PCMI 2021: Supersingular isogeny graphs in cryptography

Exercises Lecture 2: Quaternion algebras, Endomorphism rings

TA: Jana Sotáková **version July 28, 2021**

From the previous exercise sheet: See code for exercise 1-1, 1-2 and 1-3 at the website.

1-4. (Supersingular isogeny graphs) Write code to generate the supersingular isogeny graph over $\mathbb{F}_{p^2}$, using the following steps. On input coprime primes p and ℓ;

(a) Find one supersingular elliptic curve over $E_0/\mathbb{F}_{p^2}$, represented by the j-invariant;

(b) Write a neighbor function that on input an elliptic curve E, finds all the neighbours of E in the SSIG $\mathcal{G}_\ell$: (the j-invariants of) all the supersingular elliptic curves ℓ-isogenous to E.

(c) Using a breadth-first-search approach, generate the graph by starting from the curve found in Step (b) and the Neighbor function from Step (c).

You can use the code in your Sage installation or on Cocalc. For Magma, you can use and adapt the (not yet complete) code from here ssig.m.

Second lecture

1. For small primes $p \equiv 1 \bmod 12$, denote the SSIG 2-isogeny graph as $\mathcal{G}_2$.

   (a) Find the adjacency matrix A of $\mathcal{G}_2$;

   (b) Find the largest 2 eigenvalues[1] of A;

   (c) What is the spectral gap and the expansion constant c?

   (d) Find the diameter of the graph.

   (e) When $p \not\equiv 1 \bmod 12$, the vertices corresponding to curves with extra automorphisms make the graph undirected. Can you get around this?

   SSIGs have very short diameters, about $\log(p)$. However, most paths used in cryptography have significantly shorter length, about $1/2 \log p$.

2. (SIDH key exchange)

   (a) (Sanity check) Suppose both Alice and Bob choose points S_A, S_B from the same torsion group $E[2^n]$. Find the curve $E_{AB} := E/\langle S_A, S_B \rangle$ (with high probability).

   (b) We will go through the SIDH key exchange:

      i. For $p = 431$, we have $p + 1 = 432 = 2^4 \cdot 3^3$. Let $E : y^2 = x^3 + x/\mathbb{F}_p^2$.

      ii. Verify that $E/\mathbb{F}_{p^2}$ has $(p+1)^2$ points. Supersingular elliptic curves have very special group structure, which implies that $E[2^4], E[3^3] \subset E(\mathbb{F}_q)$ (see Theorem 3.7 of Schoof or, in more generality, Theorem 1.b) of Lenstra).

      iii. Set up the parameters: find a basis $P_A, Q_A \subset E[2^4]$ and a basis $P_B, Q_B \subset E[3^3]$.

[1] You already know one!

iv. Pick a secret point $S_A := m_A P_A + n_A Q_A$ for Alice; pick a secret point $S_B := m_B P_B + n_B Q_B$ for Bob. (In practice we set $m_A = m_B = 1$, you can, too.)

v. Compute the 16-isogeny $\varphi_A : E \to E_A := E/\langle R_A \rangle$ and the images of P_B, Q_B under φ_A. In practice, such isogenies are computed as chains of 2-isogenies, which is rather efficient.

vi. Symmetrically, compute the 27-isogeny $\varphi_B : E \to E_B := E/\langle R_B \rangle$ and the images of P_A, Q_A under φ_B.

vii. Compute the 16-isogeny $E_B \to E_{BA} := E_B/\langle m_A \varphi_B(P_A) + n_A \varphi_B(Q_A) \rangle$, which is the isogeny Alice computes to complete the SIDH square.

viii. Compute the isogeny 27-isogeny $E_A \to E_{AB} := E_A/\langle m_B \varphi_A(P_B) + n_B \varphi_A(Q_B) \rangle$, which is the isogeny Bob computes to complete the SIDH square.

ix. Finally, compare the j-invariants of E_{AB} and E_{BA}.