ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

A Matrix Approach for Information Security Based ECC using Mealy Machine and Fibonacci Q-Matrix

Fatima Amounas*, El Hassan El Kinani**, Moha Hajar***
* R.O.I Group, Computer Sciences Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Morocco.
** A.A Group, Mathematical Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Morocco.
*** R.O.I Group, Mathematical Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Morocco.

Abstract— Cryptography is the science of transmission and reception of secret messages. Nowadays the information security is essential in many operations in our everyday life. Many number of cipher generation and decryption algorithms exists and are being evolved due to increasing demand of users and e-commerce services. Message encryption has become very essential to avoid the threat against possible attacks by hackers during transmission process of the message. In this paper we propose a new approach for secure information transmission over communication channel based on elliptic curve using mealy machine and Fibonacci Q-matrix. Proposed approach will not only enhance the security of information but also saves computation time and reduces power requirements that will find it's suitability for future hand held devices and online transaction processing.

Index Terms— **Cryptography, Elliptic Curve, Fibonacci Q-matrix, Mealy machine.**

I. INTRODUCTION

Security of information has become a popular subject during the last decades [1, 2, 3]. One such way to secure information is cryptography. It is the art or science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (ciphertext) and then retransforming that message back to its original form. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Cryptography systems can be broadly classified into: symmetric and asymmetric.

Many symmetric key encryption techniques are available in literature. Some of them are encryption standards such as AES and DES [4]. A symmetric key scheme utilizes a shared key for encryption and decryption. The message which is encrypted using this key can only be decrypted back using the same secret key. On the other hand, in asymmetric algorithms, the decryption key cannot be calculated from the encryption key. So, keys play an important role in the security of any cryptographic algorithm.

The elliptic curve cryptosystems (ECC) were invented around 1985 independently by Miller and Koblitz. Since their introduction a broad discussion on their security and efficiency has been carried on. It is this very efficiency that makes them so interesting for us today. This is due to the fact that information technology is developing very fast. Today we use handhelds and mobile phones as we have a need in securing communications on these devices. But several constraints like limitations in memory, computing power, bandwidth requirement etc need to be considered. What we need is a cryptosystem with small keys, and a small signature size. Efficient encryption/decryption is not so important because these operations are usually done with a private key cryptosystem. ECC has exactly the desired properties. This comes from the fact, that there are no sub exponential algorithms for the ECDLP (elliptic curve discrete logarithm problem) known today. This means that we can use shorter keys (compared to other cryptosystems) for high security levels.

In our previous works [5, 6, 7], we have proposed the public-key cryptosystems based on ECC mechanism. In fact, the transformation of the message into affine points is explained. In this paper, we instead focus for new algorithm based on varying the key to increase the security of algorithm. In particular, we propose a new approach for secure information transmission over communication channel with key variability concept in symmetric key algorithms based ECC using finite state machine and Fibonacci Q-matrix. Proposed approach will not only enhance the security of information but also saves computation time and reduces power requirements.

The paper is organized as follows. Following the introduction, the basic concept of elliptic curve cryptography, Mealy machine and Fibonacci Q-matrix are outlined in section II. In section III, proposed cryptosystem is presented. Section IV discusses about the security analysis. Finally, section V describes the concluding remarks.

II. PRELIMINAIRES

A. *Review of Elliptic Curve Cryptography*

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a r andom elliptic curve element with respect to a publicly-known base point is infeasible [8]. The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements.

ECC follows Public Key Encryption technique and the security provided is based on the hardness of Discrete Logarithm Problem called Elliptic Curve Discrete Logarithm Problem (ECDLP). According to ECDLP, kP= Q, where P, Q are the points on an elliptic curve and k is a scalar. If k is significantly large then it is unviable to calculate k when the values of P and Q are given. Here k is the discrete logarithm of Q, having base P.

1) *Basics on the ECC*

An elliptic curve E can be defined over a prime field Fp or binary field F2m[9], here the Weierstrass form curve has been considered; a type of elliptic curve defined over Fp.For current cryptographic purposes, an elliptic curve defined over prime field is a plane curve which consists of the points satisfying the equation (1) where the condition 4a3 + 27b2 mod p ≠ 0 is kept to so the elliptic curve is non-singular [10].

$$y^2= x^3 + ax + b \bmod p, \quad (1)$$

along with a distinguished point at infinity, denoted “Ω”. This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

2) *ECC operations*

ECC follows the group law and logarithm problem. From the ECDL problem it is evident that the major operation involved in ECC is point multiplication. i.e. multiplication of a scalar k with a point P on the curve to obtain another point Q on the curve.

- Point Multiplication: Points P and Q lie on the elliptic curve such that when P is multiplied with a scalar k to obtain the point Q,

$$kP=Q,$$

The point multiplication operation involves series of point addition and point doubling operations. The doubling and addition method is illustrated as follows:

If k = 23, then kP = 23·P = 2(2(2(2P) + P) + P) + P.

B. *Mealy machine*

In the theory of computation, a Mealy machine is a finite state transducer that generates an output based on its current state and input. This means that the state diagram will include both an input and output signal for each transition edge. In contrast, the output of a Moore finite state machine depends only on the machine’s current state, transitions are not directly dependent upon input. Mealy machines provide a rudimentary mathematical model for cipher machines. Considering the input and output alphabet the Latin alphabet, for example, then a Mealy machine can be designed that given a string of letters (a sequence of inputs) can process it into a ciphered string (a sequence of outputs). A Mealy machine is a 6-tuple [11], and is defined as:

$$M= (Q, \sum, \Delta, \sigma, \lambda, q_0)$$

Q: A finite set of state in Mealy machine

q_0 : Is the initial state in Q.

∑: A set of inputs.

Δ : A set of outputs.

σ : It is a transition function which takes two arguments one is input state and another is input symbol. The output of this function is a single state 0.

λ : Is a mapping function:

$$\lambda \ : Q \, x\sum \rightarrow \ \Delta$$
$$t \ \rightarrow \ 0,$$

which giving the output associated with each transition.

Now, we consider a Mealy machine:

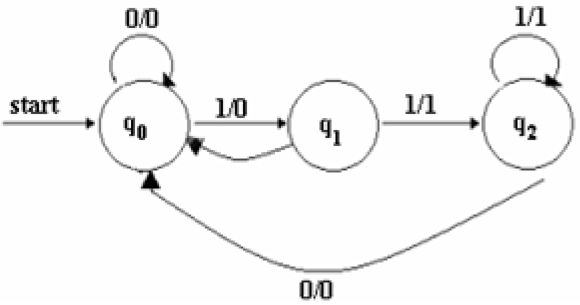

Fig 1. Mealy machine

In the above diagram 0/1 represent input/output.

C. *Fibonacci Q-Matrix*

In the last decades the theory of Fibonacci numbers was complemented by the theory of the so-called Fibonacci Q-matrix [12, 13]. This 2×2 square matrix is defined in [13] as follows:

$$Q=\begin{pmatrix} F_2 & F_1 \\ F_1 & F_0 \end{pmatrix}$$

where det(Q) = $F_2 \, F_0 – (F_1)^2= –1$.

The numbers F_0, F_1 and F_2 are the Fibonacci numbers obtained by the following recursive function:

$$\begin{cases} F_0=0, \ F_1=1 \\ F_n = F_{n-1} + \ F_{n-2} \qquad \text{if } n > 1 \end{cases}$$

It is well known [14] that, the nth power of this Q-Matrix can be computed as follows:

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

Since det(A^n)= (det(A)) ^{n}. Therefore, det(Q^n) = $(-1)^n$, for all intergers n.

The Q^{-n} matrix inverse matrix of Q^n is expressed by the formula:

$$Q^{-n} = \begin{pmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{pmatrix}$$

III. MAIN RESULTS

In this section, we provide an encryption/decryption technique based ECC using the concept of Mealy machine and Fibonacci Q-matrix. This algorithm assumes an initial message in the form of square matrix (p+1)x(p+1) where p is an integer.

In our case, we choose the Fibonacci Q_p-matrix, Q^n_p (p+1)x(p+1) as encryption key matrix, and it's inverse matrix Q^n_p as decryption key matrix.

A. *Proposed Algorithm*

1) Steps involved in encryption process

Step 1. Represent the message M.

Step 2. Split M into parts such that each one is a matrix of order (2x2).

Step 3. Choose an integer k and compute $K=kP_B$.

Step 4. Define Mealy machine with input is secure key. Then, define Fibonacci Q^n_p -matrix with n=input+output+1.

Step 5. Define Cipher Text as:

$$Cj+1= Cj.Q^n_p$$

kP is combing with the cipher text at the final stage and is sending to receiver.

2) Steps involved in decryption process

Step 1. Computes the product of the first point kP and his Private key, $K=n_B$ (kP).

Step 2. Received encoded message is represented in the matrix C.

Step 3. Define Mealy machine with input is secure key. Then, define Fibonacci Q^n_p-matrix with n=input+output+1.

Step 4. Compute the reversible matrix Q^{-n}_p.

Step 5. Apply the reversible process to recover plain text.

B. *Illustration and Example*

The chosen elliptic curve is represented by the Weierstrass equation:

$$y^2 = x^3+x+13 \mod 31.$$

The elliptic curve contains 34 points, illustrated in Table 1. In this case, the base point P is selected as (9, 10). It is the point with represents the letter 'A', as well as 2P represents the letter 'B', … , 34P represents space.

Here we use the letters 'A', 'B', …, 'Z' with some of the other symbols like ';', '(', ')', ',', '[', ']', ':' and space for illustration purpose only.

Let Fibonacci Q-matrix key be:

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

Hence we shall assume that n_B=13, k=23, P_B=(27,10), K=(6, 7). Then, the input key is: 0011000111.

In our case, we consider a Mealy machine illustrated in Figure 1.

Table 1. A set of points on E_{31}(1,13).

(9, 10)	(18, 29)	(23, 19)	(4, 22)
(25, 16)	(17, 18)	(6, 24)	(24, 29)
(16, 8)	(20, 2)	(22, 22)	(28, 13)
(27, 10)	(26, 21)	(5, 9)	(19, 3)
(10, 0)	(19, 28)	(5, 22)	(26, 10)
(27, 21)	(28, 18)	(22, 9)	(20, 29)
(16, 23)	(24, 2)	(6, 7)	(17, 13)
(25, 15)	(4, 9)	(23, 12)	(18, 2)
(9,21)	Ω		

Let the plain text be: "THANK YOU IJEIT"

The above message has 15 characters. This is split into square matrices P1, P2, P3, P4.

Where

$$P1= \begin{pmatrix} (26, 10) & (24, 29) \\ (9, 10) & (26, 21) \end{pmatrix} \qquad P2= \begin{pmatrix} (22, 22) & (0, 1) \\ (16, 23) & (5, 9) \end{pmatrix}$$

$$P3= \begin{pmatrix} (27, 21) & (0, 1) \\ (16, 8) & (20, 2) \end{pmatrix} \qquad P4= \begin{pmatrix} (25, 16) & (16, 8) \\ (26, 10) & (0, 1) \end{pmatrix}$$

Cipher text at each state is calculated for P1 in Table 2. Similarly for P2, P3, P4.

Table 2. Encryption process of P1.

In-put	Out put	Pres. state	n	Secure key	Cipher text
0	0	q_0	1	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} (17, 13) & (26, 10) \\ (5, 9) & (9, 10) \end{pmatrix}$
0	0	q_0	1	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} (26, 21) & (17, 13) \\ (19, 3) & (5, 9) \end{pmatrix}$
1	0	q_1	2	$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} (28, 18) & (24, 29) \\ (27, 10) & (23, 12) \end{pmatrix}$

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

1	1	q_2	3	$\begin{pmatrix}3&2\\2&1\end{pmatrix}$	$\begin{pmatrix}(26, 21)&(19, 28)\\(9, 21)&(22, 9)\end{pmatrix}$
0	0	q_0	1	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}(18, 2)&(26, 21)\\(28, 18)&(9, 21)\end{pmatrix}$

Table 3. Encryption process of P2.

In-put	Out put	Pres. state	n	Secure key	Cipher text
0	0	q_0	1	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}(22, 22)&(22, 22)\\(17, 18)&(16, 23)\end{pmatrix}$
0	0	q_0	1	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}(28, 18)&(22, 22)\\(23, 12)&(17, 18)\end{pmatrix}$
1	0	q_1	2	$\begin{pmatrix}2&1\\1&1\end{pmatrix}$	$\begin{pmatrix}(27, 21)&(9, 21)\\(0, 1)&(23, 19)\end{pmatrix}$
1	1	q_2	3	$\begin{pmatrix}3&2\\2&1\end{pmatrix}$	$\begin{pmatrix}(6, 7)&(3, 24)\\(17, 18)&(23, 19)\end{pmatrix}$
1	1	q_2	3	$\begin{pmatrix}3&2\\2&1\end{pmatrix}$	$\begin{pmatrix}(6, 7)&(6, 7)\\(20, 29)&(5, 9)\end{pmatrix}$

Table 4. Encryption process of P3.

In-put	Out put	Pres. state	n	Secure key	Cipher text
0	0	q_0	1	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}(27, 21)&(27, 21)\\(5, 22)&(16, 8)\end{pmatrix}$
0	0	q_0	1	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}(24, 29)&(27, 21)\\(17, 13)&(5, 22)\end{pmatrix}$
1	0	q_1	2	$\begin{pmatrix}2&1\\1&1\end{pmatrix}$	$\begin{pmatrix}(23, 19)&(25, 15)\\(6, 24)&(27, 10)\end{pmatrix}$
1	1	q_2	3	$\begin{pmatrix}3&2\\2&1\end{pmatrix}$	$\begin{pmatrix}(9, 21)&(9, 10)\\(27, 10)&(6, 7)\end{pmatrix}$
0	0	q_0	1	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}(0, 1)&(9, 21)\\(17, 18)&(27, 10)\end{pmatrix}$

Table 5. Encryption process of P4.

In-put	Oup ut	Pres. state	n	Secure key	Cipher text
0	0	q_0	1	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}(26, 21)&(25, 16)\\(26, 10)&(26, 10)\end{pmatrix}$
0	0	q_0	1	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}(5, 22)&(26, 21)\\(17, 18)&(26, 10)\end{pmatrix}$
1	0	q_1	2	$\begin{pmatrix}2&1\\1&1\end{pmatrix}$	$\begin{pmatrix}(19, 28)&(9, 21)\\(18, 2)&(24, 2)\end{pmatrix}$
1	1	q_2	3	$\begin{pmatrix}3&2\\2&1\end{pmatrix}$	$\begin{pmatrix}(19, 28)&(9, 10)\\(28, 13)&(28, 18)\end{pmatrix}$
1	1	q_2	3	$\begin{pmatrix}3&2\\2&1\end{pmatrix}$	$\begin{pmatrix}(28, 18)&(23, 19)\\(28, 13)&(27, 13)\end{pmatrix}$

The result cipher text for P1, P2, P3 and P4 respectively are illustrated in (Table 2, Table 3, Table 4, Table 5). Therefore, the cipher text is sending as:
10110010011001000010110101010111100100100100110101001100011100110001111010011101001010100100000000010100110101100011001011011010101110010010101111001111100011011110001101
After receiving the cipher text, it may be decrypted by the receiver using the inverse operation of the above algorithm based Q^{-n}.

IV. SECURITY ANALYSIS

The proposed method is a simple application of addition or multiplication of two matrices. Its elements are points on elliptic curve. But the operations are different depending on secure key and the chosen elliptic curve. It is very difficult to break the cipher text without secure key, defined operation and the chosen finite state machine.

The key is defined as point on elliptic curve and Fibonacci Q-matrix which again depends on the recurrence relation. It is very difficult to trace the secret key even when finite state machine is known. To extract the original information is highly impossible due the mathematical calculations. Due the secret key, output at each sate and the recurrence relations are the three stage attacks are at a time impossible even the Mealy machine is known. Brute force attack on key is also not possible due to the increase in key size.

V. CONCLUSION

In the present paper, we presented a new encryption scheme based ECC using Fibonacci Q-Matrix and Mealy machine. The idea behind choosing the Fibonacci Q-matrix is that they are unstable and have integer inverses. These properties make them interesting. Further, algorithm proposed is based on finite state machine (Mealy machine) and matrix multiplication using addition and doubling of points. The security level is high and breaking the cipher text is difficult due to the secret key, the chosen finite state machine, and the recurrence matrix. Finally, the proposed method can be enhanced further by using more complex techniques in key generation phase as well as using the genetic functions in a more detailed and complicated way.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

[1] H. Imai, G. Hanaoka, J. Shikata, A. Otsuka, A.C. Nascimento, "Cryptography with information theoretic security", Information Theory Workshop, Proceedings of the IEEE, pp. 20-25, 2002.

[2] W. Stallings, "Cryptography and network security", 4th edition, Prentice Hall, 2005.

[3] M.Abutaha, M.Farajallah, R.Tahboub and M.Odeh, "Cryptography Is the Science of Information Security, International Journal of Computer Science and Security, vol (5), Issue (3), 2011.

[4] Westlund, Harold B. "NIST reports measurable success of Advanced Encryption Standard". Journal of Research of the National Institute of Standards and Technology, 2002.

[5] F.Amounas, E.H. El Kinani, and A.Chillali, "An application of discrete algorithms in asymmetric cryptography", International Mathematical Forum 6 (49), pp. 2409-2418, 2011.

[6] F.Amounas and E.H. El Kinani, "An Efficient Elliptic Curve Cryptography protocol Based on Matrices", International Journal of Engineering Inventions, Vol 1, Issue 9, pp. 49-54, 2012.

[7] F.Amounas and E.H. El Kinani, "Encryption of Data using Elliptic Curve over Circulant Matrices", International Journal of Electronics Communication and computer Engineering, vol 4, No 1, pp. 1502-1506, 2013.

[8] V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology, Springer-Verlog New York, 1986.

[9] Anoop MS, "Elliptic Curve Cryptography - An implementation guide", May 2007.

[10] Darrel Hankerson, Alfred Menezes and Scott Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag New York, 2004.

[11] John E.Hopcroft, Rajeev Motwain, Jeffrey D.Ulman- "Introduction to automata theory, language, and computation" Vanstone3rd impression, 2007 CRC Press., Dorling Kindersley (India) Pvt. Ltd, 2007.

[12] A. P. Stakhov, The golden matrices and a new kind of cryptography, Chaos, Solutions and Fractals 32, 1138-1146, 2007.

[13] T. Koshy, Fibonacci and Lucas Numbers with Applications, AWiley-Interscience publication, U.S.A, 2001.

[14] V. E. Hoggat, Fibonacci and Lucas numbers, Houghton-Mifflin, Palo Alto, 1969.

EL HASSAN EL KINANI received the Ph.D in mathematical physics in 1999 from Mohamed V University Rabat Morocco. He is full professor at department of mathematics in Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco. He is interested in classical and quantum cryptography.
E-mail: elkinani_67@yahoo.com

MOHA HAJAR received the Ph.D in mathematical in 1988 from Aix-Marseille II University French. He is full professor at department of mathematics in Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco. He is interested in Mathematics and Computer Sciences.
E-mail: Moha_hajjar@yahoo.fr

FATIMA AMOUNAS received the Ph.D degree in Mathematics, Computer Science and their applications in 2013 from Moulay Ismaïl University, Morocco. She is currently an assistance Professor at Computer Sciences department at Faculty of Sciences and Technics, Errachidia, Morocco. Her research interests include elliptic curve and cryptography.
E-mail: F_amounas@yahoo.fr