Symmetric ECC with Variable Key using Chaotic Map

Haider M. Al-Mashhadi [1] and Mohammed H. Alabiech [2]

[1] Information Systems Dept, College of Information Technology, University of Basrah, Basrah, Iraq.

[2] Computer Science Department, College of Science, University of Basrah Basrah, Iraq.

Abstract

Elliptic Curve Cryptography (ECC) lately obtained a lot of care in cryptography science because it is more secure than the other cryptography methods and it is consider as one of the most significant cryptography technique. The ECC offers same security with smaller key comparing with the RSA (approximately 160 bits vs. 1024 bits), hence, this will decreases processor overhead, lowering power consumption, increase processing speed, enhance the storage efficiency, requires smaller certificates and it is good in bandwidth saving. The ECC uses high level mathematical operations. The ECC is an algebraic structure in finite fields and it is differ than other encryption algorithm because of the cipher text is a points in Cartesian coordinates. This paper proposed a new effective implementation method for symmetric encryption over ECC by use of secret shared key between two parties and this key change for every symbol in message. This technique provides authentication, confidentiality and non-repudiation.

Keywords:- Elliptic Curve Cryptography (ECC), Chaotic logistic map, symmetric encryption.

1. Introduction

The fundamental benefit in use of ECC technique is by providing same protection level with a smaller key length compared to RSA, thus will reduces the processing overhead and the processing time [1,2]. The ECC technique basically is more complicated to illustrate than either Diffie-Hellman or RSA. The ECC mathematics are substantially more concentrated than that for RSA and Discrete Logarithm (DL)[1].

The ECC technique is perfect for some environments such as email, smart cards and cellular phones. Further, because of the evident strength of the fundamental Elliptic Curve Discrete Logarithm Problem (ECDLP), ECC technique is suitable for applications which require long-term security.

Realizing the ECC technique requires good mathematical background compared to Elliptic Curves (EC). Furthermore, EC is not ellipses [1, 3], however, it is so identified to ellipses because the EC are derived from cubic equations [1].

The general equation of EC over the value in the real numbers is defined by:

$$y^2 = x^3 + ax + b, \qquad (1)$$

where a and b are real numbers both satisfies the following condition

$$4a^3 + 27b^2 \neq 0. \qquad (2)$$

x and y are any assumed real numbers[1,3,4].

When assigning values for a and b, the graph will contains negative and positive values of y related to each single value of x [1]. From above a point at infinity and all points of (x, y) plane are satisfying equation located on the EC [5]. There are two types of EC utilized in cryptographic applications: Either a prime curve over Z_p applying an equation of the third degree in which all the coefficients and the variables taking a value between (0 and p-1). The results perform modulo p and the equation below is satisfying condition

$$y^2 \bmod p = (x^3 + ax + b) \bmod p, \qquad (3)$$
$$\text{where } (4a^3 + 27b^2) \bmod p \neq 0 \bmod p. \qquad (4)$$

Or binary curve over GF(2^m) while all the coefficients and the variables are taking a value in the GF(2^m). The results perform over GF(2^m). The first one is used in the software applications and the second is used for hardware applications [1]. This paper will use prime curve over Z_p.

2. Related Works

Several researchers have been attempted to exploit the characteristics of EC to utilize them in the security techniques implementation. Koblitz and Miller were the first in using ECC technique [6]. Ravi Kodali and N. Sarma use ECC symmetric encryption with the koblitz's encoding to encode or mapping the data into points locating on EC and it is one of the main necessities of the ECC [7]. M. Aydos et.al has presented ECC execution over GF(p) on a (32 bit) RAM, microprocessor (80) MHz along with the consequences [8]. In his book, W. Stallings [1] has simplified the idea of ECC. Sangook Moon has proposed a novel and efficient technique of a scalar point multiplication and that way is different from the existing add and double by using redundant recoding, which result from radix 4 Booths algorithm [9]. Jaewon Lee presented three algorithms, to execute scalar multiplication on EC defined over higher characteristic finite fields like Optimal Extension Field [10]. L.Yong. indicated that Aydos et al.'s protocol is insecure from man in the middle attack by any attacker [11]. N.A. Saqib et.al has demonstrated that ECC security is relay on the hardness of (ECDLP) [12]. An effective technique to generate EC that relies on the composite method algorithm. It may generate several EC, which are appropriate for designing the cryptosystem this study has been presented by Bin Yu et. al. [13]. J. Nafeesa Begum and et.al in their study has improved defense messaging system of a multilevel access control applying ECC. Defense messaging system forwards a message to the parties or recipients based on the message criteria for quick action [14]. Guicheng shen et.al are presented majorly applies tools of object oriented technology and separates ECC into various layers; every layer work as a class to support OOP [15].

3. EC Example

To illustrate EC, all points that realize the equation of EC must be defined, as an example, let us take the following prime number $p = 17$, $a = 1$, $b = 1$, the equation of EC is defined as

$$y^2 \bmod 17 = (x^3 + x + 1) \bmod 17.$$

Table 1: points of the EC example.

(0,1)	(6,6)	(10,5)	(13,16)	(16,13)
(0,16)	(6,11)	(10,12)	(15,5)	
(4,1)	(9,5)	(11,0)	(15,12)	
(4,16)	(9,12)	(13,1)	(16,4)	

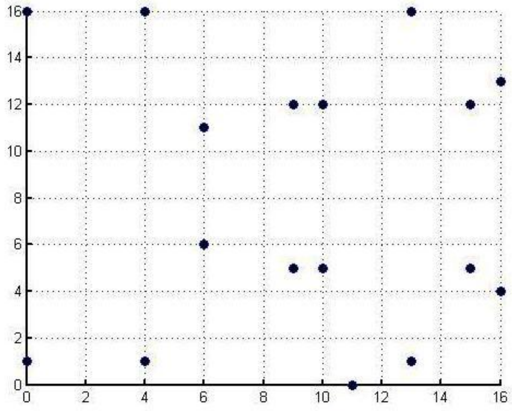

Fig. 1 Elliptic curve drawing.

Figure (1), plots the points of EC for table 1, mention the points, with single point exclusion are symmetrical about y=8.5.

4. Group Operation on EC

Let us announce the operation of group with the addition symbol (+). Addition operation for 2 points and their ordinates

First point: P=(x1, y1)
Second point: Q=(x2, y2)
Third point: R=P + Q
(x3, y3)=(x1, y1) + (x2, y2)

Now, two adding operations can be recognized:

4.1 Point Addition (P+Q)

In this case of addition $R = P + Q$ was calculated when $P \neq Q$. A line from the first point P to the second point Q will be draw to get the third point R by crossing between the line and EC plane. Mirror R crossing point on the x-axis to obtain mirrored R, Figure (2) demonstrates the point addition [2].

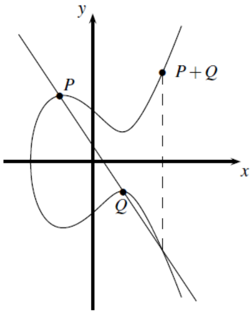

Fig. 2 Point addition [2].

4.2 Point Doubling (P+P)

In the case of doubling operation; R=P + Q have been calculated when P=Q. Therefore, $R = P + P = 2P$, in this case a tangent line will draw from first point P to get a second point R of crossing between line and EC. Mirror R crossing point on the x-axis to obtain mirrored point R, Figure (3) demonstrates the point doubling [2].

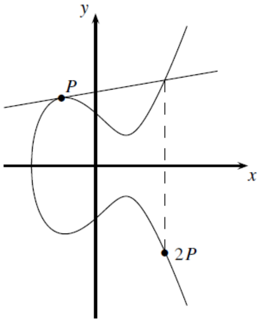

Fig. 3 Point doubling [2].

From the above; R point (addition and doubling point) can be computed from the equations as below [1,3,4].

$$x3 = (\lambda^2 - x1 - x2) \bmod p, \qquad (5)$$

$$y3 = (\lambda(x1 - x3) - y1) \bmod p, \qquad (6)$$

https://doi.org/10.20943/01201706.2428

where

$$\lambda = \begin{cases} \dfrac{y2-y1}{x2-x1} \bmod p\,;\ \text{if } P\ \neq\ Q(\text{point addtion}). \\ \\ \dfrac{3x1^2+a}{2y1} \bmod p\,;\ \text{if } P =\ Q\ (\text{point doubling}). \end{cases} \qquad (7)$$

5. Discrete Logarithm Problem (DLP)

The Fundamental guarantee of the security for ECC in the first place depends on the hardness degree of the ECDLP. Now both *Q* and *P* points are locate on EC plane where *Q*=*kP*, *k* is any number. When *P* and *Q* given, it's computationally impracticable to find the value for *k*, especially when *k* is large enough [7, 16, 17]. In the ECC technique, the sender and receiver are select a private key and the matching public key is calculated from the private key of the user by applying scalar multiplication [7].

6. Diffie-Hellman Key Exchange

Both sender and receiver (Alice and Bob) agree upon "Domain Parameters" {*a*,*b*,*p*,*G*,*n*}. *G* is called base point; *n* is the number of point of EC plus point at infinity.

Alice generates a random number *nA* < n as a private key and then a computes public key

$$PA = nA \times \mathrm{G} \qquad (8)$$

Bob doing the same:

$$PB = nB \times \mathrm{G} \qquad (9)$$

Alice sends his public key to Bob and Bob does the same. Alice computes the secret key from $nA \times P_B$ and Bop computes the secret key from $nB \times\ P_A$

The shared key between the two sides is

$$nA{\times}P_B = nA{\times}nB\ {\times}\mathrm{G}{=}\ nB{\times}nA{\times}\mathrm{G}{=}\ nB{\times}P_A \qquad (10)$$

It is worth to mention that shared key is a point [1, 2].

7. Proposed Algorithm

The proposed Algorithm is using same key at the two sides but for one time for every symbol. The proposed is applied to reduce predictability of next numbers and add some complexity and nonlinearity. One of the most well-known tools for generate unsystematic numbers is *the Chaotic method*.

A little contrast in beginning parameters will bring about a totally extraordinary conduct of the proposed method. The scheme is use one key for the current symbol at encryption and decryption process.

The key for every symbol is generated depends on the values of X according the Equation below.

The chaotic map function uses in the current work to add some nonlinear features to the encryption keys. The output of the chaotic map is quite random and has a complexity. One of the popular chaotic map functions is the logistic map that generates a sequence of real numbers by using the following equation[18, 19]:

$$X_{j+1} = rX_j(1\text{-}X_j), \qquad (11)$$

where X_0 is the initial seed and take a value 0<X<1 and 0<r<4 is the control parameter with a positive number. Then, the X value is reversed to be between [1,n-1] by using the equation below:

$$k_i = (n * X_i{}^{2} \bmod n)\ ), \qquad (12)$$

Now, multiply the value of k_i with the shared key which yields by Diffi-Hellman key exchange. The algorithmic structure for prepare of the proposed method keys is clarified in Algorithm-1.

Algorithm-1 The proposed method keys generation.

```
Input: Shared key ∈ EC, kcount is number of keys, n.
Output: Set of keys.
set $X_0 \leftarrow 0.3$
set  $r \leftarrow 3.65321$
set  $j \leftarrow 1,\ i \leftarrow 1$
$k \leftarrow (n * X_0^2 \bmod n)$
while i <= kcount
    if $k \neq 0$ then
        $key_i \leftarrow k \times$Shared key
        $i \leftarrow i+1$
    end if
    $X_j \leftarrow r \times X_{j-1} \times (1-X_{j-1})$
    $k \leftarrow (n * X_j^2 \bmod n)$
    $j \leftarrow j+1$
end while
return key
```

The algorithmic structure for encryption of the proposed method is explained in Algorithm-2.

Algorithm-2: The proposed method Encryption

```
Input: Set of keys ∈ EC, Pm is plaintext.
Output: Pc is the Ciphertext.
for i = 1 to length Pm
    $Pc_i \leftarrow Pm_i + key_i$
end for
return Pc
```

The Table 2 below display results of the proposed method encryption.

Table 2: The encrypted points process of the proposed method.

Symbol	*ASCII*	*Pm*	*key*	*Pc*
c	99	(1554,733)	(3506,4496)	(5323,2193)
o	111	(4346,239)	(1331,2676)	(998,4228)
m	109	(2111,4943)	(4860,2373)	(1080,1225)
p	112	(4348,431)	(4554,303)	(662,1458)
u	117	(1918,2735)	(407,996)	(5311,1117)
t	116	(2295,3760)	(4308,337)	(2859,2510)
e	101	(1000,4912)	(2034,3587)	(2572,1645)
r	114	(4747,3682)	(4728,3843)	(725,1527)
space	32	(5243,1002)	(3487,3215)	(4029,3668)
s	115	(1902,3091)	(831,3842)	(1689,1186)
c	99	(1554,733)	(4866,1343)	(526,5366)
i	105	(4262,2781)	(4395,3626)	(2769,2075)
e	101	(1000,4912)	(2862,2342)	(3178,2197)
n	110	(201,1644)	(2293,5275)	(4943,5415)
c	99	(1554,733)	(1387,3950)	(2561,1731)
e	101	(1000,4912)	(4496,4066)	(4962,2512)

The algorithmic structure for decryption of the proposed method is explained in Algorithm-3.

Algorithm-3: The proposed method decryption

Input: Set of keys ∈ EC, Pc is the Ciphertext.
Output: Pm is plaintext.

```
for i = 1 to length Pc
    $Pm_i \leftarrow Pc_i - key_i$
end for
return Pm
```

The Table 3 below display results of the proposed method decryption.

Table 3: The decrypted points process of the proposed method.

Pc	*key*	*Pm*	*ASCII*	*Symbol*
(5323,2193)	(3506,4496)	(1554,733)	99	c
(998,4228)	(1331,2676)	(4346,239)	111	o
(1080,1225)	(4860,2373)	(2111,4943)	109	m
(662,1458)	(4554,303)	(4348,431)	112	p
(5311,1117)	(407,996)	(1918,2735)	117	u
(2859,2510)	(4308,337)	(2295,3760)	116	t
(2572,1645)	(2034,3587)	(1000,4912)	101	e
(725,1527)	(4728,3843)	(4747,3682)	114	r
(4029,3668)	(3487,3215)	(5243,1002)	32	space
(1689,1186)	(831,3842)	(1902,3091)	115	s
(526,5366)	(4866,1343)	(1554,733)	99	c
(2769,2075)	(4395,3626)	(4262,2781)	105	i
(3178,2197)	(2862,2342)	(1000,4912)	101	e
(4943,5415)	(2293,5275)	(201,1644)	110	n
(2561,1731)	(1387,3950)	(1554,733)	99	c
(4962,2512)	(4496,4066)	(1000,4912)	101	e

8. Evaluation

The proposed method is compared with both Symmetric ECC and AlGamal ECC techniques. It uses both the public and the privet key for the sender/receiver to create shared key. This shared key will be used in either side and it is considered as a strength point of the proposed method. In every symbol, this shared key changes by use of scalar multiplication produced by applying logistic map equation. When exposed the secret key for one symbol, the rest keys of the other symbol are not exposed. Through the implementation of this work on processor Core i5-2.3GHz and RAM 4.00 GB, the time consumption for The proposed method is approximately double compared to the time of Symmetric ECC, the ratio is (215% - 219%), and the ratio to AlGamal ECC ranges from (22% - 24%).

9. Discussions & Conclusion

The main advantages of the ECC technique can be illustrated as: depressed power exhaustion, high processing speeds, low storage capacity and good bandwidth savings. In this research, an encryption technique relies on the ECC technique. Hence, every symbol in the message coded by its ASCII code, and then using scalar multiplication between ASCII code and base point (Pm) to obtain new point (Pm1) at EC to represent the symbol. The conversion from symbol to point provides two characteristics; first, an ASCII value of the symbol is changed into a pair of Cartesian coordinates in the EC plane, secondly, the conversion inserts non-linearity to the symbol (this way perfectly disguising its identity. These points are encrypting using the EC technique. Decryption of cipher message is begin by remove the mask from the point by subtract the shared key and then convert the point to the ASCII value by using the mapping points process, and then convert the value to the original symbol. The strong point of this method is the symbol key which is generated by both of sender and receiver by using the privet key and public key by using Deffi Hellman to exchange the initial parameters. The main contribution of this paper is through changing the secret key for every symbol and when exposed the secret key for one symbol is not mean for all symbol keys are exposed.

Reference

[1] William Stallings, "Cryptography and Network Security Principles and Practice", Fifth Edition, 2011.

[2] Christof Paar and Jan Pelz, "Understanding Cryptography", © Springer-Verlag Berlin Heidelberg 2010.

[3] Darrel Hankerson, Alfred Menezes and Scott Vanstone, "Guide to Elliptic Curve Cryptography", © Springer-Verlag New York, Inc. 2004.

[4] Padma Bh,, D .Chandravathi and P. Prapoorna Roja, "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method", International Journal on Computer Science and Engineering, Vol. 02, No. 05, 2010, pp.1904-1907.

[5] Moumita Roy, Nabamita Deb and Amar Jyoti Kumar, "Point Generation and Base Point Selection in ECC: An Overview", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 5, 2014, pp. 6711- 6713.

[6] V. Miller, “Uses of elliptic curves in cryptography”, in Proceedings of the Conference on the Theory and Application of Cryptographic Techniques (CRYPTO), 1985, pp. 417–426.

[7] Ravi Kishore Kodali and N.V.S Narasimha Sarma, "ECC Implementation using Koblitz’s Encoding", in Proceedings of the Conference on Communication Engineering and Network Technologies (CENT), Elsevier, 2012, pp. 411-417.

[8] M. Aydos, T. Yanik and C. K. Kog, "High-speed implementation of an ECC based wireless authentication protocol on an ARM microprocessor", lEEE Proc Commun.,Vol. 148, No.5, 2001, pp. 273-279.

[9] Sangook Moon, "A Binary Redundant Scalar Point Multiplication in Secure Elliptic Curve Cryptosystems", International Journal of Network Security, Vol.3, No.2, 2006, PP.132-137.

[10] Jaewon Lee, Heeyoul Kim, Younho Lee, Seong-Min Hong, and Hyunsoo Yoon, "Parallelized Scalar Multiplication on Elliptic Curves Defined over Optimal Extension Field", International Journal of Network Security, Vol.4, No.1,2007, PP.99-106.

[11] Liu Yongliang, Wen Gao, Hongxun Yao, and Xinghua Yu , "Elliptic Curve Cryptography Based Wireless Authentication Protocol", International Journal of Network Security, Vol.4, No.1, 2007, PP.99-106.

[12] N. A. Saqib, F. Rodriguez-Henriquez and A. Diaz-perez, "A parallel architecture for fast computation of elliptic curve scalar multiplication over GF(2m) ", in Proceedings of the 18th International Parallel and Distributed Processing symposium, USA, , 2004.

[13] Bin Yu, "Method to Generate Elliptic Curves Based on CM Algorithm", in Proceedings of the Conference on the Information Theory and Information Security, IEEE, 2010.

[14] J. Nafeesa Begum, K. Kumar and Dr. V. Sumathy, "Multilevel Access Control in Defense Messaging System Using Elliptic Curve Cryptography", in Proceedings of the International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, 2010, pp. 1-9.

[15] Guicheng shen and Xuefeng zheng, "Research on Implementation of Elliptic Curve Cryptosystem in E-Commerce", in Proceedings of the Symposium on Electronic Commerce and Security, IEEE, 2008.

[16] Muhammad Hammad Ahmed, Syed Wasi Alam, Nauman Qureshi and lrum Baig, " Security for WSN based on ECC", in Proceedings of the International Conference on Computer Networks and Information Technology (ICCNIT),2011, pp. 75-79.

[17] R K Pateriya and Shreeja Vasudevan, "Elliptic curve Cryptography in Constrained Environments", in Proceedings of the International Conference on Communication Systems and Network Technologies (CSNT), 2011, pp. 120-124.

[18] Haider M. Al-Mashhadi, Hala B. Abdul-Wahab and Rehab F. Hassan, "Chaotic Encryption Scheme for Wireless Sensor Network’s Message", in Proceedings of the World Symposium On Computer Networks and Information Security, DOI: WSCNIS.2014 © N&N Global Technology 2014, pp. 116-120.

[19] Haider M. Al-Mashhadi, Hala B. Abdul-Wahab and Rehab F. Hassan, "Data Security Protocol for Wireless Sensor Network using Chaotic Map", International Journal of Computer Science and Information Security, Vol. 13, No. 8, 2015, pp. 80-89.