

Genus 2 Isogeny Cryptography

Isogeny-based Cryptography Study Group, Week 10

Robin Visser

Mathematics Institute
University of Warwick

9 December 2022

Elliptic isogeny graph

Let's recap elliptic curve isogeny graphs:

Elliptic curve ℓ -isogeny graph

Let p be prime. Define $\mathcal{G}_1(\ell; p)$ to be the graph whose vertices are isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and whose edges are ℓ -isogenies, for a prime $\ell \neq p$.

Elliptic isogeny graph

Let's recap elliptic curve isogeny graphs:

Elliptic curve ℓ -isogeny graph

Let p be prime. Define $\mathcal{G}_1(\ell; p)$ to be the graph whose vertices are isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and whose edges are ℓ -isogenies, for a prime $\ell \neq p$.

Graph is connected.

Elliptic isogeny graph

Let's recap elliptic curve isogeny graphs:

Elliptic curve ℓ -isogeny graph

Let p be prime. Define $\Gamma_1(\ell; p)$ to be the graph whose vertices are isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and whose edges are ℓ -isogenies, for a prime $\ell \neq p$.

Graph is connected.

Graph has $\frac{p}{12}$ vertices.

Elliptic isogeny graph

Let's recap elliptic curve isogeny graphs:

Elliptic curve ℓ -isogeny graph

Let p be prime. Define $\Gamma_1(\ell; p)$ to be the graph whose vertices are isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and whose edges are ℓ -isogenies, for a prime $\ell \neq p$.

Graph is connected.

Graph has $\frac{p}{12}$ vertices.

Every vertex has $\ell + 1$ neighbours.

Elliptic isogeny graph

Let's recap elliptic curve isogeny graphs:

Elliptic curve ℓ -isogeny graph

Let p be prime. Define $\Gamma_1(\ell; p)$ to be the graph whose vertices are isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and whose edges are ℓ -isogenies, for a prime $\ell \neq p$.

Graph is connected.

Graph has $\frac{p}{12}$ vertices.

Every vertex has $\ell + 1$ neighbours.

Ramanujan. (random walks of length $O(\log p)$ give (near) uniform distribution)

Elliptic isogeny graph

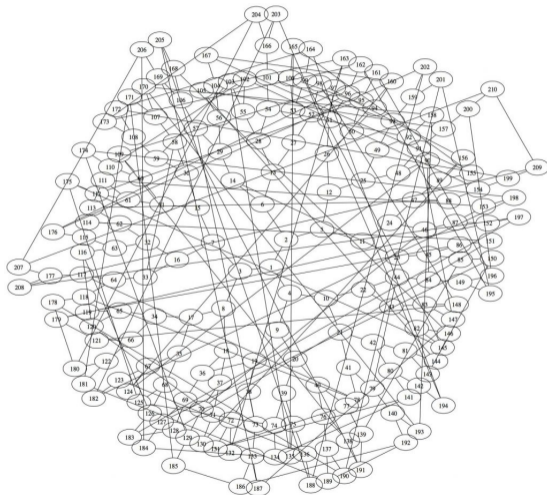


Figure: The 2-isogeny graph for $p = 2521$ (credit to Denis Charles, Microsoft Research).

Elliptic curve SIDH

Public parameters:

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m f$ 1. Let $E = \mathbb{F}_{p^2}$ be supersingular elliptic curve.

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m f - 1$. Let $E = E_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$

1. Let $E = E_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0, 1, \dots, 2^n - 1\}$

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$

1. Let $E = E_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0, 1\}$
2. Calculates $A := aP_1 + P_2 \in E[2^n]$.

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$

1. Let $E = F_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0, 1\}$
2. Calculates $A := hP_1 + [a]P_2 \in E[2^n]$.
3. Sends $(E = A; A(Q_1); A(Q_2))$ to Bob!

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$ 1. Let $E = \mathbb{F}_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $A := hP_1 + [a]P_2 \in E[2^n]$.
3. Sends $(E, A, A(Q_1), A(Q_2))$ to Bob!

Bob

1. Picks random $b \in \mathbb{F}_p \setminus \{0\}$

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$ 1. Let $E = \mathbb{F}_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $A := hP_1 + [a]P_2 \in E[2^n]$.
3. Sends $(E, A, A(Q_1), A(Q_2))$ to Bob!

Bob

1. Picks random $b \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $B := hQ_1 + [b]Q_2 \in E[3^m]$.

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$ 1. Let $E = \mathbb{F}_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $A := hP_1 + [a]P_2 \in E[2^n]$.
3. Sends $(E=A; A(Q_1); A(Q_2))$ to Bob!

Bob

1. Picks random $b \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $B := hQ_1 + [b]Q_2 \in E[3^m]$.
3. Sends $(E=B; B(P_1); B(P_2))$ to Alice!

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$

1. Let $E = \mathbb{F}_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0, 1, \dots, 2^n - 1\}$.
2. Calculates $A := hP_1 + [a]P_2 \in E[2^n]$.
3. Sends $(E=A; A(Q_1); A(Q_2))$ to Bob!
4. Calculates $A^\theta := h B(P_1) + [a] B(P_2) \in E[2^n]$.

Bob

1. Picks random $b \in \mathbb{F}_p \setminus \{0, 1, \dots, 3^m - 1\}$.
2. Calculates $B := hQ_1 + [b]Q_2 \in E[3^m]$.
3. Sends $(E=B; B(P_1); B(P_2))$ to Alice!

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$

1. Let $E = \mathbb{F}_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1; P_2\}$ for $E[2^n]$ and $\{Q_1; Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0, 1, \dots, 2^n - 1\}$.
2. Calculates $A := hP_1 + [a]P_2 \in E[2^n]$.
3. Sends $(E=A; A(Q_1); A(Q_2))$ to Bob!
4. Calculates $A^\theta := h_B(P_1) + [a]_B(P_2) \in E[2^n]$.
5. Computes shared secret key
 $s := j((E=B)=A^\theta)$

Bob

1. Picks random $b \in \mathbb{F}_p \setminus \{0, 1, \dots, 3^m - 1\}$.
2. Calculates $B := hQ_1 + [b]Q_2 \in E[3^m]$.
3. Sends $(E=B; B(P_1); B(P_2))$ to Alice!

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$ 1. Let $E = \mathbb{F}_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1; P_2\}$ for $E[2^n]$ and $\{Q_1; Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $A := hP_1 + [a]P_2 \in E[2^n]$.
3. Sends $(E=A; A(Q_1); A(Q_2))$ to Bob!
4. Calculates $A^\theta := h B(P_1) + [a] B(P_2) \in E[2^n]$.
5. Computes shared secret key
 $s := j((E=B)=A^\theta)$

Bob

1. Picks random $b \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $B := hQ_1 + [b]Q_2 \in E[3^m]$.
3. Sends $(E=B; B(P_1); B(P_2))$ to Alice!
4. Calculates $B^\theta := h A(Q_1) + [b] A(Q_2) \in E[3^m]$.

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$ 1. Let $E = \mathbb{F}_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1; P_2\}$ for $E[2^n]$ and $\{Q_1; Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_{p^2} \setminus \{0\}$
2. Calculates $A := hP_1 + [a]P_2 \in E[2^n]$.
3. Sends $(E=A; A(Q_1); A(Q_2))$ to Bob!
4. Calculates $A^\theta := h B(P_1) + [a] B(P_2) \in E[2^n]$.
5. Computes shared secret key $s := j((E=B)=A^\theta)$

Bob

1. Picks random $b \in \mathbb{F}_{p^2} \setminus \{0\}$
2. Calculates $B := hQ_1 + [b]Q_2 \in E[3^m]$.
3. Sends $(E=B; B(P_1); B(P_2))$ to Alice!
4. Calculates $B^\theta := h A(Q_1) + [b] A(Q_2) \in E[3^m]$.
5. Computes shared secret key $s := j((E=A)=B^\theta)$

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$ 1. Let $E = \mathbb{F}_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1; P_2\}$ for $E[2^n]$ and $\{Q_1; Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $A := hP_1 + [a]P_2 \in E[2^n]$.
3. Sends $(E=A; A(Q_1); A(Q_2))$ to Bob!
4. Calculates $A^\theta := h_B(P_1) + [a]_B(P_2) \in E[2^n]$.
5. Computes shared secret key $s := j((E=B)=A^\theta)$

Bob

1. Picks random $b \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $B := hQ_1 + [b]Q_2 \in E[3^m]$.
3. Sends $(E=B; B(P_1); B(P_2))$ to Alice!
4. Calculates $B^\theta := h_A(Q_1) + [b]_A(Q_2) \in E[3^m]$.
5. Computes shared secret key $s := j((E=A)=B^\theta)$

$$(E=A)=B^\theta = (E=A)=_A(B) = E=h_A; B i = (E=B)=_B(A) = (E=B)=A^\theta$$

Elliptic curve SIDH

Public parameters:

Choose some large prime $p = 2^n 3^m$ 1. Let $E = \mathbb{F}_{p^2}$ be supersingular elliptic curve.
Pick bases $\{P_1; P_2\}$ for $E[2^n]$ and $\{Q_1; Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $A := hP_1 + [a]P_2 \in E[2^n]$.
3. Sends $(E=A; A(Q_1); A(Q_2))$ to Bob!
4. Calculates $A^\theta := h B(P_1) + [a] B(P_2) \in E[2^n]$.
5. Computes shared secret key
 $s := j((E=B)=A^\theta)$

Bob

1. Picks random $b \in \mathbb{F}_p \setminus \{0\}$
2. Calculates $B := hQ_1 + [b]Q_2 \in E[3^m]$.
3. Sends $(E=B; B(P_1); B(P_2))$ to Alice!
4. Calculates $B^\theta := h A(Q_1) + [b] A(Q_2) \in E[3^m]$.
5. Computes shared secret key
 $s := j((E=A)=B^\theta)$

$$(E=A)=B^\theta = (E=A)=_A(B) = E=hA; B i = (E=B)=_B(A) = (E=B)=A^\theta \quad \therefore$$

Abelian varieties recap

Abelian varieties recap

An **abelian variety** is a complete connected algebraic variety $A=K$ with a "group law".

Abelian varieties recap

An **abelian variety** is a complete connected algebraic variety $A=K$ with a "group law".

A genus g **hyperelliptic curve** $C=K$ (for $\text{char}K \neq 2$) has a "normal" model

$$C : y^2 = f(x)$$

where $f(x)$ is squarefree polynomial and $\deg(f) = 2g + 1$ or $2g + 2$.

Abelian varieties recap

An **abelian variety** is a complete connected algebraic variety $A=K$ with a "group law".

A genus g **hyperelliptic curve** $C=K$ (for $\text{char}K \neq 2$) has a "nice" model

$$C : y^2 = f(x)$$

where $f(x)$ is squarefree polynomial and $\deg(f) = 2g + 1$ or $2g + 2$.

Given a genus g curve C , there exists an abelian variety $\text{Jac}(C)$ (the **Jacobian** of C) of dimension g which parameterises $\text{Pic}^0(C)$.

Abelian varieties recap

An **abelian variety** is a complete connected algebraic variety $A=K$ with a "group law".

A genus g **hyperelliptic curve** $C=K$ (for $\text{char}K \neq 2$) has a "nice" model

$$C : y^2 = f(x)$$

where $f(x)$ is squarefree polynomial and $\deg(f) = 2g + 1$ or $2g + 2$.

Given a genus g curve C , there exists an abelian variety $\text{Jac}(C)$ (the **Jacobian** of C) of dimension g which parameterises $\text{Pic}^0(C)$.

Given an abelian variety $A=K$, there exists a **dual** abelian variety $A^*=K$ of the same dimension which parameterises $\text{Pic}^0(A)$.

Abelian varieties recap

A **polarisation** of an abelian variety A/K is an isogeny $\lambda : A \rightarrow A^\vee$ such that $\lambda = \lambda_L (a \vee t_a L \otimes L^{-1})$ for some ample divisor L of A .

Abelian varieties recap

A **polarisation** of an abelian variety $A=K$ is an isogeny $\lambda : A \rightarrow A$ such that $\lambda^* \mathcal{O}_A(1) \cong \mathcal{O}_A(a) \otimes t_a^* \mathcal{O}_A(-1)$ for some ample divisor \mathcal{L} of A .

An abelian variety $A=K$ is **principally polarised** if $\deg(\lambda) = 1$.

Abelian varieties recap

A **polarisation** of an abelian variety $A=K$ is an isogeny $\phi : A \rightarrow A'$ such that $\phi^* \mathcal{O}_{A'}(1) = \mathcal{O}_A(a \sum t_a L - L^{-1})$ for some ample divisor L of A .

An abelian variety $A=K$ is **principally polarised** if $\deg(\phi) = 1$.

Fact: Jacobians are principally polarisable (using theta divisors).

Abelian varieties recap

A **polarisation** of an abelian variety A/K is an isogeny $\lambda : A \rightarrow A^\vee$ such that $\lambda^* \mathcal{O}_A(1) \cong \mathcal{O}_A(a \sum_{i=1}^g t_i L \otimes L^{-1})$ for some ample divisor L of A .

An abelian variety A/K is **principally polarised** if $\deg(\lambda) = 1$.

Fact: Jacobians are principally polarisable (using theta divisors).

A **superspecial** abelian variety A/K over a field K of char p if the trace of Frobenius vanishes (mod p). (equivalently, if A is isomorphic over \bar{K} to a product of supersingular elliptic curves $A = E_1 \times \dots \times E_g$).

Abelian varieties recap

A **polarisation** of an abelian variety A/K is an isogeny $\phi : A \rightarrow A^\vee$ such that $\phi^* \mathcal{O}_{A^\vee}(1) \cong \mathcal{O}_A(a \sum_{i=1}^g L_i^{-1})$ for some ample divisor L of A .

An abelian variety A/K is **principally polarised** if $\deg(\phi) = 1$.

Fact: Jacobians are principally polarisable (using theta divisors).

A **superspecial** abelian variety A/K over a field K of char p if the trace of Frobenius vanishes (mod p). (equivalently, if A is isomorphic over \bar{K} to a product of supersingular elliptic curves $A = E_1 \times \dots \times E_g$).

Let m be coprime to $\text{char}(K)$. The **Weil pairing** for A/K :

$$e_m : A[m](\bar{K}) \times A^\vee[m](\bar{K}) \rightarrow \mu_m(\bar{K})$$

satisfies the following properties:

$$e(P + Q; R) = e(P; R)e(Q; R) \text{ and } e(P; Q + R) = e(P; Q)e(P; R)$$

$$e(P; P) = 1 \text{ and } e(P; Q) = e(Q; P)^{-1}$$

$$e(P; Q) = e(P; Q) \text{ for any } \sigma \in \text{Gal}(\bar{K}/K).$$

Isogenies recap

Given an isogeny $\phi : A \rightarrow A^0$, there exists a **dual isogeny** $\hat{\phi} : \hat{A}^0 \rightarrow \hat{A}$.

Isogenies recap

Given an isogeny $\beta : A \rightarrow A^0$, there exists a **dual isogeny** $\hat{\beta} : \hat{A}^0 \rightarrow \hat{A}$.

Given an isogeny $\beta : A \rightarrow A^0$, there is a canonical isomorphism between $\ker(\beta)$ and $\ker(\hat{\beta})$.

Isogenies recap

Given an isogeny $\beta : A \rightarrow A^0$, there exists a **dual isogeny** $\hat{\beta} : \hat{A}^0 \rightarrow \hat{A}$.

Given an isogeny $\beta : A \rightarrow A^0$, there is a canonical isomorphism between $\ker(\beta)$ and $\ker(\hat{\beta})$.

Given two PPAVs $(A; \beta)$ and $(A^0; \beta^0)$, a **(polarised) isogeny** between PPAVs is an isogeny $\beta : A \rightarrow A^0$ such that $\hat{\beta} \circ \beta^0 = [d]$ for some d .

Isogenies recap

Given an isogeny $\phi : A \rightarrow A^\theta$, there exists a **dual isogeny** $\hat{\phi} : \hat{A}^\theta \rightarrow \hat{A}$.

Given an isogeny $\phi : A \rightarrow A^\theta$, there is a canonical isomorphism between $\ker(\phi)$ and $\ker(\hat{\phi})$.

Given two PPAVs $(A; \phi)$ and $(A^\theta; \phi^\theta)$, a **(polarised) isogeny** between PPAVs is an isogeny $\psi : A \rightarrow A^\theta$ such that $\psi^\theta \circ \psi = [d]$ for some d .

Given an abelian variety $A = \overline{\mathbb{F}}_p$, and a positive integer m coprime to p , a proper subgroup $G \subset A[m]$ is **maximal m -isotropic** if $e_{m|G} = \text{id}$ and G not properly contained in another isotropic subgroup $G' \subset A[m]$.

Isogenies recap

Given an isogeny $\phi : A \rightarrow A^\theta$, there exists a **dual isogeny** $\hat{\phi} : \hat{A}^\theta \rightarrow \hat{A}$.

Given an isogeny $\phi : A \rightarrow A^\theta$, there is a canonical isomorphism between $\ker(\phi)$ and $\ker(\hat{\phi})$.

Given two PPAVs $(A; \theta)$ and $(A^\theta; \theta^\theta)$, a **(polarised) isogeny** between PPAVs is an isogeny $\phi : A \rightarrow A^\theta$ such that $\hat{\phi} \circ \phi = [d]$ for some d .

Given an abelian variety $A = \overline{F}_p$, and a positive integer m coprime to p , a proper subgroup $G \subset A[m]$ is **maximal m -isotropic** if $e_{m|G} = \text{id}$ and G not properly contained in another isotropic subgroup $G' \subset A[m]$.

Let $A = \overline{F}_q$ be a PPAV, and let $G \subset A(\overline{F}_q)$ be a proper subgroup. Then there exists a PPAV $A^\theta = \overline{F}_q$ and an isogeny $\phi : A \rightarrow A^\theta$ with kernel G if and only if G is maximal m -isotropic for some m .

Isogenies recap

$(\cdot, \cdot, \cdot, \cdot, \cdot)$ -isogeny

Let $A; A^\theta$ be PPAVs of dimension d , and $\phi : A \rightarrow A^\theta$ a (polarised) isogeny. Then ϕ is a $(\cdot, \cdot, \cdot, \cdot, \cdot)$ -**isogeny** if $\ker \phi = (Z = \bar{Z})^d$ (and $\ker \phi$ is maximal $\bar{\cdot}$ -isotropic).

Isogenies recap

$(\cdot; \cdot; \cdot; \cdot; \cdot)$ -isogeny

Let $A; A^\theta$ be PPAVs of dimension d , and $\alpha : A \rightarrow A^\theta$ a (polarised) isogeny. Then α is a $(\cdot; \cdot; \cdot; \cdot; \cdot)$ -**isogeny** if $\ker \alpha = (Z = \bar{Z})^d$ (and $\ker \alpha$ is maximal $\bar{\cdot}$ -isotropic).

$(\cdot; \cdot; \cdot; \cdot; \cdot)$ -isogenies preserve superspeciality!

Isogenies recap

$(\ell; \dots; \ell)$ -isogeny

Let $A; A^\theta$ be PPAVs of dimension d , and $\alpha : A \rightarrow A^\theta$ a (polarised) isogeny. Then α is a $(\ell; \dots; \ell)$ -**isogeny** if $\ker \alpha = (Z = \ell Z)^d$ (and $\ker \alpha$ is maximal ℓ -isotropic).

$(\ell; \dots; \ell)$ -isogenies preserve superspeciality!

Richelot isogenies (i.e. (2,2) isogenies)

Let A be a PPAS. A **Richelot isogeny** $\alpha : A \rightarrow A/G$ is an isogeny where $G = (Z = 2Z)^2$ is a maximal 2-isotropic subgroup of $A[2]$.

Richelot isogenies

Computing Richelot isogenies:

Let $C=K : y^2 = f(x)$ be a genus 2 curve. Take some quadratic splitting of $f(x)$:

$$f(x) = g_1(x)g_2(x)g_3(x)$$

where $g_j(x) = g_{j,2}x^2 + g_{j,1}x + g_{j,0}$.

Richelot isogenies

Computing Richelot isogenies:

Let $C = K : y^2 = f(x)$ be a genus 2 curve. Take some quadratic splitting of $f(x)$:

$$f(x) = g_1(x)g_2(x)g_3(x)$$

where $g_j(x) = g_{j,2}x^2 + g_{j,1}x + g_{j,0}$.

Define Δ as the determinant of the matrix

$$\Delta := \det \begin{pmatrix} g_{1,0} & g_{1,1} & g_{1,2} \\ g_{2,0} & g_{2,1} & g_{2,2} \\ g_{3,0} & g_{3,1} & g_{3,2} \end{pmatrix} :$$

Richelot isogenies

Computing Richelot isogenies:

Let $C = K : y^2 = f(x)$ be a genus 2 curve. Take some quadratic splitting of $f(x)$:

$$f(x) = g_1(x)g_2(x)g_3(x)$$

where $g_j(x) = g_{j,2}x^2 + g_{j,1}x + g_{j,0}$.

Define Δ as the determinant of the matrix

$$\Delta := \det \begin{pmatrix} g_{1,0} & g_{1,1} & g_{1,2} \\ g_{2,0} & g_{2,1} & g_{2,2} \\ g_{3,0} & g_{3,1} & g_{3,2} \end{pmatrix} :$$

If $\Delta \neq 0$, then there exists a Richelot isogeny $\phi : J(C) \rightarrow J(C^\theta)$ where

$$C^\theta : y^2 = h_1(x)h_2(x)h_3(x)$$

Here, $h_i(x) := \frac{1}{\Delta} (g_{i+1}^\theta(x)g_{i+2}(x) - g_{i+1}(x)g_{i+2}^\theta(x))$ (indices taken mod 3)

Richelot isogenies

Example

Let $C = \mathbb{F}_{13}$ be the genus 2 curve $y^2 = x^5 + 3x^4 - 4x^3 + 2x^2 - 2x$.

Richelot isogenies

Example

Let $C = \mathbb{F}_{13}$ be the genus 2 curve $y^2 = x^5 + 3x^4 - 4x^3 + 2x^2 - 2x$.

We can factorise $f(x)$ over \mathbb{F}_{13} as $x(x^2 - 3x + 2)(x^2 + 6x - 1)$.

Richelot isogenies

Example

Let $C = \mathbb{F}_{13}$ be the genus 2 curve $y^2 = x^5 + 3x^4 - 4x^3 + 2x^2 - 2x$.

We can factorise $f(x)$ over \mathbb{F}_{13} as $x(x^2 - 3x + 2)(x^2 + 6x - 1)$.

We calculate $\nu = 3$ (and $\nu^{-1} = 4$) and

$$h_1(x) = g_2(x)^{\nu} g_3(x) \quad g_2(x) g_3(x)^{\nu^{-1}} = 9x^2 - 6x - 9$$

$$h_2(x) = g_3(x)^{\nu} g_1(x) \quad g_3(x) g_1(x)^{\nu^{-1}} = x^2 + 1$$

$$h_3(x) = g_1(x)^{\nu} g_2(x) \quad g_1(x) g_2(x)^{\nu^{-1}} = x^2 + 2$$

Richelot isogenies

Example

Let $C = \mathbb{F}_{13}$ be the genus 2 curve $y^2 = x^5 + 3x^4 - 4x^3 + 2x^2 - 2x$.

We can factorise $f(x)$ over \mathbb{F}_{13} as $x(x^2 - 3x + 2)(x^2 + 6x - 1)$.

We calculate $\nu = 3$ (and $\nu^2 = 4$) and

$$h_1(x) = g_2(x)^\nu g_3(x) \quad g_2(x)g_3(x)^\nu = 9x^2 - 6x - 9$$

$$h_2(x) = g_3(x)^\nu g_1(x) \quad g_3(x)g_1(x)^\nu = x^2 + 1$$

$$h_3(x) = g_1(x)^\nu g_2(x) \quad g_1(x)g_2(x)^\nu = x^2 + 2$$

Thus $J(C)$ is $(2;2)$ -isogeneous to $J(C^\nu)$ where

$$C^\nu : y^2 = (9x^2 - 6x - 9)(x^2 + 1)(x^2 - 2):$$

(3; 3)-isogenies

Theorem (Bruin–Flynn–Testa (2014))

Let $C=K$ be a genus 2 curve such that J_C has a maximal 3-isotropic subgroup. Then C admits a model $y^2 = G(x)^2 + H(x)^3$ where

$$H(x) = x^2 + rx + t;$$

$$G(x) = (s - st - 1)x^3 + 3s(r - t)x^2 + 3sr(r - t)x - st^2 + sr^3 + t$$

for some $r, s, t \in K$. (here r, s, t depend on the given maximal 3-isotropic subgroup)

(3; 3)-isogenies

Theorem (Bruin–Flynn–Testa (2014))

Let $C=K$ be a genus 2 curve such that J_C has a maximal 3-isotropic subgroup. Then C admits a model $y^2 = G(x)^2 + H(x)^3$ where

$$H(x) = x^2 + rx + t;$$

$$G(x) = (s - st - 1)x^3 + 3s(r - t)x^2 + 3sr(r - t)x - st^2 + sr^3 + t$$

for some $r, s, t \in K$. (here r, s, t depend on the given maximal 3-isotropic subgroup)

Theorem (Bruin–Flynn–Testa (2014))

Let $C_{rst}=K$ be described as above. Then $Jac(C_{rst})$ is (3; 3)-isogenous to $Jac(C^0)$ where $C^0=K$ is the genus 2 curve $3y^2 = G^0(x)^2 + 4 - stH^0(x)^3$ and where

$$G^0(x) = ((s - st - 1)x^3 + 3s(r - t)x^2 + 3rs(r - t)x + (r^3s - st^2 - t));$$

$$H^0(x) = (r - 1)(rs - st - 1)x^2 + (r^3s - 2r^2s + rst + r - st^2 + st - t)x - (r^2 - t)(rs - st - 1) \\ = r^6s^2 - 6r^4s^2t - 3r^4s + 2r^3s^2t^2 + 2r^3s^2t + 3r^3st + r^3s + r^3 + 9r^2s^2t^2 + 6r^2st - 6rs^2$$

Maximal isotropic subgroups

Theorem

Let A be a PPAS, let $G \leq A[\mathbb{F}^n]$ be a maximal \mathbb{F}^n -isotropic subgroup. Then $G = C_{\mathbb{F}^n} \times C_{\mathbb{F}^n - k} \times C_{\mathbb{F}^k}$ for some $0 \leq k \leq n$.

Proof:

Maximal isotropic subgroups

Theorem

Let A be a PPAS, let $G \leq A[\mathbb{F}^n]$ be a maximal \mathbb{F}^n -isotropic subgroup. Then $G = C_{\mathbb{F}^n} \times C_{\mathbb{F}^{n-k}} \times C_{\mathbb{F}^k}$ for some $0 \leq k \leq n$.

Proof:

Let $G = C_{\mathbb{F}^a} \times C_{\mathbb{F}^b} \times C_{\mathbb{F}^c} \times C_{\mathbb{F}^d}$ and assume wlog $a \leq b \leq c \leq d$.

Maximal isotropic subgroups

Theorem

Let A be a PPAS, let $G \leq A[\mathbb{F}^n]$ be a maximal \mathbb{F}^n -isotropic subgroup. Then $G = C_{\mathbb{F}^n} \times C_{\mathbb{F}^k}$ for some $0 \leq k \leq n$.

Proof:

Let $G = C_{\mathbb{F}^a} \times C_{\mathbb{F}^b} \times C_{\mathbb{F}^c} \times C_{\mathbb{F}^d}$ and assume wlog $a \geq b \geq c \geq d$.

As G must be proper, G must have rank ≤ 3 , and so $d = 0$.

Maximal isotropic subgroups

Theorem

Let A be a PPAS, let $G \subset A[\ell^n]$ be a maximal ℓ^n -isotropic subgroup. Then $G = C_{\ell^n} \times C_{\ell^{n-k}} \times C_{\ell^k}$ for some $0 \leq k \leq n$.

Proof:

Let $G = C_{\ell^a} \times C_{\ell^b} \times C_{\ell^c} \times C_{\ell^d}$ and assume wlog $a \geq b \geq c \geq d$.

As G must be proper, G must have rank ≤ 3 , and so $d = 0$.

Let $\phi : A \rightarrow A^\theta$ be an isogeny with kernel G . Then as $\ker(\hat{\phi}) = C_{\ell^n}^4$, this implies the kernel of ϕ is

$$C_{\ell^{n-a}} \times C_{\ell^{n-b}} \times C_{\ell^{n-c}} \times C_{\ell^{n-d}}$$

Maximal isotropic subgroups

Theorem

Let A be a PPAS, let $G \leq A[\cdot^n]$ be a maximal \cdot^n -isotropic subgroup. Then $G = C_{\cdot^n} \times C_{\cdot^n/k} \times C_{\cdot k}$ for some $0 < k < n$.

Proof:

Let $G = C_{\cdot a} \times C_{\cdot b} \times C_{\cdot c} \times C_{\cdot d}$ and assume wlog $a \leq b \leq c \leq d$.

As G must be proper, G must have rank ≤ 3 , and so $d = 0$.

Let $\hat{\cdot} : A \rightarrow A^\theta$ be an isogeny with kernel G . Then as $\ker(\hat{\cdot}) = C_{\cdot^n}^4$, this implies the kernel of $\hat{\cdot}$ is

$$C_{\cdot^n/a} \times C_{\cdot^n/b} \times C_{\cdot^n/c} \times C_{\cdot^n/d}$$

As both A and A^θ are principally polarised ($A = \hat{A}$ and $A^\theta = \hat{A}^\theta$), thus $G = \ker(\hat{\cdot})$.

Maximal isotropic subgroups

Theorem

Let A be a PPAS, let $G \leq A[\cdot^n]$ be a maximal \cdot^n -isotropic subgroup. Then $G = C_{\cdot^n} \times C_{\cdot^n-k} \times C_{\cdot k}$ for some $0 < k < n$.

Proof:

Let $G = C_{\cdot a} \times C_{\cdot b} \times C_{\cdot c} \times C_{\cdot d}$ and assume wlog $a \leq b \leq c \leq d$.

As G must be proper, G must have rank ≤ 3 , and so $d = 0$.

Let $\hat{\cdot} : A \rightarrow A^\theta$ be an isogeny with kernel G . Then as $\ker(\hat{\cdot}^4) = C_{\cdot n}^4$, this implies the kernel of $\hat{\cdot}^b$ is

$$C_{\cdot n-a} \times C_{\cdot n-b} \times C_{\cdot n-c} \times C_{\cdot n-d}$$

As both A and A^θ are principally polarised ($A = \hat{A}$ and $A^\theta = \hat{A}^\theta$), thus $G = \ker(\hat{\cdot})$.

Therefore $n-a = d$ and $n-b = c$, which yields the result. \square

Genus 2 isogeny graph

Genus 2 isogeny graph

Let p be prime. Define $\mathcal{G}_2(\ell; p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised abelian surfaces over $\overline{\mathbb{F}}_p$, and whose edges are $(\ell; \ell)$ -isogenies, for a prime $\ell \neq p$.

Genus 2 isogeny graph

Genus 2 isogeny graph

Let p be prime. Define $\mathcal{G}_2(\ell; p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised abelian surfaces over $\overline{\mathbb{F}}_p$, and whose edges are $(\ell; \ell)$ -isogenies, for a prime $\ell \neq p$.

Graph is connected.

Genus 2 isogeny graph

Genus 2 isogeny graph

Let p be prime. Define $\mathcal{G}_2(\cdot; p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised abelian surfaces over $\overline{\mathbb{F}}_p$, and whose edges are $(\cdot; \cdot)$ -isogenies, for a prime $\ell \neq p$.

Graph is connected.

Graph has $\frac{p^3}{2880}$ vertices.

Genus 2 isogeny graph

Genus 2 isogeny graph

Let p be prime. Define $\mathcal{G}_2(\ell; p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised abelian surfaces over $\overline{\mathbb{F}}_p$, and whose edges are $(\ell; \ell)$ -isogenies, for a prime $\ell \notin p$.

Graph is connected.

Graph has $\frac{p^3}{2880}$ vertices.

Every vertex has $(\ell^2 + 1)(\ell + 1)$ neighbours.

Genus 2 isogeny graph

Genus 2 isogeny graph

Let p be prime. Define $\mathcal{G}_2(\cdot; p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised abelian surfaces over $\overline{\mathbb{F}}_p$, and whose edges are $(\cdot; \cdot)$ -isogenies, for a prime $\cdot \notin p$.

Graph is connected.

Graph has $\frac{p^3}{2880}$ vertices.

Every vertex has $(\cdot^2 + 1)(\cdot + 1)$ neighbours.

Not quite Ramanujan, but close enough.

Genus 2 isogeny graph

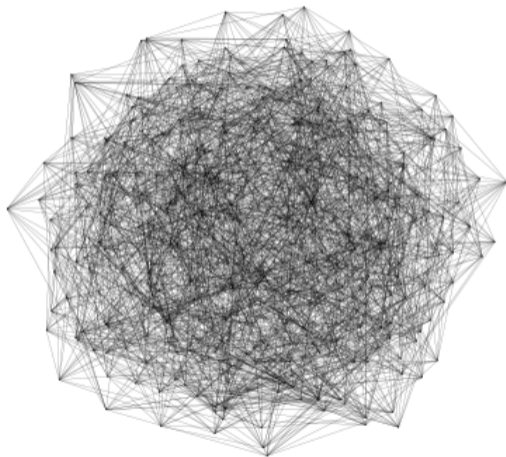


Figure: The (2,2)-isogeny graph for $p = 97$.

Genus 2 isogeny graph

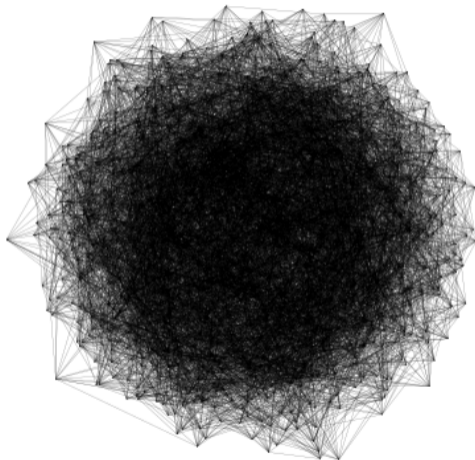


Figure: The (2,2)-isogeny graph for $p = 151$.

Genus 2 isogeny graph

Theorem

Let A be a PPAS. Then the number of PPAS's which are $(\cdot; \cdot)$ -isogenous to A is $(\cdot^2 + 1)(\cdot + 1)$.

Proof:

Genus 2 isogeny graph

Theorem

Let A be a PPAS. Then the number of PPAS's which are $(\ell; \ell)$ -isogenous to A is $(\ell^2 + 1)(\ell + 1)$.

Proof:

As the kernel of any isogeny $\phi : A \rightarrow A^\theta$ corresponds to some maximal isotropic subgroup, it suffices to count the number of maximal ℓ -isotropic subgroups of $A[\ell]$ isomorphic to C^2 .

Genus 2 isogeny graph

Theorem

Let A be a PPAS. Then the number of PPAS's which are $(\ell; \ell)$ -isogenous to A is $(\ell^2 + 1)(\ell + 1)$.

Proof:

As the kernel of any isogeny $\phi : A \rightarrow A^\theta$ corresponds to some maximal isotropic subgroup, it suffices to count the number of maximal ℓ -isotropic subgroups of $A[\ell]$ isomorphic to C^2 .

Let $A[\ell] = \langle P_1, P_2, P_3, P_4 \rangle$. We first count the number of pairs $a; b \in A[\ell]$ such that $\langle a; b \rangle = C^2$ is maximal ℓ -isotropic.

Genus 2 isogeny graph

Theorem

Let A be a PPAS. Then the number of PPAS's which are $(\ell; \ell)$ -isogenous to A is $(\ell^2 + 1)(\ell + 1)$.

Proof:

As the kernel of any isogeny $\phi : A \rightarrow A^\theta$ corresponds to some maximal isotropic subgroup, it suffices to count the number of maximal ℓ -isotropic subgroups of $A[\ell]$ isomorphic to C^2 .

Let $A[\ell] = \langle P_1, P_2, P_3, P_4 \rangle$. We first count the number of pairs $a; b \in A[\ell]$ such that $\langle a; b \rangle = C^2$ is maximal ℓ -isotropic.

Let

$$a = a_1 P_1 + a_2 P_2 + a_3 P_3 + a_4 P_4 \quad \text{for some } a_i \in \{0, 1, \dots, \ell - 1\};$$

$$b = b_1 P_1 + b_2 P_2 + b_3 P_3 + b_4 P_4 \quad \text{for some } b_i \in \{0, 1, \dots, \ell - 1\};$$

Genus 2 isogeny graph

Theorem

Let A be a PPAS. Then the number of PPAS's which are $(\ell; \ell)$ -isogenous to A is $(\ell^2 + 1)(\ell + 1)$.

Proof:

As the kernel of any isogeny $\phi : A \rightarrow A^\theta$ corresponds to some maximal isotropic subgroup, it suffices to count the number of maximal ℓ -isotropic subgroups of $A[\ell]$ isomorphic to C^2 .

Let $A[\ell] = \langle P_1, P_2, P_3, P_4 \rangle$. We first count the number of pairs $a; b \in A[\ell]$ such that $\langle a; b \rangle = C^2$ is maximal ℓ -isotropic.

Let

$$a = a_1 P_1 + a_2 P_2 + a_3 P_3 + a_4 P_4 \quad \text{for some } a_i \in \{0; 1; \dots; \ell - 1\}g;$$

$$b = b_1 P_1 + b_2 P_2 + b_3 P_3 + b_4 P_4 \quad \text{for some } b_i \in \{0; 1; \dots; \ell - 1\}g;$$

We have $\ell^4 - 1$ choices for the first element $a \in A[\ell]$.

Genus 2 isogeny graph

We now pick $b \in A[\ell]$ with order ℓ and such that $e_\ell(a; b) = 1$.

Genus 2 isogeny graph

We now pick $b \in A[\ell]$ with order ℓ and such that $e_\ell(a; b) = 1$.

Using linearity and skew-symmetry of the Weil pairing:

$$e_\ell(a; b) = e_\ell(P_1; P_2)^{a_1 b_2 - a_2 b_1} e_\ell(P_1; P_3)^{a_1 b_3 - a_3 b_1} e_\ell(P_1; P_4)^{a_1 b_4 - a_4 b_1} \\ e_\ell(P_2; P_3)^{a_2 b_3 - a_3 b_2} e_\ell(P_2; P_4)^{a_2 b_4 - a_4 b_2} e_\ell(P_3; P_4)^{a_3 b_4 - a_4 b_3} = 1$$

Genus 2 isogeny graph

We now pick $b \in A[\ell]$ with order ℓ and such that $e_\ell(a; b) = 1$.

Using linearity and skew-symmetry of the Weil pairing:

$$e_\ell(a; b) = e_\ell(P_1; P_2)^{a_1 b_2 - a_2 b_1} e_\ell(P_1; P_3)^{a_1 b_3 - a_3 b_1} e_\ell(P_1; P_4)^{a_1 b_4 - a_4 b_1} \\ e_\ell(P_2; P_3)^{a_2 b_3 - a_3 b_2} e_\ell(P_2; P_4)^{a_2 b_4 - a_4 b_2} e_\ell(P_3; P_4)^{a_3 b_4 - a_4 b_3} = 1$$

As $e_\ell(P_i; P_j) = \ell^{i,j}$ for some non-zero $i, j \in \mathbb{Z}$, this yields

$$b_4 (\ell_{1,4} a_1 + \ell_{2,4} a_2 + \ell_{3,4} a_3) = \ell_{1,2} (a_2 b_1 - a_1 b_2) + \ell_{1,3} (a_3 b_1 - a_1 b_3) \\ + \ell_{2,3} (a_3 b_2 - a_2 b_3) + \ell_{1,4} a_4 b_1 \\ + \ell_{2,4} a_4 b_2 + \ell_{3,4} a_4 b_3 \pmod{\ell}$$

Genus 2 isogeny graph

We now pick $b \in A[\ell]$ with order ℓ and such that $e_\ell(a; b) = 1$.

Using linearity and skew-symmetry of the Weil pairing:

$$e_\ell(a; b) = e_\ell(P_1; P_2)^{a_1 b_2 - a_2 b_1} e_\ell(P_1; P_3)^{a_1 b_3 - a_3 b_1} e_\ell(P_1; P_4)^{a_1 b_4 - a_4 b_1} \\ e_\ell(P_2; P_3)^{a_2 b_3 - a_3 b_2} e_\ell(P_2; P_4)^{a_2 b_4 - a_4 b_2} e_\ell(P_3; P_4)^{a_3 b_4 - a_4 b_3} = 1$$

As $e_\ell(P_i; P_j) = \ell^{i \cdot j}$ for some non-zero $i \cdot j \in \mathbb{Z}$, this yields

$$b_4 (\ell^{1,4} a_1 + \ell^{2,4} a_2 + \ell^{3,4} a_3) = \ell^{1,2} (a_2 b_1 - a_1 b_2) + \ell^{1,3} (a_3 b_1 - a_1 b_3) \\ + \ell^{2,3} (a_3 b_2 - a_2 b_3) + \ell^{1,4} a_4 b_1 \\ + \ell^{2,4} a_4 b_2 + \ell^{3,4} a_4 b_3 \pmod{\ell}$$

If $\ell^{1,4} a_1 + \ell^{2,4} a_2 + \ell^{3,4} a_3 \not\equiv 0 \pmod{\ell}$, then this gives a free choice for $b_1; b_2; b_3$, which then determines b_4 (and other cases done similarly). So we have $\ell^3 - 1$ choices for b .

Genus 2 isogeny graph

But to ensure $b \notin \text{hai}$, we must avoid $\ell - 1$ elements. This gives a total of $\ell^3 - \ell$ choices for b .

Genus 2 isogeny graph

But to ensure $b \notin \langle h, a \rangle$, we must avoid $q - 1$ elements. This gives a total of $q^3 - q - 1$ choices for b .

Thus, the number of pairs $a; b \in A[\mathbb{F}_q]$ such that that $\langle h, a; b \rangle = C^2$ is maximal q -isotropic is $(q^4 - 1)(q^3 - q - 1)$.

Genus 2 isogeny graph

But to ensure $b \notin \langle h \rangle$, we must avoid $q - 1$ elements. This gives a total of $q^3 - q$ choices for b .

Thus, the number of pairs $a; b \in A[\mathbb{F}_q]$ such that that $\langle ha; bi \rangle = C^2$ is maximal q -isotropic is $(q^4 - 1)(q^3 - q)$.

For any such subgroup $C \leq C$, there are $(q^2 - 1)(q^2 - q)$ generating pairs.

Genus 2 isogeny graph

But to ensure $b \notin \langle h \rangle$, we must avoid $q - 1$ elements. This gives a total of $q^3 - q$ choices for b .

Thus, the number of pairs $a; b \in A[\mathbb{F}_q]$ such that that $\langle ha; bi \rangle = C^2$ is maximal \mathbb{F}_q -isotropic is $(q^4 - 1)(q^3 - q)$.

For any such subgroup $C \leq C'$, there are $(q^2 - 1)(q^2 - q)$ generating pairs.

Thus, the total number of maximal isotropic $C \leq C'$ subgroups of $A[\mathbb{F}_q]$ is

$$\frac{(q^4 - 1)(q^3 - q)}{(q^2 - 1)(q^2 - q)} = (q^2 + 1)(q + 1):$$



Genus 2 SIDH

Initial Setup:

Pick a large prime $p = 2^n 3^m f - 1$.

Genus 2 SIDH

Initial Setup:

Pick a large prime $p = 2^n 3^m f + 1$.

Pick a random hyperelliptic curve $H = \mathbb{F}_{p^2}$, and let J_H denote its Jacobian.

Genus 2 SIDH

Initial Setup:

Pick a large prime $p = 2^n 3^m f + 1$.

Pick a random hyperelliptic curve $H = \mathbb{F}_{p^2}$, and let J_H denote its Jacobian.

This can be done by starting from some particular base hyperelliptic curve, e.g.

$$H_0 : y^2 = x^6 + 1.$$

Genus 2 SIDH

Initial Setup:

Pick a large prime $p = 2^n 3^m f - 1$.

Pick a random hyperelliptic curve $H = \mathbb{F}_{p^2}$, and let J_H denote its Jacobian.

This can be done by starting from some particular base hyperelliptic curve, e.g.

$$H_0 : y^2 = x^6 + 1.$$

$\text{Jac}(H_0)$ is superspecial as it is double cover of $y^2 = x^3 + 1$.

Genus 2 SIDH

Initial Setup:

Pick a large prime $p = 2^n 3^m f + 1$.

Pick a random hyperelliptic curve $H = \mathbb{F}_{p^2}$, and let J_H denote its Jacobian.

This can be done by starting from some particular base hyperelliptic curve, e.g.

$$H_0 : y^2 = x^6 + 1.$$

$\text{Jac}(H_0)$ is superspecial as it is double cover of $y^2 = x^3 + 1$.

Take a random sequence of Richelot isogenies $H_0 \rightarrow H_1 \rightarrow \dots \rightarrow H$ (taking at least $O(\log p)$ steps), to obtain a random curve H .

Genus 2 SIDH

Initial Setup:

Pick a large prime $p = 2^n 3^m f + 1$.

Pick a random hyperelliptic curve $H = \mathbb{F}_{p^2}$, and let J_H denote its Jacobian.

This can be done by starting from some particular base hyperelliptic curve, e.g.

$$H_0 : y^2 = x^6 + 1.$$

$\text{Jac}(H_0)$ is superspecial as it is double cover of $y^2 = x^3 + 1$.

Take a random sequence of Richelot isogenies $H_0 \rightarrow H_1 \rightarrow \dots \rightarrow H$ (taking at least $O(\log p)$ steps), to obtain a random curve H .

Calculate bases $\{P_1; P_2; P_3; P_4\}$ for $J_H[2^n]$ and bases $\{Q_1; Q_2; Q_3; Q_4\}$ for $J_H[3^m]$.

Genus 2 SIDH

Round 1: Alice



Genus 2 SIDH

Round 1: Alice



1. Alice chooses 12 secret random scalars $(a_1; a_2; \dots; a_{12})$ $f_0; 1; \dots; 2^n - 1$.

Genus 2 SIDH

Round 1: Alice



1. Alice chooses 12 secret random scalars $(a_1; a_2; \dots; a_{12}) \in \mathbb{F}_0; 1; \dots; 2^n \setminus \{0\}$.
2. She computes the subgroup $A \leq J_H[2^n]$, given by

$$\begin{aligned} A := & a_1P_1 + a_2P_2 + a_3P_3 + a_4P_4; \\ & a_5P_1 + a_6P_2 + a_7P_3 + a_8P_4; \\ & a_9P_1 + a_{10}P_2 + a_{11}P_3 + a_{12}P_4 \end{aligned}$$

The scalars (a_i) are chosen such that A is maximal isotropic subgroup of order 2^{2n} .

Genus 2 SIDH

Round 1: Alice



1. Alice chooses 12 secret random scalars $(a_1; a_2; \dots; a_{12}) \in \mathbb{F}_0; 1; \dots; 2^n \setminus \{0\}$.
2. She computes the subgroup $A \subseteq J_H[2^n]$, given by

$$\begin{aligned} A := & a_1 P_1 + a_2 P_2 + a_3 P_3 + a_4 P_4; \\ & a_5 P_1 + a_6 P_2 + a_7 P_3 + a_8 P_4; \\ & a_9 P_1 + a_{10} P_2 + a_{11} P_3 + a_{12} P_4 \end{aligned}$$

The scalars (a_i) are chosen such that A is maximal isotropic subgroup of order 2^{2n} .

3. Alice sends the tuple $(J_H=A; A(Q_1); A(Q_2); A(Q_3); A(Q_4))$ to Bob!

Genus 2 SIDH

How should Alice pick scalars $a_1; a_2; \dots; a_{12}$?

Genus 2 SIDH

How should Alice pick scalars $a_1; a_2; \dots; a_{12}$?

Let

$$R_1 = a_1P_1 + a_2P_2 + a_3P_3 + a_4P_4$$

$$R_2 = a_5P_1 + a_6P_2 + a_7P_3 + a_8P_4$$

$$R_3 = a_9P_1 + a_{10}P_2 + a_{11}P_3 + a_{12}P_4$$

Genus 2 SIDH

How should Alice pick scalars $a_1; a_2; \dots; a_{12}$?

Let

$$R_1 = a_1P_1 + a_2P_2 + a_3P_3 + a_4P_4$$

$$R_2 = a_5P_1 + a_6P_2 + a_7P_3 + a_8P_4$$

$$R_3 = a_9P_1 + a_{10}P_2 + a_{11}P_3 + a_{12}P_4$$

Alice needs to ensure that A is maximal ℓ^n -isotropic subgroup of $J_H[2^n]$, i.e. must choose generators $R_1; R_2; R_3$ such that $e_{2^n}(R_1; R_2) = e_{2^n}(R_1; R_3) = e_{2^n}(R_2; R_3) = 1$

Genus 2 SIDH

How should Alice pick scalars $a_1; a_2; \dots; a_{12}$?

Let

$$R_1 = a_1 P_1 + a_2 P_2 + a_3 P_3 + a_4 P_4$$

$$R_2 = a_5 P_1 + a_6 P_2 + a_7 P_3 + a_8 P_4$$

$$R_3 = a_9 P_1 + a_{10} P_2 + a_{11} P_3 + a_{12} P_4$$

Alice needs to ensure that A is maximal n -isotropic subgroup of $J_H[2^n]$, i.e. must choose generators $R_1; R_2; R_3$ such that $e_{2^n}(R_1; R_2) = e_{2^n}(R_1; R_3) = e_{2^n}(R_2; R_3) = 1$

As shown before, this is equivalent to choosing (a_i) which satisfy a system of linear congruences, i.e. we require

$$\begin{aligned} e(R_1; R_2) &= e(P_1; P_2)^{a_1 a_6 - a_2 a_5} e(P_1; P_3)^{a_1 a_7 - a_3 a_5} e(P_1; P_4)^{a_1 a_8 - a_4 a_5} \\ &\quad e(P_2; P_3)^{a_2 a_7 - a_3 a_6} e(P_2; P_4)^{a_2 a_8 - a_4 a_6} e(P_3; P_4)^{a_3 a_8 - a_4 a_7} = 1: \end{aligned}$$

Genus 2 SIDH

Alice can do the following:

Genus 2 SIDH

Alice can do the following:

- (i) Calculate the values $e_{2^n}(P_i; P_j) \pmod{2^n}$ such that $e_{2^n}(P_i; P_j) = e_{2^n}(P_1; P_2)^{ij}$.

Genus 2 SIDH

Alice can do the following:

- (i) Calculate the values $e_{2^n}(P_i; P_j) \pmod{2^n}$ such that $e_{2^n}(P_i; P_j) = e_{2^n}(P_1; P_2)^{ij}$.
- (ii) Pick random $a_1, a_2, a_3, a_4 \in \{0, 1, \dots, 2^n - 1\}$ such that at least one of the four is odd.

Genus 2 SIDH

Alice can do the following:

- (i) Calculate the values $e_{2^n}(P_i; P_j) \pmod{2^n}$ such that $e_{2^n}(P_i; P_j) = e_{2^n}(P_1; P_2)^{i \cdot j}$.
- (ii) Pick random $a_1; a_2; a_3; a_4 \in \mathbb{F}_0; 1; \dots; 2^n - 1$ such that at least one of the four is odd.
- (iii) Pick a random $k \in \mathbb{F}_0; 1; \dots; n$, and pick random $a_5; a_6; a_7; a_8$ such that

$$a_1 a_6 - a_2 a_5 + a_{1,3}(a_1 a_7 - a_3 a_5) + a_{1,4}(a_1 a_8 - a_4 a_5) \\ + a_{2,3}(a_2 a_7 - a_3 a_6) + a_{2,4}(a_2 a_8 - a_4 a_6) + a_{3,4}(a_3 a_8 - a_4 a_7) \equiv 0 \pmod{2^k}$$

- (iv) Pick random $a_9; a_{10}; a_{11}; a_{12}$ such that

$$a_1 a_{10} - a_2 a_9 + a_{1,3}(a_1 a_{11} - a_3 a_9) + a_{1,4}(a_1 a_{12} - a_4 a_9) \\ + a_{2,3}(a_2 a_{11} - a_3 a_{10}) + a_{2,4}(a_2 a_{12} - a_4 a_{10}) + a_{3,4}(a_3 a_{12} - a_4 a_{11}) \equiv 0 \pmod{2^{n-k}}$$

Genus 2 SIDH

Round 1: Bob



Genus 2 SIDH

Round 1: Bob



1. Bob also chooses 12 secret random scalars $(b_1; b_2; \dots; b_{12})$ $f_0; 1; \dots; 3^m$ $1g$.

Genus 2 SIDH

Round 1: Bob



1. Bob also chooses 12 secret random scalars $(b_1; b_2; \dots; b_{12}) \in \mathbb{F}_0; 1; \dots; 3^m - 1$.
2. He computes the group $B \subseteq J_H[3^m]$, given by

$$\begin{aligned} B := & b_1 Q_1 + b_2 Q_2 + b_3 Q_3 + b_4 Q_4; \\ & b_5 Q_1 + b_6 Q_2 + b_7 Q_3 + b_8 Q_4; \\ & b_9 Q_1 + b_{10} Q_2 + b_{11} Q_3 + b_{12} Q_4 : \end{aligned}$$

Again, the scalars (b_i) must be chosen such that B is maximal isotropic subgroup of order 3^{2m} .

Genus 2 SIDH

Round 1: Bob



1. Bob also chooses 12 secret random scalars $(b_1; b_2; \dots; b_{12}) \in \mathbb{F}_0; 1; \dots; 3^m - 1$.
2. He computes the group $B \subseteq J_H[3^m]$, given by

$$\begin{aligned} B := & b_1 Q_1 + b_2 Q_2 + b_3 Q_3 + b_4 Q_4; \\ & b_5 Q_1 + b_6 Q_2 + b_7 Q_3 + b_8 Q_4; \\ & b_9 Q_1 + b_{10} Q_2 + b_{11} Q_3 + b_{12} Q_4 : \end{aligned}$$

Again, the scalars (b_i) must be chosen such that B is maximal isotropic subgroup of order 3^{2m} .

3. Bob sends the tuple $(J_H=B; B(P_1); B(P_2); B(P_3); B(P_4))$ to Alice!

Genus 2 SIDH

Round 2: Alice

Genus 2 SIDH

Round 2: Alice

4. Alice receives Bob's tuple and calculates:

$$\begin{aligned} A^0 := & a_1 B(P_1) + a_2 B(P_2) + a_3 B(P_3) + a_4 B(P_4); \\ & a_5 B(P_1) + a_6 B(P_2) + a_7 B(P_3) + a_8 B(P_4); \\ & a_9 B(P_1) + a_{10} B(P_2) + a_{11} B(P_3) + a_{12} B(P_4) : \end{aligned}$$

Genus 2 SIDH

Round 2: Alice

4. Alice receives Bob's tuple and calculates:

$$\begin{aligned}A^0 := & a_1 B(P_1) + a_2 B(P_2) + a_3 B(P_3) + a_4 B(P_4); \\ & a_5 B(P_1) + a_6 B(P_2) + a_7 B(P_3) + a_8 B(P_4); \\ & a_9 B(P_1) + a_{10} B(P_2) + a_{11} B(P_3) + a_{12} B(P_4) : \end{aligned}$$

5. Alice thus has the isogeny $A^0 : J_H = B ! (J_H = B) = A^0$, and can compute the G2 invariants of $(J_H = B) = A^0$.

Genus 2 SIDH

Round 2: Bob

Genus 2 SIDH

Round 2: Bob

4. Similarly, Bob receives Alice's tuple and calculates:

$$\begin{aligned} B^0 := & b_1 A(Q_1) + b_2 A(Q_2) + b_3 A(Q_3) + b_4 A(Q_4); \\ & b_5 A(Q_1) + b_6 A(Q_2) + b_7 A(Q_3) + b_8 A(Q_4); \\ & b_9 A(Q_1) + b_{10} A(Q_2) + b_{11} A(Q_3) + b_{12} A(Q_4) : \end{aligned}$$

Genus 2 SIDH

Round 2: Bob

4. Similarly, Bob receives Alice's tuple and calculates:

$$\begin{aligned} B^0 := & b_1 A(Q_1) + b_2 A(Q_2) + b_3 A(Q_3) + b_4 A(Q_4); \\ & b_5 A(Q_1) + b_6 A(Q_2) + b_7 A(Q_3) + b_8 A(Q_4); \\ & b_9 A(Q_1) + b_{10} A(Q_2) + b_{11} A(Q_3) + b_{12} A(Q_4) : \end{aligned}$$

5. Bob thus has the isogeny $\phi_{B^0} : J_H = A \rightarrow (J_H = A) = B^0$, and can compute the G2 invariants of $(J_H = A) = B^0$.

Genus 2 SIDH

Round 2: Bob

4. Similarly, Bob receives Alice's tuple and calculates:

$$\begin{aligned} B^0 := & b_1 A(Q_1) + b_2 A(Q_2) + b_3 A(Q_3) + b_4 A(Q_4); \\ & b_5 A(Q_1) + b_6 A(Q_2) + b_7 A(Q_3) + b_8 A(Q_4); \\ & b_9 A(Q_1) + b_{10} A(Q_2) + b_{11} A(Q_3) + b_{12} A(Q_4) : \end{aligned}$$

5. Bob thus has the isogeny $J_{H=A} : J_{H=A} = B^0$, and can compute the G2 invariants of $J_{H=A} = B^0$.

As $J_{H=A} = B^0 = (J_{H=A}) = A(B) = J_{H=hA}; B_i = (J_{H=B}) = B(A) = (J_{H=B}) = A^0$, Alice and Bob can use their computed G2 invariants as their shared secret. :)

Security

Isogeny finding problem

Let p be a prime, and A, A^0 two superspecial p.p. abelian surfaces over \mathbb{F}_p . Find an isogeny $\phi : A \rightarrow A^0$.

Security

Isogeny finding problem

Let p be a prime, and A, A^0 two superspecial p.p. abelian surfaces over \mathbb{F}_p . Find an isogeny $\phi : A \rightarrow A^0$.

Algorithms:

Brute force exhaustive search $\mathcal{O}(p^3)$.

Security

Isogeny finding problem

Let p be a prime, and A, A^0 two superspecial p.p. abelian surfaces over \mathbb{F}_p . Find an isogeny $\phi : A \rightarrow A^0$.

Algorithms:

Brute force exhaustive search $O(p^4)$.

Meet in the middle search $O(p^4)$.

Security

Isogeny finding problem

Let p be a prime, and A, A^0 two superspecial p.p. abelian surfaces over \mathbb{F}_p . Find an isogeny $\phi : A \rightarrow A^0$.

Algorithms:

Brute force exhaustive search $O(p^3)$.

Meet in the middle search $O(p^2)$.

(Quantum) Tani's claw finding algorithm: $O(p^2)$

Claw problem: Given two functions $f : A \rightarrow C$ and $g : B \rightarrow C$, find a pair $(a; b)$ such that $f(a) = g(b)$.

Security

Adaptive Attack:

Let's assume Alice uses the same secret key $(k; a_{12})$ over some period of time.

Security

Adaptive Attack:

Let's assume Alice uses the same secret key (a_1, a_2) over some period of time.

An attacker pretending to be Bob could try to learn Alice's secret key by maliciously providing the incorrect tuple of torsion points to Alice.

Security

Adaptive Attack:

Let's assume Alice uses the same secret key (a_1, \dots, a_{12}) over some period of time.

An attacker pretending to be Bob could try to learn Alice's secret key by maliciously providing the incorrect tuple of torsion points to Alice.

"Evil" Bob can send $(B(P_1); B(P_2); B(P_3); B([2^{n-1}]P_4 + P_4))$ to Alice, which allows Evil Bob to recover the first bit of a_4 .

Security

Adaptive Attack:

Let's assume Alice uses the same secret key (a_1, \dots, a_{12}) over some period of time.

An attacker pretending to be Bob could try to learn Alice's secret key by maliciously providing the incorrect tuple of torsion points to Alice.

"Evil" Bob can send $(B(P_1); B(P_2); B(P_3); B([2^{n-1}]P_4 + P_4))$ to Alice, which allows Evil Bob to recover the first bit of a_4 .

By repeatedly sending malformed data to Alice, Evil Bob can recover Alice's full secret key.

Security

Adaptive Attack:

Let's assume Alice uses the same secret key (a_1, \dots, a_{12}) over some period of time.

An attacker pretending to be Bob could try to learn Alice's secret key by maliciously providing the incorrect tuple of torsion points to Alice.

"Evil" Bob can send $(B(P_1); B(P_2); B(P_3); B([2^{n-1}]P_4 + P_4))$ to Alice, which allows Evil Bob to recover the first bit of a_4 .

By repeatedly sending malformed data to Alice, Evil Bob can recover Alice's full secret key.

Alice could safeguard against this by performing some (sufficiently thorough) validation on the points received from Bob each time (e.g. using the Fujisaki-Okamoto transformation).

Security

Fault Attack:

An attacker with physical access to a device using Alice's private key could perform a loop-abort fault injection attack.

Security

Fault Attack:

An attacker with physical access to a device using Alice's private key could perform a loop-abort fault injection attack.

This involves injecting some random fault in a loop counter to prematurely stop Alice computing her isogeny J_H ! $J_H = A$, and instead compute the intermediate PPAS $J_H = h^{2^n - k} (a_1 P_1 + \dots)$ for some k .

Security

Fault Attack:

An attacker with physical access to a device using Alice's private key could perform a loop-abort fault injection attack.

This involves injecting some random fault in a loop counter to prematurely stop Alice computing her isogeny J_H ! $J_H = A$, and instead compute the intermediate PPAS $J_H = h^{2^n - k} (a_1 P_1 + \dots)$ for some k .

Countermeasures include adding additional counters to verify the correct number of iterations has been executed (or just running the same computation in parallel and checking the outputs are the same)

Higher Isogenies

Genus g isogeny graph

Let p be prime. Define $\mathcal{G}_g(\cdot; p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised dimension g abelian varieties over $\overline{\mathbb{F}}_p$, and whose edges are $(\cdot; \cdot; \cdot; \cdot)$ -isogenies, for a prime $\ell \neq p$.

Higher Isogenies

Genus g isogeny graph

Let p be prime. Define $\mathcal{G}_g(\cdot; p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised dimension g abelian varieties over $\overline{\mathbb{F}}_p$, and whose edges are $(\cdot; \cdot; \cdot; \cdot)$ -isogenies, for a prime $\ell \neq p$.

Graph is connected (Jordan-Zygmund).

Higher Isogenies

Genus g isogeny graph

Let p be prime. Define $\mathcal{G}_g(\cdot; p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised dimension g abelian varieties over $\overline{\mathbb{F}}_p$, and whose edges are $(\cdot; \cdot; \cdot; \cdot)$ -isogenies, for a prime $\ell \neq p$.

Graph is connected (Jordan-Zygmund).

Graph has $O(p^{g(g+1)/2})$ vertices.

Higher Isogenies

Genus g isogeny graph

Let p be prime. Define $\mathcal{N}_g(\cdot; p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised dimension g abelian varieties over $\overline{\mathbb{F}}_p$, and whose edges are $(\cdot; \cdot; \cdot; \cdot)$ -isogenies, for a prime $\ell \neq p$.

Graph is connected (Jordan-Zygmund).

Graph has $O(p^{g(g+1)/2})$ vertices.

Every vertex has $N_g(\cdot)$ neighbours, where $N_g(\cdot)$ is a polynomial in \cdot of degree $g(g+1)/2$:

$$N_g(\cdot) := \sum_{d=0}^g \binom{g-d+1}{2} \prod_{j=0}^{d-1} \frac{1 - \ell^{-g-j}}{1 - \ell^{-j+1}}$$

Higher Isogenies

Genus g isogeny graph

Let p be prime. Define $\mathcal{G}_g(\cdot; p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised dimension g abelian varieties over $\overline{\mathbb{F}}_p$, and whose edges are $(\cdot; \cdot; \cdot; \cdot)$ -isogenies, for a prime $\ell \neq p$.

Graph is connected (Jordan-Zygmund).

Graph has $O(p^{g(g+1)/2})$ vertices.

Every vertex has $N_g(\cdot)$ neighbours, where $N_g(\cdot)$ is a polynomial in \cdot of degree $g(g+1)/2$:

$$N_g(\cdot) := \sum_{d=0}^g \binom{g-d+1}{2} \prod_{j=0}^{d-1} (1 - \cdot^{g-j})$$

Not Ramanujan in general (Jordan-Zygmund), but still has good expansion properties.

Higher Attacks

Usual algorithms:

Higher Attacks

Usual algorithms:

Naive random walk: $O(p^{g(g+1)-4})$

Higher Attacks

Usual algorithms:

Naive random walk: $O(p^{g(g+1)-4})$

Meet in the middle: $O(p^{g(g+1)-8})$.

Higher Attacks

Usual algorithms:

Naive random walk: $O(p^{g(g+1)=4})$

Meet in the middle: $O(p^{g(g+1)=8})$.

Tani's claw finding quantum algorithm: $O(p^{g(g+1)=12})$.

Higher Attacks

Usual algorithms:

Naive random walk: $O(p^{g(g+1)-4})$

Meet in the middle: $O(p^{g(g+1)-8})$.

Tani's claw finding quantum algorithm: $O(p^{g(g+1)-12})$.

Theorem (Costello–Smith (2020))

Let $A; A^0$ be SSPPAV over $\overline{\mathbb{F}}_p$ of dimension $g > 1$.

1. There exists a classical $\Theta(p^{g-1})$ algorithm which finds an isogeny $\phi : A \rightarrow A^0$ in $\mathcal{G}(\cdot; p)$.
2. There exists a quantum $\Theta(\sqrt{p^{g-1}})$ algorithm which finds an isogeny $\phi : A \rightarrow A^0$ in $\mathcal{G}(\cdot; p)$.

Genus 2 Implementation

Let's go through an implementation of the genus 2 SIDH algorithm, using values provided by Flynn{Ti.

Genus 2 Implementation

Let's go through an implementation of the genus 2 SIDH algorithm, using values provided by Flynn{Ti.

Choose $p = 2^{51}3^{32}$ $1 = 4172630516011578626876079341567$ (100 bit).

Genus 2 Implementation

Let's go through an implementation of the genus 2 SIDH algorithm, using values provided by Flynn{Ti.

Choose $p = 2^{51}3^{32} - 1 = 4172630516011578626876079341567$ (100 bit).

Base hyperelliptic curve $H = \mathbb{F}_{p^2}$ defined by

$$\begin{aligned} H : y^2 = & (380194068372159317574541564775i + 1017916559181277226571754002873)x^6 \\ & + (3642151710276608808804111504956i + 1449092825028873295033553368501)x^5 \\ & + (490668231383624479442418028296i + 397897572063105264581753147433)x^4 \\ & + (577409514474712448616343527931i + 1029071839968410755001691761655)x^3 \\ & + (4021089525876840081239624986822i + 3862824071831242831691614151192)x^2 \\ & + (2930679994619687403787686425153i + 1855492455663897070774056208936)x \\ & + 2982740028354478560624947212657i + 2106211304320458155169465303811 \end{aligned}$$

Genus 2 Implementation

Alice chooses her 12 random secret scalars:

$$\begin{array}{lll} 1 = 937242395764589; & 2 = 282151393547351; & 3 = 0; \\ 4 = 0; & 5 = 0; & 6 = 0; \\ 7 = 1666968036125619; & 8 = 324369560360356; & 9 = 0; \\ 10 = 0; & 11 = 0; & 12 = 0; \end{array}$$

Genus 2 Implementation

Alice chooses her 12 random secret scalars:

$$\begin{array}{lll} 1 = 937242395764589; & 2 = 282151393547351; & 3 = 0; \\ 4 = 0; & 5 = 0; & 6 = 0; \\ 7 = 1666968036125619; & 8 = 324369560360356; & 9 = 0; \\ 10 = 0; & 11 = 0; & 12 = 0; \end{array}$$

Bob chooses his 12 random secret scalars:

$$\begin{array}{lll} 1 = 103258914945647; & 2 = 1444900449480064; & 3 = 0; \\ 4 = 0; & 5 = 0; & 6 = 0; \\ 7 = 28000236972265; & 8 = 720020678656772; & 9 = 0; \\ 10 = 0; & 11 = 0; & 12 = 0; \end{array}$$

Genus 2 Implementation

Bob computes the genus 2 curve:

$$\begin{aligned}H_A : y^2 = & (3404703004587495821596176965058i + 403336181260435480105799382459)x^6 \\ & + (3001584086424762938062276222340i + 3110471904806922603655329247510)x^5 \\ & + (1017199310627230983511586463332i + 1599189698631433372650857544071)x^4 \\ & + (2469562012339092945398365678689i + 1154566472615236827416467624584)x^3 \\ & + (841874238658053023013857416200i + 422410815643904319729131959469)x^2 \\ & + (3507584227180426976109772052962i + 2331298266595569462657798736063)x \\ & + 2729816620520905175590758187019i + 3748704006645129000498563514734:\end{aligned}$$

Genus 2 Implementation

Alice computes the genus 2 curve:

$$\begin{aligned}H_B : y^2 = & (3434394689074752663579510896530i + 3258819610341997123576600332954)x^6 \\ & + (3350255113820895191389143565973i + 2681892489448659428930467220147)x^5 \\ & + (2958298818675004062047066758264i + 904769362079321055425076728309)x^4 \\ & + (2701255487608026975177181091075i + 787033120015012146142186182556)x^3 \\ & + (3523675811671092022491764466022i + 2804841353558342542840805561369)x^2 \\ & + (3238151513550798796238052565124i + 3437885792433773163395130700555)x \\ & + 1829327374163410097298853068766i + 3453489516944406316396271485172:\end{aligned}$$

Genus 2 Implementation

Using A , Alice computes the points $A(Q_1); A(Q_2); A(Q_3); A(Q_4)$ and sends this to Bob!

$$A(Q_1) = \begin{pmatrix} x^2 + (3464040394311932964693107348618i + 1234121484161567611101667399525)x \\ + 17895775393232773855271038385i + 3856858968014591645005318326985; \\ (2432835950855765586938146638349i + 3267484715622822051923177214055)x \\ + 985386137551789348760277138076i + 1179835886991851012234054275735 \end{pmatrix} \begin{matrix} 1 \\ \mathbb{C} \\ A \end{matrix}$$

$$A(Q_2) = \begin{pmatrix} x^2 + (363382700960978261088696293501i + 3499548729039922528103431054749)x \\ + 3832512523382547716418075195517i + 3364204966204284852762530333038; \\ (3043817101596607612186808885116i + 4027557567198565187096133171734)x \\ + 4087176631917166066356886198518i + 1327157646340760346840638146328 \end{pmatrix} \begin{matrix} 1 \\ \mathbb{C} \\ A \end{matrix}$$

$$A(Q_3) = \begin{pmatrix} x^2 + (3946684136660787881888285451015i + 1250236853749119184502604023717)x \\ + 3358152613483376587872867674703i + 467252201151076389055524809476; \\ (1562920784368105245499132757775i + 987920823075946850233644600497)x \\ + 1675005758282871337010798605079i + 1490924669195823363601763347629 \end{pmatrix} \begin{matrix} 1 \\ \mathbb{C} \\ A \end{matrix}$$

$$A(Q_4) = \begin{pmatrix} x^2 + (1629408242557750155729330759772i + 3235283387810139201773539373655)x \\ + 1341380669490368343450704316676i + 1454971022788254094961980229605; \\ (2393675986247524032663566872348i + 3412019204974086421616096641702)x \end{pmatrix} \begin{matrix} 1 \\ \mathbb{C} \\ A \end{matrix}$$

Genus 2 Implementation

Finally, Alice and Bob can both compute their common G2-invariants:

$$g_1 = 1055018150197573853947249198625i + 2223713843055934677989300194259;$$

$$g_2 = 819060580729572013508006537232i + 3874192400826551831686249391528;$$

$$g_3 = 1658885975351604494486138482883i + 3931354413698538292465352257393;$$

References



Bruin, N., Flynn, E.V., Testa, D. (2014)

Descent via $(3, 3)$ -isogeny on Jacobians of genus 2 curves.

Acta Arith. 165, no. 3, 201{223.



Cassels, J.W.S., Flynn, E.V. (1996)

Prolegomena to a middlebrow arithmetic of curves of genus 2.

London Mathematical Society Lecture Note Series, 230. Cambridge University Press, Cambridge.



Costello, C., Smith, B. (2020)

The supersingular isogeny problem in genus 2 and beyond.

Post-quantum cryptography, 151{168.



De Feo, L., Jao, D., Plût, J. (2014)

Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.

J. Math. Cryptol. 8, no. 3, 209{247.

References



Flynn, E.V., Ti, Y.B. (2019)
Genus two isogeny cryptography.
Lecture Notes in Comput. Sci., 11505.



Kunzweiler, S., Ti, Y.B., Weitkamper, C. (2022)
Secret keys in genus-2 SIDH.
Lecture Notes in Comput. Sci., 13203.



Milne, J.S. (1986)
Abelian varieties.
Arithmetic geometry, 103{150, Springer, New York.



Mumford, D. (1970)
Abelian varieties.
Tata Institute of Fundamental Research Studies in Mathematics, 5.

Thank you!

..and many thanks to Diana, Alexandros, Kenji, Maryam, Arshay, James, Katerina, Muhammad, and Alvaro for their wonderful talks, and with special thanks to Diana Mocanu for organising this study group!