ELLIPTIC CURVE CRYPTOGRAPHY AND GROUP THEORY

DEEPAK JASSAL AND CORY STECYK

Abstract. Abstract goes here

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 organized 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.

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

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

where $a, b, x, y \in \mathbb{F}_q$, and a, b are chosen such that $\Delta = 16\left(4a^3 + 27b^2\right) \neq 0$ in $\mathbb{F}_q$ (Koblitz, Lozanzo-Robledo, Washington).

Date: November 27, 2025.

We define the set $E(\mathbb{F}_q) = \big\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 \equiv x^3 + Ax + B \mod p\big\} \cup \{\mathcal{O}\}$, 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 $\mathbb{F}_q$ defined by the equation (1). We define point addition $\oplus$ for points in $E(\mathbb{F}_q)$ as follows:

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

- **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 $\mathbb{F}_q$): Let $A = (x_1, y_1)$ and $B = (x_2, y_2)$ be points on $E(\mathbb{F}_q)$.

- 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 $\mathbb{F}_q$. Let $P \in E(\mathbb{F}_q)$ 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 $k \in \mathbb{F}$. We call k the discrete logarithm of Q with respect to P.*

3. Main Results

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

Theorem 3.1. *The group $(E(\mathbb{F}_q), \oplus)$ is an Abelian group.*

Proof. Closeure under $\oplus$ is apparent from the fact that by definition the resulting value is another point on the elliptic curve. Commutativity can be easily seen from either the geometric interpretation of definition (2.3) or from the formulas. As the lines $\overline{AB}$ and $\overline{BA}$ are the same exacts lines. The identity element in this group is $\mathcal{O}$. If $A = (x_1, y_1) \in E(\mathbb{F}_q)$ then it can be seen from definition (2.3) that $A^{-1} = (x_1, -y_1) \in E(\mathbb{F}_q)$, then $A \oplus A^{-1} = \mathcal{O} = e_{E\mathbb{F}_q}$.
All that is left to show that $(E(\mathbb{F}_q), \oplus)$ is a group is that associativity holds. This is not at all apparently obvious from either the geometric or algebraic definition given in (2.3). In fact, this is quite a complicated proof and it beyond the scope of this paper, so we refer the reader to §2.4 of *Elliptic Curves Number Theory and Cryptography* by *Lawrence C. Washington.* □

Theorem 3.2 (Elliptic Curve Security)**.** *ECC is more secure than RSA, and the security of ECC is realiant on the computational difficultly of the ECDLP.*

Explanation. The reason we present an explanation instead of a proof can be extrapolated from the explanation.
For RSA there are sub-exponential time algorithms such as the Index Calculus Method (Washington) than can be used to solve the discrete log problem. However for the ECDLG (elliptic curve discrete logarithm problem) there are no known sub-exponential time algorithms. Some of the best known algorithms such as Pollard's ρ algorithm have a running time of $O(\sqrt{n})$, where n is the subgroup order (Washington). So far, it has not been shown that a sub-exponential time algorithm exists of the ECDLP. So the fact that a non sub-exponential time algorithm does not exist is not a fact, but rather an assumption. This assumption is similar to how factoring large integers into primes is hard is an assumption for the RSA crytpo system.

4. Examples and Applications

Example: Constructing a Small Elliptic Curve Group. To illustrate the concepts defined above, we will construct a small elliptic curve group and perform point addition.

Let us define an elliptic curve over the finite field $\mathbb{F}_{23}$. We choose $a = 1$ and $b = 4$ for our curve equation $y^2 = x^3 + x + 4$. First, we verify the curve is non-singular (i.e., $\Delta \neq 0$) by checking the discriminant Δ:

$$\Delta = -16(4a^3 + 27b^2) = -16(4(1)^3 + 27(4)^2) = -16(4 + 432) = -6976.$$

Working modulo 23, we find $-6976 \equiv 9 \not\equiv 0 \pmod{23}$. Thus, the curve is non-singular.

Our elliptic curve is defined as:

$$E(\mathbb{F}_{23}) : y^2 = x^3 + x + 4.$$

The set of points $E(\mathbb{F}_{23})$ consists of all pairs $(x, y) \in \mathbb{F}_{23} \times \mathbb{F}_{23}$ satisfying this equation, along with the point at infinity $\mathcal{O}$.

Let us find the point $P = (0, 2)$. Substituting into the curve equation:

$$2^2 = 4 \equiv 0^3 + 0 + 4 \equiv 4 \pmod{23}.$$

The equation holds, so P is on the curve. We will now compute $2P = P \oplus P$ using the point doubling formulas from Definition 2.3.

- Since $A = B = (0, 2)$, we use the point doubling formula.
- Calculate the slope m:

$$m = \frac{3x_1^2 + a}{2y_1} = \frac{3(0)^2 + 1}{2 \cdot 2} = \frac{1}{4} \mod 23.$$

  We need the multiplicative inverse of 4 modulo 23. Since $4 \times 6 = 24 \equiv 1 \pmod{23}$, the inverse is 6.

$$m = 1 \times 6 = 6 \mod 23.$$

- Now calculate x_3:

$$x_3 = m^2 - x_1 - x_2 = 6^2 - 0 - 0 = 36 \equiv 13 \pmod{23}.$$

- Finally, calculate y_3:

$$y_3 = m(x_1 - x_3) - y_1 = 6(0 - 13) - 2 = 6(-13) - 2 = -78 - 2 = -80 \pmod{23}.$$

  Since $-80 \div 23 = -4$ with a remainder of 12 ($-80 - (-4 \times 23) = -80 + 92 = 12$), we have:

$$y_3 \equiv 12 \pmod{23}.$$

Therefore, $2P = (13, 12)$. The reader can verify that $(13, 12)$ is indeed a point on the curve E. By continuing this process, one can compute the entire group. It can be shown that $E(\mathbb{F}_{23})$ has 29 points (28 finite points and $\mathcal{O}$) and is a cyclic group.

Application: Elliptic Curve Diffie-Hellman Key Exchange (ECDH). The Elliptic Curve Diffie-Hellman (ECDH) protocol is a direct application of the group law on elliptic curves and the hardness of the ECDLP. It allows two parties, Alice and Bob, to establish a shared secret over an insecure channel.

Protocol Setup.

(1) **Public Parameters:** Alice and Bob publicly agree on:
  - An elliptic curve E defined over a finite field $\mathbb{F}_q$.
  - A base point $P \in E(\mathbb{F}_q)$ with large prime order n. (The subgroup $\langle P \rangle$ is large and cyclic.)

Key Exchange.

(1) **Alice** generates a private key, a randomly selected integer a with $1 < a < n$.
(2) **Alice** computes her public key $A = aP \in E(\mathbb{F}_q)$ and sends it to Bob.
(3) **Bob** generates a private key, a randomly selected integer b with $1 < b < n$.
(4) **Bob** computes his public key $B = bP \in E(\mathbb{F}_q)$ and sends it to Alice.
(5) **Shared Secret:**
  - **Alice** receives B and computes $S = aB = a(bP)$.
  - **Bob** receives A and computes $S = bA = b(aP)$.

  Both calculations yield the same shared secret point $S = abP \in E(\mathbb{F}_q)$.

Security. An eavesdropper, Eve, observes the public parameters E, P, q and the public keys $A = aP$ and $B = bP$. To compute the shared secret $S = abP$, Eve must solve the **Elliptic Curve Diffie-Hellman Problem (ECDHP)**: find abP given P, aP, and bP.

It is widely believed that the only feasible way to solve the ECDHP is by first solving the ECDLP (e.g., by finding a from $A = aP$ and then computing aB). Since the ECDLP is computationally intractable for well-chosen curves, Eve cannot derive the shared secret. The x-coordinate of the point S is typically used as the shared symmetric key for subsequent encryption.

5. Bibliography