As Yale University professor Serge Lang once noted in the beginning of his book *Elliptic Curves: Diophantine Analysis*, “It is possible to write endlessly on elliptic curves. (This is not a threat)." Indeed, elliptic curves form a deep and intricate subject. In this thesis, we will dive into the topic of elliptic curves, with a particular focus on their impact in the field of modern cryptography. We aim to explore their significance and key properties, highlighting the crucial role they play in many cryptographic systems. The primary aim of this thesis is to deepen our understanding of this complex topic to such an extent that we are able to implement elliptic curve cryptography (ECC) in various applications and programs. In addition to exploring the theoretical significance of elliptic curves, we will also implement a few examples of elliptic curves referenced with corresponding source code and visual representation. Furthermore, this thesis will shed light on various attacks and common mistakes in the implementation of these curves, emphasizing the importance of secure and correct practices when building cryptographic applications.

Motivation for Using Elliptic Curves

The main advantage of ECC is the degree of security it provides when considering its comparatively smaller key sizes.

Table 1: Time to Break vs Key Sizes

Time to Break (MIPS-years)	**ECC Key Size (bits)**	**RSA Key Size (bits)**
10^4	106	512
10^8	132	768
10^{11}	160	1024
10^{20}	210	2048
10^{78}	600	21000

With the keys being smaller, we are able to have better computational efficiency of the algorithms; thus, our requirements on hardware resources can lower. Another advantage is that almost all currently known systems based on the discrete logarithm problem can be converted into elliptic curve-based systems. The vast majority of elliptic curve cryptography schemes rely on the Elliptic Curve Discrete Logarithm Problem (ECDLP) for their security.

What is an Elliptic Curve?

In order to start defining elliptic curves, we first need to introduce some terms up front.

Algebraic curve:

An *algebraic curve* (over a field K) is an equation $f(X, Y) = 0$, where $f(X, Y)$ is a polynomial in X and Y with coefficients in K. A *nonsingular algebraic curve* is an algebraic curve over K without any singular points over K.

K-rational point:

A *K-rational point* is a solution (X, Y) to the equation of an algebraic curve, where both X and Y are in the field K.

Point at infinity:

The point at infinity $\mathcal{O}$ (also referred as 0) is the identity element of elliptic curve arithmetic. Adding this point to any other point (including itself) results in that other point:

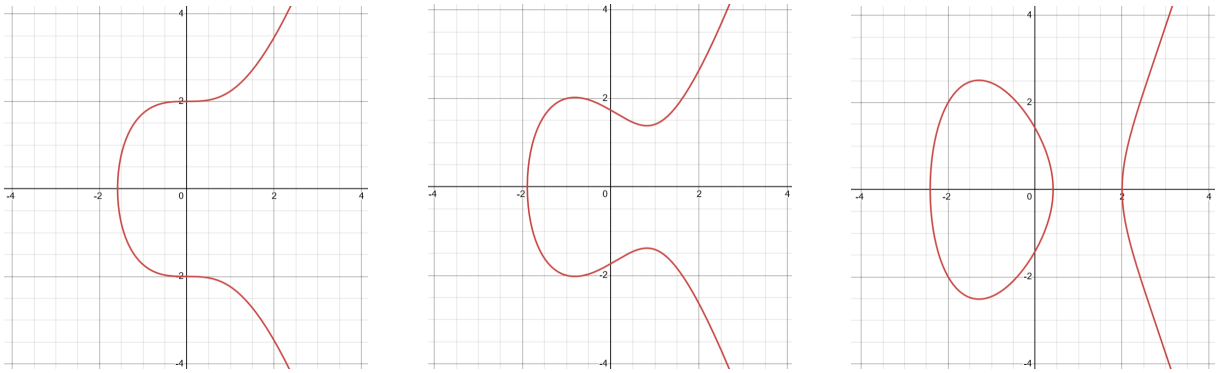
$$\mathcal{O} + P = P$$

Elliptic curve:

An *elliptic curve* over a field K is a nonsingular cubic curve, with a K-rational point (including a point at infinity). We will primarily be working with curves that are defined by The Weierstrass Form:

$E := \{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$ (where A and B are from the field K)

Elliptic curve in this equation forms a group if $4a^3 + 27b^2 \neq 0$.



(a) Curve: $y^2 = x^3 + 4$ (b) Curve: $y^2 = x^3 - 2x + 3$ (c) Curve: $y^2 = x^3 - 5x + 2$

Figure 1: Examples of elliptic curves (over $\mathbb{R}$)

Operations on Elliptic Curves

Now that we understand what an elliptic curve is, we need to define the operational rules necessary for performing point calculations on these curves.

Addition:

$$P_1 = (x_{P_1}, y_{P_1}) + P_2 = (x_{P_2}, y_{P_2}) = P_3 = (x_{P_3}, y_{P_3})$$

$$\lambda = \frac{y_{P2} - y_{P1}}{x_{P2} - x_{P1}} \quad \text{if } P_1 \neq P_2 \quad \text{and } P_1, P_2 \in E$$

$$x_{P3} = \lambda^2 - x_{P1} - x_{P2} \ , \ y_{P3} = \lambda(x_{P1} - x_{P3}) - y_{P1}$$

$$P_3(x_{P3}, y_{P3}) = P_1 + P_2$$

Negating a point:

$$P = (x_1, y_2)$$

$$-P = -(x_1, y_2) = (x_1, -y_2)$$

Subtraction:

$$P_1 - P_2 = (x_1, y_2) - (x_3, y_4) = (x_1, y_2) + (x_3, -y_4)$$

Multiplication:

Only scalar multiplication is possible. Multiplication between two points is not possible. Repeated addition is performed:

$$2P = P + P$$

$$3P = P + P + P$$

Division:

Only scalar division is possible.

$$\frac{1}{a}(x_p, y_p) = a^{-1}(x_p, y_p)$$

Specific Examples

Let's have EC E (over $\mathbb{R}$) with this formula:

$$E := \{(x, y) \in R^2 \mid y^2 = x^3 - x + 1\} \cup \{\mathcal{O}\} \text{ (over } \mathbb{R})$$

Then, let's take two points $P_1 = (x_1, y_2)$ and $P_2 = (x_3, y_4)$, and $P_3 = (x_5, y_6)$ where $P_1 + P_2 = P_3$.

Now, let's take two points $P_1 = (1, 1)$ and $P_2 = (0, -1)$.