

# Computing isogenies and applications in cryptography

Damien Robert<sup>1</sup>

<sup>1</sup>LFANT Team, IMB & Inria Bordeaux Sud-Ouest

11/01/2011 (Verimag, Grenoble)



# Discrete logarithm

## 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).
- ⇒ Usual tools of public key cryptography: asymmetric encryption, signature, zero-knowledge, PRNG...
- $G = \mathbb{F}_p^*$ : sub-exponential attacks.
- ⇒ Find **secure** groups with **efficient law**, **compact representation**.

# Abelian varieties

## Definition

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

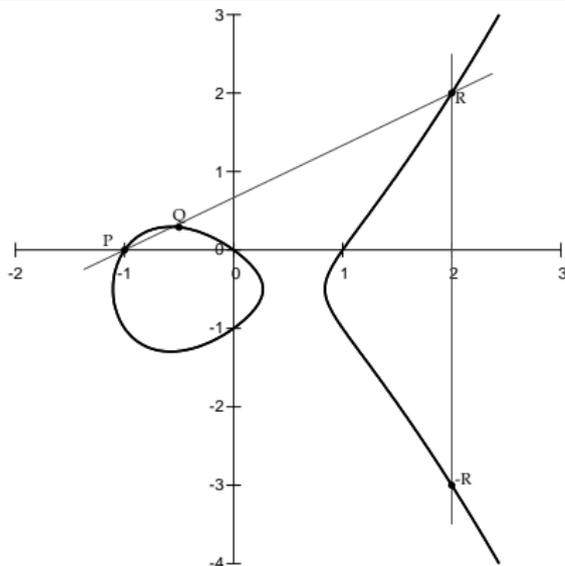
- Abelian variety = **points** on a projective space (locus of homogeneous polynomials) + an abelian group law given by **rational functions**.
- ⇒ Use  $G = A(k)$  with  $k = \mathbb{F}_q$  for the DLP.
- ⇒ Pairing-based cryptography with the **Weil** or **Tate** pairing.  
(Identity-based cryptography, Short signature, One way tripartite Diffie-Hellman, Self-blindable credential certificates, Attribute based cryptography, Broadcast encryption...)

# Elliptic curves

## Definition (char $k \neq 2, 3$ )

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

- 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

$C: y^2 = f(x)$ , hyperelliptic curve of genus  $g$ . ( $\deg f = 2g + 1$ )

- Divisor: formal sum  $D = \sum n_i P_i$ ,  $P_i \in C(\bar{k})$ .  
 $\deg D = \sum n_i$ .

- Principal divisor:  $\sum_{P \in C(\bar{k})} v_P(f) \cdot P$ ;  $f \in \bar{k}(C)$ .

Jacobian of  $C$  = Divisors of degree 0 modulo principal divisors

- + Galois action  
= Abelian variety of dimension  $g$ .
- Divisor class  $D \Rightarrow$  **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:**  $D = (u, v) \Rightarrow u = \prod (x - x_i)$ ,  $v(x_i) = y_i$ .
- **Cantor algorithm:** addition law.



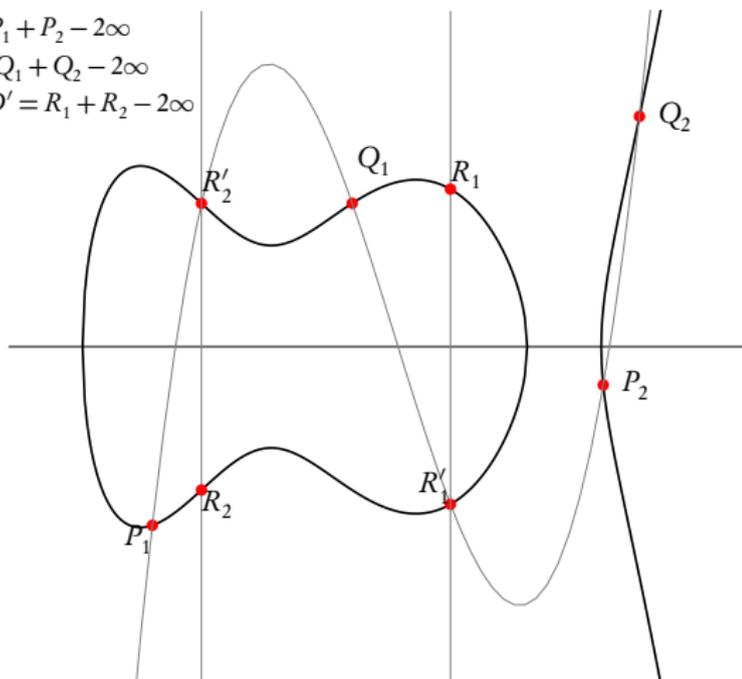


# Example of the addition law in genus 2

$$D = P_1 + P_2 - 2\infty$$

$$D' = Q_1 + Q_2 - 2\infty$$

$$D + D' = R_1 + R_2 - 2\infty$$



# Isogenies

## Definition

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

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

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

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

- *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

$$\begin{aligned} v_{0_E}(x) &= -2 & v_P(x) &\geq 0 & \text{if } P \neq 0_E \\ v_{0_E}(y) &= -3 & v_P(y) &\geq 0 & \text{if } P \neq 0_E \\ y^2/x^3(0_E) &= 1 \end{aligned}$$

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

# 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  $\mathbb{C}^g$ .

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i {}^t(n+a)\Omega(n+a) + 2\pi i {}^t(n+a)(z+b)} \quad a, b \in \mathbb{Q}^g$$

- Projective coordinates:

$$\begin{aligned} A &\longrightarrow \mathbb{P}_{\mathbb{C}}^{n^g-1} \\ z &\longmapsto (\vartheta_i(z))_{i \in Z(\bar{n})} \end{aligned}$$

where  $Z(\bar{n}) = \mathbb{Z}^g / n\mathbb{Z}^g$  and  $\vartheta_i = \vartheta \left[ \begin{smallmatrix} 0 \\ i \\ \cdot \\ n \end{smallmatrix} \right] (\cdot, \frac{\Omega}{n})$ .

# Theta functions of level $n$

- $(\vartheta_i)_{i \in \mathbb{Z}(\overline{n})}$ : basis of the theta functions of level  $n$   
 $\Leftrightarrow A[n] = A_1[n] \oplus A_2[n]$ : 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 ( $k = \mathbb{C}$ )

$$\left( \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{i+t}(x+y) \vartheta_{j+t}(x-y) \right) \cdot \left( \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{k+t}(0) \vartheta_{l+t}(0) \right) =$$

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

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

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

$$A = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

# The isogeny theorem

## Theorem

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

$$(\vartheta_i^B(x))_{i \in Z(\overline{n})} = (\vartheta_{\varphi(i)}^A(x))_{i \in Z(\overline{n})}$$

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

$$\begin{array}{ccc} z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n & \xrightarrow{[\ell]} & \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\ & \searrow \pi & \nearrow \hat{\pi} \\ & z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n & \end{array}$$

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

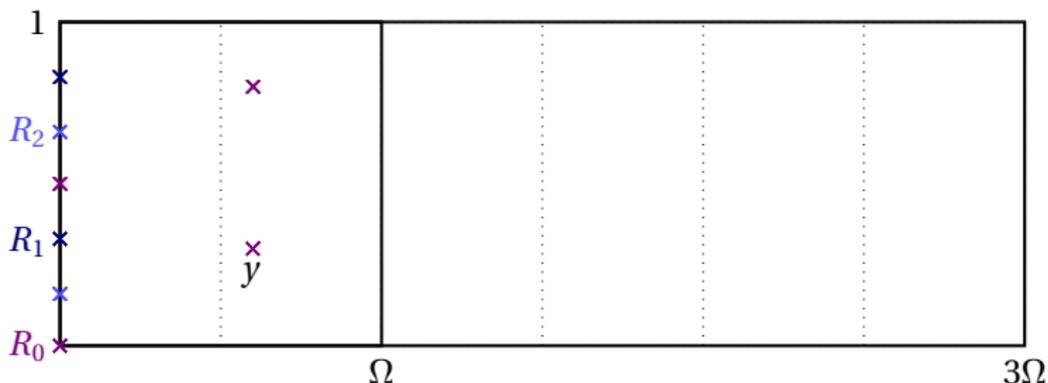
$$\begin{array}{ccc} z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n & \xrightarrow{[\ell]} & \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\ & \searrow \pi & \nearrow \hat{\pi} \\ & z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n & \end{array}$$

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

$$\begin{array}{ccc} z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n & \xrightarrow{[\ell]} & \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\ & \searrow \pi & \nearrow \hat{\pi} \\ & z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n & \end{array}$$

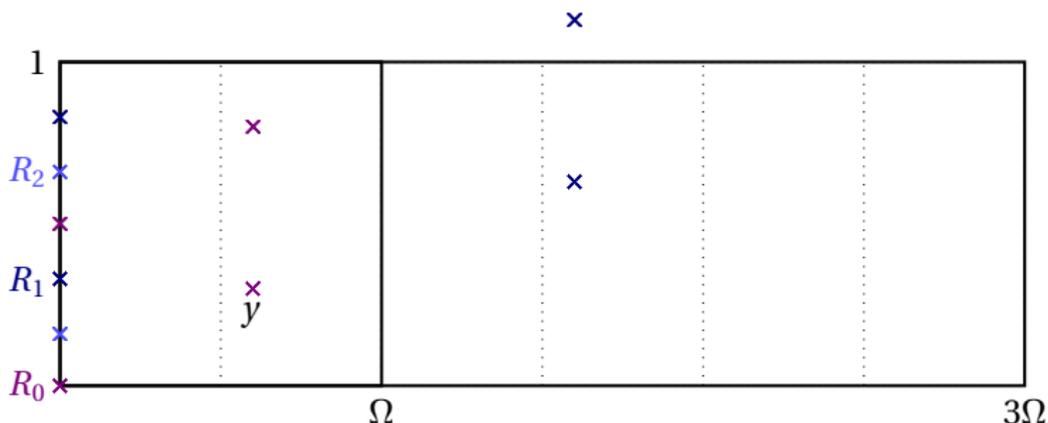
# An example with $g = 1, n = 2, \ell = 3$

$$\begin{array}{ccc}
 z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n & \xrightarrow{[\ell]} & \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
 & \searrow \pi & \nearrow \hat{\pi} \\
 & z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n & 
 \end{array}$$



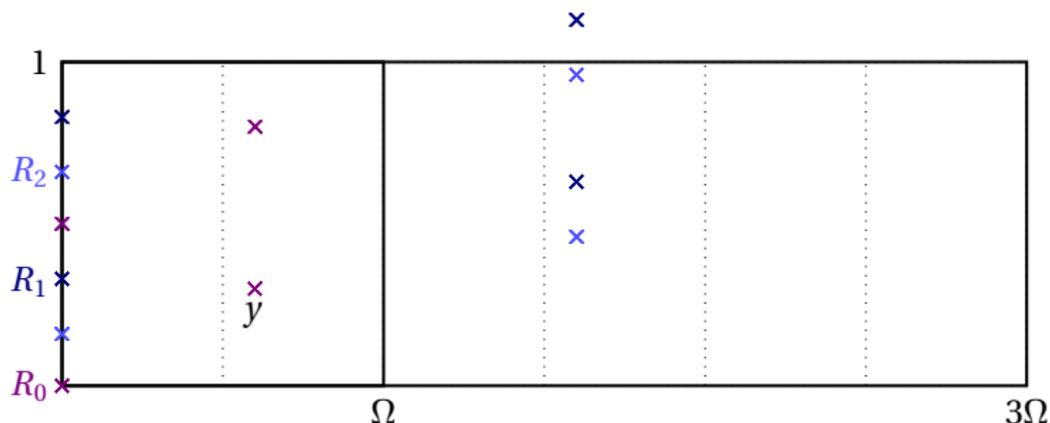
# An example with $g = 1, n = 2, \ell = 3$

$$\begin{array}{ccc}
 z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n & \xrightarrow{[\ell]} & \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
 & \searrow \pi & \nearrow \hat{\pi} \\
 & z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n &
 \end{array}$$



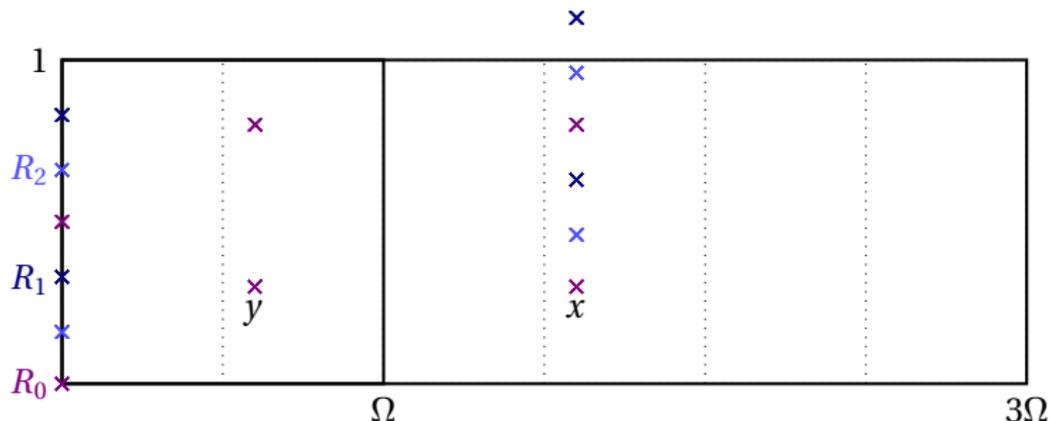
# An example with $g = 1, n = 2, \ell = 3$

$$\begin{array}{ccc}
 z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n & \xrightarrow{[\ell]} & \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
 & \searrow \pi & \nearrow \hat{\pi} \\
 & z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n & 
 \end{array}$$



# An example with $g = 1$ , $n = 2$ , $l = 3$

$$\begin{array}{ccc}
 z \in \mathbb{C}^g / (\mathbb{Z}^g + l\Omega\mathbb{Z}^g), \text{ level } ln & \xrightarrow{[\ell]} & lz \in \mathbb{C}^g / (\mathbb{Z}^g + l\Omega\mathbb{Z}^g), \text{ level } ln \\
 & \searrow \pi & \nearrow \hat{\pi} \\
 & z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n & 
 \end{array}$$



# Changing level

## Theorem (Koizumi–Kempf)

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

$$\vartheta \left[ \begin{smallmatrix} 0 \\ i_1 \end{smallmatrix} \right] \left( Y_1, \frac{\Omega}{n} \right) \cdots \vartheta \left[ \begin{smallmatrix} 0 \\ i_r \end{smallmatrix} \right] \left( Y_r, \frac{\Omega}{n} \right) = \sum_{\substack{t_1, \dots, t_r \in \frac{1}{\ell} \mathbb{Z}^g / \mathbb{Z}^g \\ F(t_1, \dots, t_r) = (0, \dots, 0)}} \vartheta \left[ \begin{smallmatrix} 0 \\ j_1 \end{smallmatrix} \right] \left( X_1 + t_1, \frac{\Omega}{\ell n} \right) \cdots \vartheta \left[ \begin{smallmatrix} 0 \\ j_r \end{smallmatrix} \right] \left( X_r + t_r, \frac{\Omega}{\ell n} \right),$$

- 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  $r = 4$ .

# Changing level and isogenies

## Corollary

Let  $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g)$  and  $B = \mathbb{C}^g / (\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g)$ . We can express the isogeny  $A \rightarrow B, z \mapsto \ell z$  of kernel  $K = \frac{1}{\ell}\mathbb{Z}^g / \mathbb{Z}^g$  in term of the theta functions of level  $n$  on  $A$  and  $B$ :

$$\vartheta \begin{bmatrix} 0 \\ i_1 \end{bmatrix} \left( \ell z, \frac{\ell\Omega}{n} \right) \vartheta \begin{bmatrix} 0 \\ i_2 \end{bmatrix} \left( 0, \ell \frac{\ell\Omega}{n} \right) \dots \vartheta \begin{bmatrix} 0 \\ i_r \end{bmatrix} \left( 0, \frac{\ell\Omega}{n} \right) =$$

$$\sum_{\substack{t_1, \dots, t_r \in K \\ F(t_1, \dots, t_r) = (0, \dots, 0)}} \vartheta \begin{bmatrix} 0 \\ j_1 \end{bmatrix} \left( X_1 + t_1, \frac{\Omega}{n} \right) \dots \vartheta \begin{bmatrix} 0 \\ j_r \end{bmatrix} \left( X_r + t_r, \frac{\Omega}{n} \right),$$

where  $X = F^{-1}(\ell z, 0, \dots, 0)$ .

## Remark

We compute the coordinates  $\vartheta \begin{bmatrix} 0 \\ j_i \end{bmatrix} \left( X_i + t_i, \frac{\Omega}{n} \right)$  in  $\mathbb{C}^g$  using differential additions.

# 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  $A \rightarrow A/K$ .
  - 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:

$$\begin{array}{ccc} A & \xrightarrow{\hat{\pi}} & B \\ \parallel & & \parallel \\ \text{Jac}(C_1) & \cdots \cdots \cdots \rightarrow & \text{Jac}(C_2) \end{array}$$

# AVIsogenies

- AVIsogenies: Magma code written by Bisson, Cosset and R.  
<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  $J \mapsto \text{Jac}(H')$  (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  $J \mapsto \text{Jac}(H')$  (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  $J \mapsto \text{Jac}(H')$  (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  $J \mapsto \text{Jac}(H')$  (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  $J \mapsto \text{Jac}(H')$  (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  $J \mapsto \text{Jac}(H')$  (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  $J \mapsto \text{Jac}(H')$  (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  $J \mapsto \text{Jac}(H')$  (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  $J \mapsto \text{Jac}(H')$  (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,  $K(\bar{k}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ , the degree of a point in  $K$  | the LCM of orders of  $X$  in  $\mathbb{F}_\ell[X]/P(X)$  for  $P | \chi$  of degree two.
- Since we are looking to  $K$  maximal isotropic,  $J[\ell] \simeq K \oplus K'$  and we know that  $P | \chi$  is such that  $\chi(X) \equiv P(X)P(\bar{X}) \pmod{\ell}$  where  $\bar{X} = q/X$  represents the Verschiebung.

### Remark

*The degree  $n$  is  $\leq \ell^2 - 1$ . If  $\ell$  is totally split in  $\mathbb{Z}[\pi, \bar{\pi}]$  then  $n | \ell - 1$ .*

# 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:  $\ell \cdot P_1$ .
- 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:  $Q'_2 = Q_2 - \alpha Q_1 = \beta P_2$ .

# Weil pairing

- Used to decompose a point  $P \in J[\ell]$  in term of a basis of the  $\ell$ -torsion (and to construct a symplectic basis).
- The magma implementation is **extremely** slow in genus 2 for non degenerate divisors.
- But since we convert the points in theta coordinates we can use the pairing in theta coordinates [LR10].

# Timings for isogenies computations

 $(\ell = 7)$ 

```
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 subgroups over Finite field of size  $3^{24}$ 
-- Convert the subgroups to theta coordinates
Time: 0.060
Computing the 1 7 -isogenies
** Precomputations for  $\ell=7$  Time: 0.180
** Computing the 7 -isogeny
    Computing the  $\ell$ -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  $y^2 = t^{615}x^6 + t^{224}x^5 + t^{37}x^4 + t^{303}x^3 + t^{715}x^2 + t^{...}$ 
```

# Timings for isogenies computations

 $(\ell = 5)$ 

```
Jacobian of Hyperelliptic Curve defined by  $y^2 = 39*x^6 + 4*x^5 + 82*x^4 + 10*x^3 + 31*x^2 + 39*x + 2$  over GF(83)
> time RationallyIsogenousCurvesG2(J,5);
** Computing 5 -rational 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
 $y^2 = 27*x^6 + 63*x^5 + 5*x^4 + 24*x^3 + 34*x^2 + 6*x + 76$  over GF(
...]
```

# Timings for isogeny graphs

 $(\ell = 3)$ 

```
Jacobian of Hyperelliptic Curve defined by  $y^2 = 41*x^6 + 131*x^5 + 55*x^4 + 57*x^3 + 233*x^2 + 225*x + 51$  over GF(271)
time isograph,jacobians:=IsoGraphG2(J,{3}: 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  $y^2 = 97*x^6 + 77*x^5 + 62*x^4 + 14*x^3 + 33*x^2 + 18*x + 40$  over GF(113)
> time RationallyIsogenousCurvesG2(J,53);
** Computing 53 -rational 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  $\ell = 53$  Time: 0.240
** Computing the 53 -isogeny
  Computing the  $\ell$ -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  $y^2 = 194*x^6 + 554*x^5 + 606*x^4 + 523*x^3 + 642*x^2 + 566*x + 112$  over GF(859)
> time RationallyIsogenousCurvesG2(J,19);
** Computing 19 -rational isotropic subgroups (extension degree
Time: 0.760
Computing the 2 19 -isogenies
** Precomputations for  $\ell=19$  Time: 11.160
** Computing the 19 -isogeny
    Computing the  $\ell$ -torsion Time: 0.250
    Changing level Time: 18.590
Time: 18.850
** Computing the 19 -isogeny
    Computing the  $\ell$ -torsion Time: 0.250
    Changing level Time: 18.640
Time: 18.900
Time: 51.060
[ <[ 341, 740, 389 ], Jacobian of Hyperelliptic Curve defined by  $y^2 = 680*x^5 + 538*x^4 + 613*x^3 + 557*x^2 + 856*x + 628$  over GF(859)
... ]
```

# A record isogeny computation!

 $(\ell = 1321)$ 

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

```
> time RationallyIsogenousCurvesG2(J,1321:ext_degree:=1);
** Computing 1321 -rational 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
```

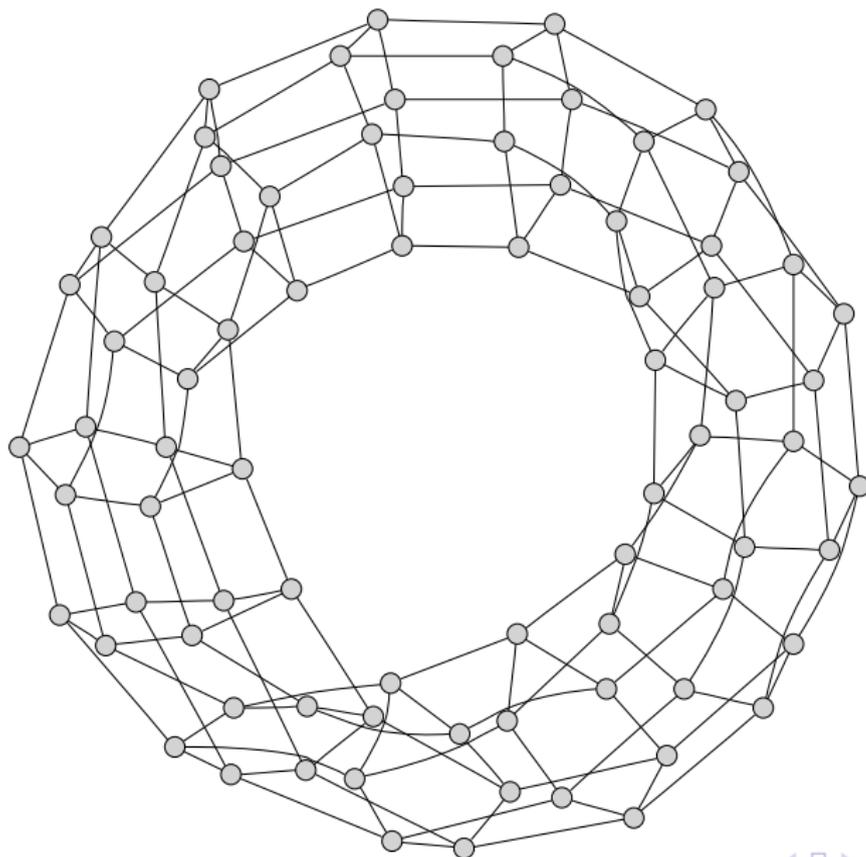
```
Time: 7004.240
```

```
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)> ]
```

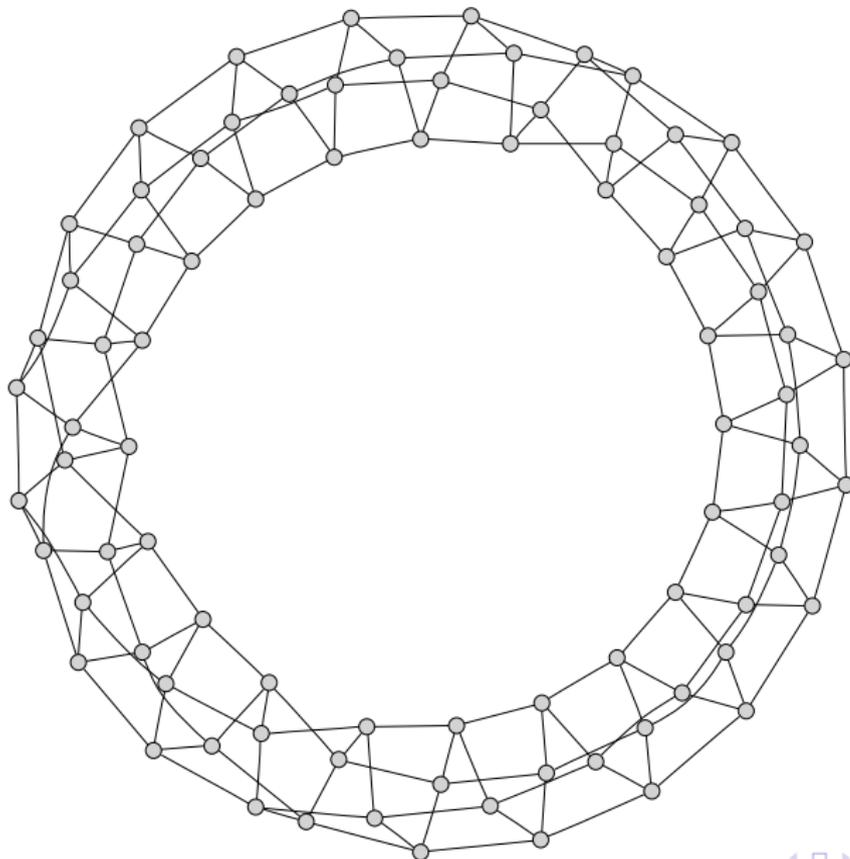
Isogeny graphs:  $\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$

$(\mathbb{Q} \mapsto K_0 \mapsto K)$



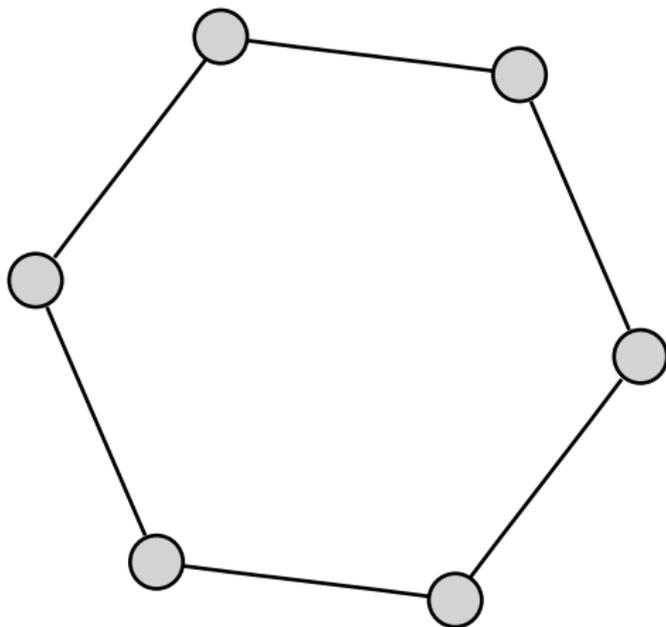
Isogeny graphs:  $\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$

$(\mathbb{Q} \mapsto K_0 \mapsto K)$



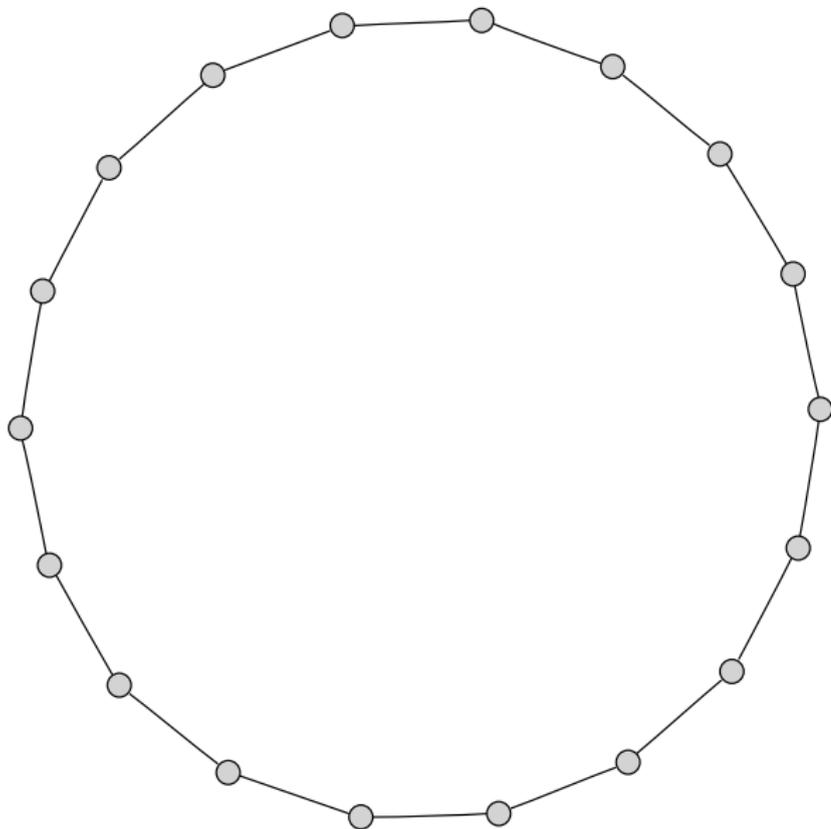
# Isogeny graphs: $\ell = q = Q\bar{Q}$

$(\mathbb{Q} \mapsto K_0 \mapsto K)$



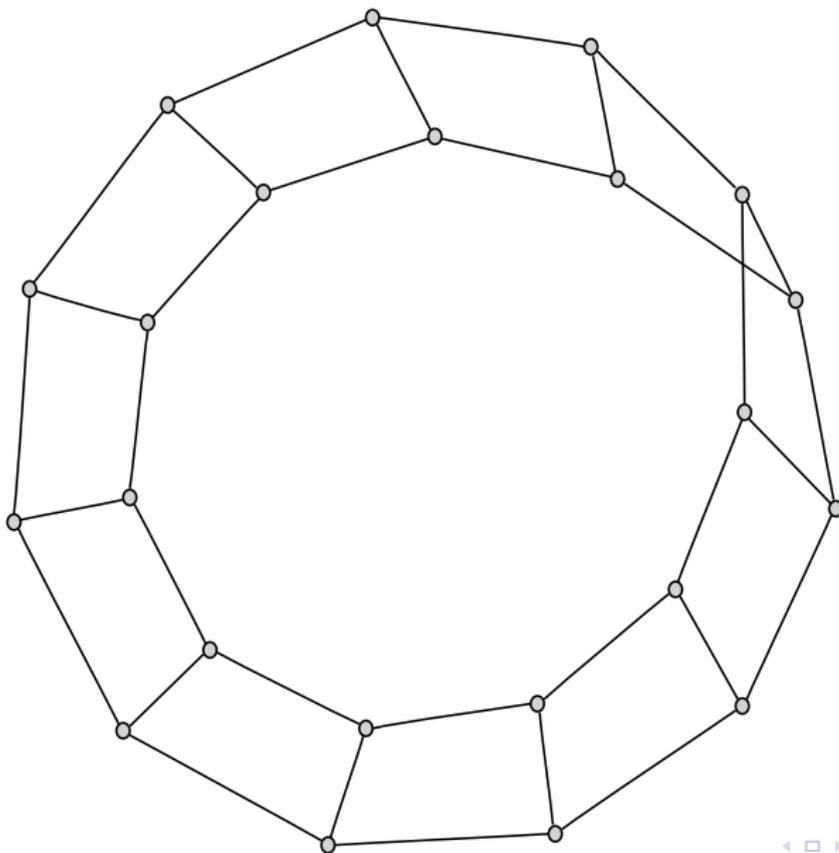
Isogeny graphs:  $\ell = q_1 q_2 = Q_1 \bar{Q}_1 Q_2^2$

$(\mathbb{Q} \mapsto K_0 \mapsto K)$



Isogeny graphs:  $\ell = q^2 = Q^2\bar{Q}^2$

$(\mathbb{Q} \mapsto K_0 \mapsto K)$



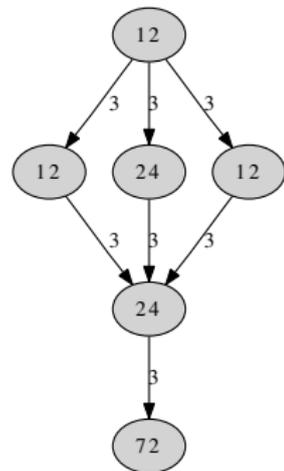
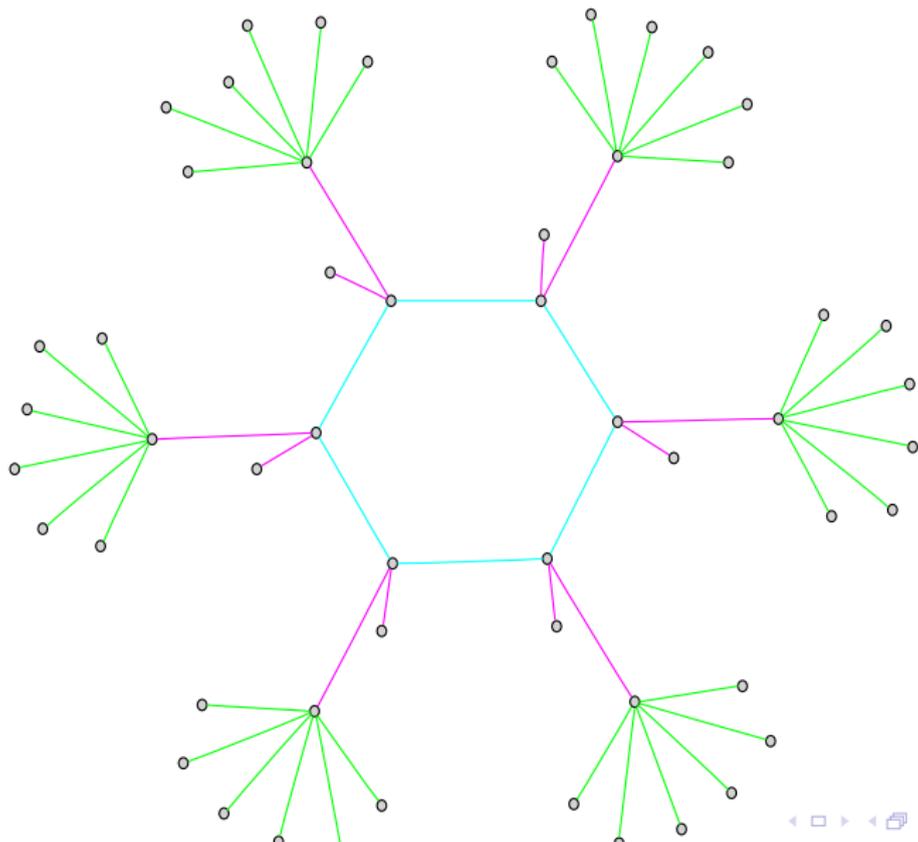
# Isogeny graphs: $\ell = q^2 = Q^4$

$(\mathbb{Q} \mapsto K_0 \mapsto K)$

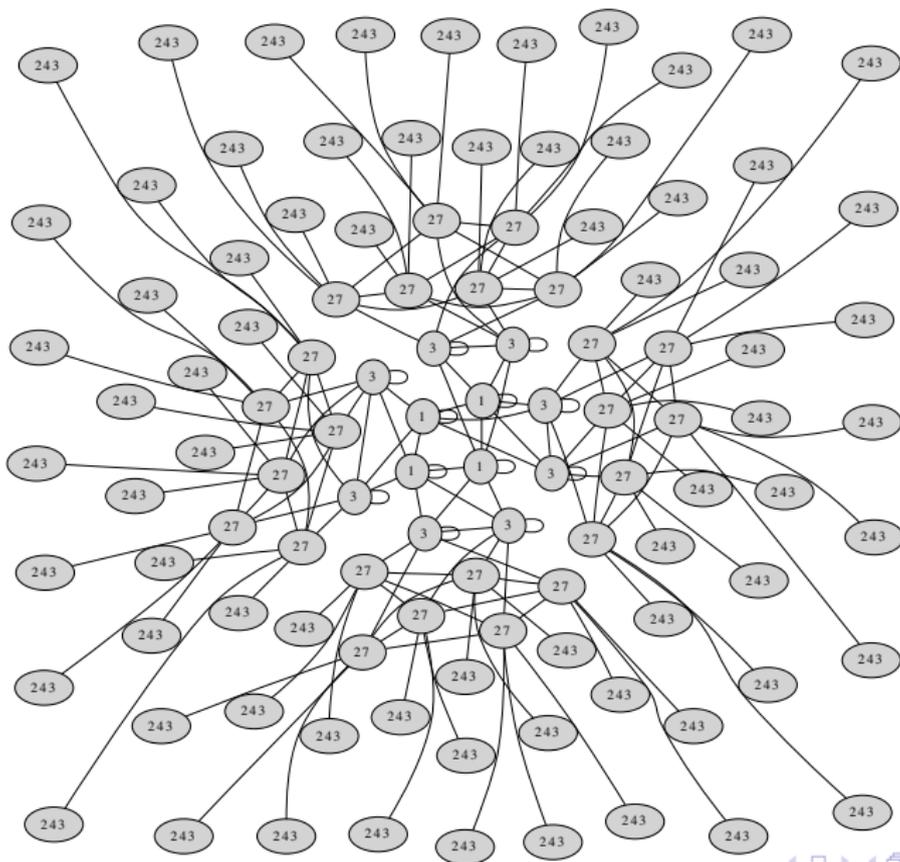




# Non maximal isogeny graphs ( $\ell = q = Q\bar{Q}$ )

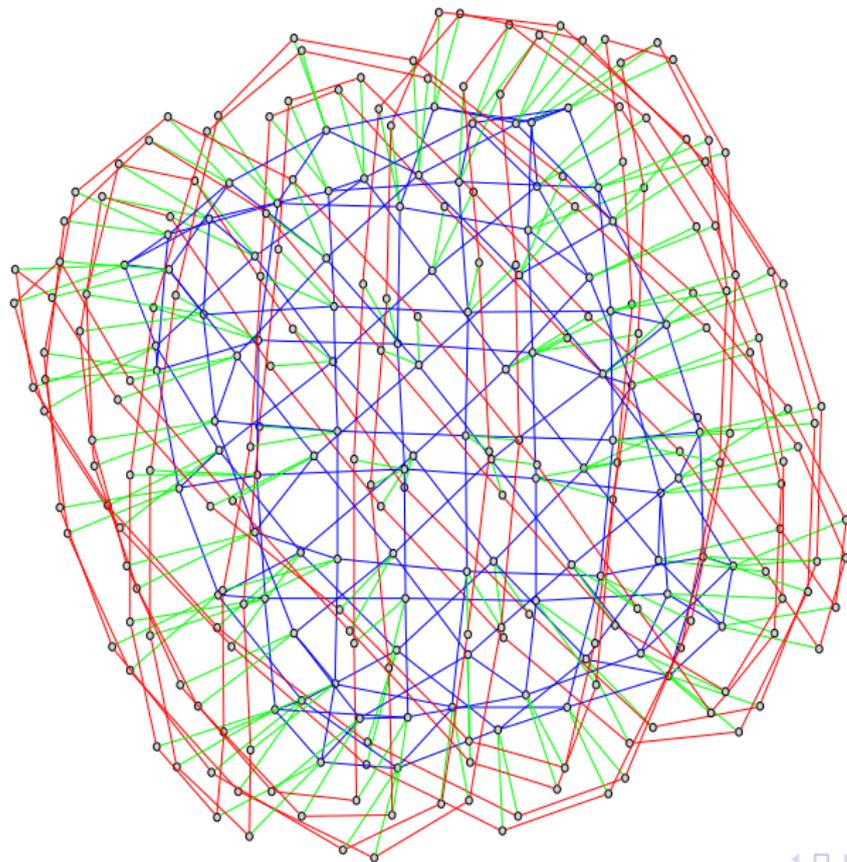


# Non maximal isogeny graphs ( $\ell = q = Q\bar{Q}$ )



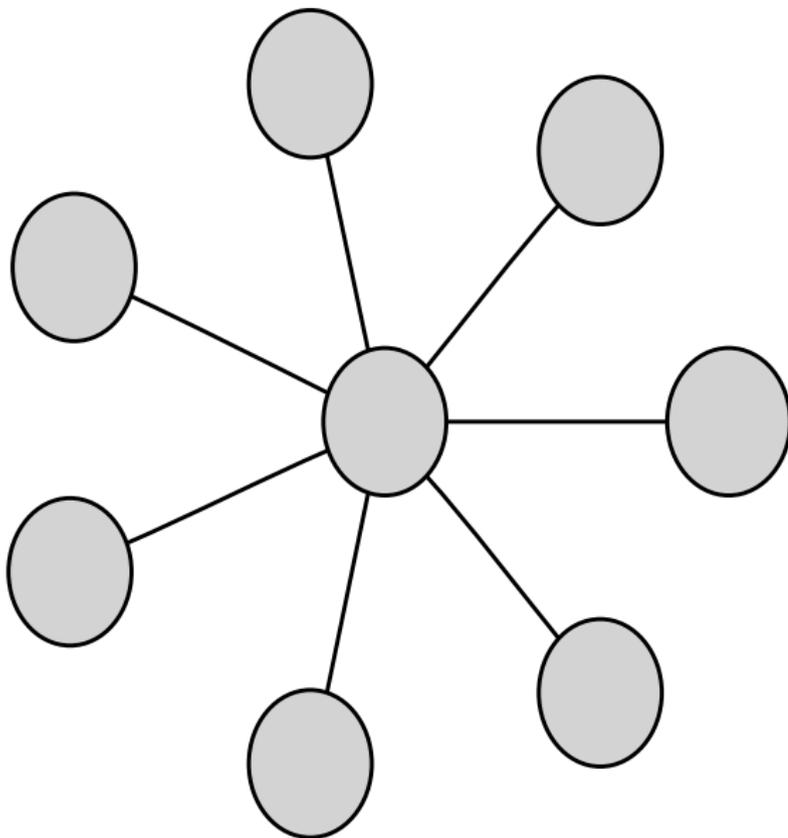


# Non maximal isogeny graphs ( $\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$ )

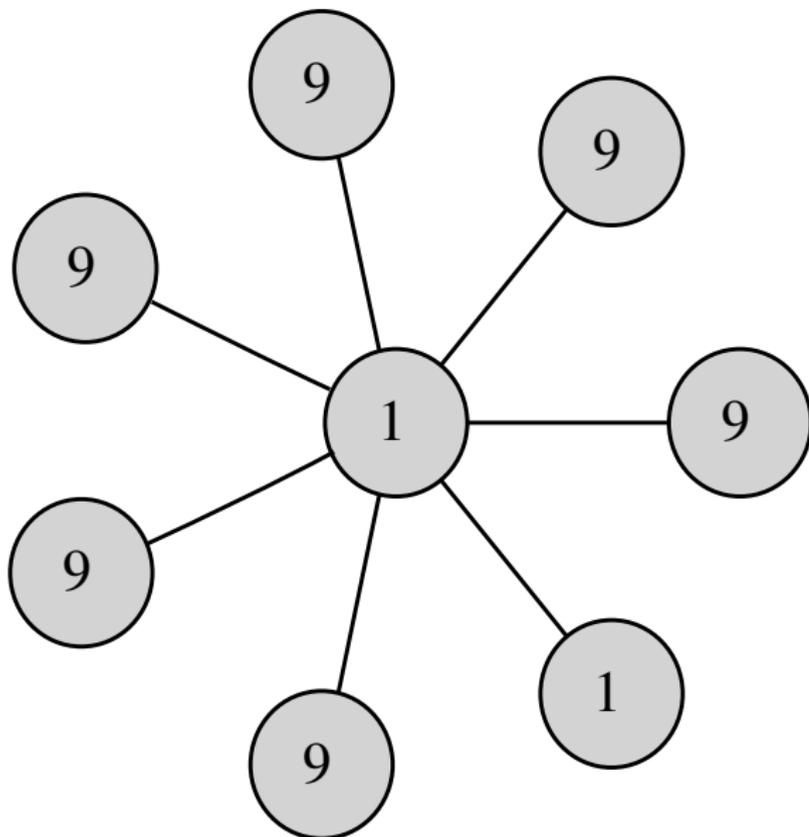




# Non maximal isogeny graphs ( $\ell = q = Q^2$ )



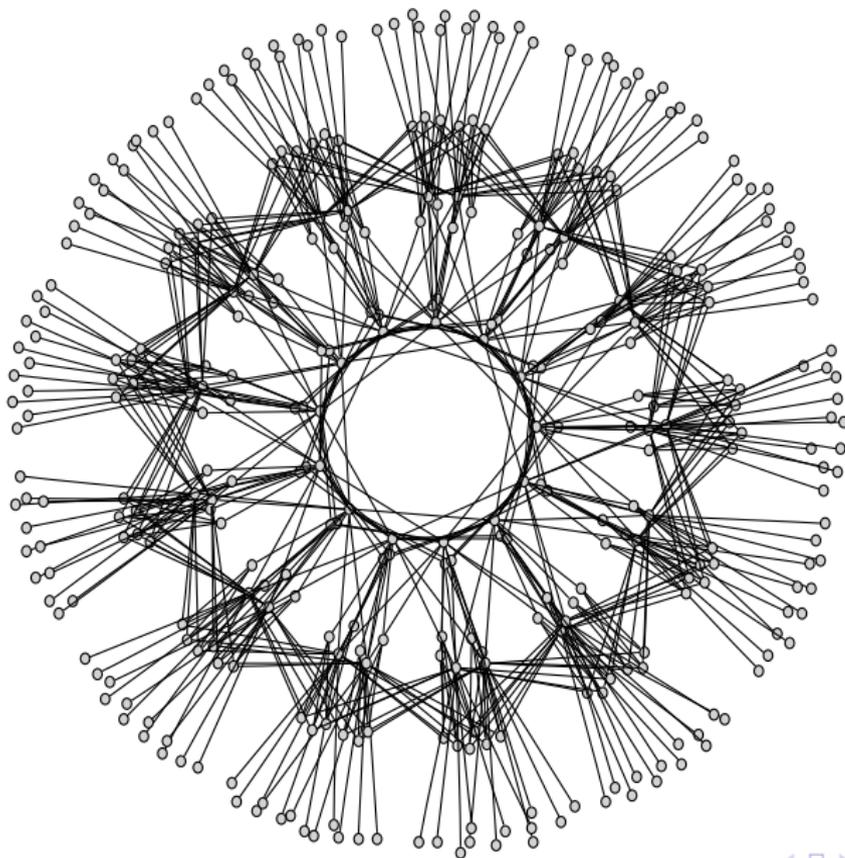
# Non maximal isogeny graphs ( $\ell = q = Q^2$ )



# 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  $J/\mathbb{F}_p$  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

- [BS09] G. Bisson and A. Sutherland. “Computing the endomorphism ring of an ordinary elliptic curve over a finite field”. In: *Journal of Number Theory* (2009) (cit. on p. 60).
- [LR10] D. Lubicz and D. Robert. *Efficient pairing computation with theta functions*. Ed. by G. Hanrot, F. Morain, and E. Thomé. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Jan. 2010. URL: <http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf> (cit. on p. 39).