Journal of Computer Science

Original Research Paper

Improvement of Menezes-Vanstone Elliptic Curve Cryptosystem Based on Quadratic Bézier Curve Technique

Dua M. Ghadi and Adil AL-Rammahi

Department of Mathematics, Faculty of Mathematics and Computer Science, University of Kufa, Iraq

Article history
Received: 16-03-2020
Revised: 24-04-2020
Accepted: 03-06-2020

Corresponding Author:
Dua M. Ghadi
Department of Mathematics, Faculty of Mathematics and Computer Science, University of Kufa, Iraq
Email: doaam.zubaidi@student.uokufa.edu.iq

Abstract: Cryptography is one of the most important applications and widely used in our life especially in the information security that needed by many government institutions, banks, communications and others to keep data over internet and other transportations that it is ensure safety of transfers between the sender and the recipient. The most important system in cryptography is public key cryptography and the mostly used is the elliptic curves cryptosystem, because of it is very efficient and secure and difficult to solve the discrete logarithm problem and find the secret key. In this study a new method is introduced using the Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC) for data based on quadratic Bézier curve techniques. The purpose of this proposal is to increase the security of this cryptosystem. We will apply this proposed method to all measurements of National Institute of Standards and Technology (NIST) tests and running time and compared it with the original method.

Keywords: Elliptic Curve Cryptosystem, Menezes-Vanstone Elliptic Curve, Bézier Curve, Encryption, Decryption, ASCII

Introduction

It is known that cryptography is one of the mathematical methods that ensure security of information communications, it contains algorithms and protocols which used to help it to do that, so cryptography it is very important for the security of communications between the sender and the recipient. Therefore, many researchers specialists in this approach developed the methods that used in cryptography to increase level of security of information exchange and reducing attacks, there are some research that has been using Bézier curves techniques like in (Srividya and Akhila, 2014) use quartic Bézier curve to improve encryption and decryption of data and to lower computational complexity which is depend on Galois field multiplication table. Abdul Wahab and Satter Jaber (2016) used quadratic Bézier curve in chebyshev to improvement NTRU and DES algorithm and also produce protocol depended on PGP behavior. Improve encryption algorithm for secure digital image depend on the scrambling the pixel's position and changing the gray value of image for pixel's image by using chaotic map and Bernstein from Bézier curve (El-Latif *et al*., 2011).

In this work, the proposition uses the Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC) based on quadratic Bézier curve for encryption and decryption that depend on Bézier's point, the parameters of t in the interval, [0,1] the key and point of message. This proposed uses the ASCII code values to represent each characters of the text.

This paper is organized as follows: Section 2 a Basic concepts of Quadratic Bézier Curve (QBC) and Elliptic Curve Cryptosystem (ECC), section 3 the proposed cryptography method using Menezes-Vanstone Elliptic Curve Cryptosystem and quadratic Bézier Curve, section 4 the implementation of example for proposed method, section 5 discussion and results of the comparison between the proposed method and the Original Method of Menezes-Vanstone Elliptic curve Cryptosystem and section 6 the conclusion and the advantages of the proposed method.

Basic Concepts of Quadratic Bézier Curve and Elliptic Curve Cryptosystem

Bézier curve it is one of the most important mathematical representations of curves and surfaces used in computer graphics and design forms. Therefore, in 1958 - 1960 was it the original development of Bézier curve in the cars manufacture by two French scientists Pierre Bézier and Paul de Casteljau. Bézier curves is polynomial curves and it is popularity used because it possess a number of mathematical properties which is easy to manipulation and analysis. A Bézier curve of degree n is specified by a sequence of n+1 points which are called the control points (Marsh, 1999).

DOI: 10.3844/jcssp.2020.715.722

Quadratic Bézier Curve (QBC)

Quadratic Bézier curve is described by three points $P_\circ$, P_1 and P_2. The first point and the third point are "anchors". The second point affect the shape of the curve. The generated curve starts at the first point $P_\circ$ going toward the second point P_1 and it settles at the third point P_2. Therefore, this curve will not pass through the second point P_1 (Armstrong, 2005).

To development of the quadratic Bézier curve let three control points $P_\circ$, P_1 and P_2 with parameter t, which it a number between in the interval (0,1) (Joy Kenneth, 2000).

** $P_1^{(1)}$ be a point on the piece $\overline{P_\circ P_1}$ and defined by (Fig. 1):

$$P_1^{(1)} = (1-t)P_\circ + tP_1 \quad (1)$$

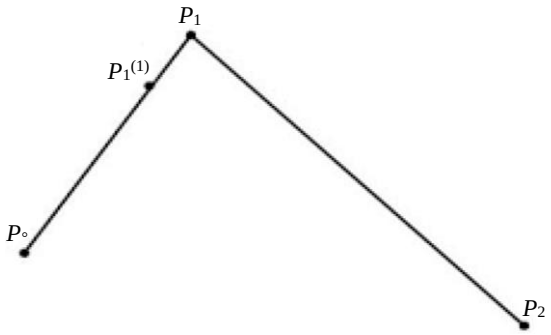

Fig. 1: representation of $P_1^{(1)}$ point.

** $P_2^{(2)}$ be a point on the piece $\overline{P_1 P_2}$ and defined by (Fig. 2):

$$P_2^{(1)} = (1-t)P_1 + tP_2 \quad (2)$$

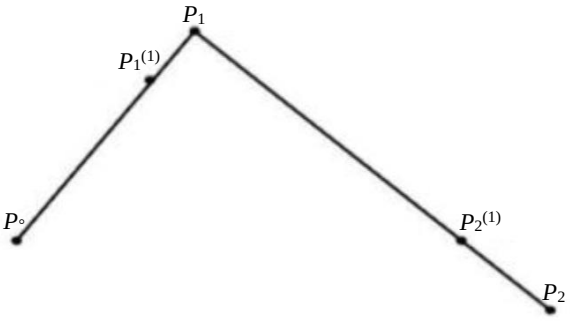

Fig. 2: representation of $P_2^{(1)}$ point.

** $P_2^{(2)}$ be a point on the piece $\overline{P_1^{(1)} P_2^{(1)}}$ and defined by (Fig. 3):

$$P_2^{(2)} = (1-t)P_1^{(1)} + tP_2^{(1)} \quad (3)$$

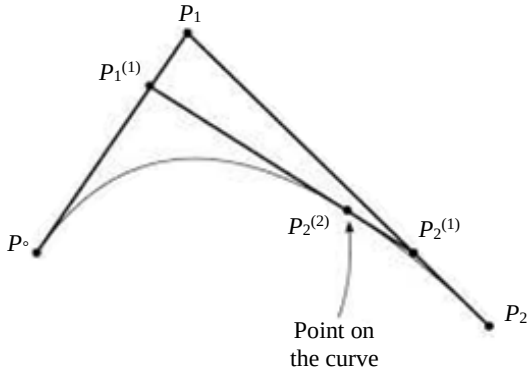

Fig. 3: representation of $P_2^{(2)}$ point on curve.

** Define $B(t) = P_2^{(2)}$

Each of this points $P_1^{(1)}$, $P_2^{(2)}$ and $P_2^{(2)}$ are a function of the parameter t and $P_2^{(2)}$ can be equated with $B(t)$ since it is a point of the curve that agree upon to the parameter value t for developing the equation of the curve. In this way $B(t)$ become the equation of Bézier curve:

$$\begin{aligned} B(t) &= P_2^{(2)}(t) \\ &= (1-t)P_1^{(1)}(t) + tP_2^{(1)}(t) \end{aligned}$$

Since, $P_1^{(1)}(t) = (1\text{-}t)P_\circ + tP_1$ and $P_2^{(1)}(t) = (1\text{-}t)P_1 + tP_2$. Then:

$$\begin{aligned} B(t) &= (1-t)\left[(1-t)P_\circ + tP_1\right] + 1\left[(1-t)P_1 + tP_2\right] \\ &= (1-t)^2 P_\circ + (1-t)tP_1 + (1-t)tP_1 + t^2 P_2 \\ &= (1-t)^2 P_\circ + 2(1-t)tP_1 + t^2 P_2 \end{aligned} \quad (4)$$

This is quadratic polynomial (Quadratic Bézier Curve):

$$x(t_1) = (1-t_1)^2 x_1 + 2t_1(1-t_1)x_2 + t_1^2 x_3 \quad (5)$$

$$y(t_2) = (1-t_2)^2 y_1 + 2t_2(1-t_2)y_2 + t_2^2 y_3 \quad (6)$$

$0 \le t_1, t_2 \le 1$, where, (x, y) are the control points.

Elliptic Curves Cryptosystem (ECC)

Elliptic curves was use in cryptography by Neal Koblitz in 1987 (Kobliz, 1987) and Miller (1986). Since then, many research papers have been published in this approach about security and efficient of elliptic curves, where elliptic curve systems have begun to receive wide agreement and have been used by private companies to keep their security products (Hankerson *et al*., 2004). There are another type of cryptosystem is called the public key cryptosystem, or asymmetric cryptosystem. The most famous cryptosystems

that used in public key cryptography are known as RSA and ECC and they provides the same level of security but ECC deals with shorter keys than keys that used in RSA it about (160-256 bit vs. 1024-3072 bit). ECC is based on the discrete logarithm problem and can be realized in EC protocols like Diffie- Hellman key exchange using elliptic curves. ECC has advantages like few of computations and (short signatures and keys) over RSA and Discrete Logarithm (DL) schemes. The elliptic curves are more associated with the mathematical than those of RSA and DL schemes (Paar and Pelzl, 2010). There are cryptosystems based on elliptic curve cryptography like ElGamal elliptic curve cryptosystem and Menezes-Vanstone elliptic curve cryptosystem and more. Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC) was one of a famous methods that used ECC and gave security for sender and recipient data (Menezes and Vanstone, 1993).

Definition 2.2.1

An elliptic curve E over a field F_p is defined by an equation:

$$E: y^2 = x^3 + ax + b \mod p \tag{7}$$

If p is an odd prime, then a and b shall satisfy ($4a^3 + 27b^2 \neq 0$) *mod p* in F_p and every point $P = (x_P, y_P)$ on E (other than the point O) in F_p (Mogollon, 2007).

Operations on Elliptic Curve

There are many arithmetic operations that used in Elliptic curve cryptosystems schemes as studied in (Stallings, 2017):

Point Addition

Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ such that $P \neq -Q$, are two points lie on an elliptic curve E defined the Equation (1). Then the sum $R = P + Q = (x_R, y_R)$ is determined by the following:

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \tag{8}$$

$$x_R = \left(\lambda^2 - x_P - x_Q\right) \mod p \tag{9}$$

$$y_R = \left[\lambda\left(x_P - x_R\right) - y_P\right] \mod p \tag{10}$$

Point Doubling

Let $P = (x_P, y_P)$ be a point lies on E. Adding the point P to itself:

$$P + P = 2P = R \tag{11}$$

where:

$$\lambda \frac{3x_P^{\,2} + a}{2y_P} \tag{12}$$

$$x_R = \left(\lambda^2 - 2x_P\right) \mod p \tag{13}$$

$$y_R = \left[\lambda\left(x_P - x_R\right) - y_P\right] \mod p \tag{14}$$

Multiplication

Let k is an integer and $P = (x_1, y_1)$ is a point lies on E. Is defined as repeated addition:

$$kP = P + P + \cdots + P \tag{15}$$

For example, the scalar multiplication $9P$ can be calculated by the following expression:

$$9P = 2\left(2\left(2P\right)\right) + P.$$

Negative of the Point

Let, $P = (x, y)$ then the negative of the point P is $-P = (x, -y)$ where, $P + (-P) = P - P = 0$.

Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC)

This cryptosystem has no analogue for Discrete Logarithm Problem (DLP), this means that it does not depend on discrete logarithm problem like ElGamal cryptosystems. Once one has a curve and a point on it, one is sure to succeed in embedding data into the system. That is not true for the elliptic curve analogue of DLP, it is a variant of the ElGamal analogue (Sadiq and Kadhim, 2009).

Therefore, in this cryptosystem the sender (Alice) and the recipient (Bob) are agree upon publicly an elliptic curve E over finite field F_p and abase point B on E. Bob chooses a secret integer d such that ($1 < d < N$), where N is the number of points of E and he computes and publishes his public key the point $Q_B = dB$ Alice wants to send the message $M = (m_1, m_2)$ to Bob, first she will choose a private random positive integer e such that ($1 < e < N$) then uses Bob's public key to compute $Q_A = eQ_B = (k_1, k_2)$ and encrypt her message by compute:

$c_1 = m_1 * k_1 \mod p$
$c_2 = m_2 * k_2 \mod p,$

where, $C = (c_1, c_2)$ is cipertext:

Send, $\{(c_1, c_2), eB\}$ *to Bob.*

When Bob decrypts the ciphertext $C = (c_1, c_2)$ he needs first to compute:

$$d(eB) = (k_1, k_2)$$

Then he computes the following:

$$m_1 = c_1 * k_1^{-1} \bmod p$$
$$m_2 = c_2 * k_2^{-1} \bmod p \text{ to get message}$$
$$M = (m_1, m_2) \text{ (Al-Saffar } et\ al.\text{, 2013)}$$

The Proposed Method

The modification of Menezes-Vanstone Elliptic curve cryptosystem MVECC has been produced in this section. This modification making the system has high level of security and more efficient than the original cryptosystem. This proposed based on the quadratic Bézier curve QBC technique (depend on the Equations (5) and (6)).

Assume that Alice and Bob want to communicate and exchange messages with each other using modified MVECC over insecure channel.

Firstly, they should agree on publicly an elliptic curve E over finite field F_p ($E(F_p)$) with equation:

$$E: y^2 = x^3 + ax + b \bmod p,$$

such that a and b satisfy the condition c:

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

and abase point B on E.

Secondly, they agree on secretly Bézier point (control point) $BP = (x, y)$ and the parameters $t = (t_1, t_2) \in [0,1] \bmod p$.

Bob chooses a private key d then computes and publish his public key by $Q_B = dB$.

Alice also chooses a secret random positive integer e and uses Bob's public key to compute $Q_A = eQ_B = (k_1, k_2)$ and computes eB.

Encryption part (Alice): Wants to send the message M to Bob, she must first convert each character in the message M to ASCII value according to Table 1, by take every two characters ($char_1$, $char_2$) in the message M and separate them to represented as a point then convert each of them into ASCII value (M_1, M_2).

Then she computes the ciphertext using Bézier point $BP = (x, y)$ and $t = (t_1, t_2) \in [0,1] \bmod p$ and the key $Q_A = (k_1, k_2)$ by:

$$c_1 = \left[x(1-t_1)^2 + 2k_1(1-t_1)t_1 + M_1 t_1^2 \right] \bmod p$$

$$c_2 = \left[y(1-t_2)^2 + 2k_2(1-t_2)t_2 + M_2 t_2^2 \right] \bmod p$$

Send, $\{(c_1, c_2), eB\}$ to Bob.

Decryption part (Bob): Receives the ciphertext, he start to compute $d(eB) = (k_1, k_2) = Q_A$ and then decrypts the ciphertext using Bézier point $BP = (x, y)$, $t = (t_1, t_2) \in [0,1] \bmod p$ and $Q_A = (k_1, k_2)$ as following:

$$M_1 = \left[c_1 - x(1-t_1)^2 - 2k_1(1-t_1)t_1 \right] . (t_1^2)^{-1} \bmod p$$
$$M_2 = \left[c_2 - y(1-t_2)^2 - 2k_2(1-t_2)t_2 \right] . (t_2^2)^{-1} \bmod p$$

Then converts the ASCII value (M_1, M_2) into characters ($char_1$, $char_2$) and rewrite to ($char_1$ $char_2$) then he get the original characters. By same way for each two characters in the message M.

Table 1: ASCII values of each printable characters

Space	32	0	48	@	64	P	80	`	96	p	112
!	33	1	49	A	65	Q	81	a	97	q	113
"	34	2	50	B	66	R	82	b	98	r	114
#	35	3	51	C	67	S	83	c	99	s	115
$	36	4	52	D	68	T	84	d	100	t	116
%	37	5	53	E	69	U	85	e	101	u	117
&	38	6	54	F	70	V	86	f	102	v	118
'	39	7	55	G	71	W	87	g	103	w	119
(	40	8	56	H	72	X	88	h	104	x	120
)	41	9	57	I	73	Y	89	i	105	y	121
*	42	:	58	J	74	Z	90	j	106	z	122
+	43	;	59	K	75	[	91	k	107	{	123
,	44	>	60	L	76	\	92	l	108	|	124
-	45	=	61	M	77	]	93	m	109	}	125
.	46	<	62	N	78	^	94	n	110	~	126
/	47	?	63	O	79	_	95	o	111	del	127

DOI: 10.3844/jcssp.2020.715.722

Implementation Example for Proposed Method

In this section, the implement the proposed method is studied in the following simple example:

Alice and Bob Agree Upon

1) Publicly: An Elliptic Curve E over F_{3023} and ($E(F_{3023})$) and B = (873, 1491) $\in E$, E: $y^2 = x^3 + 1x +$ 2825 mod 3023, where, a = 1, b = 2825 and p = 3023 satisfy the condition c: $4a^3 + 27b^2 = 4(1^3) + 27(2825^2) = 21546879 \bmod 3023 = 462 \neq 0$.
2) Secretly: Bézier point BP = (220, 260) and t = (0.75, 0.55) $\in$[0,1] mod 3023 and they compute:

$$t = \left(75 * 100^{-1}, 55 * 100^{-1}\right) \bmod 3023$$
$$t = \left(75 * 393, 55 * 393\right) \bmod 3023$$
$$t = \left(2268, 454\right)$$

Key Generation

1) Bob:
   Selects a private key d = 1465 and computes public key $Q_B = dB$ = 1465(873, 1491) = (1731, 2744)
2) Alice:
   Chooses a secret random positive integer e = 1280, uses Bob's public key to compute: $Q_A = eQ_B$ = 1280 (1731, 2744) = (1062, 1570) = (k_1, k_2)

Encryption Part (Alice)

1) Wants to send the plaintext "Cryptography" and takes two characters (*Cr*), (*yp*), (*to*), (*gr*), (*ap*) and (*hy*) separates them as a points:

$$(Cr) \to (C,r), (yp) \to (y,p), (to) \to (t,o), (gr) \to (g,r), (ap) \to (a,p) and (hy) \to (h,y)$$

2) Converts each of them into ASCII values to become:

(C, r) → (67, 114), (y, p) → (121, 112),
(t, o) → (116, 111), (g, r) → (103, 114),
(a, p) → (97, 112), (h, y) → (104, 121).

Encrypts her message (67,114) by compute:
Uses BP = (220, 260), t = (2268, 454) and Q_A = (1062, 1570) as follows:

$$c_1 = \left[x\left(1-t_1\right)^2 + 2k_1\left(1-t_1\right)t_1 + M_1 t_1^{\,2}\right] \bmod p$$
$$= \begin{bmatrix} 220\left(1-2268\right)^2 + 2\left(1062\right)\left(1-2268\right) \\ \left(2268\right) + \left(67\right)\left(2268^2\right) \end{bmatrix} \bmod 3023$$
$$= \left(-9445385156\right) \bmod 3023 = 2528$$
$$c_2 = \left[y\left(1-t_2\right)^2 + 2k_2\left(1-t_2\right)t_2 + M_2 t_2^{\,2}\right] \bmod p$$
$$= \begin{bmatrix} 260\left(1-454\right)^2 + 2\left(1570\right)\left(1-454\right) \\ \left(454\right) + \left(114\right)\left(454^2\right) \end{bmatrix} \bmod 3023$$
$$= \left(-568927116\right) \bmod 3023 = 1484$$

where, C = (2528, 1484) is ciphertext

3) Computes: eB = 1280(873, 1491) = (1085, 2103)
4) Sends {C, eB} to Bob

Decryption Part (Bob)

1) Computes $d(eB)$ = 1465(1085, 2103) = (1062, 1570) = (k_1, k_2) = Q_A
2) Decrypts the ciphertext C = (2528, 1484) by using Bézier point BP = (220, 260), t = (2268, 454) and Q_A = (1062, 1570) by compute:

$$M_1 = \left[c_1 - x\left(1-t_1\right)^2 - 2k_1\left(1-t_1\right)t_1\right].\left(t_1^{\,2}\right)^{-1} \bmod p$$
$$= \begin{bmatrix} 2528 - 220\left(1-2268\right)^2 - 2 \\ \left(1062\right)\left(1-2268\right)\left(2268\right) \end{bmatrix}.\left(2268^2\right)^{-1} \bmod 3023$$
$$= \left(9790023892\right)\left(2353\right) \bmod 3023 = 67$$
$$M_2 = \left[c_2 - y\left(1-t_2\right)^2 - 2k_2\left(1-t_2\right)t_2\right].\left(t_2^{\,2}\right)^{-1} \bmod p$$
$$= \begin{bmatrix} 1484 - 260\left(1-454\right)^2 - 2 \\ \left(1570\right)\left(1-454\right)\left(454\right) \end{bmatrix}.\left(454^2\right)^{-1} \bmod 3023$$
$$= \left(592425824\right)\left(1977\right) \bmod 3023 = 114$$

3) Converts from the ASCII values (67, 114) into characters (C, r).

4) Rewrites as (C, r) as (Cr). By the same way, for each remaining two characters until to get the original message

Results and Discussion

In this section, a comparison between the proposed method in this paper and the original method of MVECC is done the total running time in seconds to encryption and decryption of the message as in Table 2 and this

table shows that running time of the proposed method is almost the same in the original method for (1000, 3000 and 5000) characters, but the difference be in one-three seconds or the part of millisecond. According to the mathematical complexity for the number of operations which are used in the processing of encryption and decryption in Table 3 shows the proposed method possess operations of computational complexity more than in the original method and this make it more efficient from the original method where used Inv. for inverse operation, Mult. For multiplication operation, Add for addition operation and Sub for subtraction operation. In Table 4 it is done for testing of all the measurement of NIST tests between the proposed method and the original method.

We have programmed the two methods of the proposed and the original method on Core i3 computer with CPU 2.00GHz and RAM 4GB by using MATLAB R2018b (9.5.0.944444) 64-bit software to compute the running time for encryption and decryption of the messages with different sizes.

It is known that in the tests of NIST, the output values if it is a great than or equal (≥0.01) would be considered to be random and if it less than (<0.01) would be considered to be non-random. In our paper was put word "Success" for random and word "Failure" for non- random.

From Table 4, show that the Run test have been success for the original method and the proposed method, but in this test it we found that the proposed method has higher random than the original method and also at in (Random excursion variant test, Random excursion test, Non overlapping template matching test, Frequency (Monobit) test, Linear complexity test and Discrete Fourier transform test) all of them show that the proposed method have higher random than the original method. While, in the tests (Serial test, Overlapping template matching test, Maurer's universal statistical test, The longest run of ones in a block test, Frequency test within a Block test, Cumulative sums test, Approximate Entropy test and Binary Matrix Rank test) show the original method was a failure because all of tests for it have values less than (0.01) and at in the proposed method was success because values of it was great than (0.01).

Table 2: The time implementation in encryption and decryption for the proposed method and the original method

	The original method of MVECC		The proposed method	
Text characters	Encryption time/seconds	Decryption time/seconds	Encryption time/seconds	Decryption time/seconds
1000-bit	16.9303	4.2559	16.9943	5.2962
3000-bit	59.4118	15.246	59.5675	18.8306
5000-bit	85.1119	22.207	85.3577	26.5149

Table 3: The required operations for the proposed and the original methods

The original method of MVECC		The proposed method	
Encryption	Decryption	Encryption	Decryption
2Mult.	2Inv. + 2Mult.	6Mult.+ 4Add+4Sub	6Mult.+ 8Sub +2Inv.

Table 4: The randomness tests of NIST for testing a 1000-bit message for the proposed method and the original method

	Tests	The original method of MVECC	Results	The proposed method	Results
1	Run test	0.12510758813168163	Success	0.8839328393793418	Success
2	Serial test	0.0005123514118502457	Failure	0.17289182407808948	Success
3	Random excursion variant test	0.8551321405847059	Success	0.9211265554360596	Success
4	random excursion test	0.9991851051973619	Success	0.9995000204954214	Success
5	Overlapping template matching test	0.0016233947920264553	Failure	0.9063677327153351	Success
6	Non overlapping template matching test	0.24185444190641325	Success	0.4298705921548936	Success
7	Frequency (Monobit) test	0.011817618288016488	Success	0.17210447783471447	Success
8	Maurer's universal statistical test	8.07147831032501e -11	Failure	0.5135537962284511	Success
9	The longest run of ones in a block test	0.008274192337445328	Failure	0.3917392658576128	Success
10	Linear complexity test	0.016703740699514164	Success	0.9429964032844659	Success
11	Frequency test within a Block test	0.0012353209554503248	Failure	0.802503853550373	Success
12	Discrete fourier transform test	0.2641550563920085	Success	0.7822356899775442	Success
13	Cumulative sums test	0.006625202552503318	Failure	0.12937702786808813	Success
14	Approximate entropy test	0.004863219563516038	Failure	0.1870431824257016	Success
15	Binary matrix rank test	3.533009372110865e-08	Failure	0.990123117669481	Success

So, all tests in Table 4 show that the proposed method was success to had a higher random than the original method.

Robustness of Proposed Method

Assume that Eve is the attacker and she knowledgeable about the present algorithm. She can gain access and read the ciphertext $C = (c_1, c_2)$ and eB, the parameters that available to her is the elliptic curve over finite field F_p and abase point B and the public key of Bob Q_B, because these chosen in publicly. Eve can't arrives to the secret random number e for Alice and private key d for Bob and also she can't arrives to $BP = (x, y)$ and $t = (t_1, t_2) \in [0,1]$ mod p because this points chosen in secretly, only Alice and Bob knows them.

Therefore, she will have difficulty for breaking ciphertext $C = (c_1, c_2)$ because she can't get the following parameters $\{e, d, BP$ and $t\}$ and to computes and find the session keys (the keys who use to processing in the decryption to find the original message) using d or e and also BP and t (which are also has been consider as the keys) because these parameters are important for attacker to processing and find the original message. The parameters required to break the ciphertext are more than the original method.

Previously, in the original method of MVECC the parameters which can't get it was $\{e, d\}$. Therefore, the proposed method has more secure than the original method.

Finally, we can say that this proposed method showed an increase in the randomness of the output than in the original method due to the effect of $BP = (x, y)$ and $t = (t_1, t_2) \in [0,1]$ mod p on the encryption process and the processing technique which is used on it as shown the NIST measures in Table 4.

Analysis of the Proposed Method

The complexity of ECC (the difficulty of breaking it) is actually equivalent to solving the discrete logarithm problem. Finding the discrete logarithm of one element in EC does not help find the logarithm of any other element. Let $\#E$ denote order of E and let r be the largest prime factor $\#E$ of. Then the better known algorithms for finding discrete logarithms in E have complexity $0\left(\sqrt{r}/n\right)$, such that n is the number of processors working on the problem. Thus, the mathematical complexity which is based on the largest prime factor $\#E$ of and on the number of operations which are used during the processing of encryption and decryption (Al-Saffar *et al.*, 2013).

So, we will discuss analysis of the proposed method *according to the mathematical complexity* compared with the original method as follow.

The proposed method is more efficient than the original method of MVECC, because:

1) *In proposed method:* In the encryption scheme there are six multiplication operations $\{x(1\text{-}t_1)^2, 2k_1(1\text{-}t_1)t_1, M_1t_1^2, y(1\text{-}t_2)t_2$ and $M_2t_2^2\}$, four addition operations and four subtraction operations. While in decryption scheme there are needs to compute two inverse operations for $\{t_1^2$ and $t_2^1\}$ and six multiplication operations $\{x(1\text{-}t_1)^2, 2k_1(1\text{-}t_1)t_1, y(1\text{-}t_2)^2, [c_1\text{-}x(1\text{-}t_1)^2\text{-}2k_1(1\text{-}t_1)t_1](t_1^2)^{-1}$ and $[c_2\text{-}y(1\text{-}t_2)^2\text{-}2k_2(1\text{-}t_2)t_2](t_2^2)^{-1}\}$ eight subtraction operations
2) *In original method for MVECC:* In the encryption scheme there are two multiplication operations $\{m_1k_1$ and $m_2k_2\}$. While in the decryption scheme needs to compute two inverse operations for $\{k_1$ and $k_2\}$ and two multiplication operations $\{c_1k_1^{-1}$ and $c_2k_2^{-1}\}$

According the Time Implementation Between the Proposed and the Original Methods

It is known that cryptosystems often take a little different amounts of time to process different inputs, so we used different sizes bit of message and take same elliptic curve with prime number as in the example implementation in section 4 to compared between the proposed method and the original method with the time required to implement each process.

We note in the Table 2, that the proposed method is longer to decrypt than the original method, where the different was almost 1-4 sec. While in encryption the proposed method also longer to encrypt, the different was in the parts millisecond. Therefore, the different between them was very small.

Conclusion

In this paper we proposed a new technique to improve the Menezes-Vanstone Elliptic Curve Cryptosystem MVECC based on Quadratic Bezier Curve QBC to made it more secure and efficient, also used the ASCII value in this proposed to convert the text to numbers by taken every two characters in the message and separate them as a point and then convert into ASCII values. MVECC is a very important cryptosystem because of it the message not necessary be a point from the points on elliptic curve or the numbers of mathematical operations used it, so we were modified it using QBC equation and ASCII values. This proposed succeed to obtain a high level of security compared it with the original method of MVECC in all testing of the NIST according to the results in the Table 4. This modification improved the MVECC and make it has a higher level of security and the mathematical complexity of the proposed method is more efficient than the original method because it has more numbers of operations which

are used in encryption and decryption processes as shown in Table 3. Although the time implementation of the proposed method is slow compared to the original method as shown in Table 2, we have obtained much higher level security than the original method.

Acknowledgment

This paper was supported by the faculty of Computer Science and Mathematics, Department of Mathematics of University of Kufa, Iraq. We thank all reviewers for their great interest and deep reading on this paper.

Author's Contributions

Dua M. Ghadi: Introducing the algorithm, program the algorithm, studying related algorithm.

Adil AL-Rammahi: Writing the paper, depending the references, proofing the programs, proofing the algorithm.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Abdul Wahab, H.B. and T.A. Satter Jaber, 2016. Using chebyshev polynomial and quadratic bézier curve for secure information exchange.

Al-Saffar, N.F.H., M.D Said and M. Rushdan, 2013. On the mathematical complexity and the time implementation of proposed variants of elliptic curves cryptosystems. Int. J. Cryptol. Res., 4: 42-54.

Armstrong, J., 2005. Quadratic Bézier curve. TecNote TN-05-003.

El-Latif, A.A.A., X. Niu and N. Wang, 2011. Chaotic image encryption using Bézier curve in DCT domain scrambling. Proceedings of the International Conference on Digital Enterprise and Information Systems, (EIS' 11) Springer, Berlin, pp: 30-41. DOI: 10.1007/978-3-642-22603-8_3

Hankerson, D., A.J. Menezes and S. Vanstone, 2004. Guide to Elliptic Curve Cryptography. 1st Edn., Springer Science and Business Media, ISBN-10: 038795273X, pp: 312.

Joy Kenneth, I., 2000. Qudratic Bézier Curve. Visualization and Graphics Research Group Department of Computer Science University of California, Davis.

Kobliz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209. DOI: 10.1090/S0025-5718-1987-0866109-5

Marsh, D., 1999. Applied Geometry for Computer Graphics and CAD. 2nd Edn., Springer Undergraduate Mathematics Series, Springer, ISBN-10: 1852330805, pp: 288.

Menezes, A. and S. Vanstone, 1993. Elliptic curve cryptosystem and their implementation. J. Cryptography, 6: 209-224. DOI: 10.1007/BF00203817

Miller, V.S., 1986. Use of elliptic curves in cryptography. Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, (ACT' 86) Springer, Berlin, pp: 417-426. DOI: 10.1007/3-540-39799-X_31

Mogollon, M., 2007. Cryptography and security |services: Mechanisms and applications. University of Dallas, USA.

Paar, C. and J. Pelzl, 2010. Foreword by Bart Preneel. 1st Edn., Understanding Cryptography a Textbook for students and Parctitioners, Springer-Verlag.

Sadiq, A.T. and N.J. Kadhim, 2009. Enhanced menezes-vanstone elliptic curve cryptosystem. J. Al-Nahrain Univ., 12: 162-165. DOI: 10.22401/JNUS.12.1.23

Srividya, B.V. and S. Akhila, 2014. Novel cryptosystem based on Bézier curve using $GF(P^m)$. Proceedings of the International Conference on Circuits, Communication, Control and Computing, Nov. 21-22, IEEE Xplore Press, Bangalore, India. DOI: 10.1109/CIMCA.2014.7057811

Stallings, W., 2017. Cryptography and Network Security: Principles and Practices. 7th Edn., Pearson Education, ISBN-10: 0131873164, pp: 680.