PCMI 2021: Supersingular isogeny graphs in cryptography
Exercises Lecture 2: Quaternion algebras, Endomorphism rings

TA: Jana Sotáková **version July 29, 2021**

From the previous exercise sheet: See code for exercise 1-1, 1-2 and 1-3 at the website.
You can find some comments on the exercises on the next page.

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 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). Or see Bjorn's explanation on Discord.

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

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}.

You can find hints and comments on the next page.

Notes, comments

1. Generating the supersingular isogeny graph:

   (a) What is the size of the supersingular isogeny graph (SSIG):
   From the lecture,
   $$\#\text{vertices of a SSIG} \approx p/12.$$
   There is a more precise count, coming from the Eichler class number. You can look up the definition and the proof, easier to remember is that it counts all the supersingular elliptic curves, weighed by the size of their automorphism groups:

   i. Basic count is $\lfloor \frac{p-1}{12} \rfloor$.

   ii. Curves with extra automorphisms need to be counted with different weights. So:

      A. if $p \equiv 3 \bmod 4$, add 1 (for $j = 1728$);

      B. if $p \equiv 2 \bmod 3$, add 1 (for $j = 0$).

      (note that both cases above can happen for one p!).

   (b) How to find one supersingular elliptic curve. For $p \equiv 3 \bmod 4$, you can always the the elliptic curves $E : y^2 = x^3 \pm x$. Those have j-invariant 1728.
   Otherwise, there's a general algorithm due to Bröker, using CM theory.
   Suppose you have an elliptic curve E/L defined over some number field L, which has complex multiplication by an order $\mathcal{O} \subset K$ in some imaginary quadratic field K (you can assume that L is the Hilbert class field of $\mathcal{O}$ for simplicity). Now take a prime $\mathfrak{P}|p$ in L. Then E reduces to a supersingular elliptic curve mod$\mathfrak{P}$ if and only if p is non-split in K. So, the j-invariant of E, which is a root of the Hilbert class polynomial f of $\mathcal{O}$, gives a root of f in $\mathbb{F}_{p^2}$ (all j-invariants of supersingular elliptic curves are in $\mathbb{F}_p^2$).
   In other words, if p is nonsplit in K, then the roots of the Hilbert class polynomial in $\mathbb{F}_{p^2}$ give you supersingular elliptic curves, without the need to construct the elliptic curve E first.
   There is one more trick you can play. You can try to find an order $\mathcal{O}$ satisfying the above and with odd class number. Then the degree of f is odd and there will be a root already in $\mathbb{F}_p$. The class number of $\mathcal{O}$ is odd for instance if $\mathcal{O}$ is the ring of integers in $\mathbb{Q}(\sqrt{-q})$ for q a prime satisfying $q \equiv 3 \bmod 4$.
   So you just need to find a small q such that $q \equiv 3 \bmod 4$ and such that p is inert in K (p will be a lot larger than q), that is, $\left(\frac{-q}{p}\right) = -1$.

2. (a) Supersingular isogeny graphs are $k = \ell + 1$-regular, so the largest two eigenvalues of the adjacency matrix are $k = \ell + 1$ and μ_1.
   From Kristin's lecture, we know that $\mu_1 \leq 2\sqrt{k-1} = 2\sqrt{\ell}$.

   (b) The spectral gap is $k - \mu_1$, the expansion constant $\frac{k-\mu_1}{3k-2\mu_1}$. The smaller the eigenvalue, the better the expansion constant.

   (c) For $p \not\equiv 1 \bmod 12$, these definitions no longer make sense, because the graph is no longer $\ell+1$-regular, because of the choice we need to make at the vertices with extra automorphisms. Why do we need to make a choice?
   Remember, we identify an isogeny with its dual. Hence, we identify isogenies up to *post-composition* with automorphisms. Now, let ρ be an automorphism of a curve E with $\rho \neq \pm 1$ (the map $P \mapsto -P$ is a non-trivial automorphism, but it preserves subgroups, hence it

preserves kernels of isogenies). Take any isogeny φ. Then if $\rho \ker \varphi \neq \varphi$, then the isogenies φ and $\varphi \circ \rho$ are different. But, taking dual isogenies:

$$\widehat{\varphi \circ \rho} = \hat{\rho} \circ \hat{\varphi},$$

which is an isogeny *post-composed* with an automorphism. Hence, it is equivalent in the supersingular isogeny graph to $\hat{\varphi}$. So we are forced to identify the edges corresponding to the isogenies $\varphi \sim \hat{\varphi} \sim \widehat{\varphi\rho} \sim \varphi \circ \rho$. So there will not be enough edges from the vertices with special automorphisms.