Elliptic Curve Cryptography: An Efficient Approach for Encryption and Decryption of a Data Sequence

Ankita Soni[1], Nisheeth Saxena[2]

[1]Mody Institute of Technology & Science University, FET, Laxmangarh, Rajasthan, India

[2]Mody Institute of Technology & Science University, CSE dept., FET, Laxmangarh, Rajasthan, India

Abstract: ***The paper describes the basic idea of Elliptic Curve Cryptography (ECC) and the use of Elliptic curves in Elliptic curve cryptography. This paper gives an introduction to elliptic curves and the basic operations of elliptic curves. Elliptic Curve Diffie Hellman (ECDH) key exchange protocol of ECC is described. The paper illustrates the procedure of Encryption and Decryption of message by first transforming the message into an affine point on the Elliptic Curve (EC), over the finite field GF(p). In ECC we normally starts with an affine point called $P_m(x,y)$ which lies on the elliptic curve[1]. And further the process of encryption and decryption of a text message is implemented. A comparison is performed between the encrypted text messages using different key sizes, to calculate the time consumed by each. The security strength of ECC lies in the unfeasibility of solving the ECDLP (Elliptic Curve Discrete Logarithmic Problem) [2].***

Keywords: Elliptic curve cryptography (ECC), Elliptic Curve (EC), Discrete Logarithm Problem (DLP), Elliptic Curve Diffie Hellman (ECDH).

1. Introduction

Elliptic Curve Cryptography was discovered in 1985 by Neil Koblitz [3] and Victor Miller [4]. ECC is a newer approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields, and considered as a marvelous technique with low key size for the user, and hard exponential time challenge for an intruder to break into the system. In ECC a 160 bits key, provides the same security as RSA [5] 1024 bits key, thus lower computation power is required. The advantage of elliptic curve cryptosystems is the absence of sub exponential time algorithms, for attack. As ECC uses less key size to provide more security, and for this advantage it is used to perform faster cryptographic operations, running on smaller chips or more compact software. The public key cryptography-based remote authentication schemes are not suitable for mobile devices, because of the limitation in the bandwidth, computational strength, power availability or storage in mobile devices. So, various authentication schemes based on elliptic curve cryptography (ECC) are proposed [6]. Elliptic curve cryptography emerged as an attractive public key crypto-system for mobile and wireless environments and also provides bandwidth savings. Elliptic curve cryptography is very difficult to understand by attacker. So it is difficult to break.

2. What makes ECC Important? The Discrete Logarithm

The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem.

Consider the equation Q = kP, where P, Q belong to E_p (A, B) and "k < p"

- If k and P are given, it is very easy to calculate Q.
- But if P and Q are given, it is relatively hard to determine k, if k is sufficiently large. k is the discrete logarithm of Q to the base P.

This is discrete logarithm Problem for Elliptic Curve [7] and due to the complexity of Discrete logarithm Problem Elliptic curve cryptography is hard to break. Hence the main operation involved in ECC is point multiplication. i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve.

3. What is Elliptic Curve? Its Derivation and Use

An elliptic curve is a smooth, projective algebraic curve, on which there is a specified point O, which called as point at infinity or ZERO POINT. Elliptic curves are not ellipses. They are named as Elliptic curves because they are described by cubic equations, or equations with highest degree 3. An elliptic curve E in its standard form is described as

$$y^2 = x^3 + ax + b$$

This is a cubic equation as highest degree of this equation is 3. Where, the values of 'a' and 'b' are predefined and $\mathbf{4a^3 + 27b^2 \neq 0}$. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve.

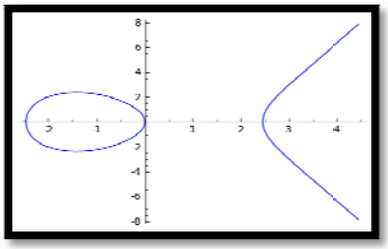

Figure 1: An elliptic curve (corresponding to the equation $y^2 = x^3 - 6x$)

3.1 EC Basic operations:

The basic operation of EC involves

- Point Multiplication
- Point Addition
- Point Doubling

3.1.1 Point Multiplication

The basic operations of elliptic curve involve point multiplication which is achieved by point addition and point doubling. In point multiplication a point on the Elliptic Curve say P is multiplied with a positive integer k to obtain another point Q on the same Elliptic curve, using Elliptic curve equations.

i.e. Q = KP
Let K = 29
So, Q = 29 P = 2(2 (2 ((P + P) +P) +P)) + P

So this example shows that point multiplication is accomplished by using point addition and point doubling repeatedly to get the result. This method is called as double and adds method. There are other efficient methods for point multiplication such as NAF (Non – Adjacent Form) and wNAF (windowed NAF) method for point multiplication [8].

3.1.2 Point Addition

It is the addition of two points of the elliptic curve; say P and Q, to get another point R on the same Elliptic curve.

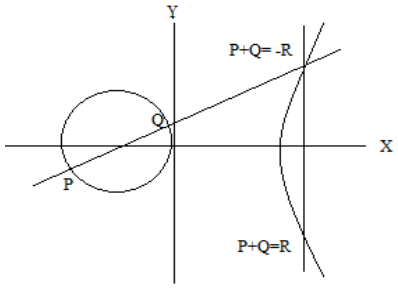

Figure 2: Point Addition

Geometric explanation

Consider 2 point P and Q on the Elliptic curve as shown in the figure 2. Then 2 conditions arises

- If Q =! -P, then a line drawn through the points P and Q will intersect the Elliptic curve at exactly one more point -R. The reflection of -R gives the point R, with respect to x axis. The R point is the result of addition of P and Q. Thus R = P+Q
- If Q = -P, the line through this point intersect at a point at infinity O.
- Hence Q + (-Q) = O, where O is additive identity of Elliptic curve group.

Analytical Explanation

Consider two distinct points $P(X_P, Y_P)$ and $Q(X_Q, Y_Q)$ .The slope of the line joining these two points is S.

$S = (Y_Q - Y_P)/(X_Q - X_P)$

As we know that R = P + Q, and R is also the point on EC so the coordinates of R (X_R, Y_R) are calculated by-

$X_R = S^2 - X_P - X_Q$

$Y_R = S(X_P - X_R) - Y_P$

3.1.3 Point doubling

Point doubling is the addition of a point say P to itself to get another point on the elliptic curve.
So R = P+P =2P

Geometric Explanation

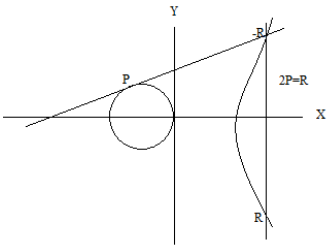

Figure 3: Point Doubling

To double a point P to get R, i.e. to find R = 2P, consider a point P on an elliptic curve as shown in figure 3. If Y coordinate of the point P is not zero then the tangent line at P will intersect the elliptic curve at exactly one more point -R. The reflection of the point -R with respect to X-axis gives the point R, which is the result of doubling the point P.

Thus R = 2P.
If Y coordinate of the point P is zero then the tangent at this point intersects at a point at infinity O. Hence 2P = O when Y = 0.

Analytical Explanation

Consider a point $P(X_P, Y_P)$ where $X_p \neq 0$
Let R = 2P, $R(X_R, Y_R)$
Then the coordinates of R $(X_R, Y_R)$are calculated by-

$X_R = S^2 - 2X_P$

$Y_R = S(X_P - X_R) - Y_P$

$S = (3 X_P^2 + a)/ 2 Y_P$

S is the tangent at point P and a is the parameter chosen with the elliptic curve.
If $Y_P = 0$, then 2P = O ,where O is the point at infinity or zero point.

3.2 Elliptic curves over Prime Field (F_P)

The cubic equation for Prime Field F_P is-

$Y^2 \bmod p = (X^3 + AX + B) \bmod p$, where $\mathbf{4A^3 + 27B^2 \bmod p \neq 0}$.

So the values of variables and coefficients of cubic equation are between 0 through p-1(set of integers), in this finite field.

All the operations as addition, subtraction, multiplication, division are performed in modular arithmetic and the values are chosen from 0 and p-1.to make cryptosystem more secure the Prime no p is chosen in a such way that there is finitely large number of points on elliptic curve. SEC

specifies curves with p ranging between 112-521[9]. The algebraic rules for point addition and point doubling can be adapted for elliptic curves over F_P. So the operations of elliptic curve over prime field F_P are described below

Point Addition

Consider two distinct points P and Q such that P = (X_P, Y_P) and Q = (X_Q, Y_Q)

Let R = P + Q where R = (X_R, Y_R), then

S = $((Y_P - Y_Q)/ (X_Q - X_P)) \bmod p$, S is the slope of the line through P and Q.

$X_R = (S^2 - X_P - X_Q) \bmod p$
$Y_R = (S (X_P - X_R) - Y_P) \bmod p$

- If Q = -P i.e. Q = $(X_P, -Y_P \bmod p)$ then P + Q = O. where O is the point at infinity.
- If Q = P then P + Q = 2P then point doubling equations are used. Also P + Q = Q + P

Point Subtraction
Consider two distinct points P and Q such that P = (X_P, Y_P) and Q = (X_Q, Y_Q)
Then P - Q = P + (-Q) where -Q = $(X_Q, -Y_Q \bmod p)$
Point subtraction is used in certain implementation of point multiplication such as NAF[8].

Point Doubling
Consider a point P such that P = (X_P, Y_P), where $Y_P \neq 0$
Let R = 2P where R = (X_R, Y_R), Then $S = ((3X_P^2 + a) / (2Y_P)) \bmod p$, S is the tangent at point P and a is one of the parameters Chosen with the elliptic curve.
$X_R = (S^2 - 2X_P) \bmod p$
$Y_R = (S(X_P - X_R) - Y_P) \bmod p$

- If $Y_p = 0$ then 2P = O, where O is the point at infinity.

Note: In the case of finite group E_p (a, b), the numbers of points N is bounded by[7]-
$\mathbf{p+ 1 -2\sqrt{p} \leq p + 1 + 2\sqrt{p}}$

4. Elliptic Curve Diffie Hellman(ECDH) Key Exchange Protocol

ECDH is a key agreement protocol that allows two communicating parties to generate a shared secret key. This shared secret key can be used for private key algorithms. To generate a shared secret key between M and N using ECDH, Both have to agree upon EC domain parameters mentioned earlier.

Note: Any third party, who doesn't have access to the private details of each device, will not be able to calculate the shared secret from the available public information.

An overview of ECDH process is defined below:

EC domain parameters used for the process are;

E_q (A,B): Elliptic curve with parameters A,B,q where q is the prime number or an integer of form 2^m
G: generator point on elliptic curve whose order is large value n.

Both the devices M and N have a key pair consisting of a private key P (a randomly selected integer less than n, where n is the order of the curve, an elliptic curve domain parameter) and a public key U = P * G (G is the generator point, an elliptic curve domain parameter).

The process of Key Exchange between M and N

1. M have a pair (P_M, U_M) , where $U_M = P_M * G$
2. N have a pair (P_N, U_N)., where $U_N = P_N * G$
3. M calculates its secret key $K = P_M * U_N$
4. N calculates its secret key $K = P_N * U_M$

NOTE: Secret Key generated by both the devices is same ,as-
$K = P_M * U_N = P_N * U_M$
$= P_M * P_N * G = P_N * P_M * G$

5. Proposed Method Description

5.1 Elliptic Curve Parameter Selection

To implement an elliptic curve cryptosystem, a number of decisions are made at different hierarchy levels depending on the underlying hardware and to achieve implementation goals.

- At the field level:
  - Selection of the underlying field (could be F_p , F_2^m or F_p^m).
  - Choosing the field representation (e.g., polynomial basis or normal basis).
  - Field arithmetic algorithms for field addition (subtraction), multiplication, reduction and inverse.

- At the elliptic curve level
  - Choosing the type of representation for the points (affine or projective co-ordinates).
  - Choosing a point addition and doubling algorithm.

- At the protocol level
  - Choosing the appropriate protocol (key-exchange or signature).
  - Choosing the algorithm for scalar multiplication *k * P*.

ECC becomes feasible for both constrained devices and high performance servers, as these choices provide a huge flexibility.

5.2 Selection of Domain Parameters

Before initiating the process of Encryption and transforming the encrypted text, there are certain parameters that must be agreed by both parties involved in secured and trusted communication using ECC. These are the Domain parameters.

The domain parameters for Elliptic curve over F_P are **p**, **a**, **b**, **G**, **n** and **h**.

Where, p is the prime number defined for finite field, a and b are the curve parameters.

G is the generator point/base point (X_G, Y_G) point on the elliptic curve chosen for cryptographic operations.
n is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between 0 and n – 1.
h is the cofactor where h must be small (h<= 4) and, preferably h=1.

5.3 Generating EC points (group elements):

An Elliptic Curve Equation is considered, to generate points or group elements of Elliptic Curve.

$Y^2 \bmod p = (X^3 + aX + b) \bmod p$

The algorithm used to generate EC points is
Algorithm pointsGen (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, sqrt(y)) (x, -sqrt(y));
x=x+1;
}

5.4 Implementing EC Operations

The Basic operations of EC are point addition, point doubling, and point multiplication as described earlier. These operations are performed with group elements or the EC points calculated using the algorithm pointsGen (a, b, p). All the operations are performed over Prime Field (F_P). It is mentioned in section 3.2 how to calculate the Slope and the new points (X, Y) of EC using these operations. These new points should be from the group elements of the EC.

5.5 Encryption and Decryption of Text Message

Now the final part consists of the process of Encryption and decryption of a text message/secret message which sender wants to send to receiver.

5.5.1 Selection of Domain Parameters and Curve Parameters

Firstly the unique values for Domain Parameters (p, n, G) and Curve Parameters (a, b) are selected. The most important factor Key size is also chosen it can be 192, 224, 256, 384, 521, 1024 etc. The value of p prime number, n order of curve and G base point depends on the value of key size. When these values are selected they are utilized in calculating Elliptic Curve points. The EC points are then calculated using the Algorithm pointgen (p,a,b).

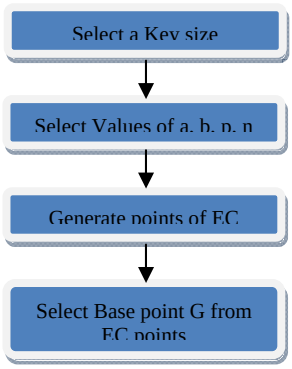

Figure 4: Block diagram for selection of Domain Parameters

5.5.2 Encryption Process

In the Encryption process it is explained that how the sender encrypts the secret message which she wants to send to receiver. Sender selects a random integer d that is between (1, n-1), where n is the order of the curve selected earlier. She than calculates Q =d* G, G is the base point chosen earlier. She sets her private key to the random number P_{r1} = d and public key P_{u1}= Q. As the text message is in characters and numbers, it is converted into bitstring and then divided into chunks for performing encryption. Each chunk is encrypted in the form of (Chosen point, Encoded Point). And then this Encrypted text (Chosen point, Encoded Point) is sent to receiver.

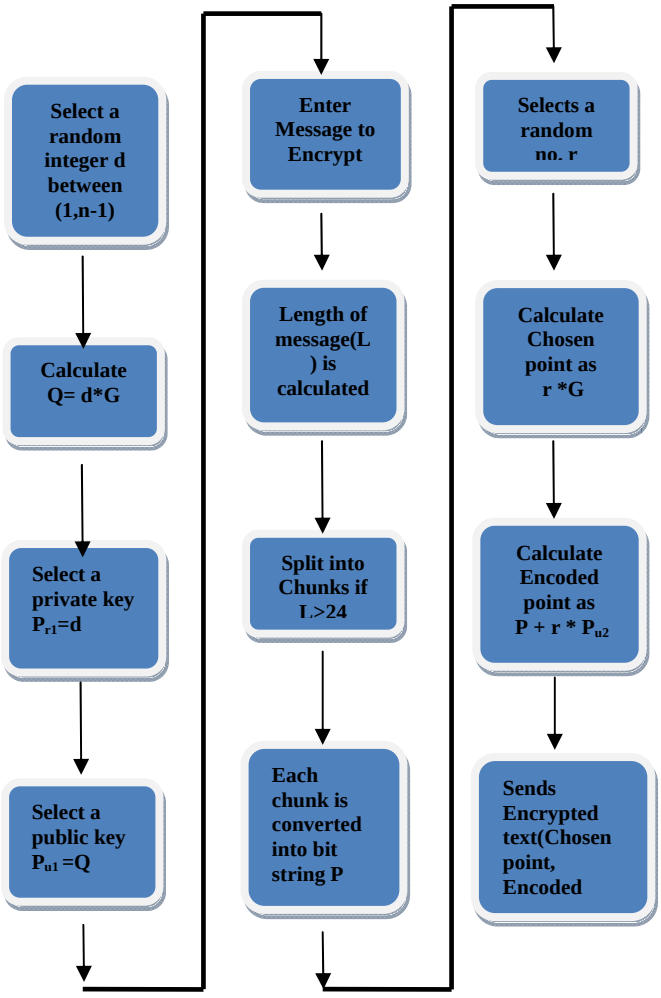

Figure 5: Block diagram of Encryption process

5.5.3 Decryption Process

The receiver also performs the calculation for choosing his private key P_{r2} and public key P_{u2}. The decryption is performed by the received encrypted text, as the encrypted text is received in chunks each chunk is decrypted one by one as messages[i].EncodedPoint – P_{r2}*messages[i].ChosenPoint

Then we get the result as bit strings, which are later converted into respective alphabet or number. And finally the send messaged is retrieved by the encrypted text.

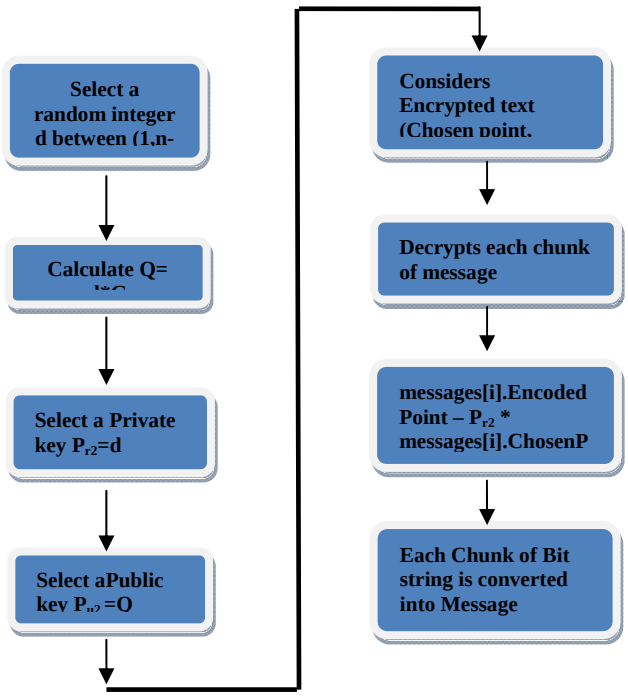

Figure 6: Block diagram of Decryption process

5.6 Key Size Comparison

After implementing the encryption and decryption modules, A new module will be generated. With the help of this module we can perform the analysis of the time consumed in encryption of a text of variable length using different key sizes. As ECC provides a wide variety of choices in various parameters before starting the encryption. So it is necessary to know that which key size should be used to encrypt a text of certain length particularly.

6. Applications

Elliptic curve cryptography is widely used in many of the areas. It is used in devices which have less storage memory. ECC is most popularly used in Smart cards. Smart cards are being used as bank (credit/debit) cards, electronic tickets and personal identification (or registration) cards. Many manufacturing companies are producing smart cards that make use of elliptic curve digital signature algorithms. ECC is used in wireless communications and in devices with low computing power and resources such as Mobile devices.

PDAs have more computing power compared to most of the other mobile devices, like cell phones or pagers. PDAs are considered to be a very popular choice for implementing public key cryptosystems. But ECC is idol choice for PDAs because they still suffer from limited bandwidth.

For implementing the ECC, Constrained devices have been considered to be the most suitable platforms. Recently, several companies have created software products that can be used on PCs to secure data, encrypt e-mail messages and even instant messages with the use of ECC.

7. Conclusion

ECC is a very encouraging and new field to work it provides more cost efficient method for encryption for devices which have less memory and to secure transmission over internet. As Elliptic curves are believed to provide good security with smaller key sizes and are more complex so they are used in Public key cryptography i.e. Elliptic curve Cryptography. In this study we have provided an overview of Elliptic Curves and their operations. The Elliptic curve operations are used for implementing Elliptic curve cryptosystem. It is important that the point multiplication and filed arithmetic should be efficient for efficient implementation of ECC. ECC provides a wide variety of range for choosing parameters to analyze particular module. The ECDH algorithm is mentioned later. And then the Further the implementation process is explained diagrammatically. We have also mentioned the application areas of ECC. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real time performance is a critical factor. But all Elliptic Curves are not used for cryptographic operations and for implementing cryptosystems, so this decision is not an easy task to choose appropriate Elliptic Curve.

References

[1] S. Maria Celestin Vigila, K. Muneeswaran, “Implementation of Text based Cryptosystem using Elliptic Curve Cryptography”, ICAC 2009

[2] Ping Wang et. al. , “An Efficient Collision Detection Method for Computing Discrete Logarithms with Pollard’s Rho”, Journal of Applied Mathematics Volume 2012

[3] N.Koblitz, Elliptic Curve Cryptosystems, *Mathematics of Computation*, volA8, 1987.

[4] V. S. Miller, “Use of Elliptic Curves in Cryptography”. Advances in Cryptology CRYPTO'85, New York, Springer-Verlag..

[5] Anoop MS, “Elliptic curve cryptography: An implementation Guide”.

[6] Konstantinos Chalkias et. al. , “Implementing Authentication Protocol for Exchanging Encrypted Messages via an Authentication Server based on Elliptic Curve Cryptography with the ElGamal’s Algorithm”, World Academy of Science, Engineering and Technology 7 2007

[7] W. Stallings, “Cryptography and Network Security”, Prentice Hall, Fourth Edition.

[8] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, “Software Implementation of Elliptic Curve Cryptography over Binary Fields, 2000”, Available at http://citeseer.ist.psu.edu/hankerson00software.html

[9] Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000, Available at http://www.secg.org/download/aid-386/sec2_final.pdf