Supersingular Elliptic Curve Isogenies

Abhay Sharma

2023/09/24

Table of Contents

Introduction

- In the context of elliptic curve cryptography and number theory, supersingular elliptic curves play a crucial role in various cryptographic protocols, particularly in the construction of isogenies-based cryptography
- Today, we'll delve into a fascinating area of cryptography that holds promise in a post-quantum world.

Understanding Elliptic Curves

- 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 $a, b \in \mathbb{F}_q$.
- E has to be smooth (non-singular), i.e., every point on the curve needs to have a unique tangent
- They have a unique geometric structure and are widely used in modern cryptography for their mathematical properties.

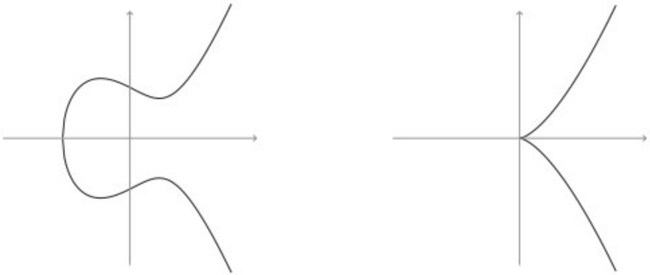

Figure – Figure Caption

Group Law of Elliptic curve

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 $(-P) = (x, -y)$,
- $P \oplus Q = (\alpha, \beta)$

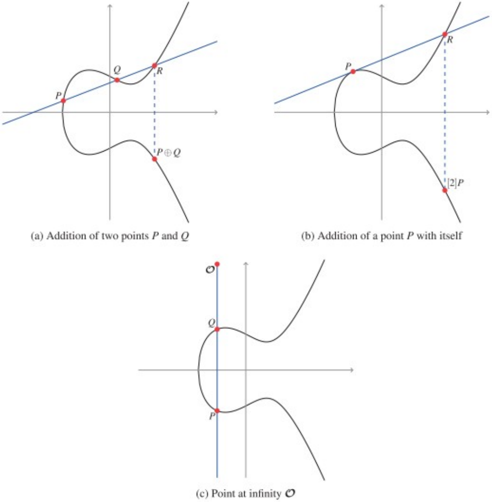

Figure – Demonstration of the Group Law on the Elliptic Curve $E : y^2 = x^3 + ax + b$ defined over $\mathbb{R}$

Hasse Interval

When $\mathbb{F}_{q}$ is a finite field, there are only finitely many points that can lie on E.

- Finding the exact number $|E(F_q)|$ of points is not easy ; however, with Hasse's theorem, we have an upper bound of

$$|E(F_q)| \leq q + 1 + |t|$$

for a field $\mathbb{F}_{q}$ with q elements, where $|t| \leq 2\sqrt{q}$, and t is called the Frobenius trace.

What Makes an Elliptic Curve "Supersingular"?

The elliptic curve E is called **supersingular** if p divides t, and **ordinary** otherwise. 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 $n \in \mathbb{N}$.

J-inverient And Isomerphism

Definition

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

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

Definition

There is an isomorphism $f : E \to E_0$ if and only if $j(E) = j(E_0)$.

Isogeny - A Key Concept

An isogeny is a mathematical map between elliptic curves.

Definition

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 $\phi(0_{E_1}) = 0_{E_2}$.

- Two elliptic curves are called **isogenous** if there is a non-constant isogeny between them
- It preserves the group structure of points on these curves.
- The degree of an isogeny is essentially the degree of polynomials describing it .
- Isogenies are the building blocks for many cryptographic schemes based on supersingular elliptic curves.

Isogeny Graph

- Each vertex of the graph represents a different j-invariant of a set of supersingular curves.
- The edges between vertices represent isogenies converting one elliptic curve to another.
- The graph is strongly connected, meaning every vertex can be reached from every other vertex.
- An isogeny graph with isogenies of degree l representing the edges is also called an l-isogeny graph

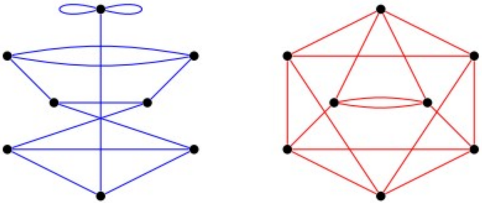

Figure – Supersingular isogeny graphs of degree 2 (left, blue) and 3 (right, red) on $\mathbb{F}_{97^2}$

Supersingular Isogeny Diffie-Hellman

The key idea of the Supersingular Isogeny Diffie-Hellman protocol (SIDH), is to let Alice and Bob take random walks in two distinct isogeny graphs on the same vertex set.

- **Random Walk :** It is possible to walk a whole graph by starting from any vertex, randomly choosing an edge, following it to the next vertex and then start the process again on a new vertex.

SIDH :High level view

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

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

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

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

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

- Alice and Bob pick seceret subgroups A and B of E.
- Alice computes the isogeny $\phi_A : E \to E/A$;Bob computes the isogeny $\phi_B : E \to E/B$.
  (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the values E/A and E/B.
- Alice obtains $A_0 = \phi_B(A)$.(similar for Bob)
- They both compute the shared secret

$$(E/B)/A_0 \approx E/ < A, B > \approx (E/A)/B_0$$

.

SIDH key exchange protocol

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 – Supersingular Isogeny Diffie-Hellman key exchange protocol.

- 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.

Challenges and Ongoing Research

- While promising, working with supersingular elliptic curves and isogenies presents challenges :
- **Computational Complexity**
- **Standardization and Adoption**
- **Ongoing Research to Improve Efficiency**
- **Staying Updated with the Latest Developments**

Conclusion

- Supersingular isogeny-based cryptography is a strong contender in the field of post-quantum security.
- It offers a potential solution to quantum computing threats.
- Its security is based on mathematical problems that have proven resistant to quantum attacks, making it a valuable choice for protecting sensitive data in a quantum computing era.