Exercises: Isogeny-based crypto

PQCrypto Summer School 2017

July 3, 2017

Key: * = more theoretical. ** = more computational. *** = these exercises are more free, you can either use algorithms that already exist in Sage to help you or try to implement your own.

1. If you are already familiar with elliptic curves, then you can safely skip this exercise. 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. (To add a point to itself, draw the tangent to E at that point as the 'line passing through both points').
   (c) Compute the minimum (positive) integer n such that $n(0, 1) = \infty$. We call $(0, 1)$ a *point of order* n.

2. If you are already familiar with isogenies, then you can safely skip this exercise. Define
$$E/\mathbb{F}_{17} : y^2 = x^3 + 1$$
and
$$E'/\mathbb{F}_{17} : y^2 = x^3 - 10.$$
   (a) Check that
$$f : (x, y) \mapsto ((x^3 + 4)/x^2, (x^3y - 8y)/x^3)$$
   defines a map $E \to E'$.
   (b) Calculate the points in the preimage of $(3, 0)$ under f.
   (c) Compute $j(E)$ and $j(E')$.
   (d) Show that E and E' are not isomorphic over $\mathbb{F}_{17}$ but that they are isomorphic over $\mathbb{F}_{17^2}$.
   Edit: to show that E and E' are not isomorphic over $\mathbb{F}_{17}$, you may make use of the following theorem:

Theorem. *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 from $E \to E'$ defined over $\overline{\mathbb{F}_q}$ is of the form*

$$\phi(x, y) = (u^2 + r, u^3 y),$$

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 $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. Assuming the theorems stated in the lectures, deduce that there are $\ell + 1$ non-isomorphic degree ℓ-isogenies (defined over $\overline{\mathbb{F}_p}$) from every elliptic curve $E/\mathbb{F}_p$. Bonus: what about ℓ^r?

4. * This exercise is to show that the Diffie-Hellman procedure given in the slides works: that is, that Alice and Bob end up at the same shared secret. Let $E/\mathbb{F}_p$ be an elliptic curve and let $\ell, \ell' \neq p$ be a prime. Recall from the lectures that

$$E[\ell] := \{P \in E(\overline{\mathbb{F}_p}) : \ell P = \infty\},$$

and that for $\infty \neq P \in E[\ell]$, we call P a point of order ℓ. For a point $P \in E(\overline{\mathbb{F}_p})$ of order ℓ, define a subgroup

$$\langle P \rangle = \{\infty, P, 2P, \ldots, (\ell - 1)P\}$$

of $E[\ell]$. Recall from the lecture that $\langle P \rangle$ defines a unique degree ℓ isogeny

$$E \to E/\langle P \rangle,$$

and that $E/\langle P \rangle$ defines an elliptic curve over $\overline{\mathbb{F}_p}$. (Check that you see how this follows from the theorems on the slide 'counting isogenies' - note that isogenies are surjective). Now for points $P, P' \in E(\overline{\mathbb{F}_p})$ of orders ℓ and ℓ' respectively, show that

$$j((E/\langle P \rangle)/\langle P' \rangle) = j((E'/\langle P' \rangle)/\langle P \rangle).$$

5. ** The modular polynomial of level 2 is given by

$$\begin{aligned}\Phi_2(X, Y) =& X^3 + Y^3 - 162000(X^2 + Y^2) + 1488(X^2 Y + XY^2) - X^2 Y^2 \\ &+ 8748000000(X + Y) + 40773375XY - 157464000000000.\end{aligned}$$

   (a) Using $\Phi_2(X, Y)$ (and Sage), compute the connected component of the degree-2-isogeny graph of elliptic curves defined over $\mathbb{F}_{1000003}$ containing the vertex corresponding to $j(E) = -3$ that was given in the lecture.

   (b) Using $\Phi_2(X, Y)$ (and Sage), compute the connected component of the degree-2-isogeny graph Γ of elliptic curves defined over $\mathbb{F}_{109^2}$ containing the vertex corresponding to $j(E) = 43$ that was given in the lecture.

(c) *** Choose a path Π starting at $j(E) = 43$ of length 5 in Γ and compute the isogeny φ_2 corresponding to Π either by implementing Elkies algorithm yourself or by asking Sage.

(d) *** The modular polynomial of level 3 is given by

$$\begin{aligned}\Phi_3(X,Y) =& 1855425871872000000000(X+Y)\\ &- 770845966336000000XY\\ &+ 452984832000000(X^2+Y^2)\\ &+ 8900222976000(X^2Y+Y^2X)\\ &+ 2587918086X^2Y^2 + 36864000(X^3+Y^3)\\ &- 1069956(X^3Y+Y^3X) + 2232(X^3Y^2\\ &+ Y^3X^2) - X^3Y^3 + X^4 + Y^4.\end{aligned}$$

Using this, or by implenting Vélu's algorithm, find a length 6 path in the degree-3-isogeny graph of elliptic curves defined over $\mathbb{F}_{109^2}$ containing the vertex corresponding to $j(E) = 43$ starting at $j(E) = 43$, and compute the corresponding isogeny φ_3.

(e) *** Choose public points $P_A, Q_A \in E[2^5]$ and $P_B, Q_B \in E[3^6]$ and secret coefficients $m_A, n_A \in \mathbb{Z}/2^5\mathbb{Z}$ and $m_B, n_B \in \mathbb{Z}/3^6\mathbb{Z}$. Compute Alice and Bob's secret isogenies corresponding to these choices and check that they arrive at the same shared secret.