November-December 2019
ISSN: 0193-4120 Page No. 5128 - 5136

Multifarious Mapping Schemes on Elliptic Curve Cryptography for IoT Security

G. Dhamodharan[1], Dr. S. Thaddeus[2]
[1]Assistant Professor, [2]Associate Professor
[12]PG & Research Department of Computer Science,
Don Bosco College (Co-Ed), Guezou Nagar, Yelagiri Hills,
Affiliated to Thiruvalluvar University.
Email: haidhamo@gmail.com

Article Info
Volume 81
Page Number: 5128 - 5136
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *24 December 2019*

Abstract

Elliptic Curve Cryptography (ECC) is a current area of enquiry in the domain of Cryptography. ECC is beneficial in various schemes of cryptography due to its lowered key size and rapid generation of key. It is suitable for IoT devices to provide security. Many IoT devices have restricted amount of storage and processing ability. They frequently need to run on low power. Heavy encryption dependent approaches are not a good fit for these constrained devices. They are incapable of performing complicated encryption and decryption quick enough to be able to secure data in real-time transmission. Transformation of text messages to elliptic curve points has always been enigmatic. Comparing to other cryptographic algorithms the arithmetic involved in elliptic curve cryptography is computationally less complicated. This paper provides an overview of elliptic curves, different mapping schemes and their application in cryptography. The emphasis is on the performance gains to be acquired by using elliptic curve cryptography as an alternative to conventional cryptosystem like RSA.

Keywords: *Elliptic Curve Cryptography, Mapping Scheme, IoT, Security.*

1. Introduction

Cryptography is amethod in securing data communicated. It encrypts and decrypts data. In cryptography there are two types namely Private and Public Key cryptography. ECC is one technique of public key cryptography that provides better security. For instance, 256 bit elliptic curve provides equal security similarto 3072 bit RSA. It is also hard to solve discrete logarithmic problems on elliptic curve. The elliptic curve over prime field encompasses coefficients of the elliptic curve and the base point, which is a point on the elliptic curve [1]. The selected curve showcased is known to both the partiessender and the receiver. Scalar multiplication is the main operation in elliptic curve cryptographythat encompasses Point doubling and Point addition.

2. Elliptic Curve Cryptography

Cryptography is conversion of text information to make them harmless and protected from impostors. Elliptic Curve Cryptography (ECC) is a public key cryptography industrializedseparately in the year 1985 by Victor Miller and Neal Koblitz [2]. In ECC we will be using the curve equation of the form

November-December 2019
ISSN: 0193-4120 Page No. 5128 - 5136

$$Y^2=x^3+mx+n \quad (1)$$

which is recognizedas Weierstrass equation, where m and n are the constants with

$$4m^3+27n\neq 0 \quad (2)$$

2.1 ECC Over Finite Field in Mathematics

Elliptic Curve Cryptographic operations in finite fields are done using the coordinate points of the elliptic curve. The equation of Elliptic curve over finite field is shown below:

$$y^2=(x^3+mx+n)\text{mod}p \quad (3)$$

2.1.1 Point Addition

The two points P1(x_1, y_1) and P2(x_2, y_2) are different. P1 + P2 = P3(x_3, y_3) is calculated using the following equations.

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod p \quad (4)$$

$$y_3 = (\lambda(x_1 - x_2) - y_1) \bmod p \quad (5)$$

$$\text{where}\lambda = \frac{y2-y1}{x2-x1} \; mod\; p \quad (6)$$

2.1.2 Point Doubling

The two points P1(x_1, y_1) and P2(x_2, y_2) are overlap. P1 + P2 = P3(x_3, y_3) is computed by the subsequent equations.

$$x_3 =(\lambda^2 - 2x_1)\text{mod } p \quad (7)$$

$$y_3=(\lambda(x_1 - x_2) - y1) \bmod p \quad (8)$$

$$\text{where}\lambda = \frac{3x_1^2+m}{2y_1} \; mod\; p (9)$$

2.1.3 Scalar Multiplication

Lease S be a random point on the elliptic curve. The operation of multiplication over S is done by the repetitive addition. To achieve encryption and decryption using ECC, k[S] plays a vital role as in exponentiation operation. K[S]= S + S + S +⋯+S times i.e, 10S = S+S+S+S+S+S+S+S+S+S (9 additions). To reduce number of additions we can use point doubling

S+S=2S(Doubling)

2S+2S=4S(Doubling)

4S+4S=8S(Doubling)

8S+2S=10S(Addition)

2.2 Elliptic Curve Cryptography Advantages

The main advantage of ECC is that it's stronger than RSA for key sizes in use nowadays. This small key is quicker and requires a smaller amountcalculating power than other first-generation encryption public key algorithms. The typical ECC key size of 256 bits is equal to a 3072-bit RSA key. To stay in advance of an invader's computing power, RSA keys must acquire longer. The welfares of ECC over RSA are mainly significant in wireless devices, where computing power, storage and battery life are constrained. ECC provides equal security for lesser bit size than RSA [3].

Key Size of ECC (In Bits)	Key Size of RSA (In Bits)	Ratio (In Bits)
106	512	1:4
132	768	1:5
160	1024	1:6
224	2048	1:9
256	3072	1:12
384	7680	1:20
512	16380	1:30

Table 1: ECC and RSA Key Size

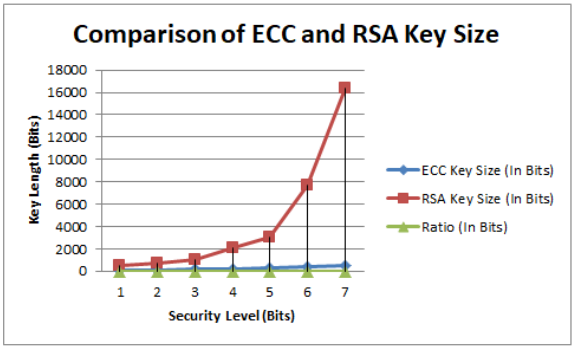

Fig 1: Comparison of ECC and RSA Key Size

November-December 2019
ISSN: 0193-4120 Page No. 5128 - 5136

2.3 Elliptic Curve Points Generation

An elliptic curve in finite field Ep(m,n) contains of all points (x,y) with the point at infinity ∞ which satisfies equation (3) by selecting m=1, n=1, and p=23.

Steps to acquire points on the elliptic curve

1: Decide y^2 mod 23 for y=0 to 22

2: From x= 0 to 22, decide $y^2 = (x^3+x+1) \bmod 23$

3: Contest the y^2 value in step 2 and step 1

4: The matching x and y will be the elliptic curve point if the x and y value is matched

5: Its converse will also be exist for any point on the elliptic curve

x	$m=(x^3+x+1) \bmod 23$	$(m^l) \bmod p = m^{11} \bmod 23$	$y^2 \epsilon Q23$	Y
0	1	1	YES	(0,1), (0,22)
1	3	1	YES	(1,7), (1,16)
2	11	22	NO	-
3	8	1	YES	(3,10), (3,13)
4	0	0	NO	-
5	16	1	YES	(5,4), (5,19)
6	16	1	YES	(6,4), (6,19)
7	6	1	YES	(7,11), (7,12)
8	15	22	NO	-
9	3	1	YES	(9,7), (9,16)
10	22	22	NO	-
11	9	1	YES	(11,3), (11,20)
12	16	1	YES	(12,4), (12,19)
13	3	1	YES	(13,7), (13,16)
14	22	22	NO	-
15	10	22	NO	-
16	19	22	NO	-
17	9	1	YES	(17,3), (17,20)
18	9	1	YES	(18,3), (18,20)
19	2	1	YES	(19,5), (19,18)
20	17	22	NO	-
21	14	22	NO	-
22	22	22	NO	-

Table 2: Generating Points on Elliptic Curve where l=(p-1)/2

2.4 Encryption and Decryption on ECC

To perform encryption and decryption, it requires private key and public key since ECC is public key cryptography. Foremost the Sender and Receiver approve upon a communal Elliptic curve calculation and a base point G. Lease the Sender private key be nSand Receiver key benR. Sender and Receiver public keys are specified by

$$Ps = nSG \quad (10)$$

and

$$Pr = nRG \quad (11)$$

correspondingly. If Sender wishes to send a text message 'Pw' to Receiver, Sender usages Receiver's public key to encrypt the text information. The cipher message is specified by

$$Pc = (kG, Pw + xPr) \quad (12)$$

where 'x' is anarbitraryinteger. An arbitraryinteger 'x' makesdistinct cipher text every time even for identical text information. This provides a stiff time for somebody who is illicitly annoying to decrypt the text information. Now by decrypting the Receiver subtracts the coordinate of 'xG' multiplied withn R from Pw + xPr.

$$Pm = (Pw + xPr - nRxG) \quad (13)$$

Now multiplication is done by many additions of points by means of the point addition and doubling. nR is the secret key of Receiver as multiplier, only the Receiver can decrypt the text message which is sent by Sender.

Encoding Plaintext usingKoblitz's Method [2]:

1: Choose an elliptic curve Ep(m,n).

November-December 2019
ISSN: 0193-4120 Page No. 5128 - 5136

2: Lease E has number of points on elliptic curve.

3: Lease alphabets consist of the numbers 0,1,2 …8,9 and the alphabets A, B, C. . . X, Y, Z coded as 10, 11,. . . 35.

4: This translates our plain text into a sequence of digits from 0 to 35.

5: Here select a base parameter, for instance k = 30, $0 \leq k \leq 50$ (Both sender and receiver should decide upon this)

6: After chosen to embed plaintext m, for each number, take $x_i = w_i k + j$, $0 \leq j < k$ and attempt to answer for y.

7: In this way, we can find y before wesuccess x = wk + k - 1.

Decode Cipher text: Ponder each point (x,y) and set m will be the largest number of integer less than (x-1)/k and then the point (x,y) deciphers asw.

Instance: Parameters of the curve are: p(23),m(1),n(1).

1. Assume character ‘A’ has to be send.
2. ‘A’ iscoded as 10.
3. x=wk+1 i.e. 10*30+1=301, it cannot answer for a y such that $y2 = (x^3 + mx + n) \mod p$.
4. So we go for x=wk+2, x=302, no y present.
5. x=wk+3, then x=303 itanswers for y and the value of y is 0.
6. Here(303, 0) is the point to encrypted and decrypted as a text information.
7. To decode the number calculate (x-1)/k i.e. (303-1)/30=302/30 is 10.1.
8. Return 10 as original message.
9. The integer 10 is here decoded to alphabet ‘A’.

3. ECC Mapping Techniques

To map a text message to a point on the elliptic curve elliptic curve mapping schemes are used. In elliptic curve cryptography, the points on the elliptic curve will be encrypted and decrypted which are transformed from a plaintext by some techniques. Here some of mapping techniques are given below:

SCHEME 1: The mapping scheme [4] for plaintext messages of variable sizes and static using elliptic curve cryptography to offer multi-fold security. This technique using elliptic curve cryptography with an Initial Vector implements mapping of a plaintext into many points on elliptic curve. In this scheme first the plaintext is alienated into blocks, each block is EX-ORed with an Initial Vector. Then the resulting block is transformed into ASCII value of base 256(0-255) formats. To convert the message block into an affine point, ASCII value is used as a multiplier to the designated base point of the elliptic curve. The affine point is hereconverted into cipher text with ECC. Likewise, the succeeding ithblock isXORed with the $(i - 1)^{th}$ block and the similar process is repetitiveuntil the completetext information is mapped onto elliptic curve.

On the other lateral, the decryption process is functional in opposite method to get the matching original text block. Also, the following i^{th} block isXORed with the $(i - 1)^{th}$ block, and this procedure will be repetitive till the entire text is regained back. The message block size is fixed beforehand starting the encryption procedure in fixed span block mapping scheme, while in adjustable length block mapping scheme.Here each word of message will be a block and to equate the length of message blocks null characters are expanded.

SCHEME 2: This mapping scheme [5, 6] finds a base point G and plots apiece character in the original message to a point on the elliptic curve will be multiplied with the ASCII value of the equivalent character of original message with the base point G. For instance, we known that the character B’s ASCII value will be plotted to point 66*G on elliptic curve where G is the base point

November-December 2019
ISSN: 0193-4120 Page No. 5128 - 5136

of elliptic curve Ep(m, n). This technique is a primeval and quicker than other mapping techniques. It is quiet in usage since the time taken to convert the text message into points on elliptic curve is less than the other schemes involved in it.

SCHEME 3: The next mapping technique [7] has offered to instrument the cryptosystem based on elliptic curve for text message based use by converting the text into an affine point in a finite field on the elliptic curve. Here using ASCII value of each character in a plaintext is first converted into affine point and the ASCII value of each character as a multiplier to the chosen generated point onto the elliptic curve. Then to get cipher text the standard elliptic curve cryptography encryption is achieved by an affine point attained; which is then transformed back to original message by performing elliptic curve cryptography decryption on the receiver side.

SCHEME 4:Balamurugan.R, et al [8] have proposed the matrix based mapping scheme and joint it with ElGamal method in elliptic curve cryptography. At First, based on non-singular matrix each character in plaintext message is mapped to points on elliptic curve. After that to get cipher textElGamal encryption is achieved on the mapped points. On other hand, ElGamal decryption is applied to obtain back original message. Now the decoded matrix andconverse of non-singular matrix is multiplied. In order to improve security using Crypt-Steg model is used [9]. In this scheme, first the message to be transferred and encrypted based on matrix mappingscheme using elliptic curve cryptography and then it is entrenched in cover text to form Stego-object.

SCHEME 5: This mapping scheme [10] provides a probabilistic mapping technique to map original message on an elliptic curve. A plaintext character C using ASCII value is convertedinto $x_i = (C.K + i) \bmod P$; where K is aarbitrary value integer like $(C + 1)\ K<P$. If $z_i=(x_i^3 + ax_i + b) \bmod P$ has a quadratic remainder y_i then plot C to (x_i,y_i) else return failed in try to map C to an elliptic curve point. To decode each point (x_i,y_i) and set C will be the largest integer value less than (x-1)/k. Then the point (x_i,y_i) can be decoded asthe character C.

SCHEME 6: The next mapping technique [11] has applied aninnovative scheme for encryption of text message using elliptic curve cryptography. Here, first the ASCII values ofplaintext is transformedand then these values will beseparated in to groups using Partition (ASCII values, groupsize, groupsize, 1, {}) (14)

The size of group is well-defined by

$$\text{groupsize} = \text{Length}(\text{Integerdigits}(p, 65536)) - 1 \quad (15)$$

Each group got large integer values of base as 65536, combined up to be nourished as the initial point into elliptic curve cryptography encryption.

The below function will produce the large integer value which is made by coalescing collection of ASCII values.

Fromdigits(GroupofASCIIvalues, 65536)(16)

Integerdigits(biginteger, 65536)(17)

Transform it back to tilt of ASCII values using above operation. Integerdigits() in Mathematical offers biginteger is the list of integers and 655536 is the base. Fromdigits() and Integerdigits() functions are converse of each other.

SCHEME 7:Phattarin Kitbumrung et al have proposed two mapping schemes and have categorized them into static and dynamic mapping scheme [12]. In static mapping scheme, first each character of plaintext message has been mapped on elliptic curve. The points which are lies on elliptic curve are transmitted through an insecure network. In this scheme the main disadvantage is that the identical alphanumeric characters from distinct plaintext message are constantly transformed onto the same (x, y) coordinate points on the elliptic curve. So, an interloper can simply

November-December 2019
ISSN: 0193-4120 Page No. 5128 - 5136

understand data using some method such as trial and error. But in dynamic scheme each character of plaintext message is mapped dynamically onto the elliptic curve. Here, though the plaintext message has same alpha-numeric characters it will be mapped onto different (x, y) coordinate points on the elliptic curve. So an interloper gets very hard to deduction which points the original characters are.

SCHEME 8: The next mapping technique [13,14] is the matrix-based mapping technique and it uses generator point. Here the matrix is used to permute the location of the points. Sender selects an elliptic curve and a base point G. Then the sender maps an alphabet A will be G, B will be 2*G, C will be 3*G, D will be 4*G and so on. These values are stored in elliptic curve data file and declare it as public. Text information is lengthened with space ((0,0) on to elliptic curve to make the text size into multiple of three. The points are organized to form a matrix M of size 3 × r. Now the sender chooses a matrix A of non-singular such that determinant (A) = ±1 to get Q = AM means a number of points placed on the elliptic curve. Then elements of matrix Q will be encrypted on the elliptic curve, and the corresponding cipher points on the elliptic curve will be generated. Now the cipher points which are generated on the elliptic curve will be sent to the receiver. Then the receiver decrypts all the cipher points on the elliptic curve to get back the original matrixMusing $M = A^{-1}Q$.

Sl. No	Mapping Scheme	Basic Mechanism	Key Factor	Security Level	Merits/Demerits	Application
1	Scheme 1	Mapping each character of a plaintext message into many points on elliptic curve and with an Initial Vector using elliptic curve cryptography.	Each block of plaintext is XORed with Initial Vector then transformed into ASCII value. Then use point multiplication to attain an affine point on elliptic curve.	Due to vigilant selection of curve, eradicates exponential time attack.	Message block maps to distinct points on ECC every time and hence hides the letter frequencies of the plaintext.	Text based
2	Scheme 2	Each character of a plaintextis converted into a base point on the elliptic curve.	Each character of plaintext multiplying by the ASCII value to obtain base point G on EC.	This is less efficient in terms of security.	This technique is a primeval and quicker than other mapping technique.	Text based
3	Scheme 3	Encoding each character of a message in a plaintext is converted into affine point on ECC.	To obtain affine points on ECC, ASCII values are used as a multiplier.	In wireless networks, it Summaries the Brute Force attack on ECC.	This scheme removes nonlinearity and masking its uniqueness since ASCII value of each character of a plaintext is	Text based

					transformed into a set of coordinate points on elliptic curve cryptography.	
4	Scheme 4	Using non-singular matrix each character in plaintext message is plottedinto points on elliptic curve.	Generation point selected from the elliptic curve points generated. The matrix encoding is achieved by using scalar multiplication of matrix non-singularwith message.	Once the presence of concealed message in the steganography is assumed, aninvader will not halt to decrypt weakly encrypted text.	There is no completely faultless encryption technique that suits all states.	Text based
5	Scheme 5	This method maps each character of plaintext message into a point if $x_i^3+ax_i+b$ is the quadratic residue of mod p.	A plaintext ASCII character is transformed to $x_i = (C.K + i) \bmod p$; If $z_i=(x_i^3 + ax_i + b) \bmod p$ has y_i then map C to (x_i,y_i) on ECC.	This is susceptible to a collision attack.	The drawback of this technique is that it is probabilistic in nature. There is collision at some point while plotting, soa collision attack can effortlessly break this mapping scheme.	Text based
6	Scheme 6	ASCII values of plaintextis grouped and then combined to plot points on the elliptic curve.	Apiece group is transformed into large number value and combined up to use as initial point for ECC operation.	Mostly eradicates known plaintext attacks and Brute force attacks.	Eliminates the essential to share a common lookup table and evades the costly operation of mapping on elliptic curve.	Text based
7	Scheme 7	According to ASCII value of each character of plaintext message and sequence ordering is plotted onto distinct points on elliptic curve in a finite filed dynamically.	This scheme reliant on sequence number of a plaintext message' character.	Ensures safeguard against frequency cryptanalysis.	Each character is mapped intodissimilar points on elliptic curve and it depends on the ASCII value of each character and it's appearing sequence.	Mobile communicat ion devices

8	Scheme 8	Using non-singular matrix the points on elliptic curve are converted fromeach character of a plaintext.	In matrix mapping method non-singular matrix used and it has only integer entries.	Eliminates Brute force attack.	Many characters of plaintext are converted into distinct points and transmitted at the same time through matrix mapping.	Text and image based

Table 3: Comparison between Various Mapping Schemes

4. Conclusion

Internet of Things offers a platform where physical world things meet the Internet to help users through numerous applications. Though, these linked devices carry a new dimension of securitydares due to the susceptibilitiesrelated with them. Elliptic curve cryptography is set up to be a perfect model for implementation on Internet of Things constrained devices where storage and speed are limited in size and these devices runs in low power. The elementarydifferences between few mapping techniques in elliptic curve have been conferred in this paper. The mapping techniques supports improve the security level specified by existing elliptic curve cryptography. Even though numerousresearches is being done in the area of various mapping techniques in elliptic curve cryptography, still few more research desires to be in deepnessconcerning the elliptic curve based cryptosystem.

References

[1] Agrawal Komaland Anju Gera, "Elliptic Curve Cryptography with hill Cipher Generation for Secure Text Cryptosystem", International Journal of Computer Applications, Vol. 106, Issue. 1, pp. 18-24.

[2] Koblitz and Neal (1987) "Elliptic Curve Cryptosystems", Mathematics of Computation, Vol. 48, Issue. 177

[3] Mahto, Dindayal, and Dilip Kumar Yadav (2018), "Performance Analysis of RSA and Elliptic Curve Cryptography", International Journal of Network Security, Vol. 20, Issue. 4, pp. 625-635

[4] Muthukuru, Jayabhaskar and Bachala Sathyanarayana (2012), "Fixed and Variable Size Text Based Message Mapping Technique using ECC", Global Journal of Computer Science and Technology, Vol. 12, Issue. 3, pp. 13-18

[5] Hankerson D, Menezes A and Vanstone S (2004), Guide to Elliptic Curve Cryptography, Springer: New York

[6] Kanaklataverma and Himani Agrawal (2013), " Elliptic Curve Cryptography using Koblitz Encoding Method", International Journal of Advanced Scientific and Technical Research, Vol. 3, Issue. 3, pp. 418-422

[7] Vigila, S.Maria Celestin and K.Muneeswaran (2009), "Implementation of Text Based Cryptosystem using Elliptic Curve Cryptography", IEEE International Conference on Advanced Computing, pp. 82-85.

[8] R. Balamurugan, V. Kamalakannan, Ganth D Rahul, and S.Tamilselvan (2014), "Enhancing Security in Text Messages using Matrix Based Mapping and ElGamal Method in Elliptic Curve Cryptography", IEEE International Conference on Contemporary Computing and Informatics, pp. 103-106.

[9] V. Kainalakaiinan and S. Tamilselvaii (2015), "An Efficient Crystography Protocol using Matrix Mapping Technique", IEEE International Conference on Communications and Signal Processing, pp. 0134-0138

[10] W Trappe and LC Washington (2006), "Introduction to Cryptography with Coding Theory" Prentice Hall: New Jersey.

[11] Singh, Laiphrakpam Dolendro and Khumanthem Manglem Singh (2015), "Implementation of Text Encryption using Elliptic Curve

Cryptography", Procedia Computer Science, Vol. 54, pp. 73-82.

[12] Kitbumrung, Phattarin, and Benchaphon Limthanmaphon (2015), "ECC Dynamic Point Encoding on Mobile Device", International Conference on Computing Technology and Information Management, pp. 37- 42.

[13] F. Amounas and E. H. ElKinani (2012), "Fast Mapping Method Based on Matrix Approach for Elliptic Curve Cryptography", International Journal of Information and Network Security, Vol. 1, Issue. 2, pp. 54-59

[14] Reyad, Omar, and Zbigniew Kotulski (2015), "Image Encryption using Koblitz's Encoding and New Mapping Method Based on Elliptic Curve Random Number Generator", International Conference on Multimedia Communications, Services and Security, pp. 34-45