Isogeny-based Cryptography - Problem Sheet

August 3, 2022

For computational exercises, we recommend using a computer algebra package (eg. SageMath `www.sagemath.org` - it is even possible to use an online version provided by CoCalc).

Mathematical Background

1) Forms of Isogenies

Recall that an isogeny $\phi : E \to E'$ between Weierstrass curves defined over a field K can be written as $\phi(x, y) = \left(\frac{p(x,y)}{q(x,y)}, \frac{s(x,y)}{t(x,y)}\right)$, for some $p(x, y), q(x, y), s(x, y), t(x, y) \in \bar{K}[x, y]$. In the lecture we claimed that ϕ can be represented in the form

$$\phi(x, y) = \left(\frac{\varphi(x)}{\psi^2(x, y)}, \frac{\omega(x)y}{\psi^3(x, y)}\right).$$

Prove this claim.

2) Isogeny Kernels

Rather than representing isogenies as rational maps, it is typically more convenient to represent them by their kernels. This translation is computed using Velu's formulae:

$$\phi(P) = \left(x_P + \sum_{Q \in G \setminus \mathcal{O}} (x_{P+Q} - x_Q), y_P + \sum_{Q \in G \setminus \mathcal{O}} (y_{P+Q} - y_Q)\right).$$

Let $E/\mathbb{F}_{29} : y^2 = x^3 + 1$, and let $K = (-1, 0) \in E(\mathbb{F}_{29})$. Using Velu's formulae, compute the co-domain of the isogeny with kernel $\langle K \rangle$. (Use the fact that in this case the resulting curve can be written in short Weierstrass form.)

3) Cyclicity

We say an isogeny ϕ is cyclic if $\ker \phi$ is a cyclic group.

(a) Give an example of a non-cyclic isogeny.

(b) Suppose $\deg(\phi) = d$ with d squarefree. Prove that φ is cyclic. Is the converse true?

(c) Let $E : y^2 = x^3 + 13$, $E' : y^2 = x^3 + x + 21$ be curves over $\mathbb{F}_{23}$, and let $\phi : E \to E'$ be the isogeny given by

$$\phi(x, y) = \left(\frac{p_1(x)}{(x - 5)q^2(x)}, \frac{p_2(x)y}{(x - 5)^2q^3(x)}\right),$$

where

$$\begin{aligned}
p_1(x) =& (x - 3)(x - 2)(x^2 + x + 1)(x^2 + 2x - 6)(x^2 + 4x - 6)(x^2 + 7x - 2)(x^2 + 10x - 3) \\
p_2(x) =& (x - 4)(x + 1)(x + 3)(x + 4)(x + 7)(x + 11)(x - 10)(x^2 + 4) \\
& (x^2 + 9x + 5)(x^2 - 10x + 8)(x^2 - 6x + 11)(x^2 - 2x - 9) \\
q(x) =& x(x + 5)(x + 6)(x + 10)(x - 9).
\end{aligned}$$

Determine whether ϕ is cyclic.

4) Dual, Traces and Degrees

In the lecture, we defined the dual of an isogeny $\phi\colon E \to E'$ to be the unique isogeny $\hat{\phi}$ such that $[\deg(\phi)] = \phi\hat{\phi}$. Prove the following (where the domain and codomain of each isogeny is such that these operations make sense)

(a) $\widehat{\phi\lambda} = \hat{\lambda}\hat{\phi}$

(b) $\hat{\hat{\phi}} = \phi$

(c) When ϕ is an endomorphism, we can make sense of the quantity $\phi + \hat{\phi}$, which we define to be the trace of ϕ. Let $\alpha, \beta, \phi \in \mathrm{End}(E)$ for some elliptic curve $E/\mathbb{F}_q$. Compute the degree and trace of the endomorphism $\alpha\phi + \beta$, assuming $\alpha\hat{\beta} \in \mathbb{Z}$. (Useful Fact: $\widehat{\phi + \lambda} = \hat{\phi} + \hat{\lambda}$.)

5) Counting Points

Prove that for every prime $p \geq 3$, the elliptic curve $E\colon y^2 = x^3 + x$ satisfies $\#E(\mathbb{F}_p) = 0 \mod 4$. Hint: Look at the arithmetic of Mongomery curves `https://eprint.iacr.org/2017/212.pdf`.

6) Supersingular Isogeny Graph

Figure 1 depicts the supersingular 2-isogeny graph over $\mathbb{F}_{p^2}$. However, it contains an error. Can you spot it? Can you explain it?

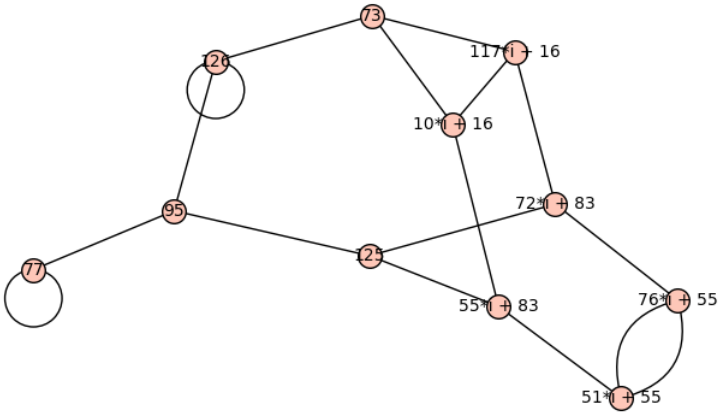

Figure 1: The supersingular 2-isogeny graph over $\mathbb{F}_{127^2}$

Now, it is your turn. For some small p and ℓ, compute the full supersingular $\ell-$isogeny graph. If you are using SageMath, you may want to take a look at `https://doc.sagemath.org/html/en/reference/plotting/sage/graphs/graph_plot.html`.

Protocols & Cryptanalysis

1) Group Actions

Let G be a finite abelian group, X a finite set, and $f : G \times X \to X$ be a group action. Show how f can be used to instantiate a Diffie-Hellman style non-interactive key exchange. What properties do we require on G, X and f for this key exchange to be secure and practical?

2) Efficient Isogeny Evaluation

When constructing ℓ-isogenies from points of order ℓ, it is preferable to work with points defined over small field extensions. Here we will see how we can minimise these extension degrees by choosing parameters carefully. Let $E/\mathbb{F}_p$ be a (not necessarily supersingular) elliptic curve. Let π denote the p-power frobenius endomorphism on E, with minimal polynomial $x^2 - tx + p$.

(a) For any prime $\ell \neq p$, show that π acts linearly on $E[\ell]$. Denote this map by π_ℓ, and write down its characteristic polynomial.

(b) Write down the eigenvalues of π_ℓ^k in terms of the eigenvalues of π_ℓ.

(c) Show that there exists an integer r such that $E[\ell] \subseteq E(\mathbb{F}_{p^r})$, and deduce an expression for the minimum such r.

(d) Given ℓ, deduce sufficient conditions on t and p such that

i. $E[\ell] \subseteq E(\mathbb{F}_p)$.

ii. $E[\ell] \subseteq E(\mathbb{F}_{p^2})$.

3) Isogeny field of definition

Now let E be a supersingular elliptic curve defined over $\mathbb{F}_p$. Prove that all ℓ-power isogenies are defined over $\mathbb{F}_{p^2}$. Does this result agree with the previous exercise? Does the same result apply for supersingular elliptic curves over $\mathbb{F}_{p^2}$?

4) The restricted endomorphism ring of a supersingular elliptic curve

Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$. Prove that the ring of all the $\mathbb{F}_p$-endomorphisms is commutative.

5) SIDH implementation

Implement SIDH for a small prime p, e.g. $p = 2^{15}3^8 - 1$. Bonus exercise: Break it!

6) Breaking the CGL hash function

Describe an attack against the CGL hash function when the initial curve has known endomorphism ring (for instance, when the initial curve is $E_0 : y^2 = x^3 + x$.) Can you find a countermeasure for your attack?

7) Meet in the middle

Let $p = 2^{19} - 1$, $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ where $i^2 = -1$. Define the curves

$$E_0 : y^2 = x^3 + x$$
$$E_1 : y^2 = x^3 + (195429i + 424412)x + (296307i + 100560)$$

Using meet-in-the-middle, compute an isogeny $\varphi : E_0 \to E_1$ defined over $\mathbb{F}_{p^2}$.