A Novel Encryption System using Layered Cellular Automata

M Phani Krishna Kishore[1] S Kanthi Kiran[2] B Bangaru Bhavya[3] S Harsha Chaitanya S[4]

Abstract— As the technology is rapidly advancing day by day sharing of information over the internet is experiencing an explosive growth, which in turn is also posing new threats and vulnerabilities in the existing systems. The quest for more stronger and reliable methodologies to tackle the security issues is unending. In this direction a new cryptographic method is proposed in this paper based on Layered Cellular Automata (LRCA) and the strengths are analyzed in comparison with the existing systems.

Index Terms – Cellular Automata (CA), Reversible Cellular Automata (RCA), Layered Cellular Automata, Symmetric key, Encryption.

I.INTRODUCTION

Over the past two decades Cryptographic techniques have become essential part of any secure digital communication. All the cryptosystems can be classified in two types Private key systems and Public key systems. In symmetric key system both the sender and receiver use the same key to reveal the information (also called as secret key encryption). In public key system the sender and the receiver uses different key (also called as asymmetric key encryption system). Even after the paradigm shift brought by the Public key cryptosystems, the traditional symmetric key encryption has not lost its importance. Still many systems depend on private key systems.

The symmetric key systems can in turn be classified into two types namely block ciphers and stream ciphers. The block ciphers breaks the plain text into fixed length blocks and encryption is performed on one block at a time; on the other hand the stream cipher encrypts the plain text at a level of one bit/byte at a time. Generally symmetric key algorithms execute much faster than the asymmetric key algorithms. Some of the popular algorithms based on symmetric key include Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Standard (IDEA) [2]. Most of the symmetric key ciphers depend on the famous Fiestel structure.

Cellular Automata is a discrete model that consists of grids of cells in which each cell can exist in finite number of states. Every cell can change its state based on the states of neighboring cells by following a prescribed rule. Cellular Automata with its inherent properties like Parallelism, Homogeneity, and Unpredictability, as well as it being easily implementable in both software and hardware systems, has become an important tool to develop cryptographic methods. Ever since Wolfram studied the first secret key process based on Cellular Automata [9], and later by Tomassini& Perrenoud [5], many researchers had explored several possible methods based on them. Public key systems are also proposed based on the Cellular Automata [3]. Several variants of Cellular Automata like 2 dimensional (2D) and multi- dimensional Automata with different types of neighborhood systems are also studied by Tomassini & Sipper [6], and recently by seredinsky et al [4] and Peter Anghelescu et al [3]. The concepts of Reversible Cellular Automata (RCA) are also used by Xuewen et al [2], Gutwitz et al [8] and recently by Xia Xuewen et al [2] to develop cryptosystems. Recently the concepts of Multi-layered Cellular Automata (MCA) are studied by Ramin Ayanzadeh et al [1]. In this paper a new cryptographic system is proposed based on the Layered and Reversible Cellular Automata (LRCA).

The remaining part of the paper is organized as follows. In section II a detailed description of Cellular Automata and Reversible Cellular Automata are presented. In section III the proposed method is introduced. In section IV, Algorithms for both encryption and decryption are presented. A detailed example is presented that outlines the working procedure of the proposed method in section V. The proposed method is analyzed for its strengths in section VI. In section VII conclusion regarding the work is given.

II.CELLULAR AUTOMATA

A Cellular Automata is a regular lattice of cells (grids) that changes their state synchronously, according to a local update rule that specifies the new state of each cell based on the old states and its neighbours gives the global change of CA. (Figure 1)

M Phani Krishna Kishore is working as a Professor, in the Department of Information Technology, GVP College of Engineering, Visakhapatnam, Andhra Pradesh, India. (e-mail: kishorempk73@gvpce.ac.in) Phone:+918912739507 (extn: 405)

S Kanthi Kiran is working as Assistant Professor, in the Department of Information Technology, GVP College of Engineering, Visakhapatnam, Andhra Pradesh, India. (e-mail: s.kanthi.kiran@gmail.com) Phone:+918912739507 (extn: 405)

B Bangaru Bhavya pursuing Master's Degree, in the department of Information Technology, GVP College of Engineering, Visakhapatnam, Andhra Pradesh, India. (e-mail: bangarubhavya@gmail.com) Phone:+918912739507 (extn: 405)

S Harsha Chaitanya S pursuing Master's Degree, in the department of Information Technology, GVP College of Engineering, Visakhapatnam, Andhra Pradesh, India. (e-mail: sriharshachaitanya@gmail.com) Phone:+918912739507 (extn: 405)

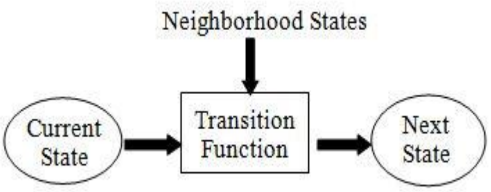

Figure 1 Updating current cell states

CA can be represented by the quadruple as, {D, K, N, f} where

D defines the dimension of CA may be 1D, 2D, 3D… (Figure 2)

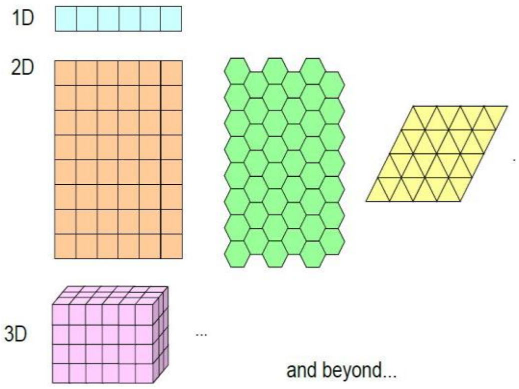

Figure 2 Dimensions of CA

K holds set of possible states of all cells in a Cellular Automata

N defines the set of neighborhood states (Figure 3)

Various neighborhood techniques are exists, in that more popularly 3neighborhood (3a), Von-Neumann (3b) and Moore neighborhoods (3c)

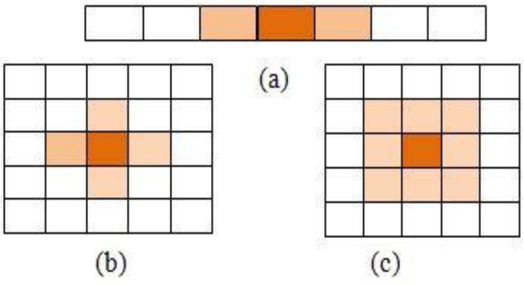

Figure 3 Neighborhood States

f is Transition function (Transition Rule).

By applying the transition rule the current state of CA moves to new state by considering the neighborhood states. In 1D CA with two neighbors 2^{2^3} rules can be generated that operates on CA. For example, consider Rule 30, which is given by

Table 1 Rule 30

Rule 30	111	110	101	100	011	010	001	000
	0	0	0	1	1	1	1	0

CAs are dynamical systems in which space and time are discrete, CAs exhibit some inherent features like parallelism, locality, simplicity, unpredictability and homogeneity thus cellular automata is naturally too fast, efficient in hardware and software implementations. There are two classes of cellular automata one is Uniform Cellular Automata and Non Uniform Cellular Automata. If all the cells obey the same rule then it is uniform cellular automata. Otherwise it is non-uniform cellular automata. Several types of boundary conditions can be considered, a CA with periodic boundary has the extreme cells are adjacent to each other. (Figure 4)

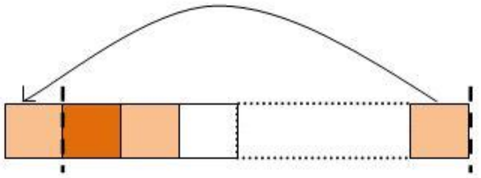

Figure 4 Periodic boundary condition

Elementary Cellular Automata

The state of all cells at time‘t’ is called configuration of CA at time ‘t’ and is denoted CA^t, the next state of the CA is denoted by CA^{t+1}. Considering the convenience to be treated by computer, many researchers only considered every cell only has two states {0, 1}. The state of a cell at the next time step is determined by the transition function along with current state of the cell and states of surrounding neighborhood cells. This phenomenon is represented as follows:

$$CA_i^{t+1} = f(C_{i-r}^t, C_{i-r+1}^t, \dots, C_{i-1}^t, C_i^t, C_{i+1}^t, \dots, C_{i+r}^t)$$

Where C_i^t means i^{th} cell at time‘t’, C_i^{t+1} means i^{th} cell at time‘t+1’, r is the neighborhood radius. Take radius as one (r=1 i.e. 3-neighborhood in the Figure (3a)) with one dimensional cellular automata then the next state of CA is represented as

$$CA_i^{t+1} = f(C_{i-1}^t, C_i^t, C_{i+1}^t)$$

Reversible Cellular Automata

By applying a rule to each cell c_i of the configuration CA_i^t a new configuration CA_i^{t+1} is obtained. This transformation can also be defined by a global transition function, which as an input takes configuration $CA^t$and results in a successive configuration CA^{t+1}. A CA is reversible if and only if the global transition function is one-to-one and hence every configuration not only has one successor but also has one predecessor.

Successor:

$$CA_i^{t+1} = f(C_{i-r}^t, C_{i-r+1}^t, \dots, C_{i-1}^t, C_i^t, C_{i+1}^t, \dots, C_{i+r}^t)$$

Predecessor:

$$CA_i^{t-1} = g(C_{i-r}^t, C_{i-r+1}^t, \dots, C_{i-1}^t, C_i^t, C_{i+1}^t, \dots, C_{i+r}^t)$$

Here f is the transition rule for moving forward and g is the transition rule for moving backward. As an example considers rules 15 and 85 are in the following way:

Table 2 Iterations/ Timesteps by Rule 15

Rule 15	111	110	101	100	011	010	001	000
	0	0	0	0	1	1	1	1
CA^t	1	0	1	1	1	0	0	0
CA^{t+1}	1	0	1	0	0	0	1	1
CA^{t+2}	0	0	1	0	1	1	1	0

Table 3 Iterations/ Timesteps by Rule 85

Rule 85	111	110	101	100	011	010	001	000
	0	1	0	1	0	1	0	1
CA^t	0	0	1	0	1	1	1	0
CA^{t+1}	1	0	1	0	0	0	1	1
CA^{t+2}	1	0	1	1	1	0	0	0

From the Table 2 and Table 3, a CA moved to n timesteps (iteration) by using one rule, another counterpart rule can be applied till the same number of timesteps to obtain the original configuration of the CA. For example, Original CA moved to next state by performing 2 iterations using the rule 15, after that by applying rule 85 on the new state of CA the original CA is reconstructed, hence the rules 15 and 85 are reversible to each other up to any number of iterations.

III.PROPOSED SYSTEM

In this paper a Layered Cellular Automata is considered where in the automata can be viewed as a system, that consists of layers, and each layer is consists of rows of 1D cellular automata. Each cell except the boundary cells is having 8 neighbors in its plane and the cells that lie on the planes other than the top and bottom are having 26 neighbors. This approach in principle invokes possibility of defining transformation functions based on the neighbors of different layers and can be of order of$2^{2^{26}}$. This may lead to analysis of a new class of CA and is much of theoretical interest.

In the proposed system (LRCA), the block encryption technique is used along with the symmetric key encryption. The text is converted into binary form and arranged in eight layers where each row is considered as a 1D CA with periodic boundary condition and with radius equal to unity. 1D rule are used for encryption on each layer.

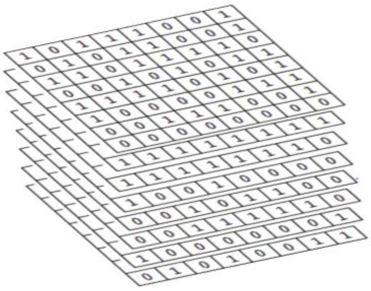

Figure 5 Layered Cellular Automata

Encryption procedure

Divide the plain text into blocks of size 4096 characters (ASCII values for each character is considered so that there in total 4096*8 bits), (padding bits are added whenever needed) and the text is converted into binary sequence and the bits are arranged into 8 layers where each layer consists of 64*64 bits. Arrange the first bits of all the characters in the first layer and second bits of all characters in the second layer and continuing this process arrange the eight bit of all the characters in the eighth layer. Then apply a CA rule set on each cell of each layer. In 1D CA, 6 reversible rules are available. In this paper 4 pairs of rules namely {15,85}, {51,51}, {170,240}, {204,204} are used, in a randomly generated order at each bit of each layer and this process is repeated for a predefined number of ways to produce the cipher bits at each cell. Again the cipher bits are converted into text by following the same process in reverse as described earlier to produce the cipher text.

Decryption procedure

The cipher text is converted back to binary form and the sequence of rules used in encryption is generated from the key the corresponding reversible rules are used in the same manner that of encryption on each cell for a predefined number of iterations, and the corresponding plain text is extracted from the binary sequence.

Pre-shared information

Both the sender and receiver shall agree on the set of rules that are to be used along with indexes created for the rules for the particular encryption. They shall also agree on the index and size in the key to be used to generate the number of iterations along with shift indicators. A random series of indexes is generated to identify the particular rule that is to be used on each cell of a layer. A shift on the sequence of rules is applied from row to row by treating the rows on the all the layers sequentially.

Key size

If only four rules are used then a random 128 bit key is generated in which subsequent 2 bits are used to identify indexes. If six rules are used then a random 192 bit key is generated in which subsequent 3 bits are used to identify indexes. In this paper a 128 bit key is used.

IV.ALGORITHM

The steps in Encryption Algorithm are as follows:

1. Divide the plain text into blocks
2. Take first block of plaintext
3. Repeat the steps from 4 to 8 until last block
4. Take each character in the block convert it into 8bit binary sequence of ASCII values
5. Arrange each character binary sequence into layers (as said above)
6. Apply the encryption ruleset on each layer to move to the next state depends upon the number of iterations)
7. Consider all the layers to form the ciphertext (as said above)
8. Store all ASCII characters to form the ciphertext.

The steps in Decryption Algorithm are as follows:

1. Divide the ciphertext into blocks
2. Take first block of ciphertext
3. Repeat the steps from 4 to 8 until last block
4. Take each character in the block convert it into 8bit binary sequence
5. Arrange each character binary sequence into layers (as said above)
6. Apply the decryption ruleset on each layer to move to the next state (depends upon the number of iterations)
7. Consider all the layers to form the plaintext (as said above)
8. Store all ASCII characters to form the plaintext.

The steps in Key generation are as follows:

1. Select the rules which are reversible
2. Index the rules for both encryption and decryption
3. Generate Random series of indexes
4. Identify rule set from random series for both encryption and decryption
5. Shifting the rules for each row for both encryption and decryption

V.EXAMPLE

Encryption Process:

Plaintext: *Cellular Automata provides parallelism*

Blocks: ||*Cellular*|| *Automat*||*a provid*||*esparal*|| *lelism00*

Plain text – *Cellular*

Table 4 plaintext

Character	ASCII value	Binary Sequence
C	67	01000011
e	101	01100101
l	108	01101100
l	108	01101100
u	117	01110101
l	108	01101100
a	97	01100001
r	114	01110010

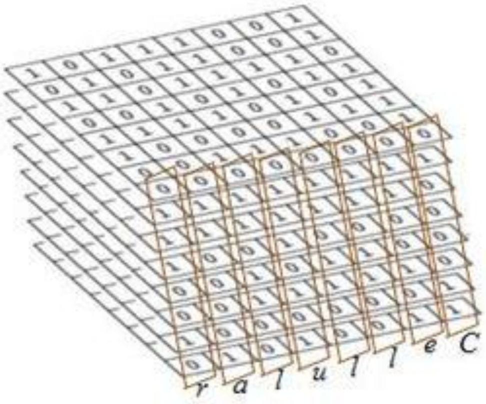

Figure 6 Layers before Encryption

After applying the encryption rule set and iterating 25 times the generated cipher text is in the figure 7.

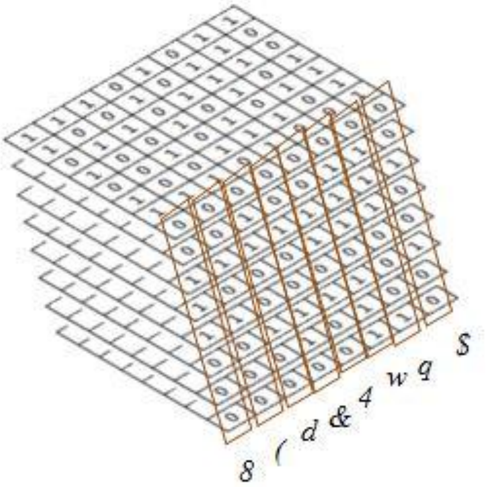

Figure 7 Layers after Encryption

Cipher text is: $qw4&d(8

Table 5 Cipher Text

Binary Sequence	ASCII value	Character
00100100	36	$
01110001	113	q
01110111	119	w
00110100	52	4
00100110	38	&
01100100	100	d
00101000	40	(
00111000	56	8

VI.ANALYSIS

Brute-force attack

Case 1:

If only pre-shared information is known, there are 2^{128} number of possible combination of keys

Case 2:

Neither pre-shared information nor the key is known then to guess the key there are $4! * 2^{128} * 120 * 2^{8}$ possibilities exists.

Proposed algorithm is compared with AES for the following parameters

1. Confusion:

Confusion refers to making the relationship between the key and cipher text as complex as possible and it is observed as the number of bits changed in the cipher text in comparison with number of bits changed in key bits. The confusion levels of proposed algorithm are compared with AES algorithm by taking plaintext of size 4k with key size 128 bit. It is observed that confusion levels obtained by the proposed algorithm are almost same as that of AES with marginal betterment.(Figure 8)

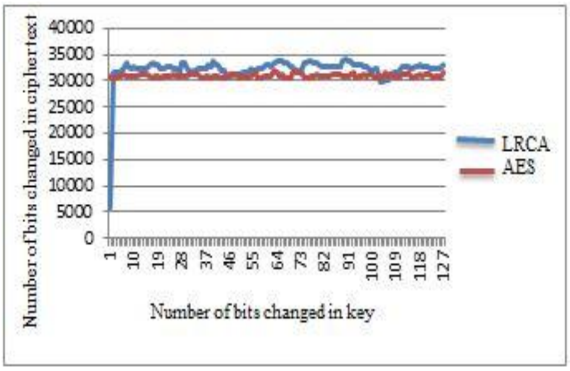

Figure 8 Comparison between LRCA and AES in the view of confusion

2. Diffusion:

Diffusion refers to making the relationship between the plain text and cipher text as complex as possible and it is observed as the number of bits changed in the cipher text in comparison with number of bits changed in plain text bits. The diffusion levels of proposed algorithm are compared with AES algorithm by taking plaintext of size 55bytes with key size 128 bit. It is observed that diffusion levels obtained by the proposed algorithm are better as compared with AES. (Figure 9)

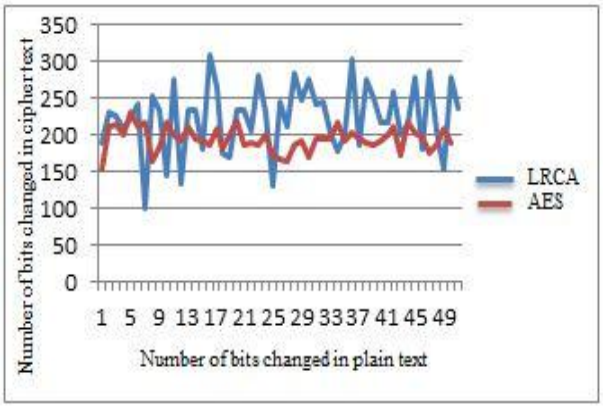

Figure 9 Comparison between LRCA and AES in the view of diffusion

3. Time Analysis:

The encryption and decryption processes taking together and observed the time taken by the LRCA and AES, time taken by the LRCA is coincide with AES when same plaintext and key used in both algorithms varying the size of the plaintext. (Figure 10)

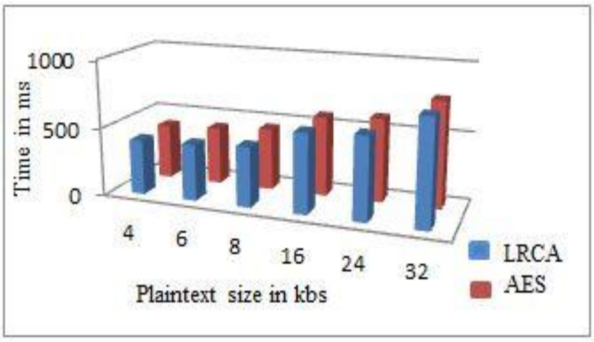

Figure 10 Comparisons between LRCA and AES

VII.CONCLUSION

In this paper the possibility of arranging text into layers of Cellular Automata, which results in a novel neighborhood system is explored, based on which a secure encryption method is developed. The proposed method is compared with AES for various parameters and is found to be on par with it.

REFERENCES

[1] RaminAyanzadeh, YaghoubMoghaddas, SaeidSetayeshi, KavehHassani and HadiGheiby Multi-Layer Cellular Automata for Generating Normal Random "*Numbers Proceedings of ICEE 2010*", May 11-13, 2010.

[2] XIA Xuewen, LI Yuanxiang, XIA Zhuliang and WANG Rong, "Data Encryption Based on Multi-Granularity Reversible Cellular Automata", *International Conference on Computational Intelligence and Security*, pp.192 -196, IEEE, 2009.

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

[4] M. Seredinsky and P. Bouvry, "Block encryption using reversible cellular automata," *ACRI 2004 The Netherlands - Amsterdam*, LNCS 3305, pp. 785–792, October 2004.

[5] M. Tomassini and M. Perrenoud, "Stream Ciphers with One- and Two-Dimensional Cellular Automata", in M. Schoenauer at al. (Eds.) *Parallel Problem Solving from Nature* - PPSN VI, LNCS 1917, Springer, 2000, pp. 722-73

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

[7] S. Nandi and Pal Chaudhuri "Analysis of Periodic and Intermediate Boundary 90/150 Cellular Automata", *IEEE Transactions on computers*, vol.45, No. 1, January 1996.

[8] J. Kari, "Cryptosystems based on reversible cellular automata", *personal communication*, 1992

[9] S. Wolfram, Cryptography with Cellular Automata, in *Advances in Cryptology: Crypto '85 Proceedings*, LNCS 218, Springer, 1986, pp. 429-432