March - April 2020
ISSN: 0193-4120 Page No. 13645 - 13654

Elliptic Curve Cryptography with a Special Focus on Reduction of the Cipher Size of ECC using Chebyshev Polynomial

CH. Suneetha[1], D. Sravana Kumar[2], T. Surendra[3], CH. Neelima[4],D Sateesh Kumar[5]
[1,3,4]Mathematics GITAM University, Visakhapatnam, India
[2]Department of Physics, Dr. VSK Government Degree College, Visakhapatnam, India
[5]Department of Mathematics, KoneruLakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
surendrat.bw@gmail.com

Article Info
Volume 83
Page Number: 13645 - 13654
Publication Issue:
March - April 2020

Article History
***Article Received**: 24 July 2019*
***Revised**: 12 September 2019*
***Accepted**: 15 February 2020*
***Publication**: 20 April 2020*

Abstract
As the internet provides access to millions of communications in every second around the world, security implications are tremendously increasing. Transfer of important files like banking transactions, tenders, and e commerce require special security and authenticated mechanism in its journey from the sender to the receiver. Recent attention of cryptography is mainly focused on use of elliptic curves in public key cryptosystems. In these days big data and its storage in the cloud is a progressing subject. Security and privacy of huge data is a challenging issue. The present paper explains an innovative block cipher for providing security to big data using elliptic curve over finite field. Though ECC is becoming popular day by day due to the reason that it provides same security level with shorter key length as RSA, it has a drawback that the cipher bandwidth is twice than that of the message. For an n space message, the cipher is 2n elliptic curve affine points. The present mechanism besides providing the robustness focuses on reduction of the cipher bandwidth equal to that of the message.

Keywords:*Encryption, Decryption, Elliptic curve over finite field, Chebyshev Polynomial*

I. INTRODUCTION

Use of elliptic curves in public key cryptography was first designed and launched by Koblitz and Miller. The principal reason for wide attraction of the researchers towards ECC is it provides the same security level as RSA with comparatively shorter key length, due to the hardness of Elliptic Curve Discrete logarithmic Problem (ECDLP). Public key cryptography is computationally very expensive for small devices unless it is accelerated by cryptographic hardware. For cryptographic purpose elliptic curve is defined by the equation
$y^2 = x^3 + ax + b, 4a^3+27b^2 \neq 0$over the finite field F_q of a prime number q.

Group laws of elliptic curve:-On an elliptic curve E defined over the finite field of integers, addition of two points uses chord-and-tangent rule to get the third point [1,2]. The set of all points on the elliptic curve over the finite field with addition as binary operation forms an abelian group with ∞, the point at infinity as identity element.

Basic Elliptic curve operations:-

1. **Addition Operation**: For given two points $P(x_1,y_1)$ and $Q(x_2,y_2)$ on the elliptic curve, sum of P and Q is $R(x_3,y_3)$ which is the reflection of the point of intersection of the line through the points P, Q and the elliptic curve about x axis. The same rule applies to two points P and – P, with the

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 13645 - 13654

same x-coordinate, where points are joined by a vertical line considered as the intersecting point on the curve at the point infinity. P + (-P) = ∞, the identity element which is the point at infinity.

For P ≠ Q, P + Q = R (x_3,y_3) [1,2]

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

Where,

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

and

2. Doubling the point on the elliptic curve:- Given P (x_1,y_1) on the elliptic curve 2 P is the reflection of the point of intersection of the tangent line at P and the elliptic curve about x axis [1,2].

For P ≠ - P, 2 P is given by (x_3,y_3) where

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2$$

and

$$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 (x_1 - x_3) - y_1$$

.

Example of addition of two points and doubling of a point are shown in the following figures 1 and figure 2 for the elliptic curve $\mathbf{y^2 = x^3 - x}$.

Figure.1: Geometric Addition

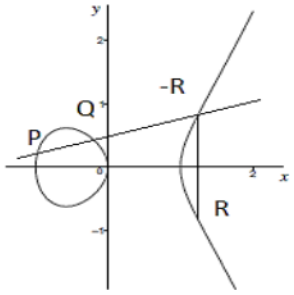
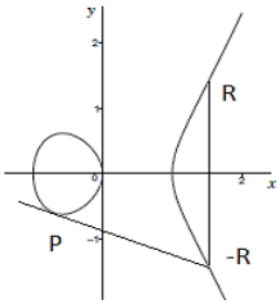


Figure 2: Geometric multiplication



Identity:- P + ∞ = ∞ + P = P for all E where ∞ is the point at infinity [1,2].

Negatives:- If P (x,y) is a point on the elliptic curve then(x,y) + (x,-y) = ∞. Where $(x,-y)$ is the negative of P denoted by – P [1,2].

Point Multiplication:-Let P be any point on the elliptic curve over finite field of integers. Then the operation multiplication of P is defined as repeated addition [5,6].

k P = P + P +……..k times.

Elliptic Curve Discrete logarithmic Problem (ECDLP):- The strength of Elliptic Curve Cryptography depends on the hard problem known as Elliptic Curve Discrete Logarithmic Problem [3,4]. For two points P, Q on the elliptic curve over the finite field and Q = x P it is relatively easy to calculate Q for given x and P but hard to determine x .

Chebyshev polynomial of first kind: The Chebyshev polynomials are orthogonal polynomials defined as the solution of the Chebyshev differential equation

$$(1-x^2)y'' - xy' + n^2 y = 0$$

The Chebyshev polynomials of the first kind are defined by the recurrence relation $T_0(x) = 1 \& T_1(x) = x$ then

$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)\ for\ n = 1,2,3....$

II. RELATED WORK

Several authors explored and came up with many encryption techniques in the history of ECC. L.D Singh &K.M. Singh [7] proposed encryption technique based on elliptic curve cryptography ECC. In that chapter they paired up the corresponding ASCII values of the characters rather than classical technique of mapping the characters to affine points on elliptic curve. SM Celestin and K. Muneeswaran [8] suggested the text encryption using ECC. In that paper they designed a new technique of encryption by mapping the corresponding ASCII values of the

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 13645 - 13654

message to affine points on the elliptic curve and adding each message point to ASCII value times the generator. Balamurugan Et.al. [9] proposed a fast mapping technique by mapping the message characters to affine points on elliptic curve and encrypting each character using ElGamal encryption with extra parameter a non-singular matrix. Keerthi K&B. Surendiran [10] suggested an encryption technique using ECC. In that chapter corresponding ASCII hexadecimal values of the message are grouped together to form x and y coordinates and encrypted in the reverse order to prevent the security attacks. ObaidurRahaman [11] proposed data and information security in modern world using ECC to remove the classical technique of mapping the characters to points in affine plane. Omar Reyad[12]designed a text message encoding technique basing on computational operations of affine points on the elliptic curve. SravanaKumar.D Et.al. [13] designed an encryption algorithm using elliptic curve cryptography with some extra parameters. Chebyshev Polynomials have been recently proposed for assigning public key cryptosystems. G.J.Fee Et.al. [14] used Chebyshev Polynomial $T_n(x)$ for replacing monomial x^n in Diffie-Hellman and in RSA algorithms. Chebyshev polynomial can be mapped into classical discrete log problem. Based on Chebyshev Polynomial, we get RSA algorithm. Kai-Yuen Cheong [15] used Chebyshev polynomial to compare chaotic encryption systems with one-way functions to get new insights for chaos-based cryptosystems. K.Prasadh Et.al [16] described public key encryption based on Chebyshev polynomial

Existing Encryption Techniques in Elliptic Curve Cryptography (ECC):

Several authors proposed many encryption and message mapping techniques in the history of ECC. Some are discussed here

Fundamental Technique: In ECC first the message is mapped to affine point P_m on the elliptic curve $E_q(a,b)$ over a finite prime field q and Q as generator. Each point P_m is encrypted to pair of points to obtain the cipher C_m. A large integer $q_B< q$ is secret key. The point $P_B = q_B*Q$, the curve and the generator point are made public. The sender encrypts P_m as pair of points

$C1 = k*Q$, $C2 = P_m + k* P_B$ where $k <q$ is a random integer. Receiver decrypts $P_m = C2 - q_B*C1$

Later on basing on this fundamental scheme many techniques were developed.

Scheme 1: In this scheme [17] an elliptic curve $E_q(a,b)$ and the points on the curve are public. The alphabets A-Z, the digits 0-9 are given numbers from 1 to 35 (say m). The sender and the receiver agree a number as the secret key k. For each m, x is calculated as $x = m*k + I$, where I is a random integer. If the point (x,y) exists with the calculated x value then the character corresponding to m is mapped to the point (x,y). Otherwise increase I by 1 and repeat the process until we find the appropriate point. The receiver obtains m as x-I/k.

Scheme2: This is almost close to scheme1. In this scheme [18] message is considered as blocks of M characters each. All the characters are written as ASCII equivalent 8 bit binary numbers and written as a big binary array of length M*8. The equivalent decimal number of M*8 is determined and it is

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 13645 - 13654

named as x value. Corresponding y value of the equation $y^2 = x^3 + ax + b$ is calculated. If y has the solution in the given range of points then the point (x,y) becomes the cipher. Otherwise increase x by 1 and repeat the process. At the receiving end the receiver ignores y value, gets the equivalent binary stream corresponding to x, divides into 8 bits from the right and writes the corresponding ASCII characters.

The two message mapping schemes discussed above are lengthy and exhaustive. Sometimes the solution for y is obtained after exhausting the set of points with so many iterations. It causes to increase the execution time and complexity. Moreover there is a collision problem that two different blocks of the message map to same point on the curve. To avoid the collision problem the authors proposed to perform the number of iterations as maximum as possible in the interval of two consecutive x values. But this is practically impossible. So, these schemes are vulnerable to chosen plain text and chosen cipher text attack.

III. PROPOSED METHOD

An elliptic curve $E_q(a,b)$ with q a prime number and having big order, points Q,2*Q,3*Q and so on (Q is generator point) are made public by the users. In selecting the elliptic curve the users take precautionary measures to protect the cipher from all types of frequent physical attacks on ECC like side channel attacks and fault analysis. To escape from the physical attacks ECC friendly curves are chosen basing on the desired features

(i) To resist against Pohlig-Hellman attack the orderof the selected curve # $E_q(a,b)$ should not be factorized into small primes.

(ii) The chosen elliptic curve should be non super singular

(iii) Should be non-anomalous. i.e., the order # $E_q(a,b) = n \neq q$.

In addition the users select the curve having prime order because if the order is prime the group is cyclic and every point acts as generator of the cyclic group. A common code table by assigning the ASCII characters to affine points called ASCII coded EC table is also public. Here 'r' is a crucial number which is an integer computed by the users from the agreed upon permutation function f(x,y). They also agree upon to use Chebyshev polynomial of first kind to find the r value.

Calculation of 'r' value as

1. User1 selects a random number α less than the order n of the curve and finds the point P1= αQ and communicates to user2 in a public channel
2. In the same manner user2 selects a random β <n and finds the point P2= βQ, communicates to user1
3. User1 computes αP2 + R = CR and communicates to user1 where R is a random point selected by user1
4. User2 retrieves the point $R = C_R - \beta P1$
5. Both compute the number $r = F[x_R, y_R]$ where x_R, y_R are coordinates of the point R, and F[x,y] is agreed function.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 13645 - 13654

Algorithmfor computing 'r' value:

Input: Big random numbers less than the order n, points on the curve

Output: A Decimal number

User1	User2
Step1: Begin	Step1: Begin
Step2:	Step2:
i. Consider a big integer α <n	i. Consider a big integer β<n
ii. Find P1 = αQ	ii. Find P2 = βQ
iii. Consider random point R	iii. compute R = (CR – β P1)modq
iv. Compute CR= (αP2 + R)modq	Step3: After obtaining R
Step3: Find r ≡f(xR,yR)	Step3: Find r ≡f(xR,yR)

Encryption:

Suppose user1 wants to transmits the message m to Bob all the characters are coded to affine points on the elliptic curve using the above common look up table and are divided into blocks of agreed length say L [P(1,1), P(1,2), P(1,L)], [P(2,1), P(2,2), P(2,L)], …… [P(n,1), P(n,2), P(n,L)]

where n is the number of blocks and L is the block length.

First block encryption:

1. Alice selects L random numbers α1, α2….αL ,finds the points A1,A2,…..AL and transmits to Bob in public channel where A1 = α1*Q, A2= α2*Q and so on AL = αL*Q
2. Similarly Bob selects random numbers β1,β2,….βL, finds B1= β1Q, B2= β2Q and so on BL= βLQ and communicates to Alice.
3. Alice encrypts the first data block as C(1,1) = T1(r)* α1*B1 + P(1,1) C(1,2) = T1(r)* α2*B2 + P(1,2) and so on C(1,L) = T1(r)* αL*BL + P(1,L) L is the block length Second data block as C(2,1) = T2(r)* α1*B1 + P(2,1) C(2,2) = T2(r)* α2*B2 + P(2,2) and so on C(2,L) = T2(r)* αL*BL + P(2,L), L is the block length
4. In general C(n,j) = Tn (r) αj{Bj} + P(n,j) n is number of blocks 1,2,3…..k and j = 1,2…..L

All the cipher points are converted to characters using the common look up table and communicated to user2.

Decryption: User2 after receiving the cipher text

1. Divides into blocks of length L each and decrypts the cipher as
2. P(1,1) = C(1,1) –T1 (r) β1A1P(1,2) = C(1,2) –T1 (r) β2{A2} and so on
3. In general P(n,j) = C(n,j) –Tn (r) βjAj, n is number of blocks 1,2,…k and j = 1 to L

Overlapping problem: The only trouble in this algorithm is overlapping problem. Occasionally there will be a case that α value and the affine point corresponding to the message character are same for two different message characters. That is P(n,i) = P(n,j) and α (or β)i= α (or β)j for i≠j. Since Tn(r), n = 1,2…k is same for entire block there will be a chance that the cipher characters repeat. In order to prevent the frequency analysis it is suggested to avoid the repetition α or β value.

Decryption: Bob after receiving the cipher divides into blocks of length L and decrypts each block as

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 13645 - 13654

$D(n,j) = P(n,j) = C(n,j) - Tn(r)\ \beta j\{Aj\}$

$= Tn(r)\ \alpha j\{Bj\} + P(n,j) - Tn(r)\ \beta j\{Aj\}$

$= Tn(r)\ \alpha j\{\beta jQ\} + M(n,j) - Tn(r)\ \beta j\{\alpha jQ\} = P(n,j)$

The affine points are converted to corresponding ASCII characters to obtain the message.

The steps involved in encryption and decryption algorithms are shown in the following flow charts 1,2& 3.

Encryption Algorithm

Input : Plain text with all types of characters, chebyshevpolynomialTn(r)

Output :Cipher text

Step1 : Begin

Step2 : (i) Consider L characters of the message at a time

(ii) Convert all the characters to affine points on the curve using common look up table

(iii) Select L random numbers αL, βL less than n and find L points on the curve AL = αL∗Q, BL = βL∗Q

(iv) Exchange AL, BL

Reverse mapping algorithm (Decryption)

Input : Cipher Text

Output : Original message

Step1 : Begin

Step2 : (i) Consider L characters at a time

(ii) Convert text characters to affine points

Step3 : P(1,j) = C(1,j) -Tn (r) βjAj, j = 1 to L

Figure.3

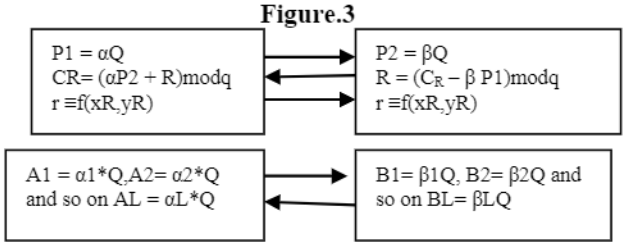


Figure. 4

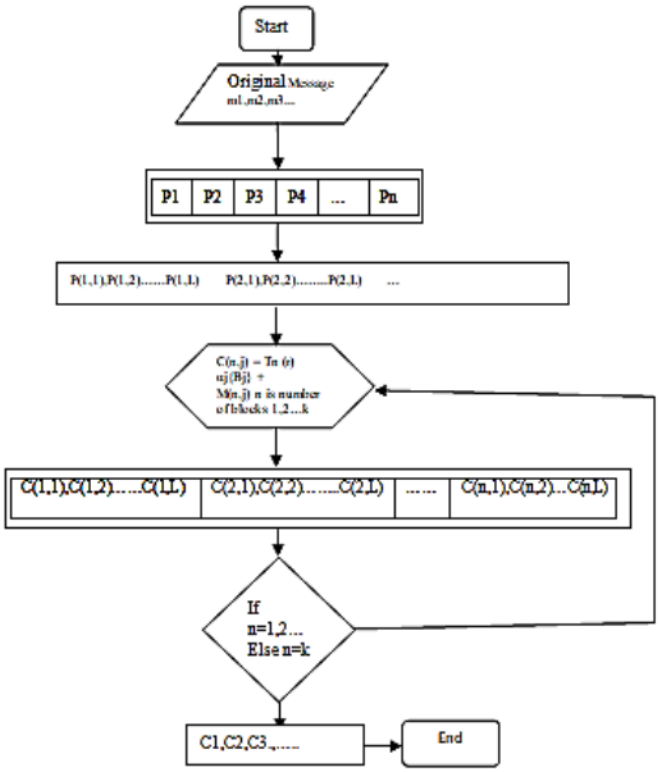
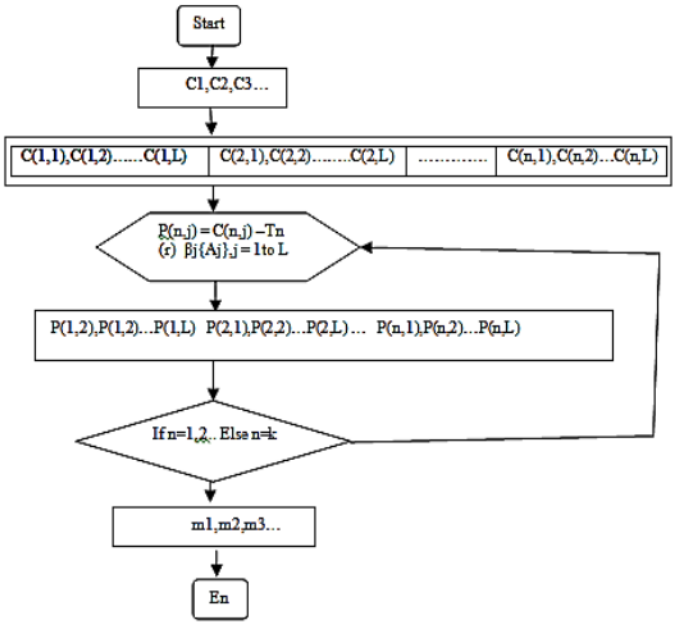


Figure.5



Implementation of the Algorithm: Consider an elliptic curve $y^2 = x^3 + 3x + 27 \bmod 331$ possessing all the above mentioned desired features for cryptography whose order is 317. The curve, the generator point Q = (301,108), and ASCII coded EC

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 13645 - 13654

table by mapping first 256 points to ASCII characters are declared as public. Let the block length L be 5 bits at a time.

Alice selects a random number α = 10 and computes P_{Alice} = (279,83) transmits to Bob. Bob selects β = 20 and computes P_{Bob} = (225,180) and transmits to Alice.

Then Alice computes C_R= 10(225,180) + (230,275) = (150,274) and sends to Bob. Then Bob retrieves R. Suppose f[x,y]modq =[x^2+y^2]modq, then both calculate r = 51

Suppose Alice wants to transmits the first message "SSSSS" to Bob, she selects 5 random numbers 4,8,16,24,36 and computes five points (206,168), (256,79), (31,11),(302,294), (199,160) and communicates to Bob. Similarly Bob selects β= 7,19,23,35,49 and computes (102,149), (44,40), (135,309),(118,75),(272,118) and sends to Alice.

Encryption: Since the message contains one block T1(r)= r = 51.The corresponding affine points from ASCII coded EC table for the characters S is (39,144). The same 'S' character is encrypted as different cipher characters **'‰»²0¯'** communicates to Bob via public channel.

Decryption: Bob after receiving the cipher '‰»²0¯' decrypts the cipher text to affine points on the curve and coded to corresponding characters from the ASCII coded EC table.

If Alice wants to communicate the second message **'GITAM UNIVERSITYVISAKHAPATNAM-530045'** it is encrypted as the affine points (291,320),(184,1),(10,323),(136,136),(9,11),(190,51), (295,152),(161,199),(144,278),(112,317), (9,320), (51, 10),(24,141),(226,16),(5,211),(231,3), (179,326),(60, 8),(114,290),(79,160),(114,41),(301,223), (228, 280), (256,252),(293,283),(53,160), (98, 255), (44, 291), (139, 256), (273,32),(150,57) (198,100), (252,250), (195,147). If the cipher points fall out of the range of ASCII code table either we consider UNICODE table in place of ASCII table or the points are transmitted as cipher text directly without converting to characters.

Salient features of a good encryption are

1. Required level of security to protect against all varieties of attack goals
2. Best performance in various dimensions
3. Computation and Communication overhead as low as possible

How the present cipher has achieved all these character is detailed below

IV. SECURITY ANALYSIS:

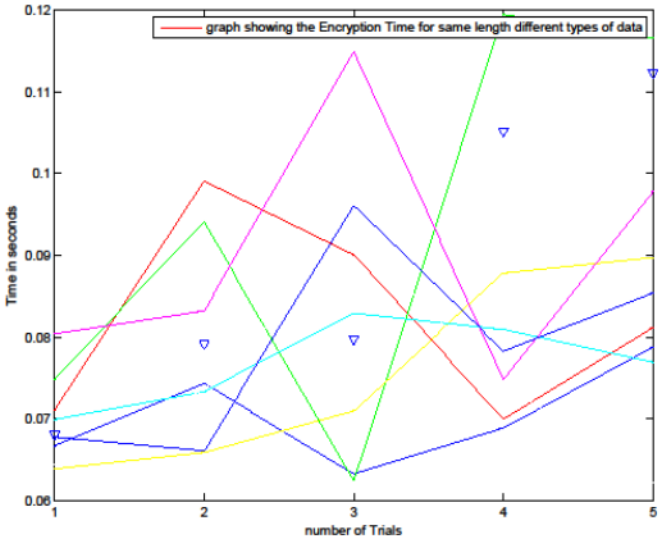
The main expected feature of an encryption algorithm is strong security attribute. The present designed algorithm is free from all types of known cryptographic attacks. In conventional ECC the message characters are mapped to a point Pm on the curve and Pm is encrypted as pair of points Cm where the same characters always goes to the same pair of points. So, there is always a threat of frequency analysis. In the proposed algorithm the plain text is encrypted taking L characters at a time. Each character in those L characters is encrypted with different α value and for each block 'r' value changes which is calculated from Chebyshev polynomial

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 13645 - 13654

r1 = T1(r) for the first block, r2 = T2(r) = $2r^2$ -1 for the second block, …

Tn(r) = 2rTn(r) –T(n-1)(r) for n^{th} block. Since α value changes for all characters in the block and 'r' is different for different blocks there is no chance of repetition in the cipher even for the repeated plain text. It is clear from the two given examples that there is no repetition of cipher points Cm. In the first example 'SSSSS' the same 'S' character is mapped to five different **'‰»²0¯'** characters. In the second example the alphabet A is repeated five times, I,T are repeated thrice each. Not even single point is repeated in the cipher. These two examples are two evidences that the present ECC algorithm is strong against frequency analysis. General attacks like chosen plain text attack and chosen cipher text attack are more effective if there is one-to-one relation between plain text and cipher text which helps in the frequency analysis. Though our proposed algorithm is one-to-one mapping technique it avoids unigram, bigram, trigram and four gram frequency analysis. So, chosen plain text and chosen cipher text attacks are highly impossible here. In cryptography timing attack is a side channel attack where the adversary breaks the cipher by observing the response time for various messages. Here the execution time for various different messages with same size is calculated for many trials. It is found that the execution time is different for different same size messages. The following graph shows different execution time for different same size messages. This assures that the side channel attacks are impossible to implement for this algorithm.



The hardness of ECC depends on the strength of Elliptic Curve Discrete Logarithmic Problem (ECDLP). A well known attack to solve ECDLP is pollard Rho attack. Implementing Pollard Rho is not possible here since α, β values vary for each character in the block of L characters. and 'r' value is different for different block. In addition this 'r' value is not public rather calculated from the function f(x,y) and Chebyshev polynomial. So, no question of Pollard Rho attack arises here.

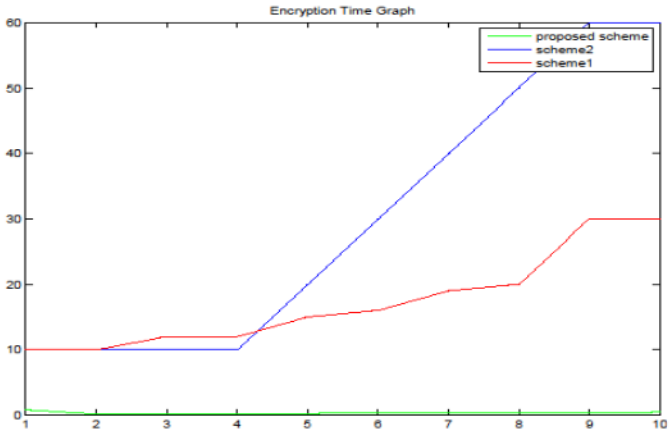
V. PERFORMANCE ANALYSIS

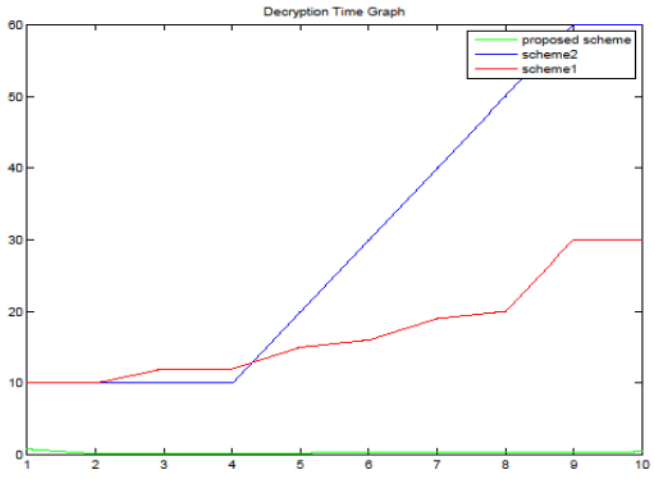
The proposed algorithm yields the same cipher bandwidth to that of the plain text. This reduces the cipher size of the conventional ECC. Though the existing mapping schemes 1,2 described above attain considerable reduction of cipher bandwidth the execution time is comparatively large in those schemes. In scheme2, searching the solution y for the taken x value in the set of points on the elliptic curve over finite field takes much iteration. Incrementing x by one and finding the solution is probabilistic and sometimes the search will be continued till the end of the last point of the set.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 13645 - 13654

Comparative encryption and decryption times are shown in the graphs here under. The execution time for the proposed algorithm is in fraction of seconds where as for the existing schemes 1,2 it is more than 10 seconds for same size of data. This good feature is the clear evidence that the proposed algorithm possesses best performance in various dimensions.





VI. CONCLUSIONS

The proposed algorithm follows all the guidelines of a good encryption scheme. It prevents the cipher from many types of active and passive attacks and keeps the cipher safe in its journey from one end to the other. It is also faster when compared to the existing mapping schemes. The main advantage of this scheme is it not only protects the cipher but also reduces the cipher bandwidth of conventional ECC. I a nutshell, the encryption algorithm presented here is faster, safer and reduces the cipher bandwidth. So, it is efficient in all directions.

REFERENCES

[1] Koblitz N., "Elliptic curve cryptosystems, mathematics of computation", Vol. 48, No. 177, pp. 203-209, January 1987.

[2] Miller V., "Uses of elliptic curves in cryptography". In advances in Cryptography (CRYPTO 1985), Springer LNCS, 1985, vol. 218, pp 417-4 26.

[3] Maurer U., A. Menzes and E. Teske, "Analysis of GHS weil decent attack on the ECDLP over characteristic two fields of composite degree". LMS journal of computation and Mathematics, 5:127-174, 2002.

[4] ArronBlumenfeld, "Discrete logarithms on Elliptic curves", 2011

[5] Menzes A., and Vanstone S. "Hand book of applied cryptography", The CRC-Press series of Discrete Mathematics and its Applications CRC-Press,1997.

[6] Miyaji, Nakabayashi and Takano "Ellipticcurves with low embedding degree", Journal of Cryptology, 2006, Volume 19, Number 4, Pages 553-562.

[7] L.D Singh & K.M. Singh "Implementation of text encryption using elliptic curve cryptography", Procedia computer science 54 (2015) 73-82, Eleventh international multi conference on information processing 2015.

[8] S. Maria Celestin Vigila& K. Muneeswaran,

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 13645 - 13654

"Implementation of text based cryptosystem using elliptic curve cryptography", International conference on advanced computing, IEEE pp 82-85 December 2009.

[9] Balamurugan .R, Kamalakannan.V, Rahul Ganth .D, &Tamilselvan.S., "Enhancing security in text message using matrix based mapping and Elgamal method in elliptic curve cryptography", 978-1-4799-6629-5/14/$31.00 ©2014 IEEE.

[10] Keerthi K, B.Surendiran, "Elliptic Curve Cryptography for Secured Text Encryption", International Conference on circuits Power and Computing Technologies [ICCPCT], 978-1-5090-4967- 7/17/$31.00 © 2017 IEEE.

[11] ObaidurRahaman, "Data and Information Security in Modern World by using Elliptic Curve Cryptography", Journal of Computer Science and Engineering 2017, 7(2): 29-44 DOI: 10.5923/j.computer.20170702.01.

[12] Omar Reyad, "Text Message Encoding Based on Elliptic Curve Cryptography and a Mapping Methodology", Inf. Sci. Lett. 7, No. 1, 7-11 (2018). Information Sciences Letters An International ournal http://dx.doi.org/10.12785/isl/070102.

[13] SravanaKumar.D, Suneetha.CH, &Chandrasekhar.A, "Encryption of data using elliptic curve over finite fields", International journal of distributed and parallel systems, Vol. 3, No. 1, January 2012.

[14] G. J. Fee and M. B. Monagan, "Cryptography using Chebyshev polynomials", www.cecm.sfu.ca/CAG/papers/Cheb.pdf

[15] Kay-Yung Cheong, "One-way functions from Chebyshev polynomials"May 2012, https://eprint.iacr.org/2012/263.pdf.

[16] K. Prasadh, K. Ramar and R. Gnanajeyaraman, "Public key cryptosystem based on chaotic Chebyshev polynomial", Journal of Engineering and Technology Research Vol.1 (7), pp. 122-128, October, 2009

[17] Bh P, Chandravathi D, PoornaRoja P, "Encoding and Decoding of a message in the implementation of elliptic curve cryptography using Koblitz method", International Journal on Computer Science and Engineering, 2010, 2(5):1904-1907

[18] AritroSengupta and Utpal Kumar Ray, "Message Mapping and Reverse Mapping in Elliptic curve Cyptosystem", Nov. 2016, http://doi.org/10.1002/sec.1702