International Journal of Computer Applications Technology and Research
Volume 5–Issue 11, 708-713, 2016, ISSN:-2319–8656

A New Security Level for Elliptic Curve Cryptosystem Using Cellular Automata Rules

Fatima Amounas
R.O.I Group, Computer Sciences Department
Moulay Ismaïl University,
Faculty of Sciences and Technics,
Errachidia, Morocco.

El Hassan El Kinani
A.A Group, Mathematical Department
Moulay Ismaïl University,
Faculty of Sciences and Technics,
Errachidia, Morocco.

Abstract: Elliptic curve cryptography (ECC) is an effective approach to protect privacy and security of information. Encryption provides only one level of security during transmission over the channel. Hence there is a need for a stronger encryption which is very hard to break. So, to achieve better results and improve security, information has to pass through several levels of encryption. The aim of this paper would be to provide two levels of security. First level comprises of plaintext using as security key compressed block to encrypt text based ECC technique and the second level comprises of scrambling method with compression using 2D Cellular rules. In particular, we propose an efficient encryption algorithm based ECC using Cellular automata and it is termed as Elliptic Curve Cryptosystem based Cellular Automata (ECCCA). This paper presents the implementation of ECCCA for communication over insecure channel. The results are provided to show the encryption performance of the proposed method.

Keywords: Cryptography, Elliptic curve, Cellular automata, Matrix, Scrambling technique, Encryption, Decryption.

1. INTRODUCTION

Security is the important factor in the public network and cryptography play an important role in this field. Cryptography is an old art of sending secret messages between sender and receiver. With the advancement of internet technologies, cryptography becomes a crucial aspect for secure communications to protect important data from eavesdroppers. In fact, cryptography is the science of devising methods that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient. Cryptography is broadly divided into two categories depending upon the key, which is defined as the rules used to convert an original text into encrypted text: - Symmetric Key Encryption and Asymmetric Key Encryption. Symmetric Key Encryption uses the same key for encryption and decryption processes. This technique is simple yet powerful but key distribution is the chief problem that needs to be addressed Whereas, Asymmetric Key Encryption use two mathematically associated keys: Public Key & Private Key for encryption. The public key is available to everyone but the data once encrypted by public key of any user can only be decrypted by private key of that particular user.

Elliptic curve cryptography is effective security solution to provide secure communication. Elliptic curve cryptography transforms a mathematical problem in to an applicable computer algorithm. Intractable problems are the center of public key cryptography and bring computationally demanding operations into a cryptosystem. Elliptic curve cryptography (ECC) is based upon the algebraic structure of elliptic curves over finite field. Elliptic curve cryptography is the most efficient public key encryption scheme based on elliptic curve concepts that can be used to create faster, smaller, and efficient cryptographic keys. As result researchers are engaged to develop different cryptographic techniques based ECC to enhance network security [1, 2, 3]. Recently, more applications propose to use the elliptic curve in encryption process and improve their efficiency using cellular automata [4, 5]. In our previous works [6, 7, 8, 9], we have proposed cryptographic algorithm for text encryption using elliptic curve. Basically this paper is proposing a new encryption algorithm based ECC using the concept of cellular automata. Finally, expected results are showing the performance of the proposed algorithm.

The rest of the paper is structured as follows. Section 2 gives detailed description of commonly employed security concepts and terminology. In particular, we present basic idea of elliptic curve cryptography. Section 3 a detailed description of Cellular automata is presented. In section 4, the proposed method is introduced. A detailed example is presented that outlines the working procedure of the proposed method in section 5. Section 6 presents an implementation of ECCCA for encryption/decryption process, using Visual Basic as the implementation tool. Section 7 concludes the paper.

2. CRYPTOGRAPHIC TERMINOLOGY

In this section, we introduce some basics security terminologies and concepts connected with cryptography. A message present in a clear form, which can be understood by any casual observer, is known as the plaintext. The encryption process converts the plaintext to a form that hides the meaning of the message from everyone except the valid communicating parties, and the result is known as the cipher text. Decryption is the inverse of encryption. The processes of encryption and decryption are controlled on a quantity known as the key, which is ideally known only to the valid users. Strength of a security scheme depends on the secrecy of the keys used.

A security protocol formally specifies a set of steps to be followed by communicating parties, so that the mutually desired security objectives are satisfied. The four main security objectives include:

- Confidentiality: This means that the secrecy of the data being exchanged by the communicating parties is maintained, i.e., no one other than the legitimate parties should know the content of the data being exchanged.

- Authentication: It should be possible for the receiver to ensure that the sender of the message is who he claims to be, and the message was sent by him.

- Integrity: It provides a means for the receiver of a message to verify that the message was not altered in transit. It checks originality of message.

- Non-repudiation: The sender of a message should not be able to falsely deny later that he sent the message, and this fact should be verifiable independently by an independent third-party without knowing too much about the content of the disputed message(s).

Security protocols realize the security objectives through the use of appropriate cryptographic algorithms. Security objectives thus provide trust on the Web. They are realized through the use of cryptographic algorithms which are divided into two categories depending on their characteristics: Symmetric algorithms and Asymmetric algorithms.

2.1 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) was first introduced by Victor Miller and Neil Koblitz in 1985. The principal attraction of ECC compared to RSA is that it offers equal security for a far smaller key size, thereby reducing processing overhead [10]. The advantage of ECC over other public key cryptography techniques such as RSA is that the best known algorithm for solving ECDLP the underlying hard mathematical problem in ECC takes the fully exponential time and so far there is a lack of sub exponential attack on ECC. ECC is based on the Discrete Logarithmic problem over the points on an elliptic curve [11].

2.2 Mathematics Background of ECC

Let E be an elliptic curve over F_p, given by an affine Weierstrass equation of the form:

$$E: y^2 = x^3 + ax + b \qquad (1)$$

with coefficients a, b $\in F_p$ such that $4a^3 + 27b^2 \neq 0$. We recall that the set $E(F_p)$ of points of any elliptic curve E in affine F_p-valued coordinates form an Abelian group (with a point at infinity denoted by Ω as the neutral element).

To encrypt a message, Alice and Bob decide on an elliptic curve and take a affine point (P) that lies on the curve. Plaintext M is encoded into a point P_M. Alice chooses a random prime integer n_A and Bob chooses a random prime integer n_B. n_A and n_B are Alice and Bob's private key respectively. To generate the public key,

Alice computes,

$$P_A = n_A P$$

and Bob Computes.

$$P_B = n_B P$$

To encrypt a message point P_M for Bob, Alice chooses another random integer named k and computes the encrypted message PC using Bob's Public key (P_B). PC is a pair of points:

$$PC = [(kP), (P_M + kP_B)]$$

Alice Sends PC to Bob as a cipher message. Bob, receiving the encrypted message PC and using his private key, n_B, multiplying with kP and add with second point in the encrypted message to compute P_M, which is corresponding to the plaintext message M,

$$P_M = (P_M + kP_B) - [n_B (kP)]$$

Addition operation for two points $P(x_1, y_1)$ and Q (x_2, y_2) over an elliptic group, if P+Q= (x_3, y_3) is given by (2) and (3) and the parameter s is calculated by (4):

$$x_3 = s^2 - x_1 - x_2 \bmod p \qquad (2)$$

$$y_3 = s(x_1 - x_3) - y_1 \bmod p \qquad (3)$$

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } P \neq Q \end{cases} \qquad (4)$$

Multiplication kP over an elliptic group is computed by repeating the addition operation k times [12, 13]. The strength of an ECC-based cryptosystem is depends on difficulty of finding the number of times that P is added to itself to get Q=kP. Reverse operation known as Elliptic Curve Discrete Logarithm Problem (ECDLP).

3. CELLULAR AUTOMATA

Cellular Automata (CA) is a discrete computing model which provides simple, flexible and efficient platform for simulating complicated systems and performing complex computation based on the neighborhood's information. CA consists of two components 1) a set of cells and 2) a set of rules. Researchers, scientists and practitioners from different fields have exploited the CA paradigm for modelling different applications [14, 15].

A cellular automaton consists of a graph where each node is a cell. The state of each cell is updated simultaneously at discrete time steps, based on the states in its neighborhood at the preceding time step. The algorithm used to compute the next cell state is referred to as the CA local rule.

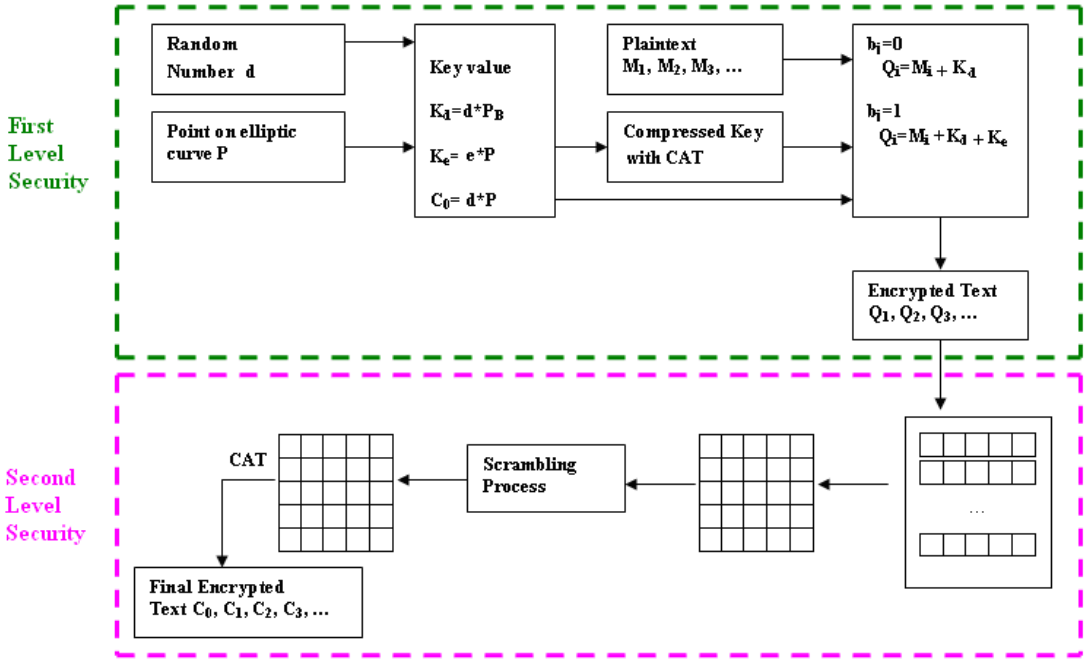


Figure 1. Model Diagram of Encryption Technique.

For 2-state 3-neighborhood cellular automata there are 2^3=8 distinct neighbourhood configurations and 2^8=256 distinct mappings from all these neighbourhood configurations to the next state, each mapping representing a CA rule [16].

A cellular automaton (CA) is a dynamic system defined by the following 4-tuple: dimension, set of finite states, neighborhood and set of rules. Dimension defines number of cells. Cells are updated accordingly to some rule. Such rule is based on the state of the cell and the neighborhood [17, 18]. Figure 2 shows two typical neighborhood options (a) Von Neumann Neighborhood (b) Moore Neighborhood.

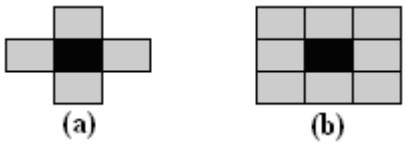
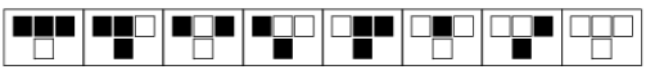


Figure 2. (a) Von Neumann Neighborhood (b) Moore Neighborhood

By applying the transition rule the current state of CA moves to new state by considering the neighborhood states.

For example:

- Rule 90:



- Rule 153:

4. PROPOSED METHOD

A new encryption method based ECC using cellular automata is presented in Figure 1. This method tries to use some asymmetric algorithm to encrypt or decrypt data using elliptic curve. The proposed scheme noted ECCCA combines the advantage of Automata theory and asymmetric encryption based ECC into a total scheme. The overall module design shows the different levels of security used (Figure 1).

In the proposed system, the first level of security starts with ECC technique, where the plaint text is used as the set of points to encrypt [19, 20, 21]. In this work, the resulting output is sent to the next process based cellular automata. In fact, the encrypted message is scrambled using the principle of spiral rotation. The proposed method explains the usage of second level of security using cellular automata since one level of security is not enough.

Let CA be the Cellular Automata, which used to scramble secure key applying the Local Rule.

4.1 Encryption procedure

The encryption is done through the following steps:

Step 1: start

Step 2: Divide the plain text into blocks of characters and embed the characters in into points on elliptic curve.

Step 3: Generate randomly one number d. Then, Compute K_d and K_e, which serve as secure keys (e is the x-coordinate of K_d).

Step 4: Generate a cellular automata rule and convert the compressed key to binary form.

Step 5: Select b=bit (j), where j is bit position (LSB→MSB), which decides which operation has to be performed.

If b = 0 ➔ compute $Q_i=M_i + K_d$
If b=1 ➔ Compute $Q_i= M_i + K_d + K_e$.

Step 6: Convert the result blocks into binary sequence and generate a compressed blocks by using CA technique.

Step 7: Arrange the first bit of all the blocks in the first row and second bits of all block in the second row and continuing this process arrange the remaining bit of all the blocks in the corresponding row of matrix.

Step 8: Apply spiral technique to scramble the data matrix and to get the cipher text.

Step 9: Stop

4.2 Decryption procedure

The decryption process involves converting the encrypted data back to its original form for the receiver's understanding. The cipher text is decrypted using the reverse process of the technique explained in encryption algorithm. The steps in decryption algorithm are as follows:

Step 1. start

Step 2. Divide the cipher text to blocks and the bits are arranged into a square matrix.

Step 3. Generate a reversible transition rule. Convert the compressed blocks to a normal form using reversible CA rule.

Step 4. Apply the corresponding reversible principle of spiral process.

Step 5. Defuse it to get the encrypted points on elliptic curve.

Step 6. Find the equivalent characters by decrypting each point.

Step 7. Accumulate characters to form the secret message.

Step 8. Stop.

5. EXPLANATION WITH EXAMPLE

We have following example on which we have applied our new encryption algorithm ECCCA, the explanation has been provided below.

For the system parameters, we used the following data:

- p and n: two prime numbers (p=29 , n=31).
- E_{29} (-1, 16) an elliptic curve defined on finite field F_{29}.
- P (5, 7): a point on elliptic curve E with order n.
- Key values:

  k= 19 and P_B=(16, 6).

  d=13 and P_A=(7, 27).

  K_d = (5,22) and K_e= (6, 20).

- CA Rule chosen: '90'

Phase 1:

Plain Text: "ENCRYPTION"

Character	Point on EC	Bit selected	Encrypted point Qi
E	(6,20)	1	(23, 3)
N	(1, 4)	0	(7, 27)
C	(18, 1)	1	(2, 14)
R	(7, 25)	0	(1, 25)
Y	(13,24)	1	(28, 25)
P	(0, 25)	0	(0, 4)
T	(14, 7)	0	(2, 15)
I	(23, 3)	1	(21, 11)
O	(0, 4)	1	(16, 6)
N	(1, 4)	0	(7, 27)

Phase2:

1	0	0	0	1	0	0	1	1	0
0	0	0	0	1	0	0	0	0	0
1	1	0	0	1	0	0	1	0	1
1	1	1	0	0	0	1	0	0	1
1	1	0	1	0	0	0	1	0	1
0	1	0	1	1	0	0	0	0	1
0	1	1	1	1	0	1	1	0	1
0	0	1	0	0	1	1	0	1	0
1	1	1	0	0	0	1	1	1	1
1	1	0	1	1	0	1	1	0	1

1	0	0	0	1	0	0	1	1	0
0	1	1	1	1	1	0	1	1	0
1	1	0	1	1	0	1	1	1	0
0	0	1	1	1	0	0	0	0	1
0	0	0	0	0	0	0	0	0	1
1	1	1	0	0	0	1	1	0	1
1	1	1	1	0	0	1	0	0	1
0	1	0	1	0	1	1	0	0	1
1	0	0	1	0	0	0	1	0	0
1	0	1	1	1	1	0	0	0	1

Therefore, the final encrypted text is compressed as follow: 0101101100000111010011100110011101000 1.

This algorithm compresses the data to reduce its length without compromising the compression efficiency and the information security.

6. RESULTS

In this section we proceed with our implementation using Visual Basic as tool. Winsock Control has been used for connecting two systems. Messages are transmit from user A to user B when a socket is created. In our implementation, we have used the curve E_{29} (-1, 16) in entire process.

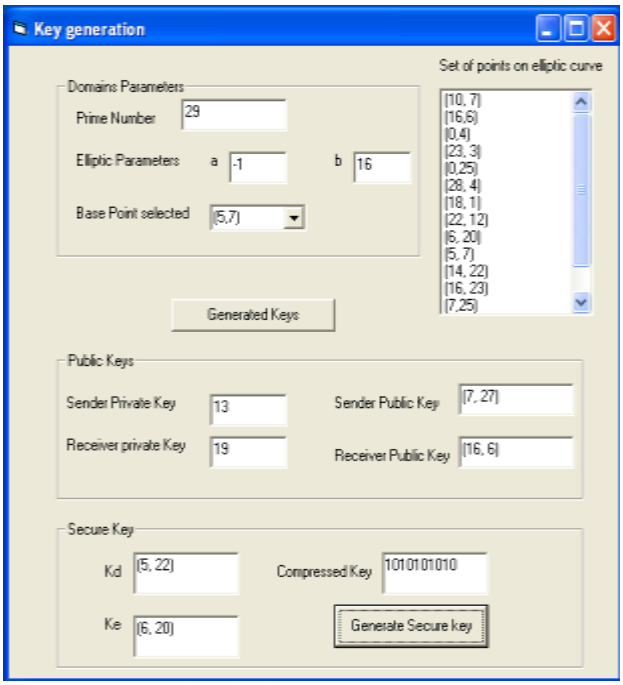


Figure 3. Shows the Key generated using CAT

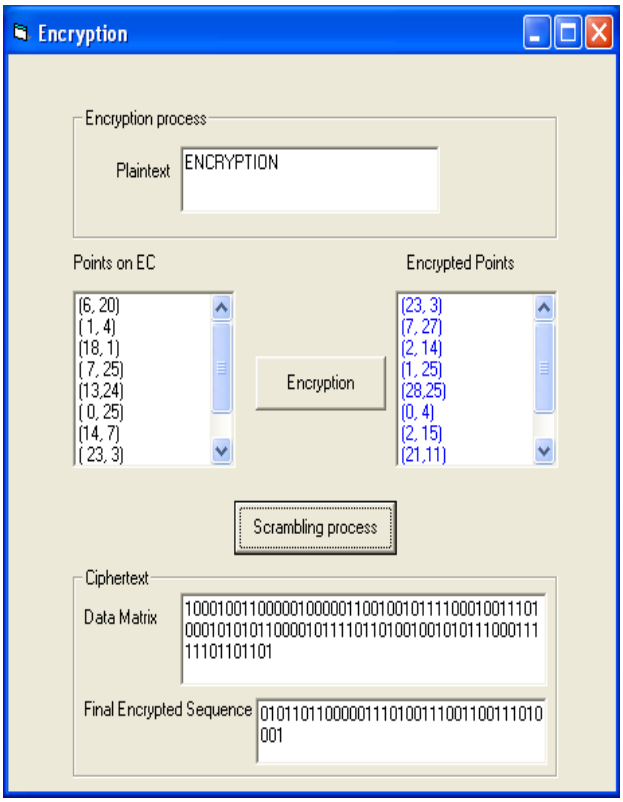


Figure 4. Encryption process

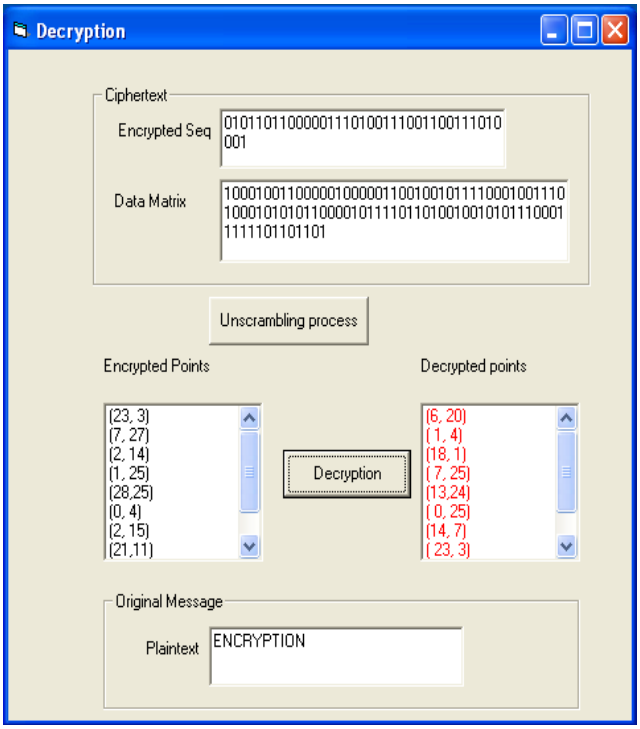


Figure 5. Decryption process

7. CONCLUSION

In this paper, we introduced the concept of cellular automata as a promising approach to enhance the security of the elliptic curve cryptosystem. By using two different levels of security, the transmitted message is much secure as compared to simple encryption method. From the above results it is clearly found that the security against few Attacks have been enhanced. Thus the proposed work of joining the elliptic curve cryptography and Cellular Automata has desirably increased the security level of the encrypted data. Our algorithm, being based on concept of CA, helps scrambling process due to rule-90. The Strength of the algorithm due to the difficulty level used in secure key generated. In fact, Cellular Automata is the strengthen method to generate strong keys. Also integration of elliptic curve cryptosystems and the concept of cellular automata has improved the security level provided by ECCCA. Therefore, it can be consider as a good alternative to some applications. In future, we are interested to extend the proposed system to image encryption and multimedia encryption.

8. REFERENCES

[1] M Shanmugasundaram and R Shanmugasundaram, "Elliptic Curve Cryptography (ECC) for Security in Mobile Communication", European Journal of Advances in Engineering and Technology, 1(2), 93-101, 2014.

[2] Moncef Amara and Amar Siad, "Elliptic Curve Cryptography and its Applications", 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), 2011.

[3] Ikshwansu Nautiyal, Madhu Sharma, "Encryption using Elliptic Curve Cryptography using Java as Implementation tool", International Journal of Advanced Research in Computer Science and Software Engineering 4 (1), pp. 620-625, 2014.

[4] MD Sadiq and Bhupalam Harish Kumar, "Efficient Cryptography using Cellular Automata Rules", International Journal of Emerging Engineering Research and Technology, Vol 3, Issue 12, 2015.

[5] Warakorn Srichavengsup and Wimol San-Um, "Data Encryption Scheme Based on Rules of Cellular Automata and Chaotic Map Function for Information Security", International Journal of Network Security, Vol.18, No.6, pp.1130-1142, 2016.

[6] F.Amounas and E.H. El Kinani, "Elliptic curve digital signature algorithm using boolean permutation based ECC", International Journal of Information & Network Security, vol. 1, no. 3, pp. 216-222, 2012.

[7] F.Amounas and E.H. El Kinani, "An efficient elliptic curve cryptography protocol based on matrices, "International Journal of Engineering Inventions, vol. 1, no. 9, pp. 49-54, 2012.

[8] F.Amounas, E.H. El Kinani and H.sadki, " An Efficient Signcryption Scheme based on The Elliptic Curve Discrete Logarithm Problem", International Journal of Information & Network Security, vol. 2, no. 3, pp. 253-259, 2013.

[9] F.Amounas, "Efficient methodology for Encrypting Amazigh Alphabet using Modified Knapsack Algorithm based ECC ", International Journal on Recent and Innovation Trends in Computing and Communication vol. 4, Issue 3, pp. 502-506, 2016.

[10] Andrej Dujella "Applications of elliptic curves in public key cryptography", Basque Center for Applied Mathematics and Universidad del Pais Vasco / Euskal HerrikoUnibertsitatea, Bilbao, 2011.

[11] Lokesh Giripunje and Sonali Nimbhorkar, "Comprehensive Security System for Mobile Network Using Elliptic Curve Cryptography over GF (p)", Vol 3, Issue 5, 2013.

[12] D. Sravana Kumar, CH. Suneetha and A. Chandrasekhar, "Encryption of data using Elliptic Curve over Finite Field", International Journal of Distributed and Parallel Systems, Vol. 3, No. 1, 2012.

[13] Sonali U. Nimbhorkar, and Dr. L. G. Malik "A Survey On Elliptic Curve Cryptography (ECC)" International Journal of Advanced Studies in Computers, Science and Engineering, vol.1 ,issue 1 pp. 1-5, 2012.

[14] M Phani Krishna Kishore, S Kanthi Kiran, B Bangaru Bhavya and S Harsha Chaitanya S, "A Novel Encryption System using Layered Cellular Automata", Proceedings of the world congress on Engineering, Vol 1, 2011.

[15] G.Shanmugasundaram, P.Thiyagarajan and S.Pavithra, "A Novel DNA Encryption System using Cellular Automata", International Journal of Security, Privacy and Trust Management, Vol 4, No 3/4, 2015.

[16] G. S. Khedkar, A.O. Amalkar and S.S.Tawani, "An Efficient Implementation of Cryptographic Algorithm Using High Speed Cellular Automata Techniques", International Journal of Engineering Research and Applications, Vol. 2, Issue 3, 2012.

[17] M. Tomassini and M. Sipper, "On the Generation of High-Quality Random Numbers by Two-Dimensional Cellular Automata", IEEE Trans. on Computers, vol. 49, No.10, pp. 1140-l151, 2000.

[18] Petre Anghelescu, SilviuIonitaand EmilSofron "Block Encryption Using Hybrid Additive Cellular Automata," Seventh International Conference on Hybrid Intelligent Systems, pp. 132- 137, 2007.

[19] F.Amounas, E.H. El Kinani, and A. Chillali, "An application of discrete algorithms in asymmetric cryptography", International Mathematical Forum, vol. 6, no. 49, pp. 2409-2418, 2011.

[20] F.Amounas and E.H. El Kinani, " Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography", International Journal of Information & Network Security, vol. 1, no. 2, pp. 54-59, 2012.

[21] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, "Implementation of Text Encryption using Elliptic Curve Cryptography", International Multi-Conference on Information Processing-2015, Procedia Computer Science 54 , pp: 73- 82, 2015.