Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 1 (2025)

An Approach for Cipher Communication Utilizing the Concepts of Elliptic Curve Cryptography

S. Sarvalakshmi[1*], CH. Suneetha[2]

[1*.] Research Scholar in Mathematics, GITAM (Deemed to be University), Visakhapatnam, India

[2.] Associate Professor in Mathematics, GITAM (Deemed to be University), Visakhapatnam, India

[1*]Corresponding Author Mail: radhika1483@gmail.com

Article History:

Received: *16-07-2024*

Revised: *30-08-2024*

Accepted: *11-09-2024*

Abstract:

Message encryption is a process of protection of the original data in transmission. Several cryptosystems were designed in the history for different environments. Public key or Asymmetric cryptosystem has become more popular in recent era where the key space consists both public and private keys. Elliptic curve cryptography dominates public key cryptosystems like Diffie Hellman key exchange and RSA. ECC is more powerful and alternative technique of RSA, with a simple replacement of exponent calculations of large prime numbers to mathematical representation of Elliptic curve points. Besides the computation ECC works with shorter key length than RSA. The present paper describes an encryption algorithm using elliptic curves over finite fields. Here a group of authentic users transmit.

Keywords: Elliptic curve cryptography, Elliptic curve points, Encryption Decryption, Generator.

1. Introduction:

Diffie Hellman Key Exchange Algorithm is a compelling protocol which utilizes exponentiation of huge groups to start an encrypted communication between two unknown communicators. It has been proposed as an internet standard and significantly enhances internet security. However, the algorithm affects from a security flaw known as a man-in-the-middle attack. Later, the Diffie Hellman Key Exchange algorithm was modified and published by several authors, on the other hand, RSA is a public key cryptosystem comes from the challenge of factorizing big integers into their prime. Even if the key size doubles, the RSA algorithm's strength will not increase although the public key operations being faster. Elliptic curve cryptography depends of the hardness of Elliptic Curve Discrete Logarithm Problem (ECDLP). The concept of elliptic curve Utilization in public key cryptography trailblazers were Koblitz and Miller. The main motive for attentive attraction of the researchers towards ECC is yields the level of security as RSA.

2. Literature Survey:

Numerous researchers employed elliptic curves over finite fields for security applications and researched the benefits of ECC over traditional cryptosystems. ECC-based text-based encryption techniques were proposed by several authors. When it comes to (Secure Sockets Layer) SSL and TLS certificates, Benjamin Clement Sebastian and Ugar Alpay Cenar [1] researched and compared the substantial advantages of ECC over RSA. Elliptic curve cryptography was used to implement text encryption by L. Dolendro and K. Manglem [2]. The writers of this chapter provided a conventional

way of mapping the characters to affine points in the curve by matching the ASCII values of the plain text characters. A proposed encryption method using elliptic curve cryptography was made by Renee Brady et al. [3]. They used Unicode to encrypt the text in that study and explored the drawbacks of sending text communications through platforms like Twitter. The text is encoded using the Koblitz method as a point on an elliptic curve. For users of online social networks, S. Thiraviya and S. Britto [4] suggested better elliptic curve cryptography. They used encryption, decryption time analysis, plain text, and cipher text size analysis in that paper. A. Shamir [5] was the first to suggest an Identity-based cryptosystem as an alternative to conventional public key infrastructure for resolving authenticity problems. A pre-communication requirement is part of the authentication system described by Aziz and Diffie [6]. The use of a nonsingular matrix to map the identical characters in the message to different positions on the curve was recommended by F. Amounas and E.H. EI Kinani [7]. Elliptic curves were suggested for encryption and decryption by Kolhekar M. and Jadhav A. [8], A. Gera and K. Agrawal [9].

Elliptic Curve Arithmetic

An irreducible cubic with a flex can be affinely transformed into a Weierstrass equation:

$Q^2 + a_1PQ + a_3Q = P^3 + a_2P^2 + a_4P + a_6$, where a_1a_2, a_3, a_4, a_6 are real and $P \in R$, $Q \in R$.The equation $y^2 = x^3 + ax + b$, $4a^3+27b^2 \neq 0$ over the finite field Fq defines an elliptic curve for cryptography purposes.

The points on the curve taking ∞, infinity point as identity element an abelian group with respect to point addition is formed

Point addition on the Curve: If $P(a_1,b_1)$ and $Q(a_2,b_2)$ are two points on the curve, $P + Q$ is obtained by taking the image or reflection of the point obtained by intersecting the line through P, Q with the curve. The reflection is considered about X-axis. For opposite points P and– P the vertical line is intersected through the curve.
The identity is $P + (-P) = \infty$. For $P(a_1,b_1), Q(a_2,b_2)$ $P + Q$ is $R(a_3,b_3)$

$$a_3 = \left(\frac{b_2-b_1}{a_2-a_1}\right)^2 - a_1 - a_1 - a_2$$

$$b_3 = \left(\frac{b_2-b_1}{a_2-a_1}\right)(a_2 - a_3) - b_1$$

Point multiplication or point doubling on the curve: - for the point $P(a_1, b_1)$, $2P$ is the image of the point obtained by intersecting the tangent through P with the curve. The image is about X- axis [1,2].
For $P \neq -P$, $2P$ is given by (a_3, b_3)

$$a_3 = \left(\frac{3{a_1}^2+a}{2b_1}\right)^2 - 2a_1$$

$$b_3 = \left(\frac{3{a_1}^2 + a}{2b_1}\right)(a_1 - a_3) - b_1$$

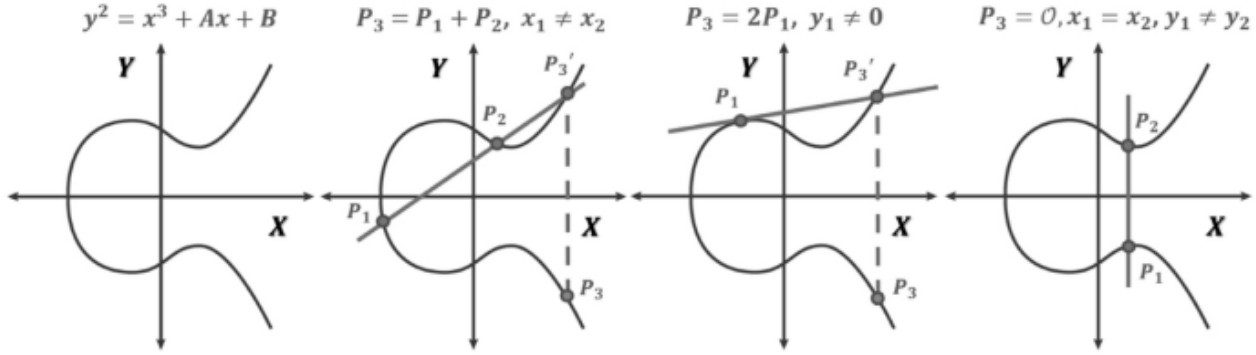

Figure 1: Elliptic curve arithmetic

Discrete Logarithmic Problem on Elliptic Curve (ECDLP): -

Above Figure 1, Elliptic Curve Cryptography is safeguarded by a hard problem called Elliptic Curve Discrete Logarithmic Problem (ECDLP) [4,5,6]. For two given points *P, Q* on the curve such that *Q* = x*P* for 'x' a big random number it is difficult to find x = $log_p Q$ for given *P, Q.*

Methodology:

An Elliptic curve $E_p(a, b)$, with prime *p* having as many points as possible and generators are selected by one of the members of asset of communicating team. In curve selection the following main features should be carefully observed.

i. The order of the curve $E_p(a, b)$ must not contain small prime factors.
ii. The curve is supposed to be not super singular.
iii. It is non anomalous; order is not equal to p $\#E_p(a, b) \neq p$

In $E_p(a, b)$ with p as prime, to have the cyclic nature of the group and to treat each point as a generator.

All the points on the curve are mapped to alphabet, numeral and alpha numeral characters and a common look up table available for all the members. This procedure is set up phase for the group set up phase trusted external services can be availed.

Individual set up phase:

The curve generator and common look up table are available for all the members of the community. Every authentic member of the group can share messages with every other member. For that a pair of authentic users of the group has to arrange a pre setup. If two users Robert and James of the group want to transmit messages before transmission, they set up private and public key system.

Robert choose two random points R_1, R_2 on the public curve and two large random prime numbers $\propto_1, \propto_2$ (less than the order).

He computes $R_3 = \propto_1 R2 + \propto_2 R_1$

$R_4 = (\propto_1 \propto_2) R_3$

He communicates R_3, R_4 to James.

Similarly, James selects two random points J_1, J_2 and large random numbers $\beta 1, \beta 2$(less than the order), computes $J_3 = \beta 1 J2 + \beta 2 J1$

$J_4 = (\beta 1 \beta 2) J_3$ and communicates to Robert.

The secret key set for Robert is $(R_1, R_2, \propto_1, \propto_2)$

The public key set for Robert to communicate is (R_3, R_4)

In the same way key set for James is (J_1, J_2, $\beta 1, \beta 2$). public key set to communicate with Robert is (J_3, J_4).

Encryption:

If James wants send message to Robert, he uses his secret keys and Robert's public keys for encrypting the messages.

Encryption stages are

1. Consider message M consisting of characters $m_1, m_2, m_3 \text{--- } m_n$. All the characters are mapped to elliptic curve points with the help of common look up table $P_1, P_2, P_3 \text{---} P_n$.
2. An additional parameter γ other than secret key set is chosen by James to encrypt the plaintext. Here γ is a big number smaller than the order of the curve different for different plaintext characters.
3. He encrypts the first point P_1 using $\gamma_1$as $E_{11} = \gamma_1 R_3$

$E_{12} = P_1 + \gamma_1 R_4$

So, the point P_1 of the message is converted to pair of points (E_{11}, E_{12}).

4. Similar series of stages 2, 3 is applied for all the plaintext elliptic curve points $P_1, P_2, P_3 \text{---} P_n$. ($En_1, En_2$) is cipher pair and $\gamma_n$is large random number for n= 1,2,3--- , where

$E_{n1} = \gamma_n R_3$

$E_{n2} = P_n + \gamma_n R_4$

The cipher pair for P_1 is (E_{11}, E_{12}), P_2 is (E_{21}, E_{22}), $P_3$is (E_{31}, E_{32}), -----, P_n is (En_1, En_2).

5. All the points $E_{11}, E_{12}, E_{21}, E_{22}, E_{31}, E_{32},$ ----, En_1, En_2 are reverse mapped to text characters, which is the cipher text C communicated to Robert in a public channel.

Decryption:

Robert converts the cipher text characters into points on the curve and

1. Considers the points pair wise (E_{11}, E_{12}), (E_{21}, E_{22}), (E_{31}, E_{32}) --- (E_{n1}, E_{n2}).
2. Decrypts each pair using his own secret keys and James's public keys to get original message.

$P_1 = E_{12} - \propto_1 \propto_2 E_{11}$

$P_2 = E_{22} - \propto_1 \propto_2 E_{21}$

$P_n = E_{n2} - \propto_1 \propto_2 E_{n1}$

Proof of the decryption

$$P_n = E_{n2} - \propto_1 \propto_2 E_{n1}$$

$$= P_n + \gamma_n R_4 - \propto_1 \propto_2 \gamma_n R_3$$

$= P_n + \gamma_n(\propto_1 \propto_2) R_3 - \propto_1 \propto_2 \gamma_n R_3$

$= P_n + \gamma_n(\propto_1 \propto_2) R_3 - \propto_1 \propto_2 \gamma_n R_3$

$= P_n$

If Robert wants to send massage to James, he uses James's public keys for encryption

$E_{n1} = \gamma_n J_3$

$E_{n2} = P_n + \gamma_n J_4$

James decrypts the pair to P_n as $P_n = E_{n2} - \beta 1 \beta 2\ E_{n1}$

Example:

Consider the elliptic curve $E_{31}(5,3)$ and there are 40 number of points on this curve. Take any point on this curve let it be G= (1,3). Now we calculate *2G,3G, ---- 40G*. Create a table by using points on the curve and assign character values, special symbols and numerals to those points.

For given message compare each letter with that table.

Take the message MRPG COLLEGE VIZIANAGARAM

By comparing each letter with the table, we get 13*G 18G 16G 7G 28G 3G 15G 12G 12G 5G 7G 5G 28G 22G 9G 26G 9G 1G 7G 1G 18G 1G 13G*

Here R_1= *(3,13)* R_2= *(4,5)* and $\propto_1$= 13 $\propto_2$= 17

R_3 = 13(4,5) + 17(3,13)

R_3 =104G+ 306G

R_3= 410 G (mod 31) = 7G

R_4= (13*17) 7G= 28 G

J_1= (6,1) J_2= (7,3) β_1=19 β_1=23

J_3=19(7,3) + 23(6,1)

J_3= 589G+299G

J_3=888G (mod 31) = 20G

J_4= (19*23)20G=29G

We have $E_{n1} = \gamma_n J_3$ and $E_{n2} = P_n + \gamma_n J_4$

Also, we consider different $\gamma_n$for different characters in our message

Here we take γ_n=6, 2, 4, 9, 11, 8, 5, 3, 7, 10, 12, 14, 15, 21, 16, 17, 22, 24, 19, 18, 25, 27, 29, 20, 23 for n= 1, 2, 3, ---25. Then by using above formula we calculate

(E_{11}, E_{12}) = (27,1) (E_{21}, E_{22}) = (9,14) (E_{31}, E_{32}) = (18,8) (E_{41}, E_{42}) = (25,20) (E_{51}, E_{52}) = (5,12)

(E_{61}, E_{62}) = (3,12) ---- (E_{n1}, E_{n2}) = (26,29), for n= 1, 2, 3, ---25.

Now compare each point with the table to get the cipher text

AINRHYTELCLGE#FPWNAHU#QKJHJWF.OOHGS.DSMIVV WZ#

Example for repeated words

Take the message GITAMGITAMGITAM

Here we take γ_n= 7, 3, 5, 10, 12, 9, 6, 4, 8, 11, 13, 15, 16, 22, 17, for n= 1, 2, 3, ---15.

Then by using above formula we calculate

(E_{11}, E_{12}) = (17,5) (E_{21}, E_{22}) = (19,14) (E_{31}, E_{32}) = (18,1) (E_{41}, E_{42}) = (36,4) (E_{51}, E_{52}) = (35,33)

(E_{61}, E_{62}) = (16,22) ---- (E_{n1}, E_{n2}) = (12,14), n= 1, 2, 3, ---15.

Now compare each point with the table to get the cipher text

QESNRA5D42PV7S8M6 OENOM322$XLN

Table 1: Table for time calculation

Message size in KB	Execution Time in Sec.
0.1	0.03816
0.2	0.04918
0.3	0.06110
0.4	0.07234
0.5	0.08318
0.6	0.09812
0.7	0.1121
0.8	0.2314
0.9	0.3145
1	0.4285

Execution time graph:

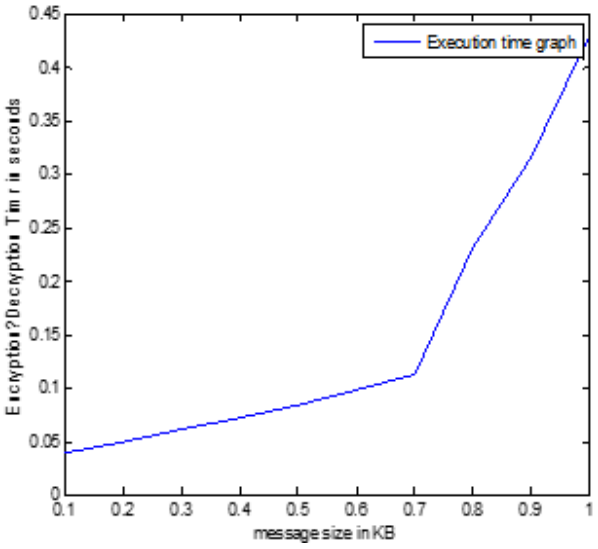

Figure 2: Execution time graph

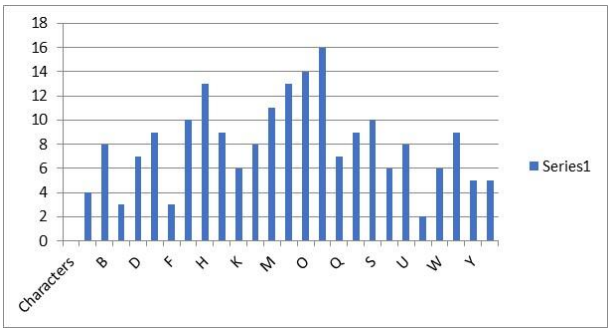

Figure 3: conventional ECC for different sizes of data (number of characters)

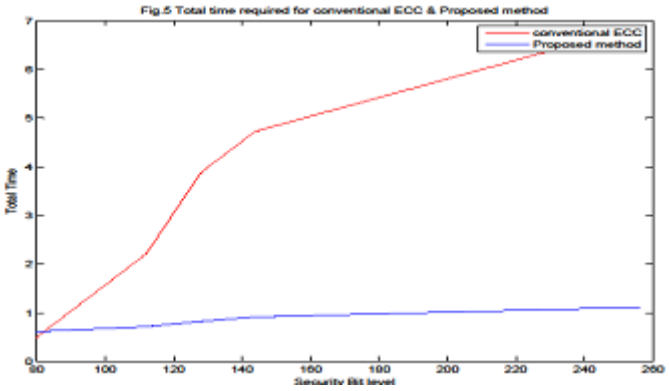

Figure 4: Total time required for conventional ECC & Proposed method

The above table 1 and figures 2,3,4 show encryption and decryption time of the present technique and conventional ECC for different sizes of data (number of characters). Present technique shows approximately same execution time when compared with conventional elliptic curve cryptography. So, the computational cost is not more than conventional ECC and the present algorithm is as fast as conventional ECC algorithm.

Security Analysis:

Here γ value is different for encrypting different message characters. Due to these same characters in the original message will be mapped to different cipher characters. In the first example given above there are repeated characters (M, R, L, A, G) in the original message. First 'R' letter is mapped to 'AI' whereas second 'R' letter is mapped to 'IV'. Similarly, the same character 'L' repeated side by side is mapped to 'FP' and 'WN' in the cipher text. Since different random numbers are used for γ(less than generator) the present encryption has achieved a good required feature to face several active and passive attacks. In the history of cryptography several authors suggested multiple encryptions using the same key. The proposed method is as starts as available multiple encryption algorithms with comparatively less computational overhead. Fig 6 shows the repetition of the English alphabets in the cipher text for 1 KB of data.

In ECC the cipher text space twice than the message space. So, English alphabets repetition will not give any information about the cipher text, because each character maps to two cipher characters. So, linear cryptanalysis and differential cryptanalysis are tough to execute for the present cipher. This hard problem protects ECC against several active and passive attacks. In Pollard –Rho attack ECDLP is cracked by exhaustive search of cipher text points (points on elliptic curve). But in the present technique conventional elliptic curve cryptographic algorithm (similar to Elgamal encryption) is modified by considering more number of points and big random numbers to construct public and secret keys. In addition, each message character is encrypted using a parameter γ (random number less than generator). This γacts as a safe guard for the cipher text. Pollard –Rho and Pohlig- Hellman attacks are quite impossible. γvalues are chosen by encryptor for different message characters. These γvalues are inherent in the cipher text.

Even for the repeated words message (SSSS------ SUSUSU------) different γ values are used to encrypting the characters. This is the basic strength of the present cipher to endure and avoid Pollard –Rho attack. Underlying γ values is helping the present cipher to overcome the weakness of ECC. So, the ECC algorithm presented here is as safe as conventional public key cryptographic techniques with small key size.

Conclusion:

The process of utilizing the concept of Elliptical Curve Cryptography (ECC) delineated to restraint intrusions in the communication of sensitive information securely. The encryption technique proposed here offers same level of security as the conventional public key cryptographic techniques as it is highly difficult to calculate the secret keys of both the legitimate entities.

References:

[1] Benjamin Clement Sebastin , UgarAlpayCenar "Advantage of using elliptic curve Cryptography in SSL/TLA, https://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Cenar+Sebastian
[2] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh "Implementation of Text Encryption using Elliptic Curve Cryptography", Procedia Computer Science 54 (2015) 73-82, www. Sciencedirect.com
[3] Rene"e Brady ,Naleceia David and Anna Tracy, "Encrypting with Elliptic Curve Cryptography, www.math.purdue.edu//Encrypting
[4] S. Thiraviya Regina Rajam and S. Britto Ramesh Kumar, "Enhanced Elliptic curve Cryptography", Indian Journal of science and technology, Vol. 8 (26), Oct 2015.
A. Shamir, "Identity- based cryptosystems and signature schemes", In Proc. CRYPTO 1984, LNCS Vol. 196, pp. 47-53, Springer 1984.
[5] Aziz& W. Diffie, "A secure communications protocol to prevent unauthorized access: privacy and authentication for wireless local area networks, IEEE personal communications, pages 25-31, first quarter 1994.
[6] F. Amounas and E.H. EI Kinani, Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography, Int J of Information and Network Security 1, 54–59 (2012).
[7] MeghaKohelekar, Anita Jadhav, "Implementation of Elliptic Curve Cryptography On Text And Image", International Journal of Enterprise Computing and Business Systems, Vol. 1 Issue 2 July 2011
[8] K. Agrawal and A. Gera, Elliptic Curve Cryptography with Hill Cipher Generation for secure Text Cryptosystem. Int J of Computer Applications 106, 18–24 (2014.
[9] Koblitz N., "Elliptic curve cryptosystems, mathematics of computation", Vol. 48, No.177, pp. 203-209, January 1987.v
[10] Miller V., "Uses of elliptic curves in cryptography". In advances in Cryptography(CRYPTO 1985), Springer LNCS, 1985, vol. 218, pp 417-4 26.
[11] Maurer U., A. Menzes and E. Teske, "Analysis of GHS weil decent attack on theECDLP over characteristic two fields of composite degree". LMS journal of computation and Mathematics, 5:127-174, 2002.
[12] T.N. Shankar and G. Sahoo, Cryptography with Elliptic Curves, Int J of Computer Science and Applications 2, 38–42 (2009).
[13] Arron Blumenfeld, "Discrete logarithms on Elliptic curves", 201115.Menzes A., and Vanstone S. "Handbook of applied cryptography", The CRC-Pressseries of Discrete Mathematics and its Applications CRC-Press,1997.
[14] Miyaji , Nakabayashi and Takano "Elliptic curves with low embedding degree", Journal of Cryptology, 2006, Volume 19, Number 4, Pages 553-562.