Cryptography using Elliptic Curve with Matrix Scrambling

Naresh S. Badve
Department of Computer Science and Engineering
Nuva college of Engineering and Technology, Nagpur, India

Abstract

Elliptic curve cryptography is additional powerful than different methodology that gains countless attention within the industry and plays vital role within the world of CRYPTOGRAPHY. This paper explains the strategy of elliptic curve cryptography victimization matrix scrambling method. during this methodology of cryptography we have a tendency to initial rework the plain text to elliptic curve so victimization matrix scrambling methodology we have a tendency to encrypt/decrypt the message. This method keeps information safe from unwanted attack to our information.

Keywords: Matrix scrambling, Elliptic Curve Cryptography, Encryption, Decryption, constant range, Random range generator, Circular shift technique, Prime Number

I. INTRODUCTION

In the world of communication network and gift era it is additional vital to secure line through that we will send and receive the info or we will communicate firmly over channel and keep information securely. Currently cryptography may be a methodology that protects information while we have a tendency to be transferring information from one network to another network. to stay safe information or avoid the disclosed data ancient and fashionable cryptography are used. There are some standard public-key secret writing algorithms that contain some advanced calculation, for instance, RSA, ElGamal. Due to properties, options and characteristic of elliptic curve cryptography increased attention of the many skilled and scientists as a result of it have opened wealth potentialities in terms of security.

Proposed a matrix scrambling algorithmic rule supported two way circular queues. In this case, we have a tendency to introduce a new secret writing methodology on elliptic curve supported matrix Scrambling technique. This paper shows a new technique of encrypting information that permits smart diffusion and has a singular technique of decrypting it back to the plaintext and is straightforward to implement victimization matrix scrambling methodology that is predicated on random function and shifting. The selection of operation performed on rows or columns is predicated on Binary worth of prime no. Therefore, the paper presents in details its implementation based on an elliptic curve given by the subsequent equation:

\[ y^2 = x^3 + x + 13 \]

II. OVERVIEW OF ELLIPTIC CURVE

The study of elliptic curves by algebraists, algebraic geometers and range theorists dates back to the center of the nineteenth century. Elliptic Curve Cryptography (ECC) was discovered in 1985 by Neil Koblitz and Victor Miller. Elliptic Curve Cryptography may be a public key Cryptography. ECC is right for environments like cellular phones and sensible cards. Moreover, due to the apparent hardness of the underlying elliptic curve separate logarithm downside (ECDLP), ECC systems also are well suited for applications that require long-run security requirements. Elliptic Curve Cryptography (ECC) may be a public key technology that gives performance blessings at higher security levels. Understanding ECC desires full mathematical background on elliptic curves. Elliptic curves aren't ellipses. The overall cubical equation of elliptic curves is \[ y^2+axy+by=x^3+cx^2+dx+e \]. except for our purpose it's sufficient to limit the equation to the shape \[ y^2=x^3+ax+b \]. Say \( EP(a,b) \) consisting of all the points \((x,y)\) that satisfy the on top of equation in conjunction with part at infinity \( O \).

For ECC, we have a tendency to are involved with a restricted kind of elliptic curve that's outlined over a finite field. Of particular interest for cryptography is what's remarked as the elliptic cluster mod \( p \), wherever \( p \) may be a prime. This is outlined as follows. Opt for 2 plus integers, a and b, but p that satisfy: \( 4a^3+27b^2 \pmod{p} \neq 0 \). Then \( EP(a, b) \) denotes the elliptic group mod \( p \) whose elements \((x, y)\) are pairs of nonnegative integers less than \( p \) satisfying: \( y^2 \pmod{p} = (x^3 + ax + b) \pmod{p} \)

III. MAIN RESULTS

In this section we offer the new methodology of secret writing of a message (plain text) and decrypting back once more to the original message (plain text)
A. The Planned Methodology Description:

1) Encryption:
The plaintext is remodeled on points of elliptic curve and therefore the corresponding code is organized into a circular queue system. Within the matrix M of n*m. The parameter p (Prime) represents the count of operations, say, the time of transformation we have a tendency to create to matrix. The ECC methodology needs that we have a tendency to choose a random integer a, that has to be unbroken secret. Then base on the binary worth of prime circular shift is performed.

Let b=bit (rj), wherever j is bit position, the worth of b is considered and supported it circular left shift or circular right shift are performed on rows. Equally as rows, circular upward shift or circular downward shift are performed on columns. The process of secret writing is completed as following:

![Encryption Process flowchart](image)

Fig. 1: Encryption Process flowchart
- **Step 1.** The plaintext is mapped into points of elliptic curve. Then the code of points is ranged into bi-directional circular queue information sequence, within the matrix of \( n \times m \):

\[
M = \begin{pmatrix}
    b_{1,1} & b_{1,2} & \cdots & b_{1,m} \\
    b_{2,1} & b_{2,2} & \cdots & b_{2,m} \\
    \vdots & \vdots & \ddots & \vdots \\
    b_{n,1} & b_{n,2} & \cdots & b_{n,m}
\end{pmatrix}
\]

- **Step 2.** \( a = \text{Random}() \), with ‘\( aP \)’ may be a random purpose that Decides that transformation is applied on matrix (Row, Columns). Once this we have a tendency to choose the code of ‘\( aP \)’ and keep in \( r \). the selection of operation performed on rows and columns is predicated on the little bit of the sequence \( r \).

- **Step 3.** Let \( b = \text{bit}(r_j) \), wherever \( j \) is bit position (LSB→MSB), that decides that transformation has got to be performed on rows and columns.

- **Step 4.** The worth of bits verified:

  - If the present bit position is one then shift row upward circularly and if current bit position is zero then shift column circular shift right. Merge the matrix information during a single string to form it additional strong.

2) **Decryption:**

The process is done by reversing the Operations done in the encryption process. The cipher text is arranged into a matrix of \( n \times m \) noted \( M \). The algorithm of decryption is given as follows:

- **Step 1:** Convert merged data into matrix \( n \times m \)

\[
M = \begin{pmatrix}
    b_{1,1} & b_{1,2} & \cdots & b_{1,m} \\
    b_{2,1} & b_{2,2} & \cdots & b_{2,m} \\
    \vdots & \vdots & \ddots & \vdots \\
    b_{n,1} & b_{n,2} & \cdots & b_{n,m}
\end{pmatrix}
\]

![Decryption Process flowchart](image)

Fig. 2: Decryption Process flowchart

- **Step 2.** Browse \( p \) (prime no.). Reverse the binary sequence of primary such that: \( r = \text{Reverse}(p) \)

- **Step 3.** For every worth \( b = \text{bit}(r_j) \), wherever \( j \) is bit position such that operation is decoded that is given as:

  - \( \text{InverseTrans}(M) \)

In the case: \( j \) LSB \_m/2, the \( \text{InverseTrans}(M) \) is depending on the worth of \( b \) transpositions are performed.
If \( b=0 \) then upward shift columns else left shift operation is performed on rows. Within the case: \( j: m/2+1\rightarrow \text{MSB} \), the InverseTrans \((M)\) depending on the worth of \( b \) transpositions are performed. If \( b=0 \) then right shift rows else downward shift operation is performed on columns. After decipherment the received message \( M \) and reverse the imbedding, we have a tendency to get the plaintext.

**B. Implementation Details of the Planned Algorithmic Rule:**

In this section, we have a tendency to take into account the elliptic curve given by the Weierstrass equation \( y^2 = x^3 + x + 13 \). Detailed method of our secret writing algorithmic rule by an example. In our case, we have a tendency to shall take \( a=58 \), then \( r=1010011101 \).

In vector \( r \), solely 10 bits is taken into account. This provides the information concerning operation on Rows and columns (Rowtrans and Coltrans).

Here in our case Alice needs to send a message “save” to Bob. First, she imbeds the message “save” into the elliptic curve \( E \). Next, she represents the plain text “save” as a series of bits recorded in matrix \( 4*10 \) as following:

Detailed method of our secret writing algorithmic rule by an example. In our case, we have to take \( a=58 \), then

\[
\begin{align*}
0 &\to 1 \quad 0 &\to 1 \\
0 &\to 1 \quad 1 &\to 0 \\
1 &\to 0 \quad 0 &\to 1 \\
1 &\to 1 \quad 0 &\to 1
\end{align*}
\]

This provides the information concerning operation on Rows and columns (Rowtrans and Coltrans).

In vector \( r \), solely 10 bits is taken into account. This provides the information concerning operation on Rows and columns (Rowtrans and Coltrans). Here in our case Alice needs to send a message “save” to Bob. First, she imbeds the message “save” into the elliptic curve \( E \). Next, she represents the plain text “save” as a series of bits recorded in matrix \( 4*10 \) as following:

Binary sequence of \( r \) is explained within the figure No. 3:

The cipher text obtained is given as:

\[
011001100100001011011001001010101110010011010011101
\]

The secret writing process:

In this section, we have a tendency to show the elaborated method of our decryption algorithmic rule with an example. Consider the cipher text obtained once secret writing as:

\[
011001100100001011011001001010101110010011010011101
\]

The secret writing is completed by reading the last sequence of bits noted \( d \) in reverse order and reverse operation each Rowtrans and Coltrans. \( d=1010011101 \) and \( r=\text{Reverse} d=1011100101 \).

The n, the method of secret writing is given below When a similar plaintext is taken and once the secret writing is performed once more, then the resultant disorganized matrix is different. For an trespasser it’d be terribly troublesome to guess on that

The technique of scrambling the matrix bits based on binary sequence of \( r \) is explained in the figure No. 3:

**Fig. 3:** Encryption Process

**Fig. 4:** Decryption Process

The cipher text obtained is given as:

\[
011001100100001011011001001010101110010011010011101
\]
purposethe secret writing method is performed and therefore improves the problem of decrypting. Our algorithm is predicated on magic parallelogram, and therefore it's easy to grasp straightforward and straightforward and simple). To implement the planned algorithm, that additionally uses solely two styles of linear array operations, circular horizontal shifting (left, right) and circular vertical shifting (up, down). Therefore it works with efficiency with very little system resources. The parameter 'm' additionally plays a crucial role in strengthening the intensity of secret writing beside the parameter 'a'. Looking on elliptic curve, the worth of parameter 'm' plays a crucial role au fait the intensity of the secret writing. 'm' mustn't be too tiny or too large. The experimental results show that the new scheme features a in no time secret writing speed and therefore the x-y coordinate is distended and it will resist all types of cryptanalytic. Thus, we have a tendency to conclude that the planned Secret writing method scheme will strengthens the elliptic curve cryptosystem against most of the present assaultive.

IV. SAMPLE OUTPUT

![Sample Output](Fig. 5: Sample Output)

V. CONCLUSION

In this paper, we've developed AN algorithmic rule secret writing and secret writing on elliptic curve victimization matrix scrambling technique. So, the usage of random purpose on elliptic curve firstly and second for choosing the operations for scrambling, avoids the regularity within the resultant cipher text that is remodeled from plaintext matrix, and hence improves the problem for decrypting. Finally, we like to suggests that the great selection of elliptic curve and a whole number worth 'a'
provides higher binary sequence, that is employed to scramble the matrix in each directions with efficiency. At the end, there's many scope to flirt with the choice of the “aP” purpose. Looking on the amount of memory demand, one will analyze the use of this algorithmic rule in tiny memory devices like sensible cards and mobile devices. This algorithmic rule is additionally applied to text secret writing, image secret writing, and transmission secret writing and then on. ECC may be a field wherever there's giant scope for higher research.

ACKNOWLEDGMENT

The authors would love to convey the colleagues and senior faculty for his or her helpful suggestions.

REFERENCES