International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 12 (2020) pp. 204-211

Received: 27 Jan, 2020; Accepted: 18 May, 2020; Published: 6 June, 2020

A Novel Method for Mapping Plaintext Characters to Elliptic Curve Affine points over Prime Field and Pseudorandom Number Generation

Saira Varghese[1]and S.Maria Celestin Vigila[2]

[1]Department of Computer Science and Engineering, Toc H Institute of Science and Technology, Kerala, India
sairav@tistcochin.edu.in

[2]Department of Information Technology, Noorul Islam Centre for Higher Education, Kumaracoil,Tamil Nadu,India
celesleon@yahoo.com

***Abstract*: Large number of active devices over the internet needs to manage huge amount of data. Demand for security of data stored in networked devices with limited computational power and battery life is challenging. Elliptic curve cryptography with smaller key size and less computational overheads protects data at lower cost. Elliptic curve cryptography requires the input to be encoded to the elliptic curve prior to encryption. This paper proposes a novel method for mapping plaintext characters as coordinates of elliptic curve in prime field. It is done by generating elliptic curve coordinates over the arithmetic operations performed on matrices built from ascii codes and its security is highly strengthened by scalar multiplication over base point G of the chosen elliptic curve. Choice of random number and private key for Elliptic curve cryptography can be further strengthened by the proposed novel cryptographically strong pseudorandom generator of 128 bits. It uses large space for choice of seed value to avoid brute force attacks and is built with permutation, substitution and x-or operations.**

***Keywords*:** Elliptic Curve Cryptography, mapping, scalar multiplication, pseudo randomness, permutation, security**.**

I. Introduction

Parallel advancements in computing field necessitate the protection of sensitive data stored in devices over the network [1]-[3].Information security is highly demanded as the digital technology is growing fast. Large amount of data including personal details are kept in various online social media and IoT devices. Sensitive data needs protection using fast and compact algorithms. Along with developments in technology chances of attacks are also increasing.

Cryptography is a branch deals with security of data. Confidentiality, integrity and availability are the triads of information security [4]. Confidentiality refers to protecting the data by encoding to another form making it difficult for attackers to read. Integrity ensures data is not altered. Availability refers to easy availability of the encoded data. Cryptography deals with encryption and decryption algorithms. Different schemes of cryptography viz. Symmetric Key Cryptography (SKC), Public Key Cryptography (PKC) and Pairing Based Cryptography (PBC) algorithms are available for securing the data. Key distribution is a great overhead in SKC and hence PKC is used for key management [5]. Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) are popular among the PKC algorithms. PKC is strongly based on the intractability of the mathematical problems based on geometry, algebra and number theory. Elliptic curves are used by PBC but pairing operation on elliptic curves requires heavier computations [6].

RSA algorithms with 1024 bit key size is being considered as secure, but uncertainties on it are arising as the computing power is increasing steeply. Now-a-days cryptographic systems using RSA are forced to shift to 2048bits or higher key size. ECC provide better security level with less key size than RSA [7]. Increasing key size causes larger memory requirements in devices using RSA. In this context several enterprises are switching over to ECC cryptosystems or Elliptic Curve Integrated Encryption Scheme (ECIES) [8].

ECC needs an encoding and decoding function for mapping messages to elliptic curve points and vice versa. Encryption and decryption using ECC can be performed only over affine points of elliptic curves. Many research works are been carried over elliptic curve mapping functions for developing secure cryptosystems. Several existing methods make use of ascii codes, but produces similar encoded points for same letters making brute force attack possible. The other methods are found to have the overheads of exchanging long common lookup tables.

This paper proposes SM-Mapping, a novel one to one mapping method for plaintext characters to elliptic curve over prime field using matrix containing values synthesized from ascii codes of plain text and matrix of scalar values of base

point G of chosen elliptic curve. The proposed method uses block by block encoding to make same characters getting mapped to different elliptic curve points to prevent brute force attack. No long common lookup tables are to be exchanged in this method. Point addition and point multiplication makes it difficult for an adversary to attack.

Pseudorandom numbers are required for accessing data for various applications over internet. Many pseudorandom generators available today are not secure on its randomness. Pseudo randomness is to be achieved based on computational unpredictability and in distinguishability. Pseudorandom generators satisfying the criteria for cryptography can be called as cryptographic pseudorandom generator. Pseudorandom generator SM-rand used in this proposed algorithm produces highly random unique 128 bit binary. The initial seed is of 96 bit and it is truly unpredictable in polynomial time. Exponential time unpredictability of seed makes SM-rand a cryptographic pseudo random generator.

Remaining sections are organized as follows: Background knowledge on elliptic curve and pseudorandom generators detailed in section II. Related work is provided in section III. Algorithms proposed in detail are presented in section IV. Experimental results and its discussions are included in section V. Conclusion section VI summarizes the relevance of research done in enhancing security of elliptic curve cryptography in modern world.

II. Background Knowledge

A. Prime Field

A finite field, F is a field containing a finite number of elements. A prime field is defined as finite field of prime order p consisting of a set of integers modulo p in which addition and multiplication is carried over modulo p.

B. Mathematics of Elliptic Curve Cryptography

Cryptography on elliptic curve is based on arithmetic applied over elliptic curve points. ECC over prime field with recommended parameters helps in efficient implementation of cryptographic systems [9]. In [9-13] details regarding ECC in prime field are dealt with. ECC uses equation of the form

$$y^2 \bmod p = \left(x^3 + ax + b\right) \bmod p \quad (1)$$

where a and b are the constants with

$$\left(4a^3 + 27b^2\right) \bmod p \neq 0 \bmod p \quad (2)$$

C. Point Addition

Addition of two distinct points $P(x_1, y_1)$ and $Q(x_2, y_2)$ to $R(x_3, y_3)$ uses chord and tangent rule.

$$x_3 = \left(\lambda^2 - x_1 - x_2\right) \bmod p \quad (3)$$

$$y_3 = \left(\lambda\left(x_1 - x_3\right) - y_1\right) \bmod p \quad (4)$$

where

$$\lambda = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) \bmod p \ \ if \ \ P \neq Q \quad (5)$$

Small change either in P or Q can cause a huge change. Inverse of a point P :(x, y) is (x, -y) is used in subtraction of elliptic curve points.

D. Point Doubling

If two points P(x1, y1) and Q(x1, y1) overlap, then R(x3, y3) can be obtained by

$$x_3 = \left(\lambda^2 - 2x_1\right) \bmod p \quad (6)$$

$$y_3 = \left(\lambda\left(x_1 - x_3\right) - y_1\right) \bmod p \quad (7)$$

where

$$\lambda = \left(\frac{3{x_1}^2 + a}{2y_1}\right) \bmod p \ if \ P = Q \quad (8)$$

Point multiplication operation is defined by the repeated addition.

E. Pseudorandom generators

Cryptographic pseudorandom number generators usually generate sequences of 0s and 1s from a seed and are deterministic with reproducible sequences. The features of pseudorandom numbers are [31] uniformity and scalability. The most popular PRNGS [31] are discussed here.

Algorithm for Linear Congruential Generator (LCG) LCG developed by D. H. Lehmer in 1949 is based on a linear recurrence equation [2] $x_{n+1} = (ax_n + c) \bmod m$ where x_0 is the initial seed and a,c and m are constants, also c and m are to be relatively prime. The limitation of LCG is that the random values should not exceed m and "chosen input attack" is possible.

Blum Blum Shub (BBS) is a PRNG [2] with the equation $x_{n+1} = x_n^2 \bmod m$ and m should be product of two large primes. Even though this is secure based on prime factorization, it is not fast.

Linear Feedback Shift Register (LFSR) is a common hardware based generator with shift register taking linear function of the previous state as the input.

III. Related Work

In the literature, many research works on the features of elliptic curve for security applications are reviewed. ECC requires the text to be encoded using a one way function prior to encryption. Some of the relevant works on mapping messages to elliptic curve points and pseudorandom number generations are discussed in this section.

In [14] ascii values of plaintext characters are grouped as big integers. The mapping scheme has the advantage of avoiding exchange of predefined tables but same plain text will be encoded differently during elliptic curve encryption only. A mapping method based on a random matrix of letters and digits generated using genetic algorithm is used in [15] but it can encode only letters and digits. In the scheme same letter will not be encoded differently. On looking into sample encoded and decoded values similar patterns can be easily identified. Security is ensured only upon encrypting the mapped points. In [16] a mapping table in which the ascii table is sequentially numbered to perform scalar multiplication over chosen base point and the table is to be exchanged for decoding. Brute force attack is possible as only 128 scalar multiplications are involved. Repeated text will be mapped to same points makes the known plaintext attack possible. In [17] the authors proposed a mapping methodology that multiplies plaintext

character with orders of base point sequentially and multiplying with a pre-defined matrix. This system used scalar multiplications that enhanced security, but requires a predefined mapping table to be exchanged. If predefined matrices are chosen same for different blocks of text same plain text will not be encoded differently.

In [18] the mapping method discussed initially relates the plaintext to predefined scalar values of chosen elliptic curve point, which in turn was multiplied by a predefined matrix to yield mapped points. This method requires predefined set of scalar values and matrix to be exchanged to the communicating party. If matrix selected is repeated, the mapped points will also repeat. In [19] various mapping schemes viz: mapping of plaintext to ascii, plaintext exored with an initial vector mapped to ascii, grouping of mapped ascii values, usage of matrix and mapping of ascii values and a sequence ordering were discussed, where in many of the methods security is compensated to a small extent for faster mapping. In [20] the plaintext is encrypted using Hill cipher and then converted to ascii but hill cipher is always prone to known plaintext attack.

In [21] mapping method the plaintext characters are grouped and converted to ascii and padded with n zeroes. Extract the decimal number corresponding to the value stored as x coordinate of elliptic curve point and substituting in elliptic curve equation y coordinate is generated. This scheme has the chance that frequent occurrence of letters may be attacked. Python's power to handle big integers make the reverse mapping simple which includes only decimal to binary conversion and then to ascii conversion which is at high risk of vulnerability of brute force attack.

In [22] mapping method converts plaintext characters into ascii and further into hexadecimal. The hexadecimals are grouped to 192 bit x and y values. This method has the advantage that no padding of bits is required but mapping will not prevent known plain text attack. . In [23] algorithm of ECIES, different coordinate system is discussed. In [24] mapping is based on ascii values of plaintext followed by ECC encryption. [27-30] is reviewed to analyze the need of confidentiality and role of elliptic curve cryptography. In [33] elliptic curve is used in pseudorandom generation and the method involves extensive operations. Substitution and permutation networks are reviewed from [34].In [36]160 bit generated by SHA-1 from message digest, current time and random binary input. It is followed by substitution for the first 80 bits and generates 128 bits by concatenation. The method depends on real random source makes it difficult to reproduce. In [37] proposed method make use of RC5 following the Feistel network and generates 64 bit output.RC5 is vulnerable to differential attacks but increasing the number of rounds can make RC5 safe. In [38] characteristics of block cipher based pseudorandom generators are discussed. In [39] paper emphasizes the need of simple permutations to make it feasible for low power devices. Younes et.al.in [40] proposed a message mapping scheme coupled with elgamal encryption for integer messages and also the paper points out the need of ECC for acquiring high security.In [41] the proposed mapping scheme involves binary and decimal conversons along with xor operations for blocks of plain text which can become interrelated if the intruder retrieves the initialization vector.

IV. Proposed Algorithms for Mapping and Pseudorandom Generation

This section describes a novel method for mapping plaintext characters to elliptic curve points. Each plaintext character is converted to its ascii value and its position is added to ascii. Then invert the binary equivalent of the obtained and in turn obtain the decimal equivalent of the inverted. This decimal will serve as x coordinate for the cubical equation of elliptic curve. The y coordinate is assigned double the value of x coordinate. Elliptic mapper algorithm will check if the supplied coordinates satisfies the equation for elliptic curve. If not, assign a large value as counter and then increment x and y and verify the elliptic curve cubical equation and repeat this till the coordinates satisfying the equation is generated. Difference between the x value supplied initially and the finally obtained x value are stored separately. The newly generated elliptic curve point is to be added with chosen scalar value of base point G, to enhance the security keys from not being limited to ascii values.SM-Mapping algorithm shown in figure 1 describes the techniques for mapping input to encoded text.

The proposed mapping scheme is suitable for applications preferring higher security. Generated different cipher text even if chosen the same scalar values for all blocks of text of a single document ensures security offered by the proposed scheme. Choosing different scalar values for different blocks will create overhead in exchanging information with users. Choice of large p values for elliptic curve can make the mapping scheme more difficult to attack for intruders.

Decoding does the reverse of the encoding process. Decoding requires the exchange of scalar values and difference matrix. This scheme is viable for secure encoding of lengthy documents comparing to other existing methods of mapping schemes discussed in section III.

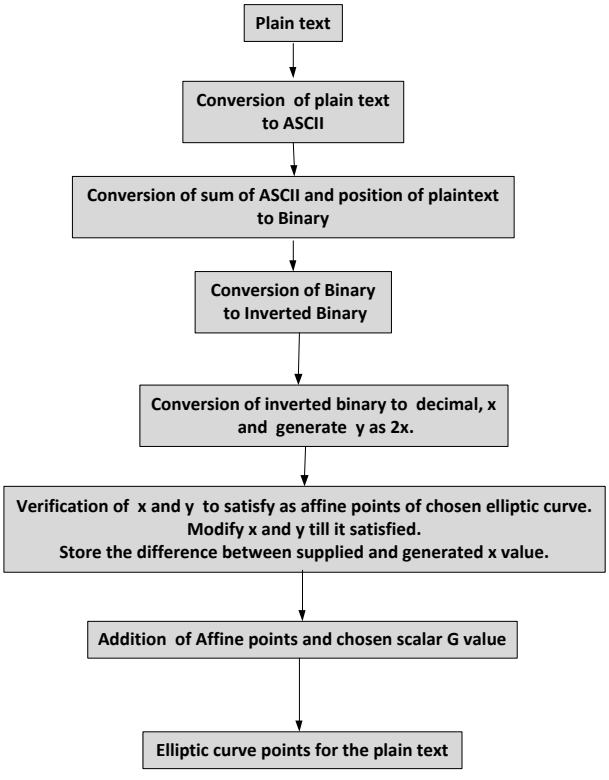

Figure 1. SM-Mapping Encoding

In our proposed SM-Mapping algorithm given in figure 2, enhanced encoding techniques are used. The plaintext characters are grouped into a block of m characters and each block is transformed into a m X n matrix where number of columns, n is fixed to two. The column values of matrix are indirectly related to ascii values of plaintext. Another m X n matrix contains the coordinates of random scalar values for base point G of the chosen elliptic curve. Addition of both matrices generates encoded values of plain text.

Input : Plaintext 'Message', Domain Parameters a, b, p, G, scalar values
Output : Encoded distinct values for plaintext with gmatrix and difference as secrets
FUNCTION encode ():
public parameters:p,a,b,G of chosen elliptic curve
1. Initialize i←0,j←0
2. while (i<m)
i←0,j←0
1) equivalentascii [i] ← message[i]
2) binarray [i] ← equivalentascii[i] + i
3) invarray[i] ← inverse of binarray[i]
4) decimalarr [i] ←decimal equivalent of invarray
5) xymatrix[i][j] ← decimalarr[i],2*decimalarray[i]
6) epmatrix [i][j] ← ellipticmapper(xymatrix[i][j])
7) difference [i] ←xymatrix[i] - epmatrix [i]
8) gmatrix[i][j] ←(s[i])(Gx,Gy)
9) mappedlist [i][j] ← Add(epmatrix, gmatrix)
10) i←i+1,j←j+1
3. return(mappedlist,gmatrix,diference)

Figure 2. Pseudo code for SM-Mapping

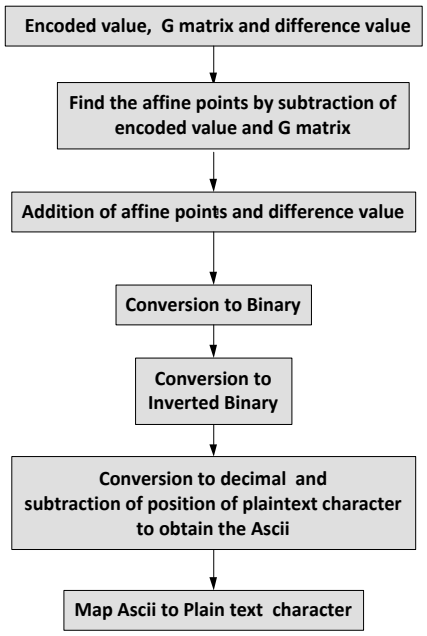

Figure 3. SM-Mapping Decoding

Decoding shown in figure 3 takes input containing encoded values and scalar G values. Resultant matrix obtained by subtracting encoded values and scalar G values is added to the trapdoor difference value .It is followed by conversion to binary and then to inverted binary and finally to decimal equivalent. Subtract the position and map the rest with ascii table to generate the plain text. [25]

The proposed mapping scheme can utilize pseudorandom numbers for choosing scalar values of chosen base point. Elliptic curve cryptosystem also uses pseudorandom numbers for encryption. Pseudorandom generators use seed as input and perform operations on the seed to produce pseudorandom numbers. Pseudorandom generators always use one way functions for expanding small seed values to longer outcomes. [26].SM-rand is a deterministic polynomial time cryptographically secure pseudorandom number generator algorithm that uses one way functions with 12 random characters as input to generate pseudo randomness. The 12 random characters is equivalent to 96 bits. Seed value is chosen to be 96 bits to overcome the polynomial time cryptanalytic attacks.

Figure 4 represents the SM-rand 128 bit generator and Figure 5 shows its pseudo code.

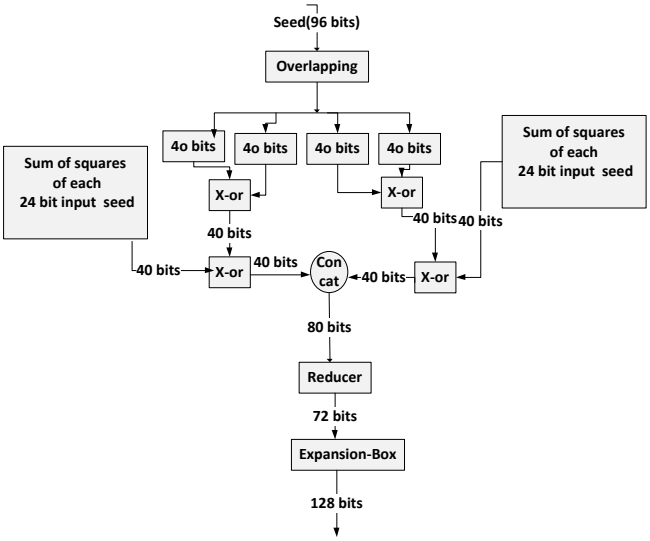

Figure 4. SM-rand

The input is overlapped to generate four 40 bits chunks. For achieving higher diffusion, a conjecture in number theory, four square theorem is also applied over the four input parts of 24 bits each to generate another 40 bit chunk. Exclusive or operation is done on each pair of 40 bits and the result is concatenated as 80 bits chunk. Reducer breaks each 20 bit of 80 bit as 'x value' and coefficients for the quadratic equation, $y=ax^2+bx+c$.First 72 bits produced from the nonlinear function serve as input to expansion box. The reducer should pad additional zeroes if fewer than 72 bits. Expansion permutation box shown in figure 6 is used to produce 128 bits out of 80 bits. On applying the same seed the randomness can be reproduced. The output obtained is unpredictable and non-reversible. For generating more number of random sequences permute the seed using the p-box shown in figure 7.

Input : seed is 12 characters (96 bit binary)
Output : 128 bit random number

FUNCTION SM_rand (seed)

1. r1←seed[1].seed[2].seed[3].seed[4] //32 bits
2. r2←seed[5] //8 bits
3. r3←r1.r2 //40 bits
4. r4←seed[8] //8 bits
5. r5←seed[9].seed[10][seed[11].seed[12] //32 bits
6. r6←r4.r5 //40 bits
7. y←(seed[0..24]^2)+(seed[24..48]^2)+(seed[48…72]^2) +(seed[72..96]^2) //40 bits
8. r7← (r3 ⊕r6) ⊕y //40 bits ex-or operation
9. r8←seed[11] //8 bits
10. r9←seed[2].seed[3].seed[4].seed[5] //32 bits
11. r10←r8.r9 //40 bits
12. r11←seed[7].seed[8].seed[9].seed[10] //32 bits
13. r12←seed[12] //8 bits
14. r13←r11.r12 //40 bits
15. r14 ← (r10 ⊕ r13) ⊕ y //40 bits ex-or operation
16. r15 ←r7.r14 //80 bits
17. R=E-dbox(Reducer(r15)) //128 bit
18. return

Plain text	First Occurrence	Second Occurrence
h	(13,16)	(4,0)
e	(12,4)	(18,20)
l	(5,4)	(13,16)
l	(6,4)	(9,16)
o	(7,11)	(19,5)

Input : 80 bit binary
Output : 72 bit binary
Function: Reducer()
1. a=dec(r15[0..19])//convert to decimal
2. b=dec(r15[21..39])
3. c=dec(r15[40..59])
4. x=r15[60…79]
5. Y=a*x*x+b*x+c
6. If len(y)<72 pad with zeroes otherwise y=[0…71]
7. return y

Figure 5.SM-rand pseudocode

1	59	73	82	65	46	21	29	37	64	49	74
5	61	75	83	63	52	22	15	38	68	53	76
30	66	84	85	7	56	23	31	39	71	60	81
13	57	86	89	8	16	24	32	40	48	70	87
14	62	92	90	9	17	25	33	51	45	3	88
47	67	93	91	10	18	26	34	42	41	4	96
6	72	94	78	11	19	27	35	43	69	55	80
2	58	95	77	12	20	28	36	44	54	50	79

Figure 6. Ebox

1	17	33	49	5	13	21	29	37	45	53	61	52	36	20	4
5	21	37	53	6	14	22	30	38	46	54	62	56	40	24	8
9	25	44	1	7	15	23	31	39	47	55	63	69	43	28	12
13	29	48	2	8	16	24	32	40	48	56	64	70	47	32	16
14	30	45	3	9	17	25	33	41	49	57	65	71	46	31	15
10	26	41	4	10	18	26	34	42	50	58	66	1	42	27	11
6	22	38	54	11	19	27	35	43	51	59	67	55	39	23	7
2	18	34	50	12	20	28	36	44	52	60	68	51	35	19	3

Figure 7.P box

V. Results and Discussions

A. *Experimental Results*

The proposed methods SM-Mapping and SM-rand is implemented using Python3 in Intel(R) Core (TM) i3-5005U CPU @ 2.00GHz processor having 4GB RAM and 64 bit OS,X-64 based processor.

B. *Performance Analysis of SM-Mapping and SM-rand*

Experimented using elliptic curve with the parameters a=1,b=1,p=23,G=(0,1) ,scalar values chosen are 1,2,3,4 and 5 for both blocks of five characters each. Table 1 shows the encoded values.

*Table 1.*Encoded points for ‘hello” in two occurrences

In this experiment the chance of using same scalar values for different block is considered. The encoded points have no relation between two occurrences.

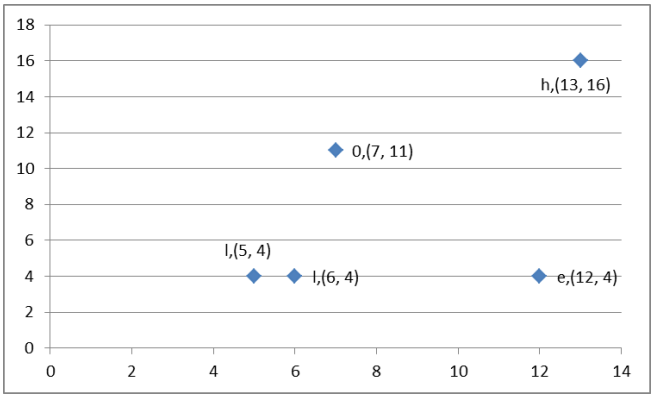

Figure .8. SM-Mapping for “hello” in first occurrence**.**

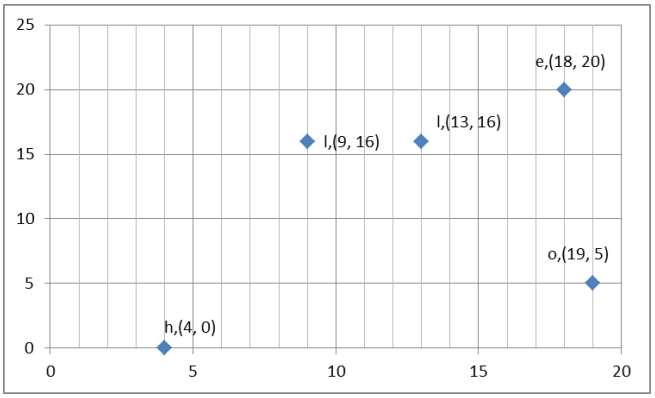

Figure.9. SM-Mapping for "hello" in second occurrence

The encoded values of hello are shown for its two occurrences in figure 8 and figure 9 clearly shows that the same plain text is mapped differently making it difficult for intruders to guess.

Statistics is one of the best measures to check randomness. The uniform distribution of bits in binary random sequence is an important analysis which can contribute to measure of randomness like entropy. The quality of 128 bit binary random sequences generated by SM-rand is tested using NIST statistical test suite [35]. Results of those statistical tests obtained as p-values are compared with α=0.01and if the obtained p-values are >= α, test is success otherwise failure. Test results of sample random 128bit binary sequences pass the test. Monobit frequency test, runs test, test for longest runs of ones in a block, approximate entropy test and cumulative sum test applied over sample 128 bit random numbers are successful.

C. Security Analysis

From the results of SM-Mapping it is clear that the proposed method is free from brute force attacks as scalar values of G matrix is randomly chosen for individual plain text characters act as first level of complex key. Plaintext is converted to elliptic curve points based on its position and followed by addition with randomly scaled elliptic curve points; generates different points for same character and makes it free from chances of frequency attacks. Randomly chosen scalar values will act as salt for key of difference values for being decoded correctly prevents the proposed scheme from pre computation attacks. The proposed mapping scheme meets confidentiality on encoding the input. This method is secure under a hard problem known as elliptic curve logarithm problem through elliptic curve scalar multiplications. In this scheme when a user is provided with matrix containing encoded elliptic curve points even if the user knows G he couldn't identify the actual scalar value of G used with each block of plain text unless specified. Unless knowing the order of scalar values of G and the difference values exchanged by data owner, the user could not decode correctly the transformed values of ascii. The order of the cipher text is to be preserved for successful decryption as position is included in encoding procedure. Hence the proposed encoding method is a trapdoor whose inversion requires extra information other than encoded points.

Summary of defending mechanism for the proposed mapping method over different cryptanalytic attacks is shown in table 2.Comparison with other mapping schemes is shown in table 3.

Type of attack	Known to Cryptanalyst	Defending mechanism of proposed mapping
Cipher text Only	Encoded value of plaintext, mapping algorithm	Scalar values chosen for G from the set of counting numbers is required for decoding is a hindrance for brute force attack.
Known plaintext	Mapping algorithm, cipher text, sample plaintext cipher text pairs formed with the secret keys	Same plaintext character will be encoded differently in different occurrences as position of plaintext varies and random scalar values for multiplication of elliptic curve point are used in encoding.
Chosen plain text	Mapping algorithm, cipher text, cipher text created for chosen plaintext	Randomness in scalar values of G is again a hindrance for observing any patterns for individual cipher text plaintext pairs.

*Table 2.*Analysis of Cryptanalytic attacks

Scheme	Scalar multiplication for mapping	Exchange of predefined tables	Same text uses different encoding in different occurrences
Laiphrakpam et.al.[14]	No	No	No
Gbashi [15]	No	Yes	No
Omar Reyad[16]	Yes	Yes	No
Kamalakannan et.al.[17]	Yes	Yes	No
Balamurugan et.al[18]	Yes	Yes	No
Aritro et.al.[21]	No	No	No
Keerthi et.al.[22]	No	No	No
Proposed Scheme	Yes	No	Yes

. *Table 3.*Comparison with other mapping schemes

SM_rand is supported by seed values of 12 characters from combination of alphabets, digits, punctuations and special characters makes the guess based attacks practically impossible.95^12 large sample space for seeds provides exponential time security to SM-rand from attackers. According to theoretical computer science for adversaries if no

adversary can distinguish SM-rand generated and other 128 bit random, indistinguishability is met [32].In addition to seed other inputs are also generated from the seed and used in pseudorandom generation makes the proposed scheme a pseudorandom generator with input [38]. Round function used in the algorithm ensures the security of SM-rand as it holds properties of diffusion,confusion and is only reproducible with knowledge of seed.SM-rand operations are composed of xor, nonlinear function and expansion permutation and hence its security is highly strengthened. Confusion or nonlinearity is gained through the quadratic equation applied over 80 bit binary to produce 72 bit binary. SM-rand also passed test of NIST suite which is a tool for breaking round function.

VI. Conclusion

The proposed mapping method suggested in this paper is proved to be more secure as same characters are encoded to different elliptic curve points. Communicating parties do not need a lengthy common look up table. Point addition and scalar multiplication on elliptic curves of large values of 'p' of elliptic curve removes the scope of guess works for the attackers. It is obvious that for the proposed pseudo random number generator an adversary cannot guess the outcomes without the knowledge of seed. Proposed mapping method and pseudo random generation for elliptic curve encryption ensures higher confidentiality of messages. ECC is a good choice for securing real time applications in smart devices with less computational power. Encryption on the encoded point using elliptic curve using the proposed pseudo random generator can make it more secure. On feeding SM-rand inputs to SHA-256 algorithm 256 bit values can be produced and can be used in block chains like Bitcoin or Etheruem.

References

[1] Mimi Ma, Debiao He, Neeraj Kumar, Kim-Kwang Raymond Choo and and Jianhua Chen, "Certificateless searchable public key encryption scheme for industrial internet of things", *IEEE Transactions on Industrial Informatics Vol. 14, No.2*,pp. 759-767,2018

[2] Shu, Xiaokui, Danfeng Yao, and Elisa Bertino. "Privacy-preserving detection of sensitive data exposure", *IEEE transactions on information forensics and security, Vol.10, No.5*, pp 1092-1103, 2015.

[3] Jian Shen, Tianqi Zhou, Xiaofeng Chen, Jin Li, and Willy Susilo,"Anonymous and traceable group data sharing in cloud computing" , *IEEE Transactions on Information Forensics and Security Vol.13,No.4*, pp. 912-925, 2018,

[4] Stallings William, *Cryptography and network security: principles and practice*. Pearson Education India, 2003.

[5] Zhe Liu, Johann Großschadl, Zhi Hu, Kimmo Jarvinen, Husen Wang and Ingrid Verbauwhede,"Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things", *IEEE Transactions on Computers Vol. 66,No.5*,pp. 773-785, 2017.

[6] Friederike Brezing and Annegret Weng, "Elliptic curves suitable for pairing based cryptography", *Designs, Codes and Cryptography* Vol.37,pp. 133-141, 2005.

[7] Reza Azarderakhsh, Kimmo U. Järvinen, and Mehran Mozaffari-Kermani, "Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications." *IEEE Transactions on Circuits and Systems I,Vol .61,No.4*,pp.1144-11554 ,2014.

[8] V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila,"A survey of the elliptic curve integrated encryption scheme", *Journal of Computer Science and Engineering, Vol.2, No.2*, pp. 160-223, 2010.

[9] Smart Nigel P,"A comparison of different finite fields for elliptic curve cryptosystems." *Computers & Mathematics with Applications Vol 42, No.1-2*, pp.91-100 , 2001.

[10] Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone," *Guide to elliptic curve cryptography*", Springer Science & Business Media, 2006.

[11] Wuqiong Pan, Fangyu Zheng, Yuan Zhao, Wen-Tao Zhu and Jiwu Jing, "An efficient elliptic curve cryptography signature server with GPU acceleration." *IEEE Transactions on Information Forensics and Security, Vol. 12, No.1*, pp.111-122, 2017.

[12] Zilong Liu, Dongsheng Liu and Xuecheng Zou,"An Efficient and Flexible Hardware Implementation of the Dual-Field Elliptic Curve Cryptographic Processor", *IEEE Transactions on Industrial Electronics Vol. 64,No.3*,pp.2353-2362,2017

[13] Koblitz, Neal, Alfred Menezes, and Scott Vanstone. "*The state of elliptic curve cryptography*." Designs, codes and cryptography Vol. 19, No.2-3, pp. 173-193, 2000.

[14] Singh Laiphrakpam Dolendro, and Khumanthem Manglem Singh, "Implementation of text encryption using elliptic curve cryptography." *Procedia Computer Science Vol 54*,pp. 73-82, ,2015.

[15] Gbashi Ekhlas Khalaf, "Proposed Secret Encoding Method Based Genetic Algorithm for Elliptic Curve Cryptography Method." *Iraqi Journal of Information Technology Vol. 8, No.3*, pp. 21-46, 2018.

[16] Omar Reyad," Text Message Encoding Based on Elliptic Curve Cryptography and a Mapping Methodology", *International Journal of Information Sciences Letters 7, Vol.1*, pp7-11, 2018.

[17] Kamalakannan, V and S. Tamilselvan, "Security enhancement of text message based on matrix approach using elliptical curve cryptosystem" ,*Procedia Materials Science ,Vol.10*, pp. 489-496, 2015.

[18] Balamurugan, R, Kamalakannan.V, Rahul Ganth.D and Tamilselvan.S, "Enhancing security in text messages using matrix based mapping and ElGamal method in elliptic curve cryptography", In *Proceedings of the IEEE International Conference on Contemporary Computing and Informatics*, pp. 103-106,2014.

[19] Dhanashree Toradmalle, Saudamini B. Ingale, Miheeka G. Chaudhary, Aishvarya Akshaya V and Anjali R. Patil, "A Survey of Different Encoding Schemes for Improving the Efficiency of Text based Cryptosystem using ECC" ,*International Journal of Computer Applications Vol.153,No.9*,pp. 39-44,2016.

[20] Agrawal, Komal, and Anju Gera. "Elliptic Curve Cryptography with Hill Cipher Generation for Secure Text Cryptosystem", *International journal of computer applications Vol.106, No.1*, pp.18-24, 2014.

[21] Sengupta, Aritro, and Utpal Kumar Ray. "Message mapping and reverse mapping in elliptic curve cryptosystem", *Security and Communication Networks, Vol. 9,No.18*, pp. 5363-5375, 2016.

[22] Keerthi K and B. Surendiran. "Elliptic curve cryptography for secured text encryption", In *Proceedings of the IEEE International Conference on Circuit, Power and Computing Technologies*, pp. 1-5,2017.
[23] Setiadi, Iskandar, Achmad Imam Kistijantoro, and Atsuko Miyaji, "Elliptic curve cryptography: Algorithms and implementation analysis over coordinate systems", In *Proceedings of the* 2nd IEEE International Conference on Advanced Informatics: Concepts, Theory and Applications,pp. 1-6, 2015.
[24] Ekta Mehta and Arun Solanki," Minimization of mean square error for improved euler elliptic curve secure hash cryptography for textual data", *Journal of Information and Optimization Sciences, Vol.38, No.6*, pp.813-826, 2017.
[25] Vigila, S. Maria Celestin, and K. Muneeswaran. "Implementation of text based cryptosystem using elliptic curve cryptography." In *Proceedings of the IEEE International Conference on Advanced Computing*, pp.82–85, 2009.
[26] H åstad, J., Impagliazzo, R., Levin, L. A., & Luby, M, "A pseudorandom generator from any one-way function." SIAM Journal on Computing 28.4, pp.1364-1396, 1999.
[27] Varghese Saira, and S. Maria Celestin Vigila, "A comparative analysis on cloud data security", *In Proceedings of the IEEE Global Conference on Communication Technologies*, pp. 507-510,2015.
[28] Antonio Cortina Reyes, Ana Karina Vega Castillo, Miguel Morales-Sandoval and Arturo D´ıaz-P érez,"A performance comparison of elliptic curve scalar multiplication algorithms on smartphones", In CONIELECOMP 2013, 23rd International Conference on Electronics, Communications and Computing, IEEE, pp. 114-119. 2013.
[29] Vigila, S. Maria Celestin, and K. Muneeswaran, "Key generation based on elliptic curve over finite prime field", *International Journal of Electronic Security and Digital Forensics Vol. 4, No.1*, pp. 65-81, 2012.
[30] Aung, Tun Myat, and Ni Ni Hla, "A Study of General Attacks on Elliptic Curve Discrete Logarithm Problem over Prime Field and Binary Field", *World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering, Vol. 4,No.11*, pp. 1153-1160,2017.
[31] Aqeel Khalique,Auqib Hamid Lone and Syed Shahabuddin Ashraf,"A Novel Unpredictable Temporal based PseudoRandom Number Generator",*International Journal of Computer Applications (0975 – 8887),Volume 117 – No.13*, pp. 23-28,May 2015
[32] Oded Goldreic,"Computational Complexity: A Conceptual Perspective", Cambridge University Press. 2008.
[33] Zbigniew Adam Kotulski and Omar Reyad "On Pseudo-Random Number Generators Using Elliptic Curves and Chaotic Systems", Applied Mathematics & Information Sciences, Vol.9, pp. 31-38, 2015.
[34] Miles Eric and Eanuele Viola,"Substitution -permutation networks, pseudorandom functions, and natural proofs", Crypto 2012, LNCS, Springer vol. 7417, pp. 68–85,2012.
[35] Zaman JKMSU and Ghosh R, "A review study of NIST Statistical Test Suite: Development of an indigenous computer package", *Institute of Radio Physics & Electronics, University of Calcutta, Kolkata, India*, 2011.
[36] Hammood, M. M., T. S. Atia, and A. Y. Yousuf. "Design and Implement Pseudo Random Number Generator for Block Cipher Encryption Algorithm ", *Tikrit Journal of Pure Science*, Vol.*14* (3), pp. 13-16, 2009.
[37] Hashim, Ashwaq Talib, and Zaid Mundher Radeef. "Proposed Pseudo Random Generator Based on RC5 Block Cipher." *Iraqi Journal Of Computers, Communication And Control & Systems Engineering 17.1* pp. 33-41,2017.
[38] Ruhault, Sylvain. "SoK: security models for pseudo-random number generators.", *IACR Transactions on Symmetric Cryptology* , pp. 506-544, 2017.
[39] Michaels, Alan J. "Improved RNS-based PRNGs." *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1-5, 2018.
[40] Younes, Lahraoui, Amal Youssef, and Lazaar Saiida, "Definition and Implementation of an Elliptic Curve Cryptosystem using a New Message Mapping Scheme.", *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, pp. 1-6, 2020.
[41] Almajed, Hisham N., and Ahmad S. Almogren,"SE-Enc: A Secure and Efficient Encoding Scheme Using Elliptic Curve Cryptography", *IEEE Access 7*,pp. 175865-175878,2019.

Author Biographies

Saira Varghese completed her B.Tech in Computer Science & Engineering from Mahatma Gandhi University, Kerala in 2005 and M.Tech from Anna University, Chennai in 2013.She is currently Assistant professor at Department of Computer Science & Engineering, TocH Institute of Science & Technology, APJ Abdul Kalam Technological University, Kerala, India. She is pursuing research in data security under Noorul Islam Centre for Higher Education.Her teaching and research interests are in Cryptography and Cloud Security.

S. Maria Celestin Vigila completed her B.E. in Computer Science and Engineering in 1996 and M.E. in Computer Science and Engineering in 1999. She completed her Ph.D. in the area of data security from Anna University, Chennai. She is currently Associate Professor in the Department of Information Technology, Noorul Islam Centre for Higher Education, Kumaracoil and member of ISTE and IET. She is the reviewer for quite a few peer reviewed international journals. Her research interest includes Cryptography and Network Security, Wireless Networks and Information Hiding.