Isogeny Based Cryptography
Mid-term Report

Dintyala Rahul Bhardwaj

Supervised by Prof. Venkata Koppula and Prof. Surjeet Kour

1 Introduction

"'We are in a race against time to deploy post-quantum cryptography before quantum computers arrive" - Bernstein and Lange

Post-quantum cryptography is essential because it addresses the imminent threat posed by quantum computers, which could potentially break widely used cryptographic algorithms like RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). Quantum algorithms, such as Shor's algorithm, can efficiently factor large integers and compute discrete logarithms, undermining the security of current encryption methods. As advancements in quantum computing accelerate, transitioning to quantum-resistant algorithms is critical to safeguard sensitive data, ensure privacy, and maintain trust in digital communication systems. Without this transition, the integrity of financial transactions, personal communications, and national security could be at risk .

The focus of this project will be to study one of the prominent candidates in post-quantum cryptography, known as "isogeny-based cryptography."

Isogenies are morphisms in the category of elliptic curves. The foundation of isogeny-based cryptography traces back to the emergence of elliptic curve cryptography in the 1980s by Miller[Mil86] and Koblitz[Kob87], who proposed the integration of elliptic curves into the Diffie-Hellman key exchange protocol. In the early 2000s, the field witnessed significant advancements with the introduction of two pivotal concepts: pairing-based cryptography (PBCs) stemming from Joux's[Jou04] exploration of one-round tripartite DDH, and isogeny-based cryptography originating from the research efforts of Couveignes[Cou06], Teske[Tes06], Rostovtsev and Stolbunov[RS06]. Initially, isogeny-based cryptography lagged behind ECCs and PBCs until the late 2010s when the threat of quantum computers, capable of nullifying the latter, became apparent. Isogeny-based cryptography has demonstrated superior resilience against the cryptographic capabilities of quantum computers.

This project aims to find, via group actions, good abstractions and hard assumptions for isogenies (along the lines of the work done by Alamati et al. in [Ala+20]) as well as building cryptography on the basis of cryptographic group actions

2 Group Actions and Hard Homogeneous Spaces

The objective of this section is to introduce group actions, for their own sake and as a means of constructing cryptographic primitives. We begin by defining group actions.

Definition 2.1 (Group Action). *A group $\mathbb{G}$ is said to act on a set $\mathcal{X}$ if there is a map $\star : \mathbb{G} \times \mathcal{X} \to \mathcal{X}$ that satisfies the following two properties :*

- *If e is the identity element of $\mathbb{G}$, then for any $x \in \mathcal{X}$, we have $e \star x = x$.*
- *For any $g, h \in \mathbb{G}$ and any $x \in \mathcal{X}$, we have $(gh) \star x = g \star (h \star x)$.*

$\diamondsuit$

Based on the additional structure in the group action, the following definitions are given :

Definition 2.2. *A group action $(\mathbb{G}, \mathcal{X}, \star)$ is said to be :*

1. ***transitive** if for every $x_1, x_2 \in \mathcal{X}$, there exist a group element $g \in \mathbb{G}$ such that $x_2 = g \star x_1$. For such a transitive group action, the set $\mathcal{X}$ is called a homogeneous space for G.*
2. ***faithful** if for each group element $g \in \mathbb{G}$, either G is the identity element or there exists a set element $x \in \mathcal{X}$ such that $x \neq g \star x$.*
3. ***free** if for each group element $g \in \mathbb{G}$, g is the identity element if and only if there exists some set element $x \in \mathcal{X}$ such that $x = g \star x$.*
4. ***regular** if it is both free and transitive.*

$\diamondsuit$

We concern ourselves with regular group actions. Regularity of a group action induces a natural bijection between $\mathbb{G}$ and $\mathcal{X}$, $g \mapsto g \star x$. So if $\mathbb{G}$ (or $\mathcal{X}$) is finite, $|\mathcal{X}| = |\mathbb{G}|$.

Let $\mathbb{G}$ be a commutative group, $\mathcal{X}$ be a set, and $\star$ be a reular group action. The for any $x_1, x_2 \in \mathcal{X}$, there exists a unique $g \in \mathbb{G}$ such that $x_2 = g \star x_1$. Borrowing the notation from [Cou06], let $g := \delta(x_2, x_1)$. We also have that $(\exists x \in \mathcal{X}, g \star x = x) \implies g = e$.

The process of utilizing a mathematical construct, such as group actions, in the design of cryptographic primitives necessitates that certain operations be computationally efficient for practical implementation, while others must be inherently difficult to guarantee intractability and security.

The following are *easy*:

1. For $\mathbb{G}$:
   (a) Given a string g, decide if it represents an element in $\mathbb{G}$.
   (b) Given strings g_1, g_2 representing two elements in $\mathbb{G}$, compute $g_1 g_2, g_1^{-1}$ and decide if $g_1 = g_2$.
   (c) Find a random element in $\mathbb{G}$ with uniform probability.
2. For $\mathcal{X}$:
   (a) Given a string x, decide if h represents an element in $\mathcal{X}$.
   (b) Given $x_1, x_2 \in \mathcal{X}$, decide if $x_1 = x_2$.
3. For $\star$: Given $g \in \mathbb{G}$ and $x \in \mathcal{X}$ compute $g \star x$.

Definition 2.3. *Let $\mathbb{G}$ be an abelian group and $(\mathbb{G}, \mathcal{X}, \star)$ be. Then the following problems are defined :*

1. ***Vectorisation Problem**: Given x_1 and $x_2 \in \mathcal{X}$, find $\delta(x_2, x_1)$.*
2. ***Parallelisation Problem**: Given x_1, x_2, and $x_3 \in \mathcal{X}$, find the unique x_4 such that $\delta(x_2, x_1) = \delta(x_4, x_3)$.*
3. ***Parallel Testing Problem**: Given x_1, x_2, x_3, and $x_4 \in \mathcal{X}$ decide whether $\delta(x_2, x_1) = \delta(x_4, x_3)$.*

$\diamondsuit$

Remark 2.4. *Note that if vectorisation is easy, then so is parallelisation. If parallelisation is easy, then so is parallel testing. We have no reason to believe necessarily, the converse of either of these implications.* $\diamondsuit$

Definition 2.5 (Hard Homogeneous Space)**.** *A homogeneous space for which all the easy assumptions are true and vectorisation and parallelisation problems are hard is called a hard homogeneous space (HHS).* $\diamondsuit$

Definition 2.6 (Very Hard Homogeneous Space)**.** *A homogeneous space for which all the easy assumptions are true and Parallel Testing Problem is hard, is called a Very Hard Homogeneous Space (VHHS).* $\diamondsuit$

Example 2.7. *Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n. Let $\mathrm{Aut}(\mathbb{G})$ be the set of automorphisms of $\mathbb{G}$. Note that any homomorphism ϕ from $\mathbb{G} \to \mathbb{G}$ is entirely described by $\phi(g)$. If $\phi(g) = g^k$. Then ϕ is an automorphism if $\{mk \pmod{n}\}_{k=1}^{n} = \mathbb{Z}_n$, which happens if and only if $\gcd(k, n) = 1$. Consider the map $\Psi : \mathrm{Aut}(\mathbb{G}) \to \mathbb{Z}_n^*$ that maps $(g \mapsto g^c) \mapsto c$. This map is clearly an isomorphism.*

Let $\mathfrak{g}$ be the set of generators of $\mathbb{G}$. Then $\mathrm{Aut}(\mathbb{G})$ *acts regularly on* $\mathfrak{g}$ *through the action* $\star : \mathrm{Aut}(\mathbb{G}) \times \mathfrak{g} \to \mathfrak{g}$, $((g \mapsto g^c), h) \mapsto h^c$.

◊

2.1 *Key Exchange*

Consider the following Key-Exchange Protocol

Construction 2.8 (Key Exchange via. Hard Homogeneous Spaces). *Let $\mathbb{G}$ be an abelian group and $\mathcal{X}$ be a hard homogeneous space for $\mathbb{G}$ with respect to the action $\star$. Alice and Bob use $(\mathbb{G}, \mathcal{X}, \star)$ to derive a shared key as follows :*

1. *Alice samples $x_0 \leftarrow \mathcal{X}$, $g_1 \leftarrow \mathbb{G}$ and sends $(x_0, x_1 = g_1 \star x_0)$ to Bob.*
2. *Bob samples $g_2 \leftarrow \mathbb{G}$ and sends $x_2 = g_2 \star x_0$ to Alice.*
3. *Alice computes $g_1 \star x_2$ and Bob computes $g_2 \star x_1$.*

◊

The correctness for this procotol is clear since $g_1 \star x_2 = g_1 \star (g_2 \star x_0) = (g_1 g_2) \star x_0 = (g_2 g_1) \star x_0 = g_2 \star (g_1 \star x_0) = g_2 \star x_1$.

An eavesdropper can learn $(x_0, x_1 = g_1 \star x_0, x_2 = g_2 \star x_0)$. If an adversary $\mathcal{A}$ can solve the parallelization problem, then $\mathcal{A}(x_0, x_1, x_2) = x_3$ such that $\delta(x_3, x_2) = \delta(x_1, x_0) = g_1$. Since $x_3 = g_1 \star x_2 = g_1 \star (g_2 \star x_0) = (g_1 g_2) \star x_0$, which is the required key, this key-exchange protocol is only as safe as the parallelisation problem is hard. We capture this in the following definition.

Definition 2.9. *Let $\mathbb{G}$ be an abelian group, $\mathcal{X}$ be a homogeneous space for $\mathbb{G}$ and $(\mathbb{G}, \mathcal{X}, \star)$ be a regular group action. We say that the Decisional HHS problem is hard for $(\mathbb{G}, \mathcal{X}, \star)$ if, for any p.p.t. adversary $\mathcal{A}$, the following quantity is negligible:*

$$\left| \Pr\left[\begin{array}{c} x_0 \leftarrow \mathcal{X}, g_1, g_2 \leftarrow \mathbb{G} \\ 0 \leftarrow \mathcal{A}(x_0, g_1 \star x_0, g_2 \star x_0, (g_1 g_2) \star x_0) \end{array} \right] - \Pr\left[\begin{array}{c} x_0 \leftarrow \mathcal{X}, g_1, g_2, g_3 \leftarrow \mathbb{G} \\ 0 \leftarrow \mathcal{A}(x_0, g_1 \star x_0, g_2 \star x_0, g_3 \star x_0) \end{array} \right] \right|$$

◊

2.2 *Authentication*

Authentication refers to the process of verifying the identity of a user, system, or entity, and ensuring that the information exchanged between two parties is genuine and that the person or entity on the other side is who they claim to be.

Couveignes adapts the Feige-Fiat-Shamir identification scheme to get the following construction.

Construction 2.10 (Authentication via. Hard Homogeneous Spaces)**.** *Let* $\mathbb{G}$ *be an abelian group and* $\mathcal{X}$ *be a hard homogeneous space for* $\mathbb{G}$ *with respect to the action* $\star$ *and* x_0 *be an element of* $\mathcal{X}$. $(\mathbb{G}, \mathcal{X}, \star, h_0)$ *are publicly known.*
Every user i *samples a group element* g_i *from* $\mathbb{G}$*, computes* $x_i = g_i \star x_0$ *and publishes* x_i*. Let Alice and Bob be user* i *and user* j *respectively. If Alice wants to confirm Bob's identity, it will do the following :*

1. *Alice will find* x_j *from the publicly available record, sample a random group element* g_a *from* $\mathbb{G}$ *and send* $x_a = g_a \star x_j$ *to Bob.*
2. *Bob computes* $x_b = g_j^{-1} \star x_a$ *and sends it to Alice.*
3. *Alice verifies whether* $x_b = g_a \star x_0$*.*

◊

Correctness follows from the following : $g_a \star x_0 = (g_j^{-1} g_a g_j) \star x_0 = g_j^{-1} \star ((g_a g_j) \star x_0) = x_b$.

3 Group Action Models

3.1 Effective Group Action (EGA)

Definition 3.1 (Effective Group Action). *A group action $(\mathbb{G}, \mathcal{X}, \star)$ is* effective *if:*

1. *$\mathbb{G}$ is finite, with efficient algorithms for:*
   (a) ***Membership testing:*** *Check if a bit string represents a valid element in $\mathbb{G}$.*
   (b) ***Equality testing:*** *Check if two bit strings represent the same element in $\mathbb{G}$.*
   (c) ***Sampling:*** *Sample an element $g \in \mathbb{G}$.*
   (d) ***Inversion:*** *Compute g^{-1} for any $g \in \mathbb{G}$.*
2. *$\mathcal{X}$ is finite, with efficient algorithms for:*
   (a) ***Membership testing:*** *Check if a bit string represents an element in $\mathcal{X}$.*
   (b) ***Unique representation:*** *Compute a canonical representation $\hat{x}$ for any $x \in \mathcal{X}$.*
3. *A known distinguished element $x_0 \in \mathcal{X}$ (origin).*
4. *An efficient algorithm exists for computing $g \star x$ given any $g \in \mathbb{G}$ and $x \in \mathcal{X}$.*

$\diamondsuit$

Definition 3.2 (One-Way Group Action). *A group action $(\mathbb{G}, \mathcal{X}, \star)$ is a one-way if the family of efficiently computable functions $\{f_x : \mathbb{G} \to \mathcal{X}\}_{x \in \mathcal{X}}$ is one-way, where $f_x : g \mapsto g \star x$.* $\diamondsuit$

Definition 3.3 (Weak Unpredictable Group Action). *A group action $(\mathbb{G}, \mathcal{X}, \star)$ is weakly unpredictable if the family of efficienly computable permutations $\{\pi_g : \mathcal{X} \to \mathcal{X}\}_{g \in \mathbb{G}}$ is* $\diamondsuit$

3.2 Restricted Effective Group Action (REGA)

In the previous section, we made the assumption (or hoped) that for *any* $g \in \mathbb{G}$ and $x \in \mathcal{X}$, computing $g \star x$ is *easy*.

The group $\mathbb{G}$, the homogeneous space $\mathcal{X}$, and the corresponding group action $\star$ we will be working with in the isogeny-based cryptography setting will be non-trivial. Evaluating the group action efficiently for all $g \in \mathbb{G}$ and $x \in \mathcal{X}$ will not be possible.

Since every group has a set of generators, if one can evaluate efficiently the group action for that set of generators, then as long as the exponents are polynomial in the security parameter, the group action can be evaluated efficiently.

[ADMP2020] capture this limitation through their definition of a *Restricted Effective Group Action* (REGA).

Definition 3.4 (Restricted Effective Group Action)**.** *Let* $(\mathbb{G}, \mathcal{X}, \star)$ *be a group action with a not-necessarily minimal generating set* $\mathbf{g} = \{g_1, \ldots, g_n\}$ *and* $G = \langle \mathbf{g} \rangle$*. The action is said to be* **g***-restricted effective if:*

1. $\mathbb{G}$ *is finite, and* $n = poly(\log |\mathbb{G}|)$*.*
2. $\mathcal{X}$ *is finite, with efficient algorithms for:*
   (a) ***Membership testing:*** *Check if a bit string represents an element in* $\mathcal{X}$*.*
   (b) ***Unique representation:*** *Compute a canonical string* $\hat{x}$ *for any* $x \in \mathcal{X}$*.*
3. *A known distinguished element* $x_0 \in \mathcal{X}$ *(origin).*
4. *There exists an efficient algorithm that, given any* $i \in [n]$ *and a bit string representation of* $x \in \mathcal{X}$*, computes* $g_i \star x$ *and* $g_i^{-1} \star x$*.*

$\diamondsuit$

3.3 *Known-Order Effective Group Action (KEGA)*

[ADMP2020] extend the Effective Group Action (EGA) model by assuming the group structure of $\mathbb{G}$ is explicitly known. By "known order," we mean that the group $\mathbb{G}$ has a known set of generators $\mathbf{g} = \{g_1, \ldots, g_n\}$ along with their corresponding orders $(m_1, \ldots, m_n)$. This is equivalent to expressing $\mathbb{G}$ as a direct sum decomposition $\mathbb{G} \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{m_i}$.

A special case of this model is when $\mathbb{G}$ is cyclic, meaning $\mathbb{G} = \langle g \rangle \cong \mathbb{Z}/m\mathbb{Z}$. We define the lattice $\mathcal{L} = \bigoplus_{i=1}^{n} m_i \mathbb{Z}$, and the map $\phi : \mathbb{Z}^n / \mathcal{L} \to \mathbb{G}$, where $(a_1, \ldots, a_n) \mapsto \prod_{i=1}^{n} g_i^{a_i}$. This mapping is an effective isomorphism, and its inverse corresponds to solving a generalized discrete logarithm problem.

If $(\mathbb{G}, \mathcal{X}, \star)$ is an instance of the EGA, it can be shown that $(\mathbb{Z}^n/\mathcal{L}, \mathcal{X}, \star)$ is also an EGA via the isomorphism ϕ. Consequently, $\mathbb{Z}^n/\mathcal{L}$ serves as a standard representation of the group $\mathbb{G}$.

Definition 3.5 (Known-Order Effective Group Action (KEGA) Model). *A Known-Order Effective Group Action (KEGA) is an EGA $(\mathbb{Z}^n/\mathcal{L}, \mathcal{X}, \star)$, where the lattice $\mathcal{L}$ is determined by the tuple $(m_1, \ldots, m_n)$, representing the orders of the generators.* ♢

Remark 3.6. *Since for an abelian group $\mathbb{G}$, Shor's Algorithm and its generalization precisely compute an isomorphism $\mathbb{G} \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{m_i}$, KEGA and abelian EGA are quantumly equivalent.* ♢

3.4 *Generic Group Action Model (GGAM)*

3.5 *Algebraic Group Action Model*

Definition 3.7 (Cyclic Effective Group Action). *Let $(\mathbb{G}, \mathcal{X}, \star, \hat{x})$ be an effective group action satisfying the following properties:*

1. *The group $\mathbb{G}$ is cyclic of order N for some known $N \in \mathbb{N}$.*
2. *There exists a generator $g \in \mathbb{G}$ with known representation (that is $\mathbb{G} = \langle g \rangle$).*
3. *For any element $h \in \mathbb{G}$, the element $a \in \mathbb{Z}_N$ satisfying $h = g^a$ is efficiently computable.*
4. *The group action is regular.*

Then $(\mathbb{G}, X, \star, \hat{x})$ is a cyclic (known-order) effective group action (CEFA). In other words, a CEGA is an EGA for which there exists an isomorphism $\phi : \mathbb{Z}_N \to \mathbb{G}$ efficiently computable in both directions. CEGA is hence, equivalently denoted by $(\mathbb{Z}_N, \mathcal{X}, \star, \hat{x})$. ♢

4 Elliptic Curves and Isogenies

Definition 4.1 (Plane Curves). *An affine plane algebraic curv $\mathcal{C}$ defined over $\mathbb{k}$ is defined by a non-constant polynomial $f(x,y) = \mathbb{k}[x,y]$, such that $\mathcal{C} : f(x,y) = 0$.* ♢

Example 4.2. $f(x,y) = y - 2x^2$, $f(x,y) = y - mx - c$ ♢

Let $\mathbb{k}$ be the algebraic closure of $\mathbb{k}$.

Definition 4.3. *The set of points (x,y) in $\mathbb{k}^2$ (resp. $\overline{\mathbb{k}}$) such that $f(x,y) = 0$ is called the set of $\mathbb{k}$-rational points (resp. set of $\overline{\mathbb{k}}$-rational points).* ♢

Definition 4.4 (Smooth Curve). *A plane curve $\mathcal{C} : f(x,y) = 0$ is called smooth if and only if $\left(\frac{\partial f}{\partial x}(x,y), \frac{\partial f}{\partial y}(x,y)\right) \neq (0,0)$ for all $(x,y) \in \mathcal{C}(\overline{\mathbb{k}})$.* ♢

Example 4.5. *Let $f(x,y) = y^2 - x^3$, $\mathcal{C} : y^2 = x^3$. Then $\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) = (-3x^2, 2y) = (0,0) \iff (x,y) = (0,0)$. Therefore, $\mathcal{C}$ is not smooth.* ♢

Since the goal of this section is to the showcase the details of the group action behind the abstraction, we will not go into too much mathematical detail and take certain results as facts.

Definition 4.6 (Elliptic Curve). *Let $\mathbb{k}$ be a field. An elliptic curve $E/\mathbb{k}$ is a smooth projective algebraic curve of genus 1 defined over $\mathbb{k}$ with a distinguished $\mathbb{k}$-rational point $\mathcal{O}_E$.* ♢

Fact 1. *Let $f(x,y) \in \mathbb{k}[x,y]$ of degree d. If the curve $\mathcal{C} : f(x,y) = 0$ is smooth, then its genus is $g = \frac{(d-1)(d-2)}{2}$.*

Considering this fact and 4.6, we equate 1 with $(d-1)(d-2)/2$ to get that $d = 3$. So, $\mathcal{C} : f(x,y) = 0$ is an elliptic curve if and only if :

1. $f(x,y) = 0$, $\frac{\partial f}{\partial x}(x,y) = 0$, $\frac{\partial f}{\partial y} = 0$ has no solution in $\mathbb{C}^2$.
2. $\deg f = 3$
3. the point at infinity is non-singular.

Lemma 4.7. *The short Weierstrass equation $y^2 = x^3 + Ax + B$ defines a genus one curve if and only if $4a_4^3 + 27a_6^2 \neq 0$.*

Proof. Suppose there were a point $(x,y) \in \overline{\mathbb{k}}^2$ such that $\partial f/\partial x = -3x^2 - A = 0$, $\partial f/\partial y = 2y = 0$, and $y^2 = x^3 + Ax + B$. These equations give us $x^3 + Ax + B = 0$, $3x^2 + A = 0$. Thefore, $\frac{2}{3}Ax + B = 0$ or $x = -\frac{3B}{2A}$. If $3(-3B/2A)^2 + A \neq 0$, then these equations have no solution. Therefore the curve is smooth if and only if $-27B^2 - 4A^3 = 0$. □

Definition 4.8 (Short Weierstrass Form). *The curve $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{k}$, $4A^3 + 27B^2 \neq 0$ is an elliptic curve defined over $\mathbb{k}$ in Short Weierstrass form.* $\Diamond$

Fact 2. *By Riemann-Roch Theorem it can be shown that any plane curve has genus one if and only if it is isomorphic to a plane curve of the form :*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

If the characteristic of $\mathbb{k}$ is not 2 (resp. 2 or 3), then a_1 and a_3 (resp. a_1, a_2, and a_3) can be made zero via a linear change of coordinates.

Combining this fact with 4.8, we note that every elliptic curve defined over $\mathbb{k}(\mathrm{char}(\mathbb{k}) \neq 2, 3)$ is isomorphic to an elliptic curve in short Weierstrass form.

Example 4.9. *$E : y^2 = x^3 + x + 3$ over $\mathbb{F}_5$, $y^2 = x^3 + 2x + 27$ over $\mathbb{F}_{47}$.* $\Diamond$

We define the following sets :

$$E(\mathbb{k}) := \{(x, y) \in \mathbb{k}^2 : y^2 = x^3 + Ax + B\}$$
$$E(\overline{\mathbb{k}}) := \{(x, y) \in \overline{\mathbb{k}}^2 : y^2 = x^3 + Ax + b\}.$$

Example 4.10. *Let $E : y^2 = x^3 + x$ over $\mathbb{F}_3$. Then $E(\overline{\mathbb{F}_3})$ is infinite whereas $E(\mathbb{F}_3) = \{(0, 0), (2, 1), (2, 2), O_E\}$.* $\Diamond$

Definition 4.11 (Group Law on Elliptic Curves). *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E different from the point at infinity, then we define a composition law $\oplus$ on E as follows :*

1. *$P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$ for any point $P \in E$.*
2. *If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 \oplus P_2 = \mathcal{O}$.*
3. *Otherwise set $\lambda := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \frac{3x_1^2 + A}{2y_1} & P = Q \end{cases}$. Then the point $P_1 \oplus P_2 = (\lambda^2 - x_1 - x_2, -\lambda x_3 - y_1 + \lambda x_1)$.*

$\Diamond$

Remark 4.12. *It can be verified that the sets $E(\mathbb{k})$, and $E(\overline{\mathbb{k}})$ along with the operation $\oplus$ form abelian groups. Whereever unambiguous, we will just write $+$ instead of $\oplus$.* $\Diamond$

Definition 4.13 (Isogeny). *Let E_1 and E_2 be two elliptic curves defined over $\Bbbk$. An isogeny $\varphi : E_1 \to E_2$ is a non-constant rational map which is also a group homomorphism.* $\diamondsuit$

Lemma 4.14. *Let E_1 and E_2 be elliptic curves over $\Bbbk$ in short Weierstrass form, and let $\varphi : E_1 \to E_2$ be an isogeny. Then φ can be defined by an affine rational map of the form $\varphi(x,y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y\right)$, where $f_1, f_2, g_1, g_2 \in \Bbbk[x]$ and* $\gcd(f_1, g_1) = \gcd(f_2, g_2) = 1$.

Definition 4.15 (Standard Form of an Isogeny). *Let E_1 and E_2 be elliptic curves over $\Bbbk$, then an isogeny $\varphi : E_1 \to E_2$ is said to be in standard form if :*

$$\varphi(x,y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y\right),$$

where $f_1, f_2, g_1, g_2 \in \Bbbk[x]$ and $\gcd(f_1, g_1) = \gcd(f_2, g_2) = 1$. $\diamondsuit$

Lemma 4.16. *Let $E_1 : y^2 = f_1(x)$ and $E_2 : y^2 = f_2(x)$ be two elliptic curves over $\Bbbk$ and let $\varphi : \varphi(x,y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y\right)$ be an isogeny from E_1 to E_2 in standard form. Then g_2^3 divides g_2^2 and g_2^2 divides $g_1^3 f_1$. Moreover, $g_1(x)$ and $g_2(x)$ have the same set of roots in $\overline{\Bbbk}$.*

Corollary 4.17. *Let $\varphi : \varphi(x,y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y\right)$ be an isogeny from $E_1 \to E_2$ in standard form. Then $\ker\varphi = \{P \in E_1(\overline{\Bbbk}) : \varphi P = O_{E_2}\} = \{(x_0, y_0) \in E_1(\overline{\Bbbk}) : g_1(x_0) = 0\} \cup \{\mathcal{O}_{E_1}\}$. The kernel of φ is a finite subgroup of $\mathbb{E}_1(\overline{\Bbbk})$.*

Definition 4.18 (Degree and Separability of an Isogeny). *Let $\varphi(x,y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y\right)$ be an isogeny in standard form. The degree of φ is $\deg\varphi :=$ $\max\{\deg f_1, \deg g_1\}$, and we say that φ is separable if the derivative of $\frac{f_1(x)}{g_1(x)}$ is non-zero; otherwise we say that φ is serparable.*

$\diamondsuit$

Example 4.19. *Let $E : y^2 = x^3 + x + 3$ over $\mathbb{F}_5$ and $E' : y^2 = x^3 + x$ over $\mathbb{F}_5$. Let $\varphi : E \to E'$, $(x,y) \mapsto \left(\frac{x^2-x-1}{x-1}, \frac{x^2-2x-2}{x^2-2x+1}y\right)$ be an isogeny in standard form. Then :*

- $\deg\varphi = 2$,
- $\left(\frac{x^2-x-1}{x-1}\right)' = 1 + \frac{1}{(x-1)^2} \neq 0$, *and*

- $\ker \varphi = \{(x_0, y_0) \in E_1(\bar{\mathbb{k}}) : x_0 - 1 = 0\} \cup \{\mathcal{O}_{E_1}\} = \{(1,0), \mathcal{O}_{E_1}\} \cong \mathbb{Z}/2\mathbb{Z}$.

$\diamondsuit$

Definition 4.20 (m-torsion subgroup)**.** *Let E be an elliptic curve over $\mathbb{k}k$. Let $[m] : E \to E$ denote the map $P \mapsto mP$. Then the kernel of $[m]$ is called the m-torsion subgroup of E.* $\diamondsuit$

Example 4.21. *Let $E : y^2 = x^3 + x + 3$ over $\mathbb{F}_5$. Let $[2] : E \to E$ denote the map $P \mapsto 2P = P + P$. The multiplication by 2 isogeny in standard form is given by : $(x, y) \mapsto \left(\frac{x^4-2x^2+x+1}{x^3+x+3}, \frac{x^6-2x+2}{x^6+2x^4+x^3+x^2+x-1}y\right)$. Then :*

- $\deg [2] = 4$,
- $[2]$ *is separable, and*
- $E[2] = \ker [2] = \{P \in E(\overline{\mathbb{F}_5}) : 2P = \mathcal{O}_E\} = \{(x_0, y) \in E(\overline{\mathbb{F}_5}) : x_0^3 + x_0 + 3 = 0\} = \{(1,0), (\alpha, 0), (4\alpha + 4), \mathcal{O}_E\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\diamondsuit$

Example 4.22. *Let $E : y^2 = x^3 + Ax + B$ over $\mathbb{k}$. Let $[-1] : E \to E$ denote the map $P \mapsto -P$ or $(x, y) \mapsto (x, -y)$. Then :*

- $\deg [-1] = 1$,
- $[-1]$ *is separable, and*
- $\ker [-1] = \{\mathcal{O}_E\}$ *is trivial.*

$\diamondsuit$

Example 4.23. *Let $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$, $q = p^n$ for a prime p. Then the Frobenius Endomorphism $\pi_E : E \to E$ maps $(x, y) \mapsto (x^q, y^q)$. Then :*

- $\deg \pi_E = q$,
- π_E *is inseparable* $((x^q)' = qx^{q-1} = 0)$, *and*
- $\ker \pi_E = \{\mathcal{O}_E\}$ *is trivial.*

$\diamondsuit$

Fact 3. *An isogeny φ is separable if and only if $|\ker \varphi| = \deg \varphi$.*

Definition 4.24 (Cyclic Isogeny)**.** *An isogeny φ is said to be cyclic if $\ker \varphi$ is a cyclic subgroup.* $\diamondsuit$

Definition 4.25 (Endomorphism, Isomorphism, Automorphism). *Let E be an elliptic curve. An isogeny from E to itself is called an endomorphism. An isogeny of degree 1 is called an isomorphism. An endomorphism which is also an isomorphism is called an automorphism.* $\diamondsuit$

Definition 4.26 (Frobenius Map). *Let E be an elliptic curve over $\mathbb{F}_p$. Define the Frobenius map $\pi : E \to E$ by $(x, y) \mapsto (x^p, y^p)$. The Frobenius map is a group homomorphism, so : $[n] \circ \pi = \pi \circ [n]$ for all $n \in \mathbb{Z}$.* $\diamondsuit$

Definition 4.27 (Supersingular Elliptic Curve). *Let E be an elliptic curve over $\mathbb{F}_q$. Then the following are equivalent :*

1. *E is supersingular.*
2. *$E[p] = \{P \in E(\overline{\mathbb{F}_q}) : pP = O_E\}$ is trivial.*
3. *$|E(\mathbb{F}_q)| \equiv 1 \pmod p$.*

$\diamondsuit$

Example 4.28. *Let $E : y^2 = x^3 + 1$ be an elliptic curve over $\mathbb{F}_5$. Then $E(\mathbb{F}_5) = \{(2, 2), (2, 3), (0, 1), (0, 4), (4, 0), O_E\}$, so $|E(\mathbb{F}_5)| = 6 \equiv 1 \pmod 5$. Hence E is supersingular.* $\diamondsuit$

Definition 4.29 (Ordinary Elliptic Curve). *Let E be an elliptic curve. If E is not supersingular, then it is ordinary.* $\diamondsuit$

Example 4.30. *Let $E : y^2 = x^3 + x$ be an ellitpic curve over $\mathbb{F}_5$. Then $E(\mathbb{F}_5) = \{(0, 0), (2, 0), (3, 0), O_E\}$, so $|E(\mathbb{F}_5)| = 4 \not\equiv 1 \pmod 5$. Hence E is ordinary.* $\diamondsuit$

Fact 4. *When $p \geq 5$,*

1. *$y^2 = x^3 + 1$ over $\mathbb{F}_p$ is supersingular if and only if $p \equiv 2 \pmod 3$.*
2. *$y^2 = x^3 + x$ over $\mathbb{F}_p$ is supersingular if and only if $p \equiv 3 \pmod 3$.*

Fact 5. *Let $\varphi : E_1 \to E_2$ be an isogeny. Then E_1 is supersingular if and only if E_2 is supersingular. E_1 is ordinary if and only if E_2 is ordinary.*

Lemma 4.31. *The Frobenius map π satisfies $\pi^2 - t\pi + p = 0$, where t is an integer known as the trace of Frobenius map and $t^2 - 4p < 0$. We call $X^2 - tX + p$ the characteristic polynomial of Frobenius.*

Remark 4.32. *One immediate consequence of this lemma is that any endomorphism in $\mathbb{Z}[\pi]$, say $\sum_{i=1}^{n} a_i \pi^i = \alpha + \beta\pi$ can be decomposed by recursively replacing π^2 with $t\pi - p$ to get an endomorphism of the form $\alpha + \beta\pi$.* $\diamondsuit$

Theorem 4.33. *If $p \neq 2, 3$, an elliptic curve E over $\mathbb{F}_p$ is supersingular if and only if the trace of Frobenius is* 0*.*

Remark 4.34. *Since in further text we concern ourselves with supersingular elliptic curves, the Frobenius endomorphism π satisfies an the equation $\pi^2 = -p$. Hence, $\mathbb{Z}[\pi] \cong \mathbb{Z}[\sqrt{-p}]$.* $\diamondsuit$

Proposition 4.35 (Vélu)**.** *Given a finite subgroup $G \leq E_1(\overline{\mathbb{F}_q})$, there exists an elliptic curve E_2 and a (separable) isogeny $\varphi : E_1 \to E_2$ with $\ker\varphi = G$. The curve E_2 and the isogeny φ are unique up to isomorphism, meaning that if $\varphi' : E_1 \to E_3$ is another isogeny with kernle G then there is an isomorphism $\eta : E_2 \to E_3$ and $\varphi' = \eta \circ \varphi$.*

Theorem 4.36. *Let E_1, E_2, and E_3 be ellitpic curves over $\Bbbk$ and $\varphi : E_1 \to E_2$, $\psi : E_1 \to E_3$ isogenies over $\Bbbk$. Suppose $\ker\varphi \subseteq \ker\psi$ and that ψ is separable. Then there is a unique isogeny $\lambda : E_2 \to E_3$ defined over $\Bbbk$ such that $\psi = \lambda \circ \varphi$.*

Corollary 4.37. *Let E_1 and E_2 be two elliptic curves over $\Bbbk$ and $\varphi : E_1 \to E_2$, an isogeny with non-cyclic kernel. Then $\varphi = [n] \circ \psi$ where $\psi : E_1 \to E_2$ is an isogeny with cyclic kernel.*

We've seen that $\mathbb{Z}[\pi]$ is a subset of the endomorphism ring of any elliptic curve and also that for the case of an super singular elliptic curve E over $\mathbb{F}_p$, $\mathbb{Z}[\pi] \cong \mathbb{Z}[\sqrt{-p}]$. Therefore any ideal of $\mathbb{Z}[\sqrt{-p}]$ can be interpreted as a set of endomorphisms of E.

Consider an elliptic curve E such that $\mathbb{Z}[\sqrt{-p}] \subseteq \mathrm{End}(E)$. Let G be a finite subgroup of $E(\overline{\mathbb{F}_p})$, and define the ideal associated to G as follows:

$$I(G) = \{a + b\sqrt{-p} \in \mathbb{Z}[\sqrt{-p}] \mid (a + b\pi)(P) = 0 \;\forall\; P \in G\}.$$

For an isogeny $\varphi : E \to E'$, we define the **kernel ideal** by:

$$I_\varphi = I(\ker\varphi) = \{a + b\sqrt{-p} \in \mathbb{Z}[\sqrt{-p}] \mid (a + b\pi)(P) = 0 \;\forall\; P \in \ker\varphi\}.$$

Proposition 4.38. *The set $I(G)$ forms an ideal. Furthermore, if $H \subseteq G$, then $I(G) \subseteq I(H)$.*

For any integral ideal $I \subseteq \mathbb{Z}[\sqrt{-p}]$, we define the set $E[I]$ as:

$$E[I] = \{P \in E \mid \alpha(P) = 0 \;\forall\; \alpha \in I\},$$

where I is identified with a subset of $\mathrm{End}(E)$, and $\alpha : E \to E$ represents the action of α on E.

Remark 4.39. *The set $E[I]$ can be viewed as the intersection of the kernels of all non-zero elements in I. Since each kernel is a finite subgroup of E, $E[I]$ is finite for any non-zero ideal I.* $\diamondsuit$

Proposition 4.40. *If I and J are two ideals in $\mathbb{Z}[\sqrt{-p}]$ such that $I \subseteq J$, then $E[J] \subseteq E[I]$.*

Since $E[I]$ is a finite subgroup of E, it defines an isogeny $\varphi_I : E \to E_I$ with kernel $E[I]$, where E_I is the image curve (up to isomorphism). Thus, we associate to each ideal I the isogeny $\varphi_I : E \to E_I$.

It is known that the degree of φ_I is given by $\deg(\varphi_I) = N(I)$, where $N(I)$ denotes the norm of the ideal I. This fact can be directly verified for ideals of the form $I = (l, \pm b + \sqrt{-d})$ in $\mathbb{Z}[\sqrt{-d}]$, where l is a prime and $b^2 \equiv -d \pmod{l}$. In such cases, $\deg(\varphi_I) = l = N(I)$. Another simple case is when $I = (n)$ and the isogeny is $\varphi_I = [n]$. The general case follows by decomposing into ideals or isogenies of prime norm or degree.

Lemma 4.41. *Let $p \equiv 1 \pmod{4}$ and let E be a supersingular elliptic curve over $\mathbb{F}_p$. Suppose I is an ideal in $\mathbb{Z}[\sqrt{-p}]$, and let $\varphi_I : E \to E'$ be the isogeny associated with I. Denote by π_E and $\pi_{E'}$ the p-power Frobenius maps on E and E', respectively. Then, we have the relation $\varphi_I \circ \pi_E = \pi_{E'} \circ \varphi_I$.*

In other words, the isogeny $\varphi_I : E \to E'$ defined by the ideal I is defined over $\mathbb{F}_p$, and E' is also defined over $\mathbb{F}_p$.

Now, let $p \equiv 1 \pmod{4}$, and let E be a supersingular elliptic curve over $\mathbb{F}_p$. Consider the ideal class group of $\mathbb{Z}[\sqrt{-p}]$. For an ideal I in $\mathbb{Z}[\sqrt{-p}]$, define $I \star E$ to be the curve E_I, which is the image of the isogeny φ_I as described above.

From Lemma 4.41, note that $E_I = I \star E$ is defined over $\mathbb{F}_p$. We now demonstrate that E_I is also supersingular, and consequently, we have $\mathbb{Z}[\sqrt{-p}] \subseteq \mathrm{End}(E_I)$.

Lemma 4.42. *Let E over $\mathbb{F}_p$ be a supersingular elliptic curve, and let $\varphi : E \to E'$ be an isogeny defined over $\mathbb{F}_p$. Then, E' is also supersingular.*

Proof. Let π be the Frobenius endomorphism on E, and let π' be the Frobenius on E'. Since E is supersingular, we have $\pi^2 = [-p]$. By Lemma 4.41, we have: $\pi'^2 \circ \varphi = \varphi \circ \pi^2 = \varphi \circ [-p] = [-p] \circ \varphi$. This implies that for all points $P \in E$, we have $\pi'^2(\varphi(P)) = [-p]\varphi(P)$. Since isogenies are surjective, it follows that $\pi'^2 = [-p]$ on all points of E'. Hence, $\pi'^2 = -p$, and therefore, E' is supersingular. $\square$

We now show that there is a well-defined action of ideal classes on the isomorphism classes of elliptic curves.

Lemma 4.43. *A non-zero principal ideal $I = (\alpha)$ corresponds to an endomorphism.*

Proof. Since $\alpha \in I$, we have $E[I] \subseteq \ker(\alpha)$. Conversely, every element of (α) is a multiple of α and thus has a kernel containing the kernel of α. Therefore, $E[I] = \ker(\alpha)$. Let $\varphi_I : E \to E_I$ be the isogeny uniquely determined by the kernel $\ker(\alpha)$. It follows that $\varphi_I = \alpha$ (up to isomorphism), which is an endomorphism. □

Lemma 4.44. *Let $I, J \subseteq \mathbb{Z}[\sqrt{-p}]$ be non-zero ideals. Then, $\varphi_{IJ} = \varphi_J \circ \varphi_I$.*

Proof. Let $P \in \ker(\varphi_J \circ \varphi_I)$. By definition, this implies that $\varphi_I(P) \in \ker(\varphi_J)$. In other words, for all $\beta \in J$, we have $\beta(\varphi_I(P)) = 0$, where 0 denotes the identity element of the elliptic curve. Since each $\beta \in J$ can be written as $\beta = a + b\pi$ for some integers a and b, applying Lemma 4.41 gives $\beta \circ \varphi_I = \varphi_I \circ \beta$. Therefore, we obtain $\varphi_I(\beta(P)) = 0$, which shows that $\alpha(\beta(P)) = 0$ for all $\alpha \in I$ and $\beta \in J$. Thus, $P \in \ker(\varphi_{IJ})$.

Now, for the converse, assume $P \in \ker(\varphi_{IJ})$. This means that for all $\alpha \in I$ and $\beta \in J$, we have $\alpha(\beta(P)) = 0$. Consequently, $\beta(P) \in E[I]$, which implies $\varphi_I(\beta(P)) = 0$. Using Lemma 4.41, it follows that $\beta(\varphi_I(P)) = 0$ for all $\beta \in J$, meaning that $\varphi_I(P) \in E[J]$. Therefore, $P \in \ker(\varphi_J \circ \varphi_I)$.

Since the kernels of φ_{IJ} and $\varphi_J \circ \varphi_I$ coincide, the isogenies φ_{IJ} and $\varphi_J \circ \varphi_I$ must also be the same, up to isomorphism.

□

Lemma 4.45. *Suppose $I \sim J$ as ideals. Let $\varphi_I : E \to E_I$ and $\varphi_J : E \to E_J$. Then $E_I \cong E_J$.*

Lemma 4.46. *Let E_1 and E_2 be supersingular elliptic curves over $\mathbb{F}_p$ such that $E_1 \cong E_2$ over $\mathbb{F}_p$. Let I be an ideal in $\mathbb{Z}[\sqrt{-p}]$. Then $I \star E_1 \cong I \star E_2$.*

Theorem 4.47. *Let $p \equiv 1 \pmod 4$. Then $Cl(\mathbb{Z}(\sqrt{-p}))$ acts on the set of isomorphism classes of curves defined over $\mathbb{F}_p$ by :*

$$(E, I) \mapsto I \star E$$

where $I \star E$ is the curve E_I defined by the isogeny $\varphi_I : E \to E_I$ with kernel $E[I]$.

5 Future Work

As highlighted in this report, a lot of different models are being studied to capture group actions in a post-quantum setting. My goal for the next few months is to do a comparative study between these various models as well as do an extensive literature review, see what primitives are yet to be built using group actions and fill in those gaps.

A recent paper by Zhandry tries to build Quantum Lightening using group actions. The goal is to understand and build on this work.

A paper by Alamati *et al.*builds a weaker version of Trap-door claw free functions using group actions and extended-LHS assumption. Another goal is to see if a stronger version of TCFs could be built using other models highlighted in this report.

References

[Mil86] Victor S. Miller. "Use of Elliptic Curves in Cryptography". In: *Advances in Cryptology — CRYPTO '85 Proceedings*. Ed. by Hugh C. Williams. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426. ISBN: 978-3-540-39799-1.

[Kob87] Neal Koblitz. "Elliptic curve cryptosystems". In: *Mathematics of computation* 48.177 (1987), pp. 203–209.

[Jou04] Antoine Joux. "A one round protocol for tripartite Diffie–Hellman". In: *Journal of cryptology* 17.4 (2004), pp. 263–276.

[Cou06] Jean-Marc Couveignes. "Hard homogeneous spaces". In: *Cryptology ePrint Archive* (2006).

[RS06] Alexander Rostovtsev and Anton Stolbunov. "Public-key cryptosystem based on isogenies". In: *Cryptology ePrint Archive* (2006).

[Tes06] Edlyn Teske. "An elliptic curve trapdoor system". In: *Journal of cryptology* 19 (2006), pp. 115–133.

[Ala+20] Navid Alamati et al. "Cryptographic group actions and applications". In: *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II 26*. Springer. 2020, pp. 411–439.