

https://dspace.org/

# Elliptic curve cryptography and related secrecy systems

**Mkhatshwa, Nokuzola**

**2022**
https://hdl.handle.net/10539/34606

Downloaded from a DSpace repository. https://dspace.org/

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG
SCHOOL OF MATHEMATICS

MASTER'S DISSERTATION

# Elliptic Curve Cryptography and Related Secrecy Systems

*Author:*
Nokuzola Mkhatshwa

*Supervisor:*
Dr. Alexander Davison

# Declaration

I declare that this dissertation is my own, unaided work. It is being submitted for the Degree of Master of Science at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination at any other University.



(Signature of candidate)

09 day of June 20 22 at Apollo Apartment

# Acknowledgement

I would like to thank my supervisor, Dr. A. Davison for the guidance and support he has shown me throughout the duration of this dissertation. My sincere gratitude goes to my family and friends for always being there for me and encouraging me to do even better. Lastly, I would like to thank the National Research Foundation (NRF) for sponsoring my tuition.

**Abstract**

In this dissertation, we discuss pre- and post-quantum cryptography. The Diffie-Hellman key-exchange protocol is known as the foundation of public-key cryptography. Public-key cryptography is widely used, Elliptic Curve Cryptography (ECC) in particular. But there is a problem: quantum computers. In 1999, Peter Shor introduced a quantum algorithm that posed a great threat to public-key cryptosystems. However, isogeny-based cryptography is not vulnerable to Shor's algorithm, hence isogeny-based cryptosystems attempts to mitigate the threats posed by quantum computers. This dissertation will review ECC, review mappings between elliptic curves (isogenies), and then show an isogeny-based, quantum-resistant version of the Diffie-Hellman key-exchange protocol.

# Contents


1 Introduction . . . . . 4
1.1 Asymmetric Cryptography . . . . . 5
1.2 Elliptic Curve Cryptography . . . . . 6
1.3 Outline . . . . . 7
2 Preliminaries . . . . . 9
2.1 Diffie-Hellman key-exchange . . . . . 9
2.2 Discrete logarithm problem . . . . . 10
3 Elliptic Curves and Elliptic Curve Arithmetic . . . . . 12
3.1 Projective spaces . . . . . 12
3.2 Group Law . . . . . 13
4 Torsion subgroups of elliptic curves . . . . . 24
5 Elliptic curves over finite fields . . . . . 26
6 Early Elliptic Curve Cryptosystems . . . . . 29
6.1 Massey-Omura elliptic curve . . . . . 29
6.2 ElGamal for elliptic curves . . . . . 30
6.3 Elliptic Curve Discrete Logarithm Problem (ECDLP) . 30
7 Isogenies . . . . . 32
8 Isogenies and their applications . . . . . 36
8.1 Elliptic curves over the Complex numbers $\mathbb{C}$ . . . . . 36
8.2 The Endomorphism Ring . . . . . 44
8.3 Schoof's algorithm . . . . . 47
8.4 Schoof-Elkies-Atkin(SEA)-algorithm . . . . . 48
8.5 Isogeny graphs . . . . . 50
8.6 Application: Irreducible polynomials . . . . . 54
9 Cryptography from isogeny graphs . . . . . 56
9.1 Expander graphs . . . . . 56
9.2 Supersingular isogeny graph-based cryptography . . . . 60

9.3 Charles, Lauter and Goren's key-exchange . . . . . 61
9.4 Security: Hardness assumption . . . . . 63
10 Post-quantum key exchange . . . . . 65
10.1 Key-exchange from isogeny graphs . . . . . 66
10.2 Supersingular Isogeny Diffie-Hellman (SIDH) . . . . . 70
10.3 Computing isogenies of a given kernel. . . . . 72
11 Conclusion . . . . . 77

**Appendix** **79**
1 Application: Factoring integers with elliptic curves . . . . . 79

# List Of Notation

| | |
|---|---|
| $\mathbb{F}$ | a finite field |
| $\bar{\mathbb{F}}$ | an algebraic closure of $\mathbb{F}$ |
| $\mathbb{A}^n$ | affine $n$ space |
| $\mathbb{A}^n(\mathbb{F})$ | the set of $\mathbb{F}-$rational points of $\mathbb{A}^n$ |
| $\bar{\mathbb{F}}[X]$ | polynomial ring |
| $V_I$ | subset of $\mathbb{A}^n$ associated to the ideal $I$ |
| $\mathbb{P}^n$ | projective $n$ space |
| $\mathbb{P}^n(\mathbb{F})$ | the set of $\mathbb{F}-$rational points |
| $\mathbb{Z}$ | integers |
| $\mathbb{C}$ | complex numbers |
| $\cdot$ | multiplication |
| $\circ$ | composition |
| $\oplus$ | group law on an elliptic curve |
| $\pi$ | Frobenius endomorphism |
| ker | kernel |
| deg | degree |
| $\#E(\mathbb{F}_q)$ | cardinality of an elliptic curve defined over a finite field with $q$ elements |
| $\Delta$ | the discriminant of a Weierstrass equation |
| $j$ | $j-$invariant of an elliptic curve |
| $[m]$ | multiplication-by-$m$ map on an elliptic curve |
| $\mathcal{O}$ | point at infinity |
| $End(E)$ | endomorphism ring of the elliptic curve |
| $E[n]$ | $n-$torsion group of the elliptic curve |
| $\psi_m$ | $m^{th}$ division polynomial |
| $\Lambda$ | a lattice |
| $\omega_1, \omega_2$ | a basis of a lattice |

# 1 Introduction

Millions of people are using the Internet as a form of communication and e-commerce. This has led to an increased need for security over file transmission and communications. Cryptography is widely used for securing data transmissions on most computers. Cryptography is about protecting information and preventing adversaries from accessing information they are not authorised to access. Computer networks are increasing and the amount of information being processed is becoming incredibly large. We need security to preserve confidentiality, non-repudiation, authentication, access of control and integrity [68].

Cryptography is a medium for secure communication between different parties. We have two types of cryptographic algorithms, namely, symmetric and asymmetric cryptography. Symmetric cryptosystems are incredibly fast and only one key is used for both encryption and decryption of data meaning that once adversaries gain access to your private key they have access to your encrypted message. To avoid this, the two parties communicating need to make sure that they securely share the private key between themselves. Asymmetric cryptosystems on the other hand are not entirely secure, however their advantage is the use of a key pair, a public key and a private key, adversaries will only have access to your public key and your private key is kept secret. A public key (known by the public) is used for the encryption of a plaintext or the verification of a digital signature, and a private key, which remains secret is used for the decryption of the ciphertext or the creation of a digital signature [3].

Asymmetric key sizes are much larger compared to symmetric key sizes. A 128-bit symmetric key gives the same security as a 2048-bit RSA key and a 256-bit elliptic curve key. We will discuss elliptic curves in Chapter 3. Notice that a elliptic curve key is twice that of a symmetric key. When it comes to the speed of encrypting and decrypting data, asymmetric cryptosystems are slower and symmetric cryptosystems are quite fast. This makes asymmetric cryptosystems less efficient as them being slow means congestion (slow encryption and decryption) which is time consuming. Digital signatures can provide non-repudiation which means that a signer cannot deny having signed a message. Our main focus will be on asymmetric cryptography. The reader should see [51] for more details on symmetric cryptography.

Asymmetric cryptosystems are mostly used for key exchange because of data security. The encryption between two parties is secure, the private key is never shared over the channel. This minimizes attacks or adversaries being able to access whatever information is being exchanged as it is considered mathematically infeasible for adversaries (or anyone) to be able to use the public key to recreate the private key.

The Diffie-Hellman algorithm is used to establish a secure communication channel for the purpose of a key exchange. The exchanged key is a private key which is then used for symmetric encryption by both parties. The Diffie-Hellman key-exchange protocol is the foundation of asymmetric cryptography.

## 1.1 Asymmetric Cryptography

In 1976, Whitfield Diffie and Martin Hellman amazed the cryptographic world with their ground-breaking paper [33] "New Directions in Cryptography" giving a scheme for key exchange employing a number-theoretic technique. Soon after, in 1978, Ronald Rivest, Adi Shamir and Leonard Adleman published the famous RSA paper [74] in which the RSA cryptosystem, the first example of a public-key, cryptosystem was introduced.

Asymmetric cryptography, also known as Public-key cryptography, has been widely studied, beginning with the Diffie-Hellman key-exchange protocol and the RSA cryptosystem [51]. The secrecy of these systems depends on the difficulty of solving certain arithmetical problems. In particular it is currently a lengthy process to solve the discrete logarithm problem, which gives the Diffie-Hellman key-exchange protocol its security. The Diffie-Hellman key exchange protocol is a key-agreement protocol between two parties, where a third party (eavesdropper) may be able to intercept the information without being able to decrypt it. In practice, it may be used to allow two parties to agree on a secret private key, after which time, private-key encryption may be used.

This is how the encryption works:

1. Amahle wants to send a message (plaintext) to her friend Bukhosi through an unsecure channel.

2. Amahle encrypts her plaintext with Bukhosi's public key to get a ciphertext(scrambled message) through encryption.

3. She then sends the encrypted ciphertext to Bukhosi.

4. Bukhosi receives the ciphertext from Amahle and use his private key to decrypt the ciphertext turning it back to a readable message (plaintext).

We mentioned that one advantage of public-key cryptography is the use of two different keys. Even though intermediaries know your public key or see your encrypted message, without the private key they will be unable to decrypt your message.

RSA and ElGamal cryptosystems are best known for their robust security. The security of the RSA cryptosystem is based on the difficulty of factorizing the product of two large prime numbers whereas the security of the ElGamal cryptosystem is based on the difficulty of finding discrete logarithms modulo a large prime [75].

## 1.2 Elliptic Curve Cryptography

The first use of elliptic curves in cryptography was in 1984 when Lenstra used elliptic curves to factor integers [5, 52]. This led to a series of laws and theorems such as Fermat's last theorem being proved using elliptic curves [5]. Furthermore, many mathematicians gained interest hence shifted their focus on elliptic curves. However, in 1985, Miller [65, 66] and Kobliz [52] introduced elliptic curve cryptography (ECC) which is one of the best cryptosystems in use.

ECC is a public-key cryptosystem for wireless/mobile environments. When compared to other older cryptosystems modulo $n$, ECC comes with essentially smaller key sizes hence faster computation. Given the hard (exponential time) problem that breaking ECC requires, it is very difficult for malicious adversaries to try and break into the system. ECC uses lower power consumptions, provides bradwidth savings and lower memory usage[43, 80]. ECC is harder to break as its security depends on the difficulty of discrete logarithm problem for an elliptic curve. Although ECC is known as a robust security system, with RSA and ElGmal coming just after it, these cryptosys-

tems (and others) are still vulnerable to attacks using quantum computers and every day we get closer to the likelihood of quantum computers being able to solve the discrete logarithm problem in seconds.

## 1.3 Outline

This dissertation is a basic overview of elliptic curves and their application to cryptography. We will first review pre-quantum cryptography by discussing the most widely used public-key cryptosystems and then we will review post-quantum cryptography where we will discuss isogeny-based cryptography.

1. We begin chapter 2 by giving preliminaries which entails the discussion of the Diffie-Hellman key-exchange and the Discrete Logarithm Problem (DLP).

2. In chapter 3 , we discuss the theory behind elliptic curves. We begin our discussion with the basic form in which elliptic curves can be expressed, then proceed with how elliptic curves form a mathematical group and conclude our discussion with the Hasse theorem which is important in cryptography.

3. In chapter 4 , we look at torsion subgroups which plays an important part on the study of elliptic curves.

4. In chapter 5 , we introduce the Frobenius endomorphism which play an important role when it comes to counting points on elliptic curves defined over finite fields and the development of Schoof's algorithm.

5. In chapter 6 , we give the basics of early encryption, namely, Massey-Omura, ElGamal and the elliptic curve discrete logarithm problem (ECDLP).

6. In chapter 7 and chapter 8 we introduce isogenies and their applications. We give a brief discussion on isogenies then proceed to elliptic curves defined over complex numbers $\mathbb{C}$, the endomorphism ring, Schoof's algorithm, Schoof-Elkies-Atkin algorithm, isogeny graphs and irreducible polynomials.

7. In chapter 9 , we discuss isogeny-base cryptography. We discuss ex-

pander graphs, supersingular isogeny-based cryptography, the Charles-Lauter-Goren key-exchange and security- the hardness-assumption.

8. In chapter 10 , we conclude the dissertation by two post-quantum key-exchanges. We discuss a key-exchange from isogeny graphs and the supersingular isogeny Diffie-Hellman (SIDH) algorithm. Then we compute isogenies of a given kernel.

# 2 Preliminaries

## 2.1 Diffie-Hellman key-exchange

The *Diffie-Hellman key-exchange* is a cryptographic protocol between two parties communicating on an unsecure public channel, whereby the two parties exchange information and any eavesdropper able to intercept that information cannot decrypt the actual message. This protocol was invented by Whitfield Diffie and Martin Hellman in the 1970s [33]. In what follows, the two parties are called Amahle and Bukhosi, and the eavesdropper is called Evah.

Suppose Amahle and Bukhosi wish to exchange a secret key. They both agree on a modulus $p$ and a primitive root $g$ of $p$, which is made public.

1. Amahle randomly selects a number $a$ (secret) and computes $A \equiv g^a \pmod{p}$ and sends it to Bukhosi.

2. Bukhosi also randomly selects a number $b$ (secret) and computes $B \equiv g^b \pmod{p}$, then sends it to Amahle.

3. Bukhosi computes the secret key $S \equiv A^b \equiv (g^a)^b \pmod{p}$.

4. Amahle also computes the secret key $S \equiv B^a \equiv (g^b)^a \pmod{p}$.

5. Both now know $S$.

Note that $S$ is the same for both Amahle and Bukhosi, because, working modulo $p$,

$$A^b \equiv g^{ab} \equiv g^{ba} \equiv B^a \pmod{p}.$$

Only $a$, $b$ and $g^{ab} \pmod{p} \equiv g^{ba} \pmod{p}$ need to be kept secret. All the other parameters $p, g, g^a \pmod{p}$, and $g^b \pmod{p}$ are sent over a public channel (we assume that Evah, the eavesdropper is able to see all these parameters except for $a$ and $b$). Once Bukhosi and Amahle have computed the shared secret, they can use it as an encryption key, only known by them, for sending messages across the same channel. The computation of $S$ from the knowledge of $A$ and $B$ is known as the Diffie-Hellman problem.

**Example 2.1.** *1. Amahle and Buhkhosi publicly agree to use modulus* $p =$

1181 *and a base* $g = 11$.

2. *Amahle randomly selects a private integer* $a = 839$ *and computes* $A = g^a \pmod{p} = 11^{839} \pmod{1181} = 777$ *and send* $A$ *to Bukhosi.*

3. *Bukhosi randomly selects a private integer* $b = 919$ *then he computes* $B = g^b \pmod{p} = 11^{919} \pmod{1181} = 531$ *and sends* $B$ *to Amahle.*

4. *Amahle computes the secret key* $S = B^a \pmod{p} = 531^{839} \pmod{1181} = 270$.

5. *Bukhosi computes the secret key* $S = A^b \pmod{p} = 777^{919} \pmod{1181} = 270$.

They both arrive to the same secret $S$, because,

$(g^a)^b \pmod{p} = g^{ab} \pmod{p}$ and

$(g^b)^a \pmod{p} = g^{ba} \pmod{p}$.

This means that, regardless of the order in which Amahle and Bukhosi computes the exponentiation they will still get the same answer.

Evah, the eavesdropper will see all exchanges occurring between Amahle and Bukhosi as their exchange is over an unsecure channel. However, Evah will not be able to solve the secret $S$ without knowing what $a$ or $b$ are nor knowing $g^{ab}$ given that she knows $g^a = 777$ and $g^b = 531$. This means that Evah has to work out the discrete logarithm problem in order to figure out $a$ or $b$, which is very hard. In general, if $a$ and $b$ are large numbers it is practically infeasible to break the encryption between two parties. It is easy when $p$ is small but hard when $p$ has hundreds of digits.

## 2.2 Discrete logarithm problem

The discrete logarithm problem for a finite group $G$ is as follows: Given $g, B \in G$, find the least positive integer $a \in \mathbb{Z}$ such that $g^a = B$. We call $a$ the discrete logarithm of $B$ in base $g$, denoted by $\log_g B$ [1].

Both the Diffie-Hellman problem and discrete logarithm problem are considered to be equivalently hard to solve for $a$ or $b$ in $g^a$ or $g^b \pmod{p}$. The

Diffie-Hellman key exchange allows Amahle and Bukhosi to exchange their keys securely in the presence of Eve, the eavesdropper. The Diffie-Hellman key-exchange security is based on the difficulty of solving the discrete log problem.

The difference between the Diffie-Hellman Problem and the Discrete Logarithm Problem is that with the former you are given $g^a$ or $g^b \pmod p$, you must find $g^{ab}$, whereas in the Discrete Logarithm Problem you need to find $a$ or $b$ from $g^a, g^b \pmod p$. Note that it is not yet proven that breaking the Diffie-Hellman key exchange protocol is equivalent to computing the discrete logarithm problem [35, 65]. But the inverse is true, if you can solve the Discrete Logarithm Problem then it means you can solve the Diffie-Hellman Problem. The security of the Diffie-Hellman key exchange protocol rests on the unproven assumptions that solving the Diffie-Hellman problem and solving the discrete logarithm problem is computationally expensive or infeasible.

Shanks' baby-step giant-step method is one of the most well-known methods for solving discrete logarithms. In [41] an attempt is made to improve Shanks' original method. For more details on Shank's method see [88]. Other well-known methods for calculating discrete logarithms are Pollard's rho-method [73], Pohlig-Hellman method [72] and the index calculus method [49]. Modern computers cannot find the given parameters fast enough but with the use of Shor's algorithm, quantum computers will be able to solve such problems quicker. One of the things that this research will look at is how to extend the Diffie-Hellman protocol to elliptic curves.

# 3 Elliptic Curves and Elliptic Curve Arithmetic

## 3.1 Projective spaces

The references used in this section are [83] and [85]. Throughout this chapter we will use $\mathbb{F}$ to denote a field and $\bar{\mathbb{F}}$ the algebraic closure of $\mathbb{F}$.

**Definition 3.1.** *Given a field $\mathbb{F}$ and a positive integer $n$, we define an* affine n-space *as a set of $n$-tuples, denoted by $\mathbb{A}^n$*

$$\mathbb{A}^n(\bar{\mathbb{F}}) = \{(x_1, ..., x_n) : x_i \in \bar{\mathbb{F}}.\}$$

Similary, $\mathbb{A}^n(\mathbb{F})$ is the set of $\mathbb{F}$-rational points in an affine $n-$space,

$$\mathbb{A}^n(\mathbb{F}) = \{(x_1, ..., x_n) : x_i \in \mathbb{F}.\}$$

Let the polynomial ring over $\bar{\mathbb{F}}$ be denoted by $\bar{\mathbb{F}}[x]$ and let $I \subset \bar{\mathbb{F}}[x]$ be an ideal. To each such $I$ we associate a subset of $\mathbb{A}^n(\mathbb{F})$,

$$V_I = \{(x_1, ..., x_n) \in \mathbb{A}^n : f(x_1, ..., x_n) = 0 \text{ for all } f \in I\}.$$

**Definition 3.2.** *(Projective space). We define a projective $n-$space as a set of all $(n+1)-$tuples*

$$(x_0, ..., x_n) \in \mathbb{A}^{n+1}$$

*with $(x_0, ..., x_n) \neq (0, ..., 0)$, modulo the equivalence relation given by*

$$(x_0, ..., x_n) \sim (y_0, ..., y_n)$$

*if and only if there exists a multiplier $\mu$ such that $x_i = \mu y_i$ for all $i$. An equivalence class $(\mu x_0, ..., \mu x_n)$ is denoted by $[x_0 : ... : x_n]$. The set of $\mathbb{F}-$rational points is the set*

$$\mathbb{P}^n(\mathbb{F}) = \{[x_0 : ... : x_n] \in \mathbb{P}^n : \text{all } x_i \in \mathbb{F}\}.$$

Before we define elliptic curves, we need one extra point called *the point at infinity*. To get this point we will split $\mathbb{P}^2(\mathbb{F})$ into two disjoint subsets:

$$Y = \{[x : y : z] \in \mathbb{P}^2 | z \neq 0]\}$$

and

$$Z = \{[x : y : z] \in \mathbb{P}^2 | z = 0]\}.$$

To get finite points in $\mathbb{P}^2(\mathbb{F})$ we let $z \neq 0$ then $[x : y : z] = [x/z : y/z : 1] \in Y$. However, if $z = 0$ we get $[x : y : 0] \in Z$. This is the line at infinity. By doing so we have divided $\mathbb{P}^2$. Thus, the points $[x : y : 0]$ are called the point at infinity.

**Definition 3.3.** *A polynomial is non-singular if it has distinct roots.*

**Definition 3.4.** *(Elliptic curve).*

*We define an elliptic curve $E$ over a finite field as a non-singular cubic curve with a $\mathbb{F}-$rational point defined over the elliptic curve $E$.*

*Such an elliptic curve is described by it's Weierstrass equation:*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

*where $a_1, ..., a_6 \in \mathbb{F}$ such that the discriminant $\Delta = 4a^3 + 27b^2 \neq 0$. We say the curve $E$ is non-singular when $\Delta \neq 0$. The elliptic curve has exactly one $\mathbb{F}-$rational point at infinity. Note that the only place where $Z = 0$ is when $X = 0$, and $Z = 0$ is the line at infinity. The Weierstrass elliptic curve intercepts the line at infinity on the point $[0 : 1 : 0]$. This point is called the point at infinity of the elliptic curve. We denote the point at infinity by $\mathcal{O} = [0 : 1 : 0]$.*

*For the field $\mathbb{F}$ with characteristic $\neq$ 2, 3 we can transform the Weierstrass equation for the affine curve to a curve of the form:*

$$y^2 = x^3 + Ax + B. \tag{1}$$

*We refer to equation 1 as the short form of the Weierstrass equation.*

## 3.2 Group Law

In this section we describe how we can produce another point if we start with a point or two point, on an elliptic curve. Let $E$ be an elliptic curve contained in $\mathbb{P}^2$, consisting of points that satisfy the Weierstrass equation 1, that is, $R = (x, y)$, as well as the point at infinity $\mathcal{O} = (0 : 1 : 0)$. The equation of the curve has degree three. If we have one rational point $R$, we can get other points by drawing a line $L$ through the curve $E$ at point $R$. The

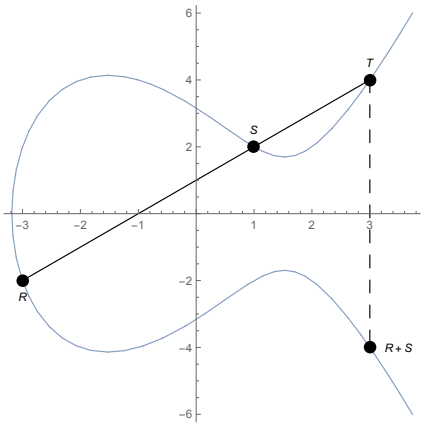



Figure 1: Addition on an elliptic curve

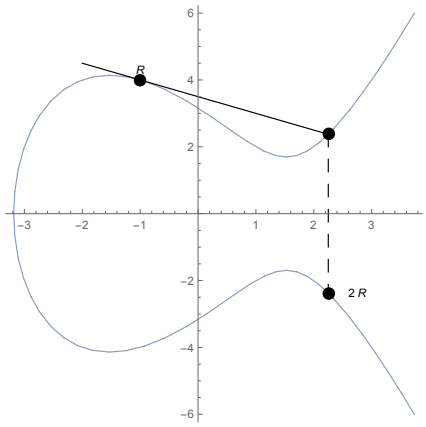



Figure 2: Multiplication on an elliptic curve

line $L$, taken with multiplicity, intersects the curve at exactly three points, namely, $R, S, T$. Drawing lines and taking multiplicities of intersections of these new points $R, S, T$ will generally give us a whole lot of new points [85, 83]. Bézout's theorem found in [85, 39] generates this.

The composition law $+$ is defined as follows:

**Definition 3.5.** *(Composition law). Let $R$ and $S$ be two distinct points on an elliptic curve. The line between point $R$ and $S$ intersect the elliptic curve $E$ at a third point $T$. Reflecting $T$ across the $x-$axis will give us another point $R+S$.*

**Proposition 3.1.** *Properties of the composition law are as follows:*

1. *Given the points $R, S, T$ and the line $L$ intersecting those three points, then*

$$(R+S)+T=\mathcal{O};$$

2. *$R+\mathcal{O}=\mathcal{O}+R=R$ for all $R \in E$;*

3. *$R+S=S+R$ for all $R, S \in E$;*

4. *There exists a point in $E$ denoted by $-R$ such that*

$$R + (-R) = \mathcal{O};$$

5. *Let* $R, S, T \in E$. *Then*

$$R + (S + T) = (R + S) + T.$$

In other words, three points are considered to add up to zero if they are collinear where $\mathcal{O}$ plays the role of zero. Under this definition of addition, points on an elliptic curve can then be considered to be an abelian group. Scalar multiplication can then be defined as repeated addition. Figures 1 and 2 give illustrations of the group law.

To do this arithmetically, consider two non-zero, non-symmetric points $R = (x_1, y_1)$ and $S = (x_2, y_2)$. For $x_1 \neq x_2$, define $\mu = \frac{y_1 - y_2}{x_1 - x_2}$ which can be thought of as the slope of the line between the two points $R$ and $S$.

Let $T$ be the intersection of this line with the curve $E$ given by

$$y - y_1 = \mu(x - x_1). \tag{2}$$

When we substitute 2 into the elliptic curve equation 1 we get

$$(y_1 + \mu(x - x_1))^2 = x^3 + ax + b. \tag{3}$$

When we expand and collect terms in $x$ we get the following monic polynomial

$$x^3 - \mu^2 x^2 + (2\mu^2 x_1 - 2\mu y_1 + a)x + (b - \mu^2 x_1^2 - y_1^2 + 2\mu x_1 y_1) = 0. \tag{4}$$

Factoring the cubic 4 yields

$$(x - x_1)(x - x_2)(x - x_3) = 0, \tag{5}$$

where the $x_3$ is the $x-$coordinate of the point T. We know that $x_1$ and $x_2$ are roots because these are the $x$ values for which the polynomial is equal to 0 and the only other possible root is $x_3$. When we expand and collect terms in $x$ we get

$$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1 x_2 + x_1 x_3 + x_2 x_3)x - x_1 x_2 x_3. \tag{6}$$

The coefficients of $x^2$ must be equal because equation 4 and 6 represent the same polynomial, giving

$$-\mu^2 = -(x_3 + x_1 + x_2). \tag{7}$$

The $x-$coordinate of the third point is computed as

$$x_3 = \mu^2 - x_1 - x_2. \tag{8}$$

To obtain the corresponding $y-$coordinate we make use of equation 2 then negate the results to get

$$y_3 = \mu(x_1 - x_3) - y_1. \tag{9}$$

or equivalently,

$$y_3 = \mu(x_2 - x_3) - y_2. \tag{10}$$

Therefore,

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) \implies R + S = T.$$

Note that in order to verify the above ($R+S = T$), you need to check whether $T$ belongs to the curve or the alignment of $R, S$, and $T$.

For the case where $S = R$: Given $x_2 = x_1$ and $y_2 = y_1$, the equations for $x_3$ and $y_3$ remains the same but a different equation is used for the slope:

$$\mu = \frac{3{x_1}^2 + a}{2y_1},$$

which is obtained by differentiating

$$y_1 = \pm\sqrt{{x_1}^3 + ax_1 + b}.$$

To verify this, we check that $T$ belongs to the curve and that we only get two intersections on the curve given by the line passing through $R$ and $S$. We will not give proofs but examples which will verify the above.

**Example 3.1.** *Given the elliptic curve $y^2 = x^3 - 7x + 10$, if $R = (3, 4)$ and $S = (2, 2)$ then $T$ is the sum of $R$ and $S$, i.e. $R + S = T$.*

*If $x_1 \neq x_2$ the slope is:*

$$\mu = \frac{y_1 - y_2}{x_1 - x_2} = \frac{4-2}{3-2} = 2.$$

*The values of* $x_3$ *and* $y_3$ *are:*

$$x_3 = 2^2 - 3 - 2 = -1,$$
$$y_3 = 2(3 - (-1)) - 4 = 4,$$

*or equivalently,*

$$y_3 = 2(2 - (-1)) - 2 = 4,$$
$$\therefore T = (x_3, y_3) = (1, 4).$$

**Example 3.2.** *Given the curve* $y^2 = x^3 - 7x + 10$ *and* $R = (-3, -2) = S$, $x_2 = x_1$ *we have:*

$$\mu = \frac{3{x_1}^2 + a}{2y_1} = \frac{3(-3)^2 - 7}{2(-2)} = -5,$$
$$x_3 = (-5)^2 - (-3) - (-3) = 31,$$
$$y_3 = (-5)(-3 - 31) - (-2) = 172,$$
$$\therefore (x_3, y_3) = (31, 172).$$

*This is* $R + R = 2R$ *(repeated addition).*

**Example 3.3.** *(Arithmetic on curves over* $\mathbb{F}_p$*).*

*Our aim is to prove that one can find points on any graph (manually) if it is non-singular. We will show steps on how to do this. We want to determine whether the elliptic curve:* $y^2 = x^3 - 47x + 96$ *over* $\mathbb{F}_{89}$ *is non-singular. To check this we will first calculate the discriminant which should be* $\Delta \neq 0$ *for the curve to be considered non-singular. We will then take a point at* $x = 1$ *to check whether it is a quadratic residue or a quadratic non-residue. We can use the Shanks-Tonelli algorithm to find the square roots* $\pm x$ *of any* $r \equiv x^2 \pmod{p}$*. Then finally compute points of the curve in* $\mathbb{F}_{89}$ *and use* Mathematica *to verify these points.*

$$\Delta \equiv -(4a^3 + 27b^2)$$
$$\equiv 8 \pmod{89}$$

$\therefore \Delta = 8 \neq 0$. *Hence the curve is non-singular.*

*Taking* $x = 1$ *gives*

$$x^3 - 47x + 96 \equiv 1 - 47 + 96 = 144 \equiv 55 \pmod{89}.$$

*We use the Shanks-Tonelli's algorithm to find that* $12^2 \equiv 55 \pmod{89}$ *which yields point* $R = (1, 12) \in E(\mathbb{F}_{89})$.

*We move to the next step where we compute* $R + R = 2R$.

$$\begin{aligned}
\mu &= \frac{3x^3 + a}{2y} \\
&= \frac{(3 + 47)}{2(12)} \\
&\equiv (50)(24^{-1}) \pmod{89} \\
&\equiv (50)(26) \pmod{89} \\
&\equiv 54 \pmod{89}.
\end{aligned}$$

*Then we calculate* $(x_3, y_3)$*:*

$x_3 = 54^2 - 2(1) \equiv 2914 \equiv 66 \pmod{89}$;

$y_3 = 12 + 54(66 - 1) \equiv 3522 \equiv 51 \pmod{89}$.

*Hence* $2R = 2(1, 12) = (66, 51)$.

*Since computing points can be tedious, we use the double and add method (see, for example, [7, 14]) which efficiently gives the following points for* $nR$*, where* $n > 2$*:*

$4R = (41, 79), 5R = (45, 81), ..., 79R = (1, 77), 80R = \mathcal{O}, 81R = (1, 12)$.

*We define the order of a point as the smallest* $n$ *such that* $nR$ *is equal to the point at infinity, i.e.,* $nR = \mathcal{O}$*. We know that* $77 + 12 \equiv 0 \pmod{89}$ *implies that* $79R = -R$ *hence 80 is the smallest multiple of the point* $R$*, i.e.,* $80R = \mathcal{O}$*. The order of the point* $R$ *is written as* $|R| = 80$.

*Table 1 is an estimate of the number of points as we add points on the elliptic curve* $y^2 = x^3 - 47x + 96$ *over* $\mathbb{F}_{89}$*, i.e.,* $nR$*, the sum of* $n$ *copies of the point* $R$.

Table 1: Points for $y^2 = x^3 + 47x + 96$ over $\mathbb{F}_{89}$

| $x$ | $y_1$ | $y_2$ | $x$ | $y_1$ | $y_2$ |
|---|---|---|---|---|---|
| 1 | 12 | 77 | 47 | 29 | 60 |
| 2 | 38 | 51 | 50 | 40 | 49 |
| 4 | 9 | 80 | 51 | 24 | 65 |
| 5 | 10 | 79 | 52 | 6 | 83 |
| 8 | 19 | 70 | 55 | 32 | 57 |
| 9 | 25 | 64 | 57 | 0 | 0 |
| 10 | 26 | 63 | 58 | 40 | 49 |
| 16 | 7 | 82 | 61 | 18 | 71 |
| 18 | 30 | 59 | 66 | 38 | 51 |
| 19 | 4 | 85 | 67 | 42 | 47 |
| 20 | 15 | 74 | 70 | 40 | 49 |
| 21 | 38 | 51 | 71 | 2 | 87 |
| 27 | 20 | 69 | 72 | 13 | 76 |
| 31 | 4 | 85 | 74 | 33 | 56 |
| 37 | 44 | 45 | 76 | 15 | 74 |
| 39 | 4 | 85 | 79 | 36 | 53 |
| 41 | 10 | 79 | 81 | 3 | 86 |
| 43 | 10 | 79 | 82 | 15 | 74 |
| 44 | 22 | 67 | 85 | 17 | 72 |
| 45 | 8 | 81 | 86 | 27 | 62 |

*Since there exist* $y \in \mathbb{F}_q$ *such that* $y^2 = x^3 + Ax + B$ *and* $(x, y), (x, -y) \in \mathbb{F}_q$ *we have 39 pairs of point, i.e,* $(x, y), (x, y')$ *where* $y \neq y'$.

Curves with the same $j-$invariant are essentially the same curve over a given field. For instance, if Amahle and Bukhosi are working on the same curves with different parameters but the same $j-$invariant, then they are definitely working on the same curve.
subsection$j-$invariant

Let $E$ be an elliptic curve defined over the closed algebraic field $\bar{\mathbb{F}}$ of characteristic $\neq 2$ or 3. The change of variables is of the form

$$(x, y) = (u^2 x', u^3 y') \tag{11}$$

with $u \in \bar{\mathbb{F}}, u \neq 0$. We introduce this because we want to preserve the Weierstrass form and only keep the coefficients for $Y^2$ and $x^3$ terms 1 for $E : y^2 = x^3 + ax + b$. The isomorphism class of a curve has an invariant.

**Definition 3.6.** *[29] (j-invariant). Let $E : y^2 = x^3 + ax + b$ be an elliptic curve, and define the j-invariant of $E$ as*

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

Note that negating the denominator gives us the discriminant, $\Delta \neq 0$.The change of variables in equation 11 preserves $j$ leaving it unchanged.

The following proposition tells that while there are many different Weierstrass equations for elliptic curves it remains that all these curves will have the same $j-$invariant.

**Proposition 3.2.** *Two curves $E_1$ and $E_2$ are isomorphic over the algebraic closure $\bar{\mathbb{F}}$ if and only if they have the same $j-$invariant [29].*

*Proof.* $\Rightarrow$ Assume that two curves $E_1$ and $E_2$ are isomorphic. We show that they have the same $j-$invariant. Our curves are

$$E_1 : y^2 = x^3 + ax + b$$

and

$$E_2 : y'^2 = x'^3 + a'x' + b'.$$

If the characteristic is not 2 or 3 then the only change of variables is of the form $(x, y) = (u^2x', u^3y')$ for some $u \in \bar{\mathbb{F}}$.

Let

$$(u^3y')^2 = (u^2x')^3 + a'(u^2x') + b'$$
$$u^6y'^2 = u^6x'^3 + a'u^2x' + b'$$
$$y'^2 = x'^3 +' x'u^{-4} + b'u^{-6}.$$

then

$$\begin{aligned} j(E_1) &= 1728\frac{4a^3}{4a^3+27b^2} \\ &= 1728\frac{4(\frac{a'}{u^4}^3)}{4(\frac{a'}{u^4})^3+27(\frac{b'}{u^6})^2} \\ &= 1728\frac{4(\frac{a'^3}{u^{12}})}{4(\frac{a'^3}{u^{12}})+27(\frac{b'^2}{u^{12}})} \\ &= 1728\frac{(\frac{1}{u^{12}})4a'^3}{(\frac{1}{u^{12}})(4a'^3+27b'^2)} \\ &= 1728\frac{4a'^3}{4a'^3+27b'^2} \\ &= j(E_2). \end{aligned}$$

Therefore $j(E_1) = j(E_2)$.

$\Leftarrow$ Assume that the characteristic of $\mathbb{F}$ is different from 2 or 3. Assume that two curves $E_1$ and $E_2$ have the same $j-$invariant. We show that they are isomorphic. The assumption that

$$j(E_1) = 1728\frac{4a^3}{4a^3+27b^2} = 1728\frac{4a'^3}{4a'^3+27b'^2} = j(E_2).$$

yields

$$\begin{gathered} 1728 \cdot 4a^3 \cdot (4a'^3+27b'^2) = 1728 \cdot 4a'^3 \cdot (4a^3+27b^2) \\ a^3 \cdot (4a'^3+27b'^2) = a'^3 \cdot (4a^3+27b^2) \\ a^3 \cdot 4a'^3 + a^3 \cdot 27b'^2 = a'^3 \cdot 4a^3 + a'^3 \cdot 27b^2 \\ a^3b'^2 = a'^3b^2. \end{gathered}$$

We consider three cases. Note that $\Delta \neq 0$ (discriminant). If $a = 0$, then $b \neq 0$. Equivalently, if $a' = 0$ then $b' \neq 0$, otherwise $\Delta = 0$.

*Case 1.* $j = 0$. If $a = 0$, then $b \neq 0$ so $a' = 0$. We take $u = (\frac{b}{b'})^{1/6}$ and we write

$$u^6 = \frac{b}{b'}$$

Substituting into $E$ we get:

$$\begin{aligned} u^6y^2 &= u^6x^3 + au^2x + b \\ u^6y^2 &= u^6x^3 + b \\ \left(\frac{b}{b'}\right)y^2 &= \left(\frac{b}{b'}\right)x^3 + b \\ y^2 &= x^3 + b' \\ y^2 &= x^3 + a'x + b'. \end{aligned}$$

*Case 2.* $j = 1728$. If $b = 0$ then $a \neq 0$, so $b' = 0$, we take $u = \left(\frac{a}{a'}\right)^{1/4}$ and write

$$u^4 = \frac{a}{a'}$$

then substitute into $E$ to get:

$$\begin{aligned} u^6y^2 &= u^6x^3 + au^2x + b \\ y^2 &= x^3 + au^{-4}x \\ y^2 &= x^3 + a\left(\frac{a}{a'}\right)^{-1}x \\ y^2 &= x^3 + a'x \\ y^2 &= x^3 + a'x + b'. \end{aligned}$$

*Case 3.* $j \neq 0, 1728$. If $ab \neq 0$ then $a'b' \neq 0$ (we would get the contradiction that $\Delta' \neq 0$ if either one of them is zero. We write

$$u = \left(\frac{a}{a'}\right)^{1/4} = \left(\frac{b}{b'}\right)^{1/6}$$

which gives us the desired isomorphism $E_1 \simeq E_2$ over $\mathbb{F}_2$. □

We conclude this section by one of the most important theorems in the world of cryptography. We introduce Hasse theorem which estimates the number of points on an elliptic curve defined over $\mathbb{F}_q$ with $q-$elements, $E(\mathbb{F}_q)$. Hasse further placed an upper and lower bound on the cardinality of $E(\mathbb{F}_q)$.

The number of points falls within these bounds and proving this relies on $n-$torsion groups. We denote the cardinality of the elliptic curve defined over the field $\mathbb{F}_q$ with $q-$elements by $\#E(\mathbb{F}_q)$.

**Theorem 3.1.** *(Hasse theorem). Let $E(\mathbb{F}_q)$ be an elliptic curve over the finite field $\mathbb{F}_q$ where $q = p^n$, $p$ a prime and $n \in \mathbb{Z}^+$. Then*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

# 4 Torsion subgroups of elliptic curves

Elliptic curves have points that are either of finite or infinite order. We say a point $P$ is of finite order if there exist an integer $n$ such that when you add $P$ $n$ times you will get the point at infinity, i.e., $nP = \mathcal{O}$. If there exist no such integer $n$ then $P$ is said to be of infinite order meaning that no matter how many times you add $P$ to itself you will never get the point at infinity. The distinction between the two orders lead to our next topic, torsion points. Torsion points of finite orders play an important role on elliptic curves. This section is derived from [97, p. 73].

**Definition 4.1.** *Let $E$ be an elliptic curve defined over a field $\mathbb{F}$. Let $n$ be a positive integer. We denote the $n-$torsion subgroup of $E$ by $E[n]$, where*

$$E[n] = \{P \in E(\bar{\mathbb{F}}) | nP = \mathcal{O}\}.$$

The $n-$torsion subgroup of $E$ contains points whose coordinates are in the algebraic closure $\bar{\mathbb{F}}$, i.e., for each $x \in \mathbb{F}$, if $y \notin \mathbb{F}$ then you can find $y \in \bar{\mathbb{F}}$.

The torsion subgroup consists of all elements of finite order. In our case, the $n-$torsion subgroup consists of all elements of order $n$. On an elliptic curve, the $n-$torsion subgroup is the kernel of the multiplication-by$-n$ map, and its structure tells us about the structure of the elliptic curve.

**Theorem 4.1.** *Let $E$ be an elliptic curve over a field $\mathbb{F}$ and let $n$ be a positive integer. We denote "isomorphic" by the symbol "$\simeq$". If the characteristic of $\mathbb{F}$ does not divide $n$, or is 0, then*

$$E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_n.$$

*If the characteristic of $\mathbb{F}$ is $p > 0$ and $p|n$, write $n = p^r n'$ with $p \nmid n'$. Then*

$$E[n] \simeq \mathbb{Z}_{n'} \times \mathbb{Z}_{n'} \text{ if } E[p^r] \simeq \{\mathcal{O}\},$$

*or*

$$E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_{n'} \text{ if } E[p^r] \simeq \mathbb{Z}_{p^r}.$$

From the above theorem 4.1 please note that $E[p^r]$ is guaranteed to be isomorphic to either $\{\mathcal{O}\}$ or $\mathbb{Z}_{p^r}$.

*Proof.* See [97, Thm. 3.2]. □

Before we give an example for $n-$torsion subgroups, it is imperative to note that for any elliptic curve with rational coefficients, the points of finite order must have integer coordinates, i.e., $P, Q \in \mathbb{Z}_n \times \mathbb{Z}_n$ can be expressed as $aP + bQ$ for some $a, b$. We will now look at the cases of the 2- and 3- torsion subgroup. We begin with the points of order 2.

**Example 4.1.** *Points of order 2:* $2P = \mathcal{O}$ *where* $P \neq \mathcal{O}$.

*If* $P = (x, y)$ *then* $-P = (x, -y)$. *This means that* $2P = \mathcal{O}$ *then* $P = -P$, *i.e.,* $(x, y) = (x, -y)$ *but this can only happen when all points of order 2 have* $y = 0$. *This means that when* $y = 0$ *we have four points:*

$$E[2] = \{\mathcal{O}, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\},$$

*where* $\alpha_1, \alpha_2, \alpha_3$ *are the roots of the cubic equation (in* $\bar{\mathbb{F}}$*).* $E[2]$ *is the direct product of two groups of order 2, i.e.,* $E[2] \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

*Points of order 3:* $E[3]$ *must satisfy* $3P = \mathcal{O}$ *if and only if* $2P = -P$. *This means that the* $x-$*value of* $2P$ *is equal to that of* $P$.

*This can be written as* $m^2 - 2x = x$, *where* $m = \frac{3x^2+A}{2y}$.

*Substituting* $y^2 = x^3 + Ax + B$ *yields*

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0. \tag{12}$$

*There are four distinct roots. This can be verified by checking if there are any common roots in equation 12 and in its derivative. We have a total of 9 points of order 3, 8 points from each* $x-$*values yielding two* $y$*-values and the point at infinity. In this case,* $E[3] \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$.

**Definition 4.2.** *An elliptic curve* $E$ *defined over a field of characteristic* $p$ *is said to be ordinary if* $E[p] \simeq \mathbb{Z}_p$ *and supersingular if* $E[p] \simeq \{\mathcal{O}\}$.

Supersingular curves were discovered by Hasse in 1936. They form a certain class of elliptic curve with a positive characteristic field with a very large endomorphism ring. We will give more details about endomorphism rings in chapter 8.

# 5 Elliptic curves over finite fields

In this section, we introduce a special endomorphism of elliptic curves $E$ defined over the finite field $\mathbb{F}$ with $q$ elements.

**Definition 5.1.** *[97, 29] (The Frobenius endomorphism). Let $\mathbb{F}_q$ be a finite field with an algebraic closure $\bar{\mathbb{F}}_q$ and let*

$$\pi : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q,$$

$$x \mapsto x^q$$

*be the Frobenius map for $\mathbb{F}_q$. We call $\pi$ the Frobenius endomorphism. Let $E$ be an elliptic curve defined over $\mathbb{F}_q$. Then $\pi$ acts on the coordinates of points in $E(\bar{\mathbb{F}}_q)$ :*

$$\pi[x : y : z] = [x^q : y^q : z^q],$$
$$\pi(\mathcal{O}) = \mathcal{O}.$$

Let $E$ be defined over $\mathbb{F}_q$ and let $[x : y : z] \in E(\bar{\mathbb{F}}_q)$ then

$$y^2z = x^3 + Axz^2 + Bz^3 \in \mathbb{F}_q. \tag{13}$$

Now $\pi[x : y : z] = [x^q : y^q : z^q]$. If we substitute this into 13 we get

$$(y^2z)^q = (x^3 + Axz^2 + Bz^3)^q.$$

Since $a^q = a$ for all $a \in \mathbb{F}_q$ and $(a + b)^q = a^q + b^q$ in $\mathbb{F}_q$ we have

$$(y^q)^2z^q = (x^q)^3 + Ax^q(z^q)^2 + B(z^q)^3.$$

Hence $[x^q : y^q : z^q] = \pi[x : y : z] \in E(\bar{\mathbb{F}}_q)$, $\pi$ maps a point on the elliptic curve to another.

Note that $[x : y : z] \in \mathbb{P}^2(F_q)$ if and only if $\pi[x : y : z] = [x : y : z]$. That is, $\pi[x] = x, \pi[y] = y$ and $\pi[z] = z$. Therefore

$$\begin{aligned} [x : y : z] \in \mathbb{P}^2(F_q) &\iff x, y, z \in \mathbb{F}_q \\ &\iff \pi[x] = x, \pi[y] = y, \pi[z] = z \\ &\iff \pi[x : y : z] = [x : y : z] \end{aligned}$$

The following proposition is important when it comes to counting points on elliptic curves defined over finite fields. The Frobenius endomorphism is also very important when it comes to the development of Schoof's algorithm. We will discuss Schoof's algorithm at a later stage. The Frobenius endomorphism is a special endomorphism of elliptic curves and every power of the Frobenius endomorphism, i.e., $\pi^n = \pi \circ \pi \circ \ ... \circ \pi$ is also an endomorphism. Another example of an endomorphism is the sum $\pi^n - 1$.

**Proposition 5.1.** *[29] Let $\pi$ be the Frobenius endomorphism of the elliptic curve $E$ defined over $\mathbb{F}_q$. Then:*

*(a)* $\ker \pi = \mathcal{O}$*;*

*(b)* $\ker(\pi - 1) = E(\mathbb{F})$.

*Proof.* (a) The Frobenius endomorphism, $\pi$ sends

$$[x : y : z] \mapsto [x^q : y^q : z^q]$$

so

$$\pi[0 : 1 : 0] = [0^q : 1^q : 0^q] = [0 : 1 : 0].$$

Suppose that

$$\pi[x : y : z] = [0 : 1 : 0]$$

yields

$$x_1^q = 0, y_1^q = \text{anything}, z_1^q = 0.$$

Therefore

$$x_1 = 0, y_1 = \text{anything}, z_1 = 0.$$

So $[x_1 : y_1 : z_1] \sim [0 : 1 : 0]$. Hence $\ker \pi = \mathcal{O}$

(b) See Proposition 4.7 in [97].

□

When we look at (b), we can see that $\pi - 1$ is just the Frobenius endomorphism minus the identity map. So $\ker(\pi - 1)$ consists of all points such that $\pi(P) = P$. The theorem is saying that $\pi$[rational point of $E$] = same point while $\pi$[point from $E(\bar{\mathbb{F}}_q)$] is never the same point. This means that $\#E(\mathbb{F}_q)$ is the number of fixed points of $\pi$, which is useful for Hasse's theorem.

The next section will be on the basics of early encryption. We will first discuss a method by Massey-Omura, then ElGamal and finally the elliptic curve discrete logarithm.

# 6 Early Elliptic Curve Cryptosystems

In this chapter will be on the basics of early encryption. We will first discuss a method by Massey-Omura, then ElGamal and finally the elliptic curve discrete logarithm.

## 6.1 Massey-Omura elliptic curve

In 1983, Massey and Omura [64] introduced the Massey-Omura scheme which uses exponentiation in $\mathbb{F}_q$ for encrypting and decrypting messages. The elliptic curve analog of Massey-Omura scheme by Kobliz [52] is as follows:

Amahle wishes to communicate with Bukhosi. Assume the the elliptic curve $E$ defined over the finite field $\mathbb{F}_q$ with $q-$elements and $n = \#E(\mathbb{F}_q)$ is public. Amahle wishes to send Bukhosi a text so she represent her text by a point $P \in E(\mathbb{F}_q)$. She randomly selects an integer $a$ with $\gcd(a, n) = 1$ and computes $P_1 = aP$ and sends it to Bukhosi. Then, Bukhosi randomly selects an integer $b$ with $\gcd(b, n) = 1$ and computes $P_2 = abP$ then transmit it back to Amahle. Amahle calculates $a^{-1} \in \mathbb{Z}_n$ and computes $P_3 = a^{-1}abP$ where $a^{-1}a \equiv 1 \pmod{n}$ and sends it back to Bukhosi. Bukhosi calculates $b^{-1} \in \mathbb{Z}_n$ and computes $P_4 = b^{-1}ba^{-1}aP = P$ where $b^{-1}b \equiv 1 \pmod{n}$.

To justify the fact that the inverse of the integer $a \pmod{n}$ and $b \pmod{n}$ cancels the integer $a$ and $b$. We have $aa^{-1} \equiv 1 \pmod{n}$ where $a^{-1}a = 1 + in$ for some $i$, which is also applicable for $b$. The group $E(\mathbb{F}_q)$ has order $n$. The order of any point $M$ is linked to the elliptic curve $E(\mathbb{F}_q)$ by Lagrange's theorem, which states that the order of every subgroup divides the order of the parent group. In other words, Lagrange's theorem implies that $nM = \mathcal{O}$ (Recall that $\mathcal{O}$ plays the role of zero, the additive identity). Therefore,

$$a^{-1}aM = (1 + in)M = M + i\mathcal{O} = M.$$

When we apply $M = bP$, we find that

$$P_3 = a^{-1}abP = bP.$$

Similarly,

$$P_4 = b^{-1}P_3 = b^{-1}bP = P.$$

Evah the eavesdropper sees the communication between Amahle and Bukhosi since they are communicating through an unsecure channel. Evah knows

$E(\mathbb{F}_q)$ and the points $aP$, $bP$, $abP = baP$ and wants to find $P$, which she could get from $a$ or $a^{-1}$ or $b$ or $b^{-1}$ or $ab$ or $ab^{-1}$, which means solving the Diffie-Hellman problem.

## 6.2 ElGamal for elliptic curves

The ElGamal cryptosystem [35] was introduced by Taher ElGamal in the 1980s. ElGmal was the first to propose a public key based on the discrete logarithm problem. He proposed two different cryptosystems, one for digital signatures and the other for encryption. The encryption between two parties is as follows:

Amahle and Bukhosi want to communicate over an unsecure channel. Bukhosi chooses an elliptic curve $E$ over a finite field $\mathbb{F}_q$. He also chooses a point $P \in E(\mathbb{F}_q)$ and an integer $b$. Bukhosi computes $B = bP$. Bukhosi's private key is the integer $a$ and his public key is the point $P$ and $B$. To send Bukhosi a message, Amahle represents her message as $T \in E(\mathbb{F}_q)$. Amahle makes use of Bukhosi's public key. Then she randomly selects an integer $a$ and computes $T_1 = aP$. She further computes $T_2 = T + abP$ and sends the pair $(aP, T + abP) = (T_1, T_2)$ to Bukhosi. Bukhosi decrypts the text by calculating $T = T_2 - bT_1 = T + abP - b(aP) = T$.

Evah the eavesdropper knows $P \in E(\mathbb{F}_q)$, $B = bP$, $T_1 = aP$ and $T_2 = T + abP$. She would have to solve the discrete logarithm problem by using $P$ and $aP$ to find $a$. Then calculating $T = T + abP - abP$. Evah could also use Bukhosi's public key $P$ and $B$ to find $b$, which she can use to decrypt the message as $T + abP - b(aP)$. Evah has no other way of finding $T$ without solving the discrete logs.

**Remarks** The security of Massey-Omura and Elgamal both rest on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) and/or the Elliptic Curve Diffie-Hellman Problem (ECDHP).

## 6.3 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve $\mathbb{F}_q$ and two points $P, Q \in E(\mathbb{F}_q)$, determine the integer $n$, such that $Q = nP$, provided that such an integer exists [52]. Here $Q$ and $n$ are the public-key and the private key.

The security of ECC is based on the difficulty of solving the ECDLP, which can be simplified as, given two points $P$ and $Q = nP$, it is hard to find the integer $n$ (especially if $n$ is very large). We can see that the Elliptic Curve Discrete Logarithm Problem is considered to much more difficult than the classic Discrete Logarithm Problem. Refer to [67] for more details on discrete logarithms.

# 7 Isogenies

We can now define the structure preserving map between elliptic curves.

**Definition 7.1.** *Let $E$ be defined over $\mathbb{F}$ with equation $f(X,Y)=0$. Take a polynomial $g(X,Y)$ such that $g=f$ where $g$ is the same as the zero function because $g(P)$ for any point $P$ on the curve is zero. We define the ring of regular functions of $E$ as*

$$\mathbb{F}[E]=\mathbb{F}/\langle f\rangle.$$

*Elements of $\bar{\mathbb{F}}(E)$ are called the rational functions of $E$.*

**Definition 7.2.** *[19] (Morphism). A rational map that is defined at every point is called a morphism.*

**Definition 7.3.** *Let $E_1$ and $E_2$ be elliptic curves. An isogeny between $E_1$ and $E_2$ is a morphism that preserves the identity of $\phi: E_1 \to E_2$ satisfying $\phi(\mathcal{O})=\mathcal{O}$. These curves are defined over the algebraic closure $\bar{\mathbb{F}}$. Two curves $E_1$ and $E_2$ are called isogenous if there exist an isogeny between them with $\phi(E_1)\neq(\mathcal{O})$. Note that $\phi$ satisfies either $\phi(E_1)=\mathcal{O}$ or $\phi(E_1)=E_2$.*

Under these definitions, an isogeny is a homomorphism that respects the addition of points.

**Theorem 7.1.** *[83] A morphism of curves is either constant or surjective.*

Any non-constant morphism of curves is surjective. This is equivalent to saying that an isogeny is a non-constant morphism that maps distinguished points of $E_1$ to distinguished of $E_2$.

The multiplication-by-$m$ map is an example of an isogeny that is an endomorphism of an elliptic curve. We construct such a map by adding points to itself $m$-times. That is, if $m>0$ then

$$[m](P)=\overbrace{P+P+P+...+P}^{m-times}$$

and

$$[m](P)=[-m](-P)$$

if $m<0$, where

$$[m]: E \to E,$$

$m \in \mathbb{Z}$. $[m]$ is defined over $\mathbb{F}$ as the elliptic curve $E$ is also defined in $\mathbb{F}$. We denote $E[m]$ as the $m-$subgroup of the curve which is also the kernel of the $[m]$ operator.

**Definition 7.4.** *[97] (Degree). If $\phi(x) = p(x)/q(x)$ then the degree of the isogeny is* $\deg(\phi) = max\{\deg(p), \deg(q)\}$.

**Definition 7.5.** *[97]*

*We say an isogeny is separable if the derivative of $p(x)/q(x) \neq 0$, otherwise it is inseparable.*

**Theorem 7.2.** *[83] Let $E_1 \to E_2$ be a non-constant isogeny of degree $m$ then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ satisfying $\hat{\phi} \circ \phi = [m]$ on $E_1$ and $\phi \circ \hat{\phi} = [m]$ on $E_2$.*

So applying $\phi$ and then $\hat{\phi}$ to a point $P$ on $E_1$ is the same as adding $P$ to itself $m$ times.

**Definition 7.6.** *[83] (Dual isogeny). Let $\phi : E_1 \to E_2$ be an isogeny of degree $m$. The dual isogeny to $\phi$ is the isogeny*

$$\hat{\phi} : E_2 \to E_1$$

*given by Theorem 7.2.*

The following theorem gives basic properties of dual isogenies.

**Theorem 7.3.** *[83] Let*

$$\phi : E_1 \to E_2$$

*be an isogeny. Then*

*(a) Let $\mu : E_2 \to E_3$ be any other isogeny. Then*

$$\widehat{\mu \circ \phi} = \hat{\phi} \circ \hat{\mu}.$$

*(b) Let $\lambda : E_1 \to E_2$ be any other isogeny. Then*

$$\widehat{\phi + \lambda} = \hat{\phi} + \hat{\lambda}.$$

*(c)* $\forall m \in \mathbb{Z}$

$$\widehat{[m]} = [m]$$

*and*

$$m^2 = \deg[m].$$

*(d)*

$$\deg \hat{\phi} = \deg \phi.$$

*(e)*

$$\phi = \hat{\hat{\phi}}.$$

**Definition 7.7.** *An isogeny from an elliptic curve defined over a finite field* $\mathbb{F}$ *to itself is called an endomorphism.*

**Note.** *All endomorphisms are isogenies apart from the zero morphism [91].*

**Theorem 7.4.** *Let* $E$ *be an elliptic curve and let* $H$ *be a finite subgroup of the elliptic curve* $E$*. There is a unique elliptic curve* $E'$ *and a separable isogeny* $\phi : E \to E'$ *satisfying* $\ker \phi = H$ *[83].*

The image of this unique separable isogeny is denoted by $E/H$. We can use Vélu's formulae to compute this unique separable isogeny with its kernel. The protocols later on are made possible by this theorem (7.4).

**Definition 7.8.** *Let* $E$ *be an elliptic curve over a finite field* $\mathbb{F}_q$*. The zeta function is defined to be*

$$Z_E(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#E(\mathbb{F}_{q^n})}{n} T^n\right).$$

**Theorem 7.5.** *Let* $E$ *be an elliptic curve over* $\mathbb{F}_q$*, and let* $\#E(\mathbb{F}_q) = q+1-t$*. Then*

$$Z_E(T) = \frac{qT^2 - tT + 1}{(1-T)(1-qT)}.$$

**Theorem 7.6.** *(Sato-Tate) Two elliptic curves* $E, E'$ *defined over a finite field* $\mathbb{F}$ *are isogenous over* $\mathbb{F}$ *if and only if* $\#E(\mathbb{F}) = \#E'(\mathbb{F})$*.*

Theorem 7.6 basically tells us that the elliptic curves have the same zeta function. The numerator of the zeta function is the characteristic equation of the Frobenius endomorphism which will be elucidated at a later stage.

# 8 Isogenies and their applications

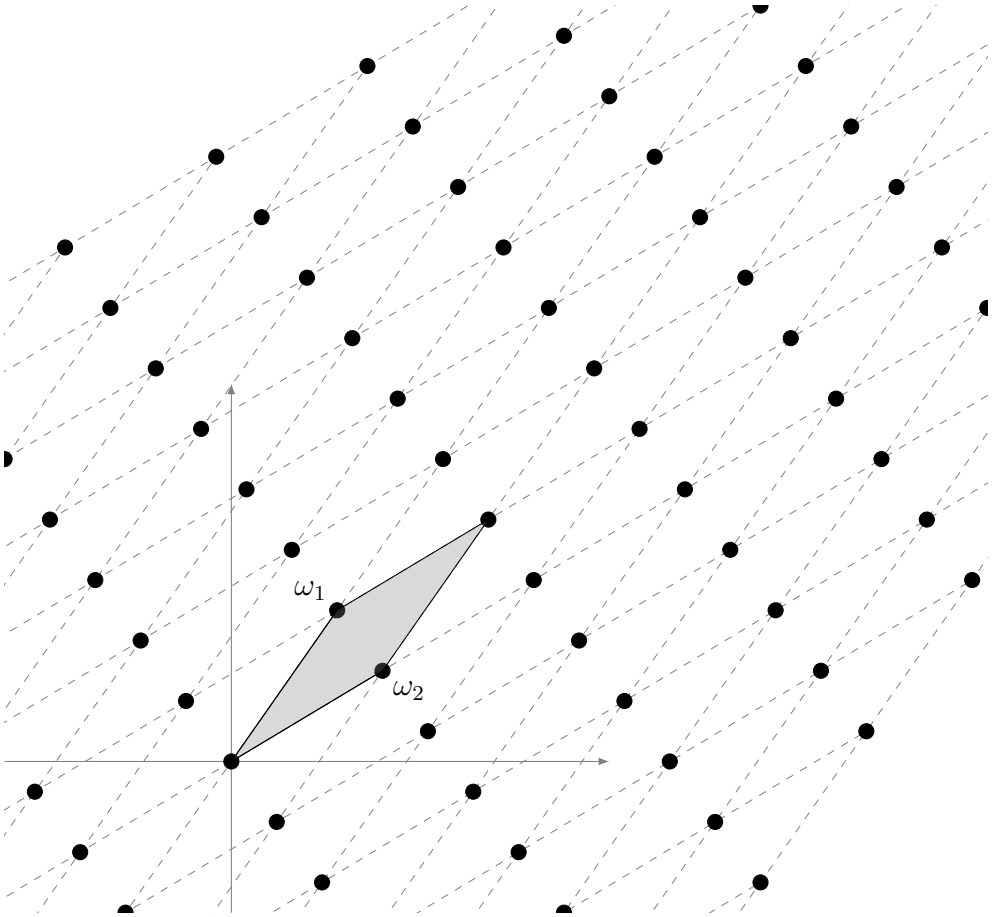



Figure 3: A positively oriented basis for the lattice (black points) forming a fundamental parallelogram (shaded).

## 8.1 Elliptic curves over the Complex numbers $\mathbb{C}$

In this section we consider elliptic curves over complex numbers. We will look at the correspondence between elliptic curves over complex numbers and the tori defined by $\mathbb{C}/\Lambda$ (lattice). We will show that we can use a lattice to define an elliptic curve over $\mathbb{C}$ and that every elliptic curve over $\mathbb{C}$ arises from a lattice. We will first define a lattice, then introduce the *Uniformization theorem* which is the correspondence between the lattice and the elliptic curve over $\mathbb{C}$. But in order to define the correspondence we will

give a brief discussion on *elliptic functions* on $\mathbb{C}$. This will enable us to construct elliptic curves with desired properties.

We define an endomorphism of an elliptic curve as a homomorphism from the elliptic curve to itself. We denote the set of all the endomorphisms of the elliptic curve by $End(E)$. The group structure on the elliptic curve makes $End(E)$ into a ring. One can choose a lattice and construct an elliptic curve with a particular endomorphism ring. Since we are working with elliptic curves over $\mathbb{C}$, the endomorphism ring is either the order in an imaginary quadratic field or $\mathbb{Z}$. We will view the order as a lattice and then prove that the endomorphism ring is in the elliptic curve corresponding to the torus.

**Definition 8.1.** *[83] (Lattice). A lattice $\Lambda \subset \mathbb{C}$ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}-$basis for $\mathbb{C}$. Then*

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2,$$

*where $\omega_1, \omega_2$ is a basis such that $\omega_1 \neq \lambda\omega_2$ for all $\lambda \in \mathbb{R}$.*

We assume that we will get a positive orientation when we switch basis $(\omega_1, \omega_2)$ to be basis $(\omega_2, \omega_1)$. This implies that we will have a positive angle from $\omega_2$ to $\omega_1$ and between $0^\circ$ and $180^\circ$ [84].

**Definition 8.2.** *A torus is defined by the quotient $\mathbb{C}/\Lambda$, where $\Lambda$ is a lattice.*

**Definition 8.3.** *A fundamental parallelogram for $\Lambda$ is a set of the form*

$$\mathcal{F} = \{a + t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 < 1\},$$

*where $a \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ is a basis for $\Lambda$ [83].*

A lattice does not have a unique basis. The following theorem shows a relationship between bases.

**Lemma 8.1.** *[85, 83] Let $\Lambda$ be a lattice, and let $(\omega_1, \omega_2)$ and $(\omega_1', \omega_2')$ be two positively oriented bases. Then*

$$\omega_1' = a\omega_1 + b\omega_2,$$

$$\omega_2' = c\omega_1 + d\omega_2,$$

*for some matrix*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

*Proof.* Suppose that we have two positively oriented bases,

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'.$$

For some integers $a, a', b, b', c, c', d, d'$ we have

$$\begin{aligned} \omega_1 &= a'\omega_1' + b'\omega_2', & \omega_1' &= a\omega_1 + b\omega_2, \\ \omega_2 &= c'\omega_1' + d'\omega_2', & \omega_2' &= c\omega_1 + d\omega_2. \end{aligned}$$

Since the basis $\omega_1$ and $\omega_2$ are $\mathbb{R}-$linearly independent we will get a unique solution ($AX = 0$), therefore we substitute the right-hand side of the equation into the left-hand side to get

$$\begin{aligned} \omega_1 &= a'(a\omega_1 + b\omega_2) + b'(c\omega_1 + d\omega_2), \\ \omega_2 &= c'(a\omega_1 + b\omega_2) + d'(c\omega_1 + d\omega_2), \end{aligned}$$

which yields

$$\begin{pmatrix} a'a + b'c & a'b + b'd \\ c'a + d'c & c'b + d'd \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We compute the determinant to show that $ad - cd > 0$:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} a' & b' \\ c' & d' \end{vmatrix} = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$$

$$ad - cb = a'd' - c'b' = \pm 1.$$

Therefore

$$ad - cd \neq 0.$$

Hence the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in the special linear group over $\mathbb{Z}$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

□

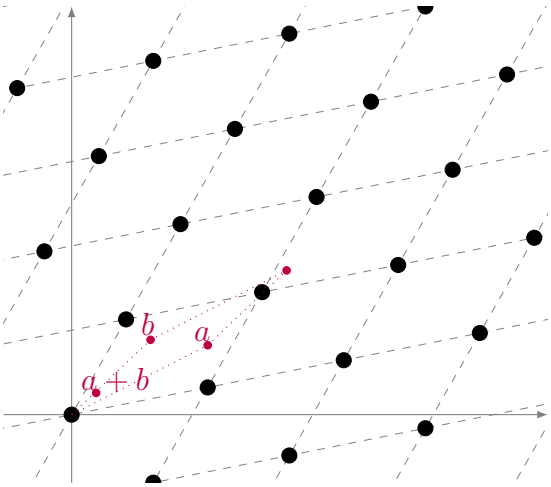



Figure 4: Addition of points in a torus (source [29]).

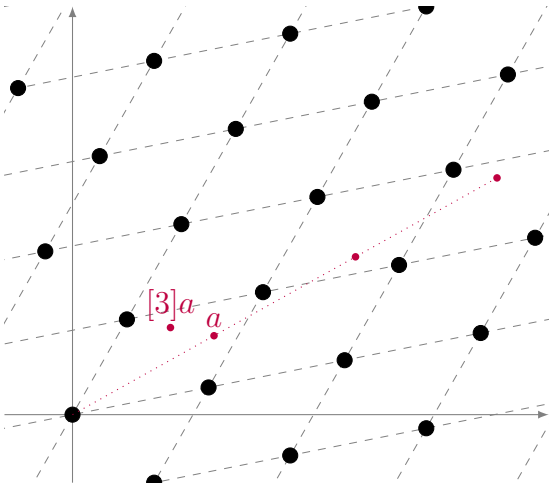



Figure 5: Scalar multiplication of points in a torus (source [29]).

**Definition 8.4.** *(Homothetic lattices). Let $\Lambda, \Lambda'$ be two lattices contained in $\mathbb{C}$. $\Lambda$ is homothetic to $\Lambda'$ if $\Lambda = \alpha\Lambda'$ for some $\alpha \in \mathbb{C}^*$.*

In simpler terms, Definition 8.4 tells us that homothety is rotating or zooming lattices around the origin.

We now define *elliptic functions* in order to see that there is a correspondence between elliptic curves and complex tori.

**Definition 8.5.** *A function $f(z)$ has a pole at $k$ of order $n$ if*

$$\lim_{z \to k} (z - k)^n f(z) = K,$$

*where $K$ is not zero or infinity.*

A function is said to have no poles if $K$ in definition 8.5 is zero or infinity.

**Definition 8.6.** *A holomorphic function is function with no poles [83]*

**Definition 8.7.** *A complex function $f$ is said to be meromorphic on an open set $\Omega$ if it is holomorphic at every point on an open set $\Omega$ except for a discrete set of poles [91].*

**Definition 8.8.** *An elliptic function $f$ (with respect to $\Lambda$) is a meromophic*

*function on $\mathbb{C}$ that is $\Lambda-$periodic [55] i.e.,*

$$f(z+\omega) = f(z),$$

*for all $z \in \mathbb{C}$ and $\omega \in \Lambda$. Note that $f$ is periodic if and only if*

$$f(z+\omega_1) = f(z) = f(z+\omega_2).$$

Definition 8.8 tells us that elliptic functions are periodic on lattices so one can view them as a function on a torus. Note that elliptic functions for lattices are also elliptic functions for sub-lattices of a lattice.

**Definition 8.9.** *The order of an elliptic function is the number of poles (counted with multiplicity) of the function in a fundamental parallelogram [83, 91].*

We can now define the *Eisenstein series of weight 2k* of a lattice. These series are examples of modular forms.

**Definition 8.10.** *Let $\Lambda$ be a lattice and let $k > 2$ be an integer. The Eisenstein series of weight $2k$ is defined as*

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}.$$

**Theorem 8.1.** *[29] (Modular $j-$invariant). The modular $j-$invariant is the function*

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{\Delta(\Lambda)},$$

$\Delta(\Lambda) = g_2(\Lambda)^3 - 27 g_3(\Lambda)^2$,
$g_2(\Lambda) = 60 G_4(\Lambda)$,
$g_3(\Lambda) = 140 G_6(\Lambda)$.

*Two lattices are homothetic if and only if they have the same modular $j-$invariant.*

To see the correspondence between an elliptic curve and a torus, we need a map from the tori $(\mathbb{C}/\Lambda)$ to an elliptic curve $(E/\mathbb{C})$. Then we need to parametrize this map by elliptic functions such as the Weierstrass $\wp$ function

and its derivative. This will prove the notion that every $\Lambda$ will always give rise to an $E/\mathbb{C}$. The next definition is an example of a non-constant elliptic function.

**Definition 8.11.** *[83] (Weierstrass $\wp$ function). Let $\Lambda$ be a lattice, the Weierstrass $\wp$ function associated to $\Lambda$ is the series*

$$\wp(z;\Lambda) = \frac{1}{\mathrm{z}^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Note that the Weierstrass $\wp$ function is constructed such that it has a pole of order 2 at each lattice point [91] and no poles elsewhere.

**Definition 8.12.** *(Riemann surfaces). A Riemann surface is a connected Hausdorff space (see [91]) with a complex structure.*

The key properties of the Weierstrass function $\wp(z,\Lambda)$ are as follows:

**Theorem 8.2.** *[83]*

1. *The Weierstrass $\wp-$function is an even elliptic function, i.e. $\wp(z) = \wp(z+\omega)$ for all $z \in \mathbb{C}$ and $\omega \in \Lambda$.*

2. *It's Laurent series around $z = 0$ is*

$$\wp(z) = \wp(z,\Lambda) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\Lambda) z^{2k}.$$

3. *For $z \in \mathbb{C}\backslash\Lambda$, the Weierstrass $\wp-$function and its derivative satisfy the relation*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

4. *The curve*

$$E : y^2 = 4x^3 - g_2 - g_3$$

*is an elliptic curve over $\mathbb{C}$. The map*

$$\tau : \mathbb{C}/\Lambda \to E(\mathbb{C}),$$

$$0 \mapsto (0:1:0),$$
$$z \mapsto [\wp(z) : \wp'(z) : 1]$$

*is an isomorphism of Riemann surfaces and a group morphism [83, VI, Thm. 3.1, Thm. 3.5, Prop. 3.6].*

Our interest is in $\wp(z)$. The Weierstrass $\wp-$function and it's derivative are related by the differential equation

$$\wp'(z,\Lambda)^2 = 4\wp(z,\Lambda)^3 - g_2(\Lambda)\wp(z,\Lambda) - g_3(\Lambda),$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$ are the invariants of the lattice. Let $x = \wp(z)$ and $y = \wp'(z))$, the differential equation, corresponds to the curve

$$y^2 = 4x^3 - g_2(\Lambda) - g_3(\Lambda).$$

Using the fact that $g_2(\Lambda) = -4A$ and $g_3(\Lambda) = -4B$ we can conclude that every lattice gives rise to an elliptic curve over $\mathbb{C}$ defined by the equation $y^2 = 4x^3 - g_2(\Lambda) - g_3(\Lambda)$ and that points are mapped from $\mathbb{C}/\Lambda$ to the elliptic curve by the map

$$\tau : \mathbb{C}/\Lambda \to E(\mathbb{C})$$
$$z \mapsto [\wp(z) : \wp'(z) : 1].$$

Note when we compare the definition 3.6 and 8.1, the two $j-$invariants, we can see that the corresponding $j-$invariant of an elliptic curve is the same as that of a lattice, i.e. $j(\Lambda) = j(E)$.

*Proof.* We know that $j(\Lambda)$ is defined as its discriminant is not equal to zero ($\Delta(\Lambda) \neq 0$). The curve

$$E : y^2 = 4x^3 - g_2 - g_3,$$

where $g_2 = -4A$ and $g_3 = -4B$, is isomorphic to the curve

$$E : y^2 = x^3 + Ax + B.$$

Hence we have,

$$\begin{aligned} j(\Lambda) &= 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} \\ &= 1728\frac{(-4A)^3}{(-4A)^3 - 27(-4B)^2} \\ &= 1728\frac{64A^3}{64A^3 + 432B^2} \\ &= 1728\frac{4A^3}{4A^3 + 27B^2} \\ &= j(E). \end{aligned}$$

Therefore $j(\Lambda) = j(E)$. □

**Theorem 8.3.** *Two lattices are homothetic if and only if* $j(\Lambda) = j(\Lambda')$.

*Proof.* ⇒Let $\Lambda_1$ and $\Lambda_2$ be two lattices. Assume they are homothetic, i.e $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}$. We want to prove that the two lattices have the same $j-$invariant. From definition 8.10 $G_{2k}(\Lambda_2) = \alpha^{-2k}G_{2k}(\Lambda_1)$. It follows immediately that $j(\Lambda_1) = j(\Lambda_2)$.

⇐ We want to prove that two lattices are homothetic. Assume that they have the same $j-$invariant. In chapter 3, Proposition 3.2 we have seen that two elliptic curves that have the same $j-$invariant are isomorphic. Therefore, by Proposition 3.2 there exists $u \in \mathbb{C}^*$ such that there is an isomorphism between the two elliptic curves. This implies that $g_2(\Lambda_1) = g_2(\Lambda_2)/u^4$ and $g_3(\Lambda_1) = g_3(\Lambda_2)/u^6$. Then for some $k > 2$ $g_k(\Lambda_1) = g_k(\alpha\Lambda_2)$. Hence $\Lambda_1 = \alpha\Lambda_2$.

□

The $j-$invariant is used to classify the homothety of a lattice which in turn corresponds to the isomorphism class of an elliptic curve [91]. We conclude this section by the Uniformization theorem which implies that every elliptic curve corresponds to a unique lattice.

**Theorem 8.4.** *[84] (Uniformization theorem). Let* $A, B \in \mathbb{C}$ *satisfy* $4A^3 +$

$27B^2 \neq 0$. *Then there is a unique lattice* $\Lambda$ *such that*

$$g_2(\Lambda) = 60G_4(\Lambda) = -4A$$

*and*

$$g_3(\Lambda) = 140G_4(\Lambda) = -4B.$$

## 8.2 The Endomorphism Ring

Recall we defined an endomorphism of an elliptic curve as a homomorphism from the elliptic curve to itself. In other words, it is isogeny from the curve to itself. An endomorphism ring of an elliptic curve defined over a field $\mathbb{K}$ consists of all isogenies from $E$ to $E$ together with the multiplication-by-zero (zero homomorphism), under multiplication (composition) and addition (point-wise) binary operations. Since the multiplication-by-$m$ map forms a subring that is isomorphic to $\mathbb{Z}$, we can say $\mathbb{Z} \subset End(E)$. We want to classify different endomorphism rings.

A vector space $V$ defined over a field $R$ is a set of vectors. The vector space $V$ is an abelian group under addition. We define a *module* as a vector space over a ring. If $V$ is a vector space defined over the field $R$, then $V$ is an $R-$module. There are two types of modules, the right $R-$module and the left $R-$module defined over the ring $R$. Note that every abelian group $L$ is a $\mathbb{Z}$-module. We can carry out subtraction and addition according to the group structure of $L$ and multiply $x \in L$ by the integer $n$. If we let $R$ be a commutative ring, then we say $V$ is an algebra over $R$. An algebra is defined as an algebraic structure (combination of a ring and a vector space) with an axiom linking the ring product with multiplication operations.

**Definition 8.13.** *[83] (Order). Let* $\mathcal{K}$ *be a* $\mathbb{Q}-$*algebra that is finitely generated over* $\mathbb{Q}$*. An order* $O$ *of* $\mathcal{K}$ *is a subring of* $\mathcal{K}$ *that is a finitely generated as a* $\mathbb{Z}-$*module and satisfies* $\mathcal{K} = O \bigotimes \mathbb{Q}$*. We will sometimes write* $O_{\mathcal{K}}$ *to avoid ambiguity.*

**Definition 8.14.** *[83] (Quaternion algebra). A quaternion algebra is an algebra of the form*

$$\mathcal{K} = \mathbb{Q} + \alpha\mathbb{Q} + \beta\mathbb{Q} + \alpha\beta\mathbb{Q},$$

*whose multiplication satisfies*

$$\alpha^2, \beta^2 \in \mathbb{Q}, \alpha^2 < 0, \beta^2 < 0, \beta\alpha = -\alpha\beta.$$

**Theorem 8.5.** *(Deuring). Let $E$ be an elliptic curve defined over a field $\mathbb{F}$ of characteristic $p$. The endomorphism ring, $End(E)$ of $E$ is either:*

1. *$\mathbb{Z}$;*
2. *An order $O$ in a quadratic imaginary field ($\mathbb{Q}(\sqrt{D})$, $D$ is the discriminant, $D < 0$). A curve whose $End(E) \simeq \{O\}$ has a complex multiplication by $O$;*
3. *An order in a quaternion algebra. The maximal order is a ring of integers of $O_{\mathcal{K}}$ of $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ containing all the other orders of $\mathcal{K}$*

*Proof.* See [83, 31, 6]. □

Therefore $\mathbb{Z}[\pi] \subset End(E) \subset O_{\mathcal{K}}$. Recall we said a curve is supersingular if $E[p] \simeq \{O\}$ and ordinary if $E[p] \simeq \mathbb{Z}_p$. The following proposition will help us prove Hasse's theorem.

**Proposition 8.1.** *[97] Let $\alpha$ and $\beta$ be endomorphisms of the elliptic curve $E$ and let $a, b$ be integers. Then*

$$\deg(a\alpha + b\beta) = a^2 \deg\alpha + b^2 \deg\beta + ab(\deg(\alpha+\beta) - \deg\alpha - \deg\beta).$$

Earlier we promised to prove Hasse's theore; we can now do so.

**Theorem 8.6** (Hasse's theorem)**.** *Let $E(\mathbb{F}_q)$ be an elliptic curve over the finite field $\mathbb{F}_q$ where $q = p^n$, $p$ a prime and $n \in \mathbb{Z}^+$. Then*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

*Proof.* Consider the map $(\pi - 1) : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q)$. We know that $\ker(\pi - 1) = E(\mathbb{F}_q)$, where the Frobenius endomorphism is the identity on $E(\mathbb{F}_q)$. We identify $E(\bar{\mathbb{F}}_q)$ as the kernel of $(\pi - 1)$ and note that $(\pi - 1)$ is a separable map so we have

$$\#E(\mathbb{F}_q) = \#\ker(\pi - 1) = \deg(\pi - 1).$$

Let $t = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\pi - 1)$. Using Proposition 8.1, for $a, b \in \mathbb{Z}$ such that $\gcd(b, q) = 1$, we have

$$\deg(a\pi - b) = a^2 q + b^2 - abt.$$

This is because $\deg(\pi) = q$ and $\deg(-1) = 1$, and so

$$\begin{aligned}\deg(a\pi - b) &= a^2(\deg(\pi)) + b^2(\deg(-1)) - ab(\deg(\pi - 1) - \deg(\pi) - \deg(-1) \\ &= a^2q + b^2 + ab(\#E(\mathbb{F}_q) - q - 1) \\ &= a^2q + b^2 + ab(q + 1 - t - q - 1) \\ &= a^2q + b^2 - abt.\end{aligned}$$

Therefore $\deg(a\pi - b) = a^2q + b^2 - abt$ as required. Since $\deg(a\pi - b) \geq 0$, we divide through by $b^2$ which gives

$$q\left(\frac{a}{b}\right)^2 - t\left(\frac{a}{b}\right) + 1 \geq 0.$$

The set of rational numbers $\frac{a}{b}$ such that $\gcd(b, q) = 1$ is dense in $\mathbb{R}$ which implies that

$$qx^2 - tx + 1 \geq 0,$$

for all $x \in \mathbb{R}$.

$qx^2 - tx + 1 \geq 0$ has no roots, thus it has a negative discriminant, meaning

$$t^2 - 4q \leq 0 \implies |t| \leq 2\sqrt{q}.$$

□

**Theorem 8.7.** *Let $E$ be an elliptic curve over a finite field. Its Frobenius endomorphism $\pi$ satisfies a quadratic equation*

$$\pi^2 - t\pi + q = 0,$$

*for some $|t| < 2\sqrt{q}$.*

*Proof.* See [83]. □

From the equation above, $\pi^2 - t\pi + q$, we call $t$ the trace of $\pi$. The trace, $t$, determines the order of the elliptic curve such that $t = \#E(\mathbb{F}_q) - (q + 1)$. If the characteristic of the field, $p$, divides $t$, then we have a supersingular curve.

**Proposition 8.2.** *[29] Let $\mathcal{K}$ be a quadratic number field, and let $O_{\mathcal{K}}$ be its ring of integers. Any order $O \subset \mathcal{K}$ can be written as $O = \mathbb{Z} + fO_{\mathcal{K}}$ for an integer $f$, called the conductor of $O$. If $d_{\mathcal{K}}$ is the discriminant of $\mathcal{K}$, the discriminant of $O$ is $f^2 d_{\mathcal{K}}$. If $O, O'$ are two orders of discriminants $f, f'$ then $O \subset O'$ if and only if $f'|f$.*

According to Washington [97], theorem 4.12, we can show this directly by letting

$$\#E(\mathbb{F}_q) = q + 1 - t.$$

We write

$$X^2 - tX + q = (X - \alpha)(X - \beta).$$

Then

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n),$$

for all $n \geq 1$ and $\alpha^n + \beta^n \in \mathbb{Z}$.

Schoof's Algorithm can be used to find $\#E(\mathbb{F}_q)$, we can use it to compute $\#E(\mathbb{F}_q) = \#E(\mathbb{F}_{q^n})$ using the above equation. The next section will give a brief overview of how Schoof's algorithm works.

## 8.3 Schoof's algorithm

The first polynomial-time algorithm used to compute $\#E(\mathbb{F}_q)$ was first published by Schoof in 1985 [78, 79]. The algorithm used to run faster than any other existing algorithms with a large $q$. However, Atkin and Elkies improved Schoof's method. The improved version is called the Schoof-Elkies-Atkin (SEA) algorithm. Using the SEA-algorithm requires you to work with a very large characteristic field. For more details on Elkies and Atkin's method see [4, 26, 10]. Satoh [77] gives a different method for counting points.

**A simple version of Schoof's algorithm**: You compute the trace, $t$, of the Frobenius endomorphism modulo $\ell$ for many small primes $\ell$. To obtain $t$, you use the Chinese remainder theorem. This will determine $\#E(\mathbb{F}_q) = q+1-t$.

If the Frobenius endomorphism is restricted to $E[\ell]$, $\ell-$torsion subgroup, then the characteristic equation is

$$\pi^2 - \pi t + q = 0,$$

where $P$ is a point in $E[\ell]$. This equation is used to find $[t]$.

To determine $t \pmod{\ell_i}$ where $\ell_i > 2$, we make use of division polynomials. The division polynomial $\psi_\ell$ is the smallest polynomial that can vanish on $E[\ell]$. More formally, we have:

**Definition 8.15.** *[83, 29] (Division polynomial). Let $E : y^2 = x^3 + ax + b$ be an elliptic curve, the division polynomials $\psi_m$ are defined by the initial values*

$\psi_1 = 1$
$\psi_2 = 2y^2$
$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$
$\psi_4 = (2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8abx - 2a^3 - 16b^2)2y^2,$

*and by the recurrence*

$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ *for* $m \geq 2$,
$\psi_2\psi_{2m} = (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m$ *for* $m \geq 3$.

*The $m-$th division polynomial $\psi_m$ vanishes on $E[m]$; the multiplication-by-$m$ map can be written as*

$$[m]P = \left(\frac{\phi_m(P)}{\psi_(P)^2}, \frac{\omega_m(P)}{\psi_(P)^3}\right),$$

*for any point $P \neq O$, where $\phi_m$ and $\omega_m$ are defined as*

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1},$$

$$\omega_m = \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2.$$

## 8.4 Schoof-Elkies-Atkin(SEA)-algorithm

Many considered Schoof's algorithm to be impractical until Elkies and Atkin improved the algorithm. Elkies came up with using good primes (Elkies primes) used to speed up calculations in modular curves and in isogenies. Atkin showed how the $\ell-$th modular polynomial can be used to determine whether $\ell$ is an Atkin prime or an Elkies prime. These improvements make use of a better understanding of how the Frobenius endomorphism acts on

the $\ell-$torsion subgroup of the elliptic curve. These insights come from a better understanding of how the restricted characteristic polynomial

$$\chi(X) = X^2 - t_\pi X + q \pmod{\ell},$$

of the Frobenius endomorphism splits over $(F)_l$ and then improve that.

We have three possible cases, we denote the roots of the characteristic polynomial by $\lambda$ and $\mu$:

- The *Elkies case*: If $\lambda \neq \mu$ then $\chi$ splits modulo $\ell$, i.e., $\chi(X) = (X - \lambda)(X - \mu)$.
- *Atkin case*: $\chi$ does not splits modulo $\ell$.
- $\chi$ is a square modulo $\ell$.

We refer to [24] and [32]. Schoof's algorithm is a deterministic polynomial-time algorithm. Schoof came up with this algorithm to compute $\#E(\mathbb{F}_q)$. Schoof computed a polynomial modulo $\psi_\ell$ that vanishes on the $\ell-$torsion subgroup $E[\ell]$ of the elliptic curve. The algorithm was rendered impractical due to the size of $\psi_\ell$ until Elkies and Atkin improved it.

Atkin improved Schoof's algorithm by using modular equations. Elkies came up with the use of good primes. Elkies showed how one can perform computations in $\ker \phi_\ell$, the kernel of the $\ell-$isogeny. The $\ell$ primes which are good primes are also known as the Elkies primes. By using this algorithm one can compute an eigenvalue of the Frobenius endomorphism, $\pi$, acting on the $\ell-$torsion point $E[\ell]$. Schoof's algorithm was considered practical after all these improvements were made which led to the SEA-algorithm. This algorithm is used for very large finite fields.

**Rough sketch of how the SEA algorithm work** Recall Schoof's algorithm [79]. Let $E/\mathbb{F}_q$ be an elliptic curve defined over $\mathbb{F}_q$. Let the characteristic of $\mathbb{F}_q$ be not equal to 2 or 3. Let $t$ denote the trace of the Frobenius endomorphism. We want to look at the action of the Frobenius endomorphism on $E[\ell]$. We compute $t$ by finding $t \pmod{\ell}$ for many small primes $\ell-$ (i.e., $\ell = 3, 5, 7, 11, ..., L$) such that

$$\prod_{\substack{\ell \leq 1 \\ \ell \neq 2, p}} \ell > 4\sqrt{q}.$$

Let $D_\pi = t^2 - 4q$ be the discriminant of the characteristic polynomial of the Frobenius endomorphism. If $D_\pi = t^2 - 4q$ is a non-zero square modulo $\ell$ then we will have two distinct eigenvalues in $\mathbb{F}_\ell$. We say $\ell$ is an Elkies prime. Otherwise, we call $\ell$ an Atkin prime. If there exist two eigenvalues for the Frobenius endomorphism then this implies that two isogenies defined in $\mathbb{F}_\ell$ exist, each with degree $\ell$ [24].

Compute the modular polynomial $\Phi_\ell(x, j)$. Then check if $\bar{\Phi}(x) = \Phi(x, j(E)) \pmod q$ has roots in $\mathbb{F}_q$. If $\bar{\Phi}(x)$ has a root in $\mathbb{F}_q$, we say that $\ell$ is an Elkies prime. Otherwise, we say $\ell$ is an Atkin prime.

To determine the value of $t$ we introduce $C$ where:

$C \pmod \ell = t_\ell$ for Elkies primes and $C \pmod \ell$ for Atkin primes.

The value of $t$ is obtained by testing if $(q + 1 - C)P = \mathcal{O}$ for each $C$.

Further improvements on the SEA-algorithm were made by Dewaghe and Couveignes-Dawaghe-Morain. For more details on these improvements see [79, 26, 10, 32, 36, 78].

## 8.5 Isogeny graphs

We now shift our focus to elliptic curves defined over finite fields. We want to look at *isogeny graphs*. Let $E_1$ and $E_2$ be elliptic curves defined over $\mathbb{F}_q$, where $\mathbb{F}_q$ is a finite field with $q$ elements and characteristic $p$. $\bar{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$. We define an isogeny as $\phi : E_1 \to E_2$. This map sends $0_{E_1}$ to $0_{E_2}$ and is also a *group homomorphism* from $E_1(\bar{\mathbb{F}}_q)$ to $E_2(\bar{\mathbb{F}}_q)$ [83]. The degree of an isogeny is its degree as an algebraic map. The scalar multiplication $[m]$ has degree $m^2$. $\ell-$isogenies are isogenies of degree $\ell$.

If you have an isogeny of degree 1 then you have an *isomorphism*."We can determine an *isomorphism class* of elliptic curves by their common $j-$invariant in $\bar{\mathbb{F}}_q$ [31]". David Kohel's thesis [53] explicates the endomorphism ring of an elliptic curve over a finite filed. He introduced $\ell-$isogenies defined on an elliptic curve over finite fields with the trace $t$. In this case $\ell$ is the degree of isogenies and is prime.

Isogenies are undirected because of the dual isogeny theorem. By this the-

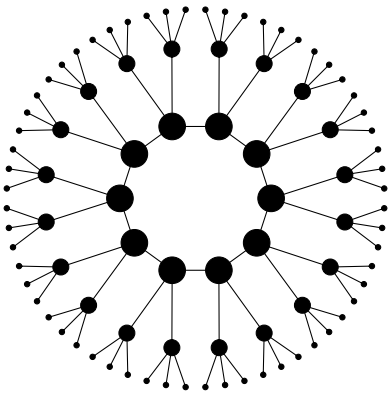


Figure 6: A volcano of 3-isogenies.

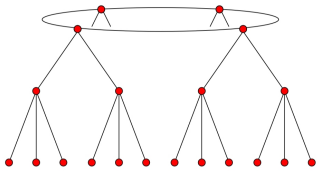


Figure 7: A different perspective of how a 3-volcano with height 2 looks like (diagram adapted from [90]).

orem we know that there will always be a corresponding isogeny for every isogeny with the same degree. Isogeny-based cryptosystems are based on isogeny graphs [31]. Isogeny graphs were first used for algorithmic applications by Mestre and Kohel [53]. Fouquent and Morain extended Kohel's work coming up with the term *isogeny volcanoes* [38, 46, 90]. There are numerous applications of isogeny volcanoes such as the computation of $End(E)$ of elliptic curves [9], the computation of modular polynomials [13] and many more. We now define isogeny graphs.

**Definition 8.16.** *[8, 31, 90] (Isogeny graphs). Given $\ell > 0$ prime, the $\ell-$isogeny graph between (isomorphism classes of) an elliptic curve defined over $\mathbb{F}_q$ is a graph whose vertices are the $j-$invariants of curves defined over $\mathbb{F}_q$ having an edge between $j_1$ and $j_2$ if and only if there exists an $\ell-$isogeny $\phi$ between some two curves $E_1$ and $E_2$ defined over $\mathbb{F}_q$ having $j-$invariant $j_1$(respectively $j_2$).*

As mentioned before, we can classify elliptic curves defined over finite fields as either supersingular or ordinary. We now shift our focus on the structure of isogeny graphs of ordinary curves which are imaginary quadratic fields then later focus on supersingular curves which are quaternion algebras. We define a maximal order of an algebraic field $\mathbb{F}$ by the set of algebraic integers in $\mathbb{F}$.

**Proposition 8.3.** *(Horizontal and vertical isogenies). Let $\phi : E \to E'$ be an $\ell-$isogeny with orders $O$ and $O'$ corresponding to $E$ and $E'$. Then, either*

*$O' \subset O$ or $O \subset O'$ and the index of one in the other divides $\ell$, this is denoted by $[O' : O] = \ell$ or $[O : O'] = \ell$. There are three possibilities:*

1. *If $O = O'$ then $\pi$ is a horizontal isogeny;*
2. *$[O' : O] = \ell$, we have an ascending isogeny;*
3. *$[O : O'] = \ell$, is a descending isogeny.*

*Proof.* See [53, 46]. □

We refer to the last two cases (descending and ascending isogenies) as vertical isogenies. This happens only if the discriminant of the finite field is divisible by $\ell$. Kohel [53] shows in his thesis that horizontal isogenies can only exist if $\ell$ does not divide the conductor of $O_E$. This depends on $(\frac{D}{\ell})$, the Legendre symbol, i.e., it will solely depend on whether the Frobenius endomorphism, $\pi$, gives an Atkin case, an Elkies case or it branches out, ramifying (branching out, say two points (same) with opposite signs) modulo $\ell$ [29].

**Proposition 8.4.** *[53] Let $E/\mathbb{F}$ be an ordinary elliptic curve with endomorphism ring $O$ of discriminant $D$, let $\ell$ be a prime, and let $(\frac{D}{\ell})$ be the Legendre symbol.*

1. *If $O_\ell$ is maximal then there are $(\frac{D}{\ell}) + 1$ isogenies of degree $\ell$ to curves with endomorphism ring isomorphic to $O$.*
2. *If $O_\ell$ is non-maximal, then there are no isogenies of degree $\ell$ to curves with endomorphism ring $O$.*
3. *If there exist more than $(\frac{D}{\ell})+1$ isogenies of degree $\ell$, up to isomorphism, then all isogenies of degree $\ell$ are defined over $\mathbb{F}$, and up to isomorphism of the pairs $(E, E')$ there are exactly*

$$\left(\ell - \left(\frac{D}{\ell}\right)\right)[O^* : O^{*\prime}]^{-1}$$

*elliptic curves $E'$ and isogenies $E \to E'$ of degree $\ell$ such that the only endomorphism ring $O'$ of $E'$ is properly contained in $O$. Note that $[O^* : O^{*\prime}]$ is the size of the orbits of the action of the automorphisms of $E$ on the set of cyclic subgroups of $E[\ell]$.*

**Definition 8.17.** *[90] An $\ell-$volcano $V$ is a connected undirected graph whose vertices are partitioned into one or more levels $V_0, ..., V_d$ such that the following hold:*

1. *The subgraph on $V_0$ (the surface) is a regular graph of degree at most 2.*

2. *For $i > 0$, each node in $V_i$ has exactly one neighbour in level $V_{i-1}$, and this accounts for every edge not on the surface.*

3. *For $i < d$, each node in $V_i$ has degree $\ell + 1$.*

*$d$ is the height of the volcano.*

The number of levels of *isogeny volcanoes* practically look like a geographic volcano, there is a crater at the top, this is formed by the cycle of the horizontal isogenies: Elkies, Atkin reducing it to a single point or ramified to two points and then there is the tree of descending isogenies from exactly each edge. The height of the volcano is given by the conductor of $\mathbb{Z}[\pi]$.

## 8.6 Application: Irreducible polynomials

Couveignes and Lercier [25] came up with the idea of irreducible polynomials forming a tower. Couveignes and Lercier's approach consists of randomly selecting a polynomial of degree $a$ and checking its irreducibility. They used Ben-Or's irreducibility test to check whether a polynomial is irreducible or not.

De Feo [29] gives an example of how we can check whether a polynomial $X^a - \beta$ is irreducible. If $a|(q-1)$, then there exists $\beta \in \mathbb{F}_q$ such that $X^a - \beta$ is irreducible, we assume that the factors of $q-1$ are known, thus one can select any element at random and test whether it has an $a-th$ root in $\mathbb{F}_q$ or not. It would be more advantageous to replace $\beta$ by a point $P \in E(\mathbb{F}_q)$ for some curve such that the point $P$ has no $\ell-$divisors in $E(\mathbb{F}_q)$.

Couveignes-Lercier [25] came up with this idea and De Feo et al [28] generalized it. The idea is to give a decomposition of the map $[\ell]$ as a composition of isogenies $\hat{\phi} \circ \phi$ and then taking the irreducible polynomial vanishing on the fiber $\phi^{-1}(P)$ [29].

Let $E$ and $E'$ be two elliptic curves defined over a finite field $\mathbb{F}_q$. Let $\phi : E \to E'$ be a $a$ degree separable isogeny. Assume that $a$ is odd and the kernel, $\ker G$, is cyclic, $G = E[\ell] \cap E(\mathbb{F}_q)$ ($E[\ell]$ intersect $E(\mathbb{F}_q)$). A polynomial,

$$f(X) = \prod_{Q \in \phi^{-1}(P)} (X - x(Q)),$$

is irreducible if and only if $\phi^{-1}(P)$ is an irreducible fiber [25]. We need to compute the isogeny $\phi$ as a rational function thus we use Vélu's formulas [95, 28] (as cited in [25, 29]).

**Definition 8.18.** *(Vélu's formulas). Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined in some field $\mathbb{F}$. Let $G$ be a finite subgroup of $E(\bar{\mathbb{F}})$. Then there exists an elliptic curve $E'$ and a separable isogeny $\phi : E \to E'$ such that $G = \ker \phi$. We define $\phi$ as follows:*

$$\phi(P) = \left( x(P) + \sum_{Q \in G \setminus \{O\}} x(P+Q) - x(Q), y(P) + \sum_{Q \in G \setminus \{O\}} y(P+Q) - y(Q) \right);$$

*and the curve $E'$ has equation $y^2 = x^3 + a'x + b'$, where*

$$a' = a - 5 \sum_{Q \in G \setminus \{O\}} (3x(Q)^2) + a),$$

$$b' = b - 7 \sum_{Q \in G \setminus \{O\}} (5x(Q)^3 + 3ax(Q) + b).$$

*Proof.* See [29, 97]. □

**Composition of isogenies**. We refer to [25]. Let $\mathbb{F}_q$ be a finite field. Let the Frobenius endomorphism of the elliptic curve $E$ be $\pi : E \to E$ and $t$ be its trace. Let $O$ be the quotient ring $\mathbb{Z}[X]/(X-1)(X-q)$ and $\tau$ be the class of $X \in O$. The ring monomorphism $\Phi : O \to End(E)$ sends $\tau$ onto $\pi$. For every $Z \subset O$, we define the kernel of $Z \in E$, denoted by $E[Z]$ as the intersection of all the kernels of the endomorphisms $\Phi(z)$ for some $z \in Z$.

Let $\ell \nmid p(q-1)$ and assume that $\ell | \#(\mathbb{F}_q)$. Because $\ell$ is co-prime to the discriminant of $O$, we have

$$X^2 - tX + q = (X-1)(X-q) \pmod{\ell},$$

thus the product of the roots of $X^2 - tX + q$ is $q$. However, because $\ell \nmid (q-1)$, we have two distinct roots, $1 \pmod{\ell}$ and $q \pmod{\ell}$. Let $I \subset O$ be the prime ideal in $O$, where $I = (\ell, \tau - 1)$. Let $I$ be the kernel of the prime ideal in the curve $E$ by $E[\ell](\mathbb{F}_q)$. Because $\ell | \#(\mathbb{F}_q)$ and $\ell$ is co-prime to $p(q-1)$ we have a cyclic group of order $\ell$ [25].

Similarly, if we let $i$ be a positive integer, we will have an ideal $I^i$ of $O$, generated by $\ell^i$ and $\tau - \lambda_i$, where integer $\lambda_i = 1 \pmod{\ell}$. The kernel, $E[I^i]$ is a cyclic group of order $\ell^i$ in $E(\bar{\mathbb{F}}_q)$. Let $E_i$ be an elliptic curve defined over $\mathbb{F}_q$ and let $\pi_i : O \to End(E_i)$ send $\tau$ onto the $q-$Frobenius endomorphism of $E_i$. We can decompose $\phi_{i+1} : E \to E_{i+1}$ as $\phi_{i+1} \circ \phi_i$ where $\phi_{i+1} : E \to E_{i+1}$ is the degree $l$ isogeny whose kernel is $E_i[\mathfrak{I}] = E_i[\ell](\mathbb{F}_q)$. $E[\mathfrak{I}^i]$ is a subgroup of $E[\ell^i]$ hence it does not contain the whole $\ell-$torsion subgroup. This leads to a cyclic chain of degree $\ell$ isogenies, i.e., horizontal isogenies forming a crater of the volcano. See figure 8.

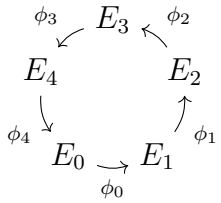



Figure 8: An isogeny cycle.

# 9 Cryptography from isogeny graphs

## 9.1 Expander graphs

For the past five decades, computer scientists devoted themselves in a huge amount of research on expander graphs. Mathematicians took an interest on expander graphs because of their explicit construction and their applications which are rather a difficult problem. There are many ways to construct expander graphs. One example would be using *Cayley graphs* which are considered to be one of the earliest construction of expander graphs [50]. Expander graphs were first studied as such by Pinsker in the 1970s [45]. They are defined as highly connected sparse finite graphs [45, 50, 57, 61]. This means that from the finite graph there are many edges leaving the set of vertices. Expander graphs can be used for error correcting codes [86] and generating pseudorandom numbers [57]. For more details on the applications of expander graphs see [60].

Let $G = (V, E)$ be an undirected graph where $V$ is a set of vertices. Two vertices $v, w \in V$ are adjacent if $vw \in E$. We assume $G$ is $k - regular$, meaning that all the vertices (i.e., each vertex) have the same degree $k$ [45]. For $A, B \subset V$ let $E(A, B) = \{(a, b)|a \in A, b \in B, (a, b) \in E\}$ denote the set of edges joining subgraph $A$ to subgraph $B$. A sequence of vertices $v \to v_1 \to ... \to w$ is formed when there is a *path* between two vertices $v, w$. In this case the vertices are connected by the edges. If there is a path connecting every $v$ and $w$ then we say that the graph is connected; if not we say it is disconnected. The length of the shortest path between $v$ and $w$ is known as the distance between the two vertices, while on the other hand the largest distance between all the vertices of a connected graph is known as a diameter. Let $Q$ be the adjacency matrix of $G$, i.e, $Q$ is an $n \times n$ matrix where $Q_{i,j}$ is the number of edges between the vertices of $v_i$ and $v_j$. $Q_{i,j}$ is either 0 or 1 if

the graph is simple if there are edges between $v_i$ and $v_j$. Since we are dealing with undirected graphs, the adjacency matrix is symmetric. Thus we have $n$ real eigenvalues

$$\lambda_1 \geq ... \geq \lambda_n.$$

**Lemma 9.1.** *If $G$ is a $k-$regular graph, then $\lambda_1$, the largest eigenvalue, satisfies*

$$k = \lambda_1 \geq \lambda_n \geq -k.$$

*Proof.* See [92]. □

**Definition 9.1.** *[92] (Expander graph). Let $\epsilon > 0$ and $k \geq 1$. A finite $k-$regular graph is said to be a (one-side) $\epsilon-$expander if one has*

$$\lambda_2 \leq (1-\epsilon)k,$$

*and a two-sided $\epsilon-$expander if one also has*

$$\lambda_n \geq -(1-\epsilon)k.$$

*A sequence $G_i = (V_i, E_i)$ of finite $k-$regular graphs is said to be a one-sided (resp. two-sided) expander family if there is an $\epsilon > 0$ such that $G_i$ is one-sided (resp. two-sided) $\epsilon-$expander for all sufficiently large $i$.*

**Theorem 9.1.** *(Ramanujan graph). Let $G$ be a $k-$regular graph on $n$ vertices where $k \geq 1$ and $n \to \infty$. Then*

$$max(|\lambda_2|, |\lambda_n|) \geq 2\sqrt{k-1} - o(1).$$

*A graph is called a Ramanujan graph if $|\lambda_i| \leq 2\sqrt{k-1}$.*

Ramanujan graphs are optimal expanders [20]. The eigenvalues of $Q(G)$ are known as the *spectrum* of the graph $G$. The spectrum of $G$ helps us with certain properties about the $k-$regular graph such as:

1. If $\lambda_1 = k$ then the corresponding eigenvector is $v_1 = 1/\sqrt{n} = (1/\sqrt{n}, ..., 1/\sqrt{n})$.
2. If $\lambda_1 > \lambda_2$ then the graph is connected.

The point of constructing expander graphs is to have sparser graphs that are connected and can be expanded to form a completed graph. A graph is either strongly connected by the $n$ vertices or it is easily disjoint by removing a few edges. This is known as *edge expansion*.

**Definition 9.2.** *[92, 61](Edge expansion). For $F$ a subset of $V$, we define the boundary of $F$, denoted by $\partial F$, as a set of all the edges of $G$ that are connecting elements of $F$ to those that are outside of $F$, $V \backslash F$. We denote the edge expansion ratio of $G$ by $h(G)$ where*

$$h(G) = \min_{F \subset V : |F| \leq |V|/2} \frac{|\partial F|}{|F|}.$$

Note that $h(G) \neq 0$ if and only if $G$ is connected and $G$ is disconnected when $h(G) = 0$.

**Theorem 9.2.** *(Discrete Cheeger inequality). The relationship between $h(G)$ and the constant $\epsilon$ that makes $G$ a one-sided $\epsilon-$expander is the discreet Cheeger inequality*

$$\frac{\epsilon}{2} k \leq h(G) \leq \sqrt{2\epsilon} k.$$

The theorem is due to Cheeger [17] and Buser [15]. Then proved by Dodzuik [34], Alon-Milman [2] and Alon in the discrete case. A *spectral gap* is used to estimate the expansion of a graph. We compute a spectral gap by $k - \lambda_2$. If the spectral gap is bounded away from the origin zero then that implies that the expansion ratio is also bounded away from the origin zero.

**Lemma 9.2.** *[92, 45] (Expander mixing lemma). Let $G$ be a $k-$regular two-sided $\epsilon-$expander with $n$ vertices. We set $\lambda = \lambda(G) = max(|\lambda_2|, |\lambda_n|)$. Then for all $F_1, F_2 \subseteq V$ :*

$$\left| |E(F_1, F_2)| - \frac{k|F_1||F_2|}{n} \right| \leq \lambda \sqrt{|F_1||F_2|}.$$

To breakdown the above equation:

- $E(F_1, F_2)$ is the number of edges between $F_1$ and $F_2$.

- $\frac{k|F_1||F_2|}{n}$ is the number of edges expected between $F_1$ and $F_2$.

**Proposition 9.1.** *[92] Let $G$ be a $k-$regular one-sided $\epsilon-$expander graph with $n$ vertices for some $\epsilon > 0$ and $n > k \geq 1$. Let any radius $r \geq 0$ and the ball $B(v,u) = \{w \in V : d(v,w) \leq r\}$, where $d(v,w)$ is the length of the shortest path from $v$ to $w$. Then, there exist a constant $c > 0$ that depends only on $k$ and $\epsilon$ such that*

$$|B(v,u)| \geq min((1+c)^r, n).$$

Expanders are required to have a low diameter and a high connectivity. $G$ has diameter $O(\log n)$, where $c$, the constant depends on $k$ and $\epsilon$ [92]. Hoory, Linial and Wigderson [45] defines a *random walk* as a sequence $v_0, v_1, v_2, ...$ of vertices of $G$ such that for every $v_i$, index $i$, there is a neighbour $v_{i+1}$ chosen uniformly at random.

**Theorem 9.3.** *The restriction of the isogeny graph to each level is a nearly Ramanujan graph [48].*

**Corollary 9.1.** *[48] At each level, the isogeny graph has the rapid mixing property: that is, starting from a given $E_1$, a random walk over the graph will reach any other curve $E_2$ with almost uniform probability (i.e. with exponentially (in $\log q$) small error) using a polynomial (in $\log q$) number of steps.*

If there is no other eigenvalue that is equal to $k$ then we know that the graph is connected. This suffices when $B \leq 3$. This was proved by [70]. Pizer proved theorem 9.3 in a sense that one can drop the level of restriction. [62] first defined the Ramanujan property which "characterizes the optimal separation between two largest eigenvalues of the graph adjacency matrix, and implies the expansion property"[54] [30, 48]. In the supersingular case, isogeny graphs are essentially Ramanujan graphs. See [70] and [71] for more details on Ramanujan graphs.

**Theorem 9.4.** *(Supersingular graphs are Ramanujan graphs). Let $p$, $\ell$ be primes, then:*

1. *For $p \geq 2$ all supersingular curves in $\bar{\mathbb{F}}_p$ are defined in $\mathbb{F}_{p^2}$;*
2. *For $p \geq 5$, the number of supersingular elliptic curves (up to $\bar{\mathbb{F}}_p-$isomorphism)*

*is*

$$[\frac{p}{2}] + \begin{cases} 0 & if p \equiv 1 \pmod{12} \\ 1 & if p \equiv 5 \pmod{12} \\ 1 & if p \equiv 7 \pmod{12} \\ 2 & if p \equiv 11 \pmod{12} \end{cases}$$

3. *If given a prime $p \geq 2$ then the graph $G$ will have a set of vertices $V$ of supersingular $j-$invariants over $\mathbb{F}_{p^2}$. There will be an edge between the two $j-$invariants over $j_1$ and $j_2$ if there is an isogeny of degree $\ell$ between the supersingular elliptic curve with the specified $j-$invariants, thus making the graph $G$ an $\ell + 1$ regular Ramanujan graph.*

*Proof.* See [83, 48, 57] □

## 9.2 Supersingular isogeny graph-based cryptography

In 2009 Charles, Lauter and Goren introduced supersingular isogeny graphs in a paper they wrote on "Cryptographic Hash Functions from expander graphs" [16] proposing two hard problems which entails finding cycles and paths of graphs. A hash function is a one-way cryptographic algorithm that converts an input data and returns an output of a fixed length of bits. Charles, Lauter and Lauter [16] calls a hash function a *"provable collision resistant hash function"* if to compute a collision means solving hard mathematical problems, i.e., the Discrete Logarithm Problem or factoring integers.

They constructed this hash function from expander graphs. In their construction the path-finding problem is as follows: Given a graph with a fixed length, one can find the path between vertices depending on their starting and end point. The input of a hash function is used for the directions for walking around the graph, and the output of the hash function is labelled as the ending vertex of the walk [16]. Finding cycles of a graph is considered to be equivalent to finding collisions in a hash function, just as finding a reverse path is equivalent to finding pre-images for a hash function [16, 20, 56]. Finding cycles in a graph is considered a hard problem [16].

In [16] Charles, Lauter and Goren proposed two families of optimal expanders, Ramanujan (also called Lubotzky-Phillips-Shanks or LPS graphs)

and the Supersingular Isogeny Graphs. These graphs were both presented at the NIST Hash Function workshops in 2005 and 2006 [56, 20]. In 2008 the LPS graphs which are based on *Cayley graphs* were broken and attacked hence leading to two attacks, a collision attack [93] and a pre-image attack [69].

According to [16] finding collisions by constructing hash functions of the LPS graph of a supersingular elliptic curve defined over the field $\mathbb{F}_{p^2}$ with $\ell-$isogenies where $\ell \neq p$ is considered to be as hard as it is to compute isogenies between supersingular elliptic curves. This is one of the best known algorithm as it takes $O(\sqrt{p}\log^2 p)$ time to solve a hard problem. The Diffie-Hellman protocol was proposed in [47] along with five hard problems concerning the security of the Diffie-Hellman protocol. We will discuss these problems when we look at the security-hardness assumption.

## 9.3 Charles-Lauter-Goren key-exchange

Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve defined over a field $\mathbb{F}_{p^2}$, where the prime $p = \ell_A^{e_A}\ell_B^{e_B} \cdot f \pm 1$, where $\ell_A$ and $\ell_B$ are small primes, $e_A$ is approximately equal to $e_B (e_A \approx e_B)$, and $f$ is a cofactor. Amahle and Bukhosi want to share a secret key by exchanging communication through an unsecure channel. Each will take a random walk on distinct isogeny graphs. $A$ denotes graphs for Amahle while $B$ denotes those of Bukhosi.

Amahle and Bukhosi generate their public parameters by selecting two points each $P_A, Q_A, P_B, Q_B$ so that $\langle P_A, Q_A\rangle = E[\ell_A^{e_A}]$ and $\langle P_B, Q_B\rangle = E[\ell_B^{e_B}]$.

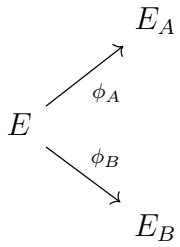
Amahle randomly selects two integers $0 \leq m_A, n_A < \ell_A^{e_A}$ where $\ell_A \nmid m_A, n_A$. Amahle then computes an isogeny $\phi_A : E \to E_A$ with kernel

$$k_A := \langle [m_A]P_A + [n_A]Q_A\rangle.$$

Similarly, Bukhosi selects two integers at random, $0 \leq m_B, n_B < 0$ where $\ell_B \nmid m_B, n_B$ and computes an isogeny $\phi_B : E \to E_B$ with kernel

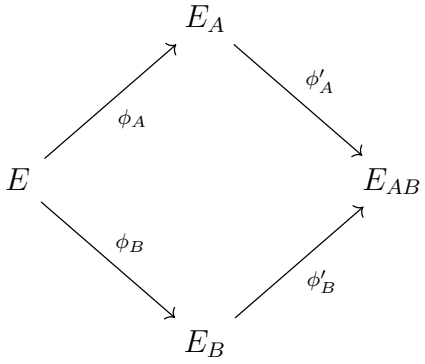
$$k_B := \langle [m_B]P_B + [n_B]Q_B\rangle.$$

We construct the following diagram for Amahle and Bukhosi:




Under the secret isogeny $\phi_A$ Amahle computes an image $\{\phi_A(P_B), \phi_A(Q_B)\}$ contained in $E_A$ and sends $\{\phi_A(P_B), \phi_A(Q_B), E_A\}$ to Bukhosi. Similarly, Bukhosi computes his points and sends $\{\phi_B(P_A), \phi_B(Q_A), E_B\}$ to Amahle.

Upon receiving Bukhosi's points, Amahle computes an isogeny $\phi'_A : E_A \to E_{AB}$ with kernel $\langle [m_A]\phi_B P_A + [n_A]\phi_B Q_A \rangle$ and Bukhosi does the same computing $\phi'_B : E_B \to E_{AB}$ with kernel $\langle [m_B]\phi_A P_B + [n_B]\phi_A Q_B \rangle$. This gives us enough information to complete the diamond for Amahle and Bukhosi,




where

$$E_{AB} = \phi'_A(\phi_B(E)) = \phi'_B(\phi_A(E)) = E/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle.$$

To compute $\phi'_B$, Amahle uses $m_A$ and $n_A$ by taking the quotient of $E_B$ by it's kernel, $\langle [m_A]\phi_B P_A + [n_A]\phi_B Q_A \rangle$, to obtain $E_{AB}$. Similarly, to compute $\phi'_A$, Bukhosi quotients $E_A$ by its kernel $\langle [m_B]\phi_A P_B + [n_B]\phi_A Q_B \rangle$ and obtains $E_{AB}$. Hence both ways results in the same elliptic curve $E_{AB}$. Amahle and Bukhosi then use the common $j-$invariant of $E_{AB}$ to form their shared key.

**Remark.** *Amahle and Bukhosi can explicitly use Vêlu's formulas to compute isogenies if given a list of points specifying a kernel, thus obtaining* $\phi_A, \phi_B, \phi'_A$

*and $\phi'_B$. However, if we put this in practice for a cryptographic size subgroup, this would be considered impossible hence one should consider a different approach since one wants to break the isogenies into m (n respectively) steps of degree $\ell_B$ ($\ell_A$ respectively). This problem will be explained in the hardness assumption.*

**Definition 9.3.** *[16] (Collision resistant). We say a hash function h is collision resistant if it is computationally infeasible to find two distinct inputs, $x, y$, which hash the same output $h(x) = h(y)$.*

**Definition 9.4.** *[16] (Preimage resistant). A hash function h is said to be preimage resistant if, given any output of h (for which a corresponding input is unknown) it is computationally infeasible to find an input x, which hashes to that output.*

## 9.4 Security: Hardness assumption

De Feo, Jao and Plût [30] introduced the hardness assumption calling it the Supersingular Computation Diffie-Hellman problem. The problems are as follows:

**Problem 9.1.** *[30, 20](Supersingular Computational Diffie-Hellman problem (SSCDH)): Let $E_A, E_B, E_{AB}, p, n, m, \ \ell_A, \ell_B, P_A, P_B, Q_A, Q_B$ be defined as above. Let $\phi_A : E \to E_A$ and $\phi_B : E \to E_B$ be isogenies whose kernels are $\langle [m_A]P_A + [n_A]Q_A\rangle$ and $\langle [m_B]P_B + [n_B]Q_B\rangle$ where the integers $m_A, n_A, m_B, n_B$ are randomly chosen and not divisible by $\ell_A(\ell_B$ respectively). Given the curves $E_A, E_B$ and their points $\phi_B(P_A), \phi_B(Q_A), \ \phi_A(P_B), \phi_A(P_B)$ find the $j-$invariant of*

$$E_{AB} \cong E/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B\rangle.$$

**Problem 9.2.** *[16] Produce a pair of supersingular elliptic curves over a finite field $E_A/\mathbb{F}_{p^2}$ and $E_B/\mathbb{F}_{p^2}$ and two different isogenies $\phi_A : E_A \to E_B$ and $\phi_B : E_B \to E_A$ of degree $\ell^n$ between them.*

Since the $ker\phi$ is cyclic then it implies that the factorization of the isogeny is unique given that the composition of the isogeny is an automorphism.

**Problem 9.3.** *[16] Find an $\ell^{2n}-$endomorphism, $\phi : E \to E$, that is not the*

*multiplication-by-$\ell^n$ map of a supersingular elliptic curve $E$ over $\mathbb{F}_{p^2}$.*

**Problem 9.4.** *[16] (Explicit isogeny). Given two supersingular elliptic curves $E_A$ and $E_B$ over a finite field $\mathbb{F}_{p^2}$, find an isogeny $\phi : E_A \to E_B$ of degree $\ell^n$ between them.*

**Problem 9.5.** *[20] (Path-finding). Let $E_A$ and $E_B$ be two supersingular elliptic curves over $\mathbb{F}_{p^2}$, where $p \neq \ell$ are primes numbers and $r > 0$. A path can be found by finding an isogeny $\phi : E_A \to E_B$ of degree $\ell^r$.*

Note that in order to break a preimage resistance of a specific hash function one needs to find a path of exactly length $r$. Problem 9.5 was introduced in [40] where it was argued that both the ordinary and supersingular cases are hard problems. A Pollard-rho type attack would be successful on problem 9.5 and 9.4 in $O(\sqrt{p}\log^2 p)$ time. However, this attack does not always lead to a path of the correct length [16].

Problem 9.2 and 9.3 are collision resistance. In order to find cycles in the graph we need to solve problem 9.3, but we must ensure that the graph does not consist of any short cycles. In this context, we can say a preimage resistance occurs when one finds a path from the starting vertex $j_0$ to another, i.e., a preimage resistant problem is associated with the isogeny path problem, whereas the collision resistant problem you find a non-trivial loop with no backtracking from the starting vertex $j_0$ to itself.

# 10 Post-quantum key exchange

We conclude this paper with two key exchange protocols that are similar to the Diffie-Hellman protocol but less efficient than the Elliptic Curve Diffie-Hellman (ECDH). The aim of this section is to help us understand the similarities and differences between a classical Diffie-Hellman and the post-quantum protocol. Firstly, we will review Couveignes's *hard homogeneous space* and then move to Supersingular Isogeny Diffie-Hellman (SIDH).

"The most stunning development in discrete logarithms came with the rise of the quantum computation paradigm: Shor's algorithm" [81, 87]. Peter Shor introduced a quantum algorithm that can be used to compute the factorization of an integer in $O(\log n)^2((\log\log n)(\log\log\log n))$ polynomial time ($n$ represent the number of bits of an integer) on a quantum computer with sufficiently many qubits [82, 81]. This is almost exponentially faster than the current best factoring algorithm known as the *number field sieve* [59] which has a sub-exponential running time of $(c(\log n)^{1/2}(\log\log n)^{2/3})$, $c$ is a constant.

In 2012, the factorization of 21 was achieved by Shor's algorithm thus making 21 the largest number factorized to date [63]. The largest number to be factorized on a quantum computer is 56153 [27]. Shor's algorithm solves the discrete algorithm problem in polynomial time thus its implementation poses a great threat to public-key cryptosystems such as Diffie-Hellman, RSA and other great security cryptosystems. For this reason, cryptographic research is underway for post-quantum cryptosystems designed to resist any quantum attacks [87].

We know that Shor's algorithm pose a threat on elliptic curve cryptography but luckily isogeny-based cryptography stands a much better chance as it is deeply routed in the theory of elliptic curve. A move from elliptic curve cryptography to isogeny-based cryptography implies that we replace points on a curve by an entire curve and the relationship between points is replaced by isogenies. Isogeny classes are not vulnerable to Shor's algorithm [87].

We now introduce two protocols based on random walks in an isogeny graph. Amahle and Bukhosi will both start on the same curve $E_0$. Their next step is to take random walks to different curves. Amahle will take a random walk to curve $E_A$ and Bukhosi will take his random walk to curve $E_B$. Both publish

their curves. Amahle begins a new walk from $E_B$, while Bukhosi begins his walk from $E_A$. Since both are repeating steps they will eventually reach a shared secret curve $E_{AB}$, which will be only known to them. Amahle and Bukhosi's walks should "commute".

## 10.1 Key-exchange from isogeny graphs

The supersingular Isogeny Diffie-Hellman (SIDH) key-exchange [47]was originally invented by Jao and De Feo. The source of inspiration for the SIDH key-exchange came from earlier key-exchange by Couveignes [23] and Rostovtev and Stolbunov [76, 89].

We can trace the origins of isogeny-based cryptography back to Couveignes' preprint "Hard Homogeneous Spaces" (HHS)[23]. We define a *"principal homogeneous space"* for a group $G$ as a set $Y$ such that for any $y, y' \in Y$, there is a unique $g \in G$ such that $g \cdot y = y'$. Equivalently, there is an isomorphism $\psi_y : g \to g \cdot y$ between the group $G$ and the set $Y$ for any $y \in Y$ [23, 31]. A *hard homogeneous space* (HHS) is defined by Couveignes to be a principal homogeneous space where one can compute the action of the group $G$ on the set $Y$ efficiently, but keeping in mind that it is computationally hard to invert the isomorphism $\psi_y$ for any $y$ [31]. A key-exchange between Amahle and Bukhosi is as follows:

1. Amahle randomly selects an element $y_0 \in Y$ and randomly picks $g_A \in G$. She then computes $y_A = g_A \cdot y_o$ and sends her key pair $(y_0, y_A)$ to Bukhosi.

2. Bukhosi does the same by randomly selecting an element $g_B \in G$ and computes $y_B = g_B \cdot y_o$. He sends $y_B$ to Amahle.

3. The shared secret key is $S(g_B, y_A) = g_B \cdot y_A = g_B \cdot (g_A \cdot y_0) = g_A \cdot (g_B \cdot y_0) = S(g_A \cdot y_B) = g_A \cdot y_B$.

For an attack to occur, adversaries would have to solve the Parallelization problem in [23] for a particular HHS in order to break the system.

**Definition 10.1.** *[44] (Cayley graph).*

*Let $S$ be a subset of a finite group $G$ satisfying*

1. $1 \notin S$, *where* 1 *denotes the identity of* $G$, *and*

2. $S = S^{-1}$, *that is,* $s \in S$ *implies that* $s^{-1} \in S$.

*A subset* $S$ *satisfying the above conditions is called a Cayley subset. The Cayley graph* $X(G, S)$ *is defined to be the graph whose vertices correspond to the elements of* $G$ *with an edge between* $g$ *and* $h$ *if and only if* $h = gs$ *for some* $s \in S$. *We call* $S$ *the connection set and say that* $X(G, S)$ *is a Cayley graph on the group* $G$.

**Definition 10.2.** *[30](Schreier graph). Let* $G$ *be a group,* $Y$ *a principal homogeneous space for* $G$ *and* $S \subset G$. *The Schreier graph* $(G, S, Y)$ *is the graph whose vertex set is* $Y$, *and where the edge* $s \in S$ *connects* $y_1$ *to* $y_2$ *if and only if* $s \cdot y_1 = y_2$.

*Note that this is isomorphic to a Cayley graph. If* $S$ *is symmetric, i.e.,* $S^{-1} = S$ ($s = s^{-1}$ *resp.), then the Schreier graph undirected [31].*

**Example 10.1.** *Let* $G = (\mathbb{Z}/13\mathbb{Z})^*$ *and* $Y = \langle y \rangle \backslash \{1\}$ *be a cyclic group of order 13 (without the identity element). The action of* $G$ *on* $Y$ *is the law:* $g \cdot y = y^g$ *for any* $g \in G$ *and* $y \in (\mathbb{Z}/13\mathbb{Z})^*$. *From definition 10.2* $S \subset G = S \subset (\mathbb{Z}/13\mathbb{Z})^*$ *implies that* $S$ *is symmetric. Therefore* $S = \{2, 3, 5, 2^{-1}, 3^{-1}, 5^{-1}\} \subset (\mathbb{Z}/13\mathbb{Z})^*$.

**Definition 10.3.** *[29] (Fractional ideal). Let* $O$ *be a fixed order in the number field* $K$. *A fractional ideal of* $O$ *is an* $O-$*submodule* $I$ *contained in* $K$ *such that for a certain non-zero* $n \in O$, *we have* $nI \subset O$.

*For some* $n$ *in* $K$ *we can define a fractional ideal as* $\langle n \rangle = nO$. *This type of fractional ideal is called principal.*

**Proposition 10.1.** *[31, 29] (Ideal class group). An ideal class group is defined as the quotient of the fractional group by the subgroup of the principal ideals, i.e.,*

$$Cl(O) = \mathcal{I}(O)/\mathcal{P}(O).$$

*This is a finite abelian group. The order of* $Cl(O)$ *is called the number of* $O$ *denoted by* $h(O)$.

**Definition 10.4.** *[30, 29] (*$\mathfrak{a}-$*torsion). Let* $E$ *be an elliptic curve defined*

*over a finite field $\mathbb{F}_q$. Let $\mathfrak{a}$ be an invertible ideal in $End(E) \simeq \{O\}$ of norm prime $p$. We define the $\mathfrak{a}-$torsion subgroup of $E$ as*

$$E[\mathfrak{a}] = \{P \in E | \beta(P) = 0 \text{ for all } \beta \in \mathfrak{a}\}.$$

The subgroup is the kernel of a separable isogeny $\phi_\mathfrak{a} : E \to E_\mathfrak{a}$. We denote the co-domain $E_\mathfrak{a} = E/E[\mathfrak{a}]$ of the separable isogeny $\phi_\mathfrak{a}$ by $\mathfrak{a} \cdot E$. Since $\mathfrak{a}$ is invertible then $\phi_\mathfrak{a}$ is always horizontal, i.e., $E(\mathfrak{a} \cdot E) \simeq End(E) \simeq \{O\}$.

**Theorem 10.1.** *[31, 29] Let $Ell_q(O)$ be the set of isomorphism classes over $\bar{\mathbb{F}}_q$ of elliptic curves with complex multiplication by $O$. Assume that $Ell_q(O)$ is non-empty, then the ideal class group, $Cl(O)$ acts freely and transitively on $Ell_q(O)$ (since the principal ideal acts trivially), i.e., if the curve is fixed as a based point then we have a map:*

$$\begin{aligned} Cl(O) &\to Ell_q(O) \\ \textit{Ideal class of} \mathfrak{a} &\mapsto \textit{Isomorphism class of} \mathfrak{a} \cdot E \\ (\mathfrak{a}, E) &\mapsto \mathfrak{a} \cdot E. \end{aligned}$$

The immediate result of theorem 10.1 is that $\#Ell_q(O) = h(O)$.

Let $\ell$ be an Elkies prime for an elliptic curve in $Ell_q(O)$. In chapter 8, section 8.5, we demonstrated how the connected components of an elliptic curve in a $\ell-$isogeny form cyclic horizontal isogenies. The restriction of the Frobenius endomorphism to $E[\ell]$ has two eigenvalues $\lambda \neq \mu$. This implies that there exist two isogenies with degree $\ell$ each. Let $\mathfrak{a} = (\pi - \lambda, \ell)$ and $\bar{\mathfrak{a}} = (\pi - \mu, \ell)$ be prime ideals, both of norm $\ell$. $E[\mathfrak{a}]$ is an eigenspace of $\lambda$, so it defines $\phi_\mathfrak{a}$ of degree $\ell$. $\mathfrak{a}$ and $\bar{\mathfrak{a}}$ are inverses of each other in the ideal class group, we have $\mathfrak{a}\bar{\mathfrak{a}} = \bar{\mathfrak{a}}\mathfrak{a} = (\ell)$, this implies that the isogeny of $\phi_{\bar{\mathfrak{a}}} : \mathfrak{a} \cdot E \to E$ of kernel $(\mathfrak{a} \cdot E \to E)[\bar{\mathfrak{a}}]$ is the dual of $\phi_\mathfrak{a}$ [31]. Let $S = \{\mathfrak{a}, \bar{\mathfrak{a}}\}$ and suppose $S$ contained in ideal class group is a symmetric subset, then its Schreier graph is a graph of horizontal isogenies and an expander graph if and only if the ideal class group is generated by $S$ [29]. The sizes of the cycles are defined by the order of $\mathfrak{a} \in Cl(O)$, thus $Ell_q(O)$ is partitioned into equally sized cycles. Rostovtsev and Stolbunov [76, 89] proposed an effective way of computing isogenies based on Couveignes' idea of a key exchange protocol based on random walks in horizontal isogenies [23].

The protocol makes use of the set of elliptic curves defined over $\mathbb{F}_q$ with a complex multiplication by $O$, however, $O$ is not computed explicitly. Instead, five parameters are determined [29]:

1. A large finite field $\mathbb{F}_q$.

2. An elliptic curve $E/\mathbb{F}_q$.

3. The discriminant, $D_\pi = t^2 - 4q$ of the elliptic curve is computed through counting points.

4. A set $L = \{\ell_1, ..., \ell_m\}$ of primes that split in $\mathbb{Z}[\pi]$, i.e., the Legendre symbol, $\left(\frac{D_\pi}{\ell_\pi}\right) = 1$.

5. The factorization of each prime $\ell_i$

$$\pi^2 - t_\pi \pi + q = (\pi - \lambda_i)(\pi - \mu_i) \pmod{\ell_i},$$

is computed, and we arbitrary choose $\lambda_i$ as one of the roots with a positive direction.

After all these steps we continue with the key exchange like the normal Diffie-Hellman protocol:

1. Amahle picks a random walk which is made of steps in $L$ in the positive direction. The walk is denoted by $\vartheta_A \in L^*$ and the termination of the walk in the curve is denoted by $E_A = \vartheta_A(E)$.

2. Similarly, Bukhosi selects a random walk $\vartheta_B$ and computes $E_B = \vartheta_B(E)$.

3. Amahle and Bukhosi exchange the curves where their walk terminates, $E_A$ and $E_B$.

4. Both compute the shared secrete:
Amahle: $S = \vartheta_A(E_B)$,
Bukhosi: $S = \vartheta_B(E_A)$.

The security of the Rostov-Stolbunov protocol lies on the isogeny path problem. One must make sure that the set $Ell_q(O)$ is large enough in order to mitigate any threats or attacks. The isogeny graphs must be connected so

that both the private and public curves are almost uniformly distributed in the set of the elliptic curve defined over $\mathbb{F}_q$ with a complex multiplication by $O$ [29]. Likewise, ideals must generate the class group, $Cl(O)$. Note that even though attackers are only able to see $E, E_A$ and $E_B$, they will not be able to break this protocol even if they are able to solve the Discrete Logarithm Problem.

## 10.2 Supersingular Isogeny Diffie-Hellman (SIDH)

In [22], four well-known classes of cryptographic primitives that remain unaffected by quantum computers are given, namely lattice-based cryptography, multivariate cryptography, code-based cryptography and hash-based cryptography. These classes remain secure in the presence of quantum computers. However, all these classes share one trait, they have a huge public key and signature size. SIDH on the other hand does not fall on any of the aforementioned classes. Proposed in 2011 [47] by Jao and De Feo, SIDH is believed to offer "post-quantum resistance". Its security properties are quite promising as it has a significantly smaller key size than other post-quantum key-exchange protocols.

SIDH began with a preprint by Rostovtsev [76]. Then a Diffie-Hellman-like cryptosystem based on the difficulty of computing isogenies between ordinary elliptic curves was proposed by Stolbunov [89] whose aim was to obtain a quantum resistant cryptographic protocol. However, Galbraith and Stolbunov [42] used a classical computer to come up with an algorithm to solve this problem in exponential time. Child, Jao and Soukharev [18] proposed a quantum algorithm that recovered private keys in Stolbunov's cryptosystem in sub-exponential time [30]. In other words, Child et al.'s quantum algorithm computes isogenies between ordinary elliptic curves in sub-exponential time. In [47] Jao and De Feo proposed SIDH which is based on the difficulty of computing isogenies on supersingular elliptic curves instead of ordinary elliptic curves. SIDH is said to resist quantum attacks as it is noncommutative, that is, the endomorphism ring of an elliptic curve is isomorphic to the maximal order in a quaternion algebra [83]. SIDH does not really fall in the HHS framework. This means that Amahle and Bukhosi's isogenies do not necessarily automatically commute, they need to publish extra information in order to complete the key-exchange protocol.

The protocol: Amahle and Bukhosi publicly agree on the following parameters:

1. A supersingular curve $E_0$ defined over a field $\mathbb{F}_{p^2}$.

2. Two small primes, $\ell_A, \ell_B \in \mathbb{Z}$.

3. A larger prime, $p = \ell_A^{e_A} \ell_B^{e_B} f \pm 1$ where $f \in \mathbb{Z}$ is a cofactor and $e_A, e_B$ are roughly the same size and half the diameter of the graph $\log(\ell_A^{e_A}) \approx \log(\ell_B^{e_B})$.

4. Two bases, $\{P_A, Q_A\}$ for $E_0[\ell_A^{e_A}] \simeq \mathbb{Z}_{\ell_A^{e_A}} \times \mathbb{Z}_{\ell_A^{e_A}}$ and $\{P_B, Q_B\}$ for $E_0[\ell_B^{e_B}] \simeq \mathbb{Z}_{\ell_B^{e_B}} \times \mathbb{Z}_{\ell_B^{e_B}}$.

Notice that if we fix $\ell_A^{e_A}$ and $\ell_B^{e_B}$ we can randomly test for $f$ values thus being able to find a desired value for which $p = \ell_A^{e_A} \ell_B^{e_B} f \pm 1$ is prime. Note that it is easy to find small primes but rather hard to find $p$. We use Bröker's [12] method to select $E_0$ with a group structure of $(\mathbb{Z}/(p \mp 1)\mathbb{Z})^2$. Bröker showed that it is easy to find a supersingular curve defined over $\mathbb{F}_{p^2}$ once you have found the prime $p = \ell_A^{e_A} \ell_B^{e_B} f \pm 1$. To find the basis $\{P_A, Q_A\}$ for $E_0[\ell_A^{e_A}]$:

1. We randomly select a point $P \in E_0(\mathbb{F}_{p^2})$ and multiply it by $(\ell_B^{e_B} \cdot f)^2$ to obtain a point $P'$ that has an order dividing $\ell_A^{e_A}$. In [47] Jao et al., states that "with high probability" the point $P'$ will actually have order $\ell_A^{e_A}$. To check this we can multiply $P'$ by $\ell_A$,$\ell_A^2$, etc. Repeat this process until you find such $P'$.

2. We use the same process to find another point $Q$ of order $\ell_A^{e_A}$. To determine whether $Q$ is independent of point $P'$ we compute the Weil pairing of two elements $e(P', Q)$ in the torsion subgroup $E[\ell_A^{e_A}]$. For this to be true, their Weil pairing must have order $\ell_A^{e_A}$. Repeat until you find your desired $Q$, then set $P_A = P'$ and $Q_A = Q$.

We perform the analogous computation to find basis $\{P_B, Q_B\}$ for $E_0[\ell_B^{e^B}]$.

Verheul [96] proposed the modification of Weil and Tate pairing. His modification entails using additional endomorphisms that exist on supersingular curves. When you use such an endomorphism, you are able to send points from one subgroup to another subgroup of the $\ell-$torsion. Verheul called

using such an endomorphism a distorsion. So if we let $E : y^2 = x^3 + ax$ be curve defined over $\mathbb{F}_p$ where $p \equiv 3 \pmod 4$ is a prime and let $P_A$ and $P_B$ be random points then we can find $Q_A$ and $Q_B$ by computing $Q_A = \phi(P_A)$ and $Q_B = \phi(P_B)$ where $-i = \sqrt{-1}$ in $\mathbb{F}_{p^2}$ and $\phi(x, y) = (-x, iy)$. The cardinality of the curve is $p + 1$.

## 10.3 Computing isogenies of a given kernel.

We describe how Amahle and Bukhosi will compute and evaluate their isogenies for a given kernel. In chapter 8, section 8.6, we saw that Vélu's formulas can be used to compute separable isogenies from a curve with a given kernel. We must also keep in mind that since all prime order groups are cyclic then all $\ell-$isogenies are also cyclic, meaning $\ell-$isogenies have cyclic kernels.

Given a cyclic subgroup $\langle R \rangle \subseteq E[\ell^e]$ of order $\ell^e$, there is an isogeny $\phi$ of degree $\ell^e$ with kernel $\langle R \rangle$ [22]. The kernel maps the elliptic curve $E$ to an isogenous elliptic curve $E/\langle R \rangle$. By Vélu's formulas we decompose $\phi$ into a chain of $e$ isogenies of degree $\ell$ as the degree of the isogeny is smooth. Define $E_0 = E$ and $R_0 = R$ and for $i \in 0, ..., e-1$

$$\phi_i = E_i \to (E_{i+1} = E_i/\langle [\ell^{e-i-1}] R_i \rangle).$$

The isogeny $\phi_i$ has a cyclic kernel group of order $\ell$. The composition $\phi_{e-1} \circ \cdots \circ \phi_0$ has a degree $\ell^e$ which together with $(\phi_{e-1} \circ \cdots \circ \phi_0)(R) = R_e = \mathcal{O}$ can be used to show that $\ker(\phi_i) = \langle R \rangle$ and hence $\phi = \phi_{e-1} \circ \cdots \circ \phi_0$ [22].

**SIDH protocol**

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_A} & E_0/\langle R_A \rangle \\ \downarrow{\scriptstyle \phi_B} & & \downarrow{\scriptstyle \phi'_A} \\ E_0/\langle R_B \rangle & \xrightarrow{\phi'_B} & E_0/\langle R_A, R_B \rangle \end{array}$$

1. $\phi_A, \phi'_A, \phi_B, \phi'_B$ represent random walks taken by Amahle and Bukhosi in the graphs of their isogenies of degree $\ell_A$ and $\ell_B$.

2. Amahle and Bukhosi randomly select subgroups:

$$\langle R_A \rangle = \langle [m_A]P_A + [n_A]Q_A \rangle \subset E[\ell_A^{e_A}],$$
$$\langle R_B \rangle = \langle [m_B]P_B + [n_B]Q_B \rangle \subset E[\ell_B^{e_B}],$$

of orders $\ell_A^{e_A}, \ell_B^{e_B}$ respectively.

3. They both compute their secret isogenies
$$\phi_A : E \to E/\langle R_A \rangle,$$
$$\phi_B : E \to E/\langle R_B \rangle.$$

4. They each publish $E_A = E/\langle R_A \rangle$ and $E_B = E/\langle R_B \rangle$ respectively.

5. Amahle needs to compute $\phi'_A : E/\langle R_B \rangle \to E/\langle R_A, R_B \rangle$ whose kernel is generated by $\phi_A(R_A)$ in order to compute the shared secret $E/\langle R_A, R_B \rangle$. In order to compute $\phi'_A$, Amahle needs to know $\phi_B(P_A)$ and $\phi_B(Q_A)$.

6. This is where Bukhosi publishes his public key $\phi_B(P_A)$ and $\phi_B(Q_A)$. Take note that even if Evah is able to see these values she will still be unable to compute $E/\langle R_A, R_B \rangle$.

7. With Bukhosi's values, Amahle will then be able to compute $\phi_B(R_A) = [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A)$ completing the protocol. Similarly, Bukhosi performs the analogous computations with Amahle's public keys.

**Example 10.2.** *Let $E_0 : y^2 = x^3 + x$ be a supersingular curve defined over $\mathbb{F}_{p^2}$, Amahle and Bukhosi agree on the prime $p = 431$ and choose $\ell_A = 2, e_A = 4, \ell_B = 3, e_B = 3$ and $f = 1$, so that $p = \ell_A^{e_A}\ell_B^{e_B} f \pm 1$. We can use $iy + x$ because $p = 3 \pmod 4$. Amahle and Bukhosi want to share a secret key exchange by communicating via an unsecure channel. Each will take a random walk on distinct isogeny graphs. A denotes graphs for Amahle and B denotes graphs for Bukhosi.*

*Amahle and Bukhosi generate their public parameters by selecting their bases:*

$$P_A = (65i + 70, 266i + 405)$$
$$P_B = (33i + 248, 189 + 32)$$

*and* $Q_A = \phi(P_A), Q_B = \phi(P_B)$, *where* $i = \sqrt{-1}$ *in* $\mathbb{F}_{431^2}$ *and* $\phi(x, y) = (-x, iy)$.

$$\begin{aligned} Q_A =& (-65i - 70, 405i - 266) \\ =& (336i + 361, 405i + 165) \\ Q_B =& (-33i - 248, 32i - 189) \\ =& (398i + 183, 32i + 242) \end{aligned}$$

*Amahle randomly selects two secret values*

$$\begin{aligned} m_A =& 101 \\ n_A =& 23 \end{aligned}$$

*where* $2 \nmid 101, 23$ *and then computes an isogeny* $\phi_A : E_0 \to E_A$ *with kernel*

$$\begin{aligned} \langle R_A \rangle =& \langle [m_A]P_A + [n_A]Q_A \rangle \\ \langle R_A \rangle =& \langle [101](65i + 70, 266i + 405) + [23](336i + 361, 405i + 165) \rangle \\ =& \langle ((412i + 183, 87i + 89) \rangle \end{aligned}$$

*Similarly, Bukhosi selects two integers at random*

$$\begin{aligned} m_B =& 250 \\ n_B =& 5 \end{aligned}$$

*where* $3 \nmid 250, 5$ *and computes an isogeny* $\phi_B : E \to E_B$ *with kernel*

$$\begin{aligned} \langle R_B \rangle =& \langle [m_B]P_B + [n_B]Q_B \rangle \\ =& \langle [250](33i + 248, 189 + 32) + [5](398i + 183, 32i + 242) \rangle \\ =& \langle ((309i + 150, 211i + 235) \rangle \end{aligned}$$

*Amahle and Bukhosi compute their secret isogenies :*
$\phi_A : E_0 \to E_A$ *i.e., the isogeny of degree 432 from elliptic curve defined by* $E_0 : y^2 = x^3 + x$ *over* $\mathbb{F}_{431^2}$ *to an elliptic curve defined by* $E_A : y^2 = x^3 + (130i + 47)x + (208i + 65)$ *over* $\mathbb{F}_{431^2}$.

*$\phi_B : E_0 \to E_B$ i.e., the isogeny of degree 216 from elliptic curve defined by $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_{431^2}$ to elliptic curve defined by $E : y^2 = x^3 + (34i + 291)x + (390i + 94)$ over $\mathbb{F}_{431^2}$. Note that the isogenies are lengthy to write down, but manageable to work with using a computer- they should NOT be done by hand.*

*Under the secret isogeny $\phi_A$, Amahle computes an image $\{\phi_A(P_B), \phi_A(Q_B)\}$ contained in $E_A$*

$$\begin{aligned}\phi_A(P_B) =&(385, 358i + 134)\\ \phi_A(Q_B) =&(429i + 43, 371i + 325)\end{aligned}$$

*and sends the image of points and the curve $\{\phi_A(P_B), \phi_A(Q_B), E_A\}$ to Bukhosi.*

*Similarly, Bukhosi computes his image of points and then he sends the points and the curve $\{\phi_B(P_A), \phi_B(Q_A), E_B\}$ to Amahle.*

$$\begin{aligned}\phi_B(P_A) =&(307i + 417, 220i + 126)\\ \phi_B(Q_A) =&(374i + 346, 353i + 28)\end{aligned}$$

*Upon receiving Bukhosi's points, Amahle computes an isogeny $\phi'_A : E_A \to E_{AB}$ with kernel*

$$\begin{aligned}\langle R'_A\rangle =&\langle [m_A]\phi_B P_A + [n_A]\phi_B Q_A\rangle\\ =&\langle [101](307i + 417, 220i + 126) + [23](374i + 346, 353i + 28)\rangle\\ =&\langle (310i + 173, 45i + 239)\rangle\end{aligned}$$

*and Bukhosi does the same computing $\phi'_B : E_B \to E_{AB}$ with kernel*

$$\begin{aligned}\langle R'_B\rangle =&\langle [m_B]\phi_A P_B + [n_B]\phi_A Q_B\rangle\\ =&\langle [250](385, 358i + 134) + [5](429i + 43, 371i + 325)\rangle\\ =&\langle (411i + 176, 302i + 104)\rangle\end{aligned}$$

*Amahle and Bukhosi can find isogenies $\phi'_B, \phi'_A$ from $E_B$ with kernel $\langle R'_A\rangle$ and from $E_A$ with kernel $\langle R'_B\rangle$ to obtain $E_{AB}$:*

*$\phi'_B : E_B \to E_{AB}$ i.e., the isogeny of degree 54 from elliptic curve defined by $E_B : y^2 = x^3 + (34i + 291)x + (390i + 94)$ over $\mathbb{F}_{431^2}$ to elliptic curve defined*

*by* $E_{AB} : y^2 = x^3 + 296x + 223$ *over* $\mathbb{F}_{431^2}$.

$\phi'_A : E_A \to E_{AB}$ *i.e., the isogeny of degree 27 from elliptic curve defined by* $E_A : y^2 = x^3 + (130i + 47)x + (208i + 65)$ *over* $\mathbb{F}_{431^2}$ *to elliptic curve defined by* $E_{AB} : y^2 = x^3 + 296x + 223$ *over* $\mathbb{F}_{431^2}$.

*We can see that both Amahle and Bukhosi arrived on the same curve* $E_{AB}$.

*Amahle and Bukhosi then use the common* $j-$*invariant of* $E_{AB}$ *to form their shared key. The common* $j-$*invariant is*

$$j(E_{AB}) = 189$$

SIDH is considered as one of the most robust quantum key-exchange method, yet there is still plenty of room for improvement such as improving it's algorithm and space efficiency [21, 22, 37] and to optimize arithmetic in finite fields [11]. See [94] for cryptographic problems underlying SIDH. SIDH has smaller key sizes in comparison to other post-quantum protocols.

# 11 Conclusion

In this dissertation we focused on pre- and post-quantum cryptography. We considered the work of [65, 66] and [52] who introduced Elliptic Curve Cryptography (ECC). ECC provides a number of benefits: compared to other cryptosystems it is faster because it has smaller keys and requires less computing power and memory. It is difficulty for adversaries to break into the cryptosystem. ECC is still vulnerable to attacks. We have seen that quantum computers poses a great threat to the Diffie-Hellman protocol as Shor's quantum algorithm can be used to break it. The idea is to move from Elliptic Curve Cryptography (ECC) to Isogeny-based Cryptography because isogeny classes are not vulnerable to Shor's algorithm. Our hope lies on the four well-known classes of cryptographic primitives that remains unaffected by quantum computers, which is why they are called quantum-safe cryptographic primitives. These classes remain secure in the presence of quantum computers. However, SIDH, one of the best post-quantum key-exchange protocol provides better securities properties because of its significantly smaller key size. SIDH does not fall in any of the aforementioned classes. Our focus has solely been on isogeny-based cryptography with a bit of lattice-based cryptography and hash-based cryptography. But, the question we should be asking ourselves is, as research is still under-way, are isogeny-based cryptosystems going to be enough to mitigate threats posed by quantum computers or are we doomed for life?

A lot of research was done on elliptic curves and isogeny-based cryptography is based on elliptic curves, meaning researchers, mathematicians and/or cryptographers can transfer their profound knowledge or concepts in this area (isogeny-based cryptography) to get more insight or better understanding on how to find solutions for the problem at hand, quantum computers. Note that isogeny-based algorithms are not only slower than any other post-quantum algorithms, but the design of various cryptographic primitives is also very hard. Hence, when it comes to choosing parameters, we should choose parameters which are safe and secure, since we already know the most common attacks. Isogeny-based algorithms are well-known for their hard problems involving two elliptic curves and calculating the isogeny between them. They are well-known for their small key sizes amongst the other quantum-safe protocols. The idea for isogeny-based algorithm is quite complex and totally different from the other algorithms we already have. It is recommended in

such a way that it is combined, e.g., with lattice-based algorithms so that if one area of the two quantum-safe algorithm fails, then the other will still be intact and secure.

# 1 Application: Factoring integers with elliptic curves

Factoring integers with elliptic curves is one of the many methods used to factor large integers into a product of small integers. H. Lestra [58] invented the Elliptic Curve Method (ECM) which is analogous to Pollard's $(p-1)-$method. Suppose that $n = pq$ where $q, p$ are distinct integers and $p < q$. The idea is to find a non-trivial divisor where $n > 1$. This is done by selecting an integer $b \pmod{n}$ and selecting a positive integer $\ell$. $\ell$ needs to be divisible by small prime powers. The next step is to calculate $b^{\ell} \pmod{n}$ and calculating $\gcd(b^{\ell} - 1, n)$ with the hope that the gcd yields a non-trivial factor of $n$.

Pollard's $(p-1)-$method will only be successful if $n = pq$ such that $p - 1$ is made up of only small prime numbers. In this case $p - 1$ must divide the positive integer $\ell$ and $p$ must not divide $b$.

The ECM algorithm is obtained by replacing the multiplicative groups $(\mathbb{Z}/p\mathbb{Z})^*$ and $(\mathbb{Z}/q\mathbb{Z})^*$ by the group of points of an elliptic curve. One condition that should be met is that $\#E(\mathbb{F}_p)$ must only have small prime factors, however, this is extremely rare hence the freedom to choose a different elliptic curve [29].

# Bibliography


[1] David Adrian et al. "Imperfect forward secrecy: How Diffie-Hellman fails in practice". In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2015, pp. 5–17.

[2] Noga Alon and Vitali D Milman. "$\lambda 1$, isoperimetric inequalities for graphs, and superconcentrators". In: *Journal of Combinatorial Theory, Series B* 38.1 (1985), pp. 73–88.

[3] Prashant Kumar Arya, Mahendra Singh Aswal, and Vinod Kumar. "Comparative study of asymmetric key cryptographic algorithms". In: *International Journal of Computer Science & Communication Networks* 5.1 (2015), pp. 17–21.

[4] Arthur OL Atkin. "The number of points on an elliptic curve modulo a prime". In: *preprint* (1988).

[5] Meenal Wankhede Barsagade and Suchitra Meshram. "Overview of history of elliptic curves and its use in cryptography". In: *International Journal of Scientific & Engineering Research* 5.4 (2014), pp. 467–471.

[6] Juliana V Belding. "Number theoretic algorithms for elliptic curves". PhD thesis. 2008.

[7] Daniel J Bernstein and Tanja Lange. "Faster addition and doubling on elliptic curves". In: *international conference on the theory and application of cryptology and information security*. Springer. 2007, pp. 29–50.

[8] Jean-François Biasse, David Jao, and Anirudh Sankar. "A quantum algorithm for computing isogenies between supersingular elliptic curves". In: *International Conference on Cryptology in India*. Springer. 2014, pp. 428–442.

[9] Gaetan Bisson and Andrew V Sutherland. "Computing the endomorphism ring of an ordinary elliptic curve over a finite field". In: *Journal of Number Theory* 131.5 (2011), pp. 815–831.

[10] Ian Blake et al. *Elliptic curves in cryptography*. Vol. 265. Cambridge university press, 1999.

[11] Joppe W Bos and Simon J Friedberger. "Arithmetic considerations for isogeny-based cryptography". In: *IEEE Transactions on Computers* 68.7 (2018), pp. 979–990.

[12] Reinier Bröker. "Constructing supersingular elliptic curves". In: *J. Comb. Number Theory* 1.3 (2009), pp. 269–273.

[13] Reinier Bröker, Kristin Lauter, and Andrew Sutherland. "Modular polynomials via isogeny volcanoes". In: *Mathematics of Computation* 81.278 (2012), pp. 1201–1231.

[14] William J Buchanan. *Finding nP when we have P for EC*. Accessed: 2020-11-26. 2020. URL: `https://asecuritysite.com/encryption/ecc_points_mult`.

[15] Peter Buser. "A note on the isoperimetric constant". In: *Annales scientifiques de l'École Normale Supérieure*. Vol. 15. 2. 1982, pp. 213–230.

[16] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. "Cryptographic hash functions from expander graphs". In: *Journal of Cryptology* 22.1 (2009), pp. 93–113.

[17] Jeff Cheeger. "A lower bound for the smallest eigenvalue of the Laplacian". In: *Proceedings of the Princeton conference in honor of Professor S. Bochner*. 1969, pp. 195–199.

[18] Andrew Childs, David Jao, and Vladimir Soukharev. "Constructing elliptic curve isogenies in quantum subexponential time". In: *Journal of Mathematical Cryptology* 8.1 (2014), pp. 1–29.

[19] Henri Cohen et al. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC press, 2005.

[20] Anamaria Costache et al. "Ramanujan graphs in cryptography". In: *Research Directions in Number Theory*. Springer, 2019, pp. 1–40.

[21] Craig Costello and Huseyin Hisil. "A simple and compact algorithm for SIDH with arbitrary degree isogenies". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2017, pp. 303–329.

[22] Craig Costello, Patrick Longa, and Michael Naehrig. "Efficient algorithms for supersingular isogeny Diffie-Hellman". In: *Annual International Cryptology Conference*. Springer. 2016, pp. 572–601.

[23] Jean Marc Couveignes. "Hard Homogeneous Spaces." In: *IACR Cryptol. ePrint Arch.* 2006 (2006), p. 291.

[24] Jean-Marc Couveignes, Laurent Dewaghe, and François Morain. *Isogeny cycles and the Schoof-Elkies-Atkin algorithm*. Tech. rep. Citeseer, 1996.

[25] Jean-Marc Couveignes and Reynald Lercier. "Fast construction of irreducible polynomials over finite fields". In: *Israel Journal of Mathematics* 194.1 (2013), pp. 77–105.

[26] Jean-Marc Couveignes and François Morain. "Schoof's algorithm and isogeny cycles". In: *International Algorithmic Number Theory Symposium*. Springer. 1994, pp. 43–58.

[27] Nikesh S Dattani and Nathaniel Bryans. "Quantum factorization of 56153 with only 4 qubits". In: *arXiv preprint arXiv:1411.6758* (2014).

[28] Luca De Feo. "Fast Algorithms for Towers of Finite Fields and Isogenies: Algorithmes Rapides pour les Tours de Corps Finis et les Isogénies". PhD thesis. Palaiseau, Ecole polytechnique, 2010.

[29] Luca De Feo. "Mathematics of isogeny based cryptography". In: *arXiv preprint arXiv:1711.04062* (2017).

[30] Luca De Feo, David Jao, and Jérôme Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247.

[31] Luca De Feo, Jean Kieffer, and Benjamin Smith. "Towards practical key exchange from ordinary isogeny graphs". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2018, pp. 365–394.

[32] Laurent Dewaghe. "Remarks on the schoof-elkies-atkin algorithm". In: *Mathematics of Computation* 67.223 (1998), pp. 1247–1252.

[33] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.

[34] Jozef Dodziuk. "Difference equations, isoperimetric inequality and transience of certain random walks". In: *Transactions of the American Mathematical Society* 284.2 (1984), pp. 787–794.

[35] Taher ElGamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". In: *IEEE transactions on information theory* 31.4 (1985), pp. 469–472.

[36] Noam D Elkies et al. "Elliptic and modular curves over finite fields and related computational issues". In: *AMS IP STUDIES IN ADVANCED MATHEMATICS* 7 (1998), pp. 21–76.

[37] Armando Faz-Hernández et al. "A faster software implementation of the supersingular isogeny Diffie-Hellman key exchange protocol". In: *IEEE Transactions on Computers* 67.11 (2017), pp. 1622–1636.

[38] Mireille Fouquet and François Morain. "Isogeny volcanoes and the SEA algorithm". In: *International Algorithmic Number Theory Symposium*. Springer. 2002, pp. 276–291.

[39] William Fulton. *Algebraic curves: an introduction to algebraic geometry*. Addison-Wesley, 1989.

[40] Steven D Galbraith. "Constructing isogenies between elliptic curves over finite fields". In: *LMS Journal of Computation and Mathematics* 2 (1999), pp. 118–138.

[41] Steven D Galbraith, Ping Wang, and Fangguo Zhang. "Computing elliptic curve discrete logarithms with improved baby-step giant-step algorithm". In: *Advances in Mathematics of Communications* 11.3 (2017), p. 453.

[42] Steven Galbraith and Anton Stolbunov. "Improved algorithm for the isogeny problem for ordinary elliptic curves". In: *Applicable Algebra in Engineering, Communication and Computing* 24.2 (2013), pp. 107–131.

[43] Vipul Gupta et al. "Performance analysis of elliptic curve cryptography for SSL". In: *Proceedings of the 1st ACM workshop on Wireless security*. ACM. 2002, pp. 87–94.

[44] Gena Hahn and Gert Sabidussi. *Graph symmetry: algebraic methods and applications*. Vol. 497. Springer Science & Business Media, 2013.

[45] Shlomo Hoory, Nathan Linial, and Avi Wigderson. "Expander graphs and their applications". In: *Bulletin of the American Mathematical Society* 43.4 (2006), pp. 439–561.

[46] Sorina Ionica and Antoine Joux. "Pairing the volcano". In: 82.281 (July 2012), pp. 581–603. DOI: 10.1090/s0025-5718-2012-02622-6.

[47] David Jao and Luca De Feo. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *International Workshop on Post-Quantum Cryptography*. Springer. 2011, pp. 19–34.

[48] David Jao, Stephen D Miller, and Ramarathnam Venkatesan. "Ramanujan graphs and the random reducibility of discrete log on isogenous elliptic curves". In: *Preprint (available from http://arxiv. org/abs/math. NT/0411378)* (2004).

[49] Antoine Joux et al. "The number field sieve in the medium prime case". In: *Annual International Cryptology Conference*. Springer. 2006, pp. 326–344.

[50] Martin Kassabov. "Symmetric groups and expander graphs". In: *Inventiones mathematicae* 170.2 (2007), pp. 327–354.

[51] Jonathan Katz et al. *Handbook of applied cryptography, 5th Ed.* CRC press, 2001.

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

[53] David Russell Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, Berkeley, 1996.

[54] David Kohel et al. "On the quaternion $\ell$-isogeny path problem". In: *LMS Journal of Computation and Mathematics* 17.A (2014), pp. 418–432.

[55] Serge Lang. "Elliptic functions". In: *Elliptic Functions*. Springer, 1987, pp. 5–21.

[56] Kristin Lauter. "Postquantum opportunities: lattices, homomorphic encryption, and supersingular isogeny graphs". In: *IEEE Security & Privacy* 15.4 (2017), pp. 22–27.

[57] Kristin E Lauter, Denis X Charles, and Eyal Zvi Goren. *Pseudorandom number generation with expander graphs*. US Patent 7,907,726. Mar. 2011.

[58] Hendrik W Lenstra Jr. "Factoring integers with elliptic curves". In: *Annals of mathematics* (1987), pp. 649–673.

[59] Arjen K Lenstra and Hendrik W Lenstra. *The development of the number field sieve*. Vol. 1554. Springer Science & Business Media, 1993.

[60] Alex Lubotzky. *Discrete groups, expanding graphs and invariant measures*. Springer Science & Business Media, 2010.

[61] Alexander Lubotzky. "Expander graphs in pure and applied mathematics". In: *Bulletin of the American Mathematical Society* 49.1 (2012), pp. 113–162.

[62] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. "Ramanujan graphs". In: *Combinatorica* 8.3 (1988), pp. 261–277.

[63] Enrique Martin-Lopez et al. "Experimental realization of Shor's quantum factoring algorithm using qubit recycling". In: *Nature photonics* 6.11 (2012), pp. 773–776.

[64] JL Massey and JK Omura. "A new multiplicative algorithm over finite fields and its applicability in public key cryptography". In: *EUROCRYPT'83 Udine, Italy* (1983).

[65] Victor S Miller. "Use of elliptic curves in cryptography". In: *Conference on the theory and application of cryptographic techniques*. Springer. 1985, pp. 417–426.

[66] Victor S Miller. "Elliptic Curves and their use in Cryptography". In: *DIMACS Workshop on Unusual Applications of Number Theory*. Vol. 21. sn. 1997.

[67] AM Odlyako. "Discrete logarithms and their cryptographic significance". In: *T. Beth* (), pp. 224–314.

[68] Payal V Parmar et al. "Survey of various homomorphic encryption algorithms and schemes". In: *International Journal of Computer Applications* 91.8 (2014).

[69] Christophe Petit, Kristin Lauter, and Jean-Jacques Quisquater. "Full cryptanalysis of LPS and Morgenstern hash functions". In: *International Conference on Security and Cryptography for Networks*. Springer. 2008, pp. 263–277.

[70] Arnold K Pizer. "Ramanujan graphs and Hecke operators". In: *Bulletin of the American Mathematical Society* 23.1 (1990), pp. 127–137.

[71] Arnold K Pizer. "Ramanujan graphs. Computational perspectives on number theory (Chicago, IL, 1995), 159–178". In: *AMS/IP Stud. Adv. Math* 7 ().

[72] Stephen Pohlig and Martin Hellman. "An improved algorithm for computing logarithms over GF (p) and its cryptographic significance (Corresp.)" In: *IEEE Transactions on information Theory* 24.1 (1978), pp. 106–110.

[73] John M Pollard. "Monte Carlo methods for index computation (????????)" In: *Mathematics of computation* 32.143 (1978), pp. 918–924.

[74] Ronald L Rivest, Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2 (1978), pp. 120–126.

[75] Kenneth H Rosen. "Elementary Number Theory and its Application, 1993". In: *Addison-Wesley Publishing Company, Exercise* 35 (), p. 100.

[76] Alexander Rostovtsev and Anton Stolbunov. "Public-Key Cryptosystem Based on Isogenies." In: *IACR Cryptology ePrint Archive* 2006 (2006), p. 145.

[77] Takakazu Satoh. "On p-adic point counting algorithms for elliptic curves over finite fields". In: *International Algorithmic Number Theory Symposium*. Springer. 2002, pp. 43–66.

[78] Rene Schoof. "Counting points on elliptic curves over finite fields". In: *Journal de theorie des nombres de Bordeaux* 7.1 (1995), pp. 219–254.

[79] René Schoof. "Elliptic curves over finite fields and the computation of square roots mod p". In: *Mathematics of computation* 44.170 (1985), pp. 483–494.

[80] Tarun Narayan Shankar and G Sahoo. "Cryptography with ellipitic curves". In: *International Journal of Computer Science And Applications* 2.1 (2009), pp. 38–42.

[81] Peter W Shor. "Algorithms for quantum computation: Discrete logarithms and factoring". In: *Proceedings 35th annual symposium on foundations of computer science*. IEEE. 1994, pp. 124–134.

[82] Peter W Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". In: *SIAM review* 41.2 (1999), pp. 303–332.

[83] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer Science & Business Media, 2009.

[84] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Springer Science & Business Media, 2013.

[85] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*. Vol. 9. Springer, 1992.

[86] Michael Sipser and Daniel A Spielman. "Expander codes". In: *IEEE transactions on Information Theory* 42.6 (1996), pp. 1710–1722.

[87] Benjamin Smith. "Pre-and post-quantum Diffie–Hellman from groups, actions, and isogenies". In: *International Workshop on the Arithmetic of Finite Fields*. Springer. 2018, pp. 3–40.

[88] Andreas Stein and Edlyn Teske. "Optimized baby step-giant step methods". In: *J. Ramanujan Math. Soc* 20.1 (2005), pp. 1–32.

[89] Anton Stolbunov. "Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves". In: *Advances in Mathematics of Communications* 4.2 (2010), p. 215.

[90] Andrew Sutherland. "Isogeny volcanoes". In: *The Open Book Series* 1.1 (2013), pp. 507–530.

[91] Andrew Sutherland. *MIT lecture notes*. Accessed: 2019-08-07. 2015. URL: `https://math.mit.edu/classes/18.783/2015`.

[92] Tao Terrence. *Expansion in groups of Lie type*. Accessed: 2020-09-07. 2011. URL: `https://terrytao.wordpress.com/2011/12/02/245b-notes-1-basic-theory-of-expander-graphs/`.

[93] Jean-Pierre Tillich and Gilles Zémor. "Collisions for the LPS expander graph hash function". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2008, pp. 254–269.

[94] David Urbanik and David Jao. "SoK: The problem landscape of SIDH". In: *Proceedings of the 5th ACM on ASIA Public-Key Cryptography Workshop*. 2018, pp. 53–60.

[95] Jacques Vélu. "Isogénies entre courbes elliptiques". In: *CR Acad. Sci. Paris, Séries A* 273 (1971), pp. 305–347.

[96] Eric R Verheul. "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems". In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2001, pp. 195–210.

[97] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2008.