DOI: 10.24996/ijs.2018.59.1A.20

ISSN: 0067-2904

A Secure Enhancement for Encoding/ Decoding data using Elliptic Curve Cryptography

Kawther E. Abdullah*, Nada Hussein M. Ali

Department of Computer Science, College of science, University of Baghdad, Baghdad, Iraq.

Abstract

The Elliptic Curve Cryptography (ECC) algorithm meets the requirements for multimedia encryption since the encipher operation of the ECC algorithm is applied at points only and that offer significant computational advantages. The encoding/decoding operations for converting the text message into points on the curve and vice versa are not always considered a simple process. In this paper, a new mapping method has been investigated for converting the text message into a point on the curve or point to a text message in an efficient and secure manner; it depends on the repeated values in $x-$ coordinate to establish a lookup table for encoding/decoding operations. The proposed method for mapping process is composed of various operations; firstly, the Exclusive OR and Circular Shift are performed on the message to enhance the diffusion property and that lead increasing the strength against cryptanalysis attack. Secondly, both parties agree on domain parameters for creating the elliptic curve and the mechanism to build the lookup table for encoding/decoding process. Thirdly, the base point is selected for generating all (x, y) pair points of the elliptic curve and extract x – coordinate values to calculate the maximum value for x and its frequency to create the lookup table. Finally, applying encoding/decoding operation for the message. The results of the proposed method are considered more efficient, secure and less time consuming compared with the ECC algorithm, besides it's suitable for preserving the confidentiality for real-time applications.

Keywords: Encryption; Decryption; Elliptic Curve Cryptography (ECC); Encoding; Decoding; Real Time Application; Voice over Internet Protocol (VOIP).

تعزيز آمن الترميز/ فك ترميز البيانات باستخدام تشفير المنحني الاهليجي

كوثر عيسى عبد الله *، ندى حسين محمد علي

قسم علوم الحاسوب، كلية العلوم، جامعة بغداد، بغداد العراق.

الخلاصة

ان خوارزمية تشفير المنحنى الإهليجي (ECC) تفي بمتطلبات تشفير الوسائط المتعددة وذلك لان تطبيق عملية التشفير لخوارزمية المنحنى الاهليجي تطبق على نقاط المنحنى فقط وهذا يقدم مزايا حسابية كبيرة .ان عمليات الترميز / فك الترميز لتحويل الرسالة النصية إلى نقاط على المنحنى والعكس بالعكس لا تعتبر دائما عملية بسيطة. في هذا البحث، تم التقصي عن طريقة جديدة لتحويل الرسالة النصية إلى نقطة على المنحنى

*Email: kawther9093@gmail.com

أو نقطة إلى رسالة نصية بطريقة فعالة وآمنة؛ حيث ان هذه الطريقة تعتمد على القيم المتكررة على المحور x– لإنشاء جدول البحث لعمليات الترميز / فك الترميز.تتألف المنهجية المقترحة لعملية التحويل من عدة عمليات؛ الخطوة الاولى وقبل إنشاء جدول البحث لتعزيز عملية (diffusion) للرسالة يتم تنفيذ (Exclusive OR and Circular Shift) لزيادة القوة ضد هجوم (تحليل الشفرات). ثانيا، يتفق الطرفان على معلمات المجال للمنحنى الإهليجي الذي تم اختياره من قبلهما وايضاً على آلية بناء جدول البحث. وثالثا، فإن النقطة الأساسية ستولد جميع نقاط الزوجx, y للمنحنى الإهليلجي، ثم تستخرج قيم الاحداثي x لحساب القيمة القصوى ل x وتكرارها لإنشاء جدول البحث. وأخيراً، تطبق عملية الترميز / فك ترميز للرسالة. نتيجة الطريقة المقترحة هي أكثر كفاءة وأمان وأقل استهلاكا للوقت، كما انها مناسبة للحفاظ على السرية التطبيقات في الوقت الحقيقي.

1. Introduction

Many applications such as e-mail, e-banking machines, e-commerce and others are vulnerable to spy, thus the demand for information security is increased to protect the data transmission over the internet. Besides, the security issue is important for digital multimedia transferring over public networks and the storing of data on diverse platforms (cloud server, hard-drive, etc.). The voice calls over the Internet are exposed for eavesdropping in contrast to traditional calls. The essential affair of protection for confidentiality, integrity, and authenticity (CIA) is the main concern for the data exchanging between unknown parties. Therefore, the growing need for the protection of multimedia content to prevent fraud and to ensure privacy which can be achieved through cryptography[1,2,3].

Voice over IP technology has been widely spread over the predominant Internet due to the advanced technologies of digital voice communication protocols and wired/wireless networks. VoIP offer advantages than the traditional Public Switched Telephone Network (PSTN). Voice communications are exposed to eavesdrop threats and protect the secrecy of information from these risks are essential and protect it without any effected in the quality of voice [4,5].

The layout of this paper is composed of the following sections: the related work of elliptic curve cryptography is introduced in section 2, section 3 describes the concept of the elliptic curve cryptosystem, section 4 discusses the proposed methodology followed by the experimental results and discussion in section 5, finally, section 6 presents the conclusions.

2. Related Work

In the literature, numerous researchers have attempted to utilize the strength of the elliptic curve to implement in different tasks of public key cryptography. This section summarizes some the features of the linked work.

In 2013 Ali Soleymani, et al. Studied a novel public key image encryption based on elliptic curves over prime group field. This research introduced a new technique for mapping pixel values to EC (Elliptic Curve) coordinates and then applying encryption/decryption algorithm on image based on ECC over the prime field (F_P) [6].

In 2014 Rahul Singh, et al. Investigated an implementation of elliptic curve cryptography for audio based application. In this paper, an implementation for ECC encryption and decryption audio file was presented [7].

In 2015 Santoshi Pote. Proposed the enhancing the security of koblitz’s method using transposition techniques for elliptic curve cryptography. This paper presented a new technique to enhance the koblitz method for encoding/decoding a message before encryption/decryption in ECC by adding "Simple Columnar Transposition Technique with multiple rounds" to produce complex cipher text and then encoding/decoding cipher text using koblitz method [8].

3. Elliptic Curves Cryptography

The Elliptic curves were suggested by Neal Koblitz and Victor Miller independently in 1985 to design a public-key cryptographic system. Since then a spate of research has been published on the security and implementation of elliptic curve efficiently in cryptography. In the late 1990’s, elliptic curve systems began receiving commercial admission when commission standards organizations specified elliptic curve protocols, and private companies comprised these protocols in their security products [9].

These days, it is fundamentally used in the resource-constrained environments, like wireless sensor networks and mobile networks, etc. There is a tendency to replace other public key cryptosystems with Elliptic Curve Cryptography systems when comparing with RSA (Rivest, Shamir, Adleman) it provides the same security level with the small key size and also less overhead process contrary with other asymmetric algorithms[10,11].

3.1 Elliptic Curves Arithmetic

ECC is a public key cryptography based on an Abelian group; the two main operations used in ECC are addition and multiplication and are performed over an elliptic curve itself. The multiplication is a repeated of addition operation, for example, $a \times k = (a + a + \cdots + a)$ which represent the addition of a with k times. Cryptanalysis search for determining k given a; $(a \times k)$ and this is called a discrete logarithm problem. The definition of elliptic curve is based on equation, two variables and two coefficients, the values of variables and coefficients are limited to elements of a finite field. There are two main types of finite fields: prime field (F_P) and binary field$(F2^n)$,in this paper the elliptic curve over the prime field (F_P) is considered [12].

3.1.1 Elliptic Curves over the Prime Field

In general, an elliptic curve E over prime field (F_P) denoted by E(F_P) and given by simplified the Weierstrass equation as follows[12]:

$$\boldsymbol{y^2 \bmod p = (x^3 + ax + b) \bmod p} \qquad (1)$$

depend on condition shown in Equation 2, where Δ denoted to the discriminant of E.

$$\Delta = (\boldsymbol{4a^3} + \boldsymbol{27b^2})\boldsymbol{mod\ p} \neq \boldsymbol{0} \qquad (2)$$

The set of points on the elliptic curve over prime field are denoted by $E_P\ (a, b)$ which satisfy Equation 1, additionally the point at infinity or zero point denoted by(O). Using different values of coefficients (a, b) will produce a different set of points $E\ (a, b)$ and consequently various curves. The creation of an elliptic curve needs to generate a group of points; these points depend on choosing the prime number p and value of coefficients (a, b) that satisfy Equation 2, while choosing the pair of points(x, y) must satisfy Equation 1. The basic two operations are addition; denoted by $+$; and doubling describes as follows[9,12]:

- **Addition Point:** if two points on an elliptic curve were added to each other, the output result represents a third point denotes the intersection of that curve. Graphically, drawing a straight line between any two points on the curve represents a tangent line and reflect the third point around the $x - axis$ as denoted in Equation 5. The formula $P + Q = -R$ represents the addition operation between points P(x,y) with Q(x,y) to produce R(x,y). Equations 3 and 4 demonstrate the aforementioned process.
- **Doubling point:** the output value of adding a point P(x,y) on the curve to itself in condition that $y_P \neq 0$ will yield the point R. One could draw a tangent line where the intersection of that line on the curve represents the cross reflection point on $x - axis$ (the R point), where $+P = 2P = -R$. Equations 3, 4, 5 and 6 are used to compute the tangent line (slope) respectively

$$\boldsymbol{x_R = (\lambda^2 - x_P - x_Q)\ mod\ P} \qquad (3)$$

$$\boldsymbol{y_R = (\lambda(x_P - x_R) - y_Q)\ mod\ P} \qquad (4)$$

$$= \begin{cases} \left(\dfrac{y_Q - y_P}{x_Q - x_P}\right) \boldsymbol{mod\ P} & \boldsymbol{if\ \ P \neq Q} \qquad (5) \\ \left(\dfrac{3x_P^2 + a}{2y_P}\right) \boldsymbol{mod\ P} & \boldsymbol{if\ P = Q} \qquad (6) \end{cases}$$

Applying Equation1 used coefficients (a,b) and the values of x, y in the range $[0, \ldots, p - 1]$ will generate a set of points on the curve called a group of points $E_P\ (a, b)$. Selecting a base point (generator point) from the group $E_P\ (a, b)$ will produce a sub group or generates all points on the curve called cyclic group. The same operations (doubling operation, addition operation) are performed on ECC for creating the aforementioned cyclic group [9].

3.2 Elliptic Curve Encryption/Decryption

The encryption/decryption process in ECC is applied to points not on the message, hence, the first step is to convert a plain text message ***m*** into a point P(x,y) on the curve to produce $\boldsymbol{P_m}$. This process called Encoding, and then the encryption process is implemented to produce a cipher point $\boldsymbol{C_m}$. Thereafter applying the decryption process for the cipher point $\boldsymbol{C_m}$ to get the plain point $\boldsymbol{P_m}$, and then decode the point $\boldsymbol{P_m}$ to retrieve the plaintext message ***m***. The Encryption/Decryption processes between two parties (Alice/Bob) using the ECC algorithm is described as in follow [12]:

- Alice and Bob agree upon the domain parameters; prime number P, a, b, and a base point (G); of the elliptic curve.
- Alice and Bob select private keys N_a, N_b respectively, the value of the private key is less than the order (number of points that generated from the base point) in the range [1 - order].
- Calculate the public keys P_a, P_b for Alice and Bob respectively from multiplying their private keys with the base point as below:

$$P_a = N_a \times G \mod P \quad (7)$$

$$P_b = N_b \times G \mod P \quad (8)$$

- The procedure for sending encrypted message from Alice to Bob is firstly encode the massage m into point P_m . Secondly, select k randomly in the range [1 - order] to make as a mask to multiply with G and P_b, then encrypt P_m with Bob public key's as in 9.

$$C_m = \{kG, P_m + kP_b\} \quad (9)$$

- Bob decrypts the received point C_m by multiplying the first point of C_m with his private key N_b and then subtracted from the second point.

$$P_m = P_m + k\times P_b - N_b \times k\times G \quad (10)$$

For analysis this as below:

$$P_m + k\times P_b - N_b \times k\times G$$

$$P_m + k\times(N_b \times G) - N_b \times k\times G = P_m$$

Finally, decoding P_m to obtain the message.

4. The Proposed Method

A new mapping method is proposed based on x -coordinate values of an elliptic curve to generate a secret lookup table, this table used to convert samples of an audio file into points on the elliptic curve and vice versa. The x –coordinate has chosen due to the repeated values of x, where each value of x is producing two values of y in the elliptic curve equation (Weierstrass equation). The proposed method requires both the sender and receiver know the following steps:

Step 1: Both parties agree on the domain parameters of an elliptic curve (a, b, prime number, base point) to plot a special elliptic curve for them.

Step 2: The values of x –coordinate are computed from the base point and then do the following:

- Find a larger value in the x – coordinate to build a frequency table.
- Compute the frequency distribution for each value of x and save it in the above table. The indexes of this table represent the values of x, while its contents are the x frequent occurrences. The table size depends on the larger value for x as explained before.
- Create a lookup table; which is also called a secret lookup table; based on the frequency distribution of x – coordinate and it is composed of two columns. The first column represents the x values depends on the frequencies of x – coordinate and must be greater than zero, this operation is repeated for 255 values and without any duplication for x – coordinate. The second column represents y values that are generated from the base point through comparison between values of x in the first column with the value of x that generated from the base point, the comparison will retrieve a value of y in the second column of the lookup table. This process will continue until filled the second column with 256 values of y. In decoding, the inverse lookup table contains just one column represents the values of x, this column is same as the first column in the encoding lookup table. Besides, it depends only on x values for the sampling of an audio file data and could be shared between the two parties in the connection process. Figure-1 illustrates the above operations.

Step 3: the build of the secret lookup table is simplified the encoding and decoding operations for both parties. At the sender side, the encoding operation is implemented by converting the data samples of audio file into points on the elliptic curve; while in the receiver side, the decoding process is applied converting these points into samples.

Step 4: A necessary process is made before encoding and decoding operations:

- In cryptography, there are two important operations (confusion and diffusion) to make the cipher more secure against attacks. Confusion represents the relation between cipher-text and key as complex as possible and diffusion refers to the relation between cipher-text and plain text. This relation must be complex to block the cryptanalysis (that based on statistical analysis). This complexity is generally implemented through of substitutions and permutations. In this work, ***XOR*** and ***Circular Rotation*** bitwise operations are applied to achieve diffusion. Moreover, these operations are efficient to perform and less time consuming, also it provides more security against statistical analysis. These advantages are obtained by removing the characteristics that exploit by an intruder such as repeated plain text values. The following steps demonstrate the above process:

❖ Select a random number IV and applied the ***XOR*** between the first sample of an audio file, the result is then ***XOR*** with a next sample until the end of the file.

❖ The Right Circular Rotation ***(RCR)*** process is implemented in ***WavFile***. The amount of rotation is determined randomly and denoted by ***Rlen***. Each sample in the audio file is shifted with different ***Rlen***. The Pseudo-code of ***RCR*** is shown as below:

```
a. For loop i=0,1,2,…, WavFile   then
b. Rlen = Rlen + i mod 8
c. If (Rlen = 0)
d.  Rlen =3
e. afterRCR(i)=( WavFile (i)<< Rlen )& 255 | WavFile (i) >> 8
f. End of loop
```

On the receiver side, the decoding operation is implemented an inverse lookup table (contains only the values of x) as mentioned in step2. Extract the x – coordinate values only from the receiving points to restore audio sample values correspond to them from the inverse lookup table, the index of each x value will be the real data of sending an audio file. Thereafter, applying Left Circular Rotation ***LCR*** and ***XOR***. The aforementioned procedures are demonstrated in Figures-(2, 3). Algorithms 1 and 2 demonstrate the creation of the lookup table and the encoding method for the proposed algorithm respectively. Algorithm 3 demonstrates the decoding operation.

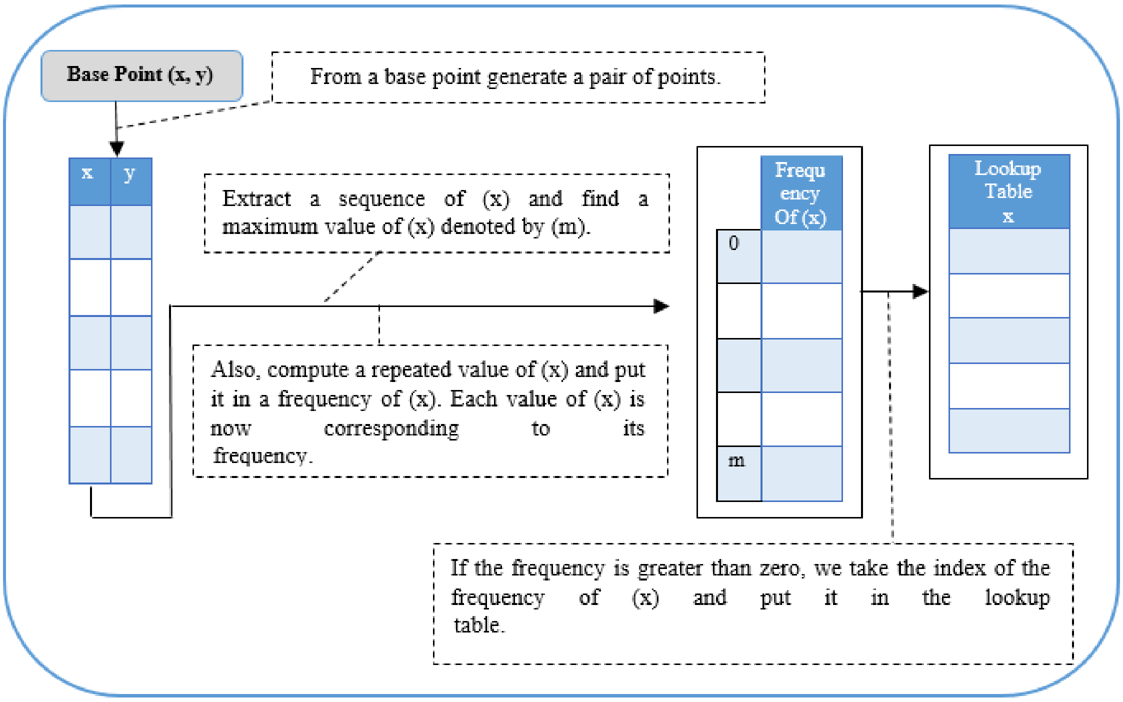

Base Point (x, y)
From a base point generate a pair of points.
x
y
Extract a sequence of (x) and find a maximum value of (x) denoted by (m).
Also, compute a repeated value of (x) and put it in a frequency of (x). Each value of (x) is now corresponding to its frequency.
Frequency Of (x)
0
m
Lookup Table x
If the frequency is greater than zero, we take the index of the frequency of (x) and put it in the lookup table.

Figure 1- Lookup Table initialization with values of x depends on the frequency of x – coordinate.

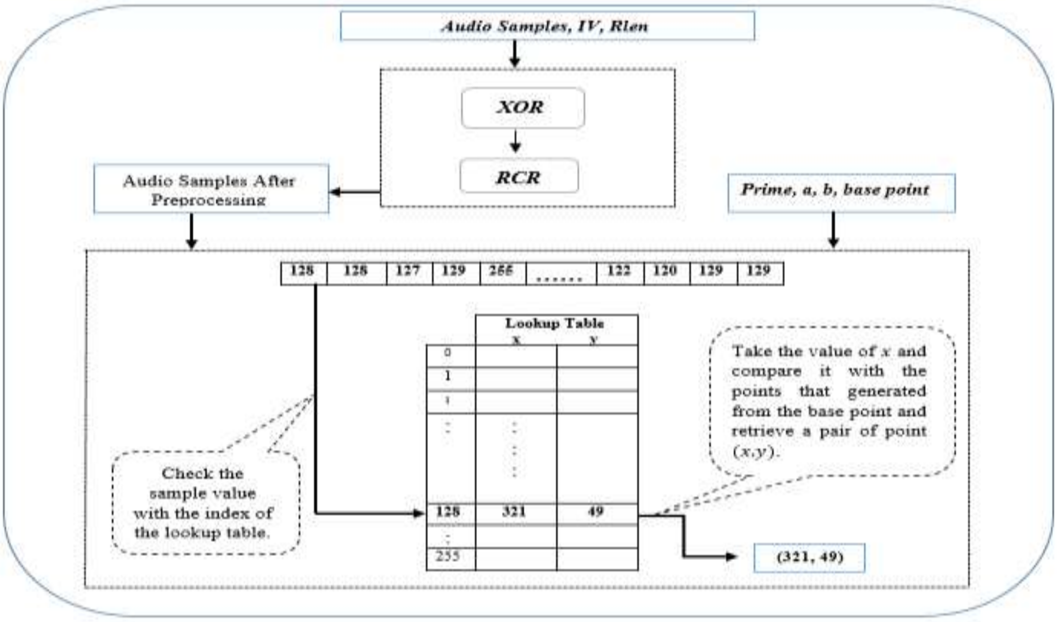

Audio Samples, IV, Rlen
XOR
RCR
Audio Samples After Preprocessing
Prime, a, b, base point
128
128
127
129
255
....
122
120
129
129
Lookup Table
x
y
0
1
128
321
49
255
Check the sample value with the index of the lookup table.
Take the value of x and compare it with the points that generated from the base point and retrieve a pair of point (x,y).
(321, 49)

Figure 2-The proposed method for encoding

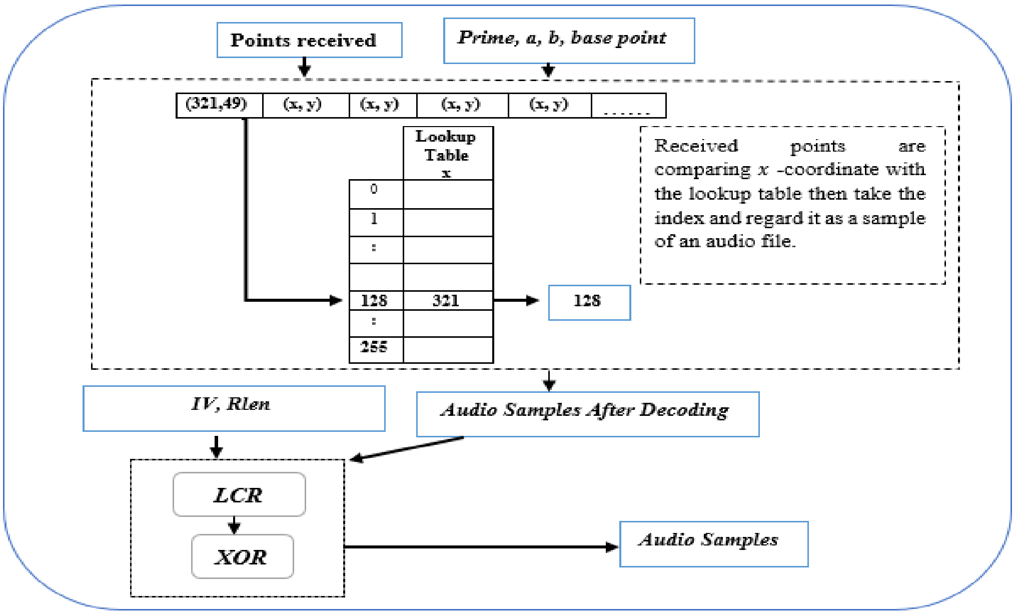

Points received
Prime, a, b, base point
(321,49)
(x, y)
(x, y)
(x, y)
(x, y)
......
Lookup Table
x
0
1
128
321
255
128
Received points are comparing x -coordinate with the lookup table then take the index and regard it as a sample of an audio file.
IV, Rlen
Audio Samples After Decoding
LCR
XOR
Audio Samples

Figure 3- The proposed method for decoding

Algorithm1: Create The Lookup Table

Input: P, a, b, G ∈ $\boldsymbol{E(F_P)}$
Output: Tbl ()

```
Step1: From the base point (G) generates the sequence of x and y coordinates.
Seqx(), Seqy()     //  Integer lists have stored the values of x and y from G respectively.
Step2: Find a maximum value of x-coordinate
    Set Max ← 0                         // Initialize a maximum value of x-coordinate.
    For I=1 to N                        // N is the number of points from the base point.
       If (Max < Seqx(I)) then
          Max=Seqx(I)
    EndFor
Step3: Determine the Frequency of x-coordinate
    Freq(Max)                    // Create an integer array to store the frequency of x-coordinate.
    For I=0 to N
        J=Seqx(I):   Freq(J)=Freq(J)+1
    EndFor
Step4: Establish the lookup table
     Tbl(255,2)                  //An integer 2 dimension array for representing the lookup table.
   Set K ← -1
    For I=0 to Max
       If (Feq(I) > 0) then
           K=K+1:   Tbl(K,0) = I
           If (Tbl(K,0) = Seqx() )
                  Tbl(K,1) = Seqy()
          If (K=255) then
              I ← Max              //Break.
      EndIf
    EndFor
End;
```

Algorithm2: The Proposed Method For Encoding

Input: wavfile (), Tbl (255,2).
Output: X (), Y().

```
Step1: Read an audio file and Store the data of the audio file (samples) in a byte array wavfile().
Step2: Convert the data of audio (Samples) into points on the curve.
X (), Y ()          // Integer arrays to store the Points.
For I=0 to Length of wavefile ()
    For J=0 to Length of Tbl (,)/2
       If (wavfile(I) = J) then
              X(I)= Tbl(J,0)    // Convert samples into points on the curve.
              Y(I)= Tbl(J,1)
               break
         EndIf
     EndFor
 EndFor
End;
```

Algorithm3: The Proposed Method For Decoding

Input: X (), Y ().
Output: wavfile()

```
Step1: Initialization the lookup table with value of x-coordinate depend on frequency of x-coordinate.
        Tbl (255)       // one-dimension array for representing lookup table.
Step2: Convert the points into samples.
   wavfile ()              // The samples are stored in a byte array.
  For I=0 to Length of X ()
     For J=0 to Length of Tbl ()
        If (X (I) = Tbl (J)) then
            wavfile(I)=J          //Convert points into samples.
             Break
          EndIf
     EndFor
EndFor
End;
```

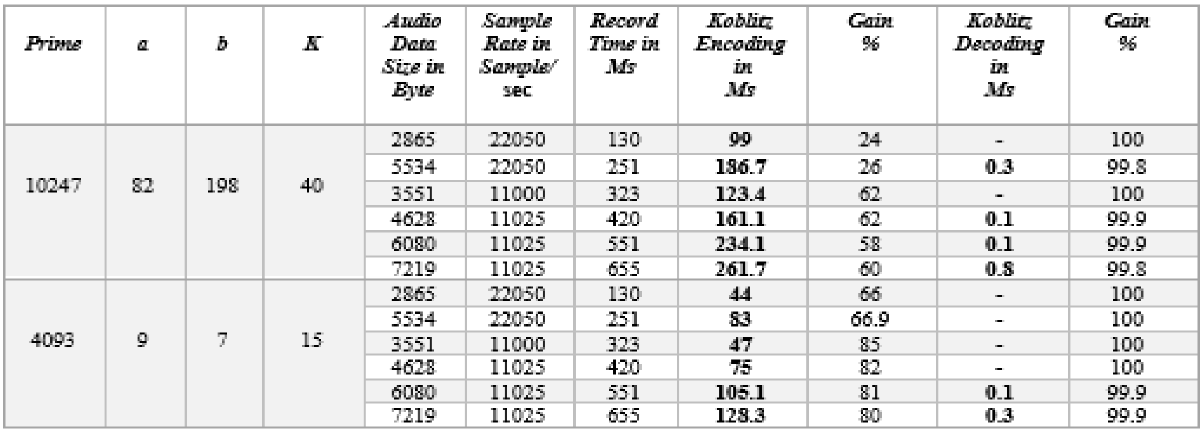
5. Experimental Result and Discussion

The proposed method was programmed in a C# language in Visual Studio 2010 on Fujitsu laptop with system configuration of i5 processor @ 2.50 GHz and 4 GB Ram on Windows 10 platform. Different audio size files are used to implement the proposed method, the obtained results are compared with Koblitz method for both the processing time and gain factors. Tables-(1, 2) are showing CPU processing times for the proposed and Koblitz methods respectively when applying on various audio data size and different elliptic curve. Table-3 illustrates the Time execution of the ECC algorithm in the encryption/decryption process.

Table 1- Time execution in millisecond for the proposed method.

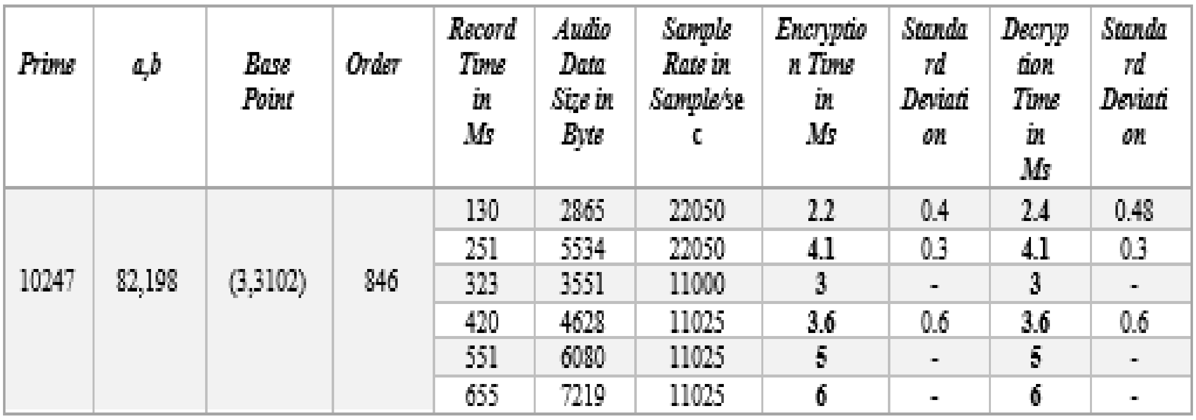
Prime	***a***	***b***	***Base Point***	***Order***	***Audio Data Size in Byte***	***Sample Rate in Sample /sec***	***Record Time in Ms***	***The proposed Encoding Time in Ms***	***Gain %***	***The proposed Decoding Time in Ms***	***Gain %***
10247	82	198	(3,3102)	846	2865	22050	130	**7**	95	**4.2**	97
					5534	22050	251	**13.7**	95	**8.1**	97
					3551	11000	323	**8.9**	97	**5.1**	98
					4628	11025	420	**11**	97	**7**	98
					6080	11025	551	**15**	97	**9.1**	98
					7219	11025	655	**17.7**	97	**11**	98
4093	9	7	(4,1110)	4093	2865	22050	130	**7**	95	**4.6**	96
					5534	22050	251	**13.6**	95	**8**	97
					3551	11000	323	**9**	97	**5.3**	98
					4628	11025	420	**11.1**	97	**7.2**	98
					6080	11025	551	**15**	97	**9**	98
					7219	11025	655	**17.7**	97	**11.1**	98

Table 2-Time execution in millisecond for the koblitz method.



Prime	***a***	***b***	***K***	***Audio Data Size in Byte***	***Sample Rate in Sample/ sec***	***Record Time in Ms***	***Koblitz Encoding in Ms***	***Gain %***	***Koblitz Decoding in Ms***	***Gain %***
10247	82	198	40	2865	22050	130	**99**	24	-	100
				5534	22050	251	**186.7**	26	**0.3**	99.8
				3551	11000	323	**123.4**	62	-	100
				4628	11025	420	**161.1**	62	**0.1**	99.9
				6080	11025	551	**234.1**	58	**0.1**	99.9
				7219	11025	655	**261.7**	60	**0.8**	99.8
4093	9	7	15	2865	22050	130	**44**	66	-	100
				5534	22050	251	**83**	66.9	-	100
				3551	11000	323	**47**	85	-	100
				4628	11025	420	**75**	82	-	100
				6080	11025	551	**105.1**	81	**0.1**	99.9
				7219	11025	655	**128.3**	80	**0.3**	99.9

Table 3-Time execution in millisecond for the encryption/decryption in ECC.



Prime	*a,b*	*Base Point*	*Order*	*Record Time in Ms*	*Audio Data Size in Byte*	*Sample Rate in Sample/sec*	*Encryption Time in Ms*	*Standard Deviation*	*Decryption Time in Ms*	*Standard Deviation*
10247	82,198	(3,3102)	846	130	2865	22050	2.2	0.4	2.4	0.48
				251	5534	22050	4.1	0.3	4.1	0.3
				323	3551	11000	3	-	3	-
				420	4628	11025	**3.6**	0.6	**3.6**	0.6
				551	6080	11025	**5**	-	**5**	-
				655	7219	11025	**6**	-	**6**	-

The encoding time in the proposed method is considered better compared to the **traditional** Koblitz method, but in the decoding operation the opposite is true. The **traditional** Koblitz method is a probabilistic method and a chance of failure depends on the selection of (K) value which is a random positive integer. The k value must be restricted for condition ($message \times K + K < prime$) and the failure rate is $1/2^K$. It's the easiest way, but less effective in the terms of the security[8,14,15]. Also, it is not suitable for any elliptic curve, for example, the curve $p = 1471,\ a = 2598, b = 1435,$ and maximum value of a message $m = 255,$ the possible value of K must be equal to 5, because $m \times K + K < p$. Hence, the probability ratio will be very small and cannot convert some a message into a point on the curve. Regardless of this curve and the probability ratio, this method contains an error ratio and may not encode some portions of the message because it depends on the probability value K. If a failure occurs, it tries another value. The **traditional** Koblitz method is not efficient for the voice transmission VOIP because the synchronization between the encoder and the decoder is not achieved and the time in the encoder is very large, in addition; it is considered one of the probabilistic methods. On the contrary, one can notice that the performance of the proposed method is suitable for the voice over the communication channel, since the time for the encoder and decoder is very good to synchronization and it is less time-consuming to protect the voice communication. Besides, the proposed method is more secure than the **traditional** Koblitz method, since each party agree on the secret lookup table in advanced and the initialization for this table is not arbitrary but dependent on the mechanism (repeated values of x-coordinate).

Table 4- Measure the Entopy of audio files before and after encryption.

		Entropy Before Encryption		**Entropy After Encryption**	
Audio Data Size in Byte	***Sample Rate in Sample/*****sec**	**1st Order Entropy**	**2nd Order Entropy**	**1st Order Entropy**	**2nd Order Entropy**
2865	22050	5.3005829912142	10.5816488283889	**7.92681087503784**	**15.8058888645756**
5534	22050	6.82787504145131	13.4415579166002	**7.96467734261951**	**15.9047085795039**
3551	11000	6.98368961202054	13.7953287670421	**7.94735830883732**	**15.853979035215**
4628	11025	6.01897599933256	11.8729075782361	**7.931405529137**	**15.8013499652364**
6080	11025	5.84580134983713	11.5089648086005	**7.87531162376325**	**15.6287578573589**
7219	11025	6.10301754906002	12.1833572710927	**7.96178241171649**	**15.9012812715187**

5.1. Security Analysis

5.1.1. Entropy Analysis: Shannon Entropy (1st Entropy and 2nd Entropy) is used to measure the secrecy of information (Randomness) after the encryption process as defined in Equations 11 and 12 as below [13]:

$$1st\ Entropy\ =\ -\sum P\ (i)\ log\ (P\ (i)) \qquad (11)$$

$$\text{2nd Entropy}\ =\ -\sum\sum \text{P (i, j) log (P (i, j))} \qquad (12)$$

Where

$P(i)$= Histogram(i) / no. of audio samples (13)

The entropy analysis illustrated in Table-4. A good cipher audio has an entropy value equal to 8 in 1st entropy and 16 in 2nd entropy.

5.1.2. Key Sensitivity: Any simple change in the key yields another different result in recovering plain audio file from a cipher audio. Figure-4 shows the encrypted audio file and the related decryption files with right and wrong keys respectively.

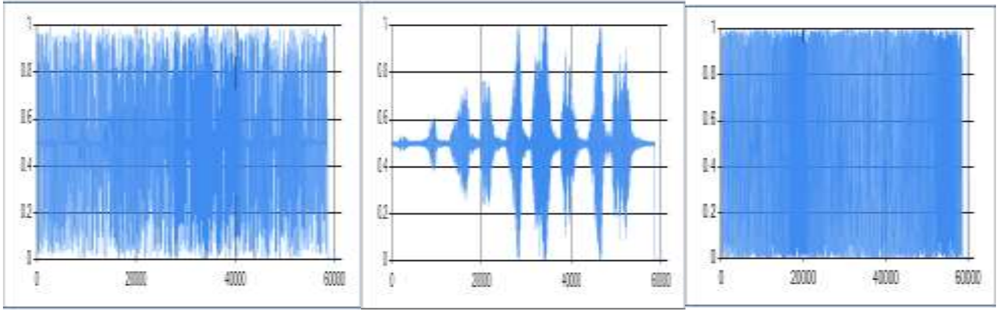


Figure 4- (a) Cipher audio; (b) Decrypted with correct key N_b;(c) Decrypted with key as N_b-1.

5.1.3. Known Plaintext Attack: even the intruder recognizes the algorithm and some pairs of plaintext-ciphertext samples, then he cannot obtain the plain audio file. The main factor for this isusing the random factor (k) which acts as a mask and it is changing every execution of the algorithm and produced various ciphers samples in each run. Also, XOR and Circular Rotation have been applied before the encryption process, this will lead to the reduce the correlation between the samples of the audio file. This approach helps to avoid known plaintext attack.

6. Conclusion

In this paper, a new technique has investigated to convert samples of an audio into points on the curve, besides changing the form of samples before applying the proposed method to make cryptanalysis more difficult to guess the points on the curve by an intruder (through exploiting statistical analysis) to achieve diffusion. The obtained results indicate that the proposed method is faster, more secure and less time-consuming when embedding a message into a point on the curve. In addition, it is concluded that the proposed method is suitable for real-time applications that need protection when transferring them over the public network.

References

1. Tawalbeh, L. and Mowafi, M. and Aljoby, W. **2013.** Use of elliptic curve cryptography for multimedia encryption. *In Institution of Engineering and Technology (IET) Information Security*, **7**(2): 67-74. doi: 10.1049/iet-ifs.2012.0147
2. Kamalakannan, V. and Tamilselvan, S. **2015.** Security enhancement of text message based on matrix approach using elliptical curve cryptosystem. *Procedia Materials Science,* **10**: 489-496, Elsevier.
3. Kumar, M. and Iqbal, A. and Kumar, P. **2016.** A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography. *Signal Processing*, **125**: 187-202, Elsevier. doi: 10.1016/j.sigpro.2016.01.017
4. Wang, C. and Liu,Y. **2011.** A dependable privacy protection for end-to-end VoIP via Elliptic-Curve Diffie-Hellman and dynamic key changes. *Journal of Network and Computer Applications*, **34**(5): 1545-1556, Elsevier.
5. Alshakhsi, S. and Hasbullah, H. **2012.** Studying the effect of transmission rate and packet size parameters on VoIP performance. *Computer & Information Science (ICCIS), 2012 International Conference*, **2**: 814-819, IEEE.
6. Soleymani, A. and Nordin, M. and Ali, Z. **2013.** A Novel Public Key Image Encryption Based on Elliptic Curves over Prime Group Field. *Journal of Image and Graphics*, **1**(1): 43–49.
7. Singh, R. and Chauhan, R. and Gunjan, V. and Singh, P. **2014.** Implementation of Elliptic Curve Cryptography for Audio Based Application. *International Journal of Engineering Research & Technology (IJERT)*, **3**(1): 2210-2214.
8. Pote, S. **2015.** Enhancing The Security of Koblitz's Method Using Transposition Techniques For Elliptic Curve Cryptography. *International Journal of Research in Engineering & Advanced Technology*, **12**(6): 158-172.
9. Hankerson, D. and Menezes, A. and Vanstone, S. **2006.** *Guide to elliptic curve cryptography*. New York. Springer Science & Business Media. E-book.
10. Liu, F. *A Tutorial on Elliptic Curve Cryptography (ECC).* Available on: http://www.academia.edu/10735665/A_Tutorial_on_Elliptic_Curve_Cryptography_ECC_A_Tutorial_on_Elliptic_Curve_Cryptography_2.
11. Sagheer, A. **2012.** Elliptic curves cryptographic techniques. *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference*, pp:1-7, IEEE.
12. William Stallings. **2014.** *Cryptography and Network Security Principles and Practice.* Sixth Edition. United States of America. Pearson Education, Inc. E-book.
13. Payingat, J. and Pattathil, D. **2015.** Pseudorandom bit sequence generator for stream cipher based on elliptic curves. *Mathematical Problems in Engineering,*2015, Hindawi. doi: 10.1155/2015/257904
14. Reyad, O. and Kotulski, Z. **2015.** Image Encryption Using Koblitz's Encoding and New Mapping Method Based on Elliptic Curve Random Number Generator. In: Dziech, A. Leszczuk, M. Baran, R. (eds). *Multimedia Communications, Services and Security*. First Edition. Switzerland: Springer, Cham, 34-45.
15. Padma, B. and Chandravathi, D. and Roja, P. **2010.** Encoding and decoding of a message in the implementation of Elliptic Curve cryptography using Koblitz's method. *International Journal on Computer Science and Engineering*, **2**(5): 1904-1907.