Mathematics Internal Assessment AA HL

Sepehr Marjovi

Introduction:

In today's digital world, the need for secure communication is more significant than anything else. Think about the last time you transferred money from your bank account or sent a message on a messaging app, everything relies on cryptography to keep your data safe. However, this security is at risk with quantum computing advancements. When I first started learning about classic cryptography such as RSA and Elliptic Curve Cryptography (ECC) in my computer science classes, I was fascinated by how it works and learnt that they provide security based on the difficulty of certain mathematical problems. However, with the advancement of quantum computers and advanced algorithms such as Shor's algorithm (Shor,1994), those problems can be easily solved which lead to a threat towards classic cryptographic systems. Therefore, I have started to look into post-quantum cryptographic systems which are cryptographic systems designed to be secure against quantum attacks. Among the various post-quantum cryptographic systems, isogeny-based cryptography, particularly Supersingular Isogeny Diffie-Hellman (SIDH) protocol grabbed my attention due to its usage of advanced mathematics.

Through this exploration, I aim to explain how isogeny-based cryptography, specifically Supersingular Isogeny Diffie-Hellman (SIDH) protocol, could help with data protection, especially in critical areas like banking. I found this topic really interesting, mainly due to its real-world significance and the complexity of the mathematics concepts behind it. In this IA, I will explore the mathematics concepts behind isogeny-based cryptography, focusing on elliptic curves, isogenies, and apply them to a real-life banking scenario where secure communication is crucial.

1 Elliptic Curves and Cryptography

1.1 Basics of Elliptic Curves

An elliptic curve is defined by an equation of :

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

where a and b are real numbers, and the curve must satisfy the equation:

$$4a^3 + 27b^2 \neq 0$$

which ensures that the curve is smooth and non-singular, meaning that the curve has no sharp points (cusps) or interactions with itself. I was wondering the reason behind the significance of smoothness. Later I learned that smoothness allows the points to form what mathematicians call a group, which is crucial for cryptographic operations. A group is a set of objects with an operation that follows a certain rule.

1.2 The Group Structure of Elliptic Curves

One of the properties of elliptic curves is that they form an algebraic group under a specific operation which is called point addition. This means that we can add to points on the curve to get a third point which also lies on the curve. Given two points P and Q on the curve, their sum will be a third point, called R and this operation satisfies the properties of a mathematical group:

- Closure: Adding two points P and Q on the curve results in another point R on the curve.
- Associativity: $(P + Q) + R = P + (Q + R)$
- Identity Element: There exists an identity element O (point of infinity) such that $P + O = P$
- Inverse Element: For every point P, there exists an inverse $-P$ such that $P + (-P) = O$

Point Addition (P ≠ Q)

Given two distinct points P (x_1, y_1) and Q (x_2, y_2) on an elliptic curve, the result is a third point R (x_3, y_3).

The way that the points are added are defined as :

- Draw a line: Draw a straight line through the points P and Q
- Find the Intersection: The line will intersect the elliptic curve at a third point, R´.
- Reflect over the x-axis: Reflect R´ over the x-axis to get R = P + Q.

Mathematically, if:

$$P\,(x_1, y_1) \neq Q\,(x_2, y_2)$$

The slope of the line between P and Q is :

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Then, the sum $R(x_3, y_3)$ is calculated as :

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m\,(\,x_1 - x_3\,) - y_1$$

Example of Point Addition

Let P = (2,2) and Q = (1,-1) on the curve $y^2 = x^3 - 4x + 4$

1. **Verify that P and Q lie on the curve.**

   - For P

   $$y^2 = (2)^2 = 4$$

   $$x^3 - 4x + 4 = (2)^3 - 4(2) + 4 = 8 - 8 + 4 = 4$$

   Since 4 = 4, P lies on the curve.

   - For Q

   $$y^2 = (-1)^2 = 1$$

   $$x^3 - 4x + 4 = (1)^3 - 4(1) + 4 = 1 - 4 + 4 = 1$$

   Since 1 = 1, Q also lies on the curve.

2. **Calculate the slope**

   Since P $\neq Q$, point addition formula must be used for the slope.

   $$\text{m} = \frac{y_2 - y_1}{x_2 - x_1}$$

   Substitute the values ($x_1 = 2,\ x_2 = 1,\ y_1 = 2,\ y_2 = -1$)

   $$\text{m} = \frac{y_2 - y_1}{x_2 - x_1} = \frac{-1-2}{1-2} = \frac{-3}{-1} = 3$$

3. **Compute x_3 and y_3**

   $$x_3 = m^2 - x_1 - x_2 = (3)^2 - 2 - 1 = 9 - 2 - 1 = 6$$

$$y_3 = m(x_1 - x_3) - y_1 = (3)(2 - 6) - (2) = 3(-4) - 2 = -12 - 2 = -14$$

4. **Resulting Point and Verification**

The sum of the P + Q is:

$$R(x_3, y_3) = P + Q = (6, -14)$$

Verify that the point lies on the curve:

$$y^2 = (-14)^2 = 196$$

$$x^3 - 4x + 4 = (6)^3 - 4(6) + 4 = 216 - 4(6) + 4 = 216 - 24 + 4 = 196$$

Since 196 = 196, R lies on the curve and is the sum of points P and Q.

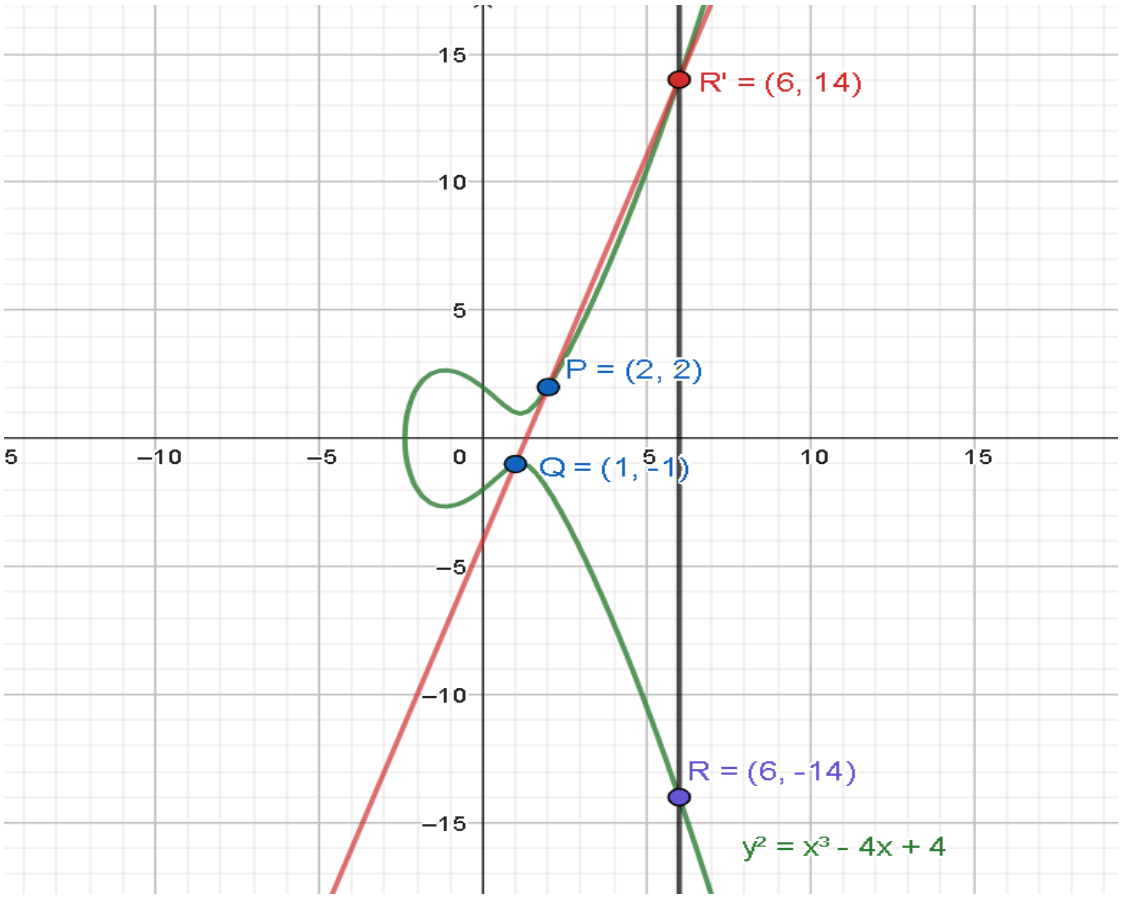

Figure 1- Graphical Illustration of Point Addition On the Elliptic Curve

$$y^2 = x^3 - 4x + 4$$

Showing Points P (2,2) and Q (1,-1) and their sum R (6,-14)

[I have drawn the graph using the website https://www.geogebra.org/graphing?lang=en]

Point Doubling(P = Q)

Given two equal points P (x_1, y_1) and Q (x_2, y_2) on an elliptic curve, the result is a third point R(x_3, y_3) = 2P.

The way that the points are added are defined as :

- Draw the tangent line: Draw the tangent line to the elliptic curve at point P.
- Find the Intersection: The tangent line will intersect the elliptic curve at a second point, R´.
- Reflect over the x-axis: Reflect R´ over the x-axis to get R = 2P.

Mathematically if,

$$\text{P}\,(x_1, y_1) = Q\,(x_2, y_2)$$

The slope of the tangent at point P is :

$$\text{m} = \frac{3x_1^2 + a}{2y_1}$$

Then, the sum $R\,(x_3, y_3)$ is calculated as :

$$x_3 = m^2 - 2x_1$$

$$y_3 = m(x_1 - x_3) - y_1$$

Example of Point Doubling

Let P = (1,1) on the curve $y^2 = x^3 - 3x + 3$

1. **Verify that P lies on the curve**

$$y^2 = (1)^2 = 1$$

$$x^3 - x + 1 = (1)^3 - 1 + 1 = 1$$

Since 1 = 1, P lies on the curve.

2. **Calculate the slope**

Since P = Q, the Point Doubling formula must be used for the slope of the tangent.

$$\text{m} = \frac{3x_1^2 + a}{2y_1}$$

Substitute the values ($x_1 = 1, y_1 = 1$, a = -3)

$$\text{m} = \frac{3x_1^2 + a}{2y_1} = \frac{3(1)^2 + (-3)}{2(1)} = \frac{3-3}{2} = \frac{}{2}$$

3. **Compute x_3 and y_3**

$$x_3 = m^2 - 2x_1 = (0)^2 - 2(1) = -2$$

$$y_3 = m(x_1 - x_3) - y_1 = (0)(1 - (-2)) - 1 = (0) - 1 = 0 - 1 = -1$$

4. Resulting Point and Verification

The result of doubling P is:

$$R(x_3, y_3) = 2P = (-2, -1)$$

Verify that the point lies on the curve:

$$y^2 = (-1)^2 = 1$$

$$x^3 - 3x + 3 = (-2)^3 - 3(-2) + 3 = -8 + 3(2) + 3 = -8 + 6 + 3 = 1$$

Since $1 = 1$, R lies on the curve and is equal to 2P.

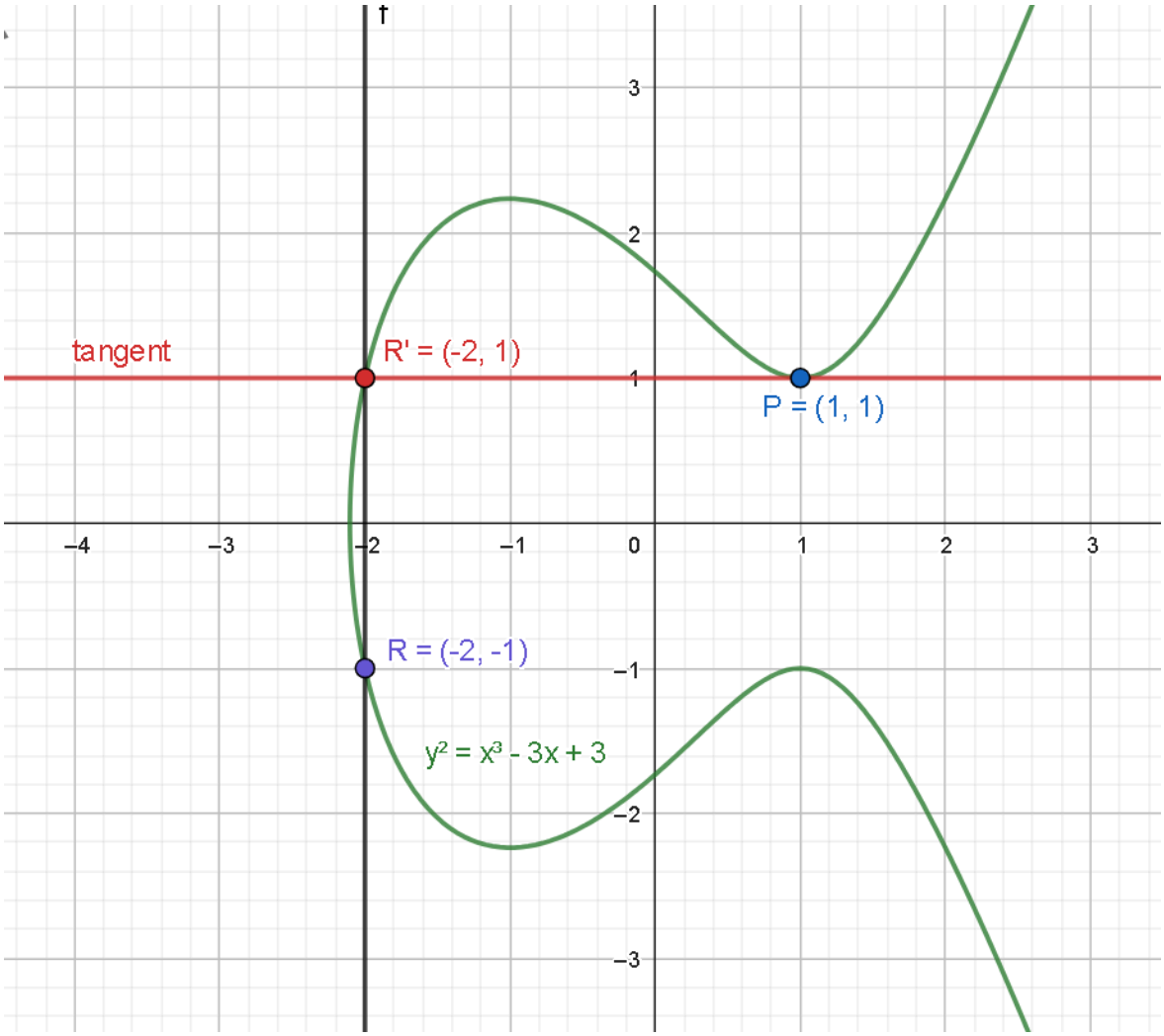

Figure 2- Graphical Illustration of Point Doubling On the Elliptic Curve

$$y^2 = x^3 - 3x + 3$$

Showing Point P (1,1) and the resulting point R (-2,-1) = 2P.

[I have drawn the graph using the website https://www.geogebra.org/graphing?lang=en]

1.3 Supersingular Elliptic Curves

Supersingular elliptic curves are special types of elliptic curves over finite fields, which satisfy special

mathematical properties which are essential for cryptography.

Key characteristics:

- **Finite Fields:** Supersingular curves are defined over finite fields F_p ,where p is a prime number.
- **Rich isogeny structure:** Supersingular curves are connected through many isogenies, forming a complex network, which is hard to navigate without a secret information .
- **Security advantage:** The difficulty of finding isogenies between supersingular elliptic curves highlights their importance for security in cryptography.

In simpler terms, we could assume that elliptic curves are cities and isogenies are roads between the cities. In the case of supersingular elliptic curves, there are many roads connecting each city to other cities, creating a complex network, which means without a map (secret information), it is difficult to find a specific road from one city to another.

1.4 Elliptic Curves in Cryptography

Further, after gaining knowledge about elliptic curves and how points on an elliptic curve could be added, I wanted to know how this applies to cryptography, where I learnt that Elliptic Curve Cryptography (ECC) relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which relies on the difficulty of finding an integer k, given an elliptic curve E over finite field, a point P (the base point) and another point (Q),

where Q = kP. While it is easy to compute Q given k and P. It is extremely difficult to find k if only Q and P are given, especially when k is a large number.

1.5 Example of Secure Communication using Elliptic Curves

To explore how elliptic curves can be used to secure communication between two parties, we are going to use two fictional parties, Alice and Bob often used discussing cryptography theories. This example shows the fundamental principles of Elliptic Curve Cryptography (ECC) in a practical scenario.

1. Public Information
    - Both Alice and Bob agree on a publicly known elliptic curve E over a finite field and a base point P on that curve.
    - This information is accessible to everyone, including potential attackers.
2. Private Keys Selection
    - Alice: Chooses a secret private number k_A, which she keeps confidential.
    - Bob: Chooses a secret private number k_B, which he also keeps confidential.
3. Generating Public Points:
    - Alice: Calculates her public point $Q_A = k_A$P by multiplying the base point P by her private number k_A.
    - Bob: Calculates his public point $Q_B = k_B$P using the same method.
4. Exchanging Public Points:
    - Alice and Bob exchange their public points Q_A and Q_B over the communication channel.
    - Even if an attacker gets these public points, they cannot easily determine the private numbers due to the difficulty of EDCLP.
5. Computing the Shared Secret:

- Alice: Uses Bob's public point to compute S = $k_A Q_B$
- Bob: Uses Alice's public point to compute S = $k_B Q_A$

6. Resulting in the same Shared Secret
    - Both computations result in the same point S on the elliptic curve because:

      S = $k_A Q_B = k_A(k_B P) = k_B Q_A = k_B(k_A \mathrm{P})$

This results in a shared Secret point S on the elliptic curve which can be used as an encryption key and for secure communication.

2. Isogenies between elliptic curves

2.1 Definition of Isogenies

An isogeny is a function between two elliptic curves that preserves the group structure. It is a way to map one elliptic curve onto another while maintaining the group structure and the way points are added together.

This property is called a homomorphism as homomorphisms are maps of one set into another that preserve the relations of the first set in the second set.

Mathematically, if E_1 and E_2 are elliptic curves, an isogeny between them $\phi : E_1 \rightarrow E_2$ satisfies:

$$\phi(P+Q) = \phi(P) + \phi(Q)$$

For all points P,Q on E_1.

Key properties of Isogenies

- Kernel of an isogeny (ker(ϕ))
    - The set of points on the elliptic curve E_1 that map to the identity element on E_2
- Degree of an isogeny (deg(ϕ))
    - A measure of the isogeny's complexity equal to the size of it's kernel, if deg(ϕ) = n, then approximately n points on E_1 map to a single point on E_2
- Dual Isogeny ($\widehat{\phi}$)
    - For every isogeny $\phi : E_1 \rightarrow E_2$, there exists a dual isogeny $\widehat{\phi}: E_2 \rightarrow E_1$

2.2 Isogenies in Cryptography

Isogenies between elliptic curves are used in cryptography to create hard mathematical problems that secure the cryptographic systems.

- Given two supersingular elliptic curves E_1 and E_2, finding an isogeny $\phi : E_1 \rightarrow E_2$ is computationally difficult, this difficulty forms the basis of some cryptographic protocols such as Supersingular Isogeny Diffie-Hellman (SIDH) protocol.
- Quantum Resistance: Unlike some problems behind security of cryptographic systems such as integer factorization or discrete logarithms, which can be solved using advanced quantum algorithms, no quantum algorithms is currently known for solving the isogeny problem, which makes it a good candidate for post-quantum security.

3. The Super-Singular Isogeny Diffie-Hellman (SIDH) Protocol

3.1 What is SIDH?

SIDH is a protocol for secure key exchange which is designed to be resistant to quantum computer attacks. It is really significant and useful for secure communication as it relies on problems which are hard for both classical and quantum computers to solve and offers security with smaller keys, which is useful for devices with limited resources.

3.2 How does SIDH work?

Setup Parameters

- Finite Field F_P : A prime field where all the calculations are performed.
- Starting elliptic curve E_0 : A supersingular elliptic curve over F_P
- Points (P_A, Q_A) and (P_B, Q_B) : Known points on E_0

Key Exchange steps:

1. Private Key Selection:
    - Alice:
        - Chooses a random integer m_A as her private key.
        - Computes her secret subgroup $S_A = (P_A + m_A Q_A)$
    - Bob:
        - Chooses a random integer m_B as his private key.
        - Computes his secret subgroup $S_B = (P_B + m_B Q_B)$

2. Compute Isogenies:
    - Alice
        - Computes the isogeny ϕ_A with the kernel S_A
        - Finds the new curve $E_A = \phi_A(E_0)$
        - Computes images $\phi_A(P_B)$ and $\phi_A(Q_B)$
    - Bob
        - Computes the isogeny ϕ_B with the kernel S_B
        - Finds the new curve $E_B = \phi_B(E_0)$
        - Computes images $\phi_B(P_A)$ and $\phi_B(Q_A)$
3. Exchange
    - Alice sends $E_A, \phi_A(P_B), \phi_A(Q_B)$ to Bob
    - Bob sends $E_B, \phi_B(P_A), \phi_B(Q_A)$ to Alice
4. Compute Shared Secret
    - Alice: Uses m_A, $E_B, \phi_B(P_A)$, and $\phi_B(Q_A)$ to compute the shared Curve E_{AB}
    - Bob: Uses m_B, $E_A, \phi_A(P_B)$, and $\phi_A(Q_B)$ to compute the shared Curve E_{AB}
5. Both Alice and Bob now share the same elliptic curve E_{AB} which is their shared secret.

4. Real-World Experiment: Stimulating SIDH in a Banking Scenario

In the banking industry, secure communication is really crucial for various reasons such as transaction security and customer's data protection and quantum-resistant cryptographic protocols such as SIDH can play a crucial role in post-quantum security. To demonstrate the practicality and importance of SIDH, I have conducted an experiment of a secure key exchange between two parties in a banking system. In this experiment

Bank A (Alice) and Bank B (Bob) need to establish secure communication over an insecure network to exchange sensitive financial information.

4.1 Experimental Setup

Parameters:

- Prime Field F_{17} . (I have chosen a small prime number for computational simplicity but much larger primes are used in real implementations)
- Starting Curve E_0: $y^2 = x^3 + x + 1 \; over \; F_{17}$
- Public Points:
    - Alice's Points (P_A,Q_A)
        - $Assume \; P_A(0,1)$ and $Q_A(4,1)$
        - Verify the points are on the curve $y^2 = x^3 + x + 1 \; over \; F_{17}$

■ For $P_A(0,1)$

y^2 mod 17 = $(1)^2$ mod 17 = 1 modulo 17 = 1

$x^3 + x + 1$ mod 17 = $((0)^3 + 0 + 1) \; mod \; 17 = 1 \; modulo \; 17 = 1$

- Since 1=1, $P_A(0,1)$ is a point on the curve $y^2 = x^3 + x + 1 \; over \; F_{17}$

- For $Q_A(4,1)$

  y^2 mod 17 = $(1)^2$ mod 17 = 1 modulo 17 = 1

  $x^3 + x + 1$ mod 17 = $((4)^3 + 4 + 1) \; mod \; 17 = 69 \; modulo \; 17 = 1$

  - Since 1=1, $Q_A(4,1)$ is a point on the curve $y^2 = x^3 + x + 1 \; over \; F_{17}$

- Bob's Points (P_B,Q_B)

  - $Assume \; P_B(9,5)$ and $Q_B(10,12)$

  - Verify the points are on the curve $y^2 = x^3 + x + 1 \; over \; F_{17}$

- For $P_B(9,5)$

  y^2 mod 17 = $(5)^2$ mod 17 = 25 modulo 17 = 8

  $x^3 + x + 1$ mod 17 = $((9)^3 + 9 + 1) \; mod \; 17 = 739 \; modulo \; 17 = 8$

  - Since 8=8, $P_B(9,5)$ is a point on the curve $y^2 = x^3 + x + 1 \; over \; F_{17}$

- For $Q_B(10,12)$

  y^2 mod 17 = $(12)^2$ mod 17 = 144 modulo 17 = 8

  $x^3 + x + 1$ mod 17 = $((10)^3 + 10 + 1) \; mod \; 17 = 1011 \; modulo \; 17 = 8$

  - Since 8 = 8, $Q_B(10,12)$ is a point on the curve $y^2 = x^3 + x + 1 \; over \; F_{17}$

4.2 Simulation Steps

1. Private Key Selection
    - Alice: Chooses $m_A = 3$ (chosen randomly)
    - Bob: Chooses $m_B = 2$ (chosen randomly)
2. Compute Secret Subgroups:
    - **Alice:** $S_A = \langle P_A + m_A Q_A \rangle = \langle (0,1) + 3 \times (4,1) \rangle$
        - Point Multiplication and Addition:
            - $\langle (0,1) + 3 \times (4,1) \rangle = \langle (0,1) + (4,1) + 2 \times (4,1) \rangle$
            - Calculating $2 \times (4,1)$ using point doubling formulas:

$$m = \frac{3x_1^2 + a}{2y_1} \; modulo \; 17 = \frac{3(4)^2 + 1}{2(1)} \; modulo \; 17 = \frac{3(16)+1}{2(1)} \; modulo \; 17 = \frac{49}{2} \; modulo \; 17 = 16$$

$$x_3 = m^2 - 2x_1 \; modulo \; 17 = ((16)^2 - 2(4)) \; modulo \; 17 = (256 - 8) \; modulo \; 17 = 248 \; modulo \; 17 = 10$$

$$y_3 = m(x_1 - x_3) - y_1 \text{ modulo } 17 = (((16)(4 - 10)) - 1) \; modulo \; 17 = (-97) \; modulo \; 17 = 5$$

- The result of $(2 \times (4,1))$ is the point (10,5)

- Calculating $\langle (4,1) + (10,5) \rangle$ using point addition formulas:

$$m = \frac{y_2 - y_1}{x_2 - x_1} \; modulo \; 17 = \left(\frac{5-1}{10-4}\right) modulo \; 17 = \left(\frac{4}{6}\right) modulo \; 17 = \left(\frac{2}{3}\right) modulo \; 17 = 12$$

$$x_3 = (m^2 - x_1 - x_2) \; modulo \; 17 = (12^2 - 4 - 10) \; modulo \; 17 = (144 - 4 - 10) \; modulo \; 17 = 130 \text{ modulo } 17 = 11$$

$$y_3 = m(x_1 - x_3) - y_1 \; modulo \; 17 = (12(4 - 11) - 1) \; modulo \; 17 = (12(-7) - 1) \; modulo \; 17 = (-85) \; modulo \; 17$$

$= 0$

- The result of $\langle (4,1) + (10,5) \rangle$ is the point (11,0)

  - Calculating $\langle (0,1) + (11,0) \rangle$ using point addition formulas:

m $= \frac{y_2 - y_1}{x_2 - x_1} \; modulo \; 17 = (\frac{0-1}{11-0}) \; modulo \; 17 = (\frac{-1}{11}) \; modulo \; 17 = 3$

$x_3 = (m^2 - x_1 - x_2) \; modulo \; 17 = (3^2 - 0 - 11) \; modulo \; 17 = (9 - 11) \; modulo \; 17 = (-2)$ modulo 17 = 15

$y_3 = m(x_1 - x_3) - y_1 \; modulo \; 17 = (3(0 - 15) - 1) \; modulo \; 17 = (3(-15) - 1) \; modulo \; 17 = (-46) \; modulo \; 17 =$ 5

- The result of $\langle (0,1) + (11,0) \rangle$is the point (15,5)

  - **As a result,** $\langle (0,1) + 3 \times (4,1) \rangle = S_A$ **(15,5)**

- **Bob:** $S_B = \langle P_B + m_B Q_B \rangle = \langle (9,5) + 2 \times (10,12) \rangle$

  - Point Addition and Doubling:

    - Calculating $2 \times (10,12)$ using point doubling formulas:

m $= \frac{3x_1^2 + a}{2y_1} \; modulo \; 17 = \frac{3(10)^2 + 1}{2(12)} \; modulo \; 17 = \frac{3(100) + 1}{2(12)} \; modulo \; 17 = \frac{301}{24} \; modulo \; 17 = 9$

$x_3 = m^2 - 2x_1 \; modulo \; 17 = ((9)^2 - 2(10)) \; modulo \; 17 = (81 - 20) \; modulo \; 17 = 61 \; modulo \; 17 = 10$

$y_3 = m(x_1 - x_3) - y_1$ modulo 17 = (((9)(10 $- 10)) - 12) \; modulo \; 17 = ((9)(0) - 12) \; modulo \; 17 = (-12) \; modulo \; 17 = 5$

- The result of $(2 \times (10,12))$ is the point (10,5)

  - Calculating $\langle (9,5) + (10,5) \rangle$ using point addition formulas:

m $= \frac{y_2 - y_1}{x_2 - x_1} \; modulo \; 17 = (\frac{5-5}{10-9}) \; modulo \; 17 = (\frac{0}{1}) \; modulo \; 17 = (0) \; modulo \; 17 = 0$

$x_3 = (m^2 - x_1 - x_2) \; modulo \; 17 = (0^2 - 9 - 10) \; modulo \; 17 = (-19) \; modulo \; 17 = 15$

$y_3 = m(x_1 - x_3) - y_1 \, modulo \, 17 = (0(9 - 15) - 5) \, modulo \, 17 = (0(-6) - 5) modulo \, 17 = (-5) \, modulo \, 17 = 12$

- The result of $\langle (9,5) + (10,5) \rangle$ is the point (15,12)

- **As a result,** $\langle (9,5) + 2 \times (10,12) \rangle = S_B$ **(15,12)**

3. Compute Isogenies and Public Data
    - Alice
        - Using the kernel S_A (15,5) Computes ϕ_A and $E_A = \phi_A(E_0)$
        - Calculates images $\phi_A(P_B)$ and $\phi_A(Q_B)$
    - Bob
        - Using the kernel S_B (15,12), Computes ϕ_B and $E_B = \phi_B(E_0)$
        - Calculates images $\phi_B(P_A)$ and $\phi_B(Q_A)$
4. Exchange Public Data
    - Alice sends $E_A, \phi_A(P_B), \phi_A(Q_B)$ to Bob
    - Bob sends $E_B, \phi_B(P_A), \phi_B(Q_A)$ to Alice
5. Compute Shared Secret
    - Alice : Uses Bob's data to compute E_{AB}
    - Bob : Uses Alice's data to compute E_{AB}

4.3 Results and Analysis

Verification

- Both Alice and Bob arrive at the same shared curve E_{AB}
- The shared curve serves as a secure key for encrypting communication.

Security

- An attacker intercepting the exchanged data would face the problem of computing the isogeny without the private keys m_A and m_B.

5. Reflection and Evaluation

I have faced many challenges in this research, one of which was the complexity of constructing the isogenies which was not in the scope of this exploration and the other one was the page limit which did not let me to manually do the modular arithmetic and I was forced to use the online calculator https://planetcalc.com/8326/ for this regard, however, I have gained valuable knowledge about SIDH and its advantages and limitations.

5.1 Advantages of SIDH

- Quantum resistance: SIDH is designed to be secure against attacks from quantum computers, which is crucial in post-quantum security systems.
- Compact key sizes: Compared to other post-quantum cryptographic methods, SIDH uses relatively small key sizes, which is useful for devices with limited storage.

5.2 Limitations of SIDH

- Computational Complexity: Isogeny calculations are more computationally intensive than operations in traditional ECC, which could impact the performance due to possible errors.
- Specialized Implementation: Requires correct and careful selection of parameters and curves, which can impact the implementation

6.Conclusion

Through this assessment I have delved into complex mathematics behind elliptic curves and isogenies

and explored Supersingular Isogeny Diffie-Hellman (SIDH) protocol. By simulating a real-world application in a banking environment, I demonstrated how SIDH could be a solution to the threat of post-quantum security attacks. While SIDH has some limitations, such as computational difficulties, its advantages in providing quantum resistant security with compact key sizes makes it a viable solution for the post-quantum cryptography security and this exploration highlights the importance of mathematics in this advanced technology.

Bibliography:

(I have to get all of them to MyBib and then add them here, and add them as in-text citation)