ELLIPTIC CURVE CRYPTOGRAPHY AND GROUP THEORY

DEEPAK JASSAL AND COREY STECYK

Abstract. This is a sample file. You can use it as a guide for your submission.

1. Introduction

Elliptic Cruve Cryptography (ECC) is powerful tool in modern day public-key cryptography. Where systems like RSA (Rivest-Shamir-Adelman) public-key cryptography needs 4096 bits, ECC needs only about 313 bits for the same level of security (Washington). This gives ECC the advantage of being more efficient, meaning less computational power is needed to implement, making it cheaper. This makes them very useful in resource constrained enviroments such as mobile devices.

ECC is an example of something that was at first studied in a strictly pure math enviroment (Lozanzo-Robledo, Washington) which was then implemented to a non-pure math setting (Washington). Elliptic curves were first studied as objects in number theory and algebraic geometry. Fermat's Last Theorem was proven By Andrew Wiles in 1994 by proving a special case of the modulatiry theorem for the Frey curve (Lozanzo-Robledo, Washington). In the mid to late 1980 Neal Koblitz and Victor Miller independantly using the points of elliptic curves in finite fields as the foundation for a cryptography system (Koblitz, Washington).

This paper is organizaed to first lay the necessecary groundwork for one to understand elliptic curves in this algebraic context. Next, will be mathematical constraints of RSA add ECC systems moving into the elliptic curve discrete logarithm problem and the Group Law. Finally a worked through example of an elliptic curve Diffie Helman key exchange protocol will be given.

2. Background

To understand ECC we must first understand the geometry and algebra behind elliptic curves.

Definition 2.1 (Finite Field)**.** A finite field F is a field with finite order. A field is a set of numbers on which addition, subtraction, multiplication, and division (by non-zero elements) is well defined.

Due to the context of this paper, we need to only consider the integers modulo q ($\mathbb{Z}_q$) where q is a prime power $q = p^k$ for some prime p and $k \geq 1 \in \mathbb{N}$.

Definition 2.2 (Elliptic Curves over Finite Fields)**.** In the context of cryptography, an elliptic curve E over a finite field $\mathbb{Z}_q$ ($q = p^k$, $p \geq 3$) is defined by the Weierstrass equation

$$y^2 = x^3 + ax + b \tag{1}$$

Date: November 23, 2025.

where $a, b, x, y \in \mathbb{Z}_q$, and a, b are chosen such that $\Delta = 16\left(4a^3 + 27b^2\right) \neq 0$ in $\mathbb{Z}_q$ (Koblitz, Lozanzo-Robledo, Washington).
We define the set $E(\mathbb{Z}_q) = \left\{(x, y) \in \mathbb{Z}_q \times \mathbb{Z}_q : y^2 \equiv x^3 + Ax + B \mod p\right\} \cup \{\mathcal{O}\}$, where $\mathcal{O}$ is a point at infinity.

Since we are discussing elliptic curves over a finite field in a group theory context it only makes sense to define a binary operation between two points on the curve.

Definition 2.3 (Point Addition on an Elliptic Curve E)**.** Let E be an elliptic curve over a finite field $\mathbb{Z}_q$ defined by the equation (1). We define point addition $\oplus$ for points in $E(\mathbb{Z}_q)$ as follows:

Geometric Definition (over $\mathbb{R}$ for intuition): Let $A, B \in E(\mathbb{Z}_q)$.

- **Identity:** The point at infinity $\mathcal{O}$ is the additive identity. Thus, for any point P, $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$.
- **Negative:** The negative of a point $A = (x_1, y_1)$ is its reflection over the x-axis, $-A = (x_1, -y_1)$. By the curve equation, $-A$ is also on the curve. By definition, $A \oplus (-A) = \mathcal{O}$.
- **Addition ($A \neq \mathcal{O}, B \neq \mathcal{O}, A \neq \pm B$):** Draw the line $\overline{AB}$ through A and B. This line intersects the curve at a third point C'. Then $A \oplus B$ is defined as $-C'$, the reflection of C' over the x-axis.
- **Doubling ($A = B$):** Draw the tangent line to the curve at point A. This line intersects the curve at another point C'. Then $A \oplus A = 2A$ is defined as $-C'$.

Algebraic Definition (for computation in $\mathbb{Z}_q$): Let $A = (x_1, y_1)$ and $B = (x_2, y_2)$ be points on $E(\mathbb{Z}_q)$.

- If $A = \mathcal{O}$, then $A \oplus B = B$.
- If $B = \mathcal{O}$, then $A \oplus B = A$.
- Else, if $x_1 = x_2$ and $y_1 = -y_2$ (i.e., $A = -B$), then $A \oplus B = \mathcal{O}$.
- Else, if $A \neq B$ (general addition), let the slope m be:

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

- Else, if $A = B$ (point doubling), let the slope m be:

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

- Then, the coordinates of $A \oplus B = (x_3, y_3)$ are given by:

$$x_3 = m^2 - x_1 - x_2 \mod p, \quad y_3 = m(x_1 - x_3) - y_1 \mod p$$

Problem 2.4 (Discrete Logarithm Problem (DLP))**.** *Given $\alpha \in G$ and $\beta \in \langle\alpha\rangle$, find the least positive integer x such that $x\alpha = \beta$ (Sutherland).*

The DLP is why breaking encrypted messages is so difficult. Trying to find x by brute force is very impractical since the easiest solution to prevent this attack from working is simply picking a very large x. It is general consensus that there is not a polynomial time algorithm to find x (Sutherland).

Problem 2.5 (Elliptic Curve Discrete Logarithm Problem (ECDLP))**.** *Let E be an elliptic curve over a finite field $\mathbb{Z}_q$. Let $P \in E(\mathbb{Z}_q)$ with $|P| = n$, and let $Q \in \langle P\rangle$. Then $Q = kP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{k \text{ times}}$ for some $k \in \mathbb{Z}$. We call k the discrete logarithm of Q with respect to P.*

3. Main Results

Perhaps an unsurprising fact about the set $E(\mathbb{Z}_q)$ with the binary operation $\oplus$ defined in definition (2.3) make a group. However, something that may be surprising is that this group $(E(\mathbb{Z}_q), \oplus)$ is an Abelian group. With this we move onto our first theorem.

Theorem 3.1.

4. Examples

5. Applications

6. Bibliography