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.

Abstract

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.

Contents

Chapter 1

Pre-requisite

This chapter covers topics of Abstact Algebra and Number Theory that are required for cryprography and elliptic curves.
This defination 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) Commutatitve 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

Chapter 2

Elliptic Curves and Cryptography

2.1 Introduction to Cryptography

2.1.1 Symmetric ciphers

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 ciphers

2.2 Elliptic Curves

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

[1]

Bibliography

[1] Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman, and Joseph H Silverman. An introduction to mathematical cryptography. 1, 2008.