Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Minimising the Cipher Length of Elliptic Curve Cryptography Basing on Chebyshev Polynomial

CH. Neelima [1], CH. Suneetha [2]
[1] *Research Scholar, Department of Mathematical Sciences, GITAM Deemed to be University, Visakhapatnam, India*
[2] *Associate Professor, Faculty of Mathematics, GITAM Deemed to be University, Visakhapatnam, India*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 19 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

Introduction: Public Key Cryptography (PKC) is one of the key components of contemporary cryptographic systems, mainly employed for securing digital communications using protocols such as SSL and TLS. PKC relies on trapdoor functions, which are computationally easy in one direction but impossible to invert without access to a secret key. RSA and the Diffie-Hellman key exchange protocol are classical algorithms that have been extensively employed for secure data transfer. More recently, Elliptic Curve Cryptography (ECC) has been in the limelight because of its high security with compact key sizes and fast computation, based on the algebraic structure of elliptic curves.

Objectives: This study will seek to alleviate one of the most significant weaknesses of ECC-based encryption—namely the expansion of ciphertext size in ElGamal encryption. The goal is to create a revised ECC-based encryption scheme that is highly secure while reducing ciphertext size. Furthermore, the proposed approach will seek to include digital signature functionality for improved data authentication and integrity.

Methods: The new encryption scheme is based on the ElGamal encryption scheme but with an addition involving Chebyshev polynomials of the first kind as a random value generator. This inclusion enables secure randomization during encryption. The new scheme guarantees that the ciphertext size is equal to the plaintext size, essentially compressing the output without loss of security. The scheme also includes digital signature functionality to ensure authenticity and non-repudiation.

Results: The revised ECC-based encryption method proves to be an enormous advancement compared to conventional ElGamal encryption in terms of ciphertext length. Without compromising the strong security attributes of ECC, the new method attains ciphertext compression, maintaining the encrypted message size equal to the plaintext size. Additionally, the scheme efficiently accommodates digital signature operations, providing improved message integrity and verification.

Conclusions: The improved encryption scheme overcomes a significant obstacle to ECC-based cryptography by decreasing ciphertext length at no cost in security. Combining Chebyshev polynomials and digital signature capability is a step towards better secure and efficient cryptographic protocols. The scheme has special application value for any scenarios involving light encryption with tight security assurances, e.g., secure messaging, cloud data encryption, and IoT transmission.

Keywords: Elliptic Curve Cryptography (ECC), Public Key Cryptography (PKC), Secure Communication, Chebyshev Polynomial, Digital Signature, Text-Based Encryption, Ciphertext Optimization, ElGamal Encryption

INTRODUCTION

The elliptic curve equation for cryptographic purposes is given by: y2 = x3 + px +q over a finite field. The condition for the curve to be non-singular is: 4p3 + 27q2 ≠ 0.The plot of an elliptic curve is symmetric along the x-axis. The points on the finite curve, along with the infinity point, form an abelian group with respect to the binary

Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

composition addition of points. The addition operation of points is defined as follows: For two points P (a1, b1) and Q (a2, b2) on the elliptic curve, the sum P + Q is the image of the point obtained by the intersection of the line PQ with the curve. This resulting point is denoted as R.

$$R = (a3, b3)$$

$$a3 = \left(\frac{b2 - b1}{a2 - a1}\right) 2 - a1 - a2$$

$$b3 = \frac{b2 - b1}{a2 - a1}(a1 - a2) - b1$$

❖ **Point doubling or Point multiplication**

For p ≠ - p, 2p is the intersection of the curve with the line that goes through P gives the point.

$$2p = (a_3, b_3)$$

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

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

❖ **Elliptic Curve Discrete Logarithmic Problem**

ECC is strong against several active and passive attacks because the resistance of (ECDLP) Discrete Logarithmic Problem. Consider points P, Q of the curve and for a random number at it is difficult to calculate the value of a, taken P and Q such that Q = a P

The present algorithm uses chebyshev polynomial of first kind and simple bit rotation operation to compute some of the parameters used in the technique.

❖ **Conventional ECC Technique Similar to El Gamal**

In conventional encryption technique of ECC the entries of the message are mapped to points on the curve. Every point says Pm maps to two points (C1, C2).

$$C1 = K \times Q, C2 = Pm + K \times PB$$

Where Q is generator, K is randomly big number, qB are large primes less than the order q of the curve Eq (a, b)

$$PB=qB \times Q$$

qB is also randomly big number and Q is generator of the group of elliptic curve points. Basing on conventional ECC scheme, other schemes were developed by researchers modifying the conventional ECC scheme.

❖ **First modified scheme of ECC**

In this modified scheme [17], points of the curve are public. English alphabets and the numbers 0 to 9 are mapped to 35 points. Sender and receiver agree to use a shared key (private) K. For each message character m, x is computed

$$x = m \times K + I, \text{ for any random integer I.}$$

If the computed x value matches to any point (x, y) of the curve then the message point m is assigned to that point. If no point is there I is incremented by 1 at each stage and repeat the same computing process until the point (x, y) with computed x value occurs. This encryption procedure is extended to the entire message characters. Decryption is

$$m = (x - I)/K.$$

❖ **Second modified Scheme of ECC**

Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Improved Encryption Scheme: This method is a modification of Scheme 1, in which the message is broken into blocks of size M. These blocks are then translated into ASCII binary values and expressed as a string of M×8 bits. The decimal value of this number is taken as x. The corresponding y value is calculated from the following elliptic curve equation:

$$Y2 = x3 + ax + b$$

When the above-calculated (x, y) pair is within the given range, it is taken as the cipher for the character of the message m. Else, x is incremented, and the loop repeats. The recipient is only interested in the x values when decrypting. However, these modified methods pose a significant computational challenge. The process of calculating y has to be run multiple times, resulting in excessive time complexity. Furthermore, cipher block collisions are a serious concern. In an attempt to reduce this, some proposals suggest increasing the number of iterations, which is impractical for real-world applications.

ELLIPTIC CURVE CRYPTOGRAPHY LITERATURE REVIEW

Some researchers have investigated text encryption based on elliptic curve cryptography (ECC), as noted below:

P. L. Sharma et al. [1] suggested a text encryption technique based on elliptic curves for increased security. The authors introduced a tailored permuted ASCII table for using elliptic curve coordinates as keys, which were utilized in a random number generator. Younes Lahraoui et al. [2] designed a message mapping hash algorithm with ECC. Their model provides message integrity by adding a tag to the ciphertext through hash functions and elliptic curve points. Shamsher Ullah et al. [3] discussed a comprehensive overview of ECC uses in data transmission. Their work explains the main advantages of ECC in distributed computing. Nadine Nibigira et al. [4] proposed a secure method for protecting sensitive data through elliptic curves. Their work emphasizes securing sensitive data by means of tools such as PyCryptodome and PyQt5. Yohan Yan [5] elaborated on ECC, comparing it with other public-key cryptosystems. He concluded that ECC plays a crucial role in the creation of new cryptography. David et al. [6] developed an ECC-based text encryption algorithm with several rounds of encryption and a 256-bit key size. L. D. Singh & K. M. Singh [7] proposed an encryption scheme in which ASCII values of characters are matched rather than the conventional affine point mapping. S. M. Celestin & K. Muneeswaran [8] proposed an ECC-based encryption technique that maps ASCII values into affine points and adds them to the generator point. Balamurugan et al. [9] introduced a rapid mapping method, encrypting message characters via ElGamal encryption with one more non-singular matrix parameter. Keerthi K & B. Surendiran [10] proposed an ECC encryption scheme wherein ASCII hexadecimal message values are coupled to create (x, y) coordinates and encrypted in reversed order to avert security attacks. Obaidur Rahaman [11] studied the function of ECC in contemporary data and information security in lieu of classical character-to-affine plane mapping algorithms. Omar Reyad [12] presented an encoding method of text messages utilizing computational operations on affine points over the elliptic curve. Sravana Kumar D et al. [13] designed an encryption algorithm utilizing ECC combined with public-key cryptosystems. G. J. Fee et al. [14] employed Chebyshev polynomials Tn(x) to substitute monomials x^n in Diffie-Hellman and RSA schemes, incorporating more security parameters. Kai-Yuen Cheong [15] compared chaotic encryption systems with one-way functions through the use of Chebyshev polynomials and gave insight into chaos-based cryptosystems. K. Prasadh et al. [16] proposed a public-key encryption system on Chebyshev polynomials. This review underlines progress in ECC-based encryption methods, highlighting their potential in reinforcing security while overcoming computational hurdles.

MATHEMATICAL MODEL EMPLOYED IN THE ALGORITHM

During this setup phase, the elliptic curve, generator, and uniform lookup table are known to everyone. A special user in the communication group picks a suitable curve, initializes a generator, and encodes ASCII characters into particular points on the curve via the uniform lookup table-1. He or she publishes these items for access to all the members. As mentioned above, the Chebyshev polynomial is a tool for a random number generator used in finding a crucial value involved in the mechanism. For this, the genuine user agrees to use a random function f(x, y). The value is different for encrypting different message characters. Each plaintext character is encrypted to two points of the curve. As given in the abstract, this paper not only addresses security issues but also focuses on bandwidth. For this, the integer multiples of the generator for all cipher points are consecutively arranged as a big binary stream.

Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Then, the complete binary string is right-rotated L times, which acts as the ciphertext. The number of right rotations is also confidential between the users. At the other end, during the decryption stage, the big binary string is left-rotated L times to proceed with decryption. The entire encryption and decryption procedure is explained in detail below.

METHODOLOGY

The curve is compatible with encryption and possesses all required features Equation Eq(a,b) has a large order, and for a prime q, the generator Q and the points 2Q,3Q,...are public. Either user can construct a uniform lookup table by assigning ASCII characters to the curve points, which is also public. This phase, known as the setup phase, is conducted by either one of the users or by a trusted third party. In this encryption scheme, 'γ' is a crucial integer obtained through a consented function f(x,y) agreed upon by the users.

- **Calculating 'γ' Value**
  - User 1 selects a random point
  - A1 = μ*Q for μ < £ , sends to user 2 via public channel.

User 2 selects a random point

- A2 = €*Q for some integer € < £ and communicates to user1

User 1 computes

- μ* A2 + B = CB sends to user1 with random point B selected by him

User 2 retrieves B as

- B = CB – β A1

Now both the users are possessing B. Then they compute the γ value as

- γ = f [xB, yB]

Where xB, yB are B point coordinates f[x, y] is consented function.

If 2 authorized users Raechel and Samuel wish to bring the messages

- Raechel selects a point R on the curve, calculates the point
- R1= [α (Q+R)] mod q and R2= [αR] mod q and declares them as her overall public keys. Likewise,
- Samuel choose a point S on the curve, calculates
- S1= [β (Q+S)]modq and S2=[βS]modq and declares as his overall public keys.
- Again Raechel computes RS=[αS2]modq,
- Samuel computes SR= [βR2]modq and publish as the particular public keys to each one.

- **Encryption**

Let us assume **Samuel** wants to convey **M** as a message in the form form of m_1, m_2, m_3,., m_n.

He first converts it into affine points P_1, P_2, P_3,., P_n on the curve with the help of a standard lookup table.

Then each message point is encrypted into a corresponding pair of cipher points E_1, E_2.

The first point P1 is encrypted as

- E11 = [γ1 Q] mod 256, E12 = [P1 + (β + γ1) R 1 – γ1 R2 + RS] mod 256

The second point P2 is encrypted as

- E21= [γ2 Q] mod 256, E22= [P2 + (β + γ2) R 1 – γ2 R2 + RS] mod256

In general,

- Ek1= [γk Q] mod256, Ek2= [Pk + (β + γk) R 1 – γk R2 + RS] mod 256, k = 1 to n.

γk is calculated from the Chebyshev polynomial as

Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- γ1= T1 (γ)
- γ2 = T2 (γ) = 2 γT1 (γ) – To (γ) = 2 γ2 -1
- ……..γk =T (k+1) (γ) = 2 γ Tk(γ) – T(k-1) (γ), k = 1 to n

The points E11, E12; E21, E22; Ek1, Ek2 are integer multiples of the generator point Q say

I1----------1, I12; I21, I22; …….Ik1, Ik2.

For instance,

- The point E11 = 15Q then I11=15;
- E12 = 24Q then I12=24.

The integers I11, I12; I21, I22; Ik1, Ik2 are converted to 8 bit ASCII binaries, arranged as a lengthy binary string of length 8 × 2k. Then the bits of the binary string B are right rotated the number of times say L (L < 2k*8) to get a new binary stream B1

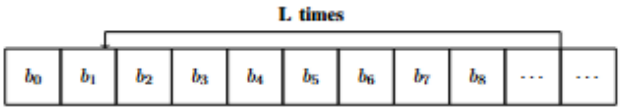

Fig. 1. Encryption Bit sequence representation repeated L times

This big binary stream B1 is converted to decimal equivalent to obtain a lengthy decimal number which acts as the cipher text C. C is sent to the receiver through public channel

- **Decryption**

The receiver after receiving C first converts to a big binary number B1. The bits of B1 are left rotated L times to get B

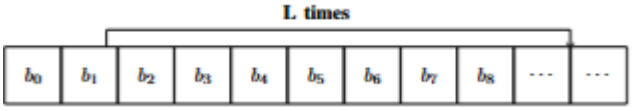

Fig. 2. Decryption Bit sequence representation repeated L times

Then the binary number is split into blocks of 8 bits each from the left and converted to decimal equivalents:

I11, I12; I21, I22;…..Ik1,Ik2.

The affine points:

E11, E12; E21, E22;….Ek1,Ek2 , k = 1 to n, are decoded to the message coded affine points P1,P2,…. as

- P1 = E12 – (α E11 +α S1 +SR)
- P2=E22 – (αE21 +α S1 + SR)
- Pk = Ek2-(αEk1 +α S1 + SR) k = 1 to n.

1. **Decryption works out properly:**
   - Pk = Ek2-(αEk1 +α S1 + SR)
   - = [Pk + (β + γk) R 1 – γk R2 + RS] -(αEk1 +α S1 + SR)
   - = [Pk + {(β + γk) α(Q+R)} – γk αR +αβS] – [α γkQ + αβ(Q+S) +βαR]
   - = Pk + αβQ+ αβR + α γkQ +α γkR - α γkR+αβS- α γkQ-αβQ- αβS- αβR = Pk

Corresponding text characters of the points from the ordinary look up table yields the primary message.

Block diagram of the proposed algorithm:

2. **Algorithm for computing 'γ' value:** The table-1 depicts an algorithm to calculate a certain value based on elliptic curve cryptography concepts. It illustrates procedures for two users, User1 and User2, to generate and

Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

share cryptographic keys. Steps include random number selection, calculation of points on a curve, modular arithmetic operation, and public and private key generation.

Table I Algorithm For Computing γ Value

User1	User2
Step1: Begin Step2: i: Find A1 = μ*Q ii: Consider random point B iii: CB=(μ*A2 + B)modq Step3: Find γ ≡f(xB,yB)	Step1: Begin Step2: i: A2 = €*Q ii: B = (CB – €* A1)modq Step3: After obtaining B find γ =f(xB,yB)
γk =T(k+1) (γ) =2 γ Tk(γ)–T (k-1) (γ) k = 1 to n and γ1 = γ	
Selects α as a random number, a point R which is on the curve Calculates R1= [α*(Q+R)]mod q, R2=[α*R]mod q and publishes as general public keys Again computes RS = [α*S2]modq and publishes as particular public key to user2	Selects β as a random number, a point S which is on the curve Calculates S1= [β*(Q+S)]mod q, S2=[β*S]modq and publishes as general public keys Again calculates SR = [β *R2]modq and publishes as particular public key to user1z

3. **Encryption Algorithm:** The encryption algorithm uses Chebyshev polynomials and elliptic curve cryptography to convert text into encrypted decimal ciphertext

Input: Plain text, Chebyshev polynomial

Output: Cipher text in form of decimal number

Step 1: Begin

Step 2:

- (i). Convert the message characters to points using common look up table
- (ii). Encrypt each point Pk to pair of points Ek1, Ek2
- Ek1= [γk Q] mod256, Ek2=[Pk + (β + γk) R 1 – γk R2 + RS]mod 256,
- k = 1 to n

Step 3:

- (i). The integer values of Ek1 =Ik1*Q,Ek2 = Ik2*Q where k = 1 to n are converted to 8 bit binary numbers and written side by side to get the big binary number B
- (ii). Bits of B are right rotated L times to get B1

Step 4: Decimal equivalent of B1 is the cipher text C

Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Step5: End

4. **Decryption Algorithm:** The decryption algorithm de ciphers encryption by converting ciphertext to binary, per forming a left rotation, obtaining ASCII values, decrypting points, and regaining the original text

Input: Cipher text in form of a big decimal number

Output: Plain text

Step 1: Begin

Step 2:

- (i). Convert the decimal number to binary equivalent B1
- (ii). Bits of B1 are left rotated L times to yield B
- (iii).B1 is split into blocks of 8 bits each and ASCII decimal
- Equivalents of each block are integers Ik1,Ik2 for k = 1 to n.

Step 3:Each pair of points Ek1,Ek2 are decrypted to Pkfor k = 1 to n

- Pk = Ek2-(αEk1 +α S1 + SR)

Step 4: Corresponding text characters from the ordinary look up table gives the primary message M

Step 5: End

5. **Example:**

Consider the elliptic curve $y^2 = x^3 + 3x + 27 \bmod 331$, which is compatible for encryption purposes and has an order of 317. Let Q (301, 108) is the generator, and the code table mapping ASCII characters to curve points is public. If two users, Raechel and Samuel, wish to intercommunicate messages, Raechel first selects a random number α = 17 and a random point R = (184, 330). She then calculates:

- $R_1 = [\alpha (Q + R)] \bmod 331 = (118, 75)$
- $R_2 = [\alpha * R] \bmod 331 = (321, 68)$

She keeps α and R as her secret keys and publishes R_1, R_2. Similarly, Samuel selects β = 19, a random point S = (166, 231), and computes:

- $S_1 = [\beta (Q + S)] \bmod 331 = (66, 134)$
- $S_2 = [\beta * S] \bmod 331 = (10, 8)$

He retains β and S as his secret keys and publishes S_1, S_2. Raechel then calculates:

- $RS = [\alpha S_2] \bmod 331 = (296, 121)$

She publishes this as a particular public key for Samuel. Both agree to use a random function $f(x, y) = x^2 + y^2 + x + y$ to compute γ for encrypting each character. Samuel calculates:

- $SR = [\beta R_2] \bmod 331 = (32, 303)$

He then publishes this as a particular public key for Raechel. If Samuel wishes to communicate the message "SSSSS" to Raechel, he transforms the characters into affine points and encrypts each character into two points E_{11}, E_{12}; E_{21}, E_{22}; .... The corresponding integers I_{11}, I_{12}; I_{21}, I_{22}; ... are converted to 8-bit binary numbers and arranged in a large binary stream:

B=10010001011101100100000100100110000100011100000000000000000000000000000000000000

This binary sequence is right rotated 10 times to produce a new binary number:

B_1=00000000001001000101110110010000010010011000010001110000000000000000000000000000

The decimal equivalent of B_1 is "171731137568993548697600", which is transmitted as the ciphertext C.

Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Upon receiving C, Raechel converts it back into binary, left rotates it 10 times to recover B, and then splits B into blocks of 8 bits to obtain the integers I_{11}, I_{12}; I_{21}, I_{22}; .... After determining the affine points E_{11}, E_{12}; E_{21}, E_{22}; ..., she decrypts them into P_1, P_2, P_3, P_4, P_5. Finally, using a common lookup table, these points are converted back into the original text: "SSSSS".

PERFORMANCE ANALYSIS

The encryption time for different sizes of data is calculated using Intel core I5 10th generator computer and MATLAB 2020, the time of encryption and decryption are in table 1 fig.3 as shown

TABLE II EXECUTION TIME TABLE

S.No	Data Size (kb)	Encryption Time (ms)	Decryption Time (ms)
1	1kb	0.71	0.63
2	2kb	0.89	0.79
3	3 kb	0.99	0.82
4	4 kb	1.02	1.99
5	5 kb	1.13	1.02
6	6 kb	1.21	1.15
7	7 kb	1.34	1.29
8	8 kb	1.45	1.34
9	9 kb	1.56	1.62
10	10 kb	1.72	1.85

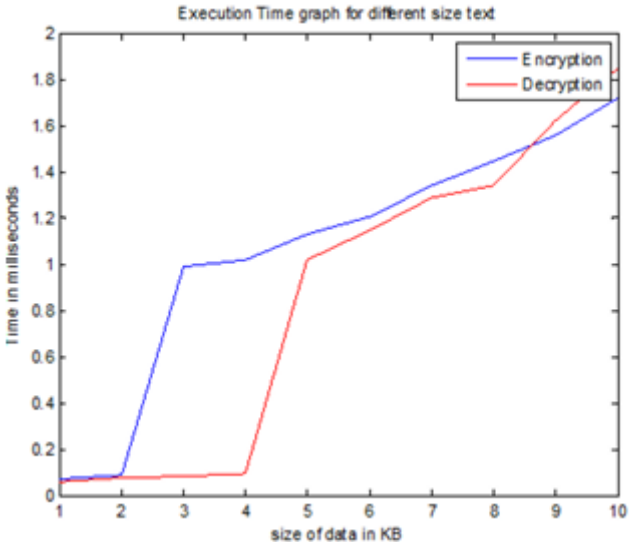

Fig. 3. The repetitions of the numbers

SECURITY ANALYSIS

Strength of the cryptographic primitive depends on different security attributes. In the present algorithm each character is encrypted using sender's secret keys, receiver's public keys andγ. γ Value is different for each character which is calculated from the shared secret point, agreed upon permutation function (x,y) and Chebyshev polynomial of I kind. The data encryption as well as cipher reduction technique presented in this paper relays on a special γ value and binary bit rotation operation. Though the elliptic curve points, generators are public, the present cipher attains extreme security like a secret key mechanism. This is because the γ value is different for different character encryption the value of γ is obtained by calling a random function. Because γ is changing with each encryption step, even duplicate text has different cipher characters assigned to it. The cipher produced is a

Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

stream of decimal digits, thus the resulting proposed encryption protocol is very robust against both passive and active attacks. Linear and differential cryptanalysis is difficult to implement on this cipher. These classical plaintext and ciphertext attacks assume a one-to-one correspondence between the cipher and the message, but in this scheme, there is no direct relationship between the length and type of the message and its cipher. The encrypted output is composed solely of integers, independent of the character make-up of the original message. The frequencies of decimal digits from 0 to 9 are estimated to the message with 1 kb size. The repetition of the numbers are shown as the following histogram fig. 4

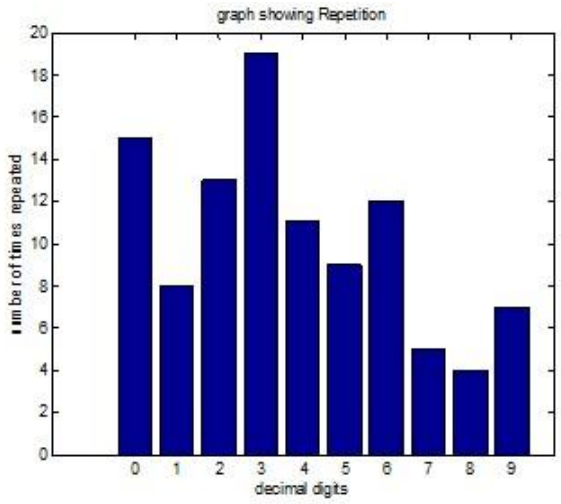

Fig. 4. The repetitions of the numbers

CONCLUSION

The encryption and cipher reduction method suggested in this paper provides confidentiality, authentication, and integrity. Most attacks on ECC, like Pollard-Rho and Pollig-Hellman, aim at the Elliptic Curve Discrete Logarithm Problem (ECDLP). Pollard-Rho, which is an exhaustive search algorithm, is a serious threat. But in the suggested algorithm, the parameter γ changes with every character encryption, so even the same characters are encrypted differently. This adaptive change of γ increases resistance against Pollard-Rho attacks. Furthermore, both active and passive attacks, e.g., ciphertext and plaintext attacks are difficult to perform because the cipher is in the form of a sequence of decimal digits. The algorithm not only enhances security but also solves the issue of cipher bandwidth. One message point was traditionally mapped to two points on the elliptic curve in a cipher. The suggested method, though, uses a binary bit rotation mechanism, which changes the structure of the cipher and minimizes communication hazards. More advancements aim at optimizing the cipher reduction method to correspond each message point with a single cipher point. This advancement optimizes efficiency without sacrificing security. In comparison with standard ECC implementations, the new method presents better safeguarding against cryptanalysis while maximizing encryption efficiency. Therefore, the adapted encryption method offers a secure and efficient alternative to standard ECC-based cryptography schemes.

ACKNOWLEDGMENT

We wish to sincerely thank all the contributors in successfully accomplishing this study of reducing the length of elliptic curve cryptography according to the Chebyshev polynomial. Appreciation is special for academic advisers, colleagues, and institutions, as their great input and continuous guidance significantly augmented this study.

REFRENCES

[1] Sharma, P.L., Gupta, S., Monga, H. et al. TEXCEL: text encryption with elliptic curve cryptography for enhanced security. Multimed Tools Appl (2024). https://doi.org/10.1007/s11042-024-19377-4

[2] Younes Lahraoui, Saiida Lazaar, Youssef Amal, and Abderrahmane Nitaj, " Securing Data Exchange with Elliptic Curve Cryptography: A Novel Hash-Based Method for Message Mapping and Integrity Assurance" Cryptography 2024, 8(2), 23; https://doi.org/10.3390/cryptography8020023
[3] Shamsher ullah, Jiangbin Zheng, Nizamud Din, Muhammad Tanveer Hussain, Farhan Ullah, Mahwish Yousaf, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey "https://doi.org/10.1016/j.cosrev.2022.100530
[4] Nadine Nibigira, Vincent Havyarimana, Zhu Xiao, "Sensitive Information Security Based on Elliptic Curves", https://doi.org/10.4236/wjet.2024.122018
[5] Yuhan Yan, "The Overview of Elliptic Curve Cryptography (ECC)" , DOI 10.1088/1742-6596/2386/1/012019.
[6] Adeniji Oluwashola David, and Olagunju Sulaimon, "Text Encryption with Improved Elliptic Curve Cryptography" Journal of Advances in Mathematics and Computer Science Volume 38, Issue 3, Page 32-41, 2023; Article no.JAMCS. 95066 ISSN: 2456-9968, DOI: 10.9734/JAMCS/2023/v38i31749.
[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, "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) 7 Information Sciences Letters An International Journal http://dx.doi.org/10.12785/isl/070102.
[13] Sravana Kumar.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