Modular polynomials for abelian surfaces

Damien Robert

LFANT project-team
INRIA Bordeaux–Sud-Ouest
damien.robert@inria.fr
http://www.normalesup.org/~robert

Evaluation seminar 2019-03-20

Outline

Principally polarised abelian varieties over $\mathbb{C}$

Definition

Principally polarised complex abelian variety A of dimension g = compact Lie group V/Λ with
- V: complex vector space of dimension g (linear data);
- Λ: $\mathbb{Z}$-lattice in V (of rank $2g$) (arithmetic data);
- + H: Hermitian form on V | $E(\Lambda,\Lambda)\subset\mathbb{Z}$ where $E := \operatorname{Im} H$ is a principal symplectic form (quadratic data: pairings).

- H : polarisation on A. Conversely, any symplectic form E on V such that $E(\Lambda,\Lambda)\subset\mathbb{Z}$ and $E(ix,iy)=E(x,y)$ for all $x,y\in V$ gives a polarisation H with $E=\operatorname{Im} H$.

⇒ Algebraic coordinates.

- Principal polarisation: over a symplectic basis of Λ, E is of the form $\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$.
- Moduli space of principally polarised abelian varieties: $\mathfrak{H}_g/\mathrm{Sp}_{2g}(\mathbb{Z})$ of dimension $g(g+1)/2$.
- $\Lambda=\Omega\mathbb{Z}^g\oplus\mathbb{Z}^g$, $H=(\Im\Omega)^{-1}$.

Isogenies

Definition

$A := V/\Lambda, B := V'/\Lambda'$ abelian varieties.
- Isogeny: $f: A\to B$ bijective linear map $f: V\to V'$ | $f(\Lambda)\subset\Lambda'$.
- Kernel: $f^{-1}(\Lambda')/\Lambda\subset A$, degree $\deg f := \#K$.
- $f:(A,H_1)\to(B,H_2)$ = ℓ-isogeny between principally polarised abelian varieties if

$$f^*H_2=\ell H_1.$$

- Two abelian varieties over a finite field are isogenous iff they have the same zeta function (Tate);

Theorem (Weil, Mumford)

$f\mapsto \operatorname{Ker} f$: {ℓ − isogenies} ⇔ {maximally isotropic subgroup of $A[\ell]$ for the Weil pairing}.

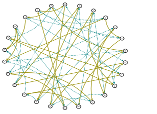
Cryptographic applications of isogenies

Transport the DLP
- Extend attacks using Weil descent [GHS02]
- Transfer the DLP from the Jacobian of an hyperelliptic curve of genus 3 to the Jacobian of a quartic curve [Smi09].

Work with smaller data
- SEA point counting algorithm [Sch95; Mor95; Elk97];
- CRT algorithms to compute class polynomials [Sut11; ES10], [Lauter-R.];
- CRT algorithms to compute modular polynomials [BLS12].

- Splitting the multiplication using isogenies can improve the arithmetic [DIK06; Gau07];
- The isogeny graph of a supersingular elliptic curve can be used to construct secure hash functions [CLG09];
- Construct public key cryptosystems by hiding vulnerable curves by an isogeny (the trapdoor) [Tes06], or by encoding informations in the isogeny graph [RS06];
- Take isogenies to reduce the impact of side channel attacks [Sma03];
- Construct a normal basis of a finite field [CL09];
- Improve the discrete logarithm in $\mathbb{F}_{q^n}$ by finding a smoothness basis invariant by automorphisms [CL08].
- Construct verifiable delay functions [De +19].

Post-quantum key exchange using isogeny graphs [DJP14]



Birational invariants for $\mathfrak{H}_2/\mathrm{Sp}_4(\mathbb{Z})$

Definition
- Igusa invariants: Siegel modular functions j_1, j_2, j_3 for $\Gamma := \mathrm{Sp}_4(\mathbb{Z})$

$$j_1 := \frac{h_4h_6}{h_{10}},\quad j_2 := \frac{h_4^2h_{12}}{h_{10}^2},\quad j_3 := \frac{h_4^5}{h_{10}^2}.$$

where the h_i are modular forms of weight i given by explicit polynomials in terms of theta constants.

- 3 Igusa invariants ⇒ birational equivalence between $\mathfrak{H}_2/\Gamma$ and $\mathbb{P}^3_{\mathbb{C}}$;
- Always determine A ⇒ need 10 invariants.
- Denominator $h_{10}=0$ ⇔ A =product of elliptic curves.
- $j_{i,\ell}(\Omega) := j_i(\ell\Omega)$ ⇒ $B := \mathbb{C}^g/(\ell\Omega\mathbb{Z}^g+\mathbb{Z}^g)$ = abelian surface ℓ-isogeneous to $A := \mathbb{C}^g/(\Omega\mathbb{Z}^g+\mathbb{Z}^g)$;
- Others ppav ℓ-isogenous to A ⇔ action of $\Gamma/\Gamma_0(\ell)$ on Ω. Index: $\ell^3+\ell^2+\ell+1$.

Modular polynomials in dimension 2

Definition (Hecke representation of ℓ-modular polynomials)

$$\Phi_{1,\ell}(j_1,j_2,j_3,Y_1)=\prod_{\gamma\in\Gamma/\Gamma_0(\ell)}(Y_1-j_{1,\ell}^{\gamma})\qquad j_{i,\ell}(\Omega)=j_i(\ell\Omega)$$

$$\Psi_{i,\ell}(j_1,j_2,j_3,Y_i)=\sum_{\gamma\in\Gamma/\Gamma_0(\ell)} j_{i,\ell}^{\gamma}\prod_{\gamma'\in\Gamma/\Gamma_0(\ell)\setminus\{\gamma\}}(Y_i-j_{1,\ell}^{\gamma'})\quad (i=2,3)$$

$$\Phi_\ell := \{\Phi_{1,\ell}(X_1,X_2,X_3,Y_1), Y_i\Phi'_{1,\ell}(X_1,X_2,X_3,Y_1)-\Psi_{i,\ell}(X_1,X_2,X_3,Y_i)\}\in\mathbb{Q}(X_1,X_2,X_3)[Y_1,Y_2,Y_3]^3.$$

- $\Phi_\ell(j_A,j_B)=0$ iff B is ℓ-isogenous to A;
- Computed via a multidimensional evaluation-interpolation approach (need to compute period matrices);

⇒ Evaluation of the modular invariants on Ω at high precision;

⇒ Generalized version of the AGM to compute theta functions in quasi-linear time in the precision [Dup06];

⇒ Need to interpolate rational functions;

- Denominator = the Humbert surface H_{ℓ^2} of discriminant ℓ^2 [BL09; Gru10]= abelian surfaces ℓ-isogenous to products of elliptic curves;
- Quasi-linear algorithm [Dup06; Mil14];
- Can be generalized to smaller modular invariants [Mil14].

Example of modular polynomials in dimension 2 [Mil14]

Invariant	ℓ	Size
Igusa	2	57 MB
Streng	2	2.1 MB
Streng	3	890 MB
Theta	3	175 KB
Theta	5	200 MB
Theta	7	29 GB

Examples
- The denominator of $\Phi_{1,3}$ for modular functions b_1, b_2, b_3 derived from theta constants of level 2 is:

$$1024b_3^6b_2^6b_1^{10}-((768b_3^8+1536b_3^4-256)b_3^8+1536b_3^8b_3^4-256b_3^8)b_1^8+$$
$$(1024b_3^6b_2^{10}+(1024b_3^{10}+2560b_3^6-512b_3^2)b_2^6-(512b_3^6-64b_3^2)b_2^2)b_1^6-$$
$$(1536b_3^8b_2^8+(-416b_3^4+32)b_2^4+32b_3^4)b_1^4-$$
$$((512b_3^6-64b_3^2)b_2^6-64b_3^6b_2^2)b_1^2+256b_3^8b_2^8-32b_3^4b_2^4+1.$$

- One coefficient of the denominator for $\Phi_{1,5}$ is 11805916207174113034240.

Evaluation-interpolation for modular polynomials [Mil14]

- Fix the values of $j_1(\Omega), j_2(\Omega), j_3(\Omega)$ in a tridimensional grid;
- Compute the period matrix $\Omega\in\mathfrak{H}_2$;
- Evaluate the Igusa invariants of the $\ell^3+\ell^2+\ell+1$ ℓ-isogenous curves:

$$\{(j_1(\ell\gamma\Omega), j_2(\ell\Omega), j_3(\ell\gamma\Omega)) \mid \gamma\in\Gamma/\Gamma_0(\ell)\}$$

- Compute $\Phi_{1,\ell}(j_1(\Omega), j_2(\Omega), j_3(\Omega), Y_1)=\prod_{\gamma\in\Gamma/\Gamma_0(\ell)}(Y_1-j_1(\ell\gamma\Omega))$ (product tree);
- $\Phi_{1,\ell}=Y_1^{\ell^3+\ell^2+\ell+1}+\sum_{i=0}^{\ell^3+\ell^2+\ell}c_i(\Omega)Y_1^i$ where the $c_i(\Omega)$ are Siegel modular functions, so are rational functions in $j_i(\Omega)$.
- Interpolate $c_i(\Omega)=Q_i(j_1(\Omega), j_2(\Omega), j_3(\Omega))$, $\quad Q_i\in\mathbb{Q}(X_1,X_2,X_3)$;
- Recover $\Phi_{1,\ell}(X_1,X_2,X_3,Y_1)$. Similarly for $\Psi_{2,\ell},\Psi_{3,\ell}$.
- Needs high precision, so a quasi-linear method to evaluate the period matrix and Igusa invariants.
- Difficulty: denominator simplifications during evaluations.

Non principal polarisations and cyclic isogenies

- If $f:(A,H_1)\to(B,H_2)$ is a cyclic isogeny between principally polarised abelian varieties, then $\operatorname{Ker} f$ is not maximal isotropic in $A[\ell]$ and f^*H_2 is not of the form ℓH_1;

Theorem ([Dudeanu-Jetchev-R.-Vuille])

$f:(A,H_1)\to(B,H_2)$ is a cyclic isogeny of degree ℓ iff there exists $\beta\in\operatorname{End}(A)^s$ a totally positive real (under the Rosati involution) element of norm ℓ of the endomorphism algebra of A and $\operatorname{Ker} f\subset A[\beta]$ is isotropic for the β-pairing e_β.

- Abelian surface with maximal real multiplication by a real quadratic field K_0: $A_\tau := \mathbb{C}^2/(O_{K_0}\oplus O_{K_0}^\vee\tau)$ where $\tau\in\mathfrak{H}_1^2$ (and K_0 is embedded into $\mathbb{C}^2$ via $K_0\otimes_{\mathbb{Q}}\mathbb{R}=\mathbb{R}^2\subset\mathbb{C}^2$);
- Moduli space: Hilbert surface $\mathfrak{H}_1^2/\mathrm{Sl}_2(O_{K_0}\oplus O_{K_0}^\vee)$.
- Forgetting $O_{K_0}\simeq\operatorname{End}(A_\tau)$ ⇒ degree 2 cover of the Humbert surface $H_{\Delta_{K_0}}$ of discriminant Δ_{K_0} in $\mathfrak{H}_2$.

Cyclic modular polynomials in dimension 2 [Milio-R.]

- $\beta\in O_{K_0}^{++}$ ⇒ β-modular polynomial Φ_β in terms of symmetric invariants of the Hilbert space $\mathfrak{H}_1^2/(\mathrm{Sl}_2(O_{K_0}\oplus O_{K_0}^\vee)\rtimes\mathrm{Sl}_2(O_{K_0}\oplus O_{K_0}^\vee)^\sigma)$;
- $N_{K_0/\mathbb{Q}}(\beta)=\ell$ ⇒ Φ_β classify the $\ell+1$ cyclic β-isogenies.
- Evaluation-interpolation approach via the action of $\mathrm{Sl}_2(O_{K_0}\oplus O_{K_0}^\vee)/\Gamma_0(\beta)$;
- Explicit back and forth between Siegel point of view and Hilbert point of view.
- Difficulty: the embedding of $\mathrm{Sl}_2(O_{K_0}\oplus O_{K_0}^\vee)$ into $\mathrm{Sp}_4(\mathbb{Z})$ is not surjective.

- If $D=2$ or $D=5$ the symmetric Hilbert moduli space is (uni-)rational and parameterized (generically) by two invariants: the Gundlach invariants;
- For general D the Hilbert space is not (uni-)rational ⇒ need to interpolate three invariants (the pullback of three Siegel invariants);
- Difficulty: Algebraic relation between the invariants we interpolate ⇒ normalise the evaluated modular polynomials by fixing a Gröbner basis.

Example of cyclic modular polynomials in dimension 2 [Milio-R.]

ℓ ($D=2$)	Size (Gundlach)	Theta	ℓ ($D=5$)	Size (Gundlach)	Theta
2	8.5KB		5	22KB	26KB
7	172KB		11	3.5MB	308KB
17	5.8MB	221KB	19	33MB	3.6MB
23	21 MB		29	188MB	21MB
31	70 MB		31	248 MB	28MB
41	225 MB	7.2MB	41	785MB	115MB
47	400 MB		59	3.6GB	470MB
71	2.2 GB				
73		81MB			
89		188MB			
97		269MB			

Examples
- For $D=2$, $\beta=5+2\sqrt{2}$ | 17, using b_1, b_2, b_3 pullback of level 2 theta functions on the Hilbert space, the denominator of $\Phi_{1,\beta}$ is

$$b_1^8b_2^{18}+(6b_3^86b_3^4+1)b_2^{16}+(15b_3^{16}24b_3^8+7b_3^2)b_2^{14}+(20b_3^{12}42b_3^8+9b_3^4+2)b_2^{12}+$$
$$(15b_3^{14}48b_3^{10}+37b_3^6+4b_3^2)b_2^{10}+(6b_3^{16}42b_3^{12}+68b_3^826b_3^4+3)b_2^8+$$

The denominators of cyclic modular polynomials

- Denominator of Φ_β = abelian surfaces with real multiplication β-isogenous to a product of elliptic curves.

⇒ Abelian surface in this locus: non commutative endomorphism ring ⇒ m-isogenous to product of elliptic curves for an infinite number of $m\in\mathbb{Z}$;

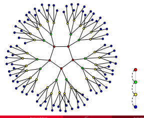
- irreducible components of this modular locus = curves which lie on an infinite number of Humbert surfaces of square discriminant m^2;
- Values m = values primitively represented by a certain quadratic form q [Kan16], [Milio-R.].
- Moduli: $H(q)$, a generalised Humbert variety.

Example

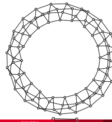
For $D=2$, $\beta=5+2\sqrt{2}$ | 17, the denominator of $\Phi_{1,\beta}$ has for irreducible component $H(8x^2+4xy+9y^2)=J_1^7J_2^6J_3^6J_2^4+J_3^6J_2+\dots$ which lie in

$$H_8\cap H_{32}\cap H_{72}\cap H_{152}\cap H_{200}\cap H_{212}\cap\dots$$

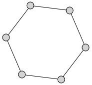
A 3-isogeny graph in dimension 1 [Koh96; FM02]



Horizontal isogeny graphs: $\ell=q_1q_2=Q_1\overline{Q_1}Q_2\overline{Q_2}$ $\quad(\mathbb{Q}\mapsto K_0\mapsto K)$

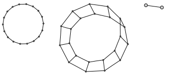


Horizontal isogeny graphs: $\ell=q=Q\overline{Q}$ $\quad(\mathbb{Q}\mapsto K_0\mapsto K)$

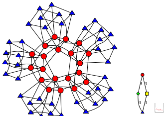


Horizontal isogeny graphs: ramified cases $\quad(\mathbb{Q}\mapsto K_0\mapsto K)$

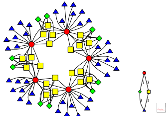
$\ell=q_1q_2=Q_1\overline{Q_1}Q_2^2$ $\qquad \ell=q^2=Q^2\overline{Q}^2$ $\qquad \ell=q^2=Q^4$



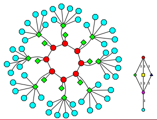
Isogeny graphs in dimension 2 ($\ell=q_1q_2=Q_1\overline{Q_1}Q_2\overline{Q_2}$)



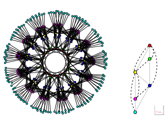
Isogeny graphs in dimension 2 ($\ell=q=Q\overline{Q}$)



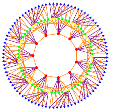
Isogeny graphs in dimension 2 ($\ell=q=Q\overline{Q}$)



Isogeny graphs and lattice of orders [illegible]



Cyclic isogeny graph in dimension 2 [illegible]



β_1 is inert and β_2 is split in K.

Principally polarised abelian varieties over $\mathbb{C}$

Definition

Principally polarised complex abelian variety A of dimension g = compact Lie group V/Λ with

- V: complex vector space of dimension g (linear data);
- Λ: $\mathbb{Z}$-lattice in V (of rank $2g$) (arithmetic data);
- + H: Hermitian form on V | $E(\Lambda,\Lambda) \subset \mathbb{Z}$ where $E := \operatorname{Im} H$ is a principal symplectic form (quadratic data: pairings).

- H : polarisation on A. Conversely, any symplectic form E on V such that $E(\Lambda,\Lambda) \subset \mathbb{Z}$ and $E(ix, iy) = E(x,y)$ for all $x, y \in V$ gives a polarisation H with $E = \operatorname{Im} H$.

$\Rightarrow$ Algebraic coordinates.

- Principal polarisation: over a symplectic basis of Λ, E is of the form $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
- Moduli space of principally polarised abelian varieties: $\mathfrak{H}_g / \mathrm{Sp}_{2g}(\mathbb{Z})$ of dimension $g(g+1)/2$.
- $\Lambda = \Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$, $H = (\mathfrak{I}\Omega)^{-1}$.

Isogenies

Definition

$A := V/\Lambda, B := V'/\Lambda'$ abelian varieties.

- Isogeny: $f : A \to B$ bijective linear map $f : V \to V' \mid f(\Lambda) \subset \Lambda'$.
- Kernel: $f^{-1}(\Lambda')/\Lambda \subset A$, degree $\deg f := \# K$.
- $f : (A, H_1) \to (B, H_2)$ = ℓ-isogeny between principally polarised abelian varieties if

$$f^* H_2 = \ell H_1.$$

- Two abelian varieties over a finite field are isogenous iff they have the same zeta function (Tate);

Theorem (Weil, Mumford)

$f \mapsto \operatorname{Ker} f : \{\ell - \textit{isogenies}\} \Leftrightarrow \{\textit{maximally isotropic subgroup of } A[\ell] \textit{ for the Weil pairing}\}$.

Cryptographic applications of isogenies

Transport the DLP

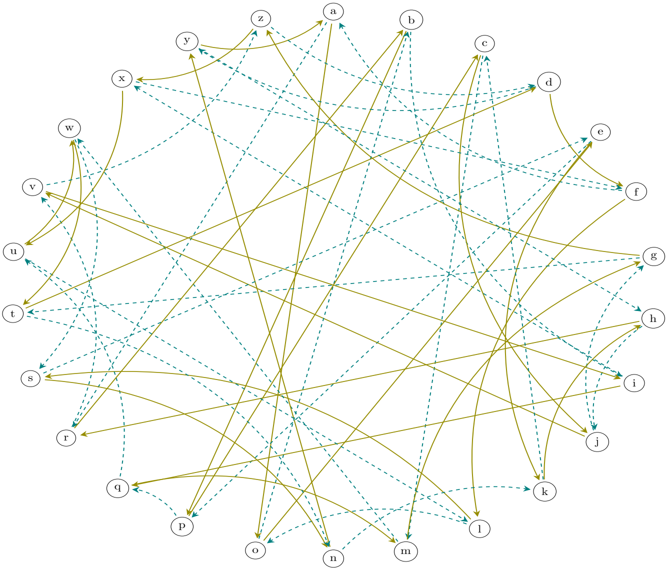
- Extend attacks using Weil descent [GHS02]
- Transfer the DLP from the Jacobian of an hyperelliptic curve of genus 3 to the Jacobian of a quartic curve [Smi09].

Work with smaller data

- SEA point counting algorithm [Sch95; Mor95; Elk97];
- CRT algorithms to compute class polynomials [Sut11; ES10], [Lauter-R.];
- CRT algorithms to compute modular polynomials [BLS12].

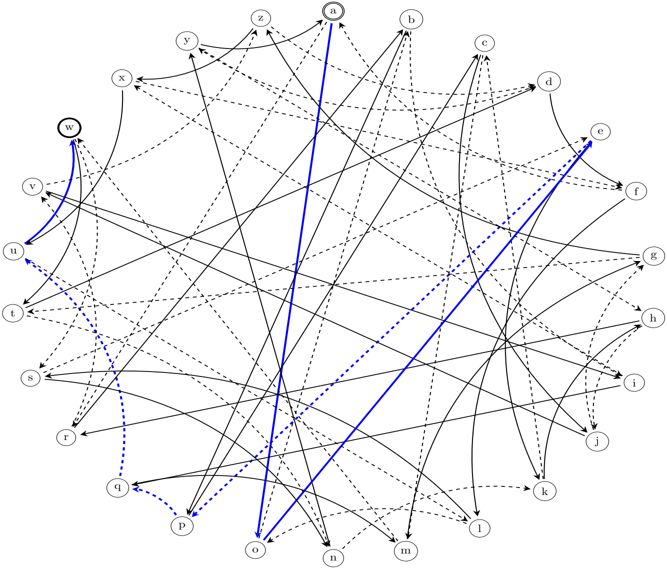
- Splitting the multiplication using isogenies can improve the arithmetic [DIK06; Gau07];
- The isogeny graph of a supersingular elliptic curve can be used to construct secure hash functions [CLG09];
- Construct public key cryptosystems by hiding vulnerable curves by an isogeny (the trapdoor) [Tes06], or by encoding informations in the isogeny graph [RS06];
- Take isogenies to reduce the impact of side channel attacks [Sma03];
- Construct a normal basis of a finite field [CL09];
- Improve the discrete logarithm in $\mathbb{F}_q^*$ by finding a smoothness basis invariant by automorphisms [CL08].
- Construct verifiable delay functions [De +19].

Post-quantum key exchange using isogeny graphs [DJP14]



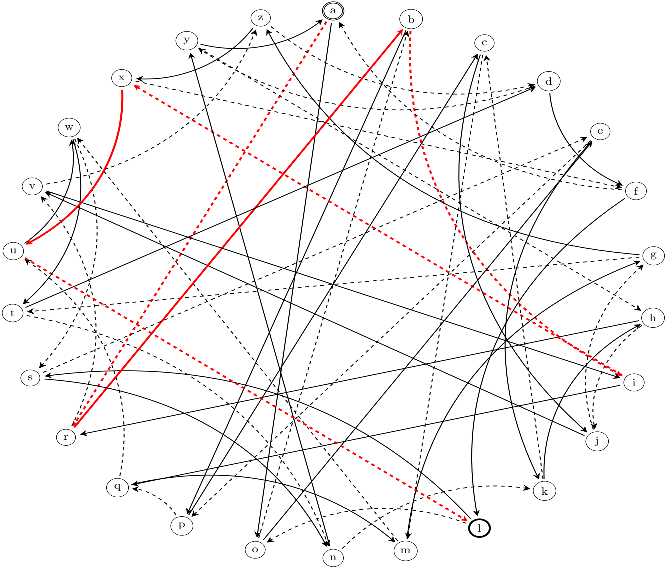
Post-quantum key exchange using isogeny graphs [DJP14]

Alice starts from 'a', follows the path 001110, and get 'w'.



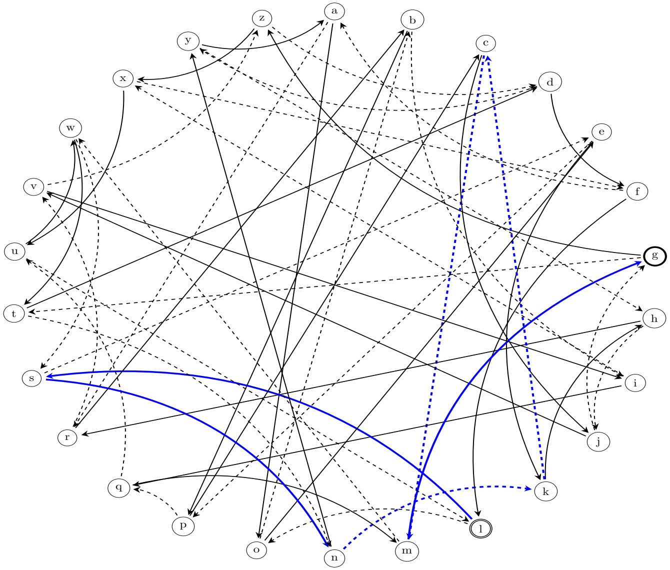
Post-quantum key exchange using isogeny graphs [DJP14]

Bob starts from ’a’, follows the path 101101, and get ‘l’.



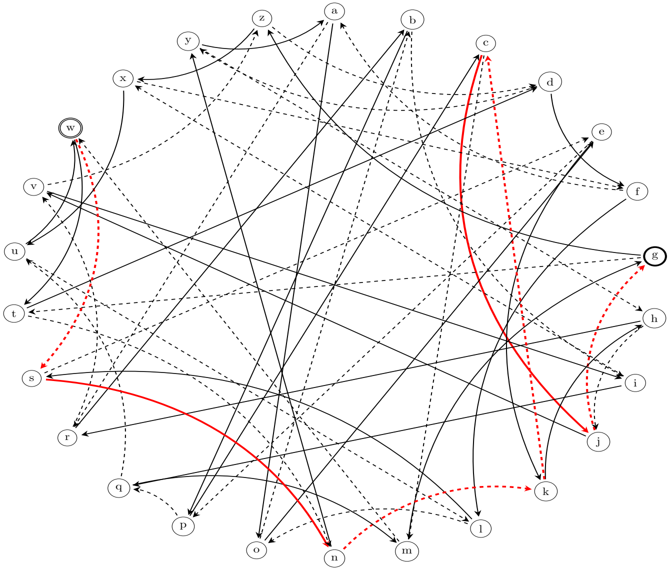
Post-quantum key exchange using isogeny graphs [DJP14]

Alice starts from 'l', follows her path 001110, and get 'g'.



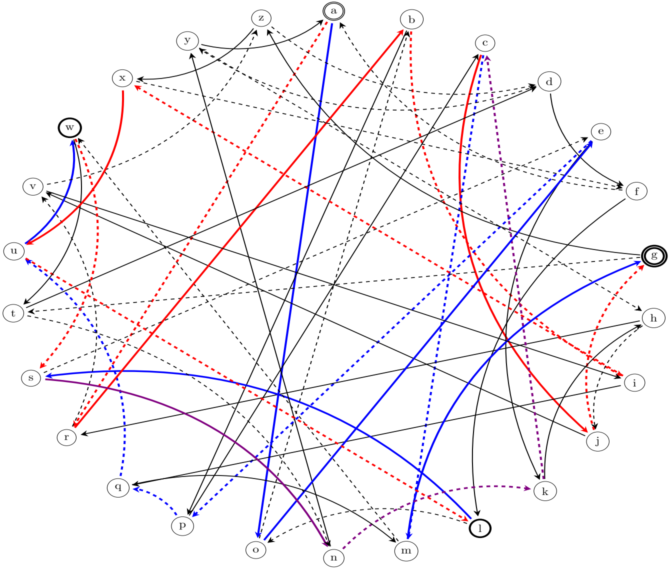
Post-quantum key exchange using isogeny graphs [DJP14]

Bob starts from 'w', follows his path 101101, and get 'g'.



Post-quantum key exchange using isogeny graphs [DJP14]

The full key exchange



Birational invariants for $\mathfrak{H}_2/\operatorname{Sp}_4(\mathbb{Z})$

Definition

- Igusa invariants: Siegel modular functions j_1, j_2, j_3 for $\Gamma := \operatorname{Sp}_4(\mathbb{Z})$

$$j_1 := \frac{h_4 h_6}{h_{10}}, \quad j_2 := \frac{h_4^2 h_{12}}{h_{10}^2}, \quad j_3 := \frac{h_4^5}{h_{10}^2}.$$

where the h_i are modular forms of weight i given by explicit polynomials in terms of theta constants.

- 3 Igusa invariants $\Rightarrow$ birational equivalence between $\mathfrak{H}_2/\Gamma$ and $\mathbb{P}^3_{\mathbb{C}}$;
- Always determine $A \Rightarrow$ need 10 invariants.
- Denominator $h_{10} = 0 \Leftrightarrow A$ =product of elliptic curves.
- $j_{i,\ell}(\Omega) := j_i(\ell\Omega) \Rightarrow B := \mathbb{C}^g/(\ell\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ = abelian surface ℓ-isogeneous to $A := \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$;
- Others ppav ℓ-isogenous to $A \Leftrightarrow$ action of $\Gamma/\Gamma_0(\ell)$ on Ω. Index: $\ell^3 + \ell^2 + \ell + 1$.

Definition

- Igusa invariants: Siegel modular functions j_1, j_2, j_3 for $\Gamma := \operatorname{Sp}_4(\mathbb{Z})$

$$j_1 := \frac{h_4 h_6}{h_{10}}, \quad j_2 := \frac{h_4^2 h_{12}}{h_{10}^2}, \quad j_3 := \frac{h_4^5}{h_{10}^2}.$$

where the h_i are modular forms of weight i given by explicit polynomials in terms of theta constants.

- 3 Igusa invariants $\Rightarrow$ birational equivalence between $\mathfrak{H}_2/\Gamma$ and $\mathbb{P}^3_{\mathbb{C}}$;
- Always determine $A \Rightarrow$ need 10 invariants.
- Denominator $h_{10} = 0 \Leftrightarrow A =$product of elliptic curves.
- $j_{i,\ell}(\Omega) := j_i(\ell\Omega) \Rightarrow B := \mathbb{C}^g/(\ell\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ = abelian surface ℓ-isogeneous to $A := \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$;
- Others ppav ℓ-isogenous to $A \Leftrightarrow$ action of $\Gamma/\Gamma_0(\ell)$ on Ω. Index: $\ell^3 + \ell^2 + \ell + 1$.

Modular polynomials in dimension 2

Definition (Hecke representation of ℓ-modular polynomials)

$$\Phi_{1,\ell}(j_1, j_2, j_3, Y_1) = \prod_{\gamma \in \Gamma/\Gamma_0(\ell)} (Y_1 - j_{1,\ell}^{\gamma}) \qquad j_{i,\ell}(\Omega) = j_i(\ell\Omega)$$

$$\Psi_{i,\ell}(j_1, j_2, j_3, Y_i) = \sum_{\gamma \in \Gamma/\Gamma_0(\ell)} j_{i,\ell}^{\gamma} \prod_{\gamma' \in \Gamma/\Gamma_0(\ell)\setminus\{\gamma\}} (Y_i - j_{1,\ell}^{\gamma'}) \quad (i = 2, 3)$$

$$\Phi_\ell := \{\Phi_{1,\ell}(X_1, X_2, X_3, Y_1), Y_i \Phi'_{i,\ell}(X_1, X_2, X_3, Y_1) - \Psi_{i,\ell}(X_1, X_2, X_3, Y_i)\} \in \mathbb{Q}(X_1, X_2, X_3)[Y_1, Y_2, Y_3]^3.$$

- $\Phi_l(j_A, j_B) = 0$ iff B is ℓ-isogenous to A;
- Computed via a multidimensional evaluation–interpolation approach (need to compute period matrices);

⇒ Evaluation of the modular invariants on Ω at high precision;

⇒ Generalized version of the AGM to compute theta functions in quasi-linear time in the precision [Dup06];

⇒ Need to interpolate rational functions;

- Denominator = the Humbert surface H_{ℓ^2} of discriminant ℓ^2 [BL09; Gru10]= abelian surfaces ℓ-isogenous to products of elliptic curves;
- Quasi-linear algorithm [Dup06; Mil14];
- Can be generalized to smaller modular invariants [Mil14].

Example of modular polynomials in dimension 2 [Mil14]

Invariant	ℓ	Size
Igusa	2	57 MB
Streng	2	2.1 MB
Streng	3	890 MB
Theta	3	175 KB
Theta	5	200 MB
Theta	7	29 GB

Examples

- The denominator of $\Phi_{1,3}$ for modular functions b_1, b_2, b_3 derived from theta constants of level 2 is:

$$1024 b_3^6 b_2^6 b_1^{10} - ((768 b_3^8 + 1536 b_3^4 - 256) b_3^8 + 1536 b_3^8 b_3^4 - 256 b_3^8) b_1^8 + \\ (1024 b_3^6 b_2^{10} + (1024 b_3^{10} + 2560 b_3^6 - 512 b_3^2) b_2^6 - (512 b_3^6 - 64 b_3^2) b_2^2) b_1^6 - \\ (1536 b_3^8 b_2^8 + (-416 b_3^4 + 32) b_2^4 + 32 b_3^4) b_1^4 - \\ ((512 b_3^6 - 64 b_3^2) b_2^6 - 64 b_3^6 b_2^2) b_1^2 + 256 b_3^8 b_2^8 - 32 b_3^4 b_2^4 + 1.$$

- One coefficient of the denominator for $\Phi_{1,5}$ is 11805916207174113034240.

Evaluation-interpolation for modular polynomials [Mil14]

- Fix the values of $j_1(\Omega), j_2(\Omega), j_3(\Omega)$ in a tridimensional grid;
- Compute the period matrix $\Omega \in \mathfrak{H}_2$;
- Evaluate the Igusa invariants of the $\ell^3+\ell^2+\ell+1$ ℓ-isogenous curves:

$$\left\{\left(j_1(\ell\gamma\Omega), j_2(\ell\Omega), j_3(\ell\gamma\Omega)\right) \mid \gamma \in \Gamma/\Gamma_0(\ell)\right\}$$

- Compute $\Phi_{1,\ell}(j_1(\Omega), j_2(\Omega), j_3(\Omega), Y_1) = \prod_{\gamma\in\Gamma/\Gamma_0(\ell)}(Y_1 - j_1(\ell\gamma\Omega))$ (product tree);
- $\Phi_{1,\ell} = Y_1^{\ell^3+\ell^2+\ell+1} + \sum_{i=0}^{\ell^3+\ell^2+\ell} c_i(\Omega) Y_1^i$ where the $c_i(\Omega)$ are Siegel modular functions, so are rational functions in $j_i(\Omega)$.
- Interpolate $c_i(\Omega) = Q_i(j_1(\Omega), j_2(\Omega), j_3(\Omega)), \quad Q_i \in \mathbb{Q}(X_1, X_2, X_3)$;
- Recover $\Phi_{1,\ell}(X_1, X_2, X_3, Y_1)$. Similarly for $\Psi_{2,\ell}, \Psi_{3,\ell}$.

- Needs high precision, so a quasi-linear method to evaluate the period matrix and Igusa invariants.
- Difficulty: denominator simplifications during evaluations.

Non principal polarisations and cyclic isogenies

- If $f:(A,H_1)\rightarrow(B,H_2)$ is a cyclic isogeny between principally polarised abelian varieties, then $\operatorname{Ker} f$ is not maximal isotropic in $A[\ell]$ and f^*H_2 is not of the form ℓH_1;

Theorem ([Dudeanu-Jetchev-R.-Vuille])

$f:(A,H_1)\rightarrow(B,H_2)$ is a cyclic isogeny of degree ℓ iff there exists $\beta\in\operatorname{End}(A)^s$ a totally positive real (under the Rosati involution) element of norm ℓ of the endomorphism algebra of A and $\operatorname{Ker} f\subset A[\beta]$ is isotropic for the β-pairing e_β.

- Abelian surface with maximal real multiplication by a real quadratic field K_0: $A_\tau:=\mathbb{C}^2/(O_{K_0}\oplus O_{K_0}^\vee\tau)$ where $\tau\in\mathfrak{H}_1^2$ (and K_0 is embedded into $\mathbb{C}^2$ via $K_0\otimes_{\mathbb{Q}}\mathbb{R}=\mathbb{R}^2\subset\mathbb{C}^2$);
- Moduli space: Hilbert surface $\mathfrak{H}_1^2/\mathrm{Sl}_2(O_{K_0}\oplus O_{K_0}^\vee)$.
- Forgetting $O_{K_0}\simeq\operatorname{End}(A_\tau)\Rightarrow$ degree 2 cover of the Humbert surface $H_{\Delta_{K_0}}$ of discriminant Δ_{K_0} in $\mathfrak{H}_2$.

Non principal polarisations and cyclic isogenies

- If $f:(A,H_1)\to(B,H_2)$ is a cyclic isogeny between principally polarised abelian varieties, then $\operatorname{Ker} f$ is not maximal isotropic in $A[\ell]$ and f^*H_2 is not of the form ℓH_1;

Theorem ([Dudeanu-Jetchev-R.-Vuille])

$f:(A,H_1)\to(B,H_2)$ is a cyclic isogeny of degree ℓ iff there exists $\beta\in\operatorname{End}(A)^s$ a totally positive real (under the Rosati involution) element of norm ℓ of the endomorphism algebra of A and $\operatorname{Ker} f\subset A[\beta]$ is isotropic for the β-pairing e_β.

- Abelian surface with maximal real multiplication by a real quadratic field K_0: $A_\tau := \mathbb{C}^2/(O_{K_0}\oplus O_{K_0}^\vee\tau)$ where $\tau\in\mathfrak{H}_1^2$ (and K_0 is embedded into $\mathbb{C}^2$ via $K_0\otimes_{\mathbb{Q}}\mathbb{R}=\mathbb{R}^2\subset\mathbb{C}^2$);
- Moduli space: Hilbert surface $\mathfrak{H}_1^2/\mathrm{Sl}_2(O_{K_0}\oplus O_{K_0}^\vee)$.
- Forgetting $O_{K_0}\simeq\operatorname{End}(A_\tau)\Rightarrow$ degree 2 cover of the Humbert surface $H_{\Delta_{K_0}}$ of discriminant Δ_{K_0} in $\mathfrak{H}_2$.

Non principal polarisations and cyclic isogenies

- If $f:(A,H_1)\rightarrow(B,H_2)$ is a cyclic isogeny between principally polarised abelian varieties, then $\operatorname{Ker} f$ is not maximal isotropic in $A[\ell]$ and $f^* H_2$ is not of the form ℓH_1;

Theorem ([Dudeanu-Jetchev-R.-Vuille])

$f:(A,H_1)\rightarrow(B,H_2)$ is a cyclic isogeny of degree ℓ iff there exists $\beta\in\operatorname{End}(A)^s$ a totally positive real (under the Rosati involution) element of norm ℓ of the endomorphism algebra of A and $\operatorname{Ker} f\subset A[\beta]$ is isotropic for the β-pairing e_β.

- Abelian surface with maximal real multiplication by a real quadratic field K_0: $A_\tau := \mathbb{C}^2/(O_{K_0}\oplus O_{K_0}^\vee\tau)$ where $\tau\in\mathfrak{H}_1^2$ (and K_0 is embedded into $\mathbb{C}^2$ via $K_0\otimes_{\mathbb{Q}}\mathbb{R}=\mathbb{R}^2\subset\mathbb{C}^2$);
- Moduli space: Hilbert surface $\mathfrak{H}_1^2/\mathrm{Sl}_2(O_{K_0}\oplus O_{K_0}^\vee)$.
- Forgetting $O_{K_0}\simeq\operatorname{End}(A_\tau)\Rightarrow$ degree 2 cover of the Humbert surface $H_{\Delta_{K_0}}$ of discriminant Δ_{K_0} in $\mathfrak{H}_2$.

Cyclic modular polynomials in dimension 2 [Milio-R.]

- $\beta \in O_{K_0}^{++} \Rightarrow \beta$-modular polynomial Φ_β in terms of symmetric invariants of the Hilbert space $\mathfrak{H}_1^2/(\mathrm{Sl}_2(O_{K_0} \oplus O_{K_0}^\vee) \oplus \mathrm{Sl}_2(O_{K_0} \oplus O_{K_0}^\vee)^\sigma)$;
- $N_{K_0/\mathbb{Q}}(\beta) = \ell \Rightarrow \Phi_\beta$ classify the $\ell + 1$ cyclic β-isogenies.
- Evaluation–interpolation approach via the action of $\mathrm{Sl}_2(O_{K_0} \oplus O_{K_0}^\vee)/\Gamma_0(\beta)$;
- Explicit back and forth between Siegel point of view and Hilbert point of view.
- Difficulty: the embedding of $\mathrm{Sl}_2(O_{K_0} \oplus O_{K_0}^\vee)$ into $\mathrm{Sp}_4(\mathbb{Z})$ is not surjective.

- If $D = 2$ or $D = 5$ the symmetric Hilbert moduli space is (uni-)rational and parameterized (generically) by two invariants: the Gundlach invariants;
- For general D the Hilbert space is not (uni-)rational $\Rightarrow$ need to interpolate three invariants (the pullback of three Siegel invariants);
- Difficulty: Algebraic relation between the invariants we interpolate $\Rightarrow$ normalise the evaluated modular polynomials by fixing a Gröbner basis.

Cyclic modular polynomials in dimension 2 [Milio-R.]

- $\beta \in O_{K_0}^{++} \Rightarrow \beta$-modular polynomial Φ_β in terms of symmetric invariants of the Hilbert space $\mathfrak{H}_1^2/(\mathrm{Sl}_2(O_{K_0} \oplus O_{K_0}^\vee) \oplus \mathrm{Sl}_2(O_{K_0} \oplus O_{K_0}^\vee)^\sigma)$;
- $N_{K_0/\mathbb{Q}}(\beta) = \ell \Rightarrow \Phi_\beta$ classify the $\ell+1$ cyclic β-isogenies.
- Evaluation–interpolation approach via the action of $\mathrm{Sl}_2(O_{K_0} \oplus O_{K_0}^\vee)/\Gamma_0(\beta)$;
- Explicit back and forth between Siegel point of view and Hilbert point of view.
- Difficulty: the embedding of $\mathrm{Sl}_2(O_{K_0} \oplus O_{K_0}^\vee)$ into $\mathrm{Sp}_4(\mathbb{Z})$ is not surjective.

- If $D=2$ or $D=5$ the symmetric Hilbert moduli space is (uni-)rational and parameterized (generically) by two invariants: the Gundlach invariants;
- For general D the Hilbert space is not (uni-)rational $\Rightarrow$ need to interpolate three invariants (the pullback of three Siegel invariants);
- Difficulty: Algebraic relation between the invariants we interpolate $\Rightarrow$ normalise the evaluated modular polynomials by fixing a Gröbner basis.

Example of cyclic modular polynomials in dimension 2 [Milio-R.]

ℓ $(D=2)$	Size (Gundlach)	Theta	ℓ $(D=5)$	Size (Gundlach)	Theta
2	8.5KB		5	22KB	26KB
7	172KB		11	3.5MB	308KB
17	5.8MB	221KB	19	33MB	3.6MB
23	21 MB		29	188MB	21MB
31	70 MB		31	248 MB	28MB
41	225 MB	7.2MB	41	785MB	115MB
47	400 MB		59	3.6GB	470MB
71	2.2 GB				
73		81MB			
89		188MB			
97		269MB			

Example of cyclic modular polynomials in dimension 2 [Milio-R.]

ℓ $(D=2)$	Size (Gundlach)	Theta	ℓ $(D=5)$	Size (Gundlach)	Theta
2	8.5KB		5	22KB	26KB
7	172KB		11	3.5MB	308KB
17	5.8MB	221KB	19	33MB	3.6MB
23	21 MB		29	188MB	21MB
31	70 MB		31	248 MB	28MB
41	225 MB	7.2MB	41	785MB	115MB

Examples

- For $D=2$, $\beta = 5+2\sqrt{2} \mid 17$, using b_1, b_2, b_3 pullback of level 2 theta functions on the Hilbert space, the denominator of $\Phi_{1,\beta}$ is

$$b_3^6 b_2^{18} + (6 b_3^8 6 b_3^4 + 1) b_2^{16} + (15 b_3^{10} 24 b_3^6 + 7 b_3^2) b_2^{14} + (20 b_3^{12} 42 b_3^8 + 9 b_3^4 + 2) b_2^{12} +$$
$$(15 b_3^{14} 48 b_3^{10} + 37 b_3^6 + 4 b_3^2) b_2^{10} + (6 b_3^{16} 42 b_3^{12} + 68 b_3^8 26 b_3^4 + 3) b_2^8 +$$
$$(b_3^{18} 24 b_3^{14} + 37 b_3^{10} + 8 b_3^6 b_3^2) b_2^6 + (6 b_3^{16} + 9 b_3^{12} 26 b_3^8 24 b_3^4 + 2) b_2^4 +$$
$$(7 b_3^{14} + 4 b_3^{10} b_3^6) b_2^2 + (b_3^{16} + 2 b_3^{12} + 3 b_3^8 + 2 b_3^4 + 1).$$

- For $\beta \mid 97$, one coefficient of the denominator of $\Phi_{1,\beta}$ is 50853993476624629 2.

- Denominator of Φ_β = abelian surfaces with real multiplication β-isogenous to a product of elliptic curves.

$\Rightarrow$ Abelian surface in this locus: non commutative endomorphism ring $\Rightarrow$ m-isogenous to product of elliptic curves for an infinite number of $m \in \mathbb{Z}$;

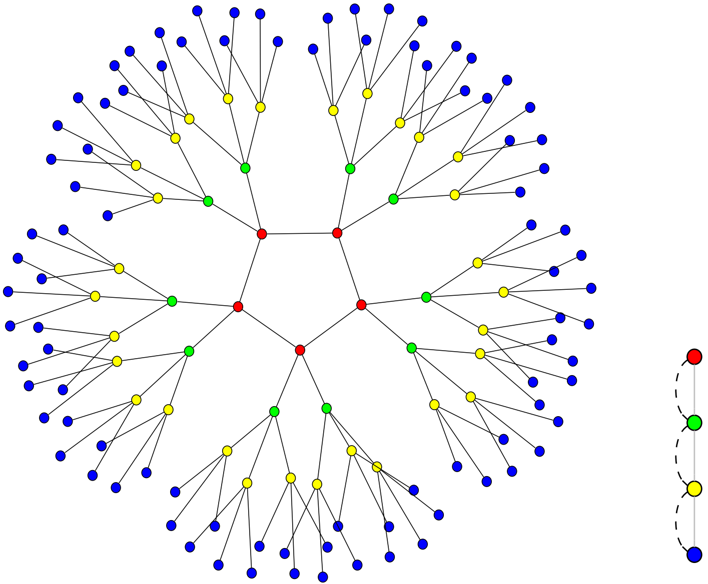
- Irreducible components of this modular locus = curves which lie on an infinite number of Humbert surfaces of square discriminant m^2;
- Values m = values primitively represented by a certain quadratic form q [Kan16], [Milio-R.].
- Moduli: $H(q)$, a generalised Humbert variety.

Example

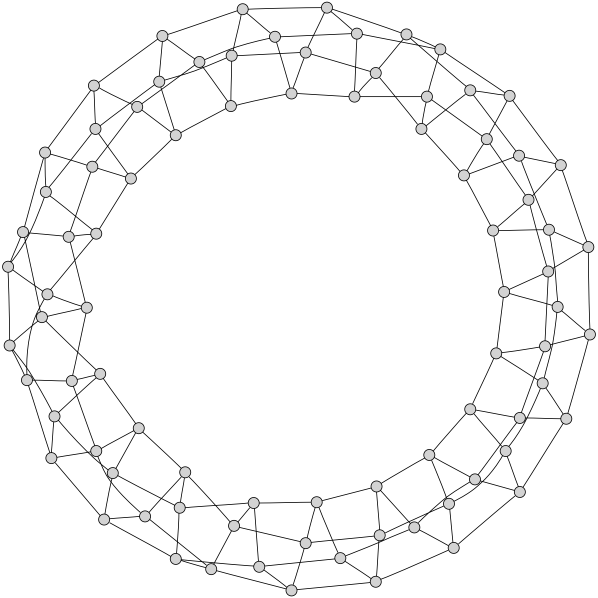
For $D=2$, $\beta=5+2\sqrt{2} \mid 17$, the denominator of $\Phi_{1,\beta}$ has for irreducible component $H(8x^2+4xy+9y^2)=J_1^7 J_1^6 J_2^3 6 J_1^6 J_2^2 + J_1^6 J_2 + \ldots$ which lie in

$$H_8 \cap H_{3^2} \cap H_{7^2} \cap H_{11^2} \cap H_{23^2} \cap H_{31^2} \ldots.$$

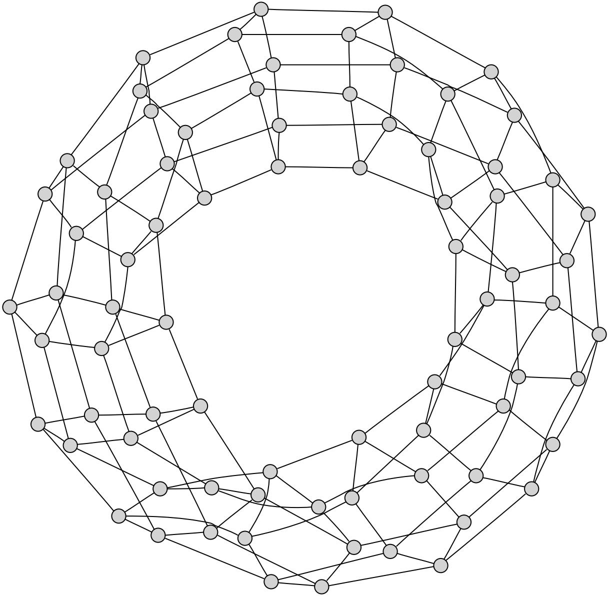
A 3-isogeny graph in dimension 1 [Koh96; FM02]

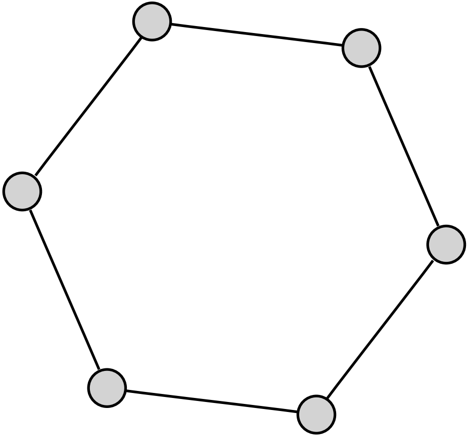


Horizontal isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q_2}$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



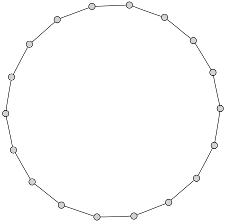
Horizontal isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q}_2$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



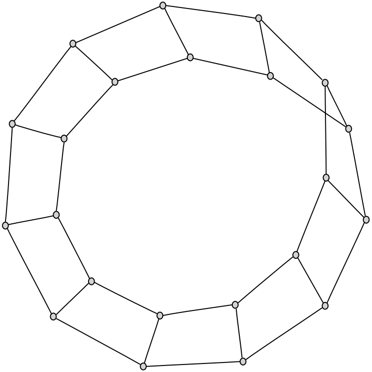


Horizontal isogeny graphs: ramified cases $(\mathbb{Q} \mapsto K_0 \mapsto K)$

$\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2^2$

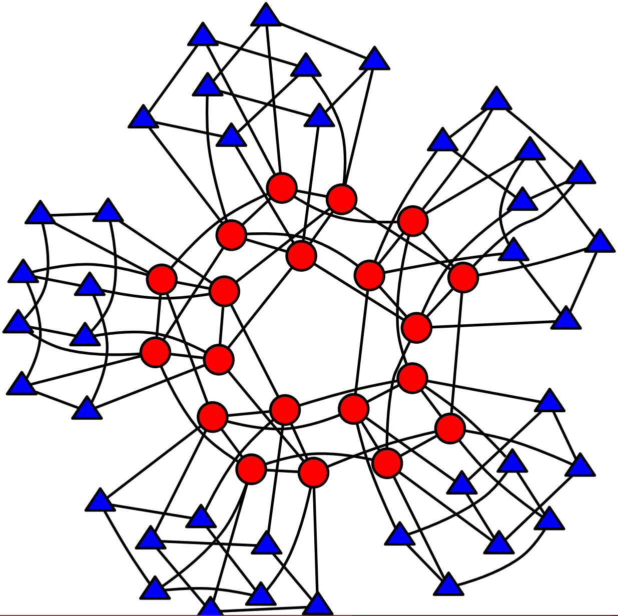


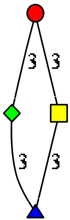
$\ell = q^2 = Q^2 \overline{Q}^2$



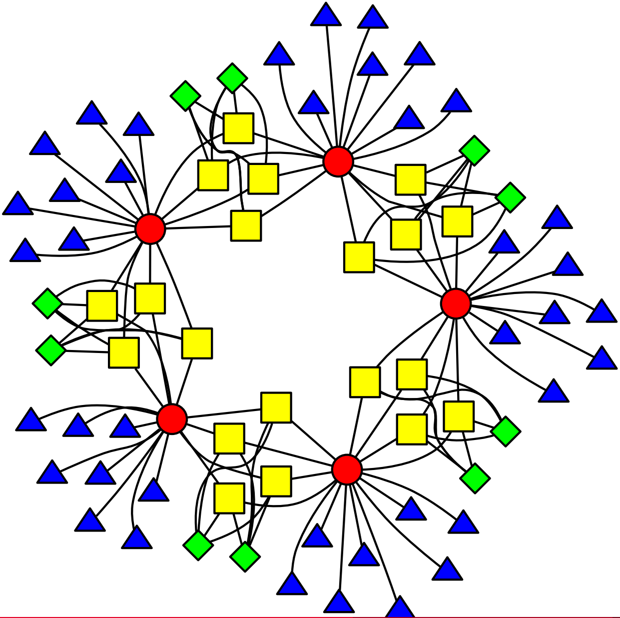
$\ell = q^2 = Q^4$

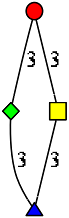
Isogeny graphs in dimension 2 ($\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q_2}$)

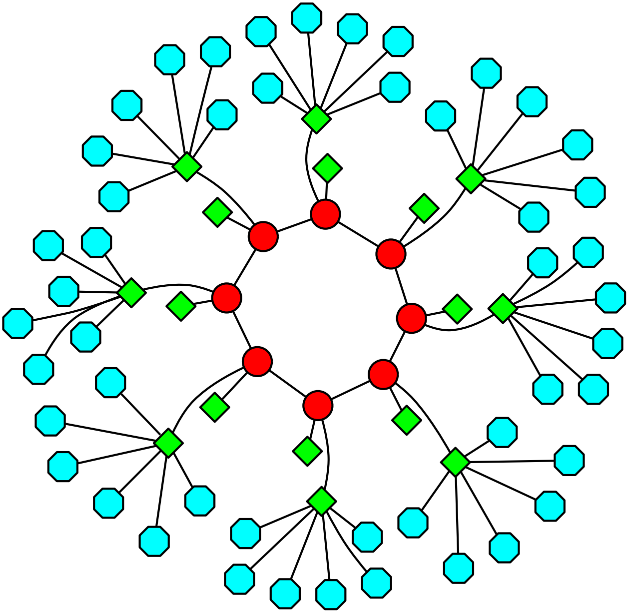


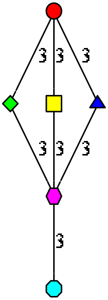


Isogeny graphs in dimension 2 ($\ell = q = Q\overline{Q}$)

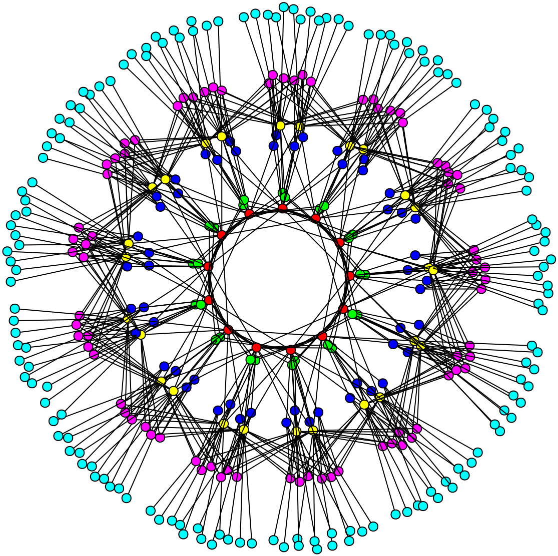


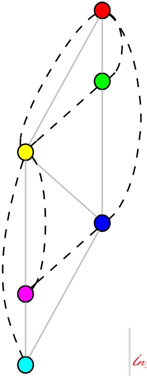




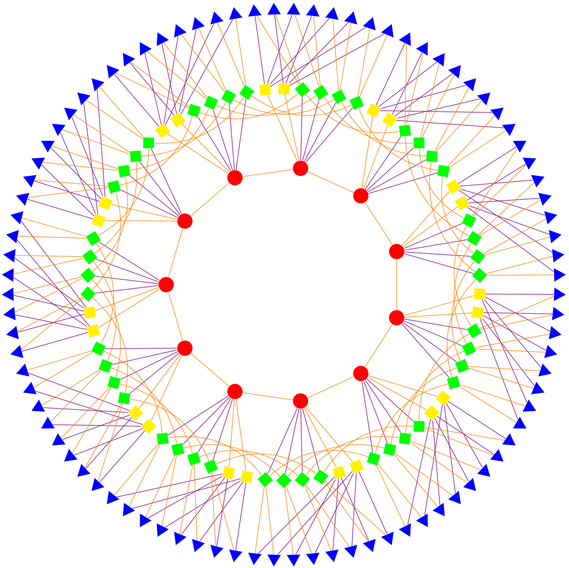

3
3
3
3
3
3
3

Isogeny graphs and lattice of orders [Bisson, Cosset, R.]

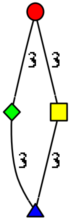




Cyclic isogeny graph in dimension 2 [IT14]



β_1 is inert and β_2 is split in K.



Bibliography

R. Bröker and K. Lauter. "Modular polynomials for genus 2". In: *LMS J. Comput. Math.* 12 (2009), pp. 326–339. ISSN: 1461-1570. arXiv: 0804.1565 (cit. on p. 14).

R. Bröker, K. Lauter, and A. Sutherland. "Modular polynomials via isogeny volcanoes". In: *Mathematics of Computation* 81.278 (2012), pp. 1201–1231. arXiv: 1001.0402 (cit. on p. 5).

D. Charles, K. Lauter, and E. Goren. "Cryptographic hash functions from expander graphs". In: *Journal of Cryptology* 22.1 (2009), pp. 93–113. ISSN: 0933-2790 (cit. on p. 5).

R. Cosset and D. Robert. "An algorithm for computing (ℓ,ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2". In: *Mathematics of Computation* 84.294 (Nov. 2015), pp. 1953–1975. DOI: 10.1090/S0025-5718-2014-02899-8. URL: http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. HAL: hal-00578991, eprint: 2011/143.

J. Couveignes and R. Lercier. "Galois invariant smoothness basis". In: *Algebraic geometry and its applications* (2008) (cit. on p. 5).

J. Couveignes and R. Lercier. "Elliptic periods for finite fields". In: *Finite fields and their applications* 15.1 (2009), pp. 1–22 (cit. on p. 5).

L. De Feo, D. Jao, and J. Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247 (cit. on pp. 6–11).

L. De Feo, S. Masson, C. Petit, and A. Sanso. "Verifiable Delay Functions from Supersingular Isogenies and Pairings". 2019. URL: https://eprint.iacr.org/2019/166.pdf (cit. on p. 5).

C. Doche, T. Icart, and D. Kohel. "Efficient scalar multiplication by isogeny decompositions". In: *Public Key Cryptography-PKC 2006* (2006), pp. 191–206 (cit. on p. 5).

A. Dudeanu, jetchev, D. Robert, and M. Vuille. "Cyclic Isogenies for Abelian Varieties with Real Multiplication". Oct. 2017. HAL: hal-01629829.

R. Dupont. "Moyenne arithmetico-geometrique, suites de Borchardt et applications". In: *These de doctorat, Ecole polytechnique, Palaiseau* (2006) (cit. on p. 14).

N. Elkies. "Elliptic and modular curves over finite fields and related computational issues". In: *Computational perspectives on number theory: proceedings of a conference in honor of AOL Atkin, September 1995, University of Illinois at Chicago*. Vol. 7. Amer Mathematical Society. 1997, p. 21 (cit. on p. 5).

A. Enge and A. Sutherland. "Class invariants by the CRT method, ANTS IX: Proceedings of the Algorithmic Number Theory 9th International Symposium". In: *Lecture Notes in Computer Science* 6197 (July 2010), pp. 142–156 (cit. on p. 5).

M. Fouquet and F. Morain. "Isogeny volcanoes and the SEA algorithm". In: *Algorithmic Number Theory* (2002), pp. 47–62 (cit. on p. 25).

S. Galbraith, F. Hess, and N. Smart. "Extending the GHS Weil descent attack". In: *Advances in Cryptology—EUROCRYPT 2002*. Springer. 2002, pp. 29–44 (cit. on p. 5).

P. Gaudry. "Fast genus 2 arithmetic based on Theta functions". In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on p. 5).

D. Gruenewald. "Computing Humbert surfaces and applications". In: *Arithmetic, Geometry, Cryptography and Codint Theory 2009* (2010), pp. 59–69 (cit. on p. 14).

S. Ionica, C. Martindale, D. Robert, and M. Streng. "Isogeny graphs of ordinary abelian surfaces over a finite field". Mar. 2014. In preparation.

S. Ionica and E. Thomé. "Isogeny graphs with maximal real multiplication.". In: *IACR Cryptology ePrint Archive* 2014 (2014), p. 230 (cit. on p. 34).

E. Kani. "The moduli spaces of Jacobians isomorphic to a product of two elliptic curves". In: *Collectanea mathematica* 67.1 (2016), pp. 21–54 (cit. on p. 24).

D. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, 1996 (cit. on p. 25).

K. E. Lauter and D. Robert. "Improved CRT Algorithm for Class Polynomials in Genus 2". In: *ANTS X — Proceedings of the Tenth Algorithmic Number Theory Symposium*. Ed. by E. W. Howe and K. S. Kedlaya. Vol. 1. The Open Book Series. Berkeley: Mathematical Sciences Publisher, Nov. 2013, pp. 437–461. DOI: 10.2140/obs.2013.1.437. URL: http://www.normalesup.org/~robert/pro/publications/articles/classCRT.pdf. Slides: 2012-07-ANTS-SanDiego.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-X), July 2012, San Diego, USA), HAL: hal-00734450, eprint: 2012/443.

D. Lubicz and D. Robert. "Computing isogenies between abelian varieties". In: *Compositio Mathematica* 148.5 (Sept. 2012), pp. 1483–1515. DOI: 10.1112/S0010437X12000243. arXiv: 1001.2016 [math.AG]. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf. HAL: hal-00446062.

D. Lubicz and D. Robert. "Computing separable isogenies in quasi-optimal time". In: *LMS Journal of Computation and Mathematics* 18 (1 Feb. 2015), pp. 198–216. DOI: 10.1112/S146115701400045X. arXiv: 1402.3628. URL: http://www.normalesup.org/~robert/pro/publications/articles/rational.pdf. HAL: hal-00954895.

E. Milio. "A quasi-linear algorithm for computing modular polynomials in dimension 2". In: *arXiv preprint arXiv:1411.0409* (2014) (cit. on pp. 14–16).

E. Milio and D. Robert. "Modular polynomials on Hilbert surfaces". Sept. 2017. HAL: hal-01520262.

F. Morain. "Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques". In: *J. Théor. Nombres Bordeaux* 7 (1995), pp. 255–282 (cit. on p. 5).

A. Rostovtsev and A. Stolbunov. “Public-key cryptosystem based on isogenies”. In: *International Association for Cryptologic Research. Cryptology ePrint Archive* (2006). eprint: http://eprint.iacr.org/2006/145 (cit. on p. 5).

R. Schoof. “Counting points on elliptic curves over finite fields”. In: *J. Théor. Nombres Bordeaux* 7.1 (1995), pp. 219–254 (cit. on p. 5).

N. Smart. “An analysis of Goubin’s refined power analysis attack”. In: *Cryptographic Hardware and Embedded Systems-CHES 2003* (2003), pp. 281–290 (cit. on p. 5).

B. Smith. *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*. Feb. 2009. arXiv: 0806.2995 (cit. on p. 5).

A. Sutherland. “Computing Hilbert class polynomials with the Chinese remainder theorem”. In: *Mathematics of Computation* 80.273 (2011), pp. 501–538 (cit. on p. 5).

E. Teske. “An elliptic curve trapdoor system”. In: *Journal of cryptology* 19.1 (2006), pp. 115–133 (cit. on p. 5).