SLMath summer school on post-quantum cryptography

Exercise sheet on isogeny-based cryptography

- Questions 1-5 are designed to give you familiarity with elliptic curves and isogenies.
- Questions 6-9 are designed to give you familiarity with computing with class-group actions and CSIDH.
- Questions 10-12 are designed to give you familiarity with quaternion algebras as endomorphism rings of supersingular elliptic curves.
- Questions 13-14 are designed to give you familiarity with applying Kani's lemma to problems in isogeny-based cryptography.

1. In answering this question, you should use SageMath as a calculator, but if you are new to elliptic curves we suggest to write your own code for the group law and Vélu's formulae in order to gain familiarity with the concepts. Both of these are implemented directly in SageMath: once you have written your own code you can check the correctness by comparing with the output of the inbuilt commands. Define

$$E/\mathbb{Q} : y^2 = x^3 + 1$$

and observe that $(-1, 0)$, $(0, 1) \in E(\mathbb{Q})$.

   (a) Compute $(-1, 0) + (0, 1)$ using the group law.

   (b) Compute $2 \cdot (0, 1)$ using the group law.

   (c) Compute the minimum positive integer n such that $n(0, 1) = \mathcal{O}$. We call $(0, 1)$ a *point of order n*.

   (d) Using Vélu's formula, compute an isogeny from E with kernel generated by $(0, 1)$.

   (e) If E is defined as an elliptic curve $/\mathbb{Q}$ in SageMath, the command

```
E.torsion_points()
```

returns all the $\mathbb{Q}$-rational points on E with finite order. By making use of this command and the

```
.order()
```

command, deduce how many distinct $\mathbb{Q}$-rational 3-isogenies there are from E.

2. Define
$$E/\mathbb{F}_{17} : y^2 = x^3 + 1$$
and
$$E'/\mathbb{F}_{17} : y^2 = x^3 - 10;$$
let $f : E \to E'$ be the map you computed in question 1(d) reduced modulo 17.

   (a) Calculate the points in the preimage of $(3, 0)$ under f.

   (b) Compute $j(E)$ and $j(E')$.

   (c) Show that E and E' are isomorphic over $\mathbb{F}_{17^2}$.

   (d) Show that E and E' are *not* isomorphic over $\mathbb{F}_{17}$. For this you may make use of the following theorem:

   Theorem 1. *Let $E : y^2 = x^3 + ax + b$ and $E' : y^2 = x^3 + a'x + b'$ be elliptic curves over $\mathbb{F}_q$. Every isomorphism $E \to E'$ defined over $\overline{\mathbb{F}}_q$ is of the form*
   $$\varphi(x, y) = (u^2x + r, u^3y),$$
   where $u, r \in \overline{\mathbb{F}}_q$. The isomorphism is defined over $\mathbb{F}_q$ if and only if $u, r \in \mathbb{F}_q$.

3. Let ℓ be a prime. Show that there are $\ell+1$ size-ℓ subgroups of $\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$.

   (a) Recall that this implies that there are $\ell+1$ non-isomorphic ℓ-isogenies from any given elliptic curve E/k. Are these isogenies defined over k?

   (b) Bonus: what happens for ℓ^r?

4. (a) Using the in-built SageMath commands for isogeny computation, compute the connected component of the 2-isogeny graph of elliptic curves defined over $\mathbb{F}_{1000003}$ containing a vertex corresponding to $j(E) = -3$.

   (b) Using the in-built SageMath commands for isogeny computation, compute the connected component of the 2-isogeny graph of elliptic curves defined over $\mathbb{F}_{109^2}$ containing a vertex corresponding to $j(E) = 43$.

5. Recall the *Diffie-Hellman key exchange*: Let $G = \langle g \rangle$ be a cyclic group in which the Discrete Logarithm Problem is hard, and suppose that g and G are public values such that the g is of (public) prime order ℓ.

- Alice samples a secret key sk_a from $\{1, \ldots, \ell\}$ and computes and publishes $\text{pk}_a = g^a$.
- Bob samples a secret key sk_b from $\{1, \ldots, \ell\}$ and computes and publishes $\text{pk}_b = g^b$.
- Alice and Bob can then both compute their shared secret value

$$g^{ab} = \text{pk}_b^{\text{sk}_a} = \text{pk}_a^{\text{sk}_b}.$$

Recall also the definition of a *group action*. Suppose that G is a group with group operation $*$ and S is a set. We say that G *acts* on S if there exists a map

$$f : G \times S \to S$$

such that

- For every $g, h \in G$ and $s \in S$, we have that $f(g * h, s) = f(g(f(h, s))$.
- For every $s \in S$, if id is the identity of G then $f(id, s) = s$.

Suppose that you are given a group action of a commutative group G on a set S which is efficiently computable and hard to invert, and for which S has no known efficiently computable group structure. Construct a Diffie-Hellman-style key exchange algorithm in which the public keys and shared secret are elements of S, and the secret keys are elements of G.

6. [1] Let ℓ be an odd prime and p a prime satisfying $\ell | (p + 1)$. Let

$$E_A/\mathbb{F}_p : y^2 = x^3 + Ax^2 + x$$

be supersingular and let $\pi : (x, y) \mapsto (x^p, y^p)$ be the p-power Frobenius endomorphism on E. Let $I = \langle [\ell], \pi - [1] \rangle$ be an ideal of $\text{End}(E_A)$.

   (a) Prove that $H_I := \cap_{\alpha \in I} \ker(\alpha) \subseteq E_A(\mathbb{F}_p)[\ell]$.

   (b) Fix $\ell = 3$, $p = 419$, and $A = 220$.

      (i) Verify that E_A is supersingular.

      (ii) Compute H_I for these parameters.

      (iii) Compute $f_I : E_A \to E_A/H_I$ for these parameters.

      (iv) Let $I' = ([3]\pi + [5]) \cdot I$. Compute $f_{I'} : E_A \to E_A/H_{I'}$ for these parameters.

   (c) Prove that $\langle 2, \sqrt{-p} - 1 \rangle$ is *not* an invertible fractional ideal of $\mathbb{Z}[\sqrt{-p}]$. (*This implies that* $\langle [2], \pi - [1] \rangle$ *does not represent an element of the class group, which is why we can only use odd primes in the CSIDH class group action*).

7. [2] Let $p = 419$ and let $E_0/\mathbb{F}_p : y^2 = x^3 + 220x^2 + x$.

[1] Based on an exercise written by Tanja Lange.
[2] Based on an exercise written by Tanja Lange.

(a) Find a point P of order 105 on E_0. Compute $R = 35P$ (using in-built Sage commands) and check that the order of R is 3.

(b) Compute the isogeny φ_3 of kernel $\langle R \rangle$. What is the order of $\varphi_3(P)$? Why is this the order?

(c) Compute the isogeny φ_5 of kernel $\langle 7\varphi_3(P) \rangle$ and the isogeny φ_7 of kernel $\langle \varphi_5 \circ \varphi_3(P) \rangle$.

(d) What is the codomain of the isogeny of kernel $\langle P \rangle$?

8. Let $p = 839 = 2^3 \cdot 3 \cdot 5 \cdot 7 - 1$. Write a toy implementation of a CSURF key exchange in SageMath.

9. Read about Schnorr's Identification Protocol in section 21.3.1 of Cryptography Made Simple by Nigel Smart (available for free at `https://mog.dog/files/SP2019/Cryptography%20Made%20Simple.pdf`). Suppose that, for a given set of CSIDH parameters p and ℓ, you know that the class group of $\mathbb{Z}[\sqrt{-p}]$ is cyclic and you know a generator g. How would you adapt the basic ID protocol as presented in Cryptography Made Simple to depend on the hardness of inverting the CSIDH group action rather than on the Discrete Logarithm Problem in $(\mathbb{Z}/q\mathbb{Z})^*$?

10. Let $p \equiv 2 \pmod 3$ and $E/\mathbb{F}_p : y^2 = x^3 + 1$. Prove that $\mathrm{End}(E)$ is not commutative.

11. [3] Consider the quaternion algebra $B = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$ with $i^2 = j^2 = -1$ and $k = ij = -ji$. Prove that the order $\mathbb{Z}[1, i, j, k]$ is not maximal.

12. [4] Choose a quaternion algebra $B_{p,\infty}$ and compute a maximal order $\mathcal{O}$. Choose a small prime $\ell \neq p$. Use Sage to compute a representative of every left ideal class[5] of norm ℓ of $\mathcal{O}$ and then compute the right orders for these ideals. (Note: if p is very small you might only have one ideal class).
Optional: restrict to (still not too big) $p \equiv 2 \pmod 3$ or $p \equiv 3 \pmod 4$. Choose a small ℓ that divides $p + 1$. Compute the full ℓ-ideal quaternion maximal order graph (up to isomorphism) and map onto the equivalent ℓ-isogeny graph.

13. Suppose that you are given supersingular elliptic curves

$$E_0/\mathbb{F}_p : y^2 = x^3 + x$$

and $E_A/\mathbb{F}_{p^2}$ such that there exists a secret isogeny $f : E_0 \to E_A$ of given degree a. Let B be an integer coprime to a and let $\langle P_0, Q_0 \rangle = E_0[B]$. Suppose also that you are given $mf(P_0)$ and $mf(Q_0)$ for some unknown $m \in \mathbb{Z}/B\mathbb{Z}$. Using the 'lollipop' technique and Kani's lemma, describe an algorithm to recover f. Does this attack extend to other starting elliptic curves E_0?

[3] Based on an exercise written by Laia Amorós.
[4] Based on an exercise written by Laia Amorós.
[5] i.e. your left-ideals should not be principal multiples of each other.

14. Let $p = 191 = 2^6 \cdot 3 - 1$ and let $E_0/\mathbb{F}_p : y^2 = x^3 + x$. Let $\iota : (x, y) \mapsto (-x, iy)$, $\pi : (x, y) \mapsto (x^p, y^p)$, and $\alpha = \iota \circ \pi + 2\pi + 2\iota + 4$ be endomorphisms of E_0.

    (a) Compute a basis $\{P_0, Q_0\}$ of $E_0[2^6]$.

    (b) Compute $\alpha(P_0)$ and $\alpha(Q_0)$.

    (c) How would you compute the image of a random point in E_0 under an isogeny of degree 39, via Kani's lemma?
    Optional: if you know something about dimension 2 abelian surfaces, and want to try computing this, you'll need the following. You need to compute a chain of (2,2)-isogenies, where

    - The first is from a product of elliptic curves to a Jacobian (*glueing*)
    - The middle (2,2)-isogenies are between Jacobians (*Richelot*),
    - The last is from a Jacobian to a product of elliptic curves (*splitting*).

    Jack's note, shared on the Slack, gives simple formulae for glueing and splitting, which you can and should use. For Jacobian to Jacobian, Ben Smith's thesis is a good reference.