PAWS 2025: MATHEMATICAL CRYPTOGRAPHY
PROBLEM SET 5

GIACOMO BORIN, JOLIJN COTTAAR, ELI ORVIS, GABRIELLE SCULLARD

The goal for the exercises in Problem Set 5 is to practice with the concepts of cryptographic group actions, isogenies, and CSIDH.

(1) (Beginner) Consider the following elliptic curves in short Weierstrass form defined over $\mathbb{F}_5$:

$$E_1 : y^2 = x^3 + x + 1, \quad E_2 : y^2 = x^3 + 3x + 1, \quad E_3 : y^2 = x^3 + 1.$$

Which of the elliptic curves can be written in Montgomery form over $\mathbb{F}_5$? Find a coordinate transformation if it exists.

(2) (Intermediate) Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{F}_q$. Show that the map

$$\begin{aligned} \pi \ : \ & E \to E, \\ & (x, y) \mapsto (x^q, y^q) \end{aligned}$$

defines an isogeny. This essentially requires showing two properties:

(a) π is well-defined, i.e. if $P = (x, y) \in E$, then $\pi(P) = (x^q, y^q) \in E$ as well.

(b) π is a group homomorphism.

Note that this is an example of an isogeny which is not separable.

(3) (Beginner) Let $(G, \circ)$ be a cyclic group with neutral element id and assume that $\#G = N$ is prime. Show that

$$\begin{aligned} (\mathbb{Z}/N\mathbb{Z})^* \times G\backslash\{id\}, & \to G\backslash\{id\} \\ (n, x) & \mapsto \exp_x(n) = \underbrace{x \circ x \circ \cdots \circ x}_{n \text{ times}} \end{aligned}$$

is a regular group action.

(4) (Beginner) In this exercise we consider a group action based on matrix multiplication. Let $\mathbb{F}_p$ be a finite field (for some large prime p). Consider

$$\mathbb{G} = \left\{ \begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix} | c_1, c_2 \in \mathbb{F}_p \right\}, \qquad X = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} | x_1, x_2 \in \mathbb{F}_p \right\} = \mathbb{F}_p^2,$$

and the group action

$$\begin{aligned} \star : \mathbb{G} \times X & \to X, \\ (A, x) & \mapsto A \cdot x \end{aligned}$$

(a) Show that $\star$ defines a commutative group action. Is the group action regular?

(b) Sketch a Diffie-Hellman protocol based on the group action and convince yourself it works correctly.

(c) Show that $\star$ is not a cryptographic group action. Find a polynomial-time algorithm to solve GA-DLP for this group action.

(5) (Intermediate) Let $\star : \mathbb{G} \times X \to X$ be a group action, and assume that the group action is effective. In particular, you may assume the following operations can be performed efficiently.

- Evaluating the group action: Given $g \in \mathbb{G}, x \in X$, compute $g \star x$.

- Group operation: Given $g_1, g_2 \in \mathbb{G}$, compute $g_1 \circ g_2$.
- Equivalence checking: Given $x, x' \in \mathbb{G}$, decide if $x = x'$.

In the following, you are supposed to find analogues of the baby-step giant-step algorithm.

(a) First consider a cyclic group, i.e. assume that $\mathbb{G} \cong \mathbb{Z}/N\mathbb{Z}$ for some N. Find an algorithm to solve GA-DLP in time $O(\sqrt{N})$ in this setting.

(b) Now assume that $\mathbb{G}$ is an arbitrary abelian group, i.e. $\mathbb{G} \cong \mathbb{Z}/N_1\mathbb{Z} \times \ldots \times \mathbb{Z}/N_r\mathbb{Z}$ for some integers $N_1, \ldots, N_r$ with $N_{i+1} \mid N_i$ for all $i = 1, \ldots, r-1$. Adapt the algorithm from (a) to solve GA-DLP in this setting.
(Hint: It makes sense to first consider the case $r = 2$. Is there a difference between the cases $N_1 = N_2$ and $N_2 \ll N_1$?

(6) (Intermediate) Let $\mathbb{F}_q$ be a finite field, $k < n$ integers, and let $X = \mathbb{F}_q^{k \times n}$ be the set of $k \times n$ matrices over $\mathbb{F}_q$. Further we define $\mathbb{G} = GL_k(\mathbb{F}_q) \rtimes \mathcal{P}_n$, where $GL_k(\mathbb{F}_q)$ are invertible $k \times k$ matrices over $\mathbb{F}_q$ and $\mathcal{P}_n$ is the group of $n \times n$ permutation matrices.

We consider the group action

$$\begin{aligned} \star: \ \mathbb{G} \ \times \ X &\to X \\ ((S, P), A) &\mapsto S \cdot A \cdot P. \end{aligned}$$

In a slightly more general form, this group action is used as a one-way function in the signature scheme LESS. We note that this is not a commutative group action.

(a) Let $q = 3$, $k = 2$, $n = 4$, and consider the following matrices

$$A_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \end{pmatrix}$$

Find $g = (S, P) \in \mathbb{G}$ so that $g \star A_1 = SA_1P = A_2$. Is the solution unique?

(b) In the setting of (a), consider

$$A_3 = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Is there an element $g \in \mathbb{G}$ so that $g \star A_1 = A_3$?
Remark: it is assumed to be hard to solve this problem in general (for large parameters).

(c) Is the group action $\star$ free, transitive, or regular?

(7) (Beginner, sage) Use Sage to sketch the CSIDH graph with $p = 59 = 4 \cdot 3 \cdot 5 - 1$ (as in Example 4.26).

(a) Verify that the supersingular Montgomery coefficients are $A = 0, 6, 11, 28, 29, 30, 31, 48, 53$.

(b) To draw edges corresponding to 3-isogenies: For each curve E_A, compute a point $P_3 \in E_A[3](\mathbb{F}_p)$, a 3-isogeny ϕ_3 with $\ker(\phi_3) = \langle P_3 \rangle$, and the codomain of ϕ_3 (in Montgomery form).
(Hint: You can compute a generator of $E(\mathbb{F}_p)$ using *.gens*(); use it to compute a point of order 3.)

(c) To draw edges corresponding to 5-isogenies: For each curve E_A, compute a point $P_5 \in E_A[5](\mathbb{F}_p)$, a 5-isogeny ϕ_5 with $\ker(\phi_5) = \langle P_5 \rangle$, and the codomain of ϕ_5 (in Montgomery form).

You can sketch the graph by hand or use Sagemath. Here a small example on how to use Graphs in sage (you can read more on `https://doc.sagemath.org/html/en/reference/graphs/sage/graphs/generic_graph.html#methods`)

```
sage: G = Graph()
sage: G.add_vertices([1,2,3])
sage: G.add_edge((0,1,'3'))          # edge 0 -> 1, '3' is the label
sage: G.add_edge((0,3,'5'))          # edge 0 -> 3, '5' is the label
sage: G.show(color_by_label = True) # different colors for labels
```

(8) (Intermediate) In this exercise, we analyze the setting of CSIDH for $p = 59$ in more detail (using the second graph in Figure 16 in the lecture notes). Assume that the secret key space is $\{-2, -1, 0, 1, 2\}^2$.
  (a) Say Alice's public key is $A = 28$. What was her secret key? In other words, what is $\mathrm{dlog}_{E_0}(E_{28})$? Is the answer unique?
  (b) Say Bob's public key is $B = 11$. What is the shared session key? Is the answer unique?
  (c) Is the group action $\star : \{-2, -1, 0, 1, 2\} \times V \to V$ transitive? Is it free?
  (d) Now consider the smaller secret key space $\{-1, 0, 1\}^2$. Is the group action $\star : \{-1, 0, 1\} \times V \to V$ transitive? Is it free?
  (e) Describe the relations between possible secret keys in $\mathbb{Z}^2$, and represent the equivalence classes of secret keys as $\mathbb{Z}^2/\Lambda$, where Λ is a lattice $\Lambda \subset \mathbb{Z}^2$. Is the group action $\star : \mathbb{Z}^2/\Lambda \times V \to V$ transitive? Is it free?

(9) (Advanced.) We consider a CSIDH graph for some prime $p = 4 \cdot \ell_1 \cdots \ell_n - 1$.
  (a) Let A be the label of a vertex in the CSIDH graph. Show that there exists a vertex with label $-A$ as well. (Hint: This means showing that $E_A(\mathbb{F}_p) = E_{-A}(\mathbb{F}_p)$.)
  (b) Consider $E_0 : y^2 = x^3 + x$. Let $P_1 = (x_1, y_1) \in E(\mathbb{F}_p)$ and denote $ord(P) = N$ for some $N \mid p+1$. Show that $P_1' = (x_1, iy_i) \in E(\mathbb{F}_{p^2})$, and moreover $ord(P_1') = N$ as well.
  Hint: One way to show this is by using the explicit group law (Theorem 3.7 in the lecture notes). It is instructuve to consider $N = 2, 3$ and then conclude for general N.
  (c) Now consider the isogeny $\phi : E_0 \to E$ with kernel $\langle P_1 \rangle$. Using Vélu's formulas (Theorem 4.13 in the lecture notes), one finds that $E : y^2 = x^3 + ax + b$ for some a, b. Further consider the isogeny $\phi' : E \to E'$ with kernel $\langle P_1' \rangle$. Show that $E' : y^2 = x^3 + ax - b$ when using the same formulas.
  In the CSIDH setting, we work with elliptic curves in Montgomery form. For the next part of the exercise, you may either use the previous result and convert the equation for E and E' to Montgomery form (tedious). Or you can use isogeny formulas from the literature which directly work with curves in Montgomery form (see [1, Proposition 1]).
  (d) With $P_1, P_1' \in E_0[N]$ as before, now consider the isogeny $\psi : E_0 \to E_{-A}$ with kernel $\ker(\psi') = \langle P_1' \rangle$.
  We note that the elliptic curve E_{-A} is the **quadratic twist** of the curve E_A. The two curves are isomorphic over $\mathbb{F}_{p^2}$ bu not over $\mathbb{F}_p$ (unless $A = 0$).

(10) (Sage, Advanced) Let ℓ be a prime such that $(\ell, p) = 1$. One can define the **supersingular ℓ-isogeny graph** whose vertices are supersingular elliptic curves over $\mathbb{F}_{p^2}$ (up to isomorphisms), and whose edges are ℓ-isogenies between supersingular elliptic curves.

As seen in Remark 4.25.v, we can assume the graph is undirected since each isogeny $\phi : E \to E'$ can be associated to the dual one $\hat{\phi} : E' \to E$. Also, we consider two ℓ-isogenies equivalent if they have the same kernel. One way to phrase a fundamental problem in isogeny-based cryptography is: "Given two supersingular elliptic curves, find a path between them in the supsersingular ℓ-isogeny graph."
  (a) In the lecture, **supersingular** was defined only for elliptic curves over $\mathbb{F}_p$. Over $\mathbb{F}_{p^2}$ an elliptic curve E is supersingular if and only if $\#E(\mathbb{F}_{p^2}) - p^2 - 1 \equiv 0 \pmod{p}$.[1] List all supersingular curves over $\mathbb{F}_{59^2}$.
  (b) To label the vertices we need a unique identifier. Before we used the Montgomery coefficient, but now we need a more general one: the j-invariant. For an elliptic curve in short Weierstrass form, $y^2 = x^3 + ax + b$, the j-invariant is given by

$$j = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

[1] This is a consequence of Exercise 5.10 in Silverman's Arithmetic of Elliptic Curves.

(i) Compute the j-invariants for the two elliptic curves $E : y^2 = x^3 + x$ and $E' : y^2 = x^3 + 1$. (We have seen previously that E is supersingular if and only if $p \equiv 3 \pmod 4$ and E' is supersingular if and only if $p \equiv 2 \pmod 3$.)

(ii) Compute the j-invariants corresponding to vertices in CSIDH for $p = 59$.

(iii) Compute the j-invariant of the curves from the previous point.

(c) Show that there are $\ell + 1$ edges starting at any given vertex.

(hint: each edge corresponds to a subgroup of $E[\ell]$ of order ℓ)

(d) Generate the 3-isogeny graph for $p = 59$, using the following code:

```
sage: E = EllipticCurve(GF(59^2), j=1728)
sage: G = E.isogeny_ell_graph(3, directed=False, label_by_j=True)
sage: G.show()
```

(i) Check that the graph has the properties you expect (i.e. has all the correct j-invariants and has 4 outgoing edges from each vertex), except at $j = 0, 17$.[2] *One can use* $p \equiv 1 \pmod{12}$ *to avoid this issue at* $j = 0, 1728$.

(ii) Do the same for $\ell = 5$.

(iii) Compare these graphs to the CSIDH graph for $p = 59$.

(iv) Do the same for $p = 419$ and compare to the CSIDH graph.

(v) Do the same for $p \equiv 1 \mod 12$ and see if the graph changes.

References

[1] Joost Renes. "Computing isogenies between Montgomery curves using the action of (0, 0)". In: *International conference on post-quantum cryptography.* Springer. 2018, pp. 229–247.

[2] that is 1728 mod 69