International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-5, August 2015
ISSN: 2395-3470
www.ijseas.com

Complexity Analysis Of Improved ECC Algorithm

VIVEK, RAHUL OLYAN And SACHIN MALIK
Students
Amity School of Engineering And Technology

ABSTRACT:- The ECC is public key cryptosystem .It based on the discrete logarithm problem. ECC has a high level of security which can be achieved with considerably shorter keys than other conventional public key cryptography. This project focuses on the improvements of ECC algorithm and how they effect on the overall complexity in space and time .The algorithm developed in the minor project on ECC is first improved in terms of security and performance by developing new modules and then comparing previously developed and new improved ECC algorithm. Two different algorithms of ECC are to be implemented and compared on the basis of their overall complexity using MATLAB and Hardware description language.

Index Terms:- Secret Key Cryptography, Elliptic Curve Cryptography (ECC), public key cryptography

INTRODUCTION

Cryptography is the science of keeping information secure. It involves encryption and decryption of messages. Encryption is the process of converting a plain text into cipher text and decryption is the process of getting back the original message from the encrypted text. Cryptography, in addition to providing confidentiality, also provides Authentication, Integrity and Non-repudiation.

There have been many known cryptographic algorithms. The crux of any cryptographic algorithm is the "seed" or the "key" used for encrypting/decrypting the information. Many of the cryptographic algorithms are available publicly, though some organizations believe in having the algorithm a secret. The general method is in using a publicly known algorithm while maintaining the key a secret.Based on the key, cryptosystems can be classified into two categories: Symmetric and Asymmetric. In Symmetric Key Cryptosystems, we use the same key for both Encryption as well as the corresponding decryption. i.e. if K was the key and M was the message, then, we have $D_K(E_K(M)) = M$

Asymmetric or Public key or shared key cryptosystems use two different keys. One is used for encryption while the other key is used for decryption. The two keys can be used interchangeably. One of the keys is made public (shared) while the other key is kept a secret. i.e. let k1 and k2 be public and private keys respectively. Let M be the message, then $D_{k2}(E_{k1}(M)) = D_{k1}(E_{k2}(M)) = M$ In general, symmetric key cryptosystems are preferred over public key systems due to the following factors:

PROPOSED METHOD DESCRIPTION

Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. An elliptic curve is usually defined to be the graph of an equation

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

where x, y,A and B belong to a specified field. These curves are of great use in a number of applications, largely because it possible to take two points on such a curve and generate a third. In fact, we will show that by defining an addition operation and introducing an extra point, 1, the points on an elliptic curve form an additive abelian group. Such a group can then be used to create an analogue of the discrete logarithm problem which is the basis for several public key cryptosystems. This project will introduce the mathematics behind elliptic curves and then demonstrate how to use them for cryptography.

Finite Fields

A field of a finite number of elements is denoted F_q or GF(q), where q is the number of elements. This is also known as a Galois Field.

The order of a Finite field F_q is the number of elements in F_q. Further, there exists a finite field F_q of order q iff q is a **prime power**, i.e. either q is prime or $q = p^m$, where p is prime. In the latter case, p is called the characteristic of F_q and m is called the extension degree of F_q and every element of F_q is a root of the polynomial

Let us consider two classes of Finite fields F_p (Prime Field, p is a prime number) and F_{2^m} (Binary finite field). The efficient implementation of finite field arithmetic is an important prerequisite in elliptic curve system because curve operations are performed using arithmetic operations in the underlying field. Three kinds of fields that are especially amenable for the efficient implementation of elliptic curve systems are prime fields, binary fields, and optimal extension fields. Efficient algorithms for software implementation of addition, subtraction, multiplication and inversion in these fields are discussed at length.

2.1.2) Elliptic Curves

Elliptic curves have, over the last three decades, become an increasingly important subject of research in number theory and related fields such as cryptography. They have also played a part in numerous other mathematical problems over hundreds of years. For example, the congruent number problem of finding which integers n can occur as the area of a right angled triangle with rational sides can be expressed using elliptic curves. In this chapter we set out the basic mathematics of elliptic curves, starting with their derivation and definition followed by the proof that points upon them form an additive abelian group. Elliptic curves are not ellipses, instead, they are cubic curves of the form

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

Elliptic curves over R^2 (R^2 is the set R x R, where R = set of real numbers) is defined by the set of points (x, y) which satisfy the equation $y^2 = x^3 + Ax + B$ along with a point O, which is the point at infinity and which is the additive identity element. The curve is represented as E(R).

The following figure is an elliptic curve satisfying the equation $y^2 = x^3 - 3x + 3$.

PROPOSED ALGORITHM

genPoints (a, b, p)
{

x=0;
While(x <p)
$y^2 = (x^3 + ax + b) \bmod p$;
if (y^2 is a perfect square in GF(p))
output[(x,√y) , (x, -√y)];
x=x+I;
}
{

Key Distribution

Let U_A and U_B be legitimate users
$U_A = \{P_A, n_A\}$ --Key pair for U_A
$U_B = \{P_B, n_B\}$ -- Key pair for U_B
Send the Public key of U_i , to U_A
Send(P_B,U_A);
Send the Public key of Ux to U_B
Send (P_A, U_B);

Encryption at A

$P_{m1} = aP_m$
-- a: Ascii value of text
-- P_m: random point on EC
$P_B = n_B * G$
-- G is the base point of EC
-- n_B is the private key
CipherText={k_G,P_{ml}+k*P_B}

Decryption at B

Let k_G be the first point and
Pml + k*P_B be the second point
n_B k_G = n_B * first point;
Calculate $P_{ml} = P_{ml} + kP_B - n_B k_G$;
Calculate the P_m value from P_{ml}
using discrete logarithm.

Improved Algorithm

Let x(i) be the point computed by algorithm , lying on the Curve.
for i= 0 to k-1
x(i) = m * k + i
if (X == x(i))
else i = i+1
Point on the curve to map the ASCII value is calculated.

IMPLEMENTATION OF THE PROPOSED ALGORITHM

ECC Arithmetic Operations

An elliptic curve $E(F_p)$ over a finite field F_p is defined by the parameters a, b $\in F_p$ (a, b satisfy the relation $4a^3 + 27b^2 \neq 0$), consists of the set of points (x, y) $\in F_p$, satisfying the equation $y^2 = x^3 + ax + b$. The set of

points on $E(F_p)$ also include point **O**, which is the point at infinity and which is the identity element under addition.

The Addition operator is defined over $E(F_p)$ and it can be seen that $E(F_p)$ forms an abelian group under addition.

The addition operation in $E(F_p)$ is specified as follows.

- $P + O = O + P = P, \forall P \in E(F_p)$
- If $P = (x , y) \in E(F_p)$, then $(x, y) + (x, - y) = O$. (The point $(x, - y) \in E(F_p)$ and is called the negative of P and is denoted -P)
- If $P = (x_1, y_1) \in E(F_p)$ and $Q = (x_2, y_2) \in E(F_p)$ and $P \neq Q$, then $R = P + Q = (x_3, y_3) \in E(F_p)$, where $x_3 = m^2 - x_1 - x_2$, $y_3 = m (x_1 - x_3) - y_1$, and (m is slope)

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

i.e. the sum of 2 points can be visualized as the point of intersection $E(F_p)$ and the straight line passing through both the points.

- Let $P = (x, y) \in E(F_p)$. Then the point $Q = P + P = 2P = (x_1, y_1) \in E(F_p)$,

where $x_1 = m^2 - 2x$, $y_1 = m (x - x_1) - y$, where $m = (3x^2 + a) / 2y$.

This operation is also called doubling of a point and can be visualized as the point of intersection of the elliptic curve and the tangent at P.

We can notice that addition over $E(F_p)$ requires one inversion, two multiplications, one squaring and six additions. Similarly, doubling a point on $E(F_p)$ requires one inversion, two multiplication, two squaring and eight additions. if given a point P(x, y) on an EC, one needs to compute kP, where k is a positive integer.

This is achieved by a series of doubling and addition of P.

Say, given k =13, entails the following sequence of operations, by which the efficiency of the scalar multiplication of the points is improved

ELLIPTICAL CURVE DISCRETE LOGARITHM PROBLEM

The strength of the Elliptic Curve Cryptography lies in the Elliptic Curve Discrete Log Problem (ECDLP). The statement of ECDLP is as follows.

Let E be an elliptic curve and $P \in E$ be a point of order n. Given a point $Q \in E$ with

$$Q = mP, \text{ for a certain } m \in \{2, 3, \ldots\ldots, m - 2\}.$$

Find the m for which the above equation holds.

When E and P are properly chosen, the ECDLP is thought to be infeasible. Note that m = 0, 1 and m - 1, Q takes the values O, P and - P. One of the conditions is that the order of P i.e. n be large so that it is infeasible to check all the possibilities of m.

DISCUSSIONS & CONCLUSION

In this paper, a text based Elliptic Curve
Cryptosystem is implemented. The Lookup table consisting of the ASCII values mapped with the points on the ECC curve has been replaced by an algorithm**.** It is Concluded in this report that new Improved ECC provides greater security also the new ECC is more dynamic , flexible in terms data formats and inputs.The new algorithm has two base point two level encryption technique.The implementation of the ECC algorithm on hardware using vhdl provides an insight on the performance of the algorithm on the hardware

ACKNOWLEDGEMENT

We owe a great many thanks to a great many people who helped and supported me during the writing of this report. My sincere and genuine thanks go to **Mrs. Pinki Nayak** (HOD Department of ECE ASET , New Delhi) for providing us with the opportunity for the final year project report.

Our deepest thanks to **Mr. Deepak Gambhir,** the Guide of the project for guiding and correcting various documents with attention and care. He has taken pain to go through the project and make necessary correction as and when needed.

Lastly, we would like to acknowledge everybody who though remain unmentioned yet have been connected with our project.

We would also thank other members without whom this project would have been a distant reality. We also extend our heartfelt thanks to my family and well wishers.

REFERENCES

[1] Koblitz N., Menezes A.J., and Vanstone S.A. The state of elliptic curve cryptography. Design, Codes, and Cryptography. Vol 19, Issue 2-3, 2000, page 173-193.

[2] A. Karatsuba and Y. Ofman, Multiplication of multi digit numbers on automata, Sov. Phys. Dokl., Vol.7, 1963, 595-596.

[3] Nedjah, N. and Mourelle, L.M. (Eds.), Embedded Cryptographic Hardware: Methodologies and Applications, Nova Science Publishers, Hauppauge, NY, USA, 2004.

[4].S. Bajracharya, **C. Shu**, K. Gaj, and T. El-Ghazawi, Implementation of Elliptic Curve Cryptosystems over GF(2n) in Optimal Normal Basis on a Reconfigurable Computer.

[5]. Menezes A.J., Teske E., and Weng A. Weak fields for ECC.CORR 2003-15, Technical Report, University of Waterloo, 2003..