Novel Scheme of Cryptography Based on Mixed Rule RCA and Dynamic Key Generation

[1]Oinam nickson meetei, [2] Dr.A. Kumaravel
[1]P.G Scholar, [2] Dean & Professor, Department of Computer Science & Engineering
Bharath University, Chennai, India

Abstract: **Confusion and diffusion are the core issues of robust cryptography. We try to strengthen this aspect by proposing a new cryptography scheme that support 128 bit block size. All components in our system are chosen to be based on cellular automata so as to achieve higher parallelism and to simplify in the hardware and software implementation for applications with high degree of security. The main objective of this paper is to increase the confusion and diffusion rate by novel schemes of mixing (reversible cellular automata) RCA and mix rule reversible cellular automata(MRRCA). We apply set of different bit permutation methods for this purpose**

Keywords: **Cryptographic system, MRRCA-Mix Rule Reversible CA,RCA-Reversible Cellular Automata.**

I.INTRODUCTION

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 main concern of this paper is secret key systems. In such systems the encryption key and the decryption key are same (symmetric key). The encryption process is based on generation of pseudorandom bit sequences, and CAs can be effectively used for this purpose. Cellular Automata (CA) is an organized lattice of cells and each cell have finite number of states, such as "TRUE" (T) or "FALSE" (F). The lattice dimensions can be of any finite value. Each cell within a collection of cells is called as hood. It is characterized relatively with respect to a particular cell. To start with at time t=0, a state is assigned to the cells. The new states of the cell depend on its own previous state and states of its neighborhood. The new states are assigned based on some predefined rule using mathematical calculations.

Encryption, by theory requires highly complex actions such as permuting, flipping and altering data in such a way that it is undecipherable and provides complex relationship with the original text and the keys. This relationship should be non-linear so that decryption is as tough as possible. The encryption process must be faster in time and cheaper in terms of the components involved [7]. CA provides a basic structure for highly parallel and complex operations upon which a basic encryption scheme can be built. The message encryption is done by Pseudo Random Number Generators (PRNGs) using CA. The generation of new states in One-Dimensional (1-D) CA, can be considered as a sequence of random numbers [8]. Different security schemes have been proposed including symmetric key, hash functions and public key cryptography as observed by[8]. Further as stated by Wolfram [9], Rule 30 promotes the use of large integers in the pseudo random number generation. Owing to this interesting chaotic property of the peculiar CA, Wolfram states that, this kind of CA is used as random number generator.

II.CELLULAR AUTOMATA (CA)

A cellular automata is a regular lattice of cells (grids).In states of each cell are updated synchronously at discrete time steps according to a local update rule. This local rule is a function of the present state of its neighbors. For instance, in a 2-state 3-neighborhood CA, the evolution of i^{th} cell (xi) of X can be formulated as a function of the present state of $(i-1)^{th}$, i^{th}, and $(i+1)^{th}$ cells; $xi(t+1) = f(xi-1(t), xi(t), xi+1(t))$. The vector $x(t) =(x1(t), x2(t), \ldots, xn(t))$ is called the configuration at time t of the n-cell CA. Here, f denotes the next state function. There are $2^{23} = 256$ possible different next state functions for a 2-state, 3-neighborhood CA. Each of these next state function specified by a decimal number, is called as rule number. Fig 1. Shows the updating process of current state and table 1 shows the next states computed according to rule 30,45,51,60,86,90,102,105,150,153,165,195 and 218 .The topmost row of table 1 shows all possible 8 configurations at instant t.

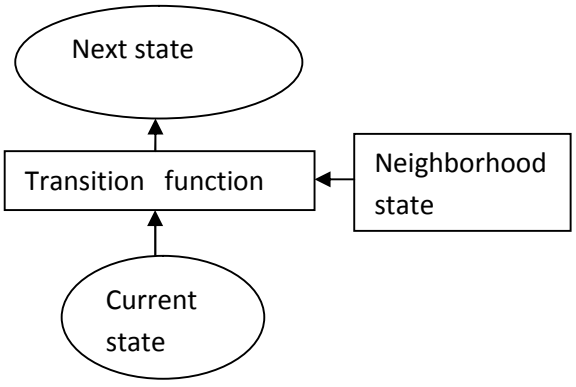

Fig 1. Process of updating current cell states.

III.REVERSIBLE CA (RCA)

Reversible cellular automata are cellular automata in which the previous configurations can be retrieved from the given current configuration(s). Our proposed algorithm uses second order reversible class CA (RCA) [11] in which, the configuration of the i^{th} state on clock cycle (t+1) is determined by the states of the n-neighborhood configuration at clock cycle t and the self configuration at (t−1) clock cycle. In reverse, one can determine the configuration at (t − 1)clock cycle from the configurations at t and (t + 1) clock cycle. For example a 3-neighborhood second order RCA can be expressed as

$xi(t + 1) = f(xi-1(t), xi(t), xi+1(t))$ xor $xi(t - 1)$;

$xi(t - 1) = f(xi-1(t), xi(t), xi+1(t))$ xor $xi(t + 1)$.

IV.PROPOSE SCHEME

A. Next state configuration of various CA rules:

The next state configuration for various rules used in our propose scheme are shown in table 1.

TABLE 1
NEXT STATE CONFIGURATION FOR CA RULES

Neigh-borhood State:	111	110	101	100	011	010	001	000	Rule No.
Next State :	0	0	0	1	1	1	1	0	30
Next State:	0	0	1	0	1	1	0	1	45
Next State:	0	0	1	1	0	0	1	1	51
Next State:	0	0	1	1	1	1	0	0	60
Next State :	0	1	0	1	0	1	1	0	86
Next State :	0	1	0	1	1	0	1	0	90
Next State:	0	1	1	0	0	1	1	0	102
Next State :	0	1	1	0	1	0	0	1	105
Next State :	1	0	0	1	0	1	1	0	150
Next State:	1	0	0	1	1	0	0	1	153
Next State :	1	0	1	0	0	1	0	1	165
Next State:	1	1	0	0	0	0	1	1	195
Next State :	1	1	0	1	1	0	1	0	218

B. Dynamic RCA key generation

RCA is CA in which the preceding pattern can be recovered from the current pattern. Our proposed algorithm utilizes RCA (second order) [2]. Given below is an example of a 3-neighborhood second order RCA

$x_i (t - 1) = f(x_{i-1}(t), (x_i(t), x_{i+1}(t)))$ XOR $x_i (t + 1)$

$x_i (t + 1) = f(x_{i-1}(t), (x_i(t), x_{i+1}(t)))$ XOR $x_i (t - 1)$

Here, the states $x_i(t + 1)$ and $x_i (t - 1)$ are denoted respectively by the terms ξ_i and y_i. ξ is obtained based on two initial patterns of (Y, X) at time steps (t - 1) and t. Then, using two successive patterns (ξ, X), the initial pattern Y can be figured out. This operation is denoted as follows [7].

ξ = RCA (Y, X); Y = RCA (ξ, X).

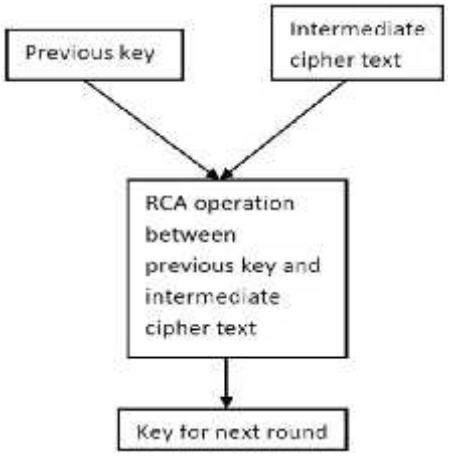

Fig 2. Dynamic RCA key schedule.

The dynamic RCA key schedule generates the next round key from the previous key pattern and corresponding cipher text for each encryption and decryption round. For each round of key generation we applied RCA operation between the previous key and the intermediate cipher text in order to increase the complexity between the previous and present key.

C. Bit permutation

The Bit-Permutation (BP) operation permutes the i^{th} bit into $((9* i) \bmod 31 + 1)^{th}$ bit. The idea behind this permutation is to place the three neighborhood bits into three different bytes. This increases the rate of diffusion and makes differential cryptanalysis difficult. Moreover implementation of this permutation is very simple can be hard-wired simply by wire-crossings.

D.Mixed rules RCA

Mixed rules RCA (MRRCA) is a RCA operation in which we applied different set of rules for each RCA operations The rules for MRRCA are selected from table 1.

E.Main algorithm

We defined a new 128 bits cryptography algorithm based on the above method as shown in fig 3. Our entire scheme comprises XOR, bit permutation, RCA, MRRCA and dynamic RCA key generation.

F.Decryption

All the method uses in our proposed scheme are reversible(XOR,RCA,MRRCA),decryption is obtained as a result of this. The cipher text is decrypt from the cipher text and the decryption keys. In reverse way using the decryption key

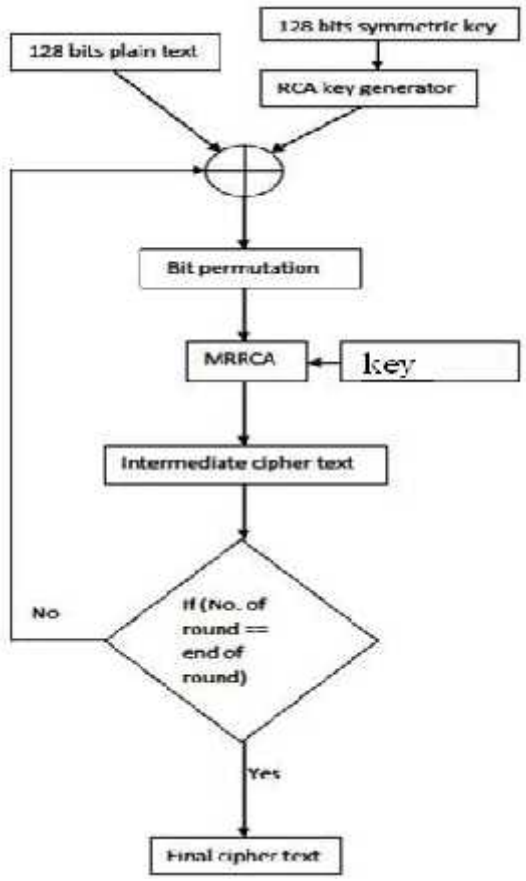

Fig 3.Proposed Encryption Scheme

Pseudocode for proposed scheme:

```
        Input: Plaintext Text, P;
        K: User 128 bits key;
        Output: Cipher Text, C;
        Intermediate cipher text: IC;
BEGIN
  READ  P;
  READ  K;
  //Apply Dynamic RCA key generator//
   IC:=P;
   Keyschedule(k) ; // Key generated by key generator for L^th round
is schedule by by Key schedule//
   For L:=1 to end of round do
        S^L:=IC ⊕ k^L;
      B^L = block permutation on S^L;
       IC:= MRRCA(B^L,k^L);
        endfor
END
```

V.PERFOMANCE ANALYSIS

The necessary requirement of good cryptography is based on the relation between the plain text, cipher text and the key. This relation is measure in term of diffusion and confusion rate. Our proposed scheme is implemented and tested and proof the necessary criteria for efficient cryptography.

A.Software Performance analysis

Table 2 tabulated the results of comparison between the execution speed of AES(optimized code) and the proposed scheme (non-optimized code) on an Intel Core i3-330M Processor 2.13 GHz in windows XP, C platform.

The implementation speed of our scheme is faster than the AES algorithm. This could be possible due to the inherited parallelism feature of CA.

Table 2
Execution Time for Block Encryption

Key size	Proposed scheme	AES
128 bit	0.91micro second	1.8micro second

B.Diffusion:

The complexity between the cipher text and the plain text is measured in terms of confusion rate y and it is observed as the number of bits changed in the cipher text in comparison with the key. The graph shown in Fig.9 was obtained by observing the number of bits change between the plain text and the cipher text for several 16 bytes input. On an average the number of bit change is 85.82 out of 128 bits, this proof the fact that the statistical

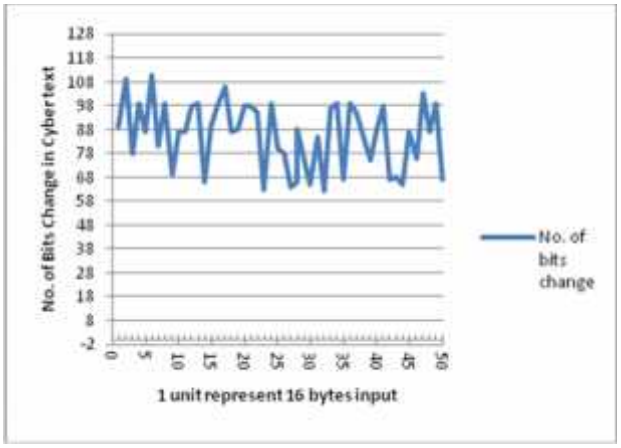

Fig.4. No. of bits change between cipher text and plain text.(Diffusion Rate)

properties of the cipher-text are pseudo-random and independent of the statistical properties of the plain text. Hence our proposal scheme further increased the diffusion level.

C.Confusion:

The complexity between the cipher text and the key is measured in terms of confusion rate y and it is observed as the number of bits changed in the cipher text in comparison with the key. The graph shown in Fig.5 was obtained by observing the number of bits change between the cipher text and the key for several 16 bytes input. On an average the number of bit change is 86.28 out of 128 bits, this proof the fact that the statistical properties of the cipher-text are pseudo-random and independent of the statistical properties of the key. Hence our proposal scheme further increased the confusion level.

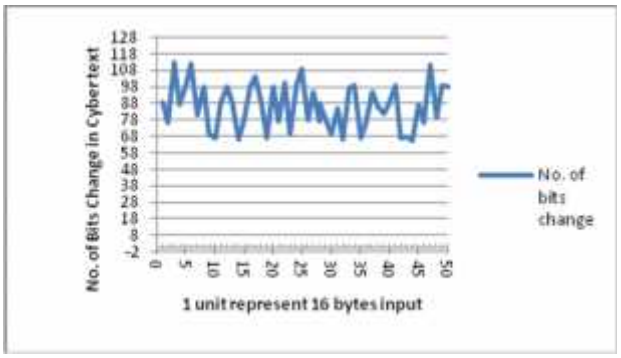

Fig.5. No. of bits change between cipher text and key (Confusion Rate).

VI.CONCLUSION

The proposed scheme is tested, we have comparable results with the standard AES. In this paper we have tried with a lightweight cryptographic algorithm based on symmetric key based on multi rule reversible cellular automata and dynamic RCA key generation. This approach increases the number of bits change between the plain text and the cipher text and between the cipher text and the encryption key as a result of this diffusion and confusion rate are increases. Moreover the previous key and the intermediate cipher has been applied for next round key generation this results in increasing the security against the Bruch force attack. Hence our proposed method further strengthens the previous scheme.

Reference

[1] N. A. Moldovyan, P. A. Moldovyan, and D.H. Sum- merville, "On software implementation of fast DDP- based ciphers," International Journal of Network Security, Vol. 4, No. 1, pp. 81-89, 2007.

[2] S. Tripathy, and S. Nandi, "Cryptosystem for lowpower devices", Turbocoding-2006, Munich, Germany Apr. 2006.

[3] S. Wolfram, "Cryptography with Cellular Automata, Crypto '85, LNCS 218, pp. 429-432Springer-Verlag, 1986.

[4] S. Wolfram, "Random sequence generation by cellula automata," Advances in Applied Maths, vol. 7no. 2, pp. 123-169, 1986.

[5] S. Wolfram, A New kind of Science, Wolfram medi Inc. 2002.

[6] B.Schneier, "Applied Cryptography," Wiley,New York, 1996.

[7] S Tripathy and S Nandi,LCASE: "Lightweight Cellular Lightweight Cellular Automata-based Symmetric-key Encryption," International Journal of Network Security, Vol.8, No.2 , Mar. 2009.

[8] Palash Sarkar, "A Brief History of Cellular automata," Journal of ACM Computing Surveys (CSUR), Volume 32 Issue 1, March 2000.

[9] S. Wolfram, "Cryptography with Cellular Automata," Crypto '85, LNCS 218, pp. 429- 432, Springer-Verlag, 1986.

[10] T. Toffoli and N. Margolus, "Invertible cellular automata: A review," Physica D, vol. 45, pp. 229-253, (reprinted with correction as of Oct. 2001).

[11] T. Toffoli, and N. Margolus, "Invertible cellular automat: A review," Physica D, vol. 45, pp. 229-253(reprinted with correction as of Oct. 2001).

[12] Franciszek Seredynski, Pascal Bouvry, and Albert Y. Zomaya. "Cellular automata Computations and secret key cryptography," *Parallel Computing Journal*, 30(5-6):753–766, 2004.

[13] F. Standaert, G. Piret, G. Rouvroy, J. Quisquater, and J. Legat, "ICEBERG : An involutional cipher efficient for block encryption in reconfigurable hard- ware," FSE '04, LNCS 3017, pp. 279-299, Springer- Verlag, 2004.

[14] N. Sklavos, N. A. Moldovyan, and O. Koufopavlou, "High speed networking: Design and implementation of two new DDP-based ciphers, Mobile Networks and Applications-MONET," Vol. 25, No. 1-2, pp. 219-231, Springer-Verlag, 2005.

[15] S. Wolfram, "Random sequence generation by cellular automata," Advances in Applied Maths, vol. 7, No. 2, pp. 123-169, 1986.