Elliptic Curve Cryptography

A Dissertation for

MAT-651 Discipline Specific Dissertation

Credits: 16

Submitted in partial fulfilment of Masters Degree

M.Sc. in Mathematics

by

Ms. CALLISTA VALANKA CABRAL

22P0410006

ABC ID : 948-380-101-489

201905881

Under the Supervision of

Dr. MANVENDRA TAMBA

School of Physical & Applied Sciences

Mathematics Discipline

GOA UNIVERSITY
APRIL 2024

Examined by: Seal of the School

DECLARATION BY STUDENT

I hereby declare that the data presented in this Dissertation report entitled, "Elliptic Curve Cryptography" is based on the results of investigations carried out by me in the Mathematics Discipline at the School of Physical & Applied Sciences, Goa University under the Supervision of Dr. Mannvendra Tamba and the same has not been submitted elsewhere for the award of a degree or diploma by me. Further, I understand that Goa University will not be responsible for the correctness of observations / experimental or other findings given the dissertation.

I hereby authorize the University authorities to upload this dissertation on the dissertation repository or anywhere else as the UGC regulations demand and make it available to any one as needed.

Signature: Valanka

Student Name: Callista Valanka Cabral

Seat no: 22P0410006

Date: 08/05/2024

Place: GOA UNIVERSITY

COMPLETION CERTIFICATE

This is to certify that the dissertation report "Elliptic Curve Cryptography" is a bonafide work carried out by Ms. Callista Valanka Cabral under my supervision in partial fulfilment of the requirements for the award of the degree of Master of Science in Mathematics in the Discipline Mathematics at the School of Physical & Applied Sciences , Goa University.

Signarure : ____________________

Supervisor : Dr. Manvendra Tamba

Date: 08/05/2024

Signature of Programme director of the Mathematics

Date: 10/5/2024

Place: Goa University

School of Physical and Applied Sciences ★ Goa University

School Stamp

PREFACE

This Project Report has been prepared in partial fulfilment of the requirement for the Subject: MAT - 651 Discipline Specific Dissertation of the programme M.Sc. in Mathematics in the academic year 2023-2024.

The topic assigned for the research report is: " Elliptic Curve Cryptography." This survey is divided into four chapters. Each chapter has its own relevance and importance. The chapters are divided and defined in a logical, systematic and scientific manner to cover every nook and corner of the topic.

FIRST CHAPTER :

The Introductory stage of this Project report is based on overview of Number Theory and basic Algebra, where few basic results and definitions are listed.

SECOND CHAPTER:

This chapter deals with Elliptic Curves . In this topic we discuss how Elliptic Curves are defined. We also see how we geometrically interpret certain operations which then further on are used to define The Group Law. Elliptic Curves on Finite fields forms the base for Cryptography.

THIRD CHAPTER:

In this chapter we have introduced what is RSA, one of the most widely used cryptosystems that are used till date. The main aim here was to Understand how the algorithm works so that it is evident when we compare the difference in key size. We also see what Diffie Hellman key Exchange Protocol is and about Discrete Logarithm Problem. We solve examples using the same as well.

FOURTH CHAPTER:

This the main chapter in which we deal with Elliptic Curve Cryptography. Before heading to ECC we see how Elliptic curve Diffie Hellman Key Exchange and Elliptic Curve Discreete Logarithm Problem is defined. Further more we discuss the cyptography algorithm and then see the majoy key comparison between RSA and ECC. AN application of ECC that is Elliptic Curve Digital Signatures is also discussed in this Chapter.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my gratitude to my Mentor, Dr. Manvendra Tamba, who was a continual source of inspiration. He pushed me to think imaginatively and urged me to do my work without hesitation, he suggested me the topic on Elliptic Curves. His vast knowledge, extensive experience, and professional competence in Algebra and Number Theory enabled me to successfully accomplish this project. This endeavour would not have been possible without his help and supervision. I could not have asked for a finer mentor in my studies.

I would like to extend my gratitude to our Programme director of Mathematics Discipline Dr. Kunhanandan for his constant support and guidance. I would like to thank the Dean of School of Physical and Applied Sciences, Prof. Ramesh Pai for providing all the facilities for successful completion of the dissertation.

I want to express my heartfelt gratefulness to Dr. Jessica Fernandes e Pereira and Mr. Brandon Fernandes whose rich knowledge and guidance in Latex typing helped me with completion of this Dissertation.

Last but not the least I would like to thank my parents for always being there for me, for without them i wouldn't have been able to complete this dissertation

ABSTRACT

Elliptic Curve Cryptography (ECC) is one of the strongest and most efficient cryptographic techniques in modern cryptography. Smaller ciphertexts, keys, and signatures and faster generation od keys and signatures are key features of ECC.
Elliptic Curve is obtained from the Weierstrass Equation. Implementation of elliptic curve in cryptography requires smaller chips size, less power consumption and increase in speed. Diffie Hellman and Discrete Logarithm Problem are methods that are used in Cryptography. Elliptic Curve Cryptography is a simple yet very efficient algorithm used in encryption. The main aim of this article is to understand the simple working Rule of Elliptic Curves and then further see how it is implemented in cryptography. We also see the comparison between one of the most used algorithm RSA and Elliptic Curve Algorithm. Elliptic Curve is also widely used in Digital Signature Algorithm.

Keywords: Elliptic Curve Cryptography (ECC); RSA code; Elliptic Curve Digital Signature Algorithm (ECDSA); Diffie Hellman Key Exchange Protocol; Discrete Logarithm Problem

Table of contents

List of figures

Notations and Abbreviations

$E(K)$	Elliptic Curve over field K
F_p	Finite field over p
$E_P(a,b)$	$y^2 = x^3 + ax + bmodp$
ECC	Elliptic Curve Cryptography
RSA	Rivest Shamir Adleman
DHE	Diffie Hellman Key Exchange
ECDHE	Elliptic Curve Diffie Hellman Key Exchange
DLP	Discrete Logarithm Problem
ECDLP	Elliptic Curve Discrete Logarithm Problem
DSA	Digital Signature Algorithm

Chapter 1

INTRODUCTION

1.1 Introduction

Number Theory

Number Theory is a branch of pure mathematics that is devoted to study of the integers and arithmetic Functions.One of the important goal of number theory is to understand different and interesting relations between sorts of numbers and to prove these relations are true.

Elliptic Curve

Elliptic curves are curve that are defined by a certain cubic equation in two variables. The set of rational solutions to this equation has an extremely interesting structure, including a group law. The theory of elliptic curves was essential in Andrew Wiles' proof of Fermat's last theorem. Computational problems involving the group law are also used in many cryptographic applications, and in algorithms for factoring large integers.

Cryptography

Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. We shall see more about this in Chapter 3.

1.2 Motivation

Elliptic Curves are a important part of Number Theory. The theory of elliptic curves was essential in Andrew Wiles' proof of Fermat's last theorem. Elliptic curves also play a major role in Cryptography. Elliptic Curve Cryptography (ECC) offers equivalent security with lower computing power and battery resource usage And One of the most important practical benefits is significantly reduced key sizes compared to other crypto systems.

1.3 Basic Results and Definitions

Genus: Genus of curve determines its properties to a remarkable extent-in particular, by the trichotomy g=0, g=1 0r g $\geq$ 2.
Genus 1 : Genus 1 curves are simplest nontrivial algebric curves, they have very rich structure. Elliptic curve genus being 1 indicates they have one handle/ one hole making them equivalent to torus[5].
Rational Line A rational number is a quotient of two integers. A point (x,y) in the plane is a rational point if both coordinates are rational numbers. A line is called rational line if the equation of line can be written with rational numbers, i.e if equation is $ax+by+c=0$ a,b,c are rational. A line through them is rational. Also if you have two rational lines their intersect is also rational.[6]

Rational points on curve We say that conic is rational if we can write equation with Rational numbers. To see intersection of rational line with Rational conic, if we use analytical geometry to find coordinates of these points,we will come out with quadratic equation for x coordinate of intersection. And if conic and line are rational, quadratic equation will have rational coefficients. So points of intersection will be rational if and only if roots of quadratic equation are rational.[6]

Group

A Group ($G, \cdot$) is a set G together with operation $\cdot$ satisfying following Axioms:

1. Closure: If $x, y \in G$ then $x \cdot y \in G$
2. Associativity: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in G$
3. Identity : There exist an element $e \in G$ such that $a \cdot e$= $e \cdot a$ = a for all $a \in G$
4. Inverse: For each $a \in G$ there is an element $a^{-1} \in G$ such that $a \cdot a^{-1}$=$a^{-1} \cdot a$=e

The number of elements of a group G is called its order. It is denoted by |G|.

Corollary 1.3.0.1. *An elememt k is generator of $\mathbb{Z}_n$ iff gcd(k,n)=1*

Some properties of mod function are as follow:

- Addition Property: (A+B) mod C = ((A mod C) + (B mod C)) mod C
- Mod of negative number(-A) mod C= (-A+C) mod C
- Multiplication Property : (A*B) mod C = ((A mOd C) *(B mod C))mod C
- Modular Inverse: (A*A^{-1}) $\cong$ 1 mod C

Chapter 2

ELLIPTIC CURVES

Definition 2.0.0.1. [7] An elliptic curve E (over a field $\mathbb{K}$) is a smooth projective curve of genus 1 (defined over $\mathbb{K}$). given by:

$$E = \{(x,y)|y^2 = x^3 + Ax + B\}$$

where A and B belong to field such as $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_{|}$. There is also an requirement that the discriminant

$$\Delta = 4A^3 + 27B^2 \quad \text{is non zero}$$

Equivalently polynomial $x^3 + Ax + B$ has distinct roots. This ensures that curve is non singular.

We toss an extra point $\mathscr{O}$ that is "at infinity"

So set E is

$$E = \{(x,y) : y^2 = x^3 + Ax + B\} \cup \{\mathscr{O}\}$$

2.1 Geometry of Curves

Geometry Of Elliptic Curves was referred from [5] Point Addition

1. Start with two points P and Q on E
2. Draw line L through P and Q.
3. Line L intersects cubic curve E in third point call it R.
4. Draw vertical line through R. It hits E at another point
5. We define the sum of P and Q on E to be the reflected point. We denote it by P + Q

We can see the visualisation in the following image:::

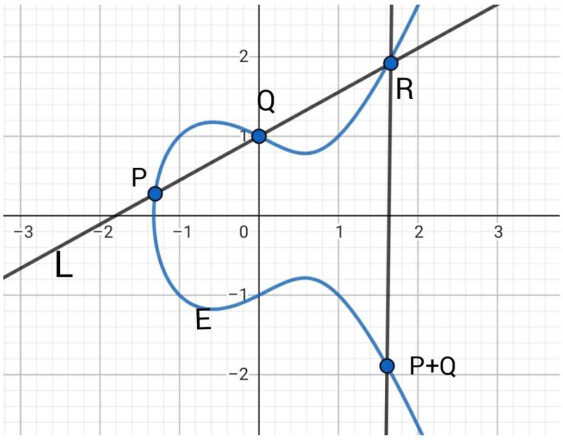


Figure 2.1: Point Addition

Point Doubling

1. If we think adding P to Q and let Q approach P then line L becomes tangent to E at P.
2. Then we take third intersection at pt R reflect across x- axis and call resulting point P + P or 2P.

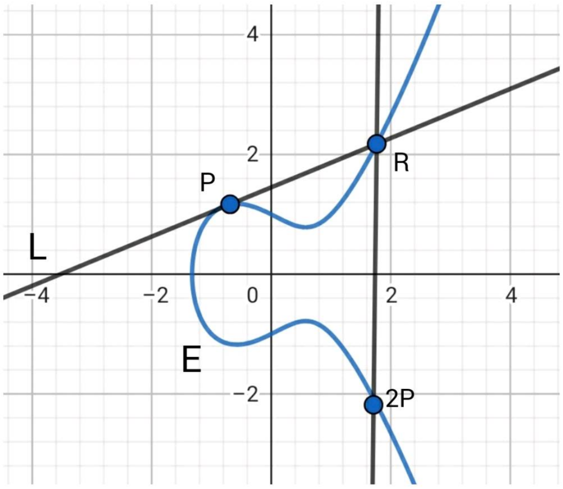


Figure 2.2: Point Doubling: here line L is tangent to E at P

Point at Infinity

1. Let P $\in$ E. We denote reflected point by -P.
2. Vertical line through P and -P doesn't intersect E at third point. And we need third point P + (-P).
3. Since there is no point in plane that works we create extra point $\mathscr{O}$ "at infinity".

   Rule: $\mathscr{O}$ is a point on every vertical line.

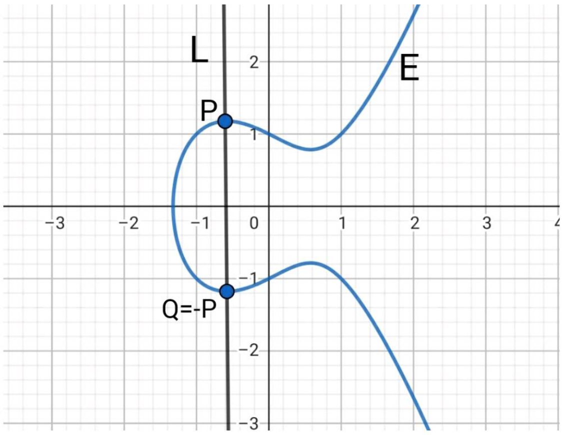


Figure 2.3: We denote point at infinity as $\mathscr{O}$

2.2 Algebra of Curves

This section is referred from [7] Suppose we want to add points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on the curve

$$E : y^2 = x^3 + Ax + B$$

Let line connecting P_1 and P_2 be

$$L : y = m(x - x_1) + y_1$$

We find the intersection between curve E and line L by solving

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

Upon solving we get

$$m^2(x^2-2xx_1+x_1^2)+2my_1x-2my_1x_1+y_1^2=x^3+Ax+B$$

$$\implies 0=x^3-m^2x^2+(2m^2x_1+2my_1+A)x+(B+2my_1x_1-y_1^2-m^2x_1^2)$$

This is a cubic equation in x For any cubic polynomial x^3+ax^2+bx+c and roots r,s,t then we have

$$x^3+ax^2+bx+c=(x-r)(x-s)(x-t)=x^3-(r+s+t)x^2+(st+rt+rs)x-rst$$

$\therefore r+s+t=-a$

hence if we know two roots we can obtain the third In our case we have

$$x^3-m^2x^2+(2m^2x_1+2my_1+A)x+(B+2my_1x_1-y_1^2-m^2x_1^2)$$

$$=(x-x_1)(x-x_2)(x-x_3)$$

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

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

The slope of L is given by

$$m=\begin{cases}\frac{y_2-y_1}{x_2-x_1} & \text{if} \quad P_1\neq P_2\\ \frac{3x_1^2+A}{2y_1} & \text{if} \quad P_1=P_2\end{cases}$$

Summary Addition Algorithm for $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on curve E: $y^2 = x^3 + Ax + B$ is given by

- If $P_1 \neq P_2 and x_1 = x_2$ the $P_1 + P_2 = \mathcal{O}$
- If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = 2P_1 = \mathcal{O}$
- If $P_1 \neq P_2 and x_1 \neq x_2$

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

- If $P_1 = P_2$ and $y_1 = 0$, then

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

moreover $P + \infty = P$ for all points P on E.

Example: 2.2.0.1. *Given points $P_1 = (1,2)$ and $P_2 = (3,4)$ on elliptic curve $y^2 = x^3 - 7x + 10$ find $P_1 + P_2$ and $(P_1 + P_2) + P_2$*

Solution,

Let the third point of intersection be denoted by Q

Line passing through (1,2) and (3,4) is given by $y = x + 1$

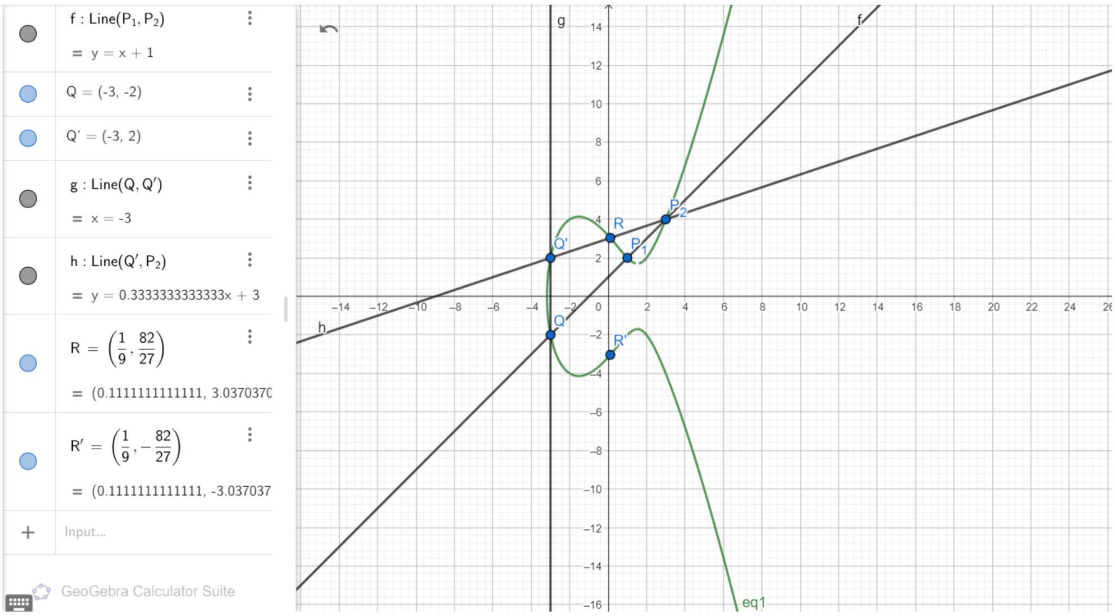
Substituting this in the equation of curve we get equation

$x^3 - x^2 - 9x + 9 = 0$ whose factors are $(x-1)(x-3)(x+3) = 0$

Thus x-coordinate of Q is -3 and y coordinate is -2. which is (-3,-2)

$\therefore Q' i.e P_1 + P_2$ is given by (-3,2).

To find sum of $(P_1 + P_2) + P_2$ *we perform similar procedure; line through (-3,2) and (3,4) given by* $y = \frac{1}{3}x + 3$
solving we get roots $(x - \frac{1}{9})(x+3)(x-3) = 0$ *so* $R = (\frac{1}{9}, \frac{82}{27})$
$\therefore R' = (P_1 + P_2) + P_2 = (\frac{1}{9}, -\frac{82}{27})$



f : Line(P₁, P₂)
= y = x + 1

Q = (-3, -2)

Q' = (-3, 2)

g : Line(Q, Q')
= x = -3

h : Line(Q', P₂)
= y = 0.3333333333333x + 3

R = $\left(\frac{1}{9}, \frac{82}{27}\right)$
= (0.1111111111111, 3.037037C

R' = $\left(\frac{1}{9}, -\frac{82}{27}\right)$
= (0.1111111111111, -3.037037

Figure 2.4: Representation

2.3 Group Law

Theorem 2.3.0.1. *[7] Addition of points on elliptic curve E satisfies following properties*

1. *Commutativity:* $P_1 + P_2 = P_2 + P_1 \ \forall P_1, P_2 \in E$

2. *Existence of Identity:* $P + \mathscr{O} = P \ \forall P$ *on E*

3. *Existence of Inverse: Given point P on E* $\exists P'$ *on E with* $P + P' = \mathscr{O}$*. This point* P' *denoted as* $-P$

4. *Associativity:* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P3)\ \forall P_1, P_2, P_3$ *on E*

In other words points on E forms an additive abelian group with $\mathscr{O}$ *as identity element.*

Proof. The proof of commutativity follows from the formulas, as slope of line through any two points calculated either way is the same. i.e

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

Also from the fact that line drawn through P_1 to P_2 is the same as line drawn from P_2 to P_1. Identity property holds by definition i.e If $P_1 = P_2$ and $y_1 = 0$, then

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

moreover $P + \infty = P$ for all points P on E.

For inverse let P' be reflection of P across x axis then $P + P' = \infty$

Associative property can be visualized as law of composition.We start with 2 points P_1 and P_2 and perform certain procedure to obtain third point $P_1 + P_2$. Then we repeat procedure with $(P_1 + P_2)$ and P_3 to obtain $(P_1 + P_2) + P_3$. If we instead start by adding P_2 and P_3 then computing $P_1 + (P_2 + P_3)$ we obtain the same point.

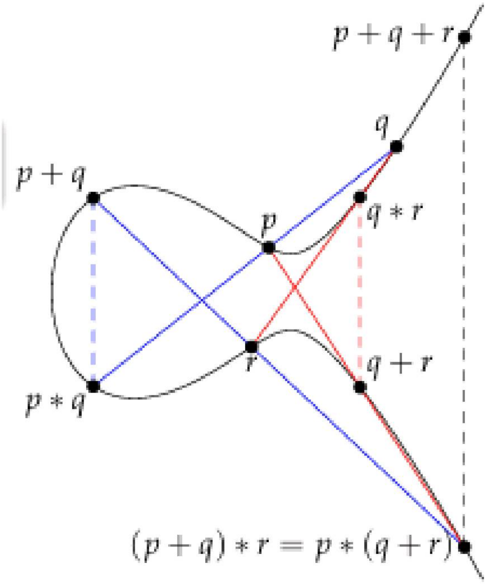


Figure 2.5: Visualization of Associative Law

□

Definition 2.3.0.2. Elliptic Curve over Rationals For an Elliptic curve defined as $E = \{(x,y)|y^2 = x^3 + Ax + B\}$ over the field $\mathbb{Q}$.

Corollary 2.3.0.3. *[7] If P and Q are rational points on an Elliptic curve, so also is $P+Q$.*

Proof. The line L through P and Q has rational coefficients, this is also true when P=Q and L is a tangent line. Upon substituting L in E we obtain a cubic with rational coefficients and two rational roots. The third root of $P*Q$, is rational as the third root can be obtained from the coefficient of

x^2 of the cubic polynomial and the other two roots.The other coordinate is rational via L. □

Definition 2.3.0.4. Elliptic Curve over finite field [4] An Elliptic curve over a finite field $\mathbb{F}_{|}$ is given by

$$E = \{(x,y)|y^2 = x^3 + Ax + B\} \quad mod\ p$$

together with imaginary point $\mathscr{O}$ and $a, b \in \mathbb{F}_{|}$ satisfying

$$\Delta = 4A^3 + 27B^2 \quad mod\ p \text{ is non zero}$$

Elliptic curves over finite fields do not have a nice graph as in case of Elliptic curve over Real Field. Here Elliptic curves are discrete points in plane. So, geometric Representation is not the same as we geometrically interpreted in terms of Real fields but the concept is the same we use same addition operator with calculation done in modulo.

Summary of the Algebra of the curve Addition Algorithm for $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on curve E: $y^2 = x^3 + Ax + B$ mod p is given by

- If $P_1 \neq P_2 and x_1 = x_2$ the $P_1 + P_2 = \mathscr{O}$
- If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = 2P_1 = \mathscr{O}$
- If $P_1 \neq P_2 and x_1 \neq x_2$

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

- If $P_1 = P_2$ and $y_1 = 0$, then

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

moreover $P + \infty = P$ for all points P on E.

Real Life Example : One of the real life example of Elliptic curve is curve used for bitcoin named as $secp256k1$. this curve is given by $y^2 = x^3 + 7$ which is defined over finite field $\mathbb{Z}_{2^{256}-2^{32}-977}$ [2]

Example: 2.3.0.5. *If P =(5,11) on elliptic curve* $y^2 = x^3 + 2x + 3$ *mod* 17, *find* 2*P and* 3*P*

Solution,

For P= (5,11) = (x_1, y_1) *we have,*

$$\begin{aligned}
m &= \frac{3x_1^2 + a}{2y_1} \quad mod p \\
&= \frac{3 * 5^2 + 2}{2 * 11} \quad mod 17 \\
&= \frac{75 + 2}{22} \quad mod 17 \\
&= 12 \\
x_2 &= m^2 - x_1 - x_1 \quad mod\ p \\
&= 12^2 - 5 - 5 \quad mod\ 17 \\
&= 134 \quad mod\ 17 \\
&= 15 \\
y_2 &= m(x_1 - x_3) - y_1 \quad mod\ p \\
&= 12(5 - 15) - 11 \quad mod\ 17 \\
&= -131 \quad mod\ 17 \\
&= 5
\end{aligned}$$

Thus point $Q(x_2, y_2)$ *= (15,5) and hence, 2P = (15,12). Next, to obtain 3P we have 2P + P. where 2P = (15,12) and P= (5,11).*

Now,

$$\begin{aligned}
m =& \frac{y_2 - y_1}{x_2 - x_1} \quad mod\ p \\
=& \frac{12 - 11}{15 - 5} \quad mod\ 17 \\
=& 1 * 10^{-1} \quad mod\ 17 \\
=& 12 \\
and\ x_3 =& m^2 - x_1 - x_2 \quad \text{mod } 17 \\
=& 12^2 - 5 - 15 \quad mod\ 17 \\
=& 124 \quad mod\ 17 \\
=& 5 \\
and\ y_3 =& m(x_1 - x_3) - y_1 \quad mod\ 17 \\
=& 12(5 - 5) - 11 \quad mod\ 17 \\
=& -11 \quad mod\ 17 \\
=& 6
\end{aligned}$$

Hence we obtain 3P = P + 2P = (5,-6) = (5,11)

Obtaining of points in finite field

Let us see how to obtain points of the curve defined by $y^2 = x^3 + x + 1$.

Hence the points on the graph are: (2,0), (0,1), (0,10), (8,2), (8,9), (3,3),

x/y	y^2 mod 11	$x^3 + x + 1$ mod 11
0	0	1
1	1	3
2	4	0
3	9	9
4	5	3
5	3	10
6	3	3
7	5	10
8	9	4
9	4	2
10	1	10

(1,5),(1,6),(4,5),(4,6), (6,5),(6,6), (3,8).

$\therefore$ the order of the curve $y^2 = x^3 + x + 1 mod 11$ is 13.

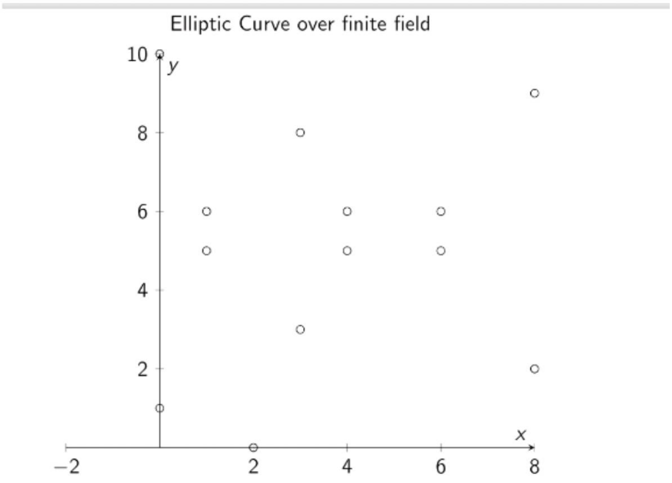


Figure 2.6: Graph of Elliptic curve over Finite fields

Chapter 3

CRYPTOGRAPHY

3.1 Introduction

This Chapter is mainly referred from [1]

Cryptography is the art of protecting and hiding information and communicating through the use of codes and algorithms so that those for whom the information is intended can read and process it. Cryptography was used by people for transmission of information and had become increasingly important in wars.

Cryptography's history is very long. It had been discovered for about 400 years. Before 1949, classical codes were used in cryptography. Classical codes have low intensity which states that they can be cracked easily. Between 1950 and 1975 cryptography gradually entered into people's

mind and became a science. From then onwards till date, the key in cryptography has made great progress. From that point forward, cryptography began to divide into several branches.
Cryptography systems are of two types

- Private Key Cryptography also referred to as Symmetric Cryptography
- Public key Cryptography also referred to as Asymmetric Cryptography

We will be studying about the asymmetric i.e. public key, algorithms of public key cryptosystem are very different from symmetric algorithms. Most public-key algorithms are based on number theoretic functions. This is quite different from symmetric ciphers, where the goal is usually not to have a compact mathematical description between input and Output.
Principle of Private Key Cryptography
A system is symmetric with respect to two properties:

1. The same secret key is used for encryption and decryption
2. The encryption and decryption function are very similar.

Principle of Public key cryptography
The use of public -key cryptography represents a major shifting from

previous methodologies. Until recently, most cryptographies relied on the fundamental tools of substitution and permutation. However , unlike traditional single-key encryption, public key algorithms are based on mathematical functions and are asymmetric in nature and require requiring the usage of two keys. In order to overcome these drawbacks Diffie, Hellman and Merkle had a revolutionary proposal based on the following idea: It is not necessary that the key processed by the person who encrypts the message is secret rather crucial part is that the receiver can only decrypt using the secret key.

1. Each system generates a pair of keys.
2. Each system publishes its encryption key (public key) keeping its companion key private.
3. If A wishes to send a message to B it encrypts the message using B's public key
4. When B receives the message, it decrypts the message using its private key. No one else can decrypt the message because only B knows its private key.

3.2 RSA Cryptosystem

The R.S.A crypto scheme , sometimes referred to as the Rivest-Shamir-Adleman algorithm is currently the most widely used asymmetric cryptographic scheme, even though elliptic curves and discrete logarithm schemes are gaining ground.

Using the R.S.A algorithm the keys are used together in one of the following ways

- Encrypting with Public Key

  Sending messages only the intended recipient can read.

  Let us consider Bob encrypts a plain text message with Alice's public key, then Alice decrypts the cipher text message with her private key. Since Alice is the only one with access to the private key, the encrypted message cannot be read by anyone besides Alice.

- Signing with your private key.

  Verifying that you're the one who sent a message.

  Alice encrypts a plain text message with her private key, then sends the cipher text to Bob. Bob decrypts the cipher text with Alice's public key. Since the public key can only be used to decrypt messages signed with Alice's private key, we can trust Alice was the author of the original message.

In practice, RSA is often used together with a symmetric cipher such as AES where the symmetric ciper does the actual bulk data encryption. The underlying one way function of RSA is the integer factorization problem. Multiplying two large primes is computationally easy but factoring the resulting product is very hard.

3.2.1 RSA Encryption and Decryption

RSA encryption and decryption is done in integer ring $\mathbb{Z}_n$ and modular computation play a central role. RSA encrypts plain text x where we consider the bit string representing x to be an integer in $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$. As a consequence the binary value of plain text x must be less than n. The same holds for cipher text. Encryption with public key and decryption with private key are shown below:

RSA Encryption: Given public key (n,e) = k_{pub} and plain text x, the encryption function is

$$y = ek_{pub}(x) \cong x^e \quad mod\ n$$

Where x,y $\in \mathbb{Z}_n$

RSA Decryption: Given the private key d = k_{pr} and cipher text y, the decryption function is

$$x = dk_{pr}(y) \cong y^{d} \quad mod\ n$$

Where x,y $\in \mathbb{Z}_n$

In practice x,y,n and d are very long numbers, usually 1024 bit long or more. The value e sometimes referred to as encryption exponent or public exponent and the private key d is sometimes called decryption exponent or private exponent. If Alice wants to send an encrypted message to Bob, Alice needs to have his public key (n.e) and Bob decrypts with his private key d.

3.2.2 Key Generation and Distribution

Output: public key $k_{pub} = (n,e)$ and private key $k_{pr} = (d)$ where n is the key size.

1. choose two large prime numbers p and q
2. Compute $n = pq$
3. Compute $\phi(n) = (p-1)(q-1)$
4. Select public exponent e $\in \{1,2,3,\cdot,\phi(n)-1\}$ such that gcd(e,$\phi(n)$) $= 1$

5. Compute private key d such that $d * e \cong 1 mod \phi(n)$

The condition gcd(e,$\phi(n)) = 1$ ensures that the inverse of e exists modulo $\phi(n)$ so that there is always a private key d.

Example: 3.2.2.1. *Here is an example of RSA encryption and decryption. Parameters used here are relatively small, but this is made in order to understand the basic idea of the RSA Algorithm.*
Bob (the receiver) generates his public key (n,e) using method discussed above

1. *Choose p=3 and q=11*
2. *n =pq= 3*11= 33*
3. *$\phi(n)$ = (3-1)(11-1)=20*
4. *Bob decides to choose e = 3 as his public key*
5. *$d \cong e^{-1}$ mod 20 $=$ 7 mod 20*

SO we have Bob's public key to be (33,3) and his private key to be (33,7) Suppose Alice wants to send a message x=4 to Bob. She uses bob's Public key to encrypt her message. the message x=4 becomes

$$y = x^e modn = 4^3 mod33 = 31 mod33$$

Bob receives text as y=31.

He uses his private key d=7 to decrypt the cipher text

$$x = y^d modn = 31^7 mod33 = 4$$

*Note that the private and public exponents fulfill the condition $e * d$ = 3*7 $\cong$ 1 mod $\phi(n)$*

Practical RSA Parameters are much larger. The RSA modulus n should be at least 1024 bit long, which results in a bit length of p and q of 512.

3.3 Diffie-Hellman Key Exchange Protocol

The Diffie Hellman Key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel. The point is to agree on a key that two parties can use for encryption, in such a way that an eavesdropper cannot obtain the key.

3.3.1 Diffie Hellman Algorithm

Steps in the Algorithm are as follows:

- Alice and Bob agree on a prime number p and a generator g

- Alice chooses a secret number a, and sends Bob $(g^a \, modp)$
- Bob chooses a secret number b, and sends Alice $(g^b \, modp)$
- Alice computes $(g^b \, modp)^a \quad mod\ p$
- Bob computes $(g^a \, modp)^b \quad mod\ p$

Both Alice and Bob can use this number as their key. Notice that p and g need not be protected.

Example: 3.3.1.1. • *Alice and Bob agree on p= 23 and* $\alpha = 5$

- *Alice chooses* $X_a = 6$ *and sends* 5^6 *mod 23 = 8 to Bob*
- *Bob chooses* $X_b = 15$ *and sends* 5^{15} *mod 23 = 19 to Alice.*
- *Alice computes* 19^6 *mod 23 = 2*
- *Bob computes* 8^{15} *mod 23 = 2*

Then 2 is the shared key.

Clearly a much larger values of a,b,and p are required An eavesdropper cannot discover this value even if she knows p and g.
Suppose p is a prime of around 300 digits and a and b at least 100 digits each

Discovering the shared secret given g,p , $(g^{a} mod p)$, $(g^{b} mod p)$ would take longer than lifetime of universe using the best known algorithm. This is called Discrete Logarithm problem.
How can two parties agree on a secret value when all their messages might be overheard by an eavesdropper? The Diffie Hellman algorithm accomplishes this and is still widely used. With sufficiently large inputs Diffie Hellman is very secure.

3.4 Discrete Logarithm Problem

Discrete Logarithm Problem (DLP) in $\mathbb{Z}_p$, given is the finite cyclic group $\mathbb{Z}_p$ of order $p-1$ and a primitive element $\alpha \in \mathbb{Z}_p$ and another element $\beta \in \mathbb{Z}_p$
The DLP is the problem of determining the integer $1 \ \leq \ x \ \leq \ p-1$ such that

$$\alpha^{x} = \beta \quad mod\ p$$

An integer x must exist since alpha is a primitive element and each group element can be expressed as a power of any primitive element. This integer x is called discrete logarithm of β to the base α and can formally write

$$x = log_{\alpha}\, \beta \quad mod\ p$$

Computing discrete logarithms modulo prime is very hard problem if the parameters are sufficiently large. Since exponentiation $\alpha^{\beta} mod p$ is computationally easy, this forms a one- way function.

Example: 3.4.0.1. *For the prime p=1999 the ring Z_p is a finite field and the non zero elements of $Z^*{}_p$ forms a group G under under multiplication modulo p:*

$$G = Z^*{}_p = \{1, 2, \cdots, p-1\}$$

Furthermore the element α = 3 is generator of G, also known as a primitive element modulo p

$$G = \{1, \alpha, \alpha^2, \cdots, \alpha^{p-2}\}$$

It is easy to compute that

$$3^{789} \cong 1452 \quad mod \ p$$

However it is not nearly easy to determine that x=789 given that x is in the range 0 to 1997 and satisfies equation

$$3^{x} \cong 1452 \quad mod \ 1999$$

Chapter 4

CRYPTOGRAPHY USING EC

4.1 Introduction

[8] Elliptic curve Cryptography (ECC) is the newest member of the three families of established public key algorithms of practical relevance introduced. ECC has been around since the mid 1980's. ECC provides the same level of security as RSA or discrete logarithm systems with considerably shorter operands (approximately 160-256 bit vs. 1024-3072 bit). ECC is based on generalized discrete logarithm problem, and thus DL-protocols such as Diffie- Hellman key exchange also done using elliptic curves.
ECC has performance advantages(fewer computations) and bandwidth advantages (shorter signatures and keys) over RSA and Discrete Logarithm

(DL) schemes. The mathematics of elliptic curves are considerably more involved than those of RSA and DL schemes.

4.1.1 Elliptic Curve Discrete Logarithm Problem

This section is referred from [1]. As discussed earlier DLP is the problem of finding the number y given some base number g, where

$$x = g^y mod p$$

for some large prime number p. Cryptography with an elliptic curve defined over finite field $\mathbb{F}_q$ has a similar problem, the problem of finding integer k given a base point P where the point

$$Q = kP$$

here P,Q $\in E(\mathbb{F}_q)$,
This is called elliptic curve discrete logarithm problem or ECDLP.(Instead of numbers, elliptic curve's problem operate on points, and multiplication is used instead of exponentiation)
In other words given an elliptic curve E defined over a finite field F_q and two points P.Q $\in E(F_q)$ find an integer k such that Q= kP.

4.1.2 Elliptic Curve Diffie Hellman

[1] Given some fixed number g, Alice picks a secret random number a, computes X= g^a and sends Bob and Bob picks secret random number b and sends Y=g^b to Alice.
Both then compute secret key with the other's public key to produce same XY=YX=g^{ab}.
In case of ECC.

- Alice picks a secret number a, computes X=aP (point P multiplied by a) and sends X to Bob.
- Bob picks a secret random b, computes point Y=bP and sends Alice.
- both compute same shared secret XY = abP This method called Elliptic Curve Diffie Hellman or ECDH.

This method is called Elliptic Curve Diffie Hellman or ECDH. ECDH is to ECDLP what DH is to DLP its as secure as ECDLP is hard, DH protocols that rely on DLP can therefore be adapted to work with elliptic curves and rely on ECDLP as a hardness assumption.

4.2 Algorithm for ECC

[8] The steps in the ECC Algorithm are as follow:

Step 1: Encode plain text message as a point on curve

Let us consider a point to be encoded plain text message on the curve.

Step 2: Establish Public key and private key

- Choose a generator point G $\in E_p(a,b)$
- Suppose User B wants to send user A a message.
- User A will generate his private key n_A and public key P_A.
- Using the shared public key of user A user B will encrypt his message.
- Secret key k is generated by user B which lies in $\{1,2,3,\cdots,p-1\}$

Step 3: Encrypt message using public key Cipher point will be

C_m = { kG, P_m + kP_A }

this point will be sent to receiver.

Step 4: Decrypt using private key For decryption multiply first point in the pair with receiver's private key

Example: 4.2.0.1. *Suppose Alice and Bob want to share some message between each other. First they agree on a common curve. Consider the* *curve to be* $y^2 = x^3 + x + 1 \quad mod\ 11$

The point to encode plain text message on the curve is (4,6)

Alice wants to send bob a message. Since for encryption we need public key and decryption private key first bob will compute both. He first chooses a generator point G to be (1,5) $\in E_{11}(1,1)$

Next He chooses her private key $n_b = 2$ *and computes public key to be* P_b

$$P_b = 2G = G + G = (1,5) + (1,5)$$

$$\begin{aligned} \lambda =& \frac{3*1^2+1}{2*5} \quad mod\ 11 \\ =& \frac{4}{10} \quad mod\ 11 \\ =& 7 \\ Next, x_3 =& \lambda^2 - x - x \quad mod\ p \\ =& 7^2 - 1 - 1 \quad mod\ 11 \\ =& 47 \quad mod\ 11 \\ =& 3 \\ y_3 =& \lambda(x - x_3) - y \\ =& 7(1-3) - 5 \quad mod\ 11 \\ =& -19 \quad mod\ 11 \\ =& 3 \end{aligned}$$

Hence P_b= (3,3)

Now since Alice wants to send him a message he shares his public key P_b with Alice. Suppose secret key generated by Alice is 2. Then the cipher text generated will be

$$C = (kG, M + kP_b)$$

which on computation yields to [(3,3),(4,5)].

Cipher key can be seen as C=[C_1, C_2].

To decrypt it the receiver will multiply its private key to C_1 and subtract it from C_2 thus giving:

$$M = C_2 - n_B C_1 =$$

$$(4,5) - 2(3,3) = (4,5) - (6,5) =$$

$$(4,5) + (6,-5)$$

which on computation yields in (4,6) which is the original message.

4.3 Comparison between ECC and RSA

The biggest differentiation between ECC and RSA is key size compared to cryptographic strength This section is referred from [8] The key of RSA Cryptography is obtained by the product of lage prime numbers which there after results in a larger number is a public key which is difficult to

Symmetric Key size (bits)	RSA Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

dissemble. However the efficiency of generating two large prime numbers is lower than that of elliptic curve cryptography.

Elliptic Curve Cryptography (ECC) uses inverse operation of addition in an elliptic curve as the key and can achieve high encryption without complex operation so its efficiency is relatively higher. Main advantages of ECC over RSA are as follow:

Firstly, ECC has better security level. The Elliptic Curve Cryptosystem provides stronger protection and is better than other encryption algorithms at preventing attacks, making websites and infrastructure more secure than traditional encryption methods.

Secondly, ECC is better for mobile internet. ECC has a relatively shorter key of 256 bits so it takes up less storage. As more and more users use mobile devices for various online activities ECC provides better customer experience.

Thirdly, ECC can provide better security with shorter key lengths. For example the key strength of 256 bit elliptic curve is same as that of 3072 bit RSA key. According to the tests of relevant foreign authorities, response time of web server is more than 10 times faster than RSA when using ECC Algorithm on IIS servers.

4.4 Application of ECC

Elliptic Curve Digital Signature Algorithm This section is referred from [7] A signature doesn't refer to real signature but a private key "signs" certain information. Other people can verify information is actually signed by user A through user A's public key.

Alice wants to sign a document m, which is an integer. Alice chooses an Elliptic Curve over a finite field F_q . she chooses a base point G in $E(F_q)$ of order r. Finally Alice chooses a secret number a and computes Q=aG. Alice makes public the following information

$$F_q, E, r, G, Q$$

To sign message Alice does the following

1. Chooses a random integer with $1 \leq k \leq r$ and computes R= kG= (x,y)
2. Computes $s = k^{-1}(m+ax)(modr)$

The signed document is (m, R, s) To verify the signature, Bob does the following

1. Computes $u_1 = s^{-1}m(modr)$ and $u_2 = s^{-1}x(modr)$
2. Computes V= $u_1G + u_2Q$
3. Declares signature is valid if V=R

If the message is signed correctly verification equation holds

$$V = u_1G + u_2Q = s^{-1}mG + s^{-1}xQ = s^{-1}(mG + xaG) = kG = R$$

The main difference between ECDSA and Elgamal system is the verification process.

Chapter 5

CONCLUSIONS

In **Chapter 2** we have have seen the definition of Elliptic curve and how it is defined on Real field $\mathbb{R}$, Rational field $\mathbb{Q}$ and finite field $\mathbb{F}_{|}$ where p is a prime.

The curve defined on a finite field is not a smooth curve. However Elliptic curves defined on Finite fields play a major role in Cryptography which we see in the chapter 4. Basic Operations like point addition, point doubling and point at infinity are mentioned in this chapter

In **Chapter 3** Cryptography, in this modern times plays a key role to safeguard the information being shared between two parties being leaked by a third person. In this Chapter we learn about the different cryptosystems. One of the most widely used Asymmetric Cryptographies is the RSA Cryptography about which we learn here.

Diffie -Hellman is an Algorithm in which two people can exchange keys. Diffie Hellman is however not used to encrypt or Decrypt data. And Discrete logarithms are quickly computable in a few special cases, however, no efficient method is known for computing them in general. In cryptography, the computational complexity of the discrete logarithm problem and its application, was first proposed in the Diffie–Hellman problem. The complexity of Discrete Logarithm Problem defines how strong the cryptography is.

In **Chapter 4** In this chapter we come to the main topic of our paper that is cryptography using Elliptic Curves. Small key sizes make ECC very appealing for devices with limited storage pr processing power which are becoming common in the IoT. Application of elliptic curve cryptography in internet digital signature and SM2 are very efficient. References taken from [3] [4]

Bibliography

[1] Moses Aweda. “CRYPTOGRAPHY ON ELLIPTIC CURVES”. In: (Dec. 2021).

[2] explaincbot. *Secp256k1 : A Key Algorithm in Cryptocurrencies*. Tech. rep. Aug. 2023. URL: https://www.nervos.org/knowledge-base/secp256k1_a_key%20algorithm_(explainCKBot).

[3] Vivek Kapoor, Vivek Abraham, and Ramesh Singh. “Elliptic curve cryptography”. In: *Ubiquity* 2008 (May 2008), p. 7. DOI: 10.1145/1378355.1378356.

[4] Bilel Selikh. “On elliptic curves and application to cryptography”. PhD thesis. Aug. 2023. DOI: 10.13140/RG.2.2.25775.10405.

[5] Joseph H Silverman. “An introduction to the theory of elliptic curves”. In: *Brown University. June* 19 (2006), p. 2006.

[6] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*. Vol. 9. Springer, 1992.

[7] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. CRC press, 2008.

[8] Yuhan Yan. “The Overview of Elliptic Curve Cryptography (ECC)”. In: *Journal of Physics: Conference Series* 2386 (Dec. 2022), p. 012019. DOI: 10.1088/1742-6596/2386/1/012019.