Information Sciences Letters

Volume 7
Issue 1 *Jan. 2018*

Article 2

2018

Text Message Encoding Based on Elliptic Curve Cryptography and a Mapping Methodology

Omar Reyad
Computer Science Branch, Faculty of Science, Sohag University, Egypt, ormak4@yahoo.com

Information Sciences Letters
An International Journal

http://dx.doi.org/10.12785/isl/070102

Text Message Encoding Based on Elliptic Curve Cryptography and a Mapping Methodology

Omar Reyad

Computer Science Branch, Faculty of Science, Sohag University, Egypt

Received: 22 Nov. 2017, Revised: 22 Dec. 2017, Accepted: 28 Dec. 2017
Published online: 1 Jan. 2018

Abstract: Elliptic Curve Cryptography (ECC) is a public-key cryptosystem which can be used for message encryption, key agreement protocols and digital signature applications. ECC offers high level of security with smaller key sizes makes it ideal for applications which run on small devices that have power and memory constraints such as smart cards and cell phones. Encoding (converting a plaintext message to a point) and Decoding (converting a point to a plaintext message) are important functions in encryption and decryption schemes using ECC before transmission over public networks and unsecured channels. In this paper, we proposed a text message encoding scheme which is based on computational operations on points that lie on a predefined elliptic curve (EC). For any ECC-based encryption scheme, the mapping methodology of a plaintext message onto a coordinate on an affine curve is a mandatory prerequisite. ASCII character codes are considered for the mapping method to convert a plaintext message into coordinates of the predefined EC-points. Discussing the mapping methodology, creating the mapping table and the converting process are given in detail along with their implementations.

Keywords: Elliptic Curve Cryptography, Encoding, Decoding, Finite Prime Field.

1 Introduction

Cryptography is a practical means for protecting private and sensitive information. Elliptic curve cryptography (ECC) is a public-key cryptosystem first introduced in 1985 by Miller [1] and Koblitz [2]. Since then, many researchers tried to employ ECC on different data types and improve it's efficiency by proposing various encryption techniques [3]. The most attractive advantage that motivated cryptographers to use ECC was the well suitability of it in the constrained environments where processing power, storage, bandwidth or power consumption is of primary interest [4]. These characteristics of ECC motivated us to study the potential of using it for encoding the American Standard Code for Information Interchange (ASCII) character codes for any ECC-based encryption scheme .

The fundamental issue of protecting the confidentiality, integrity as well as authenticity of plaintext messages through various communication entities has become a major concern especially with the increasing use of digital techniques for transmitting and storing these messages. In most cryptographic systems, we must have a method for mapping our plaintext message into a numerical value upon which we can perform mathematical operations. In order to use elliptic curves, we need a method for mapping a plaintext message onto a point on an elliptic curve [5]. Elliptic curve cryptosystems then use elliptic curve operations (Add, Double, Multiply) on that point to yield a new point that will serve as the ciphertext.

In this paper, we proposed a secure plaintext message encoding scheme using EC-points operations. The encoding process of the ASCII character code is done and implemented by using the proposed mapping methodology. The decoding process is accomplished by using the mapping methodology to obtain the plaintext messages. The simulation analysis demonstrated that the proposed plaintext message encoding scheme has large key space and can satisfy the performance requirements for the confidentiality of digital messages.

The rest of the paper is organized as follows: In Section 2, we presented preliminaries that contain discussion about some related works. Also the description of EC over finite prime field constructions are discussed. The proposed scheme for text message encoding and decoding are discussed in Section 3. In Section 4, we

* Corresponding author e-mail: ormak4@yahoo.com

discussed the proposed scheme related results while conclusions are given in Section 5.

2 Preliminaries

2.1 Related Works

Several attempts have exploited the strength use of ECC in various tasks of public-key cryptography such as encryption and authentication. In [2], a probabilistic method for encoding a message to a point on an elliptic curve has given by Koblitz, where the message is first converted to a series of numbers. Each number 'n' is then multiplied by an auxiliary base parameter 'k' and take it as the x-coordinate of the curve point and try to solve for y. An implementation of elliptic curve cryptography using Koblitz method is given in [6]. A method for encrypting messages using elliptic curves over finite field is proposed in [7], where each character in the message is encoded to a point on the curve by using a code table which is agreed upon by communicating parties and each message point is encrypted to a pair of cipher points. In [8], the authors have suggested the use of a nonsingular matrix to map same characters in the message to different points on the curve. The use of a two dimensional alphabetic table to convert plaintext characters to two dimensional coordinate representation have suggested in [9]. These points are then added with elliptic curve points for encryption. In [10], the message is encrypted using Hill cipher algorithm and ASCII value of cipher characters are used to find points on the elliptic curve. An implementation of message encryption using ECC is discussed in [11] where an affine point is chosen first and a character is transformed to a point on the curve by multiplying its ASCII value with the chosen affine point. This point is then encrypted by ElGamal elliptic curve encryption method. In [12] authors have proposed an extension of Koblitz method by using mirrored elliptic curves. The application method of transposition techniques on the plaintext before using Koblitz method to encode message to the curve was suggested in [13]. In [14], authors have suggested the use of an initial vector and XOR operation is done on plaintext character and initial vector before the characters are mapped to the curve. Thus, encryption of mapped points will result in a polyalphabetic cipher. A secure method for embedding plaintext on an elliptic curve using Time Dependent Multiple Random Cipher (TDMRC) code and Koblitz method was proposed in [15]. In [16], a fast mapping technique using a non-singular matrix was proposed. First mapping the message to points on elliptic curve and later uses ElGamal encryption method to encode the points using a non-singular matrix. A brief background of encryption/decryption and key exchange using ECC was described in [17]. The authors have used mapping table to map the ASCII value to Elliptic curve coordinate. In [18], a new technique to perform text cryptography using ECC has been implemented where the classic technique of mapping the characters to affine points in the elliptic curve has been removed. Two different mapping methods of the alphanumeric characters on to the x- and y-coordinate of the Elliptic curve defined over a finite field $\mathbb{Z}_p$ is proposed in [19].

Table 1: Mapping method for ASCII character codes

ASCII Code	Symbol	$[k]G$	Mapped Point
0	NULL	$[1]G$	$(283,315)$
1	SOH	$[2]G$	$(483,112)$
2	STX	$[3]G$	$(368,312)$
3	ETX	$[4]G$	$(454,484)$
4	EOT	$[5]G$	$(410,439)$
5	ENQ	$[6]G$	$(154,108)$
6	ACK	$[7]G$	$(188,48)$
7	BEL	$[8]G$	$(453,425)$
8	BS	$[9]G$	$(347,117)$
9	HT	$[10]G$	$(166,219)$
⋮	⋮	⋮	⋮
50	2	$[51]G$	$(238,120)$
51	3	$[52]G$	$(392,51)$
52	4	$[53]G$	$(477,321)$
53	5	$[54]G$	$(93,365)$
54	6	$[55]G$	$(435,228)$
55	7	$[56]G$	$(21,455)$
56	8	$[57]G$	$(265,451)$
57	9	$[58]G$	$(335,22)$
58	:	$[59]G$	$(286,350)$
59	;	$[60]G$	$(126,343)$
⋮	⋮	⋮	⋮
100	d	$[101]G$	$(363,109)$
101	e	$[102]G$	$(474,326)$
102	f	$[103]G$	$(407,302)$
103	g	$[104]G$	$(248,448)$
104	h	$[105]G$	$(474,326)$
105	i	$[106]G$	$(407,302)$
106	j	$[107]G$	$(248,448)$
107	k	$[108]G$	$(474,326)$
108	l	$[109]G$	$(407,302)$
109	m	$[110]G$	$(248,448)$
⋮	⋮	⋮	⋮
125	}	$[126]G$	$(474,326)$
126	∼	$[127]G$	$(407,302)$
127	DEL	$[128]G$	$(248,448)$

2.2 Elliptic Curve over Finite Prime Field

Let E be an elliptic curve over $\mathbb{F}_p$, $p>3$, given by an affine Weierstrass equation of the form [20]:

$$E: y^2 = x^3 + ax + b, \tag{1}$$

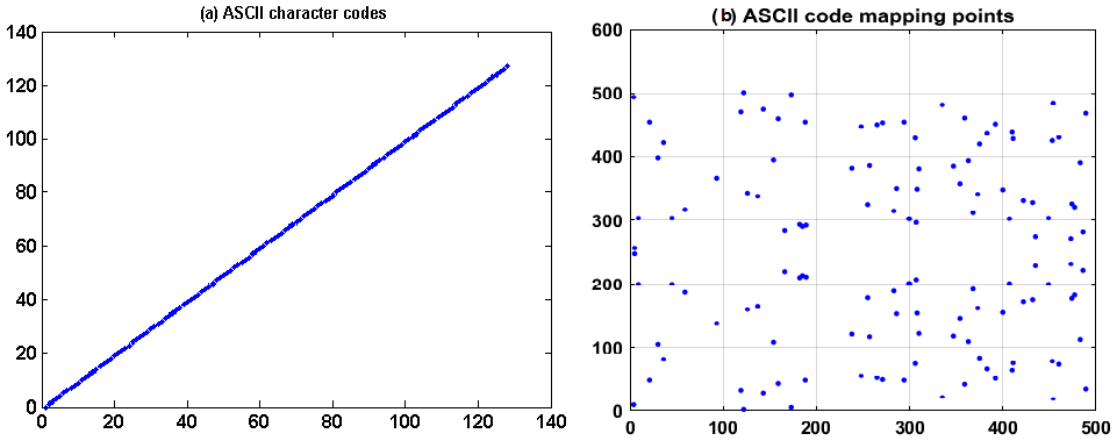

Fig. 1: Resulted encoded points

where a and b are coefficients belonging to $\mathbb{F}_p$ such that $4a^3+27b^2 \neq 0$ (this last condition ensures that E has no singular point over $\mathbb{F}_p$). The set $E(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points is simply defined as

$$E(\mathbb{F}_p) = \{O\} \cup \{P = (x,y); x,y \in \mathbb{F}_p; y^2 = x^3 + ax + b\}, \tag{2}$$

where O represents the point at infinity. Such an elliptic curve E admits an addition law. Equipped with this addition law, $E(\mathbb{F}_p)$ becomes a finite abelian group, where O is the neutral element.

To encrypt a message, Alice and Bob pick an elliptic curve E and select an affine point $G \in E(\mathbb{F}_p)$. Plaintext m is encoded into a point P_m. Alice choose a random prime integer x and Bob choose a random prime integer y. Alice and Bob's private keys are x and y respectively. To generate the public key, Alice computes $P_A = [x]G$ and Bob computes $P_B = [y]G$. To encrypt a message point P_m for Bob, Alice chooses another random integer k and computes the encrypted message P_C using Bob's public key P_B. Then, P_C is a pair of points given by the following equation:

$$P_C = [([k]G), (P_m + [k]P_B)]. \tag{3}$$

Alice sends the encrypted message P_C to Bob. Bob receives the ciphered message and multiplying his private key, y, with $[k]G$ and subtract it from the second point in the encrypted message to compute P_m. The result is the plaintext message m indicated by the following equation:

$$P_m = [(P_m + [k]P_B) - ([yk]G)]. \tag{4}$$

Points addition and points doubling are the basic EC operations [21]. Assume that $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are two points of E, then their sum which is $P_3 = (x_3, y_3)$ can be obtained as follows:

$$P_3 = P_1 + P_2 = \begin{cases} O & \text{if } P_1 = -P_2 \\ (x_3, y_3) & \text{if } P_1 \neq -P_2 \end{cases} \tag{5}$$

where (in the latter case)

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = (x_1 - x_3)\lambda - y_1 \end{cases} \tag{6}$$

with

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{if } x_1 = x_2 \ \ and \ \ y_1 \neq 0 \end{cases} \tag{7}$$

It turns out that point P_3 belongs to the curve E, and even is an element of $E(\mathbb{F}_p)$ if both P_1 and P_2 are. Recall that the computations of the algebraic quantities above are done (mod p) at each step in practice.

Using this addition law, one can compute, like in any abelian group, any multiple $[k]G$ for any $G \in E(\mathbb{F}_p)$ and any integer k, as follows:

$$[k]G = \begin{cases} \underbrace{G + \ldots + G}_{\text{k times}} & \text{if } k \geq 1 \\ O & \text{if } k = 0 \\ \underbrace{(-G) + \ldots + (-G)}_{\text{k times}} & \text{if } k \leq -1 \end{cases} \tag{8}$$

Therefore, multiplication on EC requires a scalar multiplication operation $[k]G$, defined for a point $G = (x,y)$ on EC and a positive integer k as k times addition of G to itself. This scalar multiplication can be done by a series of addition and doubling operations of G. The strength of an ECC-based cryptosystem depends on

the difficulty of finding the number k of times G is added to itself to get $[k]G$ (P_A). This reverse operation is known as the Elliptic Curve Discrete Logarithm Problem (ECDLP) and is considered the core hardness of ECC [22].

3 The Proposed Text Message Encoding Scheme

The problem of encoding plaintext messages as points on an EC is not as simple as it was in the conventional case. In particular, there is no known polynomial time, deterministic algorithm for writing down points on an arbitrary elliptic curve E (mod p). However, there are fast probabilistic methods for finding points, and these can be used for encoding messages. The proposed encoding scheme uses a mapping table to encode plaintext message characters to an elliptic curve points. The aim of the method is to provide an additional level of security in the elliptic curve encryption schemes by making use of the hardness nature of the ECDLP. The characters in the plaintext message m are first represented as numbers k and these numbers are then encoded to different points on the curve using the mapping table. These points can be converted to cipher points by using the EC point operations. The letter frequencies in the plaintext are not preserved in the ciphertext and thus the cryptanalysis based on letter frequency can be defeated. This method is more suitable for encrypting short messages such as Short Message Service (SMS) and Multimedia Messaging Service (MMS) which are used in mobile phones for non-voice communications.

3.1 The Mapping Methodology

To encode a plaintext message m that consists of a number of characters and each character is represented by ASCII character code, which used a 7-bit character code of between 0 and 127 according to the standard ASCII table, we need to encode $k = 128$ numbers. In this case, each character should be considered as a text message and mapped to a point on a predefined EC. The mapping method proposed in this section is based on a map table. To create this table, an elliptic curve E with at least 128 points, which is all possible points on the finite field, is generated first. Then, we find point G of order ℓ equal at least 129 and as close to 129 as possible on E. The order of point G is $\ell = k+1$, that is we have different points

$$\{G, [2]G, [3]G, ..., [k]G\} \tag{9}$$

with $[\ell]G = O$ is infinity point and k is integer. The row indexes start from 0 and end with 127 where each row stands for a character code value as listed in Table 1.

3.2 ASCII Code Implementation

In our experiment, in order to define the implementation process clearly, we used the following EC equation:

$$E : y^2 = x^3 + 4x + 1 \tag{10}$$

over $\mathbb{F}_{503}$, where the order of E is $N = \#E(\mathbb{F}_p) = 516$. We also select generator point $G = (283, 315)$ of order $\ell = 129$ for our mapping method.

Starting from the first character in the plaintext message, the corresponding point with the intensity value in the table is mapped to this character and continues to the last character. So, we encode plaintext message characters as points of E assigning all character codes to all points as the following:

$$0 \Longrightarrow G, 1 \Longrightarrow [2]G, 2 \Longrightarrow [3]G, \cdots, 127 \Longrightarrow [128]G. \tag{11}$$

In Table 1 are presented results of the mapping method for ASCII character codes. The first column represent ASCII character values as $\{m = 0, ..., 127\}$ and the second column shows ASCII corresponding symbols. The third column shows how ASCII values are mapped according to $[k]G$ with $\{k = 1, ..., 128\}$. In the fourth column, the EC mapped points are resulted for all ASCII character values with successful iteration of k.

4 Results and Discussion

It is important to ensure that EC encoded points obtained from the proposed text message encoding method are distributed uniformly on the predefined elliptic curves over a finite field of p elements.

The encoded EC-points resulted from mapping the ASCII values are shown in Fig. 1(b). It is clear that using EC-points operations in the encoding text message scheme improves the distribution of the original ASCII values which are shown in Fig. 1(a). So, the resulting EC-points encoded sequences have good uniformity of distribution properties over E.

5 Conclusions and Future Work

In this work, we have presented a new scheme for plaintext message encoding based on EC-points operations applied after encoding process of ASCII character codes was done by a mapping method. The mapping method for encoding ASCII character codes to EC-points is used. The decoding process is done vice-versa. The method implementation was done and the encoded EC-points was obtained. The obtained EC-points from each step in the proposed message encoding scheme are plotted demonstrated that the encoded EC-points are uniformly distributed on the used elliptic curves.

The work presented here can be subject to future studies. One possible extension is the application of one of the specified modes of operation such as the Cipher Block Chaining (CBC) mode to the message encoding of two or more points at the same time in such a way that provides confidentiality and authenticity.

References

[1] V. Miller, Uses of elliptic curves in cryptography, In: Williams HC (ed) Advances in Cryptology-CRYPTO'85, LNCS 218, 417–426 (1986).

[2] N. Koblitz, Elliptic curve cryptosystems, J Mathematics of Computation 48, 203–209 (1987).

[3] O. Reyad, Z. Kotulski and W.M. AbdElhafiez, Image Encryption using Chaos-Driven Elliptic Curve Pseudo-Random Number Generators, J. Appl. Math. Inf. Sci. 10, 1283-1292 (2016).

[4] N. Gura, A. Patel, A. Wander, H. Eberle and S.C. Shantz, Comparing elliptic curve cryptography and RSA on 8-bit CPUs, In: Joye M, Quisquater JJ (eds) CHES 2004, LNCS 3156. Springer, Heidelberg, 119-132 (2004).

[5] W. Trappe and L.C. Washington, Introduction to Cryptography with Coding Theory, Pearson Education Int (2006).

[6] O. Reyad and Z. Kotulski, Image Encryption Using Koblitz's Encoding and New Mapping Method Based on Elliptic Curve Random Number Generator, In: Dzich A et al (eds) MCSS 2015, CCIS 566. Springer, Heidelberg, 34–45 (2015).

[7] D.S. Kumar, C.H. Suneetha and A. Chadrasekhar, Encryption of data using Elliptic Curve over finite fields, Int J of Distributed and Parallel Systems 3, 301–308 (2012).

[8] F. Amounas and E.H. EI Kinani, Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography, Int J of Information and Network Security 1, 54–59 (2012).

[9] T.N. Shankar and G. Sahoo, Cryptography with Elliptic Curves, Int J of Computer Science and Applications 2, 38–42 (2009).

[10] K. Agrawal and A. Gera, Elliptic Curve Cryptography with Hill Cipher Generation for secure Text Cryptosystem. Int J of Computer Applications 106, 18–24 (2014).

[11] M.C. Vigila and K. Muneeswaran, Implementation of text based cryptosystem using elliptic curve cryptography, ICAC IEEE 10, 82–85 (2009).

[12] M.S. Srinath, V. Chandrasekaran, Elliptic Curve Cryptography using Mirrored Elliptic Curves over Prime Fields, Int Conference on Information and Knowledge Engineering IKE 10, 271–277 (2010).

[13] S. Pote, Enhancing the Security of Koblitz's Method Using Transposition Techniques for Elliptic Curve Cryptography, Int J of Research in Eng and Adv Tech 2, 158–172 (2015).

[14] J. Muthukuru and B. Sathyanarayan, Fixed and Variable Size Text Based Mapping Techniques using ECC, Global Journal of Computer Science and Technology 12, 13–18 (2012).

[15] M.C. THOMAS and V. PAUL, Secure method for embedding plaintext on an elliptic curve using TDMRC code and Koblitz method, J of Theoretical and Appl Inf Tech 84, 298–304 (2016).

[16] R. Balamurugan, V. Kamalakannan, D.R. Ganth and S. Tamilselvan, Enhancing Security in Text Messages Using Matrix based Mapping and ElGamal Method in Elliptic Curve Cryptography, Int Conference on Contemporary Computing and Informatics IEEE 31, 103–106 (2014).

[17] M. Kolhekar and A. Jadhav, Implementation of Elliptic Curve Cryptography on Text and Image, Int J of Enterprise Computing and Business Systems 1, 1–13 (2011).

[18] L.D. Singh and K.M. Singh, Implementation of Text Encryption using Elliptic Curve Cryptography, Procedia Computer Science 54, 73–82 (2015).

[19] R.O. Srinivasa and P.S. Setty, Efficient Mapping Methods for Elliptic Curve Cryptography, Int J of Engineering Science and Technology 2, 3651–3656 (2010).

[20] D. Hankerson, S. Vanstone and A. Menezes, Guide to Elliptic Curve Cryptography, Springer-Verlag, New York (2004).

[21] J.H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, New York (2009).

[22] O. Reyad and Z. Kotulski, Pseudo-Random Sequence Generation from Elliptic Curves over a Finite Field of Characteristic 2, In: Federated Conference on Computer Science and Inf. Sys., FedCSIS, ACSIS 8, IEEE, 991–998 (2016).

Omar Reyad is currently a Lecturer of Computer Science at Sohag University, Egypt. He received his PhD in Informatics from the Faculty of Electronics and Information Technology, Warsaw University of Technology, Poland. He received his MSc in Computer Science from Sohag University, Egypt. His main research interests are in Elliptic curve cryptography, Cryptographic protocols, Biometric security and Chaos-based cryptography.