Isogeny-based Cryptography

Luciano Maino

University of Bristol - Advanced Cryptology

1 Introduction

As you may have heard in previous lectures, there is another branch of cryptography which is dealing with the problem of designing cryptosystems that are secure against quantum computers; this branch is called *post-quantum cryptography*. The examples of cryptosystems we have shown in previous lectures are all vulnerable to the quantum threat due to the fact their hardness assumptions are stated in terms of commutative groups. We therefore need to look into a different direction.

We have already seen that elliptic curves are particularly amenable to cryptography thanks to their fast arithmetic. More importantly, elliptic curves have been widely studied in cryptography. So, if we want to have quantum-resistant cryptosystems that are also efficient, continuing to use elliptic curves is a promising approach.

Since the group structure of elliptic curve is commutative, we have to rely on a different mathematical object involving elliptic curves. The solution is to look at maps between elliptic curves. In the next sections, we explain how to use some special maps, called *isogenies*, to design cryptosystems. These cryptosystems will actually mimic the constructions we have previously shown.

2 Isogenies

The word "isogeny" itself hints at the property we are after. In a certain sense, isogenies preserve the same "type", the same "genus". Let's formally define them.

Definition 1 (Simplified). *Let E and E' be two elliptic curves defined over a field K. An* isogeny $\varphi : E \to E'$ *is a homomorphism of groups between E and E'. Isogenies are defined by rational maps, i.e. the ratio of two polynomials. The field of definition of an isogeny coincides with the field of definition of the rational maps.*

The degree *of an isogeny is equal to its degree as a rational map. Concretely (up to edge cases), isogenies are uniquely determined by their kernels, and the size of their kernels equals the degree of the isogeny.*

Given an isogeny $\varphi : E \to E'$ there exists another isogeny $\widehat{\varphi} : E' \to E$ of the same degree as φ. Such an isogeny is called the dual isogeny *of φ.*

Example 2. Let $E\colon y^2 = x^3 + x$ be an elliptic curve defined over $\mathbb{F}_{19^2}$ and let $i \in \mathbb{F}_{19^2}$ be a root of $x^2 + 1 \in \mathbb{F}_{19^2}[x]$, i.e. $i = \sqrt{-1}$. The isogeny $\varphi\colon E \to E'$, with kernel $\langle (i, 0) \rangle$ is given by:

$$\begin{aligned} \varphi\colon \quad E \quad &\to E'\colon y^2 = x^3 + 11x + 14i \\ (x, y) &\mapsto \left(\tfrac{x^2 - ix - 2}{x - i}, \tfrac{x^2 y - 2ixy + y}{x^2 - 2ix - 1} \right). \end{aligned}$$

Questions: What's the degree of this isogeny? What's special about the denominators of these rational maps?

2.1 Vélu's formulae

To compute isogenies, we can rely on the *Vélu's formulae*, which were introduced by Vélu in [4]. We briefly recall them below.

Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve and suppose we want to compute the isogeny $\varphi\colon E \to E'\colon y^2 = x^3 + a'x + b'$ with kernel $\langle P \rangle$, where P is a point of odd order ℓ. The quantities a' and b' are defined as follows:

$$a' = a - 10 \cdot \sum_{k=1}^{\frac{\ell-1}{2}} (3x_{[k]P}^2 + a), \qquad \text{and} \qquad b' = b - 14 \cdot \sum_{k=1}^{\frac{\ell-1}{2}} (2y_{[k]P}^2 + x_{[k]P}(3x_{[k]P}^2 + a)).$$

Each point in $\langle P \rangle$ is sent to the identity on E'. Let $Q = (x, y) \in E \setminus \langle P \rangle$, then $\varphi(Q) = (x', y')$, where

$$\begin{aligned} x' &= x + \sum_{k=1}^{\frac{\ell-1}{2}} \left(2 \cdot \frac{(3x_{[k]P}^3 + a)}{x - x_{[k]P}} + \left(\frac{2y_{[k]P}}{x - x_{[k]P}} \right)^2 \right), \\ y' &= y - 2 \cdot \sum_{k=1}^{\frac{\ell-1}{2}} \left(4y_{[k]P}^2 \frac{y}{(x - x_{[k]P})^3} + (3x_{[k]P}^3 + a) \frac{y}{(x - x_{[k]P})^2} \right). \end{aligned}$$

These formulae are not the most efficient ones when it comes down to concrete computations. The best asymptotic algorithm to compute isogenies is the so-called square-root Vélu [1].

2.2 Endomorphism Rings

An endomorphism is an isogeny $\varphi : E \to E$, where the domain and codomain coincide. We denote the set of all endomorphisms by $\mathsf{End}(E)$.

Example 3. Let $m \in \mathbb{Z}$. The map $[m]\colon E \to E$ acting as the scalar multiplication $[m]P$ is an endomorphism. Its degree is equal to m^2.[1]

The set $\mathsf{End}(E)$ is endowed with a ring structure. To be more precise:

- the endomorphism $[0]\colon E \to E$ is the zero of the ring;
- given $\alpha, \beta \in \mathsf{End}(E)$, the endomorphism $\alpha \cdot \beta$ is the endomorphism $P \mapsto \alpha(\beta(P))$;
- given $\alpha, \beta \in \mathsf{End}(E)$, the endomorphism $\alpha + \beta$ is the endomorphism $P \mapsto \alpha(P) \oplus \beta(P)$.

[1] This is not entirely true, but it is enough for the applications we have in mind. To be more precise, this property holds when $\gcd(m, \mathrm{char}(K)) = 1$, where K is the field of definition for the elliptic curve E.

From now on, let us assume we are working over a finite field $\mathbb{F}_q$. If the endomorphism ring $\mathsf{End}(E)$ is commutative, the curve E is said to be *ordinary*, otherwise is said to be *supersingular*.

Supersingular elliptic curves are the types of elliptic curves encountered in almost all isogeny-based cryptosystems, since they enjoy some extra properties.

Given E an elliptic curve defined over $\mathbb{F}_p$, we have a very special endomorphism, called the *Frobenius* endomorphism.

$$\begin{array}{rccc} \pi\colon & E & \to & E \\ & (x,y) & \mapsto & (x^p, y^p). \end{array}$$

3 CSIDH

We know sketch the main idea behind one of the most famous isogeny-based protocols: *Commutative Supersingular Isogeny Diffie-Hellman (CSIDH)* [2].[2] It provides a drop-in replacement for the classical non-quantum-resistant cryptosystems via a *transitive and free group action*.

Definition 4. *Let G be a group whose neutral element is e and let S be a non-empty set. A* group action $\star\colon G \times S \to S$ *is a binary operation such that:*

- *for all $s \in S$, $e \star s = s$;*
- *for all $s \in S$ and for all $g_1, g_2 \in G$, $g_1 \star (g_2 \star s) = (g_1 \cdot g_2) \star s$.*

We say that the action $\star$ is free *if $g \star s = s$, for some $s \in S$, implies that $g = e$. Additionally, we say that the action $\star$ is* transitive *if for all $s_1, s_2 \in S$ there exists $g \in G$ such that $g \star s_1 = s_2$.*

We now describe the transitive and free group action in CSIDH. First, what is the set S? We will now work with supersingular curves E defined over $\mathbb{F}_p$, where p is a prime of the form $4 \cdot \ell_1 \cdot \ldots \ell_n - 1$ for some small distinct primes ℓ_i. We define $\mathsf{End}_{\mathbb{F}_p}(E)$ to be the set of all the endomorphisms defined over $\mathbb{F}_p$. The set we will use for the CSIDH action is $\mathcal{S}_p$, which is the set of all the the elliptic curves defined over $\mathbb{F}_p$ such that $\mathsf{End}_{\mathbb{F}_p}(E) \simeq \mathbb{Z}[\sqrt{-p}]$.

Which group can we use in CSIDH to have a free, transitive group action? The group used in CSIDH is the ideal class group $\mathcal{I}(\mathbb{Z}[\sqrt{-p}])$, which we are not going to describe in this short note. Rather, we will describe some of its elements.

For each $i = 1, \ldots, n$, we have that the elements $(\ell_i, \sqrt{-p} \pm 1) \in \mathcal{I}(\mathbb{Z}[\sqrt{-p}])$. These elements are technically equivalence classes of fractional ideals, but for the case at hand we will consider them as a tuple. How do they act on $\mathcal{S}_p$?

Let $E \in \mathcal{S}_p$. We denote by $P_i^- = (x, y)$ a point of order ℓ_i on E such that $x, y \in \mathbb{F}_p$, and we denote by $P_i^+ = (x, y)$ a point of order ℓ_i on E such that $x \in \mathbb{F}_p$ but $y \notin \mathbb{F}_p$. The action of $(\ell_i, \sqrt{-p} + 1)$ on E is the curve E^+, where $\varphi^+ : E \to E^+$ is the isogeny with kernel $\langle P_i^+ \rangle$. Mutatis mutandis, for the action of $(\ell_i, \sqrt{-p} - 1)$. One can prove that for all $E \in \mathcal{S}_p$, we have

$$((\ell_i, \sqrt{-p} + 1) \cdot (\ell_i, \sqrt{-p} - 1)) \star E = E.$$

[2] CSIDH is pronounced "sea side". I strongly recommend reading this paper.

This means that $(\ell_i, \sqrt{-p}+1)^{-1} = (\ell_i, \sqrt{-p}-1)$.

We now know how to compute the action of some of the elements in $\mathcal{I}(\mathbb{Z}[\sqrt{-p}])$ onto $\mathcal{S}_p$. However, one can argue that knowing how to compute the action of the $(\ell_i, \sqrt{-p} \pm 1)$'s is actually close enough to knowing how to compute the action of all the elements in $\mathcal{I}(\mathbb{Z}[\sqrt{-p}])$.

We fix a positive integers m and then restrict to computing the actions of elements of the form

$$(\ell_1, \sqrt{-p}+1)^{e_1} \cdot \ldots \cdot (\ell_n, \sqrt{-p}+1)^{e_n},$$

where $e_1, \ldots, e_n \in [-m; m]$. In other words, we have an action of $[-m; m]^n$ onto $\mathcal{S}_p$.

We now explain how to create a Diffie-Hellman key exchange using the CSIDH group action. We first fix a curve in $\mathcal{S}_p$, say E_0. In a key-exchange setting, we have two parties, Alice and Bob. Alice's secret key consists in a tuple of integers $(a_1, \ldots, a_n)$, whereas her public key is given by

$$E_A = (\ell_1, \sqrt{-p}+1)^{a_1} \cdot \ldots \cdot (\ell_n, \sqrt{-p}+1)^{a_n} \star E_0.$$

Similarly, Bob has a secret key $(b_1, \ldots, b_n)$, and its associated public key

$$E_B = (\ell_1, \sqrt{-p}+1)^{b_1} \cdot \ldots \cdot (\ell_n, \sqrt{-p}+1)^{b_n} \star E_0.$$

Given Bob's public key E_B, Alice computes the shared secret key

$$E = (\ell_1, \sqrt{-p}+1)^{a_1} \cdot \ldots \cdot (\ell_n, \sqrt{-p}+1)^{a_n} \star E_B,$$

and similarly does Bob. Both parties end up with the same shared key because $\star$ is a transitive and free action group action of a commutative group.

Remark 5. The CSIDH framework is very "malleable" and offers a useful tool to construct more advanced cryptographic primitives such as digital signature schemes, ring signatures, and so on.

4 On the Security of Isogeny-based Cryptography

The most general problem underlying isogeny-based cryptography is the *Pure isogeny problem.*

Definition 6. *Let E and E' be two elliptic curves defined over $\mathbb{F}_q$. Compute, if it exists, an isogeny connecting E and E'.*

The hardness of this problem depends on many factors. In the case of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, where the prime p is large enough, the problem is believed to be hard.

Unfortunately, when designing a cryptosystem, it is hard to rely on this very general problem. Cryptographers tend to rely on other problem which may be easier to solve compared to the pure isogeny problem.

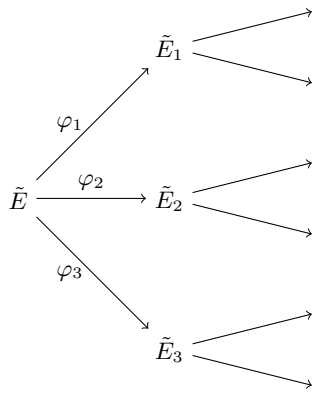
For instance, a problem which has been used for quite some time in isogeny-based cryptography is the *Supersingular Isogeny with torsion problem*, which we briefly recall below.

Definition 7. *Let ℓ_A, ℓ_B be two small distinct primes and let p be a prime of the form $f \cdot \ell_A^{e_A} \ell_B^{e_B} - 1$ for some $f, e_A, e_B > 0$. Also, let E and E' be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ connected by an unknown isogeny $\varphi : E \to E'$ of degree $\ell_A^{e_A}$ and let P, Q be two points that generate $E_A[\ell_B^{e_B}]$. Given $(\varphi(P), \varphi(Q))$, recover the isogeny φ.*

This problem has resisted several attempts of cryptanalysis but was eventually completely broken in 2022. The technique used to achieve this is quite advanced, and for this reason, we will focus on an easier way to attack a harder variant of this problem.

Definition 8. *Let ℓ be a small prime and let p be a prime of the form $f \cdot \ell^e - 1$ for some $f, e > 0$. Also, let E and E' be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ connected by an unknown isogeny of degree ℓ^e. Recover any isogeny $\varphi : E \to E'$ of degree ℓ^e.*

A standard way to attack this sort of problems in cryptography is the *meet-in-the-middle* attack. Suppose that $\ell = 2$ and e is even. Given any elliptic curve $\tilde{E}$, there exists three distinct isogenies of degree two, say $\varphi_1 : \tilde{E} \to \tilde{E}_1$, $\varphi_2 : \tilde{E} \to \tilde{E}_2$ and $\varphi_3 : \tilde{E} \to \tilde{E}_3$. Then starting from one of the image curves $\tilde{E}_i$, we will have other three isogenies of degree two. However, one of these isogenies will be the dual of the isogeny $\varphi_i : \tilde{E} \to \tilde{E}_i$. As a result, we only two distinct isogenies that do not take us back. Pictorially, we have the following situation.



Given the two curves E and E', we know that there exist at least one isogeny of degree 2^e. To recover such an isogeny, we could try to compute all the isogenies of degree $2^{e/2}$ originating from E and E' and then look for a match between the nodes; see Figure 1.

This approach, known as the meet-in-the-middle attack, requires computing roughly $\approx 2^{e/2}$ operations. It also needs to store $\approx 2^{e/2}$ nodes, which for large enough e can soon become a problem. There exist variants of this attack where one can lower storage requirements at the cost of a higher computational cost.

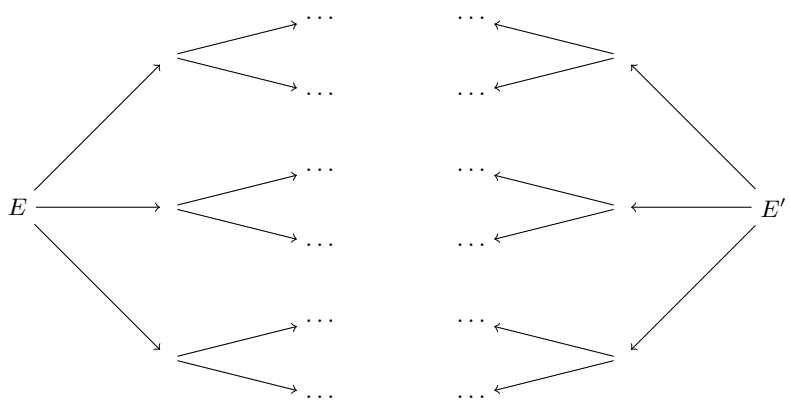


Fig. 1. Meet-in-the-middle attack.

5 Additional Readings

- Isogeny-based cryptography school, https://isogenyschool2020.co.uk/schedule/.
- "Mathematics of Isogeny Based Cryptography", De Feo [3].
- CRYPTOHACK, https://cryptohack.org/.

References

1. Bernstein, D.J., De Feo, L., Leroux, A., Smith, B.: Faster computation of isogenies of large prime degree **4**(1), 39–55 (2020). https://doi.org/10.2140/obs.2020.4.39
2. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology – ASIACRYPT 2018, Part III. Lecture Notes in Computer Science, vol. 11274, pp. 395–427. Springer, Heidelberg, Germany, Brisbane, Queensland, Australia (Dec 2–6, 2018). https://doi.org/10.1007/978-3-030-03332-3_15
3. De Feo, L.: Mathematics of isogeny based cryptography (2017), https://arxiv.org/abs/1711.04062
4. Vélu, J.: Isogénies entre courbes elliptiques. Comptes-Rendus de l'Académie des Sciences **273**, 238–241 (1971)