A Novel Encryption System Based on PGP Using Elliptic Curve Cryptosystem and Bézier Curve for Secure Information Exchange

Dua Mohammed Ghadi
Wasit Education Directorate, Ministry of Education, Iraq.
Email: mdua1093@gmail.com

Abstract. This paper presents an approach to generating a secure ciphertext. Quadratic Bézier curve equation has been used in this paper to add more secure and complexity to elliptic curve cryptosystem. Proposed method using quadratic Bézier curve with ElGamal elliptic curve cryptosystem (ElGamal ECC). The idea of proposed method is encrypt the key that has been generated by public key in ElGamal elliptic curve cryptosystem by using quadratic Bézier curve equation based on PGP behavior. The proposed method have been more efficiency and complex. This method have been compared with different keys size to computing the randomness tests National Institute of Standards and Technology (NIST) and running time for the encryption and decryption process.

Keywords: Quadratic Bézier Curve, ElGamal Elliptic Curve Cryptosystem, Encryption, Decryption, PGP.

1. Introduction
At a time when the network is used to communicate between tens of millions of people and is being more widely used as a medium for trade, security has become a critical problem to address[1]. The protection of information is a never-ending problem. Preventing a leak of original text information became a challenging and necessary task as sensitive text content was spread over a long period of time to other people in ancient times. Several steganographic and encryption methods have been suggested to solve this problem[2]. Cryptography is a technicality of provides security to information. In cryptography all these information is offered in the encrypted form and only authorized receiver can decrypt it. The main goal of cryptography is to keep information confidentiality. The plaintext used in cryptography refers to the original message before encryption and it is a transmission in a form that is easily readable to anyone. Cipher text is an encrypted information, mean that the ciphertext is unreadable by users without the suitable encryption algorithm to decrypt it.
Elliptic curve cryptography (ECC) is one of the effective encryption algorithm which was used for first time by Neal Koblitz [3] and Victor Miller [4]. In the past few years, many researchers have developed some methods of cryptography especially in elliptic curves cryptography. In 2012, three methods of elliptic curve cryptographic was implemented, where this methods is never need to calculate the inverse operations, also never need to embed the message as points in the elliptic
curve[5]. Also, some of researchers used Bézier curve techniques to improve cryptosystems such as in 2014 used public key cryptography technique based on quartic Bézier curve over Galois field GF(p^n) to improve data security and reduces computational complexity [6]. In 2016, proposed protocol for exchange secret information based on PGP protocol behavior, combine between chaotic system technique (chebyshev polynomial) and secure curve concepts (quadratic Bézier curve)[7].

In this paper, The proposed method for keep message confidentiality when sending is discussed. In this research, we were able to change the key by encrypt it and by using PGP behavior nature and quadratic Bézier curve equation.

2. Quadratic Bézier Curve
The Bézier curve of degree is specified by a sequence of points which are called the control points[8]. Bézier curve is defined by its control points[9]. A degree n Bézier curve has n + 1 control points whose blending functions are denoted \( B_i^n(t) \);

\[
B_i^n(t) = \binom{n}{i}(1-t)^{n-i}t^i, \quad i = 0, 1, 2, ..., n
\]

Recall that

\[
\binom{n}{i} = \frac{n!}{i!(n-i)!}
\]

\( B_i^n(t) \) is also referred to as the \( i \)th Bernstein polynomial of degree \( n \). The equation of a Bézier curve is thus [8]:

\[
r(t) = \sum_{i=0}^{n} \binom{n}{i}(1-t)^{n-i}t^i P_i
\]

Then

\[
r(t) = \sum_{i=0}^{n} B_i^n(t) P_i, \quad 0 \leq t \leq 1.
\]

Quadratic Bezier curve has been described by three points \( P_0, P_1 \) and \( P_2 \). The first point \( P_0 \) and the third point \( P_2 \) are "anchors". The second point \( P_1 \) affect the shape of the curve. The generated curve starts at the first point \( P_0 \) going toward the second point \( P_1 \) and it settles at the third point \( P_2 \). Therefore, this curve does not pass through the second point \( P_1 \) [10]. We can derivative the quadratic Bézier curve equation with parameter \( t \), which it a number between in the interval [0,1] by the following[11]:

- \( P_1^{(1)} \) be a point on the piece \( \overline{P_0P_1} \) and defined by:
  \[
P_1^{(1)} = (1-t)P_0 + tP_1
  \]

Figure 1. representation of \( P_1^{(1)} \) point

- \( P_2^{(1)} \) be a point on the piece \( \overline{P_1P_2} \) and defined by
  \[
P_2^{(1)} = (1-t)P_1 + tP_2
  \]
Figure 2. representation of $P_2^{(1)}$ point.

- $P_2^{(2)}$ be a point on the piece $P_1^{(1)} P_2^{(1)}$ and defined by

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

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

- Define $r(t) = P_2^{(2)}$

All of these points $P_1^{(1)}$, $P_2^{(1)}$ and $P_2^{(2)}$ are a function of the parameter $t$ and $P_2^{(2)}$ can be equated with $r(t)$ 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 $r(t)$ become the equation of Bézier curve:

$$r(t) = P_2^{(2)}(t)$$

$$= (1 - t)P_1^{(1)}(t) + t P_2^{(1)}(t)$$

Since $P_1^{(1)}(t) = (1 - t)P_0 + t P_1$ and $P_2^{(1)}(t) = (1 - t)P_1 + t P_2$

Then

$$r(t) = (1 - t) [(1 - t)P_0 + t P_1] + t [(1 - t)P_1 + t P_2]$$

$$= (1 - t)^2 P_0 + (1 - t)t P_1 + (1 - t)t P_1 + t^2 P_2$$

$$= (1 - t)^2 P_0 + 2(1 - t)t P_1 + t^2 P_2$$  \hspace{1cm} (4)

Where (4) is quadratic polynomial (Quadratic Bézier Curve equation).

So, let $(x(t_2), y(t_2))$ is a parametric form of quadratic Bézier curve $r(t)$ with the points $P_0 = (x_1, y_3), P_1 = (x_2, y_2)$ and $P_3 = (x_3, y_3)$

Where

$$x(t_1) = (1 - t_1)^2 x_1 + 2t_1(1 - t_1)x_2 + t_1^2 x_3$$  \hspace{1cm} (5)

$$y(t_2) = (1 - t_2)^2 y_1 + 2t_2(1 - t_2)y_2 + t_2^2 y_3$$  \hspace{1cm} (6)
such that $t_1, t_2 \in [0,1]$. 

![Quadratic Bézier Curve](image)

Figure 4. Quadratic Bézier Curve

### 3. Elliptic Curves (EC) over Prime field $F_p$

An elliptic curve $E$ over $F_p$ is defined by an equation [12]:

$$E: y^2 = x^3 + ax + b \mod p \quad (7)$$

Let $p$ be an odd prime ($p > 2,3$), then $a$ and $b$ satisfy the condition $(4a^3 + 27b^2 \neq 0) \mod p$ in $F_p$, and every point $P = (x_p, y_p)$ on $E$ (otherwise the point $O$) in $F_p$.

#### 3.1. Operations on Elliptic Curve over Prime Field $F_p$

The arithmetic operation which are using during in elliptic curve schemes are [13]:

- **Point Addition**
  
  Given two points on $E$ defined the equation (2), the coordinates of them are $P = (x_p, y_p)$ and $Q = (x_Q, y_Q)$ such that $P \neq -Q$. Then, the sum $R = P + Q = (x_R, y_R)$ is:

  \[
  \begin{align*}
  \lambda &= \frac{y_q - y_p}{x_q - x_p} \\
  x_R &= \left(\lambda^2 - x_p - x_q\right) \mod p \\
  y_R &= \left[\lambda(x_p - x_R) - y_p\right] \mod p
  \end{align*}
  \quad (8) (9) (10)
  \]

- **Point Doubling**
  
  Let $P = (x_p, y_p)$ be a point on $E$. Adding the point $P$ to itself to obtain another point:

  $P + P = 2P = R \quad (11)$

  Where

  \[
  \begin{align*}
  \lambda &= \frac{3x_p^2 + a}{2y_p} \\
  x_R &= \left(\lambda^2 - 2x_p\right) \mod p \\
  y_R &= \left[\lambda(x_p - x_R) - y_p\right] \mod p
  \end{align*}
  \quad (12) (13) (14)
  \]

- **Multiplication**
  
  Let $k$ is a positive integer and $P = (x, y)$ is a point belong to $E$. So, defined as repeated addition as follows:

  \[
  kP = P + P + \cdots + P
  \]

  $k$-times \quad (15)
3.2. Elliptic Curve Discrete Logarithm Problem (ECDLP)

A point \( B \in E(F) \) of order \( n \), and a point \( Q \) on \( E(F) \) is the multiple of \( B \), and determined to find the integer \( \alpha \in \mathbb{Z}_n \) such that \( Q = \alpha B \).

In ECC schemes, the parameters \( E, F, B \) are chosen in public and \( n \) calculated. Then, the user choose a random integer \( \alpha \) from \( [1,n-1] \) and computes \( Q = \alpha B \). The user's public key is \( Q \), while the user's private key is \( \alpha \). Clearly, if the ECDLP is easy, then an attacker can deduce \( \alpha \) from \( Q \). Thus, the difficulty of solving the ECDLP is very important for the security of all elliptic curve schemes[14].

4. ElGamal Elliptic Curve Cryptosystem

In this cryptosystem [15], the elliptic curve \( E \) over finite prime field \( F_p \), and let base point \( B \in E(F_p) \) are public. Bob chooses a secret random private integer \( d \) and computes his public key \( Q_B = dB \).

Alice wants to send the message point \( M \) to Bob, she chooses a secret random positive integer \( e \) and computes by Bob's public key \( eQ_B = QA \) and then she computes to encrypt her message:

\[ C = M + QA \text{ (where } C \text{ is cipher text).} \]

Alice sends \( \{C, eB\} \) to Bob. Bob will then use his private key \( d \) to compute \( d(eB) = QA \), Bob computes to decrypt ciphertext by:

\[ M = C - QA. \]

5. Proposed Framework

In this section, we were able to encrypt the key based on PGP behavior nature and quadratic Bézier curve equation. This proposal aim to increase the security features by adding a new hybrid process it between quadratic Bézier curve and points of EC to make the hybrid key points (encrypted key).

Usually in this method, the secret message point \( M \) must be point related to points of EC and then the agreement between the Sender (Alice) and the receiver (Bob). Alice generates the secret key (master key \( QA \)) by public key's Bob \( (Q_B) \), and in this stage, a new secret key produces (session key \( QA \)) based on master key \( (QA) \) and that key using to encrypt message. Alice before send the encrypted message (ciphertext), encrypts the master key \( QA \) based on quadratic Bézier curve equation. The Receiver (Bob) when he received the ciphertext and encrypted key, decrypts the secret key using the quadratic Bézier curve equation and then decrypts the ciphertext using \( QA \) for obtain the original message.

A new method to create the session key based on master key. Alice converts by using MATLAB programming the master key \( QA \) to binary bits, and then convert it into decimal and multiplied this decimal with the master key itself, to produce the point that called the session key.

5.1. Proposed Algorithm

The full encryption and decryption process of the proposed method is explained in algorithm by the following:

**Step.1** The Agreement Process Between the Sender and Receiver Stage
1. Publicly on an elliptic curve over finite field \( E(F_p) \).
2. Publicly on a base point \( B \in E(F_p) \).
3. Secretly on secret control points of Bézier \( BP_1 = (x_1,y_1), BP_2 = (x_2,y_2) \) and \( t = (t_1,t_2) \in [0,1] \), and they compute \( t \) by: \( t = (t_1,t_2) \in [0,1] mod p \).

**Step.2** Key Generation Stage
1. The receiver chooses random integer \( d \).
2. Calculate the public key \( Q_B \) based on integer \( d \): \( dB = Q_B \). Then keep \( d \) secret.
3. The sender chooses random integer \( e \) as a secret.
4. Calculate the master key \( QA \) secret key by using \( e \) and \( Q_B \) as follow:

\[ eQ_B = QA = (x_3,y_3) \text{ point on } E(F_p). \]
5. Convert by using MATLAB programming the master key \( QA \) to binary bits \( (Bin.) \) and then to decimal \( (Dec.) \), then compute \( n = (Dec.) mod p \).
6. Calculate the session key \( QA \) by using \( n \) and \( QA: nQA = QA \).
Step.3 Encryption Stage
1. Select the message point $M$ related to $E(P_a)$.
2. Encrypt the message point $M$ based on session key $Q_a$ by: $C = M + Q_a$. $C$ is ciphertext.
3. Encrypt the master key $Q_A = (x_3, y_3)$ using $BP_1 = (x_1, y_1), BP_2 = (x_2, y_2)$ and $t = (t_1, t_2) \in [0,1] \mod p$. by:
   $$k_1 = x_1(1 - t_1)^2 + 2x_2(1 - t_1)t_1 + x_3t_1^2 \mod p$$
   $$k_2 = y_1(1 - t_2)^2 + 2y_2(1 - t_2)t_2 + y_3t_2^2 \mod p$$
   $K = (k_1, k_2)$ is ciphertext.
4. Send $\{C, K\}$ to the receiver side.

Step.4 Decryption Stage
1. Receive $\{C, K\}$ from the sender side.
2. Find the master key $Q_A$ by decrypt $K = (k_1, k_2)$ using $BP_1 = (x_1, y_1), BP_2 = (x_2, y_2)$ and $t = (t_1, t_2) \in [0,1] \mod p$.
   $$x_3 = [k_1 - x_3(1 - t_1)^2 - 2x_2(1 - t_1)t_1].(t_1^2)^{-1} \mod p$$
   $$y_3 = [k_2 - y_3(1 - t_2)^2 - 2y_2(1 - t_2)t_2].(t_2^2)^{-1} \mod p$$
   $Q_A = (x_3, y_3)$ is master key.
3. Convert by using MATLAB programming the master key $Q_A$ to binary bits (Bin.) and then to decimal(Dec.), then compute $n = (Dec.) \mod p$.
4. Calculate the session key $Q_a$ by using $n$ and $Q_A : n Q_A = Q_a$.
5. Decrypt the ciphertext $C$ based on session key $Q_a$: $M = C - Q_a$.
6. Obtain the message $M$.

5.2 Implementation of Proposed Framework
This section introduced the evaluation of our proposed work. The evaluation was performed to display that the proposed method provides high level of security, which makes it suitable for secure data. The proposed method stages implement by the example below:

Step.1 The Agreement Stage Between Alice and Bob
1. Alice and Bob Publicly agree on an elliptic curve $E$ over $F_{141}$ and $B = (2, 12) \in E$.
   $$E: y^2 = x^3 + 3x + 7 \mod 41,$$ where $a = 3, b = 7, p = 41$ satisfy the condition
   $$[4a^3 + 27b^2] \mod 41 = [4(3^3) + 27(7^2)] \mod 41 = 37 \neq 0.$$ The points of ($E(F_{141})$) are:
   $$(2, 12), (2, 29), (3, 17), (3, 24), (4, 1), (4, 40), (6, 6), (6, 35), (7, 17), (7, 24), (8, 16), (8, 25), (9, 5), (9, 36), (11, 10), (11, 31), (12, 7), (12, 34), (14, 13), (14, 28), (16, 16), (16, 25), (17, 16), (17, 25), (20, 20), (20, 21), (22, 15), (22, 26), (23, 5), (23, 26), (24, 2), (24, 39), (25, 2), (25, 39), (26, 20), (26, 21), (27, 3), (27, 38), (30, 18), (30, 23), (31, 17), (31, 24), (33, 2), (33, 39), (36, 20), (36, 21).
2. Alice and Bob Secretly agree on Bézier points $BP_1 = (3, 5), BP_2 = (6, 9)$ and $t = (0.5, 0.7) \in [0,1] \mod 41$, and they compute:
   $$t = (0.5, 0.7) \in [0,1] \mod 41$$
   $$t = (5 * 10^{-1}, 7 * 10^{-1}) \mod 41$$
   $$t = (5 * 37, 7 * 37) \mod 41$$
   $$t = (21, 13).$$

Step.2 Key Generation Stage
1. Bob chooses a random integer $d = 20$ as a private key, and then computes the public key: $Q_B = dB = 20(2, 12) = (31, 17)$, and keep $d$ secret.
2. Alice chooses a random integer \( e = 24 \) as a secret key, and uses Bob's public key to compute the master key: \( Q_A = eQ_B = 24(31, 17) = (7, 17) \).

3. Alice converts using MATLAB programming the master key \( Q_A = (7, 17) \) to binary bits: \( Q_A = 11110001 \), and then converts it to decimal \( \text{Dec.} = 241 \), and computes

\[
\begin{align*}
  n &= \text{Dec.} \mod p \\
  n &= 241 \mod 41 = 36.
\end{align*}
\]

4. Calculate the session key \( Q_a \) by: \( Q_a = n Q_A = 36(7, 17) = (16, 25) \).

**Step.3** Encryption Stage (Alice)

1. Chooses a message point \( M = (20, 20) \).

2. Encrypts the message \( M \) and based on session key \( Q_a \) by compute:

\[
C = M + Q_a = (20, 20) + (16, 25) = (4, 1).
\]

3. Encrypts the master key \( Q_A = (7, 17) \) using \( BP_1 = (3, 5) \), \( BP_2 = (6, 9) \) and \( t = (21, 13) \) by:

\[
\begin{align*}
  k_1 &= x_1(1-t_1)^2 + 2x_2(1-t_1)t_1 + x_3 t_1^2 \mod p \\
  &= 3(1-21)^2 + 2(6)(1-21)(21) + (7)(21^2) \mod 41 \\
  &= -753 \mod 41 = 26. \\
  k_2 &= y_1(1-t_2)^2 + 2y_2(1-t_2)t_2 + y_3 t_2^2 \mod p \\
  &= 5(1-13)^2 + 2(9)(1-13)(13) + (17)(13^2) \mod 41 \\
  &= 785 \mod 41 = 6.
\end{align*}
\]

\( K = (26, 6) \) is a hybrid key.

4. Sends \( \{C, K\} \) to Bob.

**Step.4** Decryption Stage (Bob)

1. Receives \( \{C, K\} \).

2. Decrypts \( K = (26, 6) \) using \( BP_1 = (3, 5) \), \( BP_2 = (6, 9) \) and \( t = (21, 13) \) by computes to find the master key \( Q_A \):

\[
\begin{align*}
  x_3 &= [k_1 - x_1(1-t_1)^2 - 2x_2(1-t_1)t_1].(t_1^2)^{-1} \mod p \\
  &= [26 - 3(1-21)^2 - 2(6)(1-21)(21)].(21^2)^{-1} \mod 41 \\
  &= (3866)(4) \mod 41 = 7 \\
  y_3 &= [k_2 - y_1(1-t_2)^2 - 2y_2(1-t_2)t_2].(t_2^2)^{-1} \mod p \\
  &= [6 - 5(1-13)^2 - 2(9)(1-13)(13)].(13^2)^{-1} \mod 41 \\
  &= (2094)(33) \mod 41 = 17
\end{align*}
\]

\( Q_A = (7, 17) \) is the master key.

3. Converts using MATLAB programming the master key \( Q_A = (7, 17) \) to binary bits:

\( Q_A = 11110001 \), and then converts it to decimal \( \text{Dec.} = 241 \), and compute

\[
\begin{align*}
  n &= \text{Dec.} \mod p \\
  n &= 241 \mod 41 = 36.
\end{align*}
\]

4. Calculate the session key \( Q_a \) by: \( Q_a = n Q_A = 36(7, 17) = (16, 25) \).

5. Decrypts the ciphertext \( C = (4, 1) \) to find the message point \( M \) by compute:

\[
\begin{align*}
  M &= C - Q_a \\
  &= (4, 1) - (16, 25) \\
  &= (4, 1) + (16, -25 \mod 41) \\
  &= (4, 1) + (16, 16) \\
  &= (20, 20).
\end{align*}
\]

6. **Experimental Results for Proposed Framework**

The proposed framework is implemented on a 2.00 GHz CPU and 4 GB RAM Core i3 computer using MATLAB R2018b (9.5.0.944444) 64-bit program to verify its performance with current key agreement protocols. To calculate the level of security that is guaranteed by the proposed cryptosystem, the time of encryption and decryption for the master key of this proposed method is...
analyzed. As we know, the more time it takes to encrypt and decrypt, the stronger the cryptosystem's security. As the suggested approach implements by control points (Bézier points) and uses the quadratic Bézier curve equation at both encryption and decryption process stages, it provides additional user data security and protects users from various types of network threats. The results are calculated using NIST[16] with Random Numbers Analyser application to prove the randomness and the security of this method.

The proposed method with quadratic Bézier curve equation has been used for different cipher keys sizes (130-bit and 250-bit) and ciphertext between original method and proposed method for (1000-bit) during tests. The results were calculated via the Frequency test, frequency within a block test, runs test, serial test and approximate entropy.

![Figure 5](image1.png)  ![Figure 6](image2.png)

**Figure 5.** The randomness for different keys size in proposed method.  **Figure 6.** The randomness test for original method and proposed method.

In the Table.1, the results were measured by a timing process within the MATLAB program itself. Each test was conducted for many times and the results have been averaged. The proposed method has been applied for same keys sizes that used in randomness tests (130-bit and 250-bit) during encryption and decryption processes.

| Key size | Encryption time in second | Decryption time in second | Total time |
|----------|---------------------------|---------------------------|------------|
| 130-bit  | 0.0067161                 | 0.0086863                 | 0.0154024  |
| 250-bit  | 0.0130829                 | 0.0088987                 | 0.0219816  |

For analysis of the proposed method according to the mathematical complexity, in encryption process there are six multiplication operations \{ x_1(1 - t_1)^2, 2x_2(1 - t_1)t_1, x_3t_2^2, y_1(1 - t_2)^2, 2y_2(1 - t_2)t_2, x_3t_2^2 \}, four addition operations and four subtraction operation. While in decryption process there is a need to compute two inverse operations for \{ (t_1^2)^{-1} \text{ and } (t_2^2)^{-1} \} and six multiplication operations \{ x_1(1 - t_1)^2, 2x_2(1 - t_1)t_1, [k_1 - x_1(1 - t_1)^2 - 2x_2(1 - t_1)t_1], (t_1^2)^{-1}, y_1(1 - t_2)^2, 2y_2(1 - t_2)t_2 \text{ and } [k_2 - y_1(1 - t_2)^2 - 2y_2(1 - t_2)t_2], (t_2^2)^{-1} \} eight subtraction operations.

7. **Conclusion**

Dependent on the modified key and quadratic Bézier curve equation, this paper introduces the strengthening of the ElGamal elliptic curve cryptosystem. In order to achieve stronger cryptography requirements, the transmission key (master key) of the proposed system is encrypted based on quadratic Bézier curve equation. According to the randomness tests for the proposed method, the
proposed method for master key encryption and ciphertext appears to be successful in the tests as seen in Figure 5 and Figure 6. The proposed method succeeded in increasing the security features of the session key in encrypting and decrypting the message point as seen in these tests, as well as the mathematical complexity of this method in the encryption and decryption stage.

References
[1] Fairouz Mushtaq Sher Ali, 2014 Combination of Classical Cipher with Stream Cipher for Improving Data Security. Al-Qadisiyah Journal of Pure Science. Vol.(19) No. 3, pp. 190-197.
[2] Mohaimen Hassan and Alaa Kadhim, 2020 New Image Encryption Based on Pixel Mixing and Generating Chaos System. Al-Qadisiyah Journal of Pure Science Vol.(25) Issue (4), pp. 1-14.
[3] N. Koblitz, 1987 Elliptic curve cryptosystems. Mathematics of Computation 48(1987): 203-209.
[4] V.S. Miller, 1986 Use of elliptic curves in cryptography. Advanced in Cryptology. Proceedings of Crypto85. Lecture note in Computer Science. v. 218, pp. 417-426.
[5] M.S. Ali, 2012 Elliptic curves cryptographic techniques. Proceeding of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS’2012). IEEE.
[6] B.V.Srividya, S. Akhila, 2014 Novel cryptosystem based on Bezier curve using GF(Pm). International Conference on Circuits. Communication. Control and Computing. IEEE.
[7] Hala Bahjet Abdul Wahab, Tanya Abdul Satter Jaber, 2016 Using Chebyshev Polynomial and Quadratic Bézier Curve for Secure Information Exchange. Engineering and Technology Journal. No.5, pp.:666-674.
[8] Duncan Marsh, 1999 Applied Geometry for Computer Graphics and CAD. Second edition. Springer Undergraduate Mathematics Series.
[9] Iulian Nicolae Carpatorea, 2012 A Graphical Traffic Scenario editing and evaluation software. Master thesis. School of Information Science. Computer and Electrical Engineering Halmstad University. Halmstad. Sweden.
[10] Armstrong, Jim. 2005 Quadratic Bézier curve. TecNote TN-05-003.
[11] Kenneth I. Joy, 2000 QUADRATIC BÉZIER CURVE. Visualization and Graphics Research Group Department of Computer Science University of California. Davis.
[12] Manul Mogollon, 2007 Cryptography and security Services: Mechanisms and Applications. University of Dallas. USA.
[13] William Stallings, 2017 Cryptography and Network Security: Principles and Practices. Seven Edition. Pearson Education.
[14] Alfred Menezes, 2001 Evaluation of Security Level of Cryptography: The Elliptic Curve Discrete Logarithm Problem (ECDLP). University of Waterloo.
[15] Song Y. Yan, 2002 Number Theory for Computing. Second Edition. Springer. Berlin.
[16] Rukhim A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., et al. 2010 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application. In NIST Special Publication 800-22: Revision 1a, Lawrence E. Bassham III. NIST: Gaithersburg. MD. USA.