Algorithms on abelian varieties for cryptography

Damien Robert\textsuperscript{1}

\textsuperscript{1}Microsoft Research

12/01/2012 (Telecom ParisTech++)
Outline

1. Public-key cryptography
2. Abelian varieties
3. Theta functions
4. Isogenies
5. Examples
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). So we can use the DLP for public key cryptography.

$\Rightarrow$ We want to find secure groups with efficient addition law and compact representation.
**Pairing-based cryptography**

**Definition**

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

**Example**

- If the pairing $e$ can be computed easily, the difficulty of the DLP in $G_1$ reduces to the difficulty of the DLP in $G_2$.
  
  $\Rightarrow$ MOV attacks on supersingular elliptic curves.

- Identity-based cryptography [BF03].
- Short signature [BLS04].
- One way tripartite Diffie–Hellman [Jou04].
- Self-blindable credential certificates [Ver01].
- Attribute based cryptography [SW05].
- Broadcast encryption [GPS+06].
Example of applications

Tripartite Diffie–Hellman

Alice sends $g^a$, Bob sends $g^b$, Charlie sends $g^c$. The common key is

$$e(g, g)^{abc} = e(g^b, g^c)^a = e(g^c, g^a)^b = e(g^a, g^b)^c \in G_2.$$ 

Example (Identity-based cryptography)

- **Master key**: $(P, sP), s$. $s \in \mathbb{N}, P \in G_1$.
- **Derived key**: $Q, sQ$. $Q \in G_1$.
- **Encryption**: $m \in G_2$: $m' = m \oplus e(Q, sP)^r, rP$. $r \in \mathbb{N}$.
- **Decryption**: $m = m' \oplus e(sQ, rP)$. 
Definition (car \( k \neq 2, 3 \))

An elliptic curve is a plan curve of equation

\[ y^2 = x^3 + ax + b \quad 4a^3 + 27b^2 \neq 0. \]
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**.
- Abelian variety of dimension 1 = elliptic curves.

$\Rightarrow$ Abelian varieties are just the generalization of elliptic curves in higher dimension.

**Pairings on abelian varieties**

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

$$e_W : A[\ell] \times A[\ell] \to \mu_{\ell} \subset \mathbb{F}_q^*.$$
Abelian surfaces

Abelian varieties of dimension 2 are given by: 5 quadratic equations in $\mathbb{P}^7$.

\[(4a_1 a_2 + 4a_5 a_6)X_1 X_6 + (4a_1 a_2 + 4a_5 a_6)X_2 X_5 = (4a_3 a_4 4a_4 a_3)X_3 X_4 + (4a_3 a_4 4a_4 a_3)X_7 X_8;\]

\[(2a_1 a_5 + 2a_2 a_6)X_1^2 + (2a_1 a_5 + 2a_2 a_6)X_2^2 + (-2a_2^2 - 2a_2^2 - 2a_2^2 - 2a_2^2)X_3 X_3 = (2a_3^2 + 2a_4^2 + 2a_3^2 + 2a_4^2)X_4 X_8 + (-2a_1 a_5 - 2a_2 a_6)X_5^2 + (-2a_1 a_5 - 2a_2 a_6)X_6^2;\]

\[(4a_1 a_6 + 4a_2 a_5)X_1 X_2 + (-4a_3 a_4 - 4a_3 a_4)X_3 X_8 = (4a_3 a_4 + 4a_3 a_4)X_4 X_7 + (-4a_1 a_6 - 4a_2 a_5)X_5 X_6;\]

\[(2a_1^2 + 2a_2^2 + 2a_5^2 + 2a_6^2)X_1 X_5 + (2a_1^2 + 2a_2^2 + 2a_5^2 + 2a_6^2)X_2 X_6 + (-2a_3 a_3 - 2a_4 a_4)X_3^2 = (2a_3 a_3 + 2a_4 a_4)X_4^2 + (2a_3 a_3 + 2a_4 a_4)X_5^2 + (2a_3 a_3 + 2a_4 a_4)X_6^2;\]

\[(2a_1^2 - 2a_2^2 + 2a_5^2 - 2a_6^2)X_1 X_5 + (-2a_1^2 + 2a_2^2 - 2a_5^2 + 2a_6^2)X_2 X_6 + (-2a_3 a_3 + 2a_4 a_4)X_3^2 = (-2a_3 a_3 + 2a_4 a_4)X_4^2 + (2a_3 a_3 - 2a_4 a_4)X_5^2 + (-2a_3 a_3 + 2a_4 a_4)X_6^2;\]

where the parameters satisfy 2 quartic equations in $\mathbb{P}^5$:

\[a_1^3 a_5 + a_1^2 a_2 a_6 + a_1 a_2^2 a_5 + a_1 a_5^2 + a_1 a_5 a_6^2 + a_2 a_5 a_6 + a_2 a_5^2 a_6 + a_2 a_5^3 a_6 - 2a_4^2 - 4a_3 a_4 - 2a_4 = 0;\]

\[a_1^2 a_2 a_6 + a_1 a_2^2 a_5 + a_1 a_5 a_6 + a_2 a_5^2 a_6 - 4a_3 a_4^2 = 0\]

The most general form actually use 72 quadratic equations in 16 variables.
Jacobian of hyperelliptic curves

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

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

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

Jacobian of \( C = \text{Divisors of degree 0 modulo principal divisors} \)
+ 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.
Abelian varieties as Jacobians

Dimension 2: Jacobians of hyperelliptic curves of genus 2:

\[ y^2 = f(x), \deg f = 5. \]

\[ D = P_1 + P_2 - 2\infty \]
\[ D' = Q_1 + Q_2 - 2\infty \]
Dimension 2: Jacobians of hyperelliptic curves of genus 2:

\[ y^2 = f(x), \, \text{deg} \, f = 5. \]

\[ D = P_1 + P_2 - 2\infty \]
\[ D' = Q_1 + Q_2 - 2\infty \]
Abelian varieties as Jacobians

Dimension 2: Jacobians of hyperelliptic curves of genus 2:
\[ y^2 = f(x), \ \text{deg} \ f = 5. \]

\[ D = P_1 + P_2 - 2\infty \]
\[ D' = Q_1 + Q_2 - 2\infty \]
\[ D + D' = R_1 + R_2 - 2\infty \]
Abelian varieties as Jacobians

Dimension 3
Jacobians of hyperelliptic curves of genus 3.

Jacobians of quartics.
Abelian varieties as Jacobians

Dimension 4

Abelian varieties do not come from a curve generically.
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 an hyperelliptic curve)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\tilde{O}(q)$ (Jacobian of a quartic)</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).
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 are 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:

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

- Projective coordinates:

$$A \quad \longrightarrow \quad \mathbb{P}^{ng-1}_{\mathbb{C}}$$

$$z \quad \longmapsto \quad (\vartheta_i(z))_{i \in \mathbb{Z}(\overline{n})}$$

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

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

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

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

  $$\iff A[n] = A_1[n] \oplus A_2[n]: \text{symplectic decomposition.}$$

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

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

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

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

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

\[
A = \frac{1}{2} \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1
\end{pmatrix}
\]
Example: addition in genus 1 and in level 2

Differential Addition Algorithm:

**Input:** \( P = (x_1 : z_1), \ Q = (x_2 : z_2) \)

and \( R = P - Q = (x_3 : z_3) \) with \( x_3 z_3 \neq 0 \).

**Output:** \( P + Q = (x' : z') \).

1. \( x_0 = (x_1^2 + z_1^2)(x_2^2 + z_2^2) \);
2. \( z_0 = \frac{A^2}{B^2} (x_1^2 - z_1^2)(x_2^2 - z_2^2) \);
3. \( x' = \frac{x_0 + z_0}{x_3} \);
4. \( z' = \frac{x_0 - z_0}{z_3} \);
5. Return \( (x' : z') \).
Cost of the arithmetic with low level theta functions (car $k \neq 2$)

<table>
<thead>
<tr>
<th></th>
<th>Mumford</th>
<th>Level 2</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 coordinates</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></td>
<td></td>
<td>$7M + 6S + 1m_0$</td>
</tr>
</tbody>
</table>

Multiplication cost in genus 1 (one step).
The Weil pairing on elliptic curves

- Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $k$ (car $k \neq 2, 3$).
- Let $P, Q \in E[\ell]$ be points of $\ell$-torsion.
- Let $f_P$ be a function associated to the principal divisor $\ell(P - 0)$, and $f_Q$ to $\ell(Q - 0)$. We define:

$$e_{W,\ell}(P,Q) = \frac{f_Q(P - 0)}{f_P(Q - 0)}.$$ 

- The application $e_{W,\ell} : E[\ell] \times E[\ell] \to \mu_\ell(\overline{k})$ is a non degenerate pairing: the Weil pairing.
The Weil and Tate pairing with theta coordinates

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

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

\[e_{W,\ell}(P, Q) = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_P^0 \lambda_Q^1}.\]

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

\[e_{T,\ell}(P, Q) = \frac{\lambda_P^1}{\lambda_P^0}.\]
Why does it work?

\[ 0_A \quad \alpha P \quad \alpha^4(2P) \quad \ldots \quad \alpha^\ell(\ell P) = \lambda_0^\ell P 0_A \]

\[ \beta^4(2Q) \quad \frac{r^2 \alpha^2}{\beta}(2P + Q) \quad \ldots \quad \frac{r^\ell \alpha^{\ell(\ell - 1)}}{\beta^\ell - 1}(\ell P + Q) = \lambda_1^\ell P \beta^Q \]

\[ \beta^\ell(\ell Q) = \lambda_0^\ell P 0_A \quad \frac{r^\ell \beta^{\ell(\ell - 1)}}{\alpha^\ell - 1}(P + \ell Q) = \lambda_1^\ell Q \alpha P \]

We then have

\[ \lambda_0^\ell P = \alpha^\ell \lambda_0^\ell P, \quad \lambda_0^\ell Q = \beta^\ell \lambda_0^\ell Q, \quad \lambda_1^\ell P = \frac{r^\ell \alpha^{\ell(\ell - 1)}}{\beta^\ell} \lambda_1^\ell P, \quad \lambda_1^\ell Q = \frac{r^\ell \beta^{\ell(\ell - 1)}}{\alpha^\ell} \lambda_1^\ell Q, \]

\[ e_{W,\ell}(P, Q) = \frac{\lambda_1^\ell P \lambda_0^\ell Q}{\lambda_0^\ell P \lambda_1^\ell Q} = \frac{\lambda_1^\ell P \lambda_0^\ell Q}{\lambda_0^\ell P \lambda_1^\ell Q} = e_{W,\ell}(P, Q), \]

\[ e_{T,\ell}(P, Q) = \frac{\lambda_1^\ell P}{\lambda_0^\ell P} = \frac{r^\ell}{\alpha^\ell \beta^\ell} \frac{\lambda_1^\ell P}{\lambda_0^\ell P} = \frac{r^\ell}{\alpha^\ell \beta^\ell} e_{T,\ell}(P, Q). \]
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.

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

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

- **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) $\Rightarrow$ Verify a curve is secure.
- Compute the class field polynomials (CM-method) $\Rightarrow$ Construct a secure curve.
- Compute the modular polynomials $\Rightarrow$ Compute isogenies.
- Determine $\text{End}(A)$ $\Rightarrow$ 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

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

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

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

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

**Theorem**

- Let $\varphi : \mathbb{Z}(\overline{n}) \to \mathbb{Z}(\ell \cdot \overline{n})$, $x \mapsto \ell \cdot x$ be the canonical embedding. Let $K = A_2[\ell] \subset A_2[\ell \cdot n]$.
- Let $(\vartheta_i^A)_{i \in \mathbb{Z}(\overline{n})}$ be the theta functions of level $\ell \cdot n$ on $A = \mathbb{C}^g/ (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$.
- Let $(\vartheta_i^B)_{i \in \mathbb{Z}(\overline{n})}$ 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:
  
  \[(\vartheta_i^B(x))_{i \in \mathbb{Z}(\overline{n})} = (\vartheta_{\varphi(i)}^A(x))_{i \in \mathbb{Z}(\overline{n})}\]

**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 $g = 1$, $n = 2$, $\ell = 3$

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

$\pi$

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

$\hat{\pi}$
An example with $g = 1$, $n = 2$, $\ell = 3$

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

$\pi$

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

$\hat{\pi}$
An example with $g = 1$, $n = 2$, $\ell = 3$

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

$\pi$  

$\hat{\pi}$  

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

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

$$\pi$$

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

Diagram:

```
1
R2
R1
R0

\Omega

3\Omega
```
An example with $g = 1$, $n = 2$, $\ell = 3$

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

The diagram illustrates the relationship between $z$ and $\ell z$ modulo $\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g$. The horizontal line $\pi$ represents the mapping from $z$ to $\ell z$, while the vertical line $\hat{\pi}$ represents the mapping in the level $\ell n$.
An example with $g = 1$, $n = 2$, $\ell = 3$

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

$$\pi \quad \pi$$

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

1

$R_0$

$R_1$

$R_2$

$\Omega$

$3\Omega$
An example with $g = 1$, $n = 2$, $\ell = 3$

$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g)$, level $\ell n$ \hspace{1cm} $[\ell]$ \hspace{1cm} $\ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g)$, level $\ell n$

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

Diagram:

1

$R_2$

$R_1$

$R_0$

$\Omega$

$3\Omega$
Theorem (Koizumi–Kempf)

Let $F$ be a matrix of rank $r$ such that $^tFF = \ell \text{Id}_r$. 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

$$\vartheta \left[ \begin{array}{c} 0 \\ i_1 \\ \vdots \\ i_r \end{array} \right] (\frac{\Omega}{n}) \ldots \vartheta \left[ \begin{array}{c} 0 \\ i_r \end{array} \right] (\frac{\Omega}{n}) = \sum_{t_1, \ldots, t_r \in \frac{1}{\ell} \mathbb{Z}^g / \mathbb{Z}^g} \vartheta \left[ \begin{array}{c} 0 \\ j_1 \\ \vdots \\ j_r \end{array} \right] (X_1 + t_1, \frac{\Omega}{\ell n}) \ldots \vartheta \left[ \begin{array}{c} 0 \\ j_r \end{array} \right] (X_r + t_r, \frac{\Omega}{\ell n}),$$

(Two is the isogeny theorem applied to $F_A : A^r \rightarrow A^r$.)

- If $\ell = a^2 + b^2$, we take $F = \left( \begin{array}{cc} a & b \\ -b & a \end{array} \right)$, 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 $r = 4$.

$\Rightarrow$ We have a complete algorithm to compute the isogeny $A \mapsto A/K$ given the kernel $K$ [Cosset, Lubicz, R.].
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 $J \to \text{Jac}(H')$ (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.
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 basis 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 $J \rightarrow \text{Jac}(H')$ (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 $J \to \text{Jac}(H')$ (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

Let $H$ be a hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \text{Jac}(H)$, $\ell$ an 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.
Computing the right extension

- $J = \text{Jac}(H)$ abelian variety of dimension 2. $\chi(X)$ the corresponding zeta function.
- Degree of a point of $\ell$-torsion | the order of $X$ in $\mathbb{F}_\ell[X]/\chi(X)$.
- If $K$ rational, $K(\overline{k}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$, the degree of a point in $K$ | the LCM of orders of $X$ in $\mathbb{F}_\ell[X]/P(X)$ for $P \mid \chi$ of degree two.
- Since we are looking to $K$ maximal isotropic, $J[\ell] \simeq K \oplus K'$ and we know that $P \mid \chi$ is such that $\chi(X) \equiv P(X)P(\overline{X}) \mod \ell$ where $\overline{X} = q/X$ represents the Verschiebung.

Remark

The degree $n$ is $\leq \ell^2 - 1$. If $\ell$ is totally split in $\mathbb{Z}[\pi, \overline{\pi}]$ then $n \mid \ell - 1$. 
Computing the $\ell$-torsion

- We want to compute $J(\mathbb{F}_{q^n})[\ell]$.
- From the zeta function $\chi(X)$ we can compute random points in $J(\mathbb{F}_{q^n})[\ell^\infty]$ uniformly.
- If $P$ is in $J(\mathbb{F}_{q^n})[\ell^\infty]$, $\ell^m P \in J(\mathbb{F}_{q^n})[\ell]$ for a suitable $m$. This does not give uniform points of $\ell$-torsion but we can correct the points obtained.

**Example**

- Suppose $J(\mathbb{F}_{q^n})[\ell^\infty] = \langle P_1, P_2 \rangle$ with $P_1$ of order $\ell^2$ and $P_2$ of order $\ell$.
- First random point $Q_1 = P_1 \Rightarrow$ we recover the point of $\ell$-torsion: $\ell P_1$.
- Second random point $Q_2 = \alpha P_1 + \beta P_2$. If $\alpha \neq 0$ we recover the point of $\ell$-torsion $\alpha \ell P_1$ which is not a new generator.
- We correct the original point: $Q'_2 = Q_2 - \alpha Q_1 = \beta P_2$. 
Isogeny graphs for elliptic curves
Horizontal isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q}_2$
Horizontal isogeny graphs: \( \ell = q_1 q_2 = Q_1 \bar{Q}_1 Q_2 \bar{Q}_2 \)
Horizontal isogeny graphs: $\ell = q = Q\overline{Q}$

$(\mathbb{Q} \leftrightarrow K_0 \leftrightarrow K)$
Horizontal isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2^2$
Horizontal isogeny graphs: $\ell = q^2 = Q^2 \bar{Q}^2$
Horizontal isogeny graphs: $\ell = q^2 = Q^4$
General isogeny graphs ($\ell = q = Q\overline{Q}$)
General isogeny graphs ($\ell = q = Q\overline{Q}$)
General isogeny graphs \((\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q}_2)\)
General isogeny graphs \((\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q}_2)\)
General isogeny graphs \( (\ell = q_1 q_2 = Q_1 Q_2) \)
Isogeny graph and lattice of orders in genus 2
Isogeny graph and lattice of orders in genus 2
Isogeny graph and lattice of orders in genus 2
Isogeny graph and lattice of orders in genus 2
Isogeny graph and lattice of orders in genus 2
Isogeny graph and lattice of orders in genus 2
Isogeny graph and lattice of orders in genus 2
Isogeny graph and lattice of orders in genus 2
Applications and perspectives

- Modular polynomials in genus 2.
- Isogenies using rational coordinates?
- How to compute cyclic isogenies in genus 2?
- Dimension 3.
Thank you for your attention!
Bibliography


