SUPER SINGULAR ELLIPTIC CURVE ISOGENY

A FOURTH YEAR PROJECT REPORT

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF B.Sc. IN COMPUTATIONAL MATHEMATICS

BY

1. Sujit Acharya (22618)

2. Abhay Sharma (22635)

3. Bhupendra Shah (22634)

DEPARTMENT OF MATHEMATICS
SCHOOL OF SCIENCE
KATHMANDU UNIVERSITY
DHULIKHEL, NEPAL

November 2023

CERTIFICATION

This project entitled “SUPER SINGULAR ELLEPTIC CURVE ISOGENY” is carried out under my supervision for the specified entire period satisfactorily, and is hereby certified as a work done by following students

1. Sujit Acharya (22618)
2. Bhupendra Shah (22634)
3. Abhay Sharma (22635)

in partial fulfillment of the requirements for the degree of B.Sc. in Computational Mathematics, Department of Mathematics, Kathmandu University, Dhulikhel, Nepal.

____

Dr.Gokul K.C
Associate Professor
Department of Mathematics
School of Science, Kathmandu University
Dhulikhel, Kavre, Nepal
Date: November 24, 2023

APPROVED BY:

I hereby declare that the candidate qualifies to submit this report of the Mathematics Project (MATH 402) to the Department of Mathematics.

____

Head of the Department
Department of Mathematics
School of Science
Kathmandu University
Date: December 18, 2023

ACKNOWLEDGMENTS

This research was carried out under the supervision of **Dr.Gokul K.C** . We would like to express our sincere gratitude towards our supervisors for providing us with excellent supervision, guidance and suggestion for accomplishing this work. We are thankful to the entire faculty of Department of Mathematics for encouraging, supporting and providing this opportunity.

We would also like to thank everyone who helped us directly and indirectly during the duration of completing our project work.

ABSTRACT

The advent of quantum computers and the potential threat posed by Shor's Algorithm to asymmetric cryptographic methods has spurred a surge in research and standardization efforts for post-quantum cryptography. This study explores a promising solution – encryption systems based on supersingular isogenies, including the Supersingular Isogeny Diffie-Hellman protocol. These systems leverage well-studied isogenies and offer decent performance with compact key sizes, setting them apart from other post-quantum contenders. We delve into the mathematical foundations, key protocols, and innovative adaptations of established schemes in the supersingular isogeny context. While these cryptographic schemes exhibit promise in terms of performance and quantum resistance, they introduce increased protocol complexity, presenting a notable trade-off

KEYWORDS: isogeny cryptography, Supersingular Isogeny Diffie–Hellman

CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background

Public-key cryptography (PKC) is an essential technology in our information-driven society that facilitates secure communication without the need to share encryption keys in advance. The security of PKC relies on the computational complexity of certain mathematical problems, such as the integer factorization problem and the discrete logarithm problem. These problems underpin the security of the cryptography currently in use and are generally believed to be challenging for classical computers to solve efficiently.

However, in 1994, Peter Shor introduced a groundbreaking quantum algorithm, known as Shor's algorithm, which can solve these problems in polynomial time [9] with a low degree. This development marked a significant advance in the field of quantum computing and raised concerns about the potential impact on the security of existing cryptographic systems.

In recent years, major IT companies worldwide have made significant strides in the development of large-scale quantum computers, harnessing the principles of quantum mechanics to execute algorithms that far surpass the capabilities of classical computers. Shor's algorithm, as previously mentioned, stands as a prime example of such quantum algorithms. It adeptly solves complex problems like integer factorization and the discrete logarithm problem within a group in polynomial time with a low degree. This poses a substantial threat to traditional public-key cryptography (PKC) systems, including widely used methods like RSA and Elliptic Curve Cryptography, as their security relies on the computational difficulty of these problems, which can be efficiently solved by quantum computers.

Consequently, there is a growing need for quantum-resistant cryptography, a realm known as post-quantum cryptography (PQC). PQC aims to establish cryptographic systems based on mathematical problems for which no known polynomial-time quantum algorithm can provide a solution. Since 2016, the National Institute of Standards and Technology (NIST) has been actively engaged in the standardization process of PQC, recognizing its crucial role in the evolving landscape of digital security[1].

Among the promising candidates for PQC, isogeny-based cryptography has garnered attention. This cryptographic approach relies on the challenging problem of computing isogenies between two given elliptic curves over a finite field. The intricate nature of this task forms the cornerstone of the security provided by isogeny-based cryptography, presenting a captivating convergence of mathematical principles and cryptographic innovation. It serves as a testament to the ongoing efforts to ensure the confidentiality and integrity of sensitive information in the post-quantum era.

1.2 Related work

Isogeny-based cryptography was initially proposed by Couveignes in 1997, introducing the concept of Hard Homogeneous Spaces (HHS). Couveignes used HHS to create a quantum-resistant key exchange protocol and demonstrated the CM-action of an ideal class group of an imaginary quadratic field on ordinary elliptic curves as an example of HHS[3]. In 2006, Rostovtsev and Stolbunov independently developed a similar method, leading to what is now known as the CRS scheme[8]. However, the CRS scheme is notably slow when it comes to computing an action of ideal classes on ordinary curves. Although efforts have been made to improve its performance, it is currently far from being a practical solution. The challenge of constructing ordinary curves suitable for isogeny computation remains unresolved.

The first application of isogenies between supersingular elliptic curves in cryptography emerged in 2009 when Charles, Lauter, and Goren created a cryptographic hash function using supersingular isogeny graphs[2]. Subsequently, in 2017, Jao and De Feo introduced a Diffie-Hellman style key exchange protocol based on supersingular isogenies. This protocol models random walks in isogeny graphs. A critical advantage is that the order of supersingular elliptic curves depends on the characteristic of the field of definition. By using a prime of specific form, torsion points from a quadratic extension of the prime field can be efficiently derived, and isogeny computations are implemented effectively using Vélu's formula[7]. This scheme is known as the Supersingular Isogeny Diffie-Hellman (SIDH). Additionally, a key encapsulation mechanism called SIKE, based on SIDH, was submitted to NIST's competition for the standardization of post-quantum cryptography (PQC).

Following the initiation of NIST's standardization process for post-quantum cryptography (PQC), Castryck and his team introduced an efficient method for the action of an ideal class group on supersingular elliptic curves. This development marked the first practical instantiation of Hard Homogeneous Spaces (HHS). Leveraging this innovative action, they devised an efficient key exchange protocol based on isogenies, which they named the Commutative Supersingular Isogeny Diffie-Hellman (CSIDH).

These cryptographic schemes, namely SIDH and CSIDH, have now become standards in the field of isogeny-based cryptography. Extensive research has been conducted on these schemes, exploring both their security and efficiency aspects. However, due to space limitations, not all of these studies can be covered here. In this paper, serving as an introduction to isogeny-based cryptography, we will provide an overview of how supersingular isogenies are employed to construct public-key cryptography through the creation of SIDH and CSIDH.

1.3 Objectives

The primary objective of supersingular elliptic curve isogeny in the field of cryptography is to provide a foundation for post-quantum cryptographic schemes that offer secure communication and data protection even in the presence of powerful quantum computers. Specifically, supersingular elliptic curve isogeny (SECI) serves several key objectives:

- Quantum Resistance:

  One of the primary goals of SECI is to provide cryptographic protocols that are resistant to attacks by quantum computers. Quantum computers have the potential to break many classical cryptographic systems (e.g., RSA, ECC) using algorithms like Shor's algorithm, which can efficiently solve the discrete logarithm problem and factor large integers. SECI-based protocols aim to withstand quantum attacks and ensure the long-term security of communication.

- Secure Key Exchange:

SECI is used to establish shared secret keys securely between two parties. This is crucial for secure communication, including secure messaging, secure data transmission, and secure access to online resources. It ensures that an eavesdropper, even with access to quantum computing capabilities, cannot derive the shared secret key.

- Privacy and Confidentiality:
  SECI-based cryptographic schemes protect the privacy and confidentiality of data exchanged over the internet. It ensures that sensitive information remains confidential and is not exposed to unauthorized parties

- Post-Quantum Security:
  As quantum computing technology advances, the need for cryptographic schemes that are secure against quantum attacks becomes more pressing. SECI provides a potential solution to this challenge by relying on the computational hardness of certain problems related to isogenies.

- Cryptographic Research:
  SECI serves as a platform for cryptographic research, encouraging the development of new algorithms, protocols, and security analyses. It fosters innovation and the continuous improvement of post-quantum cryptographic techniques.

1.4 Limitations

Supersingular elliptic curve isogeny (SECI) has several limitations and challenges:

- Computational Complexity: SECI-based cryptographic schemes can be computationally intensive, particularly when generating isogenies. This complexity can impact performance and practicality, especially for resource-constrained devices.

- Standardization and Adoption: SECI is a relatively new area in cryptography, and standardization efforts are ongoing. The adoption of SECI-based protocols may take time and faces competition from established cryptographic methods.

- Ongoing Research: SECI is still an evolving field with ongoing research, which means that new vulnerabilities or improvements may be discovered over time.

- Quantum Attacks on Quantum Computers: While SECI aims to be quantum-resistant, there is a theoretical possibility that quantum computers could develop new algorithms to attack SECI-based schemes in the future. Research in post-quantum cryptography is ongoing to address these concerns.

It's important to note that ongoing research and development efforts are addressing some of these limitations, and SECI-based cryptography holds promise as a quantum-resistant cryptographic solution. However, these challenges should be considered when implementing SECI in real-world applications.

CHAPTER 2

MATHEMEMATICAL FOUNDATION

2.1 Elliptic Curves

Elliptic curves are a staple technology in today's world. They are used in many areas of public-key cryptography and are valued for their small size and computational efficiency. An elliptic curve E is defined by a specific equation, and a point $P = (x, y)$ with the coordinates x and y is said to lie on the curve E if the values for x and y satisfy the equation[10].

Definition 1 *An elliptic curve E defined over a field* $\mathbb{F}_q$ *is given by the short Weierstrass Equation*

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

where a,b $\in F_q$

Additionally, E has to be smooth (non-singular), i.e., every point on the curve needs to have a unique tangent

Figure 2.1 shows two different curves in Weierstrass form, both of which are defined over the field of the rational numbers R. Additionally, the curve on the left is smooth and hence qualifies as an elliptic curve. The one on the right, however, has a p at $(0, 0)$, and it is easy to see that at this point, infinitely many tangents exist[10]. Hence, the curve on the right is singular (not smooth) and thus not an elliptic curve.

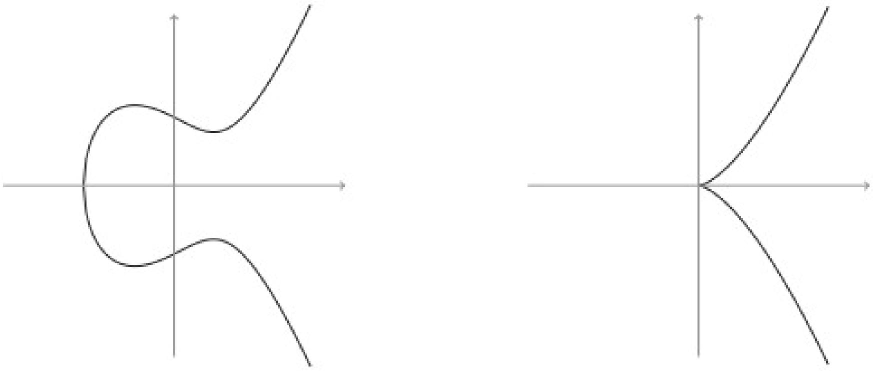


Figure 2.1: The elliptic curve $y^2 = x^3 - x + 1$ (left) and the non-elliptic curve $y^2 = x^3$ (right), both defined over $\mathbb{R}$

Definition 2 *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Then an elliptic curve group $E(\mathbb{F}_q)$ is formed by the union of $\mathbb{F}_q$-rational points on E and the neutral element O. Let $P = (x, y)$, $Q = (x_0, y_0)$ be in $E(\mathbb{F}_q)$. Let O denote the neutral element. We define the group law by the following rules:*

- $P \oplus O = O \oplus P = P$*,*
- $P \oplus (-P) = (-P) \oplus P = O$ *for* $(-P) = (x, -y)$*,*
- $P \oplus Q = (\alpha, \beta)$ *with*

$$\alpha = \lambda^2 - x - x_0$$

$$\beta = -\lambda\alpha - y + \lambda x$$

where,

$$\alpha = \frac{3x^2 + a}{2y} \text{ if } P \neq Q$$

,

$$\alpha = \frac{3x^2 + a}{2y} \text{ if } P = Q$$

.

It is clear that when $\mathbb{F}_q$ is a finite field, there are only finitely many points that can lie on E. Finding the exact number $|E(\mathbb{F}_q)|$ of points is not easy; however, with Hasse's theorem, we have an upper bound of $|E(\mathbb{F}_q)| \leq q+1+|t|$ for a field $\mathbb{F}_q$ with q elements With $|t| \leq 2\sqrt{q}$, where t is called the Frobenius trace. The elliptic curve E is called **supersingular** if p

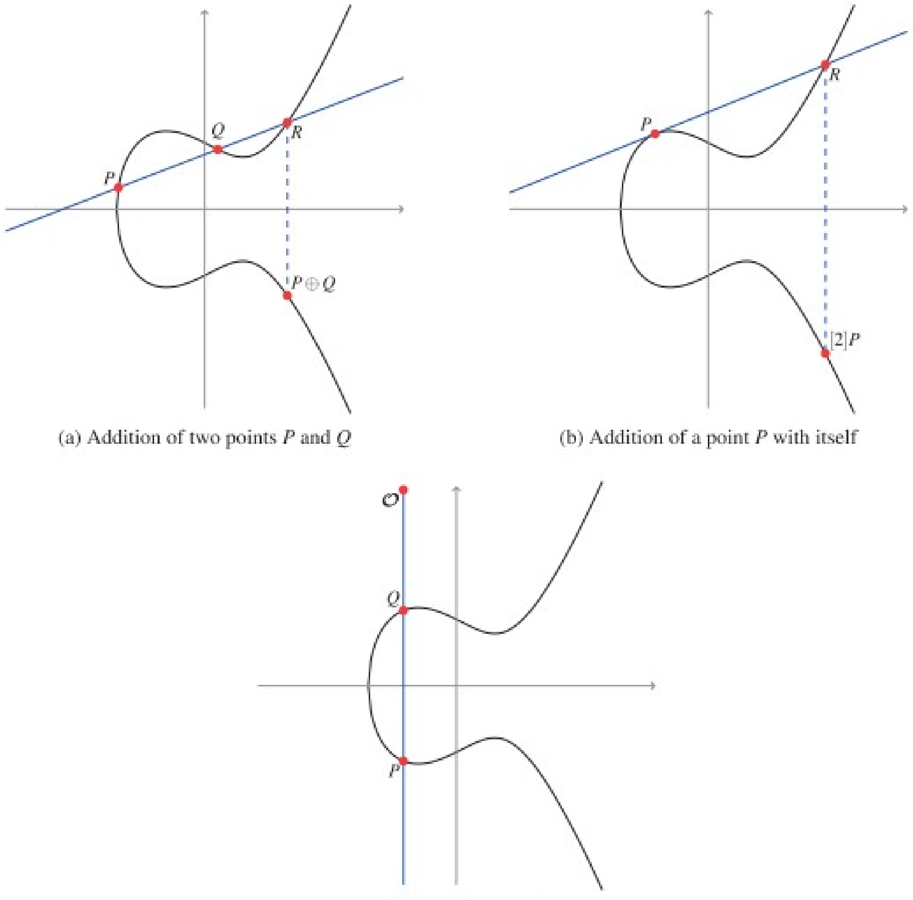
divides t, and **ordinary** otherwise[6]. Hence, the orders of supersingular elliptic curves over a prime field $\mathbb{F}_p$ are determined by the characteristic $p > 3$:

$$\#E(\mathbb{F}_p) = p + 1$$

It follows that E is supersingular if $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$, and in fact for supersingular curves, one has $\#E(\mathbb{F}_{q^n}) \equiv 1 \pmod{p}$ for all $n \in \mathbb{N}$.

For $n \in \mathbb{N}$, define $E[n] = \{P \in E(\mathbb{F}_q) : [n]P = 0\}$. If $p \nmid n$, then $\#E[n] = n^2$, and group theoretically, $E[n]$ is a direct product of two cyclic groups of order n. If E is supersingular, then $E[p] = \{0\}$, while if E is ordinary, then $\#E[p] = p$.

Figure 2.2 intuitively shows the group operation in its geometric representation for the elliptic curve $E : y^2 = x^3 - x + 1$ defined over $\mathbb{R}$. Figure 2.2(a) displays the addition of two distinct points P and Q. A line is drawn through the two points, and the third intersection with the elliptic curve, here labeled R, is mirrored at the x-axis, finally giving us the point $P \oplus Q$. Figure 2.2(b) shows what happens when we add a point P to itself:



(a) Addition of two points P and Q

(b) Addition of a point P with itself

(c) Point at infinity $\mathcal{O}$

Figure 2.2: Demonstration of the Group Law on the Elliptic Curve $E : y^2 = x^3 - x + 1$ Defined over $\mathbb{R}$

we draw the tangent line through point P and mirror the resulting intersection with E at the x-axis, resulting in point $2P$. This demonstrates why we have required E to be smooth (have a unique tangent at every point) — otherwise, we would have no way to add a point P to itself. Finally, Fig. 2.2(c) demonstrates what happens if we add a point to its inverse: here, $Q = -P$. We draw a line through both points and receive the neutral element of our group, the point at infinity O. This also shows why we mirror the point of intersection after drawing a line through two points: if we 'draw' a line through O and P, we intersect E at $Q = -P$. If we now mirror Q at the x-axis, we return to point P, which is exactly what we have required with $P \oplus O = P$.

Definition 3 *Let $E(\mathbb{F}_q)$ be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$ defined over a field $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) \in \{2, 3\}$. The j-invariant of E is defined as:*

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

Definition 4 *An isomorphism of elliptic curves $f : E \to E_0$ is a morphism that satisfies $f(0_E) = 0_{E_0}$, and whose inverse (over the algebraic closure) is also a morphism. It follows that an isomorphism is a bijection $E(\overline{\mathbb{F}}_q) \to E_0(\overline{\mathbb{F}}_q)$.*

Since **isomorphisms** are over $\mathbb{F}_q$, they are not necessarily maps from $E(\mathbb{F}_q)$ to $E_0(\mathbb{F}_q)$. There is an isomorphism $f : E \to E_0$ if and only if $j(E) = j(E_0)$[6].

2.2 Group Structure of Supersingular Curves

Let p be a prime, and let E be a supersingular curve defined over a finite field $\mathbb{F}_q$ with $q = p^m$ elements. Let t be the trace of the Frobenius endomorphism of $E/\mathbb{F}_q$. Then one of the following is true[5]:

- If m is odd and:

  - $t = 0$, or

  - $p = 2$ and $t^2 = 2q$, or

  - $p = 3$ and $t^2 = 3q$;

- If m is even and:

  - $t^2 = 4q$, or

  - $t^2 = q$, and $j(E) = 0$, and E is not isomorphic to $y^2 = x^3 \pm 1$, or

  - $t^2 = 0$, and $j(E) = 1728$, and E is not isomorphic to $y^2 = x^3 \pm x$.

  The group structure of $E(\mathbb{F}_q)$ is one of the following:

- If $t^2 = q$, $2q$, or $3q$, then $E(\mathbb{F}_q)$ is cyclic.
- If $t = 0$, then $E(\mathbb{F}_q)$ is either cyclic or isomorphic to $\mathbb{Z}/(q+1)\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
- If $t = \pm 2\sqrt{q}$, then $E(\mathbb{F}_q) \cong (\mathbb{Z}/(\sqrt{q} \pm 1)\mathbb{Z})^2$.

2.3 Isogenies

Let E_1 and E_2 be two elliptic curves over $\mathbb{F}_q$. An **isogeny** is a morphism $\phi : E_1 \to E_2$ such that $\phi(0_{E_1}) = 0_{E_2}$. One can show that isogenies are group homomorphisms, so they are "morphisms" both in the sense of algebraic geometry and group theory. Two elliptic curves are called **isogenous** if there is a non-constant isogeny between them[4].

The **degree** of an isogeny is essentially the degree of polynomials describing it . The degree of an isogeny is also, in general, the number of points in the kernel (an exception is inseparable isogenies such as the **Frobenius map** $\pi(x, y) = (x^p, y^p)$ on elliptic curves over $\mathbb{F}_p$).

A basic example of an isogeny is the **multiplication by** n **map** $[n]$ on an elliptic curve E for $n \in \mathbb{N}$, which we already defined by $[n]P = P + P + \ldots + P$ (n times). This maps 0 to itself, is a group homomorphism, and is described by rational functions coming from the group law. The kernel is precisely the set of points $E[n]$ defined earlier.

2.4 Isogeny Graph

One interesting thing we can do with isogenies is viewing them as edges in a graph. The nodes of the graph then take the form of the **isomorphism classes** of the elliptic curves the isogenies map between, in other words, every node can be labeled with a corresponding j-invariant. The resulting graph is then called an **isogeny graph**. The shape of an isogeny graph depends on two things: the field K that the elliptic curves are defined over and the degree ‘ of the isogenies between them. An isogeny graph with isogenies of degree l representing the edges is also called an **l-isogeny** graph. In general, an isogeny graph is not connected— instead, it consists of many small connected components, each consisting of isomorphism classes of isogenous elliptic curves. These components can be further divided: since supersingular elliptic curves can only be isogenous to other supersingular elliptic curves, it follows that no component in the isogeny graph can contain isomorphism classes of both ordinary and supersingular elliptic curves at the same time. Thus, we can divide the graph into ordinary and supersingular components — we obtain the **ordinary isogeny** graph and the **supersingular isogeny** graph.

CHAPTER 3

POST-QUANTAM KEY EXCHANGE: SIDH

In recent years, there has been a growing recognition of the need to revise cryptographic standards in anticipation of the potential emergence of general-purpose quantum computers. The concern stems from the knowledge that Shor's algorithm, a well-known quantum algorithm, could efficiently solve problems like integer factorization and the discrete logarithm problem on a quantum computer, thereby rendering cryptographic protocols such as RSA and ECDH vulnerable. Consequently, the cryptographic community is actively engaged in the quest for cryptographic primitives that would withstand quantum computing, ensuring they do not succumb to polynomial-time attacks on quantum computers.

The two participants, Alice and Bob, start from the same common curve E_0, and take a (secret) random walk to some curves E_A and E_B. After publishing their respective curves, Alice starts a new walk from E_B, while Bob starts from E_A. By repeating the "same" secret steps, they both eventually arrive on a shared secret curve E_S, only known to them. While the idea may seem simple, its realization is far from easy. Indeed, as opposed to the hash function case, we cannot be content with an arbitrary labeling of the graph edges. We must instead use the algebraic properties of the isogeny graphs to ensure that Alice and Bob's walks "commute"[5, 7].

3.1 Supersingular Isogeny Diffie-Hellman

The key idea of the Supersingular Isogeny Diffie-Hellman protocol (SIDH)[7, 5], is to let Alice and Bob take random walks in two distinct isogeny graphs on the same vertex set. In practice, we choose a large enough prime p, and two small primes ℓ_A and ℓ_B. The vertex set is going to consist of the supersingular j-invariants defined over $\mathbb{F}_{p^2}$, Alice's graph is going to be made of ℓ_A-isogenies, while Bob is going to use ℓ_B-isogenies. Figure **??** shows a toy example of such graphs, where $p = 97$, $\ell_A = 2$, and $\ell_B = 3$.

It is worth noting that a separable isogeny is uniquely defined by its kernel, and in this case, the degree $\deg \phi = \# \ker \phi$. More precisely, a walk of length e_A in the ℓ_A-isogeny graph corresponds to a kernel of size $\ell_A^{e_A}$, and this kernel is cyclic if and only if the walk does not backtrack.

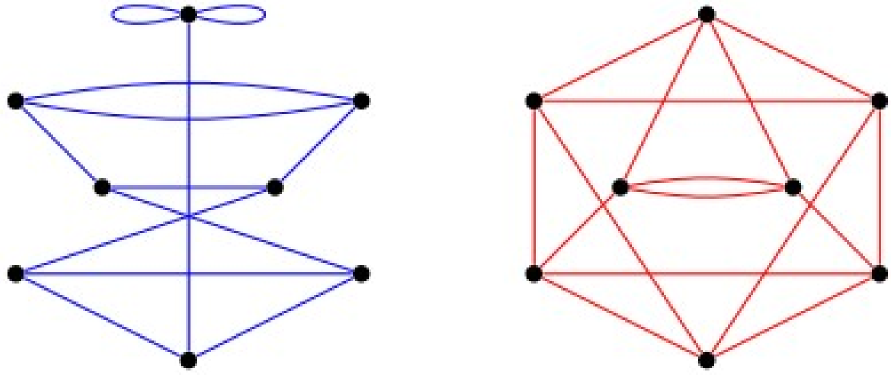


Figure 3.1: Supersingular isogeny graphs of degree 2 (left, blue) and 3 (right, red) on $\mathbb{F}_{97^2}$

Hence, Alice choosing a secret walk of length e_A is equivalent to her choosing a secret cyclic subgroup $\langle A \rangle \subset E[\ell_A^{e_A}]$. If we let Alice choose one such subgroup, and Bob choose similarly a secret $\langle B \rangle \subset E[\ell_B^{e_B}]$, then there is a well-defined subgroup $\langle A \rangle + \langle B \rangle = \langle A, B \rangle$, defining an isogeny to $E/\langle A, B \rangle$. Since we have taken care to choose $\ell_A \neq \ell_B$, the group $\langle A, B \rangle$ is cyclic of order $\ell_A^{e_A} \cdot \ell_B^{e_B}$.This is illustrated in Figure 3.2.

At this point, we would like to define a protocol where Alice and Bob choose random cyclic subgroups $\langle A \rangle$ and $\langle B \rangle$ in some large enough torsion groups and exchange enough information to both compute $E/\langle A, B \rangle$ (up to isomorphism) without revealing their respective secrets. We are faced with two difficulties[7], though:

- The points of $\langle A \rangle$ (or $\langle B \rangle$) may not be rational. Indeed, in general, they may be defined over a field extension of degree as large as $\ell_A^{e_A} \cdot \ell_B^{e_B}$, thus requiring an exponential amount of information to be explicitly represented.

- The diagram in Figure 3.2 shows no way by which Alice and Bob could compute $E/\langle A, B\rangle$ without revealing their secrets to each other.

$$\ker\alpha = \langle A\rangle \subset E[\ell_A^{e_A}]$$

$$\ker\beta = \langle B\rangle \subset E[\ell_B^{e_B}]$$

$$\ker\alpha' = \langle\beta(A)\rangle$$

$$\ker\beta' = \langle\alpha(B)\rangle$$

$$\begin{tikzcd}
E \arrow[r, "\alpha"] \arrow[d, "\beta"'] & E/\langle A\rangle \arrow[d, "\beta'"] \\
E/\langle B\rangle \arrow[r, "\alpha'"'] & E/\langle A, B\rangle
\end{tikzcd}$$

Figure 3.2: Commutative isogeny diagram constructed from Alice's and Bob's secrets. Quantities known to Alice are drawn in blue, those known to Bob are drawn in red

Of all the cases, the only one we are concerned with is $q = p^2$, and $E(\mathbb{F}_q) \cong (\mathbb{Z}/(p\pm1)\mathbb{Z})^2$. Since we have full control over p, we can choose it so that $E(\mathbb{F}_q)$ contains two large subgroups $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$ of coprime order. Hence, once $\ell_A^{e_A}$ and $\ell_B^{e_B}$ are fixed, we look for a prime of the form $p = \ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f \mp 1$, where f is a small cofactor. In practice, such primes are abundant, and we can easily take $f = 1$. This solves the first problem: $E(\mathbb{F}_q)$ now contains $\ell_A^{e_A-1}(\ell_A + 1)$ cyclic subgroups of order $\ell_A^{e_A}$, each defining a distinct isogeny; hence, a single point $A \in E(\mathbb{F}_q)$ is enough to represent an isogeny walk of length e_A.
The second problem is solved by a very peculiar trick, which sets SIDH apart from other isogeny-based protocols. The idea is to let Alice and Bob publish some additional information to help each other compute the shared secret. Let us summarize what quantities are known to Alice and Bob.
To set up the cryptosystem, they have publicly agreed on a prime p and a supersingular curve E such that:

$$E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_B^{e_B}\mathbb{Z})^2 \oplus (\mathbb{Z}/f\mathbb{Z})^2.$$

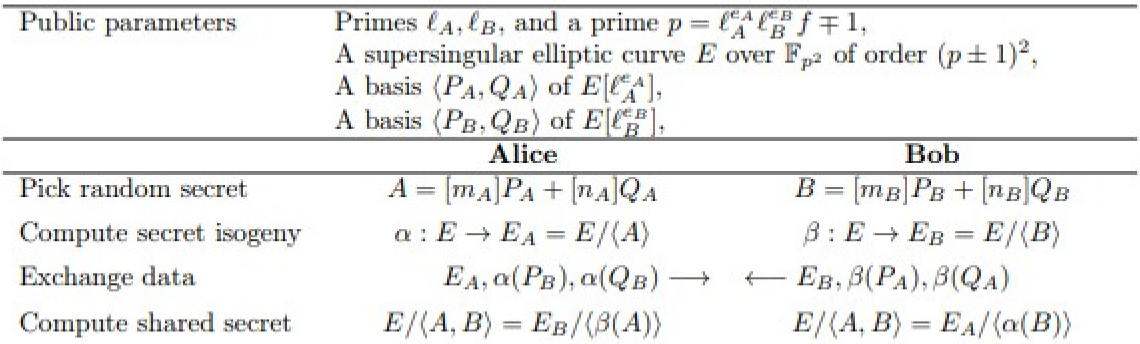
It will be convenient to also fix public bases of their respective torsion groups:

$$E[\ell_A^{e_A}] = \langle P_A, Q_A\rangle, E[\ell_B^{e_B}] = \langle P_B, Q_B\rangle$$

. To start the protocol, they choose random secret subgroups:

$$\langle A\rangle = \langle [m_A]P_A + [n_A]Q_A\rangle \subset E[\ell_A^{e_A}],$$

$$\langle B\rangle = \langle [m_B]P_B + h[n_B]Q_B\rangle \subset E[\ell_B^{e_B}],$$



Public parameters	Primes ℓ_A, ℓ_B, and a prime $p = \ell_A^{e_A} \ell_B^{e_B} f \mp 1$, A supersingular elliptic curve E over $\mathbb{F}_{p^2}$ of order $(p \pm 1)^2$, A basis $\langle P_A, Q_A \rangle$ of $E[\ell_A^{e_A}]$, A basis $\langle P_B, Q_B \rangle$ of $E[\ell_B^{e_B}]$,	
	Alice	**Bob**
Pick random secret	$A = [m_A]P_A + [n_A]Q_A$	$B = [m_B]P_B + [n_B]Q_B$
Compute secret isogeny	$\alpha : E \to E_A = E/\langle A \rangle$	$\beta : E \to E_B = E/\langle B \rangle$
Exchange data	$E_A, \alpha(P_B), \alpha(Q_B) \longrightarrow$	$\longleftarrow E_B, \beta(P_A), \beta(Q_A)$
Compute shared secret	$E/\langle A, B \rangle = E_B/\langle \beta(A) \rangle$	$E/\langle A, B \rangle = E_A/\langle \alpha(B) \rangle$

Figure 3.3: Supersingular Isogeny Diffie-Hellman key exchange protocol.

They choose random secret subgroups of respective orders $\ell_A^{e_A}$ and $\ell_B^{e_B}$ and compute the secret isogenies:

$$\alpha : E \to E/\langle A \rangle,$$

$$\beta : E \to E/ < B_i..$$

They respectively publish $E_A = E/\langle A \rangle$ and $E_B = E/\langle B \rangle$.

Now, to compute the shared secret $E/ < \langle A, B \rangle$, Alice needs to compute the isogeny $\alpha^| : E/\langle B \rangle \to E/\langle A, B \rangle$, which kernel is generated by $\beta(A)$. We see that the kernel of $\alpha^|$ depends on both secrets, thus Alice cannot compute it without Bob's assistance. The trick here is for Bob to publish the values $\beta(P_A)$ and $\beta(Q_A)$: they do not require the knowledge of Alice's secret, and it is conjectured that they do not give any advantage to an attacker in computing $E/\langle A, B \rangle$.

From Bob's published values, Alice can compute $\beta(A)$ as $[m_A]\beta(P_A) + [n_A]\beta(Q_A)$ and complete the protocol. Bob performs the analogous computation, with the help of Alice. The protocol is summarized in Figure 3.3, and schematized in Figure 3.4.

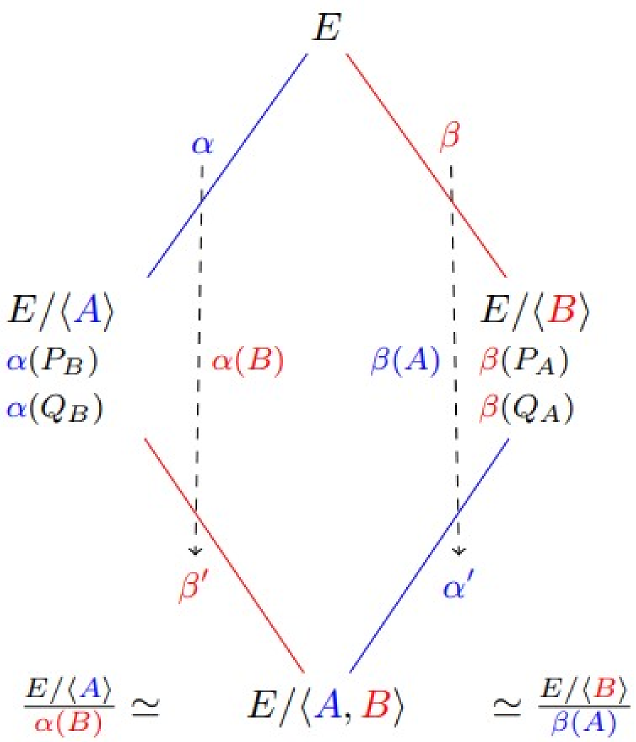


Figure 3.4: Schematics of SIDH key exchange. Quantities only known to Alice are drawn in blue, quantities only known to Bob in red.

It is clear that the key space of SIDH depends on the size of the subgroups $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$, hence we must take $\ell_A^{e_A} \approx \ell_B^{e_B}$ so as to make attacks equally hard against Alice or Bob's public data. However, this puts serious constraints on the isogeny walks performed in SIDH. We have seen that the size of the supersingular isogeny graph is $O(p)$, whereas the size of Alice's (or Bob's) public key space is only $O(\sqrt{p})$. In other words, Alice and Bob take random walks much shorter than the diameter of the graph. At the moment, it is not clear how this affects the security of the protocol.

CHAPTER 4

CONCLUSION

Supersingular isogeny-based cryptography stands out as a promising candidate for the post-quantum cryptographic landscape. Its security relies on mathematical problems that have proven resilient to attacks by quantum computers, making it a valuable contender for protecting sensitive information in a quantum-powered world. Moreover, it offers the advantage of smaller key sizes and message exchanges compared to some other post-quantum proposals.

One of the most noteworthy applications of this cryptographic approach is the SIDH key agreement protocol, which remains secure against classical and quantum attacks due to its fully exponential nature. The best-known quantum attack on SIDH, the claw problem solution, is known to have optimal complexity in a black-box setting. However, it is essential to emphasize the need for in-depth research by experts in quantum algorithms to thoroughly evaluate the quantum hardness of underlying problems, such as the isogeny problem.

Furthermore, the SIDH protocol reveals a wealth of information that has yet to be fully explored by existing claw and graph path finding algorithms. This highlights the necessity for continued investigation and development in this field. We can only hope that this paper serves as both a starting point and a catalyst for the much-needed research and exploration of the potential of Supersingular isogeny-based cryptography in the context of post-quantum security. As we move forward in the era of quantum computing, the importance of robust and reliable cryptographic solutions cannot be overstated, and Supersingular isogeny-based crypto represents a significant step in the right direction

REFERENCES

[1] Gorjan Alagic, Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al., *Status report on the first round of the nist post-quantum cryptography standardization process*, (2019).

[2] Denis X Charles, Kristin E Lauter, and Eyal Z Goren, *Cryptographic hash functions from expander graphs*, Journal of CRYPTOLOGY **22** (2009), no. 1, 93–113.

[3] Jean-Marc Couveignes, *Hard homogeneous spaces*, Cryptology ePrint Archive, Paper 2006/291, 2006, `https://eprint.iacr.org/2006/291`.

[4] Jean-Marc Couveignes, *Hard homogeneous spaces*, Cryptology ePrint Archive (2006).

[5] Luca De Feo, *Mathematics of isogeny based cryptography*, arXiv preprint arXiv:1711.04062 (2017).

[6] Steven D Galbraith and Frederik Vercauteren, *Computational problems in supersingular elliptic curve isogenies*, Quantum Information Processing **17** (2018), 1–22.

[7] David Jao and Luca De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4, Springer, 2011, pp. 19–34.

[8] Alexander Rostovtsev and Anton Stolbunov, *Public-key cryptosystem based on isogenies*, Cryptology ePrint Archive, Paper 2006/145, 2006, `https://eprint.iacr.org/2006/145`.

[9] Peter W Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM review **41** (1999), no. 2, 303–332.

[10] Philipp STRATIL, Shingo HASEGAWA, and Hiroki SHIZUYA, *Supersingular isogeny-based cryptography: A survey*, Interdisciplinary Information Sciences **27** (2021), no. 1, 1–23.