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 $\Gamma_1(\ell, p)$ 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 $\ell \neq p$.

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.

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 $\approx \frac{p}{12}$ 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 $\approx \frac{p}{12}$ 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 $\approx \frac{p}{12}$ vertices.
- Every vertex has $\ell + 1$ neighbours.
- Ramanujan. (random walks of length $O(\log p)$ give (near) uniform distribution)

Elliptic isogeny graph

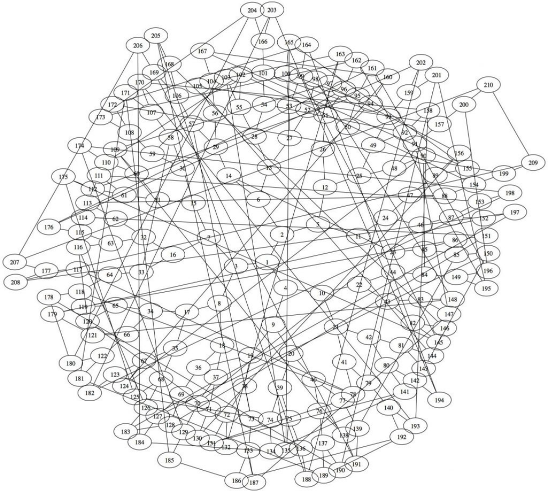

Figure: The 2-isogeny graph for $p = 2521$ (credit to Denis Charles, Microsoft Research).

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

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \dots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.
3. Sends $(E/A, \phi_A(Q_1), \phi_A(Q_2))$ to Bob!

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.
3. Sends $(E/A, \phi_A(Q_1), \phi_A(Q_2))$ to Bob!

Bob

1. Picks random $b \in \{0, 1, \ldots, 3^m - 1\}$.

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.
3. Sends $(E/A, \phi_A(Q_1), \phi_A(Q_2))$ to Bob!

Bob

1. Picks random $b \in \{0, 1, \ldots, 3^m - 1\}$.
2. Calculates $B := \langle Q_1 + [b]Q_2 \rangle$.

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.
3. Sends $(E/A, \phi_A(Q_1), \phi_A(Q_2))$ to Bob!

Bob

1. Picks random $b \in \{0, 1, \ldots, 3^m - 1\}$.
2. Calculates $B := \langle Q_1 + [b]Q_2 \rangle$.
3. Sends $(E/B, \phi_B(P_1), \phi_B(P_2))$ to Alice!

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.
3. Sends $(E/A, \phi_A(Q_1), \phi_A(Q_2))$ to Bob!
4. Calculates $A' := \langle \phi_B(P_1) + [a]\phi_B(P_2) \rangle$.

Bob

1. Picks random $b \in \{0, 1, \ldots, 3^m - 1\}$.
2. Calculates $B := \langle Q_1 + [b]Q_2 \rangle$.
3. Sends $(E/B, \phi_B(P_1), \phi_B(P_2))$ to Alice!

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.
3. Sends $(E/A, \phi_A(Q_1), \phi_A(Q_2))$ to Bob!
4. Calculates $A' := \langle \phi_B(P_1) + [a]\phi_B(P_2) \rangle$.
5. Computes shared secret key
   $s := j((E/B)/A')$

Bob

1. Picks random $b \in \{0, 1, \ldots, 3^m - 1\}$.
2. Calculates $B := \langle Q_1 + [b]Q_2 \rangle$.
3. Sends $(E/B, \phi_B(P_1), \phi_B(P_2))$ to Alice!

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.
3. Sends $(E/A, \phi_A(Q_1), \phi_A(Q_2))$ to Bob!
4. Calculates $A' := \langle \phi_B(P_1) + [a]\phi_B(P_2) \rangle$.
5. Computes shared secret key $s := j((E/B)/A')$

Bob

1. Picks random $b \in \{0, 1, \ldots, 3^m - 1\}$.
2. Calculates $B := \langle Q_1 + [b]Q_2 \rangle$.
3. Sends $(E/B, \phi_B(P_1), \phi_B(P_2))$ to Alice!
4. Calculates $B' := \langle \phi_A(Q_1) + [b]\phi_B(Q_2) \rangle$.

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.
3. Sends $(E/A, \phi_A(Q_1), \phi_A(Q_2))$ to Bob!
4. Calculates $A' := \langle \phi_B(P_1) + [a]\phi_B(P_2) \rangle$.
5. Computes shared secret key
   $s := j((E/B)/A')$

Bob

1. Picks random $b \in \{0, 1, \ldots, 3^m - 1\}$.
2. Calculates $B := \langle Q_1 + [b]Q_2 \rangle$.
3. Sends $(E/B, \phi_B(P_1), \phi_B(P_2))$ to Alice!
4. Calculates $B' := \langle \phi_A(Q_1) + [b]\phi_B(Q_2) \rangle$.
5. Computes shared secret key
   $s := j((E/A)/B')$

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.
3. Sends $(E/A, \phi_A(Q_1), \phi_A(Q_2))$ to Bob!
4. Calculates $A' := \langle \phi_B(P_1) + [a]\phi_B(P_2) \rangle$.
5. Computes shared secret key
   $s := j((E/B)/A')$

Bob

1. Picks random $b \in \{0, 1, \ldots, 3^m - 1\}$.
2. Calculates $B := \langle Q_1 + [b]Q_2 \rangle$.
3. Sends $(E/B, \phi_B(P_1), \phi_B(P_2))$ to Alice!
4. Calculates $B' := \langle \phi_A(Q_1) + [b]\phi_B(Q_2) \rangle$.
5. Computes shared secret key
   $s := j((E/A)/B')$

$$(E/A)/B' = (E/A)/\phi_A(B) \cong E/\langle A, B \rangle \cong (E/B)/\phi_B(A) = (E/B)/A'$$

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.
- Pick bases $\{P_1, P_2\}$ for $E[2^n]$ and $\{Q_1, Q_2\}$ for $E[3^m]$.

Alice

1. Picks random $a \in \{0, 1, \ldots, 2^n - 1\}$.
2. Calculates $A := \langle P_1 + [a]P_2 \rangle \subset E[2^n]$.
3. Sends $(E/A, \phi_A(Q_1), \phi_A(Q_2))$ to Bob!
4. Calculates $A' := \langle \phi_B(P_1) + [a]\phi_B(P_2) \rangle$.
5. Computes shared secret key $s := j((E/B)/A')$

Bob

1. Picks random $b \in \{0, 1, \ldots, 3^m - 1\}$.
2. Calculates $B := \langle Q_1 + [b]Q_2 \rangle$.
3. Sends $(E/B, \phi_B(P_1), \phi_B(P_2))$ to Alice!
4. Calculates $B' := \langle \phi_A(Q_1) + [b]\phi_B(Q_2) \rangle$.
5. Computes shared secret key $s := j((E/A)/B')$

$$(E/A)/B' = (E/A)/\phi_A(B) \cong E/\langle A, B \rangle \cong (E/B)/\phi_B(A) = (E/B)/A' \quad :)$$

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 $\mathrm{char} K \neq 2$) has affine 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 $\mathrm{char} K \neq 2$) has affine 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 $\mathrm{Jac}(C)$ (the **Jacobian** of C) of dimension g which parameterises $\mathrm{Pic}^0(C)$.

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 $\mathrm{char} K \neq 2$) has affine 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 $\mathrm{Jac}(C)$ (the **Jacobian** of C) of dimension g which parameterises $\mathrm{Pic}^0(C)$.
- Given an abelian variety A/K, there exists a **dual** abelian variety $A^\vee/K$ of the same dimension which parameterises $\mathrm{Pic}^0(A)$.

Abelian varieties recap

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

Abelian varieties recap

- A **polarisation** λ of an abelian variety A/K is an isogeny $\lambda : A \to A^\vee$ such that $\lambda = \lambda_{\mathcal{L}}$ $(a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1})$ 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** λ of an abelian variety A/K is an isogeny $\lambda : A \to A^\vee$ such that $\lambda = \lambda_{\mathcal{L}}$ $(a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1})$ for some ample divisor $\mathcal{L}$ of A.
- An abelian variety A/K is **principally polarised** if $\deg(\lambda) = 1$.
  Fact: Jacobians are principally polarisable (using theta divisors).

Abelian varieties recap

- A **polarisation** λ of an abelian variety A/K is an isogeny $\lambda : A \to A^\vee$ such that $\lambda = \lambda_{\mathcal{L}}$ $(a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1})$ for some ample divisor $\mathcal{L}$ 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 $\overline{K}$ to a product of supersingular elliptic curves $A \cong E_1 \times \cdots \times E_g$).

Abelian varieties recap

- A **polarisation** λ of an abelian variety A/K is an isogeny $\lambda : A \to A^\vee$ such that $\lambda = \lambda_{\mathcal{L}}$ $(a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1})$ for some ample divisor $\mathcal{L}$ 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 $\overline{K}$ to a product of supersingular elliptic curves $A \cong E_1 \times \cdots \times E_g$).
- Let m be coprime to $\mathrm{char}(K)$. The **Weil pairing** for A/K:

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

  satisfies the following properties:
  - $e(P+Q,R) = e(P,R)e(Q,R)$ and $e(P,Q+R) = e(P,Q)e(P,R)$
  - $e(P,P) = 1$ and $e(P,Q) = e(Q,P)^{-1}$
  - $e(P^\sigma, Q^\sigma) = e(P,Q)^\sigma$ for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Isogenies recap

- Given an isogeny $\phi : A \to A'$, there exists a **dual isogeny** $\hat{\phi} : \hat{A}' \to \hat{A}$.

Isogenies recap

- Given an isogeny $\phi : A \to A'$, there exists a **dual isogeny** $\hat{\phi} : \hat{A}' \to \hat{A}$.
- Given an isogeny $\phi : A \to A'$, there is a canonical isomorphism between $\ker(\widehat{\phi})$ and $\widehat{\ker(\phi)}$.

Isogenies recap

- Given an isogeny $\phi : A \to A'$, there exists a **dual isogeny** $\hat{\phi} : \hat{A}' \to \hat{A}$.
- Given an isogeny $\phi : A \to A'$, there is a canonical isomorphism between $\ker(\widehat{\phi})$ and $\widehat{\ker(\phi)}$.
- Given two PPAVs (A, λ) and (A', λ'), a **(polarised) isogeny** between PPAVs is an isogeny $\phi : A \to A'$ such that $\hat{\phi} \circ \lambda' \circ \phi = [d]\lambda$ for some d.

Isogenies recap

- Given an isogeny $\phi : A \to A'$, there exists a **dual isogeny** $\hat{\phi} : \hat{A}' \to \hat{A}$.
- Given an isogeny $\phi : A \to A'$, there is a canonical isomorphism between $\ker(\widehat{\phi})$ and $\widehat{\ker(\phi)}$.
- Given two PPAVs (A, λ) and (A', λ'), a **(polarised) isogeny** between PPAVs is an isogeny $\phi : A \to A'$ such that $\hat{\phi} \circ \lambda' \circ \phi = [d]\lambda$ 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 $e_m|_G = \mathrm{id}$ and G not properly contained in another isotropic subgroup $G' \subset A[m]$.

Isogenies recap

- Given an isogeny $\phi : A \to A'$, there exists a **dual isogeny** $\hat{\phi} : \hat{A}' \to \hat{A}$.
- Given an isogeny $\phi : A \to A'$, there is a canonical isomorphism between $\ker(\widehat{\phi})$ and $\widehat{\ker(\phi)}$.
- Given two PPAVs (A, λ) and (A', λ'), a **(polarised) isogeny** between PPAVs is an isogeny $\phi : A \to A'$ such that $\hat{\phi} \circ \lambda' \circ \phi = [d]\lambda$ 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 $e_m|_G = \mathrm{id}$ and G not properly contained in another isotropic subgroup $G' \subset A[m]$.
- Let $A/\mathbb{F}_q$ be a PPAV, and let $G \subset A(\mathbb{F}_q)$ be a proper subgroup. Then there exists a PPAV $A'/\mathbb{F}_q$ and an isogeny $\phi : A \to A'$ with kernel G if and only if G is maximal m-isotropic for some m.

Isogenies recap

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

Let A, A' be PPAVs of dimension d, and $\phi : A \to A'$ a (polarised) isogeny. Then ϕ is a $(\ell, \dots, \ell)$-**isogeny** if $\mathrm{ker}\phi \cong (\mathbb{Z}/\ell\mathbb{Z})^d$ (and $\mathrm{ker}\phi$ is maximal ℓ-isotropic).

Isogenies recap

$(\ell, \ldots, \ell)$-isogeny

Let A, A' be PPAVs of dimension d, and $\phi : A \to A'$ a (polarised) isogeny. Then ϕ is a $(\ell, \ldots, \ell)$-**isogeny** if $\ker\phi \cong (\mathbb{Z}/\ell\mathbb{Z})^d$ (and $\ker\phi$ is maximal ℓ-isotropic).

- $(\ell, \ldots, \ell)$-isogenies preserve superspeciality!

Isogenies recap

$(\ell, \ldots, \ell)$-isogeny

Let A, A' be PPAVs of dimension d, and $\phi : A \to A'$ a (polarised) isogeny. Then ϕ is a $(\ell, \ldots, \ell)$-**isogeny** if $\ker\phi \cong (\mathbb{Z}/\ell\mathbb{Z})^d$ (and $\ker\phi$ is maximal ℓ-isotropic).

- $(\ell, \ldots, \ell)$-isogenies preserve superspeciality!

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

Let A be a PPAS. A **Richelot isogeny** $\phi : A \to A/G$ is an isogeny where $G \cong (\mathbb{Z}/2\mathbb{Z})^2$ 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 $\phi : J(C) \to J(C')$ where

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

  Here, $h_i(x) := \delta^{-1}(g'_{i+1}(x)g_{i+2}(x) - g_{i+1}(x)g'_{i+2}(x))$ (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 $\delta = -3$ (and $\delta^{-1} = 4$) and

$$
\begin{aligned}
h_1(x) &= g_2(x)'g_3(x) - g_2(x)g_3(x)' = 9x^2 - 6x - 9 \\
h_2(x) &= g_3(x)'g_1(x) - g_3(x)g_1(x)' = x^2 + 1 \\
h_3(x) &= g_1(x)'g_2(x) - g_1(x)g_2(x)' = -x^2 + 2
\end{aligned}
$$

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 $\delta = -3$ (and $\delta^{-1} = 4$) and

$$\begin{aligned} h_1(x) &= g_2(x)'g_3(x) - g_2(x)g_3(x)' = 9x^2 - 6x - 9 \\ h_2(x) &= g_3(x)'g_1(x) - g_3(x)g_1(x)' = x^2 + 1 \\ h_3(x) &= g_1(x)'g_2(x) - g_1(x)g_2(x)' = -x^2 + 2 \end{aligned}$$

- Thus $J(C)$ is $(2,2)$-isogeneous to $J(C')$ where

$$C' : y^2 = (9x^2 - 6x - 9)(x^2 + 1)(x^2 - 2).$$

$(3,3)$-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 $y^2 = G(x)^2 + \lambda H(x)^3$ 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 $y^2 = G(x)^2 + \lambda H(x)^3$ 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 $\mathcal{J}ac(C_{rst})$ is $(3,3)$-isogenous to $\mathcal{J}ac(C')$ where C'/K is the genus 2 curve $-3y^2 = G'(x)^2 + 4\Delta st H'(x)^3$ and where

$$G'(x) = \Delta((s - st - 1)x^3 + 3s(r-t)x^2 + 3rs(r-t)x + (r^3 s - st^2 - t)),$$

$$H'(x) = (r-1)(rs - st - 1)x^2 + (r^3 s - 2r^2 s + rst + r - st^2 + st - t)x - (r^2 - t)(rs - st - 1$$

$$\Delta = r^6 s^2 - 6r^4 s^2 t - 3r^4 s + 2r^3 s^2 t^2 + 2r^3 s^2 t + 3r^3 st + r^3 s + r^3 + 9r^2 s^2 t^2 + 6r^2 st - 6rs^2$$

Maximal isotropic subgroups

Theorem

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

Proof:

Maximal isotropic subgroups

Theorem

Let A be a PPAS, let $G \subset A[\ell^n]$ be a maximal ℓ^n-isotropic subgroup. Then $G \cong C_{\ell^n} \times C_{\ell^{n-k}} \times C_{\ell^k}$ 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 $a \geq b \geq c \geq d$.

Maximal isotropic subgroups

Theorem

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

Maximal isotropic subgroups

Theorem

Let A be a PPAS, let $G \subset A[\ell^n]$ be a maximal ℓ^n-isotropic subgroup. Then $G \cong C_{\ell^n} \times C_{\ell^{n-k}} \times C_{\ell^k}$ 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 $\phi : A \to A'$ be an isogeny with kernel G. Then as $\ker(\hat{\phi} \circ \phi) = C_{\ell^n}^4$, this implies the kernel of $\widehat{\phi}$ 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 $G \subset A[\ell^n]$ be a maximal ℓ^n-isotropic subgroup. Then $G \cong C_{\ell^n} \times C_{\ell^{n-k}} \times C_{\ell^k}$ 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 $\phi : A \to A'$ be an isogeny with kernel G. Then as $\ker(\hat{\phi} \circ \phi) = C_{\ell^n}^4$, this implies the kernel of $\widehat{\phi}$ is
$$C_{\ell^{n-a}} \times C_{\ell^{n-b}} \times C_{\ell^{n-c}} \times C_{\ell^{n-d}}$$
- As both A and A' are principally polarised ($A \cong \hat{A}$ and $A' \cong \hat{A}'$), thus $G \cong \ker(\hat{\phi})$.

Maximal isotropic subgroups

Theorem

Let A be a PPAS, let $G \subset A[\ell^n]$ be a maximal ℓ^n-isotropic subgroup. Then $G \cong C_{\ell^n} \times C_{\ell^{n-k}} \times C_{\ell^k}$ 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 $\phi : A \to A'$ be an isogeny with kernel G. Then as $\ker(\hat{\phi} \circ \phi) = C_{\ell^n}^4$, this implies the kernel of $\widehat{\phi}$ is
$$C_{\ell^{n-a}} \times C_{\ell^{n-b}} \times C_{\ell^{n-c}} \times C_{\ell^{n-d}}$$
- As both A and A' are principally polarised ($A \cong \hat{A}$ and $A' \cong \hat{A}'$), thus $G \cong \ker(\hat{\phi})$.
- 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 $\Gamma_2(\ell, p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised abelian surfaces over $\overline{\mathbb{F}}_p$, and whose edges are (ℓ, ℓ)-isogenies, for a prime $\ell \neq p$.

Genus 2 isogeny graph

Genus 2 isogeny graph

Let p be prime. Define $\Gamma_2(\ell, p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised abelian surfaces over $\overline{\mathbb{F}}_p$, and whose edges are (ℓ, ℓ)-isogenies, for a prime $\ell \neq p$.

- Graph is connected.

Genus 2 isogeny graph

Genus 2 isogeny graph

Let p be prime. Define $\Gamma_2(\ell, p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised abelian surfaces over $\overline{\mathbb{F}}_p$, and whose edges are (ℓ, ℓ)-isogenies, for a prime $\ell \neq p$.

- Graph is connected.
- Graph has $\approx \frac{p^3}{2880}$ vertices.

Genus 2 isogeny graph

Genus 2 isogeny graph

Let p be prime. Define $\Gamma_2(\ell, p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised abelian surfaces over $\overline{\mathbb{F}}_p$, and whose edges are (ℓ, ℓ)-isogenies, for a prime $\ell \neq p$.

- Graph is connected.
- Graph has $\approx \frac{p^3}{2880}$ vertices.
- Every vertex has $(\ell^2 + 1)(\ell + 1)$ neighbours.

Genus 2 isogeny graph

Genus 2 isogeny graph

Let p be prime. Define $\Gamma_2(\ell, p)$ to be the graph whose vertices are isomorphism classes of superspecial principally polarised abelian surfaces over $\overline{\mathbb{F}}_p$, and whose edges are (ℓ, ℓ)-isogenies, for a prime $\ell \neq p$.

- Graph is connected.
- Graph has $\approx \frac{p^3}{2880}$ vertices.
- Every vertex has $(\ell^2 + 1)(\ell + 1)$ neighbours.
- Not quite Ramanujan, but close enough.

Genus 2 isogeny graph

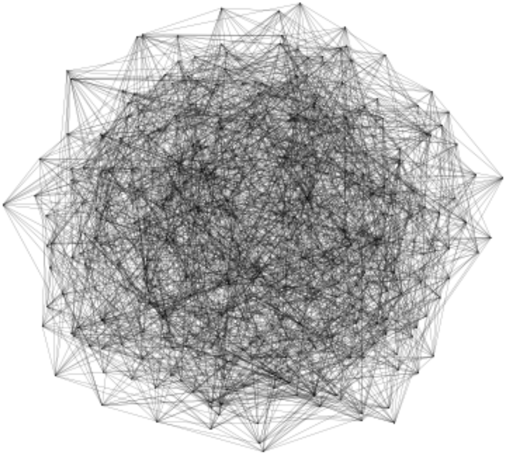

Figure: The (2,2)-isogeny graph for $p = 97$.

Genus 2 isogeny graph

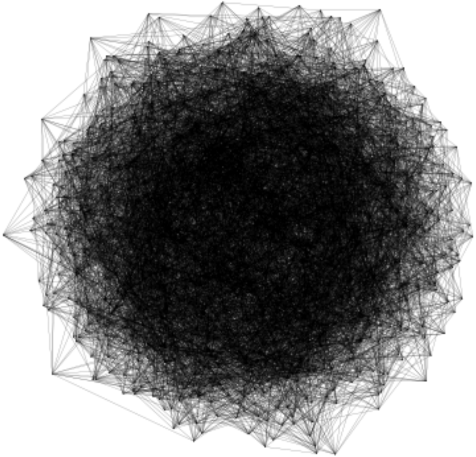

Figure: The (2,2)-isogeny graph for $p = 151$.

Genus 2 isogeny graph

Theorem

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

Proof:

Genus 2 isogeny graph

Theorem

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

Proof:

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

Genus 2 isogeny graph

Theorem

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

Proof:

- As the kernel of any isogeny $\phi : A \to A'$ corresponds to some maximal isotropic subgroup, it suffices to count the number of maximal ℓ-isotropic subgroups of $A[\ell]$ isomorphic to C_ℓ^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 $\langle a, b \rangle \cong C_\ell^2$ is maximal ℓ-isotropic.

Genus 2 isogeny graph

Theorem

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

Proof:

- As the kernel of any isogeny $\phi : A \to A'$ corresponds to some maximal isotropic subgroup, it suffices to count the number of maximal ℓ-isotropic subgroups of $A[\ell]$ isomorphic to C_ℓ^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 $\langle a, b \rangle \cong C_\ell^2$ is maximal ℓ-isotropic.
- Let

$$a = a_1P_1 + a_2P_2 + a_3P_3 + a_4P_4 \quad \text{for some } a_i \in \{0, 1, \ldots, \ell-1\},$$
$$b = b_1P_1 + b_2P_2 + b_3P_3 + b_4P_4 \quad \text{for some } b_i \in \{0, 1, \ldots, \ell-1\}.$$

Genus 2 isogeny graph

Theorem

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

Proof:

- As the kernel of any isogeny $\phi : A \to A'$ corresponds to some maximal isotropic subgroup, it suffices to count the number of maximal ℓ-isotropic subgroups of $A[\ell]$ isomorphic to C_ℓ^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 $\langle a, b \rangle \cong C_\ell^2$ is maximal ℓ-isotropic.
- Let

$$a = a_1 P_1 + a_2 P_2 + a_3 P_3 + a_4 P_4 \quad \text{for some } a_i \in \{0, 1, \ldots, \ell - 1\},$$
$$b = b_1 P_1 + b_2 P_2 + b_3 P_3 + b_4 P_4 \quad \text{for some } b_i \in \{0, 1, \ldots, \ell - 1\}.$$

- 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:

$$\begin{aligned} e_\ell(a,b) = {} & e_\ell(P_1,P_2)^{a_1b_2 - a_2b_1} e_\ell(P_1,P_3)^{a_1b_3 - a_3b_1} e_\ell(P_1,P_4)^{a_1b_4 - a_4b_1} \\ & \cdot e_\ell(P_2,P_3)^{a_2b_3 - a_3b_2} e_\ell(P_2,P_4)^{a_2b_4 - a_4b_2} e_\ell(P_3,P_4)^{a_3b_4 - a_4b_3} = 1 \end{aligned}$$

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:

$$\begin{aligned} e_\ell(a,b) = {} & e_\ell(P_1,P_2)^{a_1b_2-a_2b_1} e_\ell(P_1,P_3)^{a_1b_3-a_3b_1} e_\ell(P_1,P_4)^{a_1b_4-a_4b_1} \\ & \cdot e_\ell(P_2,P_3)^{a_2b_3-a_3b_2} e_\ell(P_2,P_4)^{a_2b_4-a_4b_2} e_\ell(P_3,P_4)^{a_3b_4-a_4b_3} = 1 \end{aligned}$$

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

$$\begin{aligned} b_4(\alpha_{1,4}a_1 + \alpha_{2,4}a_2 + \alpha_{3,4}a_3) \equiv {} & \alpha_{1,2}(a_2b_1 - a_1b_2) + \alpha_{1,3}(a_3b_1 - a_1b_3) \\ & + \alpha_{2,3}(a_3b_2 - a_2b_3) + \alpha_{1,4}a_4b_1 \\ & + \alpha_{2,4}a_4b_2 + \alpha_{3,4}a_4b_3 \pmod{\ell} \end{aligned}$$

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:

$$\begin{aligned} e_\ell(a, b) = {} & e_\ell(P_1, P_2)^{a_1 b_2 - a_2 b_1} e_\ell(P_1, P_3)^{a_1 b_3 - a_3 b_1} e_\ell(P_1, P_4)^{a_1 b_4 - a_4 b_1} \\ & \cdot e_\ell(P_2, P_3)^{a_2 b_3 - a_3 b_2} e_\ell(P_2, P_4)^{a_2 b_4 - a_4 b_2} e_\ell(P_3, P_4)^{a_3 b_4 - a_4 b_3} = 1 \end{aligned}$$

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

$$\begin{aligned} b_4(\alpha_{1,4} a_1 + \alpha_{2,4} a_2 + \alpha_{3,4} a_3) \equiv {} & \alpha_{1,2}(a_2 b_1 - a_1 b_2) + \alpha_{1,3}(a_3 b_1 - a_1 b_3) \\ & + \alpha_{2,3}(a_3 b_2 - a_2 b_3) + \alpha_{1,4} a_4 b_1 \\ & + \alpha_{2,4} a_4 b_2 + \alpha_{3,4} a_4 b_3 \pmod{\ell} \end{aligned}$$

- If $\alpha_{1,4} a_1 + \alpha_{2,4} a_2 + \alpha_{3,4} a_3 \not\equiv 0 \pmod{\ell}$, 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 $b \notin \langle a \rangle$, we must avoid $\ell - 1$ elements. This gives a total of $\ell^3 - \ell$ choices for b.

Genus 2 isogeny graph

- But to ensure $b \notin \langle a \rangle$, we must avoid $\ell - 1$ elements. This gives a total of $\ell^3 - \ell$ choices for b.
- Thus, the number of pairs $a, b \in A[\ell]$ such that that $\langle a, b \rangle \cong C_\ell^2$ is maximal ℓ-isotropic is $(\ell^4 - 1)(\ell^3 - \ell)$.

Genus 2 isogeny graph

- But to ensure $b \notin \langle a \rangle$, we must avoid $\ell - 1$ elements. This gives a total of $\ell^3 - \ell$ choices for b.
- Thus, the number of pairs $a, b \in A[\ell]$ such that that $\langle a, b \rangle \cong C_\ell^2$ is maximal ℓ-isotropic is $(\ell^4 - 1)(\ell^3 - \ell)$.
- For any such subgroup $C_\ell \times C_\ell$, there are $(\ell^2 - 1)(\ell^2 - \ell)$ generating pairs.

Genus 2 isogeny graph

- But to ensure $b \notin \langle a \rangle$, we must avoid $\ell - 1$ elements. This gives a total of $\ell^3 - \ell$ choices for b.
- Thus, the number of pairs $a, b \in A[\ell]$ such that that $\langle a, b \rangle \cong C_\ell^2$ is maximal ℓ-isotropic is $(\ell^4 - 1)(\ell^3 - \ell)$.
- For any such subgroup $C_\ell \times C_\ell$, there are $(\ell^2 - 1)(\ell^2 - \ell)$ generating pairs.
- Thus, the total number of maximal isotropic $C_\ell \times C_\ell$ subgroups of $A[\ell]$ is

$$\frac{(\ell^4 - 1)(\ell^3 - \ell)}{(\ell^2 - 1)(\ell^2 - \ell)} = (\ell^2 + 1)(\ell + 1).$$

$\square$

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. $H_0 : y^2 = x^6 + 1$.
  - $\mathrm{Jac}(H_0)$ 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. $H_0 : y^2 = x^6 + 1$.
    - $\mathrm{Jac}(H_0)$ is superspecial as it is double cover of $y^2 = x^3 + 1$.
    - Take a random sequence of Richelot isogenies $H_0 \to H_1 \to \cdots \to H$ (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. $H_0 : y^2 = x^6 + 1$.
  - $\mathrm{Jac}(H_0)$ is superspecial as it is double cover of $y^2 = x^3 + 1$.
  - Take a random sequence of Richelot isogenies $H_0 \to H_1 \to \cdots \to H$ (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 $(a_1, a_2, \ldots, a_{12}) \subset \{0, 1, \ldots, 2^n - 1\}$.

Genus 2 SIDH

Round 1: Alice

1. Alice chooses 12 secret random scalars $(a_1, a_2, \ldots, a_{12}) \subset \{0, 1, \ldots, 2^n - 1\}$.
2. She computes the subgroup $A \subset J_H[2^n]$, given by

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

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

Genus 2 SIDH

Round 1: Alice

1. Alice chooses 12 secret random scalars $(a_1, a_2, \ldots, a_{12}) \subset \{0, 1, \ldots, 2^n - 1\}$.
2. She computes the subgroup $A \subset J_H[2^n]$, given by

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

   The scalars (a_i) are chosen such that A is maximal isotropic subgroup of order ℓ^{2n}.
3. Alice sends the tuple $(J_H/A, \phi_A(Q_1), \phi_A(Q_2), \phi_A(Q_3), \phi_A(Q_4))$ to Bob!

Genus 2 SIDH

How should Alice pick scalars $a_1, a_2, \ldots, a_{12}$?

Genus 2 SIDH

How should Alice pick scalars $a_1, a_2, \ldots, a_{12}$?

- Let

$$
\begin{aligned}
R_1 &= a_1 P_1 + a_2 P_2 + a_3 P_3 + a_4 P_4 \\
R_2 &= a_5 P_1 + a_6 P_2 + a_7 P_3 + a_8 P_4 \\
R_3 &= a_9 P_1 + a_{10} P_2 + a_{11} P_3 + a_{12} P_4
\end{aligned}
$$

Genus 2 SIDH

How should Alice pick scalars $a_1, a_2, \ldots, a_{12}$?

- 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 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 $a_1, a_2, \ldots, a_{12}$?

- 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 ℓ^n-isotropic subgroup of $J_H[2^n]$, i.e. must choose generators R_1, R_2, R_3 such that $e_{2^n}(R_1, R_2) = e_{2^n}(R_1, R_3) = e_{2^n}(R_2, R_3) = 1$
- As shown before, this is equivalent to choosing (a_i) which satisfy a system of linear congruences, i.e. we require

$$e(R_1, R_2) = e(P_1, P_2)^{a_1 a_6 - a_2 a_5} e(P_1, P_3)^{a_1 a_7 - a_3 a_5} e(P_1, P_4)^{a_1 a_8 - a_4 a_5} \cdot e(P_2, P_3)^{a_2 a_7 - a_3 a_6} e(P_2, P_4)^{a_2 a_8 - a_4 a_6} e(P_3, P_4)^{a_3 a_8 - a_4 a_7} = 1.$$

Genus 2 SIDH

Alice can do the following:

Genus 2 SIDH

Alice can do the following:

(i) Calculate the values $\alpha_{i,j} \pmod{2^n}$ such that $e_{2^n}(P_i, P_j) = e_{2^n}(P_1, P_2)^{\alpha_{i,j}}$.

Genus 2 SIDH

Alice can do the following:

(i) Calculate the values $\alpha_{i,j} \pmod{2^n}$ such that $e_{2^n}(P_i, P_j) = e_{2^n}(P_1, P_2)^{\alpha_{i,j}}$.

(ii) Pick random $a_1, a_2, a_3, a_4 \in \{0, 1, \ldots, 2^n - 1\}$ such that at least one of the four is odd.

Genus 2 SIDH

Alice can do the following:

(i) Calculate the values $\alpha_{i,j} \pmod{2^n}$ such that $e_{2^n}(P_i, P_j) = e_{2^n}(P_1, P_2)^{\alpha_{i,j}}$.

(ii) Pick random $a_1, a_2, a_3, a_4 \in \{0, 1, \ldots, 2^n - 1\}$ such that at least one of the four is odd.

(iii) Pick a random $k \in \{0, 1, \ldots, n\}$, and pick random a_5, a_6, a_7, a_8 such that

$$\begin{aligned} &a_1 a_6 - a_2 a_5 + \alpha_{1,3}(a_1 a_7 - a_3 a_5) + \alpha_{1,4}(a_1 a_8 - a_4 a_5) \\ &+ \alpha_{2,3}(a_2 a_7 - a_3 a_6) + \alpha_{2,4}(a_2 a_8 - a_4 a_6) + \alpha_{3,4}(a_3 a_8 - a_4 a_7) \equiv 0 \mod 2^k \end{aligned}$$

Genus 2 SIDH

Alice can do the following:

(i) Calculate the values $\alpha_{i,j} \pmod{2^n}$ such that $e_{2^n}(P_i, P_j) = e_{2^n}(P_1, P_2)^{\alpha_{i,j}}$.

(ii) Pick random $a_1, a_2, a_3, a_4 \in \{0, 1, \ldots, 2^n - 1\}$ such that at least one of the four is odd.

(iii) Pick a random $k \in \{0, 1, \ldots, n\}$, and pick random a_5, a_6, a_7, a_8 such that

$$\begin{aligned} &a_1 a_6 - a_2 a_5 + \alpha_{1,3}(a_1 a_7 - a_3 a_5) + \alpha_{1,4}(a_1 a_8 - a_4 a_5) \\ &+ \alpha_{2,3}(a_2 a_7 - a_3 a_6) + \alpha_{2,4}(a_2 a_8 - a_4 a_6) + \alpha_{3,4}(a_3 a_8 - a_4 a_7) \equiv 0 \mod 2^k \end{aligned}$$

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

$$\begin{aligned} &a_1 a_{10} - a_2 a_9 + \alpha_{1,3}(a_1 a_{11} - a_3 a_9) + \alpha_{1,4}(a_1 a_{12} - a_4 a_9) \\ &+ \alpha_{2,3}(a_2 a_{11} - a_3 a_{10}) + \alpha_{2,4}(a_2 a_{12} - a_4 a_{10}) + \alpha_{3,4}(a_3 a_{12} - a_4 a_{11}) \equiv 0 \mod 2^{n-k} \end{aligned}$$

Genus 2 SIDH

Round 1: Bob

Genus 2 SIDH

Round 1: Bob

1. Bob also chooses 12 secret random scalars $(b_1, b_2, \ldots, b_{12}) \subset \{0, 1, \ldots, 3^m - 1\}$.

Genus 2 SIDH

Round 1: Bob

1. Bob also chooses 12 secret random scalars $(b_1, b_2, \ldots, b_{12}) \subset \{0, 1, \ldots, 3^m - 1\}$.
2. He computes the group $B \subset J_H[3^m]$, given by

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

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 $(b_1, b_2, \dots, b_{12}) \subset \{0, 1, \dots, 3^m - 1\}$.
2. He computes the group $B \subset J_H[3^m]$, given by

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

   Again, the scalars (b_i) must be chosen such that B is maximal isotropic subgroup of order 3^{2m}.
3. Bobs sends the tuple $(J_H/B, \phi_B(P_1), \phi_B(P_2), \phi_B(P_3), \phi_B(P_4))$ to Alice!

Genus 2 SIDH

Round 2: Alice

Genus 2 SIDH

Round 2: Alice

4. Alice receives Bob's tuple and calculates:

$$
\begin{aligned}
A' := \langle\, & a_1\phi_B(P_1) + a_2\phi_B(P_2) + a_3\phi_B(P_3) + a_4\phi_B(P_4), \\
& a_5\phi_B(P_1) + a_6\phi_B(P_2) + a_7\phi_B(P_3) + a_8\phi_B(P_4), \\
& a_9\phi_B(P_1) + a_{10}\phi_B(P_2) + a_{11}\phi_B(P_3) + a_{12}\phi_B(P_4)\rangle.
\end{aligned}
$$

Genus 2 SIDH

Round 2: Alice

4. Alice receives Bob's tuple and calculates:

$$\begin{aligned} A' := \langle & a_1\phi_B(P_1) + a_2\phi_B(P_2) + a_3\phi_B(P_3) + a_4\phi_B(P_4), \\ & a_5\phi_B(P_1) + a_6\phi_B(P_2) + a_7\phi_B(P_3) + a_8\phi_B(P_4), \\ & a_9\phi_B(P_1) + a_{10}\phi_B(P_2) + a_{11}\phi_B(P_3) + a_{12}\phi_B(P_4)\rangle. \end{aligned}$$

5. Alice thus has the isogeny $\phi_{A'} : J_H/B \to (J_H/B)/A'$, and can compute the G2 invariants of $(J_H/B)/A'$.

Genus 2 SIDH

Round 2: Bob

Genus 2 SIDH

Round 2: Bob

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

$$
\begin{aligned}
B' := \langle & b_1\phi_A(Q_1) + b_2\phi_A(Q_2) + b_3\phi_A(Q_3) + b_4\phi_A(Q_4), \\
& b_5\phi_A(Q_1) + b_6\phi_A(Q_2) + b_7\phi_A(Q_3) + b_8\phi_A(Q_4), \\
& b_9\phi_A(Q_1) + b_{10}\phi_A(Q_2) + b_{11}\phi_A(Q_3) + b_{12}\phi_A(Q_4)\rangle.
\end{aligned}
$$

Genus 2 SIDH

Round 2: Bob

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

$$\begin{aligned} B' := \big\langle & b_1\phi_A(Q_1) + b_2\phi_A(Q_2) + b_3\phi_A(Q_3) + b_4\phi_A(Q_4), \\ & b_5\phi_A(Q_1) + b_6\phi_A(Q_2) + b_7\phi_A(Q_3) + b_8\phi_A(Q_4), \\ & b_9\phi_A(Q_1) + b_{10}\phi_A(Q_2) + b_{11}\phi_A(Q_3) + b_{12}\phi_A(Q_4)\big\rangle. \end{aligned}$$

5. Bob thus has the isogeny $\phi_{B'} : J_H/A \to (J_H/A)/B'$, and can compute the G2 invariants of $(J_H/A)/B'$.

Genus 2 SIDH

Round 2: Bob

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

$$\begin{aligned} B' := \langle & b_1\phi_A(Q_1) + b_2\phi_A(Q_2) + b_3\phi_A(Q_3) + b_4\phi_A(Q_4), \\ & b_5\phi_A(Q_1) + b_6\phi_A(Q_2) + b_7\phi_A(Q_3) + b_8\phi_A(Q_4), \\ & b_9\phi_A(Q_1) + b_{10}\phi_A(Q_2) + b_{11}\phi_A(Q_3) + b_{12}\phi_A(Q_4)\rangle. \end{aligned}$$

5. Bob thus has the isogeny $\phi_{B'} : J_H/A \to (J_H/A)/B'$, and can compute the G2 invariants of $(J_H/A)/B'$.

As $(J_H/A)/B' = (J_H/A)/\phi_A(B) \cong J_H/\langle A, B\rangle \cong (J_H/B)/\phi_B(A) = (J_H/B)/A'$, 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' two superspecial p.p. abelian surfaces over $\mathbb{F}_{p^2}$. Find an isogeny $\phi : A \to A'$.

Security

Isogeny finding problem

Let p be a prime, and A, A' two superspecial p.p. abelian surfaces over $\mathbb{F}_{p^2}$. Find an isogeny $\phi : A \to A'$.

Algorithms:

- Brute force exhaustive search: $O(\sqrt{p^3})$.

Security

Isogeny finding problem

Let p be a prime, and A, A' two superspecial p.p. abelian surfaces over $\mathbb{F}_{p^2}$. Find an isogeny $\phi : A \to A'$.

Algorithms:

- Brute force exhaustive search: $O(\sqrt{p^3})$.
- Meet in the middle search: $O(\sqrt[4]{p^3})$.

Security

Isogeny finding problem

Let p be a prime, and A, A' two superspecial p.p. abelian surfaces over $\mathbb{F}_{p^2}$. Find an isogeny $\phi : A \to A'$.

Algorithms:

- Brute force exhaustive search: $O(\sqrt{p^3})$.
- Meet in the middle search: $O(\sqrt[4]{p^3})$.
- (Quantum) Tani's claw finding algorithm: $O(\sqrt[6]{p^3})$
  - Claw problem: Given two functions $f : A \to C$ and $g : B \to C$, find a pair (a, b) such that $f(a) = g(b)$.

Security

Adaptive Attack:

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

Security

Adaptive Attack:

- Let's assume Alice uses the same secret key $(a_1, \ldots, a_{12})$ 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.

Security

Adaptive Attack:

- Let's assume Alice uses the same secret key $(a_1, \ldots, a_{12})$ 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 $(\phi_B(P_1), \phi_B(P_2), \phi_B(P_3), \phi_B([2^{n-1}]P_4 + P_4))$ 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 $(a_1, \ldots, a_{12})$ 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 $(\phi_B(P_1), \phi_B(P_2), \phi_B(P_3), \phi_B([2^{n-1}]P_4 + P_4))$ 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 $(a_1, \ldots, a_{12})$ 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 $(\phi_B(P_1), \phi_B(P_2), \phi_B(P_3), \phi_B([2^{n-1}]P_4 + P_4))$ 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 (a_i) could perform a *loop-abort fault injection* attack.

Security

Fault Attack:

- An attacker with physical access to a device using Alice's private key (a_i) 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 $J_H \to J_H/A$, and instead compute the intermediate PPAS $J_H/\langle 2^{n-k}(a_1 P_1 + \dots)\rangle$ for some k.

Security

Fault Attack:

- An attacker with physical access to a device using Alice's private key (a_i) 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 $J_H \to J_H/A$, and instead compute the intermediate PPAS $J_H/\langle 2^{n-k}(a_1P_1 + \dots)\rangle$ 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 $\Gamma_g(\ell, p)$ 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 $(\ell, \ldots, \ell)$-isogenies, for a prime $\ell \neq p$.

Higher Isogenies

Genus g isogeny graph

Let p be prime. Define $\Gamma_g(\ell, p)$ 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 $(\ell, \ldots, \ell)$-isogenies, for a prime $\ell \neq p$.

- Graph is connected (Jordan–Zaytman).

Higher Isogenies

Genus g isogeny graph

Let p be prime. Define $\Gamma_g(\ell, p)$ 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 $(\ell, \ldots, \ell)$-isogenies, for a prime $\ell \neq p$.

- Graph is connected (Jordan–Zaytman).
- Graph has $O(p^{g(g+1)/2})$ vertices.

Higher Isogenies

Genus g isogeny graph

Let p be prime. Define $\Gamma_g(\ell, p)$ 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 $(\ell, \dots, \ell)$-isogenies, for a prime $\ell \neq p$.

- Graph is connected (Jordan–Zaytman).
- Graph has $O(p^{g(g+1)/2})$ vertices.
- Every vertex has $N_g(\ell)$ neighbours, where $N_g(\ell)$ is a polynomial in ℓ of degree $g(g+1)/2$:

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

Higher Isogenies

Genus g isogeny graph

Let p be prime. Define $\Gamma_g(\ell, p)$ 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 $(\ell, \ldots, \ell)$-isogenies, for a prime $\ell \neq p$.

- Graph is connected (Jordan–Zaytman).
- Graph has $O(p^{g(g+1)/2})$ vertices.
- Every vertex has $N_g(\ell)$ neighbours, where $N_g(\ell)$ is a polynomial in ℓ of degree $g(g+1)/2$:

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

- Not Ramanujan in general (Jordan–Zaytman), 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' be SSPPAV over $\overline{\mathbb{F}}_p$ of dimension $g > 1$.

1. *There exists a classical $\widetilde{O}(p^{g-1})$ algorithm which finds an isogeny $\phi : A \to A'$ in $\Gamma_g(\ell, p)$.*
2. *There exists a quantum $\widetilde{O}(\sqrt{p^{g-1}})$ algorithm which finds an isogeny $\phi : A \to A'$ in $\Gamma_g(\ell, p)$.*

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 $p = 2^{51}3^{32} - 1 = 417263051601157862687607934156 7$ (100 bit).
- Base hyperelliptic curve $H/\mathbb{F}_{p^2}$ defined by

$$
\begin{aligned}
H : y^2 = {} & (380194068372159317574541564775i + 1017916559181277226571754002873)x^6 \\
& + (3642151710276608808804111504956i + 1449092825028873295033553368501)x^5 \\
& + (490668231383624479442418028296i + 3978975720631052645817531474 33)x^4 \\
& + (577409514474712448616343527931i + 1029071839968410755001691761655)x^3 \\
& + (4021089525876840081239624986822i + 3862824071831242831691614151192)x^2 \\
& + (2930679994619687403787686425153i + 1855492455663897070774056208936)x \\
& + 2982740028354478560624947212657i + 2106211304320458155169465303811
\end{aligned}
$$

Genus 2 Implementation

Generators $\{P_1, P_2, P_3, P_4\}$ for the torsion subgroup $J_H[2^{51}]$:

$$P_1 = \begin{pmatrix} x^2 + (264326874493579662529366972622 7i + 1373559437243573104036867095531)x \\ +2040766263472741296629084172357i + 4148336987880572074205999666055, \\ +(2643644763015937217035303914167i + 3102052689781182995044090081179)x \\ +1813936678851222746202596525186i + 3292045648641130919333133017218 \end{pmatrix},$$

$$P_2 = \begin{pmatrix} x^2 + (1506120079909263217492664325998i + 1228415755183185090469788608852)x \\ +5109408167235382100244130228 14i + 3259278052139309431266216461 92, \\ +(1580781382037244392536803165134i + 3887834922720954573750149446163)x \\ +1675733503935551369607524150 82i + 1225135781040742113572860497457 \end{pmatrix},$$

$$P_3 = \begin{pmatrix} x^2 + (3505781767879186878832918134439i + 1904272753181081852523334980136)x \\ +6469795898834613232809063389 62i + 4034664704609474610987965706 90, \\ +(3113113466362205793505243872 79i + 1018806370582980709002197493273)x \\ +1408004869895332587263994799989i + 1849826149725693312283086888829 \end{pmatrix},$$

$$P_4 = \begin{pmatrix} x^2 + (2634314786447819510080659494014i + 7254063357492780530102393527 2)x \\ +1531966532163723578428827143067i + 1430299038689444680071540958109, \\ +(3957136023963064340486029724124i + 3043482304086144567096978137 20)x \end{pmatrix}.$$

Genus 2 Implementation

Generators $\{Q_1, Q_2, Q_3, Q_4\}$ for the torsion subgroup $J_H[3^{32}]$:

$$Q_1 = \begin{pmatrix} x^2 + (2630852063481114424941031847450i + 6619970040259422444839947486 7)x \\ +4973004886751519319702156870 05i + 7595632336168655095030949639 84, \\ +(1711990417626011964235368995795i + 3370542528225682591775373090846)x \\ +2409246960430353503520175176754i + 1486115372404013153540282992605 \end{pmatrix},$$

$$Q_2 = \begin{pmatrix} x^2 + (9504328296174436964757725518 84i + 3809766229231883691707469450961)x \\ +1293886731023444677607106763783i + 2152044083269016653158588262237, \\ +(3613765124982997852345558006302i + 4166067285631998217873560846741)x \\ +2494877549970866914093980400340i + 3422166823321314392366398023265 \end{pmatrix},$$

$$Q_3 = \begin{pmatrix} x^2 + (1867909473743807424879633729641i + 3561017973465655201531445986517)x \\ +6145503558568172997962571584 20i + 3713818865406510298963726073088, \\ +(8465655047965316947606522926 61i + 2430149476747360285585725491789)x \\ +3827102507618362281753526735086i + 8788436826079659618324972589 82 \end{pmatrix},$$

$$Q_4 = \begin{pmatrix} x^2 + (2493766102609911097717660796748i + 2474559150997146544698868735081)x \\ +8438860144918495410256763964 48i + 2700674753803982658674811115656, \\ +(2457109003116302300180304001113i + 3000754825048207655171641361142)x \end{pmatrix}.$$

Genus 2 Implementation

Alice chooses her 12 random secret scalars:

$$\begin{aligned} \alpha_1 &= 937242395764589, & \alpha_2 &= 282151393547351, & \alpha_3 &= 0, \\ \alpha_4 &= 0, & \alpha_5 &= 0, & \alpha_6 &= 0, \\ \alpha_7 &= 1666968036125619, & \alpha_8 &= 324369560360356, & \alpha_9 &= 0, \\ \alpha_{10} &= 0, & \alpha_{11} &= 0, & \alpha_{12} &= 0. \end{aligned}$$

Genus 2 Implementation

Alice chooses her 12 random secret scalars:

$$\begin{aligned}
\alpha_1 &= 937242395764589, & \alpha_2 &= 282151393547351, & \alpha_3 &= 0,\\
\alpha_4 &= 0, & \alpha_5 &= 0, & \alpha_6 &= 0,\\
\alpha_7 &= 1666968036125619, & \alpha_8 &= 324369560360356, & \alpha_9 &= 0,\\
\alpha_{10} &= 0, & \alpha_{11} &= 0, & \alpha_{12} &= 0.
\end{aligned}$$

Bob chooses his 12 random secret scalars:

$$\begin{aligned}
\beta_1 &= 103258914945647, & \beta_2 &= 1444900449480064, & \beta_3 &= 0,\\
\beta_4 &= 0, & \beta_5 &= 0, & \beta_6 &= 0,\\
\beta_7 &= 28000236972265, & \beta_8 &= 720020678656772, & \beta_9 &= 0,\\
\beta_{10} &= 0, & \beta_{11} &= 0, & \beta_{12} &= 0.
\end{aligned}$$

Genus 2 Implementation

Bob computes the genus 2 curve:

$$
\begin{aligned}
H_A : y^2 = {} & (340470300458749582159617696505 8i + 403336181260435480105799382459)x^6 \\
& + (300158408642476293806227622234 0i + 311047190480692260365532924751 0)x^5 \\
& + (101719931062723098351158646333 2i + 159918969863143337265085754407 1)x^4 \\
& + (246956201233909294539836567868 9i + 115456647261523682741646762458 4)x^3 \\
& + (841874238658053023013857416200i + 422410815643904319729131959469)x^2 \\
& + (350758422718042697610977205296 2i + 233129826659556946265779873606 3)x \\
& + 272981662052090517559075818701 9i + 374870400664512900049856351473 4.
\end{aligned}
$$

Genus 2 Implementation

Alice computes the genus 2 curve:

$$
\begin{aligned}
H_B : y^2 = {} & (343439468907475266357951089653 0i + 325881961034199712357660033295 4)x^6 \\
& + (335025511382089519138914356597 3i + 268189248944865942893046722014 7)x^5 \\
& + (295829881867500406204706675826 4i + 904769362079321055425076728309)x^4 \\
& + (270125548760802697517718109107 5i + 787033120015012146142186182556)x^3 \\
& + (352367581167109202249176446602 2i + 280484135355834254284080556136 9)x^2 \\
& + (323815151355079879623805256512 4i + 343788579243377316339513070055 5)x \\
& + 182932737416341009729885306876 6i + 345348951694440631639627148517 2.
\end{aligned}
$$

Genus 2 Implementation

Using ϕ_B, Bob computes the points $\phi_B(P_1), \phi_B(P_2), \phi_B(P_3), \phi_B(P_4)$ and sends this to Alice!

$$\phi_B(P_1) = \pm \begin{pmatrix} x^2 + (5769674700352243844470716918 59i + 3905591233169141993601703381059)x \\ +1497608451125872175852448359137i + 2622938093324787679229413320405, \\ (2205483026731282488507766835920i + 1887631895533666975170960498604)x \\ +2270438136719486828147096768168i + 1098893079140511975119740789184 \end{pmatrix},$$

$$\phi_B(P_2) = \pm \begin{pmatrix} x^2 + (2002807208424762458028352734 43i + 3878472110821865480924821702529)x \\ +4766280318107577344887407192 90i + 2957584612454518004162519574871, \\ (3949908621907714361071815553277i + 6306393236207359666367183210 43)x \\ +9015976423853241579257009768 89i + 2429302320101537821240219151082 \end{pmatrix},$$

$$\phi_B(P_3) = \pm \begin{pmatrix} x^2 + (4133157753622694250606077231439i + 2486410359530824865039464484854)x \\ +2178006463745651824830649066 26i + 1249364962732904444334902689884, \\ (1265490246594537172661646499003i + 2130834160349159007051974433128)x \\ +2580286680987425601000738010969i + 5780466101921461146984665307 58 \end{pmatrix}$$

$$\phi_B(P_4) = \pm \begin{pmatrix} x^2 + (6601102003779684073844190837i + 8710635072963118478554914007 4)x \\ +2330339334251130536871893039627i + 1494511552650494479113393669713, \\ (1706314262702892774109446145989i + 3539074449728790590891503255545)x \end{pmatrix}$$

Genus 2 Implementation

Using ϕ_A, Alice computes the points $\phi_A(Q_1), \phi_A(Q_2), \phi_A(Q_3), \phi_A(Q_4)$ and sends this to Bob!

$$\phi_A(Q_1) = \begin{pmatrix} x^2 + (3464040394311932964693107348618i + 1234121484161567611101667399525)x \\ +1789577539323277385527103 8385i + 3856858968014591645005318326985, \\ (2432835950855765586938146638349i + 3267484715622822051923177214055)x \\ +9853861375517893487602771380 76i + 1179835886991851012234054275735 \end{pmatrix},$$

$$\phi_A(Q_2) = \begin{pmatrix} x^2 + (3633827009609782610886962935 01i + 3499548729039922528103431054749)x \\ +3832512523382547716418075195517i + 3364204966204284852762530333038, \\ (3043817101596607612186808885116i + 4027557567198565187096133171734)x \\ +4087176631917166066356886198518i + 1327157646340760346840638146328 \end{pmatrix},$$

$$\phi_A(Q_3) = \begin{pmatrix} x^2 + (3946684136660787881888285451015i + 1250236853749119184502604023717)x \\ +3358152613483376587872867674703i + 4672522011510763890555248094 76, \\ (1562920784368105245499132757775i + 9879208230759468502336446004 97)x \\ +1675005758282871337010798605079i + 1490924669195823363601763347629 \end{pmatrix},$$

$$\phi_A(Q_4) = \begin{pmatrix} x^2 + (1629408242557750155729330759772i + 3235283387810139201773539373655)x \\ +1341380669490368343450704316676i + 1454971022788254094961980229605, \\ (2393675986247524032663566872348i + 3412019204974086421616096641702)x \end{pmatrix}$$

Genus 2 Implementation

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

$$
\begin{aligned}
g_1 &= 1055018150197573853947249198625i + 2223713843055934677989300194259,\\
g_2 &= 8190605807295720135080065372232i + 3874192400826551831686249391528,\\
g_3 &= 1658885975351604494486138482883i + 3931354413698538292465352257393.
\end{aligned}
$$

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., Weitkämper, 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!