$$\sum_{t_1, \ldots, t_r \in \frac{1}{\ell} \mathbb{Z}g / \mathbb{Z}g} \vartheta \begin{bmatrix} 0 \\ j_1 \\ \vdots \\ j_r \end{bmatrix} \left( X_1 + t_1, \frac{\Omega}{\ell n} \right) \cdots \vartheta \begin{bmatrix} 0 \\ j_r \end{bmatrix} \left( X_r + t_r, \frac{\Omega}{\ell n} \right),$$

If $\ell = a^2 + b^2$, we take $F = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, so $r = 2$.

In general, $\ell = a^2 + b^2 + c^2 + d^2$, we take $F$ to be the matrix of multiplication by $a + bi + cj + dk$ in the quaternions, so $r = 4$. 
Computing isogenies [Cosset, Lubicz, R.]

- Let $A/k$ be an abelian variety of dimension $g$ over $k$ given in theta coordinates. Let $K \subset A$ be a maximal isotropic subgroup of $A[\ell]$ ($\ell$ prime to 2 and the characteristic). Then we have an algorithm to compute the isogeny $A \to A/K$.

- Need $O(\#K)$ differential additions in $A$ + $O(\ell^g)$ or $O(\ell^{2g})$ multiplications $\Rightarrow$ fast.

- The formulas are rational if the kernel $K$ is rational.

$\Rightarrow$ Work in level 2.

$\Rightarrow$ Convert back and forth to Mumford coordinates:

$$
\begin{align*}
A & \xrightarrow{\hat{\pi}} B \\
\text{Jac}(C_1) & \longrightarrow \text{Jac}(C_2)
\end{align*}
$$
AVIsogenies

- AVIsogenies: Magma code written by Bisson, Cosset and R. [http://avisogenies.gforge.inria.fr](http://avisogenies.gforge.inria.fr)
- Released under LGPL 2+.
- Implement isogeny computation (and applications thereof) for abelian varieties using theta functions.
- Current release 0.2: isogenies in genus 2.
**Implementation**

$H$ hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \text{Jac}(H)$, $\ell$ odd prime, $2\ell \wedge \text{car } k = 1$. Compute all rational $(\ell, \ell)$-isogenies $J \rightarrow \text{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a “symplectic” basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels $K$.
4. For each kernel $K$, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in $K$ in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of $J/K$.
7. Compute the Igusa invariants of $J/K$ (“Inverse Thomae”).
8. Distinguish between the isogeneous curve and its twist.
**Implementation**

$H$ hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \text{Jac}(H)$, $\ell$ odd prime, $2\ell \wedge \text{car} \ k = 1$. Compute all rational $(\ell, \ell)$-isogenies $J \to \text{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a “symplectic” basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels $K$.
4. For each kernel $K$, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in $K$ in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of $J/K$.
7. Compute the Igusa invariants of $J/K$ (“Inverse Thomae”).
8. Distinguish between the isogeneous curve and its twist.
Implementation

$H$ hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \text{Jac}(H)$, $\ell$ odd prime, $2\ell \wedge \text{car} \ k = 1$. Compute all rational $(\ell, \ell)$-isogenies $J \to \text{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a “symplectic” basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels $K$.
4. For each kernel $K$, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in $K$ in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of $J/K$.
7. Compute the Igusa invariants of $J/K$ (“Inverse Thomae”).
8. Distinguish between the isogeneous curve and its twist.
Implementation

$H$ hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \text{Jac}(H)$, $\ell$ odd prime, $2\ell \wedge \text{car } k = 1$. Compute all rational $(\ell, \ell)$-isogenies $J \rightarrow \text{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a “symplectic” basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels $K$.
4. For each kernel $K$, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in $K$ in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of $J/K$.
7. Compute the Igusa invariants of $J/K$ (“Inverse Thomae”).
8. Distinguish between the isogeneous curve and its twist.
Implementation

$H$ hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \text{Jac}(H)$, $\ell$ odd prime, $2\ell \wedge \text{car} \ k = 1$. Compute all rational $(\ell, \ell)$-isogenies $J \to \text{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.

2. Compute a “symplectic” basis of $J[\ell](\mathbb{F}_{q^n})$.

3. Find the rational maximal isotropic kernels $K$.

4. For each kernel $K$, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).

5. Compute the other points in $K$ in theta coordinates using differential additions.

6. Apply the change level formula to recover the theta null point of $J/K$.

7. Compute the Igusa invariants of $J/K$ (“Inverse Thomae”).

8. Distinguish between the isogeneous curve and its twist.
Implementation

$H$ hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \text{Jac}(H)$, $\ell$ odd prime, $2\ell \wedge \text{car } k = 1$. Compute all rational $(\ell, \ell)$-isogenies $J \to \text{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a “symplectic” basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels $K$.
4. For each kernel $K$, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in $K$ in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of $J/K$.
7. Compute the Igusa invariants of $J/K$ (“Inverse Thomae”).
8. Distinguish between the isogeneous curve and its twist.
Implementation

$H$ hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \text{Jac}(H)$, $\ell$ odd prime, $2\ell \land \text{car} \, k = 1$. Compute all rational $(\ell, \ell)$-isogenies $J \rightarrow \text{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.

2. Compute a “symplectic” basis of $J[\ell](\mathbb{F}_{q^n})$.

3. Find the rational maximal isotropic kernels $K$.

4. For each kernel $K$, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).

5. Compute the other points in $K$ in theta coordinates using differential additions.

6. Apply the change level formula to recover the theta null point of $J/K$.

7. Compute the Igusa invariants of $J/K$ (“Inverse Thomae”).

8. Distinguish between the isogeneous curve and its twist.
Implementation

$H$ hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \text{Jac}(H)$, $\ell$ odd prime, $2\ell \wedge \text{car } k = 1$. Compute all rational $(\ell, \ell)$-isogenies $J \to \text{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.

2. Compute a “symplectic” basis of $J[\ell](\mathbb{F}_{q^n})$.

3. Find the rational maximal isotropic kernels $K$.

4. For each kernel $K$, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).

5. Compute the other points in $K$ in theta coordinates using differential additions.

6. Apply the change level formula to recover the theta null point of $J/K$.

7. Compute the Igusa invariants of $J/K$ (“Inverse Thomae”).

8. Distinguish between the isogeneous curve and its twist.
Implementation

$H$ hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \text{Jac}(H)$, $\ell$ odd prime, $2\ell \wedge \text{car} \, k = 1$. Compute all rational $(\ell, \ell)$-isogenies $J \to \text{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a “symplectic” basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels $K$.
4. For each kernel $K$, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in $K$ in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of $J/K$.
7. Compute the Igusa invariants of $J/K$ (“Inverse Thomae”).
8. Distinguish between the isogeneous curve and its twist.
Timings for isogenies computations

(J = 7)

Jacobian of Hyperelliptic Curve defined by $y^2 = t^{254}x^6 + t^{223}x^5 + t^{255}x^4 + t^{318}x^3 + t^{668}x^2 + t^{543}x + t^{538}$ over GF(3^6)

> time RationallyIsogenousCurvesG2(J,7);
** Computing 7 -rational isotropic subgroups
  -- Computing the 7 -torsion over extension of deg 4
  !! Basis: 2 points in Finite field of size 3^24
  -- Listing subgroups
  1 subgroup over Finite field of size 3^24
  -- Convert the subgroups to theta coordinates
  Time: 0.060

Computing the 1 7 -isogenies
** Precomputations for l= 7 Time: 0.180
** Computing the 7 -isogeny
  Computing the l-torsion Time: 0.030
  Changing level Time: 0.210
  Time: 0.430

Time: 0.490

[ <[ t^620, t^691, t^477 ]>, Jacobian of Hyperelliptic Curve defined by
$y^2 = t^{615}x^6 + t^{224}x^5 + t^{37}x^4 + t^{303}x^3 + t^{715}x^2 + t^{128}x + t^{17}$]
Jacobian of Hyperelliptic Curve defined by \( y^2 = 39x^6 + 4x^5 + 8x^4 + 10x^3 + 31x^2 + 39x + 2 \) over GF(83)

> time RationallyIsogenousCurvesG2(J,5);
** Computing 5 -rationnal isotropic subgroups
  -- Computing the 5 -torsion over extension of deg 24
  Time: 0.940
  !! Basis: 4 points in Finite field of size 83^24
  -- Listing subgroups
  Time: 1.170
  6 subgroups over Finite field of size 83^24
  -- Convert the subgroups to theta coordinates
  Time: 0.360
  Time: 2.630
  Computing the 6 5 -isogenies
  Time: 0.820
  Time: 3.460
  [
    [ 36, 69, 38 ],
    Jacobian of Hyperelliptic Curve defined by \( y^2 = 27x^6 + 63x^5 + 5x^4 + 24x^3 + 34x^2 + 6x + 76 \) over GF... ]
Timings for isogeny graphs \((\ell = 3)\)

Jacobian of Hyperelliptic Curve defined by \(y^2 = 41x^6 + 131x^5 + 55x^4 + 57x^3 + 233x^2 + 225x + 51\) over GF(271)

\[
time \text{isograph,jacobians} := \text{IsoGraphG2}(J,\{3\}; \text{save_mem} := -1);
\]

Computed 540 isogenies and found 135 curves.
Time: 14.410

- Core 2 with 4BG of RAM.
- Computing kernels: \(\approx 5s\).
- Computing isogenies: \(\approx 7s\) (Torsion: \(\approx 2s\), Changing level: \(\approx 3.5s\)).
Going further (\(\ell = 53\))

Jacobian of Hyperelliptic Curve defined by \(y^2 = 97x^6 + 77x^5 + 62x^4 + 14x^3 + 33x^2 + 18x + 40\) over GF(113)

> time RationallyIsogenousCurvesG2(J,53);
** Computing 53 -rationnal isotropic subgroups
  -- Computing the 53 -torsion over extension of deg 52 Time: 8.610
!! Basis: 3 points in Finite field of size 113^52
  -- Listing subgroups Time: 1.210
2 subgroups over Finite field of size 113^52
  -- Convert the subgroups to theta coordinates Time: 0.100
Time: 9.980
Computing the 2 53 -isogenies
  ** Precomputations for \(l = 53\) Time: 0.240
  ** Computing the 53 -isogeny
    Computing the \(l\)-torsion Time: 7.570
    Changing level Time: 1.170
Time: 8.840
  ** Computing the 53 -isogeny
Time: 8.850
Time: 27.950
Going further \((\ell = 19)\)

Jacobian of Hyperelliptic Curve defined by \(y^2 = 194x^6 + 554x^5 + 606x^4 + 523x^3 + 642x^2 + 566x + 112\) over \(\text{GF}(859)\)

```plaintext
> time RationallyIsogenousCurvesG2(J,19);
** Computing 19 -rationnal isotropic subgroups (extension degree 18)
  Time: 0.760
Computing the 2 19 -isogenies
  ** Precomputations for l= 19 Time: 11.160
  ** Computing the 19 -isogeny
    Computing the l-torsion Time: 0.250
    Changing level Time: 18.590
  Time: 18.850
  ** Computing the 19 -isogeny
    Computing the l-torsion Time: 0.250
    Changing level Time: 18.640
  Time: 18.900
Time: 51.060
[ [< 341, 740, 389 ], Jacobian of Hyperelliptic Curve defined by y^2 = 680x^5 + 538x^4 + 613x^3 + 557x^2 + 856x + 628 over GF(859) ]
```
A record isogeny computation!  \( (\ell = 1321) \)

- \( J \) Jacobian of \( y^2 = x^5 + 41691x^4 + 24583x^3 + 2509x^2 + 15574x \) over \( \mathbb{F}_{42179} \).
- \#J = 2^{10}1321^2.

\[
> \text{time RationallyIsogenousCurvesG2}(J, 1321; \text{ext\_degree:=} 1);
\]

** Computing 1321 -rationnal isotropic subgroups  
Time: 0.350

Computing the 1 1321 -isogenies  
** Precomputations for \( l = 1321 \)  
Time: 1276.950

** Computing the 1321 -isogeny  
Computing the \( l \)-torsion  
Time: 1200.270

Changing level  
Time: 1398.780

Time: 5727.250

Time: 7004.240

Time: 7332.650

[ <[ 9448, 15263, 31602 ]>, Jacobian of Hyperelliptic Curve defined by  
\( y^2 = 33266*x^6 + 20155*x^5 + 31203*x^4 + 9732*x^3 + 4204*x^2 + 18026*x + 29732 \) over GF(42179) ]

- Core 2 with 32GB of RAM.
Isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q}_2$ $(\mathbb{Q} \leftrightarrow K_0 \leftrightarrow K)$
Isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q}_2$ 

$(\mathbb{Q} \leftrightarrow K_0 \leftrightarrow K)$
Isogeny graphs: $\ell = q = \overline{QQ} \quad (\mathbb{Q} \leftrightarrow K_0 \leftrightarrow K)$
Isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2^2$ 

($\mathbb{Q} \hookrightarrow K_0 \hookrightarrow K$)
Isogeny graphs: $\ell = q^2 = Q^2Q^2$

$(\mathbb{Q} \leftrightarrow K_0 \leftrightarrow K)$
Isogeny graphs: $\ell = q^2 = Q^4$

$(\mathbb{Q} \leftrightarrow K_0 \leftrightarrow K)$
Non maximal isogeny graphs \((\ell = q = \overline{QQ})\)
Non maximal isogeny graphs ($\ell = q = Q\bar{Q}$)
Non maximal isogeny graphs ($\ell = q = Q\overline{Q}$)
Non maximal isogeny graphs \((\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q}_2)\)
Non maximal isogeny graphs \( (\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q}_2) \)
Non maximal isogeny graphs $(\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q}_2)$
Non maximal isogeny graphs ($\ell = q = Q^2$)
Non maximal isogeny graphs ($\ell = q = Q^2$)
Applications and perspectives

- Computing endomorphism ring. Generalize [BS09] to higher genus, work by Bisson.
- Class polynomials in genus 2 using the CRT. If $K$ is a CM field and $J/F_p$ is such that $\text{End}(J) \otimes \mathbb{Z} \mathbb{Q} = K$, use isogenies to find the Jacobians whose endomorphism ring is $O_K$. Work by Lauter+R.

- Modular polynomials in genus 2 using theta null points: computed by Gruenewald using analytic methods for $\ell = 3$.
- Isogenies using rational coordinates? Work by Smith using the geometry of Kummer surfaces for $\ell = 3$ ($g = 2$). Cassels and Flynn: modification of theta coordinates to have rational coordinates on hyperelliptic curves of genus 2.
- How to compute $(\ell,1)$-isogenies in genus 2?
- Look at $g = 3$ (associate theta coordinates to the Jacobian of a non hyperelliptic curve).
Thank you for your attention!
Bibliography


