MMVECC Encryption Algorithm for Redundancy Problem Solving and Authentication Verification

Mostafa Ahmed Mohamed Sayed and Liu Rongke

***Abstract*—Based on Elliptic Curve Discrete Logarithm Problem (DLP), Elliptic Curve Cryptography (ECC) shows promise in the public key cryptography methods. In this article, a new algorithm based on ECC is introduced, which has lower complexity than Menezes-Vanstone algorithm. Meanwhile our method introduces "one-time pad" to increase the security, and solve data redundancy encryption problem while at the same time maintains the authenticity of the transmitted message, which cannot be fabricated by the eavesdropper and cannot be denied by the legal transmitter. The simulations result shows that the redundancy problem is totally solved, and the correctness of the algorithm is verified through an example. A comparisons and resistance to different attacks are included also in the essay.**

***Index Terms*—ECC, mvecc, ElGamal, one-time pad, Menezes-vanstone cryptosystem.**

I. Introduction

Information security is crucial in various communication systems. However, with the existence of the eavesdropper/attacker, the message transmitted in the channel is not always safe and it needs to be secured. Cryptography is invented to keep the secret message away from illegal receivers, making the message of the authenticated transmitter non-forgery and undeniable. There are two categories of cryptography: the public-key cryptography and the symmetric-key cryptography.

In the symmetric-key cryptography systems, such as AES, the transmitter and the receiver share the same private key. The secret transmission of the private key is difficult to be managed. In the public-key cryptography system, the identity between private key of the transmitter and the receiver is not necessary. Instead, each side owns a pair of keys, namely, the public key and the private key. The public key is generated by the private key and shared in the channel. Alice uses the private key of her own and the public key of Bob to encrypt the message, and Bob decrypts the message with his private key and the public key of Alice. Without prior knowledge of private key, it is not practical for the eavesdropper to decrypt the message, for that reason the system is called computationally secure system.

The first public key cryptography is RSA, introduced by Rivest in 1977 [1], based on the hardness of integer factorization problem. However, RSA is usually combined with secure socket layer protocol (SSL), which may slows down the web servers for 3-9 times [2].

Elliptic Curve Cryptography is first introduced by Miller [3] and Koblitz [4], based on the Discrete Logarithm Problem [5]. With short-length key, ECC can achieve the same security as RSA [1], [6] In hardware implementation, ECC algorithm has smaller capacity, faster computation and less power consumption [7], which will bring benefit in wireless communications and portable devices [8].

Boruah proposed ElGamal ECC implementation [9] and refined algorithm based on Menezes Vanstone ECC is proposed by Kurt [10], [11] The FPGA implementation of ECC is introduced in [12]-[14]. In order to increase the security level and achieve perfect secrecy, a different key has to be used with each message as told by Shannon, so that using of one time pad algorithms raises the security level from computationally secure to unconditionally secured systems.

In this paper, the mathematical model of several previous works are examined and evaluated. Based on the previous work, a new ECC algorithm is proposed. The proposed Modified Menezes-Vanstone ECC (MMVECC) algorithm is one time pad algorithm that is used to heal many problems such as allowing rapid key change without need of key management complexity, and it solves the redundancy problem based on using one time pad technique.

The complexity for calculating the modular inverse of the curve parameter is reduced by XOR operation substitution. Meanwhile the "one-time pad" is kept along with the constant part of the public key at Alice's side to ensure the authenticity, making Eve's fabricated massage distinguishable and Alice message undeniable.

The paper is organized as follows, section II drive the problem formulation through describing previous methods that are used and it also describe development and contributions that are introduced and shows how far it fulfills and solve some related security issues, while section III shows the proposed solution to the problems in section II. In section III, the proposed model based on Menezes-Vanstone algorithm will be clarified by mathematical model and flowchart diagram, and it will be verified through an example. In Section IV, results of our proposed method will be presented and Section V will draw a conclusion to the paper.

II. Problem Formulation and Related Work

In order to highlight the proposed contribution the theoretical background, previous contributions, and problems have to be presented in this section. The main challenge in public key filed of research embodies in complexity reduction represented in the number of multiplications in

Manuscript received March 3, 2017; revised April 13, 2017.

Mostafa Ahmed Mohamed Sayed and Liu Rongke are with School of Electronic and Information Engineering, Beihang University (BUAA), Beijing, China,(e-mail: mostafa_adawy@ymail.com, rongke_liu@buaa.edu.cn).

DOI: 10.7763/IJMO.2017.V7.569

RSA or number of additions on the curve in ECC.

There is other kind of complexity, which is the computational complexity resulted from key management, where this kind of complexity limits the number of key exchange. Although reducing the number of exchanging keys is actually reducing the computational complexity, it resulted in redundancy problems caused by using constant keys for encrypting repeated input data. In this section the complexity problems and redundancy problems are discussed and in order to represent it the scenario of public key encryption is represented as in next paragraphs.

In the public key cryptography, Alice and Bob possess a pair of keys, respectively. The private key is owned by the master exclusively (P_a symbolizes the private key of Alice and P_b symbolizes the private key of Bob) and the public key is exchanged in the channel (Q_a symbolizes the private key of Alice and Q_b symbolizes the public key of Bob), which is known by both sides of the communicator as well as the potential illegal eavesdropper. In the Elliptic Curve Cryptography, the public keys are derived from the attached private keys and the base point (denote as B) on the elliptic curve, the algorithm for the public key is

$$Q_a = P_a \cdot B \qquad (1)$$

$$Q_b = P_b \cdot B \qquad (2)$$

At the transmitter, the message is encrypted by the point multiplication result of Alice's secret key Pa and Bob's public key Q_b, which are points on elliptic curve $y^2 = x^3 + a.x + b$. At the receiver, the message is decrypted by the point multiplication result of Alice's public key Q_a and Bob's private key P_b . Since that

$$Q_a \cdot P_a = P_b \cdot B \cdot P_a = P_b \cdot (B \cdot P_a) = Q_a \cdot P_b \qquad (3)$$

Bob can decode the message without knowing prior knowledge of Alice's private key. Meanwhile the illegal eavesdropper Eve possesses neither of the private keys; she is unable to decrypt the message only with the public keys, due to the hardness to solve Discrete Logarithm Problem.

ElGamal [15] introduced the first Public-key encryption based ECC. In the following text, $\{j_{1i}\}$ denotes the public key for the i^{th} session and $\{j_{2i}\}$ denotes the encrypted message for the i^{th} session, then

$$j_{1i} = Q_{ai} \qquad (4)$$

$$j_{2i} = M + Q_b \cdot P_{ai} \qquad (5)$$

M denotes the unencrypted message. In (4) and (5), j_{1i} ,$j_{2i}$are points on the elliptic curve $y^2 = x^3 + a.x + b$. The above method is not universal since the horizontal ordinate of the unencrypted message, X_M, is coordinated by the transmission message. In correspondence, the vertical ordinate of unencrypted message, Y_M, is defined by

$$y = \sqrt{x^3 + a \cdot x + b}\; mod\ P \qquad (6)$$

In (6) P is the Galois Field parameter. Since $\sqrt{x^3 + a \cdot x + b}$ maybe not an integer, Y_M is not constantly exist in the Galois Field. In this case, the message point M in (5) cannot be established. Another problem of ElGamal's algorithm lies in its low efficiency. In the following text, X_{J_1} and Y_{J_1} denotes the horizontal ordinate and the vertical ordinate of J_{1i} in (4), while X_{J_2} and Y_{J_2}denotes the horizontal ordinate and the vertical ordinate of J_{2i} in (5), respectively. In the 160 bit ECC system, X_{J_1}, Y_{J_1}, X_{J_2}, Y_{J_2} are 160-bit binary arrays, among them only X_{J_2}possesses useful message, while $X_{J_1}$is used for transmitting the public key of the i^{th} session and Y_{J_1}, Y_{J_2} is entirely dependent to X_{J_1},X_{J_2}, which can be presented as shown in next equation, and the efficiency of the ElGamal algorithm is at most1/4.

$$H\left(Y_{J_1},\ Y_{J_2} \middle| X_{J_1}, X_{J_2} \right) = 0 \qquad (7)$$

One modification of ElGamal's algorithm [16] aims to solve the problem that the unencrypted message point $M(X_M,Y_M)$ cannot be projected to the elliptic curve. In the modification, the message is transferred to blocks of 8-bit arrays by American Standard Code for Information Interchange (ASCII) or four bits by hexadecimal message [17].

Then, the blocks will be point-multiplied by the base point B on the elliptic curve, generating the points M' on the curve. Then the message points undergo the following calculation:

$$j_{2i} = \acute{M} + Q_b \cdot P_{ai} \qquad (8)$$

However, although the modification projects the binary message to the elliptic curve, it increases sharply the decryption complexity of the legal receiver. Since $\acute{M} = M \cdot B$, Bob faces the discrete logarithm problem to decrypt M from M' and B, and the only way to finish the task is to try the possible M one by one, from 0~255. Meanwhile, the modification lowers the transmission efficiency, and is not very useful in application.

Menezes-Vanstone comes up with a more available modification based on ElGamal model [18]. X_c and Y_c denotes the horizontal ordinate and vertical ordinate of $P_{ai} \cdot Q_b$, respectively. And $\{M_1, M_2\}$ are message sequences. As shown in Fig 1, where it represents the encryption and decryption data flow between Alice and Bob. Menezes-Vanstone applies X_c and Y_c to encrypt the message M_1, M_2, respectively, and the output stream for i the session at Alice is

$$J_{1i} = Q_{ai} \qquad (9)$$

$$J_{2i} = M_1 \cdot X_c mod\ P \qquad (10)$$

$$J_{3i} = M_2 \cdot Y_c mod\ P \qquad (11)$$

After receiving $\{J_{1i}, J_{2i}, J_{3i}\}$ Bob recovers X_c and Y_c from$P_b.Q_{ai}$, and extract original message $\{M_1, M_2\}$ by the steps in (12) and (13):

$$M_1 = J_{2i} \cdot X_c^{-1} mod \qquad (12)$$

$$M_2 = J_{3i} \cdot Y_c^{-1} mod\ P \qquad (13)$$

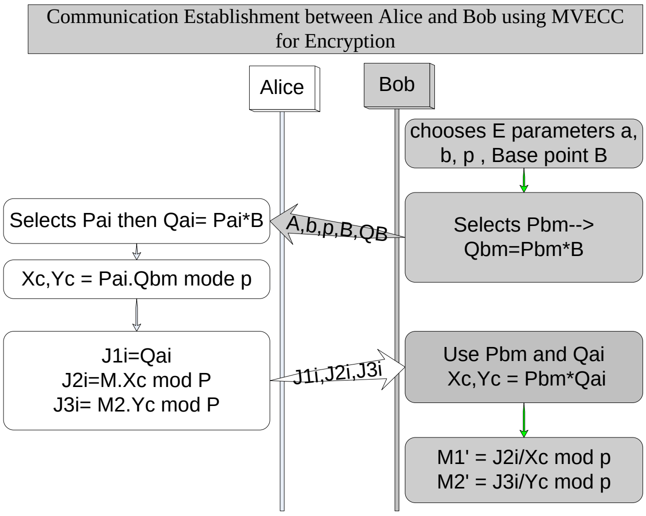

Fig. 1. Data Flow protocol using Menezes Encryption Scheme

Menezes-Vanstone algorithm calculates the modular inverse X_c^{-1} and Y_c^{-1}. In hardware implementation costs time and reduces throughput. Although there are many modifications that are used to reduce this complexity through converting division and multiplications operation into addition and subtraction operation as discussed in [18], where the author in this paper uses (14) and (15) instead of (12) and (13).

$$M_1 = J_{2i} - X_C - Y_C mod\ P \tag{14}$$

$$M_2 = J_{3i} - J_{2i} mod\ P \tag{15}$$

The problem of using such simple operation is its vulnerability to be detected where half of data M_2 can be discovered very easily by just subtracting J_{3i} fromJ_{2i}, where J_{3i}, J_{2i}, P are publicly transmitted. Recently Al-Saffar algorithm presented many solutions that can be used to reduce the reciprocal or division operation, but it still based on other complex operation like multiplication [19].

In the above-mentioned algorithms, the public key is changing very session rather than every block. In other to further increase security and to achieve “one-time pad”, the private and public key of Alice needs to change for every block. However, if ElGamal or Menezes-Vanstone algorithm is directly applied for “one-time pad” without strong key exchange technique, authenticity of Alice will be vulnerable. In that case Eve may pretend to be Alice and send fabricated message to cheat Bob.

In the same time, Alice may deny the message she has sent without authentic signature, where every key change in previous algorithms needs key management before it to insure the identity of the transmitter the problem that makes it very difficult to change the key rapidly. Although slow key change rate can partially reduce the computational complexity needed to manage the key change, but it can be resulted in a kind of security weakness especially in case of redundant data as shown in Fig. 2.

III. Proposed Method

The proposed algorithm heals many problems such as high complexity and low efficiency in ElGamal [15] without affecting the security level as discussed in [18], where it based on replacing the modular inverse function in MVECC by non linear LFSR. Using of NLFSR increases the efficiency through extending the LFSR output and also it reduces the complexity, compared to multiplication function used in [19] which also has high complexity.

There are other important problems that are cured by the proposed algorithm is the personal authentication that is used to prevent modification attacks, non-repudiation attacks, and data redundancy problem without increasing the complexity through using hash functions and key exchange as in [20].

In this section, a new encryption method based on ECC public key encryption is proposed. We will propose a method to decrease the complexity of Menezes-Vanstone algorithm. Meanwhile the message transmitted is authenticated, so that Bob can verify the source of the message and discriminate the faked message fabricated by Eve, while Alice cannot deny the message she sent. The sample method that is proposed allows also speeding up the key change rate so that it solves the redundancy problem.

A. The Proposed Algorithm MMVECC Mathematical Modeling and Flow Chart

In the proposed method, Alice possesses two private keys; one is constant, denoted as P_{aM}, and the other change along with the blocks, denoted as P_{ai}. As a result, two distinct public keys are generated respectively, denoted as Q_{aM} and Q_{ai}. The fixed public key is verified between the Alice and Bob just one time in the beginning using any method of key exchange. The fixed public key is used for signing every message transmitted from the sender to the receiver while the frame public key or varying key is used to change the stream cipher to allow one time pad technique and to solve redundancy problem through achieving Shannon principle of perfect secrecy.

MMVECC Encryption *Algorithm’s steps are as follows:*

1) Calculate the fixed public key Q_{aM} and Q_{bM} from P_{aM} and P_{bM}.
2) Alice selects variable $P_{ai}$to generate from public key Q_{ai}, where $J_{1i} = Q_{ai}$.
3) The encryption stream cipher at Alice’s side is calculated as follows:

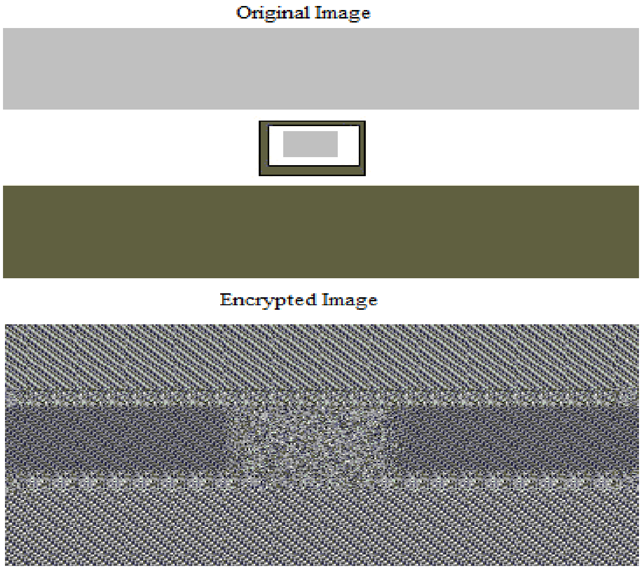

Fig. 2. Fixed key redundant data encryption problem.

$$(X_c, Y_c) = (P_{ai} + P_{aM}) \cdot Qb \qquad (16)$$

4) $C_1 = \{X_c, Y_c\}$ is undergone thorough nonlinear element for substitution (Sboxs) as the first step of NLFSR
5) Send set C1' at output of the s-box to the N-stage LFSR register.
6) Repeat Step 4 and Step 5 for n times.
7) The output set of Step 5, denoted as $C_2 = \{\acute{X}_c, \acute{Y}_c\}$will be XORed with the unencrypted message set $M = \{M_1, M_2\}$

$$J_{2i} = M_1 \oplus \acute{X}_c \ mod\ P \qquad (17)$$

$$J_{3i} = M_2 \oplus \acute{Y}_c \ mod\ P \qquad (18)$$

After receiving signals, Bob conduct the following steps:

1) Get $C_1 = \{X_c, Y_c\}$ from (13), where Q_{ai} is J_{1i}.

$$C_1 = \{X_c, Y_c\} = (Q_{aM} + Q_{ai}) \cdot P_b \qquad (19)$$

2) Input the set C_1 to the s-box, the s-box is the same as that of Alice
3) The output of the s-box to the N-stage LFSR.
4) Repeat Step 2 and Step 3 for n times.
5) The output set of Step 4, denoted as $C_2 = \{\acute{X}_c, \acute{Y}_c\}$, will be XORed with received message

$$M_1 = J_{2i} \oplus \acute{X}_c \ mod\ P \qquad (20)$$

$$M_2 = J_{3i} \oplus \acute{Y}_c \ mod\ P \qquad (21)$$

Proof of correctness

To proof of correctness and equality of (16) and (19) can be derived as follows:

$$\begin{aligned} C_1 = \{X_c, Y_c\} &= (Q_{aM} + Q_{ai}) \cdot P_{bM} \\ &= (P_{aM} \cdot B + P_{ai} \cdot B) \cdot P_{bM} \\ &= (P_{aM} + P_{ai}) \cdot (P_{bM} \cdot B) \\ &= (P_{aM} + P_{ai}) \cdot Q_{bM} \end{aligned}$$

The flowchart of MMVECC is shown in Fig 4, where every frame is encrypted by different key without any need for increasing the complexity except for just one point addition in decoding as shown in (19) and one scalar addition as shown in (16). Actually this simple modification makes the algorithm very immune against modification attacks and non-repudiation or impersonating attacks as will be discussed in next section.

B. Verification Example for the Proposed Method

This example is just for simple elliptic curve with short key length to clarify the proposed algorithm steps.

Let us select the prime number p= 105557, a=1111, b=2224, and B = [105280, 12229] so $4 * (1111)^3 + 27 * (2224)^2 \bmod 105557 \neq 0$, then the number of points = $(105557 - 1)^{1/2} = 105143$

Setup global keys and parameters

- Selecting the secret key for Alice master key ka_M to be 13351 then the public key 13351*(105280, 12229) mode 105557 = (89757, 24623) = QA_M
- Selecting the secret key for Bob master key kb_M to be 10255 then the public key 10255*(105280, 12229) mode 105557= (80710, 41398) = QB_M

Setup the frame Key

- Selecting the secret key for Alice frame key ka_i to be 29281 then the public key 29281*(105280, 12229) mode 105557= (46790, 7938) = QA_i

Encryption Process

- Calculate C1, C2 = $(Ka_i + ka_M).QB_M$ = (29281+13351). (80710, 41398) mode 105557 = (48706, 61219).
- Calculate $(R1, R2) = NLFSR(C1 \,\&\, C2)$ =(21458, 16598).
- Calculate $(y1, y2) = (R1 + M1\ mod\ p,\ R1 + M1\ mod\ p)$, for (M1, M2) = (54321, 12345) = (75779, 28943).

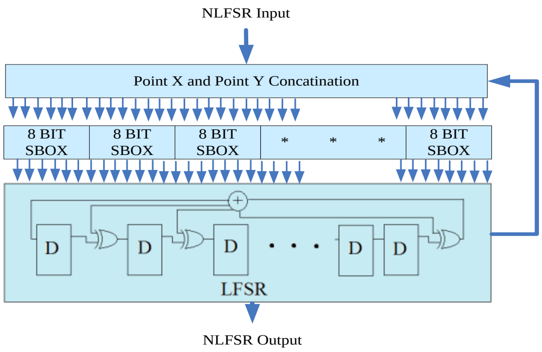

Fig. 3. The NLFSR structure.

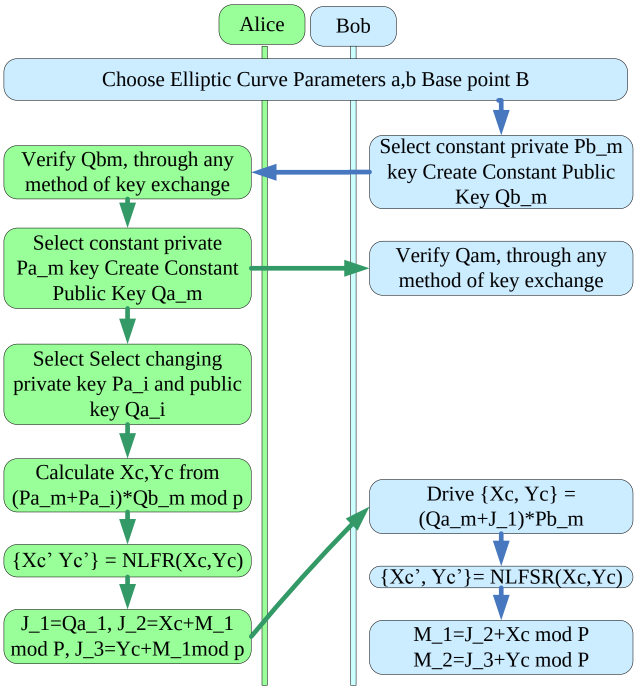
Alice
Bob
Choose Elliptic Curve Parameters a,b Base point B
Verify Qbm, through any method of key exchange
Select constant private Pb_m key Create Constant Public Key Qb_m
Select constant private Pa_m key Create Constant Public Key Qa_m
Verify Qam, through any method of key exchange
Select Select changing private key Pa_i and public key Qa_i
Calculate Xc,Yc from (Pa_m+Pa_i)*Qb_m mod p
Drive {Xc, Yc} = (Qa_m+J_1)*Pb_m
{Xc' Yc'} = NLFR(Xc,Yc)
{Xc', Yc'}= NLFSR(Xc,Yc)
J_1=Qa_1, J_2=Xc+M_1 mod P, J_3=Yc+M_1mod p
M_1=J_2+Xc mod P
M_2=J_3+Yc mod P

Fig. 4. Data flow protocol using the proposed scheme.

Decryption Process

- Calculate C1, C2 = $(QA_i + QA_M).kb_M$ = ((46790, 7938) + (89757, 24623)). 10255 mode 105557 = (49872, 19159). 10255 mode 105557 = (48706, 61219).
- Calculate $(R1, R2) = NLFSR(C1\,\&\,C2)$ =(21458, 16598).
- Calculate $\left(\acute{M}1, \acute{M}2\right) = (y1 - R1\,mod\,p,\ y1 - R2\,mod\,p)$, = (75779-21458, 28943-16598) mod 105557 = (54321, 12345).

IV. Result and Analysis

A. Complexity Reduction

The presented algorithm reduces the complexity of the Menezes-Vanstone algorithm since XOR operation is applied as a substitute of the point multiplication, and the modular inverse Xc^{-1} and Yc^{-1} are no longer be calculated. On the other hand, the constant key P_{aM} and Q_{aM} are introduced as a signature of Alice, making the message sent by Alice undeniable and the message fabricated by Eve distinguishable.

B. Resistance to attacks

Upon the previous example every frame is signed by master key while encrypted by frame key, so that if there are an attacker tried to send encrypted information using other Algorithms like ElGamal or Menezes, he just prepares a random key and calculate its public key then, calculate very easily where all these parameters are public, and there is nothing that can differentiate Eve from Alice.

Actually this is maybe not representing a problem if there is key exchange before every frame transmission, but unfortunately this is not a case. The proposed algorithm signed every frame with the secret key of the master where it prevents fake transmissions and resists non repudiation attacks. Eve cannot modify nor do fake transmission, where he does not have the secret signature key (P_{aM} fixed key). Also he does not have secret encryption key (P_{ai} variable key).

C. Redundancy Problem Solving

Redundancy problem is not meaning that the encryption algorithm is weak, but it means that the way or the method of using this algorithm to treat data is not right. For that reason different modes of operation is used to solve such problems even in public key encryption this problem can be solved by increasing some random data to change the similar input data. However, random data insertion method partially solves the redundancy problem; it reduces the data rate, where it based on insertion of an unwanted data.

In the redundancy problem, the ciphered output suffers from distinguishable patterns existence especially at the edges of the image, as shown in Fig 2. Using the proposed algorithm totally heal this problem , where it based on changing the key with every frame meanwhile the ciphered output is totally random while the input is repeated pixels as shown in Fig. 5 .

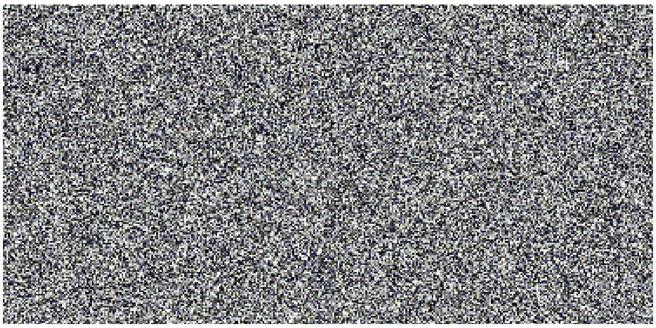

Fig. 5. Encrypted image using the proposed encryption Algorithm MMVECC.

V. Conclusion

The proposed MMVECC is a modified version of MVECC algorithm. It has two modifications. The first modification is represented in the replacement of modular inverse function by NLFSR, and the second modification is the use of two keys (fixed key and variable key) instead of one fixed key. Although the represented modification is simple, but it resulted in complexity reduction and it increases the security level through changing the key with every frame without increasing the headache of key management. The proposed method is represented and verified by a verification example. The encryption results show how far the output is random and it also shows how it doesn't reflect any distinguishable patterns although the input is repeated frames.

References

[1] R. L. Rivest, "A method for obtaining digital signatures and public key cryptosystems," *Communications of ACM*, pp. 120-126, 1978.

[2] C. Coarfa and P. Druschel, "Performance analysis of TLS web servers," *Network and Distributed Systems Security Symposium*, 2002.

[3] V. S. Miller, "Use of elliptic curves in cryptography," *Advances in Cryptography*, pp. 417-426, 1985.

[4] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, pp. 203-209, 1987.

[5] *Stinson, Douglas: Cryptography: Theory and Practice*, CRC Press 1995.

[6] V. Gupta, "Performance analysis on elliptic curve cryptography," pp. 87-94, 2002.

[7] M. Fu and C. Wei, "Elliptic curve cryptography elgamal encryption and the transmission scheme," in *Proc. International Conference on Computer Application and System Modeling*, pp. 51-53, 2010.

[8] K. G. Silakari, "ECC over RSA for asymmetric encryption: A review," *International Journal of Computer Science Issues*, pp. 370-375, 2011.

[9] D. B. Saikia, "Implementation of ElGamal elliptic curve cryptography over prime field," in *Proc. IEEE International Conference on Information Communication and Embedded Systems*, 2014.

[10] M. K. Yerlika, "A new modified cryptography based on Menezes Vanstone elliptic curve cryptography algorithm that uses characters' hexadecimal values," *International Journal of Electronic Security and Digital Forensics*, pp. 11-24, 2013.

[11] K. H. Rahouma, *A Modified Menezes-Vanstone Elliptic Curve Multi-Keys Cryptosystem*, 2005.

[12] H. L. Jian, "FPGA implementation of elliptic curve cryptography and Tate pairing over a binary field," *Journal of Systems Architectures*, pp. 1077-1088, 2008.

[13] M. Reaz and J. Jalil, "PGA implementation of elliptic curve cryptography engines for personal systems," *Wseas Transactions on Circuits and Systems*, pp. 82-91, 2012.

[14] J. H. Hao, "An FPGA implementation of elliptic curve cryptography for future secure web transaction," in *Proc. ISCA International Conference on Parallel Distributed Computer Systems*.

[15] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 469–472, 1985.

[16] V. SMC, "Muneeswaran: A new elliptic curve cryptosystem for securing sensitive data applications," *International Journal of Electronic Security and Digital Forensics*, vol. 5, no. 1, pp. 11–24, 2013.

[17] Z. E. D. Shahrul, "Modified elgamal elliptic curve cryptosystem using hexadecimal representation," *Indian Journal of Science and Technology*, vol. 8, no. 15, 2015.

[18] Z. E. D. Shahrul, "A new modification for menezes-vanstone elliptic curve cryptosystem," *Journal of Theoretical and Applied Information Technology*, vol. 86, no. 3, pp. 290-297, 2016.

[19] N. F. H. A. S. Mohamad, "On the mathematical complexity and the time implementation of proposed variants of elliptic curves cryptosystems," *International Journal of Cryptology Research*, vol. 4, no.1, 2013.

[20] D. L. Kwangjo, "Security enhancement of remote user authentication scheme using bilinear pairings and ECC," in *Proc. IFIP International Conference in on Network and Parallel Computing*, pp. 144-147, 2007.

Mostafa Ahmed Mohamed Sayed was born in Egypt in 1981. He received his bachelor in electric engineering from Military Technical College, Nasr City Cairo, Egypt in 2003.

He received his master of Science in communication and information security from Military Technical College, Cairo 2011.

He works as a researcher and assistant lecturer, Egypt.

Currently He is a PHD candidate in Beihang University, Beijing China (BUAA).

He is interested in communication, channel coding and information security