Bulletin of Pure and Applied Sciences
Section - E - Mathematics & Statistics
Vol. 41E, No.1, January-June 2022.P.104-108

Print version ISSN 0970 6577
Online version ISSN 2320 3226
DOI: 10.5958/2320-3226.2022.00015.7

Original Article

Content Available online at: https://bpasjournals.com/math-and-stat/

Message Mapping Technique Using Elliptic Curve Cryptosystem

***P. L. Sharma[1], Shalini Gupta[2], Kritika Gupta[3], Ashima[4], Sushil Kumar[5]**

Author's Affiliation:
[1,2,3,4,5]Department of Mathematics & Statistics, Himachal Pradesh University, Summer Hill, Shimla - 171005, India

***Corresponding Author: P. L. Sharma,** Professor, Department of Mathematics & Statistics, Himachal Pradesh University, Summer Hill, Shimla - 171005, India
E-mail: plsharma1964@gmail.com

How to cite this article: Sharma P. L., Gupta S, Gupta K, Ashima, Kumar S. (2022). Message Mapping Technique Using Elliptic Curve Cryptosystem. *Bull. Pure Appl. Sci. Sect. E Math. Stat.* 41E(1), 104-108.

ABSTRACT

There are several mapping techniques to map the characters of the message to points on an elliptic curve using Elliptic Curve Cryptography. In the present paper, we propose a new mapping technique based on XOR operation. This mapping technique helps us in mapping the three characters simultaneously to a single point on an elliptic curve without the need of Code Table.

KEYWORDS: Elliptic curve cryptography, Encryption, Decryption, Mapping Schemes, Cryptanalysis.

AMS Classification: 12E20, 94A60.

1. INTRODUCTION

Cryptography is the most common method for securely sharing the information between sender and receiver, see [3, 7, 8, 10]. It mostly deals with data encryption and decryption, see [4, 13, 14]. Miller [9] and Koblitz [5] independently discovered Elliptic Curve Cryptography (ECC), a public key cryptography, in 1985. Koblitz et al. [6] proposed the problem of discrete logarithm for group of elliptic curves. It provided higher speed and higher security.

To encrypt a message with the ECC encryption algorithm, each character must be mapped to a point P_m on the elliptic curve, and then this point P_m must be encrypted to the corresponding cipher text. Mapping should be done in such a way that the encrypted message is more secure against various cryptographic attacks, as shown in [12, 15, 16].

To map the message to a point on an elliptic curve, various mathematicians have proposed several mapping algorithms. The most popular mapping approach is multiplying the ASCII value of each character with the generator point of the elliptic curve to map each character in the message to a point on the elliptic curve, as shown in [3]. Because this strategy is always one-to-one, it is susceptible to a frequency analysis attack. Amounas and Kinani [1] suggested a matrix-based mapping technique in 2012. This method avoids the frequency analysis attack by using a matrix to permute the places of the points obtained using the above-mentioned scheme. This method, however, was vulnerable to chosen plaintext attack.

Another mapping scheme used the concept of quadratic residues to map the message characters to the points on an elliptic curve, however this scheme was probabilistic and prone to collision attack, see [3]. Bh et al. [2] suggested a mapping system based on the Koblitz approach, however it was sensitive to cryptanalysis in general. Muthukuru and Sathyanarayana [11] introduced a new fixed length block mapping technique that maps the message to points on an elliptic curve using the XOR operation. This method, however, was vulnerable to both chosen plaintext and man-in-the-middle attacks.

Received on 20.01.2022/ Revised on 27.04.2022/ Accepted on 30.05.2022
Online First Published on June 15, 2022 at https://www.bpasjournals.com/

In the present paper, we propose a new mapping scheme using the XOR operation. This mapping technique eliminates the requirement for a Code Table by mapping all three characters to a single point on an elliptic curve at the same time.

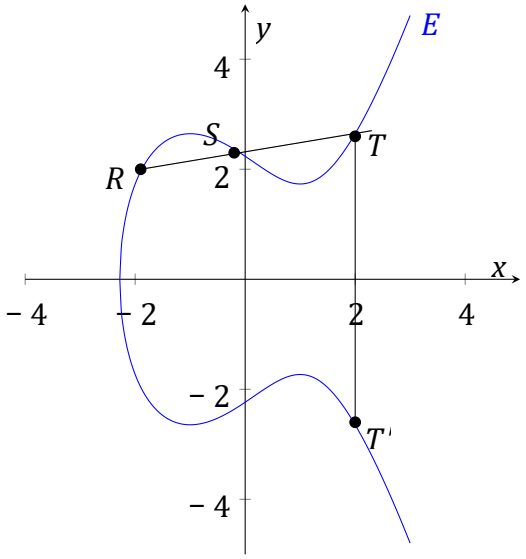
2. PRELIMINARIES

2.1 Group Law on Elliptic Curves

Let $E(F_p)$ be an elliptic curve defined over the finite field F_p, then the set of points of $E(F_p)$ together with the addition operation form an abelian group with point of infinity as the identity element. We use chord and tangent rule to add two points on elliptic curve.

2.2 Geometry of Point Addition on Elliptic Curve

Let $R(r_1, s_1)$ and $S(r_2, s_2)$ be two distinct points on the elliptic curve $E(F_p)$, respectively. To add these two points, we construct a line across R and S, which will meet the curve at the third point T (say). Taking the reflection of this point T about x-axis gives us point T' on E, which is the sum of points R and S.

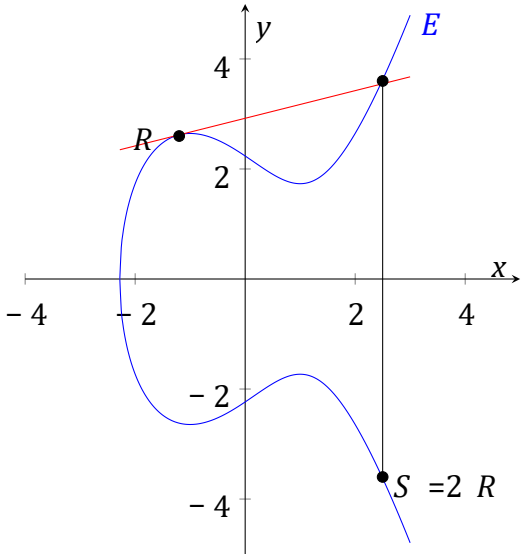


2.3 Identity

Let R be any point of the elliptic curve, then $R + O = O + R = R \; \forall R \in E(F_p)$, where O is the point of infinity and is known as the identity element of the group $E(F_p)$.

2.4 Geometry of Point Doubling in Elliptic Curve

To double the value of a point R on an elliptic curve, we draw a tangent to the curve at point R, this tangent will further intersect the curve at another point, and reflecting this point about the x-axis will give us point S, which is $2R$.



2.5 Point Addition

Let F_p be any finite field with prime p. Then the equation of elliptic curve over F_p is given by $y^2 = (x^3 + ax + b) \ mod \ p$.

Let $R(r_1, s_1)$ and $S(r_2, s_2)$ be two distinct points on $E(F_p)$ and $R + S = T(r_3, s_3)$, then r_3 and s_3 are given by

$$r_3 = \{\lambda^2 - r_1 - r_2\} \ mod \ p$$

and

$$s_3 = \{\lambda(r_1 - r_3) - s_1\} \ mod \ p,$$

where

$$\lambda = \frac{s_2 - s_1}{r_2 - r_1} \ mod \ p.$$

2.6 Point Doubling

Consider two overlapping points R and S on elliptic curve over F_p and $R(r_1, s_1)$ and $S(r_2, s_2) = T(r_2, s_2)$, then r_2 and s_2 are given by

$$r_2 = \{\lambda^2 - 2r_1\} \ mod \ p$$

and

$$s_2 = \{\lambda(r_1 - r_2) - s_1\} \ mod \ p,$$

where

$$\lambda = \frac{3{r_1}^2 + a}{2s_1} \ mod \ p.$$

3. PROPOSED MAPPING SCHEME

Let Alice and Bob be two communicating parties who wants to communicate some message between them. Both, Alice and Bob will agree on some elliptic curve of the form $y^2 = x^3 + ax + b \ mod \ p$, where p is a prime. Let G be the generator point of the elliptic curve. Alice maps the characters of the message to points on elliptic curve by using XOR operation and then encrypts the message point to corresponding cipher text using ECC encryption algorithm given in [7].

Encryption Side:

Step 1: Convert each character of the message to its corresponding ASCII values and further divide the ASCII values into the groups containing ASCII values of three characters each. ASCII values of each character containing less than three digits must be written in the form of three digits by including zero from the left side of the digits.

Step 2: Convert the ASCII values of the first group and x-coordinate of specificpublic key generated by receiver only for the sender into binary form.

Step 3: Perform XOR operation between $x-$coordinate of specific public key generated by receiver for the sender only and binary form of ASCII values of first group and let the resultant be named as 't'.

Step 4: Convert the binary form of 't' to its decimal value and multiply it with generator point of elliptic curve, the resultant will be the mapped message point corresponding to the first three characters of the message.

To map the next three characters of the message, we will follow the same procedure as above but in step 3, we will perform XOR operation between y-coordinate of specific public key generated by receiver for the sender only and binary form of ASCII values of second group.

Similarly, to map the next three characters of the message, we will follow same process but in step 3, we will perform XOR operation between x-coordinate of specific public key generated by sender for the receiver only and binary form of ASCII values of third group. To map the next three characters of the message, in step 3 XOR operation will be performed between y-coordinate of specific public key generated by sender for the receiver only and binary form of ASCII values of third group.

After this, to map the next characters of the message we will keep on adding one in x −coordinate of specific public key generated by receiver for the sender and use it in step three to perform XOR operation.

In case group contain less than 3 characters add ASCII value 032 for each missing character.

Decryption Side:
After performing the decryption algorithm mentioned in [7], Bob will get P_m corresponding to the first three characters of the message and get the original text of the message using the following steps:

Step 1: He obtain 'i ′ corresponding to iG = P_m and converts 'i' to the corresponding binary form using ASCII table.

Step 2: In the next step, he performs XOR operation between binary form of 'i' and the binary form of x-coordinates of specific public key generated by receiver for the sender only and convert the resultant to its decimal value and divide this decimal value to three parts containing three digits each and each part will correspond to ASCII values of real message.

Following the same procedure, he will get the remaining characters of the message to the corresponding mapped points. In step 2, XOR operation of 'i' must be performed with the same value as taken by the sender.

4. ILLUSTRATION

Suppose Alice and Bob be two parties who wants to communicate a message 'Indian' between them. Both the parties agree on an elliptic curve $y^2 = x^3+x+13$ *mod* 31 with the generator point G = (9,10) and specific public key generated by the receiver for the sender only be (8, 29). Specific Public Key will be generated in the similar manner as mentioned in [7].

Encryption Side
To map the characters of the message 'Indian' to point on the elliptic curve, Alice divides the characters of the message in two groups containing three letters each. First group contains the letter 'Ind' and the second group contains the letter 'ian'. He will follow the following steps to map the characters of first group to point on elliptic curve.

Step 1: He converts the ASCII values of 'Ind' to binary form and get '010010010110111001100100' as the resultant.

Step 2: He converts the x-coordinate of the specific public key generated by the receiver for the sender only to binary form and get '00010010'.

Step 3: He performs the XOR operation between '00010010' and '010010010110111001100100' to obtain'010010010110111001100110' and converts it to decimal value to get 73110102.

Step 4: Multiply 73110102 with the generator point G, that is, 73110102 G = (4,22) = P_m which is the corresponding mapped point and encrypt this point using ECC Encryption Algorithm and send the corresponding cipher text to Bob.

Decryption Side
After receiving cipher text from Alice, Bob obtains the mapped point P_m using ECC Encryption Algorithm. Now to get back the character corresponding to P_m, he follows the following steps:

Step 1: He obtain 'i' corresponding to iG= P_m = (9,21), that is, he gets 'i'= 73110102 and convert this to corresponding binary code to get '010010010110111001100110'.

Step 2: In the next step, he performs XOR operation between '00010010' and '010010010110111001100110' to get '010010010110111001100100' and convert this to decimal value to get 073110100. Dividing '073110100' into three parts containing three digits each and each part will correspond to ASCII values of real message and text characters corresponding to these values are 'Ind'.

To map the remaining characters of the message he will follow the same procedure as mentioned in the proposed scheme.

5. ACKNOWLEDGEMENTS

All the authors thankfully acknowledge the support of UGC-SAP. Also, third, fourth and fifth authors acknowledge the support of DST-INSPIRE, CSIR and UGC, respectively.

REFERENCES

1. Amounas, F. and Kinani, E. H. El (2012). Fast mapping method based on matrix approach for elliptic curve cryptography, *International Journal of Information & Network Security*, 1(2), 54-59.
2. Bh, P.,Chandravathi, D. and Prapoorna, R. P. (2010). Encoding and decoding of a message in the implementation of elliptic curve cryptography using Koblitz's Method, *International Journal on Computer Science and Engineering*, 2(5).
3. Hankerson, D., Menezes, A. J. and Vanstone, S. (2004). Guide to Elliptic Curve Cryptography, Springer Professional Computing (1st ed.), Springer -Verlag New York.
4. Johnston, A. M. and Gemmell, P. S. (2002). Authenticated key exchange provably secure against the man-in-middle attack, *Journal of Cryptology*, 2, 139-148.
5. Koblitz, N. (1987). Elliptic curve cryptosystem, *Mathematics of Computation*, 48(177), 203-209.
6. Koblitz, N., Menezes, A. J. and Vanstone, S. (2000). The State of elliptic curve cryptography, *Design, Codes and Cryptography*, 19, 173-193.
7. Kumar, D. S., Suneetha, CH. and Chandrasekhar, A. (2012). Encryption of data using elliptic curve over finite fields, *International Journal of Distributed and Parallel Systems (IJDPS)*, 3, 301-308.
8. Lidl, R. and Niederreiter, H. (1983). Finite fields, Encyclopedia of Mathematics and its Applications, Addison Wesley, Reading, MA. 20.
9. Miller, V. S. (1986). Uses of elliptic curves in cryptography, *In Advances in Cryptology CRYPTO'85 Proceedings*, Crypto 1985, 218, 417-426.
10. Mullen, G. L. and Panario, D. (2013). Handbook of Finite Fields (1st ed.), Chapman and Hall/CRC.
11. Muthukuru, J. and Sathyanarayana, B. (2012). Fixed and variable size text based message mapping techniques using ECC, *Global Journal of Computer Science and Technology*, 12(3) 12-18.
12. Sharma, P. L., Gupta, K., Badoga, N. K. and Ashima (2021). A new mapping scheme using elliptic curve cryptography, *The Journal of Oriental Research Madras*, XCII-LXXVIII, 38-48.
13. Silverman, J. H. (2009). The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 106.
14. Singh, L. D. and Singh, K. M. (2015). Implementation of text encryption using elliptic curve cryptography, *Procedia Computer Science*, 54, 73-82.
15. Trappe, W. and Washington, L. C. (2006). Introduction to Cryptography with Coding Theory (2^{nd} ed.), Prentice Hall: New Jersey.
16. Washington, L. C. (2008). Elliptic Curves Number Theory and Cryptography (2^{nd} ed.), Chapman and Hall/CRC.

****