Journal of Theoretical and Applied Information Technology
31st March 2016. Vol.85. No.3
© 2005 - 2016 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NEW MODIFICATION FOR MENEZES-VANSTONE ELLIPTIC CURVE CRYPTOSYSTEM

[1] ZIAD E. DAWAHDEH*, [2] SHAHRUL N. YAAKOB, [3] ROZMIE RAZIF BIN OTHMAN
[1,2,3] School of Computer and Communication Engineering
UniMAP University, Perlis, Malaysia
E-mail: [1] mziadd@hotmail.com
*Corresponding Author

ABSTRACT

Information security algorithms are widely used in the recent times to protect data and messages over internet. Elliptic Curve Cryptography (ECC) is one of the most efficient techniques that are used for this issue, because it is difficult for the adversary to solve the elliptic curve discrete logarithm problem to know the secret key that is used in encryption and decryption processes. A new efficient method has been proposed in this paper to improve the Menezes-Vanstone Elliptic Curve Cryptography (MVECC). This modification reduces the running time needed for encryption and decryption processes compared with the original method and another two methods. In the modified method, only addition and subtraction operations are used, and no inversion or multiplication operations because it consumes a long time comparing with addition and subtraction, and this makes the proposed algorithm faster in computations and running time than the original and other methods. Moreover, the modified method uses the hexadecimal ASCII value to encode each character in the message before encryption, which makes the algorithm more secure and complicated to resist the adversaries.

Keywords: *Elliptic Curve Cryptography, Menezes-Vanstone Elliptic Curve Cryptosystem, Encryption, Decryption, Hexadecimal ASCII.*

1. INTRODUCTION

Cryptography is one of the mathematical techniques that ensure secure communications within a non-secure channel. Public key cryptography (asymmetric cryptography) is one of the famous techniques used recently. The private key of the sender is different from the private key of the receiver. The two parties need first to generate the private and public keys for each party and then agree upon elliptic curve domain parameters. Plaintext is the message that will be sent and after encryption it called ciphertext. The receiver needs to decipher the ciphertext by his private key to read the message [1]. Both sender and receiver are exchanging their public keys, which are not secret by using Elliptic Curve Diffie Hellman technique (1976) [2]. Therefore, each entity has a private key which is secret, and a public key which is not secret and shares among internet. Elliptic curve cryptography (ECC) is one of the effective public key cryptography techniques. It used for the first time by Miller [3] and Koblitz [4]; Miller proposed analogues of the Diffie-Hellman key exchange protocol and Koblitz proposed analogues of ElGamal. It depends on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which cannot be solved by the adversary. The level of difficulty in solving the DLP can be increased by selecting a base point G whose order is very large (the order of G is the smallest positive integer n such that $nG=O$) [5][24]. ECC provides a smaller key size with a little amount of memory and low power [6][7] compared to others systems like RSA, where a key size of 160 bits in ECC is equivalent to that accorded by 1024 bits in RSA. ECC has some advantages that make it widely used these days such as small storage capacity, faster computations and reduction of the power consumption [8]. ElGamal in 1985 was the first one who proposed public key encryption technique that based on the discrete logarithm problem. The security of ElGamal is based on the difficulty of computing discrete logarithms [9]. Lenstra in 1987 gave an important role for the elliptic curves in integer factorization [10]. Menezes Vanstone

© 2005 - 2016 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Elliptic Curve Cryptosystem (MVECC) was one of the famous techniques that used ECC and gave security for the data [11]. We used this technique in our paper and updated it to make it more efficient and secure and simplified the mathematical calculations by replacing the inverse operation by addition and multiplication.

Several studies have been presented by many researchers. For instance, Williams Stallings in 2011 introduced study about ECC in his book [12]. Ali Makki (2012) proposed three techniques based on the elliptic curve. He reduced the calculation time compared with the original method by using multiplication operation instead of inverse operation [13]. Hongqiang in 2013 proposed an approach to generate a random number k and sped up computing the scalar multiplication in the encryption and decryption processes [14]. Najlae Al-Saffar in 2013 proposed three methods to encrypt and decrypt a message using the Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC) [15]. An implementation of ElGamal ECC for encryption and decryption a message was also proposed by Debabrat Boruah in 2014 [16]. Meltem Kurt and Tarik Yerlikaya in 2013 presented a modified cryptosystem using hexadecimal to encrypt data. Their study depended on Menezes Vanstone ECC algorithm by adding additional features [17]. Qasem Abu Al-Haija' et al computed the standard ECC point doubling over $GF(p)$ without using inverse operations by converting the inversion to multiplication operation [18]. Ahmed Tariq and Nasreen Kadhim proposed a new method for the MVECC. They made the system more security and more confusion than the original algorithm, and used the inverse operation only once [19].

In this study, a new method uses Menezes-Vanstone Elliptic Curve Cryptography (MVECC) for encryption and decryption of the plaintext has been proposed by using only addition and subtraction operations without using inverse and multiplication operations, which makes the computations easier and faster. Hexadecimal ASCII value is used to represent each character in the message before encryption. The small amount of memory needed, less computations, small key size and bandwidth saving are some advantages for using ECC that make it more usable than other techniques because it leads to higher speeds and power efficiency which makes it suitable for some applications like e-commerce and mobile banking systems [13].

This paper is organized as follows. Section 2 presents a mathematical introduction to elliptic curve function over prime field. Section 3 describes the original algorithm Menezes-Vanstone Elliptic Curve Cryptography. Section 4 explains the modified cryptosystem for Menezes-Vanstone in both encryption and decryption. Section 5 explains an example for the proposed method. The comparison between the proposed method and Menezes-Vanstone method (MVECC), Ali Makki method, and Al-Saffar method is discussed in Section 6. Finally, Section 7, shows the conclusion and displays the advantages of the proposed method.

2. INTRODUCTION TO ELLIPTIC CURVE

Definition 2.1 An elliptic curve E over a prime field F_p is defined by

$$E: y^2 \equiv x^3 + ax + b \ (mod\ p) \quad (1)$$

where $a, b \in F_p$, $p \neq 2, 3$, and satisfy the condition $4a^3 + 27b^2 \not\equiv 0 \ (mod\ p)$. The elliptic curve group $E(F_p)$ is the set of all points (x, y) that satisfy the elliptic curve Equation (1) beside a special point O at infinity [1][20].

2.2 Elliptic Curve Operations

2.2.1 Point Addition

Suppose $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, where $P \neq Q$, are two points lie on an elliptic curve E defined in Equation (1). The sum $P + Q$ results a third point R which is also lies on E. To add two points on E there are some cases on the coordinates of the points P and Q. These cases are given as follows [17]

- If $P \neq Q \neq O$ with $x_1 \neq x_2$, then sum of P and Q in this case is defined by

  $$P + Q = R = (x_3, y_3) \quad (2)$$

  where

  $$\lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)} \quad (3)$$

  $$x_3 \equiv (\lambda^2 - x_1 - x_2) \ (mod\ p) \quad (4)$$

  $$y_3 \equiv (\lambda(x_1 - x_3) - y_1) \ (mod\ p) \quad (5)$$

- If $x_1 = x_2$ but $y_1 \neq y_2$ then $P + Q = O$.

© 2005 - 2016 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.2.2 Point Doubling

Let $P = (x_1, y_1)$ be a point lies on E. Adding the point P to itself is called doubling point on an elliptic curve E [21][22]. In other words

$$P + P = 2P = R = (x_3, y_3) \quad (6)$$

where

$$\lambda = \frac{3\,{x_1}^2 + a}{2\,y_1} \quad (7)$$

$$x_3 \equiv (\lambda^2 - 2x_1)\ (mod\ p) \quad (8)$$

$$y_3 \equiv (\lambda(x_1 - x_3) - y_1)\ (mod\ p) \quad (9)$$

2.2.3 Scalar Multiplication

Suppose k is an integer and $P = (x_1, y_1)$ is a point lies on E. The scalar multiplication can be defined by

$$kP = \underbrace{P + P + \cdots + P}_{k-times} \quad (10)$$

In other words, adding a point P to itself k times [21].

A scalar multiplication kP can be computed using the point doubling and point addition laws. For example, the scalar multiplication $9P$ can be calculated by the following expression:

$$9P = 2\big(2(2P)\big) + P.$$

2.2.4 Inverse Operation

Let $P = (x, y)$, then the negative of the point P is $Q = -P = (x, -y)$ where $P + Q = O$ [23].

Definition 2.3 The order of an elliptic curve is defined as the number of points of the curve and denoted by $\#E$ [1][23].

Definition 2.4 Let P be an element of the elliptic curve group $E(F_p)$, then P is a generator point if $ord(P) = \#E$ [1][23].

3. MENEZES-VANSTONE ELLIPTIC CURVE CRYPTOSYSTEM (MVECC)

MVECC is a cryptosystem that has no analogue for discrete logarithm problem; this means that it does not depend on discrete logarithm problem like ElGamal cryptosystems. Therefore, sender does not need to embed the plaintext on the EC but only mask it. In ElGamal elliptic curve the sender needs to map each character in the plaintext to a point on the elliptic curve before the encryption, where in MVECC no needs for mapping but only replacing each character with an ordered pair that is not required to be a point on E and this makes MVECC more efficient than ElGamal technique [19].

When the sender (user A) wants to send a message $M = (m_1, m_2)$ to user B, they need first to agree upon the elliptic curve $E(F_p)$ and the base point G. Each party chooses a private key randomly from the interval $[1, n]$; d for user A and e for user B, and computes his public key by multiplying his private key by the base point ($P_A = d.G$ and $P_B = e.G$). User A computes the secret key K by multiplying his private key d by user B public key P_B

$$K = e.P_A = d.P_B = d.e.G = (k_1, k_2)$$

Then ciphers the message by calculating

$$c_1 = m_1 * k_1\ \ mod\ p$$

$$c_2 = m_2 * k_2\ \ mod\ p$$

And sends $\{P_A, (c_1, c_2)\}$ to user B.

When user B wants to decrypt the ciphertext (c_1, c_2) he needs first to multiply his private key e by user A public key P_A and computes the secret key $K = e.P_A = e.d.G = (k_1, k_2)$, then computes the following

$$m_1 = c_1 * {k_1}^{-1}\ \ mod\ p$$

$$m_2 = c_2 * {k_2}^{-1}\ \ mod\ p$$

to get the original message $M = (m_1, m_2)$ [15].

Any adversary can only see P_A and P_B and cannot find the message M without solving the ECDLP which is very difficult without knowing the private keys *d* and *e*. So, MVECC is an efficient and secure technique.

4. THE MODIFIED CRYPTOSYSTEM

The modification of Menezes-Vanstone Elliptic Curve Cryptosystem (MMVECC) has been introduced in this section. This modification speeding up the calculations and making the system more efficient than the original technique and all the previous proposed methods, where it is never needed to calculate the inverse operation in both encryption and decryption operations. In addition, it makes the message more complicated for the adversary because we use the hexadecimal ASCII value for each character in the message instead of the decimal value. Suppose user A and user B wishing to communicate and exchange messages using MMVECC over insecure channel. Firstly, they should agree on the elliptic curve function E

© 2005 - 2016 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and sharing the domain parameters $\{a, b, p, G\}$, where a, b are the coefficients of the elliptic function and p is a large prime number and G is the generator point. When user A (the sender) wants to send a message M to user B (the receiver), each parties need to choose randomly a private key from the interval $[1, p-1]$, n_A for user A and n_B for user B. The public key for each user can be generated as follows

$$P_A = n_A . G$$
$$P_B = n_B . G$$

Each user computes the secret key $K = (x, y)$ by multiplying his private key by the public key of the other user

$$K = n_A . P_B = n_B . P_A = n_A . n_B . G = (x, y)$$

One of the contribution in this paper depends on using the hexadecimal ASCII value instead of the decimal value and this makes the system more conflict. Suppose user A wants to send a message M to user B. Firstly, he converts each character in the message M into hexadecimal ASCII value of two digits $(h_1 h_2)_{16}$, then separates the value into two values $(h_1, h_2)_{16}$ and converts each value of h_1 and h_2 to decimal values d_1 and d_2 respectively [25]. Then he computes the ciphertext message (c_1, c_2) as follows

$$c_1 = (d_1 + x + y) \ mod \ p$$
$$c_2 = (d_2 + c_1) \ mod \ p$$

and send the point (c_1, c_2) to user B.

Now, when user B receives the ciphertext message (c_1, c_2), he starts the decryption process by doing the following calculations

$$d_1 = (c_1 - x - y) \ mod \ p$$
$$d_2 = (c_2 - c_1) \ mod \ p$$

then converts the decimal values d_1 and d_2 to hexadecimal values h_1 and h_2 respectively, and writes them as $(h_1 h_2)_{16}$, then finds the match character from the hexadecimal ASCII table to get the original character. Repeat the previous procedure for each character in the message M.

The Proposed Algorithm (MMVECC)

Step 1: Key Generation

User A

1. Choose the private key $n_A \in [1, p-1]$
2. Compute the public key $P_A = n_A . G$

User B

1. Choose the private key $n_B \in [1, p-1]$
2. Compute the public key $P_B = n_B . G$

The secret key will be $K = n_A . P_B = n_B . P_A = n_A . n_B . G = (x, y)$

Step 2: Encryption (user A)

1. Convert each character of the message M to hexadecimal ASCII value of two digits $(h_1 h_2)_{16}$.
2. Rewrite the value $(h_1 h_2)_{16}$ as $(h_1, h_2)_{16}$ then convert it to two decimal values $(d_1, d_2)_{10}$.
3. Compute the secret key $K = n_A . P_B = (x, y)$. // n_A the private key of user A and P_B the public key of user B
4. Compute $c_1 = (d_1 + x + y) \ mod \ p$.
5. Compute $c_2 = (d_2 + c_1) \ mod \ p$.
6. Send (c_1, c_2) to user B.

Step 3: Decryption (user B)

1. Compute the secret key $K = n_B . P_A$.
2. Compute $d_1 = (c_1 - x - y) \ mod \ p$.
3. Compute $d_2 = (c_2 - c_1) \ mod \ p$.
4. Convert $(d_1, d_2)_{10}$ to hexadecimal $(h_1, h_2)_{16}$ and rewrite it as $(h_1 h_2)_{16}$.
5. Find the match character for $(h_1 h_2)_{16}$ from the hexadecimal ASCII table.

5. IMPLEMENTATION EXAMPLE

Suppose that user A wants to send a message to user B and they agreed to use the elliptic curve function

$$E: \ y^2 \equiv x^3 + x + 3 \ (mod \ 31)$$

where $A = 1, B = 3, p = 31$; which satisfies the condition $4A^3 + 27B^2 = 4(1)^3 + 27(3)^2 = 4 + 243 = 247 \ mod \ 31 = 30 \neq 0$, then the points of the elliptic curve $E_{31}(1, 3)$ are shown in Table 1.

Table 1: points on the elliptic curve $E: y^2 \equiv x^3 + x + 3 \ (mod \ 31)$

(1, 6)	(6, 15)	(15, 13)	(21, 4)	(26, 11)
(1, 25)	(6, 16)	(15, 18)	(21, 27)	(26, 20)
(3, 8)	(9, 11)	(17, 2)	(22, 3)	(27, 11)
(3, 23)	(9, 20)	(17, 29)	(22, 28)	(27, 20)
(4, 3)	(12, 10)	(18, 5)	(23, 14)	(28, 2)
(4, 28)	(12, 21)	(18, 26)	(23, 17)	(28, 29)
(5, 3)	(14, 8)	(20, 5)	(24, 5)	(30, 1)
(5, 28)	(14, 23)	(20, 26)	(24, 26)	(30, 30)

© 2005 - 2016 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The order of the elliptic curve $E_{31}(1,3)$ is 41, which is prime number, so we can choose any point from Table1 as base point or generator, let us choose $G = (1,6)$ [26]. So, the domain parameters are $\{A, B, p, G\} = \{1, 3, 31, (1,6)\}$. Suppose user A wants to send the message "**Computer**" to user B, he should first convert each character of the message "**Computer**" to the hexadecimal value from the ASCII table, then separates each value into two values and converts them to decimal values

C → $(43)_{16}$ → $(4, 3)_{16}$ → $(4, 3)_{10}$
o → $(6F)_{16}$ → $(6, F)_{16}$ → $(6, 15)_{10}$
m → $(6D)_{16}$ → $(6, D)_{16}$ → $(6, 13)_{10}$
p → $(70)_{16}$ → $(7, 0)_{16}$ → $(7, 0)_{10}$
u → $(75)_{16}$ → $(7, 5)_{16}$ → $(7, 5)_{10}$
t → $(74)_{16}$ → $(7, 4)_{16}$ → $(7, 4)_{10}$
e → $(65)_{16}$ → $(6, 5)_{16}$ → $(6, 5)_{10}$
r → $(72)_{16}$ → $(7, 2)_{16}$ → $(7, 2)_{10}$

Now, apply the proposed algorithm (MMVECC) on the first character "**C**". Firstly, user A should convert the character "**C**" to $(43)_{16}$ hexadecimal value from the ASCII table, then separate the hexadecimal value 43 into two values $(4, 3)_{16}$ and convert them to decimal values $(4, 3)_{10}$, then follow the following steps

Step 1: Key Generation

User A

1. Choose the private key $n_A = 13 \in [1, 30]$.
2. Compute the public key $P_A = n_A.G = 13(1,6) = (3, 23)$.

User B

1. Choose the private key $n_B = 17 \in [1, 30]$.
2. Compute the public key $P_B = n_B.G = 17(1,6) = (24, 5)$.

User A and user B will exchange their public keys P_A and P_B.

Step 2: Encryption (user A)

1. "C" → $(43)_{16}$
2. $(43)_{16}$ → $(4, 3)_{16}$ → $(4, 3)_{10} = (d_1, d_2)_{10}$
3. $K = n_A.P_B = 13(24, 5) = (20, 5) = (x, y)$
4. $c_1 = d_1 + x + y = (4 + 20 + 5)\ mod\ 31 = 29\ mod\ 31 = 29$
5. $c_2 = d_2 + c_1 = (3 + 29)\ mod\ 31 = 32\ mod\ 31 = 1$
6. Send $(29, 1)$ to user B.

Step 3: Decryption (user B)

1. $K = n_B.P_A = 17(3, 23) = (20, 5) = (x, y)$
2. $d_1 = (c_1 - x - y)\ mod\ p = (29 - 20 - 5)\ mod\ 31 = 4\ \ mod\ 31 = 4$
3. $d_2 = (c_2 - c_1)\ mod\ p = (1 - 29)\ mod\ 31 = -28\ \ mod\ 31 = 3$
4. Convert $(4, 3)_{10}$ to hexadecimal $(4, 3)_{16}$ and rewrite it as $(43)_{16}$.
5. Find the match character for $(43)_{16}$ from the hexadecimal ASCII table which is "**C**".

The same processes for the other characters "**omputer**" should be repeated.

6. RESULTS and DISCUSSIONS

In this section, a comparison between the proposed method in this paper (MMVECC), Menezes-Vanstone method (MVECC), Ali Makki method, and Al-Saffar method is done on the mathematical operations and running time. Let us denote the addition operation by *Add*, the subtraction operation by *Sub*, the multiplication operation by *Mult*, and the inverse operation by *Inv*. Table 2 summarizes the mathematical operations that is needed for each method in encryption and decryption.

Table 2: The required operations for each method

The method	Encryption	Decryption
MVECC	2 Mult	2Mult + 2 Inv
Al-Saffar method	2 Mult + 2 Add	2 Mult + 1 Inv + 2 Sub
Ali Makki method	3 Mult + 3 Add	2 Mult + 2 Sub
The proposed method (MVECC)	3 Add	3 Sub

It shows that no multiplication or inverse operations are needed in the proposed method, only addition and subtraction. Whereas, in all other methods multiplication operation is needed, and inverse operation is needed in MVECC and Al-Saffar method. This makes the proposed method

© 2005 - 2016 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

easier in calculations and more efficient in encryption and decryption time than all other methods.

Table 3 summarizes the total running time in seconds that is needed for encryption and decryption in the proposed method (MMVECC) and the other three methods. It shows the total time in seconds for each method in encryption and decryption processes on messages from different sizes. It is clear that the time needed for the proposed method is less than the time needed for each of the other methods, and this leads to the fact that the proposed method is easier in the mathematical calculations and more efficient than the original method (MVECC) and the other two methods. We have programmed the four methods on Core i5 computer with CPU 2.53 GH_z and RAM 4 GB by using MATLAB R2013a (8.1.0.604) 32-bit software to compute the encryption and decryption time on messages with different sizes.

Figure 1 represents the total time in seconds for encryption and decryption processes on messages from different sizes. The graph shows that the proposed method (MMVECC) time is less than the time required for the other methods, and when the size of the message increases the difference in the time is also increases.

7. CONCLUSIONS

Information security is one of the most important issues in the recent times. ECC is one of the most efficient public key cryptosystems that is secured against adversaries because it is difficult for them to solve the elliptic curve discrete logarithm problem to find the secret key. Its strengthened security comes from the small key size that is used in it with the same security level compared to the other cryptosystems like RSA. ECC is one of the most effective techniques that is useful to be used in portable devices, chip cards, smart cards, and mobile devices because it has a fast computations and works on small memory and low power consumption.

In this paper, a new efficient method has been proposed to improve the Menezes-Vanstone Elliptic Curve Cryptography. The main contribution is to reduce the running time needed for encryption and decryption processes as shown in Table 3. In the proposed method, no inverse or multiplication operations are used because it consumed time in calculation, only addition and subtraction operations are used as shown in Table 2, which make the computations faster and reduce the running time. Using the hexadecimal ASCII value to encode each character before encryption as shown in the previous example is another contribution in this work, which makes computations also easier and faster and the proposed method more secure from the adversaries.

REFERENCES:

[1] Hankerson, Darrel, Menezes, Alfred J., Vanstone, Scott, Guide to Elliptic Curve Cryptography, Springer-Verlag, 2004.

[2] Diffie, W. and Hellman, "New Directions in Cryptography."IEEE Trans. On Information Theory, IT-22, vol.6, pp.644-654, 1976.

[3] V. S. Miller, Use of elliptic curves in cryptography, Advanced in Cryptology, Proceedings of Crypto85, Lecture note in Computer Science, v. 218, Springer Verlag, pp. 417-426,1986.

[4] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, 48 (1987), 203-209.

[5] Su, Pin-Chang, Erl-Huei Lu, and Henry Ker-Chang Chang. "A knapsack public - key cryptosystem based on elliptic curve discrete logarithm." *Applied mathematics and computation* 168.1 (2005): 40-46.

[6] Alese, B. K., Philemon E. D., Falaki, S. O., Comparative Analysis of Public-Key Encryption Schemes, International Journal of Engineering and Technology Volume 2 No. 9, 2012.

[7] Rajadurga, K., and S. Ram Kumar. "GF (2m) Based Low Complexity Multiplier for Elliptic Curve Cryptography Systems." *Networking and Communication Engineering* 6, no. 4 (2014): 150-155.

[8] Fu Minfeng and Chen Wei, Elliptic curve cryptosystem EIGamal encryption and transmission scheme, International Conference on Computer Application and System Modeling (ICCASM 2010), 978-1-4244-7237-6/10 ©2010 IEEE.

[9] T. ElGamal. " A Public Key Cryptosystem and a Signature Scheme Based on Discrete

© 2005 - 2016 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Logarithms." IEEE Trans. On Information Theory 31 vol.4, pp.469-472, 1985.

[10] H. W. Lenstra, "Factoring integers with elliptic curves", Annals of Mathematics 126, pp. 649-673,1987.

[11] A. Menezes, S. Vanstone, " Elliptic curve Cryptosystem and their implementation", Journal of cryptography 6 (4), pp. 209 - 224, 1993.

[12] William Stallings, Cryptography and Network Security: Principles and Practices, Fifth Edition, Prentice Hall, 2011.

[13] Ali M. Sagheer, Elliptic curves cryptographic techniques, Proceeding of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS'2012), © 2012 IEEE, 12-14 December 2012, Gold Coast, Australia.

[14] Hongqiang Lv; Hui Li; Junkai Yi; Hao Lu, Optimal Implementation of Elliptic Curve Cryptography, International conference on service operations and logistics and informatics, 978-1-4799-0529-4©2013 IEEE.

[15] Al-Saffar, Najlae F. Hameed, Md Said, and Mohamad Rushdan. "On the Mathematical Complexity and the Time Implementation of Proposed Variants of Elliptic Curves Cryptosystems. " *International Journal of Cryptology Research* 4.1 (2013): 42-54.

[16] Boruah, D; Saikia, M., Implementation of ElGamal Elliptic Curve Cryptography over prime field using C, International conference on Information Communication and Embedded Systems, 978-1-4799-3835-3©2014 IEEE.

[17] Kurt, M., Yerlikaya, Y., A new modified cryptosystem based on Menezes Vanstone elliptic curve cryptography algorithm that uses characters' hexadecimal values, ISBN: 978-1-4673-5612-1©2013 IEEE.

[18] Q. Abu Al-Haija', M. Alkhatib and A. B. Jaafar, Choices on Designing Gf (P) Elliptic Curve Coprocessor Benefiting From Mapping Homogeneous Curves In Parallel Multiplications, International Journal on Computer Science and Engineering (IJCSESSN : 0975-3397 Vol. 3 No. 2 Feb 2011.

[19] Sadiq, Ahmed Tariq, and Nasreen J. Kadhim. ENHANCED MENEZES - VANESTONE ELLIPTIC CURVES CRYPTOSYSTEM, Journal of Al-Nahrain University, Vol.12(1), March, 2009, pp.162-165.

[20] Hoffstein, Jeffrey, Jill Pipher, and Joseph H. Silverman. "Elliptic Curves and Cryptography." In *An Introduction to Mathematical Cryptography*, pp. 299-371. Springer New York, 2014.

[21] Biswojit Nayak (2014), Signcryption schemes based on elliptic curve cryptography, Master Thesis, National Institute of Technology Rourkela, India.

[22] Udin, M. N., Halim, S. A., Jayes, M. I., Kamarulhaili , H., Application of message embedding technique in ElGamal elliptic curve cryptosystem, Statistics in Science, Business, and Engineering (ICSSBE), 2012.

[23] Oswald, Elisabeth. "Introduction to elliptic curve cryptography." *Institute for Applied Information Processing and Communication, Graz University Technology* (2002).

[24] Wenger, Erich, and Paul Wolfger. "Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster." In *Selected Areas in Cryptography--SAC 2014*, pp. 363-379. Springer International Publishing, 2014.

[25] Dawahdeh, Ziad E., Shahrul N. Yaakob, and Ali Makki Sagheer. " Modified ElGamal Elliptic Curve Cryptosystem using Hexadecimal Representation."*Indian Journal of Science and Technology* 8.15 (2015).

[26] Ali, M, Sagheer, Enhancement of elliptic curves cryptography methods, MSc. Thesis, University of Technology, Baghdad, Iraq, 2004.

© 2005 - 2016 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: Encryption And Decryption Time In Seconds On Different Messages

Message size (characters)	MVECC method	Al-Saffar method	Ali Makki method	The proposed method (MMVECC)
1000	0.0859	0.0728	0.0559	0.0388
5000	0.3036	0.2724	0.2110	0.1675
10000	0.6061	0.5206	0.3955	0.3407
20000	1.2205	0.9931	0.7673	0.6861
40000	2.3337	2.1500	1.7186	1.4125
80000	5.2036	4.2681	3.3731	2.7628

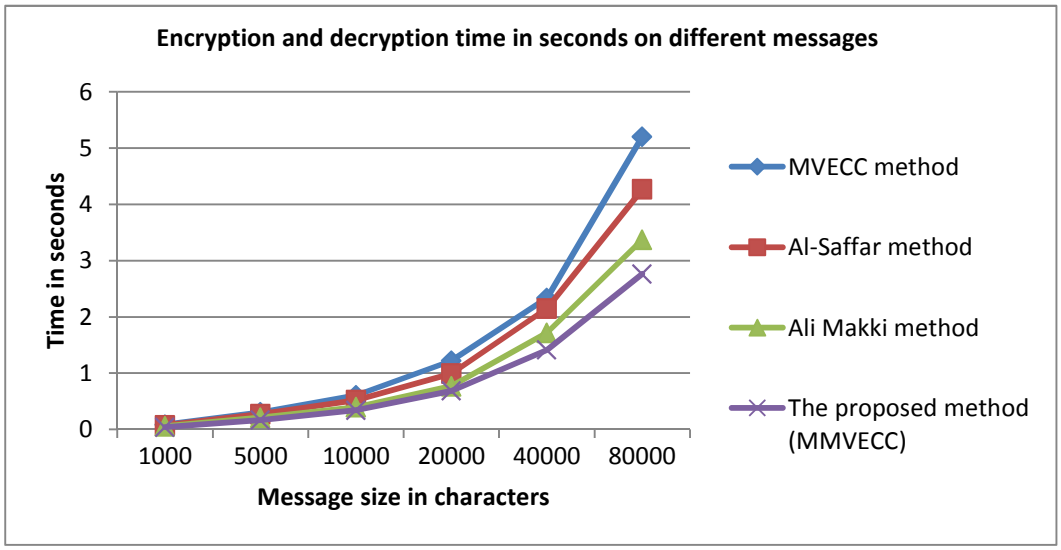

Figure 1: Encryption And Decryption Time In Seconds For Different Messages