Elliptic Curve Cryptography

Dissertation

Integrated Masters of Science
In
Applied Mathematics

Submitted by
Harsh Kumar Chourasia

supervised by
Dr. Ram Krishna Panday

Department of Mathematics
Indian Institute of Technology, Roorkee
Department of Mathematics
Roorkee-247667

Declaration

I hereby certify that the work which is being presented in the thesis entitled **Elliptic Curve Cryptography** in the partial fulfillment of the requirement for the award of the degree of Integrated Master of Science in Applied Mathematics and submitted to the Department of Mathematics, Indian Institute of Technology Roorkee, is an authentic record of my own work carried out during a period from January 2022 to April 2022 under the supervision of **Dr. R.K. Panday**, Associate Professor, Mathematics Department, Indian Institute of Technology Roorkee. The matter presented in this report has not been submitted by me for the award of any other degree of this or any other institute.

Harsh Kumar Chourasia
I. M.Sc, Applied Mathematics
Department of Mathematics
IIT Roorkee
Date:
Place:

CERTIFICATE

This is certified that the above statement made by the candidate is correct to the best of my knowledge.

Dr. RK Panday
Associate Professor
Department of Mathematics
IIT Roorkee
Date:
Place:

Abstract

This text discuss about Cryptography using Elliptic Curves. It has many practical applications end-to-end encryption, data and password storing, cryptocurrencies

Acknowledgments

I would like to thank my supervisor, Ram Krishna Panday, Department of Mathematics, Indian Institute of Technology Roorkee for his guidance through each stage of the process.

I would finally like to thank Prof Premananda Bera, Head of Department, Department of Mathematics, Indian Institute of Technology for giving me the permission to carry out this work at IIT Roorkee

Harsh Kumar Chourasia
I. M.Sc, Applied Mathematics
Department of Mathematics
IIT Roorkee
Date:
Place:

Contents

Chapter 1

Pre-requisite

This chapter covers topics of Abstract Algebra and Number Theory that are required for cryptography and elliptic curves.
This definition of Group, Ring, Field are as follows

1.1 Group

The set G is equipped with single operation $*$ such the the 4 below properties are satisfied is called a Group.
(1) Closure: $\forall x, y \in G, x * y \in G$
(2) Additive identity: $\exists 0 \in G$, such that $\forall x \in G$, $0 * x = x * 0 = x$
(3) Associative Property: $\forall x, y, z \in G$, $(x * y) * z = x * (y * z)$
(4) Inverse: $\forall x \in S, \exists y \in G$ such that$x * y = 0$ where y is known as inverse of x and is denoted by x^{-1}

1.1.1 Abelian Group

The set G is equipped with single operation $*$ such the the 5 below properties are satisfied is called a Abelian Group.
(1) Closure: $\forall x, y \in G, x * y \in G$
(2) Additive identity: $\exists 0 \in G$, such that $\forall x \in G$, $0 * x = x * 0 = x$
(3) Associative Property: $\forall x, y, z \in G$, $(x * y) * z = x * (y * z)$
(4) Commutative Property: $\forall x, y \in G$, $x * y = y * x$
(5) Inverse: $\forall x \in G, \exists y \in G$ such that $x * y = 0$ where y is known as inverse of x and is denoted by x^{-1}

So, a abelian group G is a group with $\forall x, y \in G, x * y = y * x$

1.2 Ring

A ring is a set R with two operations $+$ and $*$ which satisfy the below properties
(1) It is abelian group under $+$
(2) Closure under $*$: $x, y \in R \Rightarrow x * y \in R$
(3) Associative under $*$: $x, y, z \in R \Rightarrow (x * y) * z = x * (y * z)$
(4) Distributive property $x, y, z \in R$

$$x * (y + z) = x * y + x * z$$

$$(x + y) * z = x * z + y * z$$

1.3 Field

A Field is a set F with two operations $+$ and $*$ with following properties
(1)Commutative group under $+$
(2)Commutative group under $*$
(3)Distributive property $x, y, z \in F$

$$x * (y + z) = x * y + x * z$$

$$(x + y) * z = x * z + y * z$$

1.4 Fermat's little theorem

Theorem: Let p be any prime number. For any number a such that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$
Proof: Assume p is a prime number and $p \nmid a$
Every integer is congruent to one of $0, 1, 2, \cdots, p-1 \pmod{p}$
Only focus on non zero congruence classes, because $0 \pmod{p}$ contains all the multiples of p (and $p \nmid a$). Focus on $0, 1, 2, \cdots, p-1$
Multiply all of these by a:

$$a, 2a, \cdots, (p-1)a$$

Show that this is a rearrangement of $0, 1, 2, \cdots, p-1$
Case 1: None of these are congruent to 0.
Suppose $r.a \equiv 0 \pmod{p}$
Then $p \nmid r.a$, but this is impossible since $p \nmid a$ and $r < p$
Case 2: These are distinct, no two are congruent to each other.

Pick two values $r.a$,$s.a$

$$0 < r < p$$

$$0 < s < p$$

Let's show that $r.a \not\equiv s.a \pmod{p}$
So look at $r.a - s.a = (r - s).a$. As $p \nmid a$, so can $p \mid (r - s)$?

$$0 < r < p$$

$$-p < -s < 0$$

Adding these inequalities gives you:

$$-p < r - s < p$$

So, $p \nmid (r - s)$ which means $a, 2a, \cdots, (p-1)a$ is a rearrangement of $1, 2, \cdots, (p-1)$.

$$a, 2a, \cdots, (p-1)a \equiv 1, 2, \cdots, (p-1) \pmod{p}$$

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$$

$$a^{p-1} \equiv 1 \pmod{p}$$

Chapter 2

Elliptic Curves and Cryptography

2.1 Introduction to Cryptography

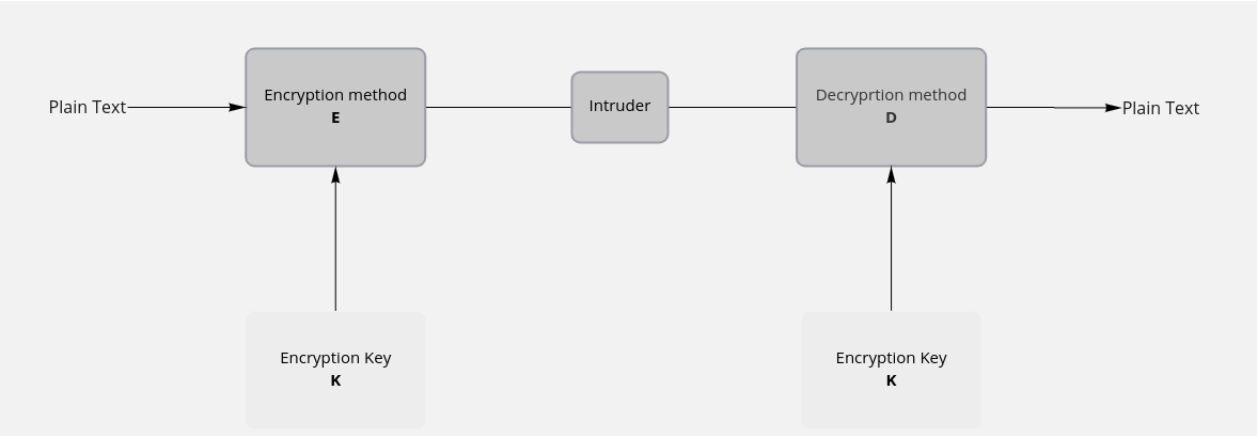
According to Wikipedia, **Cryptography, or cryptology is the practice and study of techniques for secure communication in the presence of adversarial behavior.**
Some of the application of Cryptography includes:

- End-to-end Encryption for e-mail, messaging apps, GSM phones.
- Storing Data: Biggest consumer application of cryptography includes Kindle, iPod which stores books and songs in encrypted format to protect copyright.
- Storing Password: Storing passwords in plane text is not secure. If an attacker has access to the system they can read the password. If the password is converted into hash using one way mapping function and stored. Every time a user logs in, the password will be converted into hash and compared with the stored password.

There are mainly two type of cryptography: Symmetric key cryptography and Asymmetric key cryptography.

2.1.1 Symmetric cryptography

Let Alice want to share a message m with Bob. They do so by using a common key and knowledge of some algorithm to encrypt and decrypt message. Alice encrypts the message using the key to produce the cipher text. Now Bob can use key with cipher text to decrypt message.



2.1.2 Asymmetric cryptography

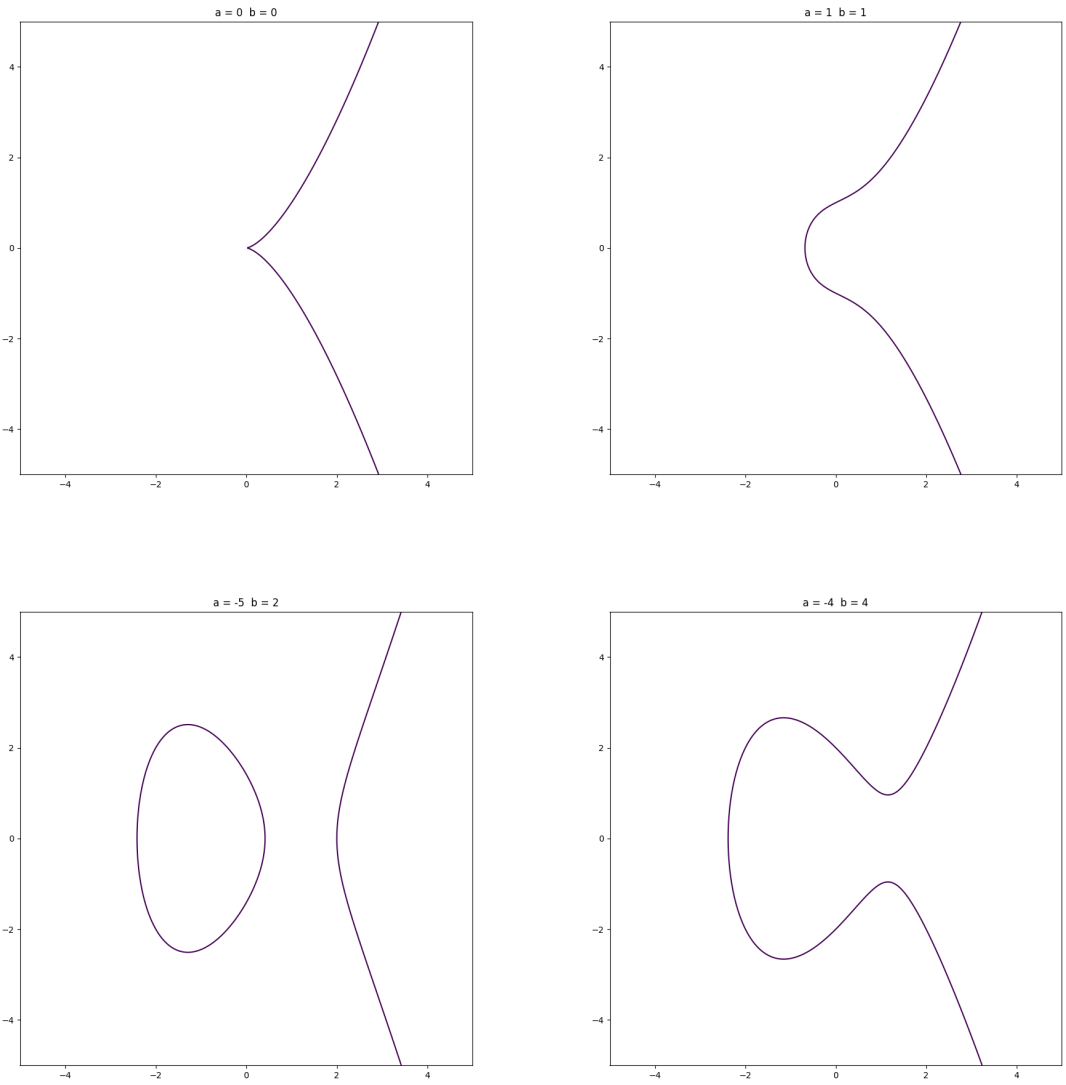
Asymmetric cryptography works by using private and public key pairs. Each user has a private,public key pair. Public key can be shared freely across the network and is used to verify the owner of a message. Private keys is not transmitted across the network. Private are used to encrypt the message. The major advantage of asymmetric cryptography is that there is no need of a shared key.

2.2 Elliptic Curves

Equation of type $y^2 = x^3+ax+b$ are called Weierstrass equations. It is named after Karl Weierstrass $(1815 - 1897)$ who studied them in 19^{th} century.
Definition:Elliptic curves are solution sets of Weierstrass equations

$$E : y^2 = x^3 + ax + b...(1)$$

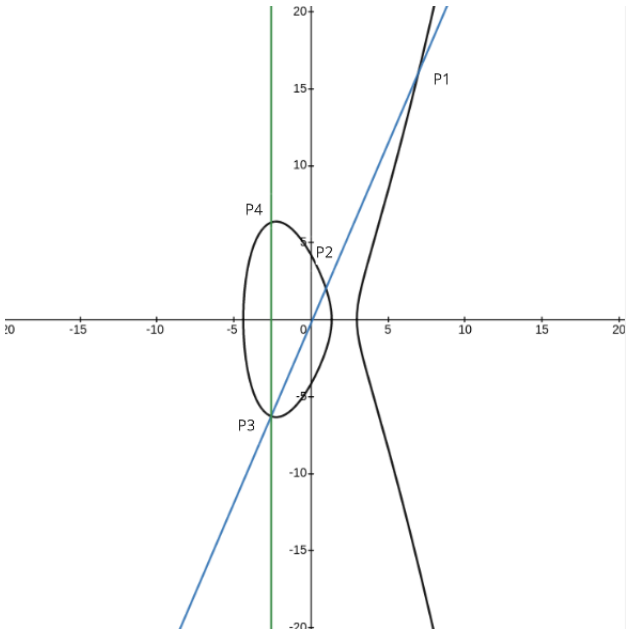
with $\{ \mathscr{O} \}$ where $\Delta_E = 4a^3+27b^2 \neq 0$. $\Delta_E \neq 0$ guarantees that the equation $x^3 + ax + b$ has no repeated roots i.e. $x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3)$ where e_1, e_2, e_3 are distinct



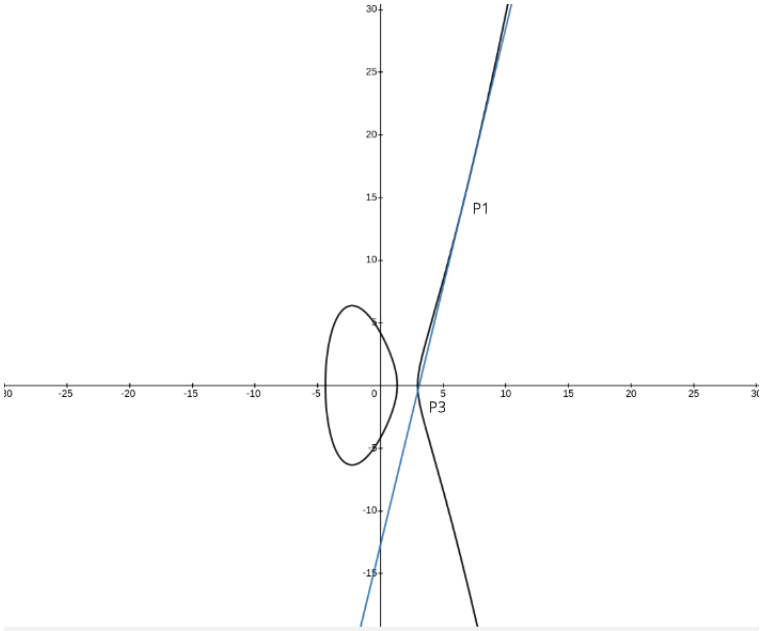
If (x,y) satisfies eq(1), then (x,-y) is also a solution of equation (1). So, elliptic curves are symmetric about x-axis.
The definition of addition "+" operator is a not the usual definition one might expect

$$(a, b) + (c, d) \neq (a + c, b + d)$$

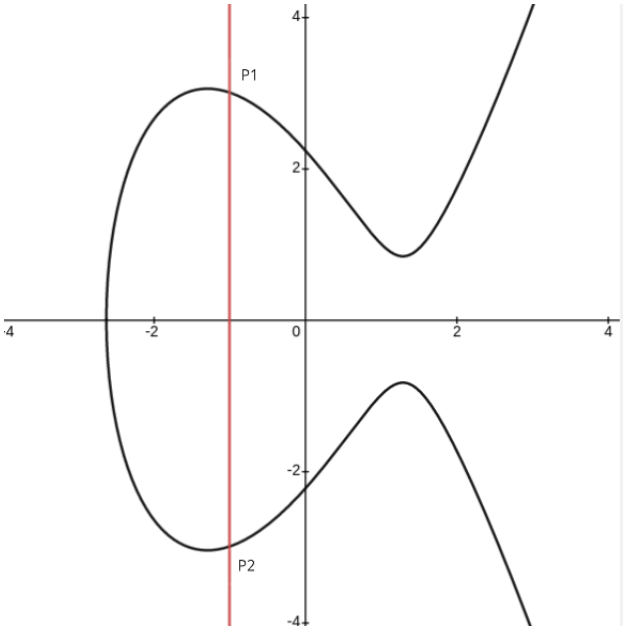
Two points P_1 and P_2 on elliptic curve. If we make a line L that passes through P_1 and P_2, it will intersect the curve at point $P_3 = (x_3, y_3)$. The reflection of P_3 from x-axis i.e. $(x_3, -y_3)$ is called the sum of points P_1 and P_2



So, what is $P_1 + P_1$? This is the limiting case where $P_2 \to P_1$ and the Line L becomes the tangent to E at P_1. This line will intersect E at P_2. The reflection of P_2 is $P_1 + P_1$.



What is happened when we try to add two points on the curve when $P_1 = (x, y)$ and $P_2 = (x, -y)$. In this case line L is $x = a$. L will not intersect the curve at third point. In this case we define $P_1 + P_2 = \mathscr{O}$. We define $\mathscr{O}$ as the point in infinity that lies on every vertical point.
$P + \mathscr{O} = P$



Theorem: Let E be Elliptic curve. Then E forms abelian group under addition. The following below statements are true:

1. $P_1 + \mathscr{O} = \mathscr{O} + P_1 = P_1$ for all $P_1 \in E$
2. $P_1 + (-P_1) = \mathscr{O}$ for all $P_1 \in E$
3. $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for all $P_1, P_2, P_3 \in E$
4. $P_1 + P_2 = P_2 + P_1$ for all $P_1, P_2 \in E$

2.3 Elliptic Curves over Finite Field

2.4 Discrete Logarithm problem

2.4.1 The elliptic curve discrete logarithm problem

2.4.2 Double and add algorithm

2.4.3 How hard is the ECDLP?

2.5 Elliptic curve cryptography

2.6 Diffie–Hellman

2.6.1 Diffie–Hellman key exchange

[**?**]