A Novel Scheme of Encryption based on Random Rules Reversible Cellular Automata

[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: **One of the issues of efficient cryptographic scheme is deal with the generation of pseudorandom number. We try to strengthen this aspect by increasing the length of block ciphers and the complexity of keys. We present a new block cipher that will support 128,192 and 256 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 key goal of our scheme is to increase the complexity by novel scheme of mixing RCA(Reversible Cellular Automata),RRRCA(Random Rules RCA) and the series of bit permutation. In this direction a new cryptographic method is proposed in this paper and the strengths are analyzed.**

Keywords**: Cryptographic system, RCA-Reversible Cellular Automata, RRRCA-Ramdom Rules Reversible CA, Pseudorandom number.**

I.INTRODUCTION

Cryptography refers to the art of protecting transmitted information from unauthorized Interception or tampering. The other side of the coin, cryptanalysis, is the art of breaking such secret ciphers and reading the information, or perhaps replacing it with different information. Sometimes the term cryptology is used to include both of these aspects. Cryptography is closely related to another part of communication theory, namely coding theory. This involves translating information of any kind (text, scientific data, pictures, sound, and so on) into a standard form for transmission, and protecting this information against distortion by random noise. There is a big difference, though, between interference by random noise, and interference by a purposeful enemy, and the techniques used are quite different.

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)... An extensive overview of currently known or emerging cryptography techniques used in both type of systems can be found in [8]. One of such a promising cryptography techniques is applying cellular automata (CAs). The main concern of this paper is secret key systems. In such systems the encryption key and the decryption key are the same. The encryption process is based on generation of pseudorandom bit sequences, and CAs can be electively used for this purpose. CAs for systems with a secrete key were first studied by Wol f ram [12].

II.CELLULAR AUTOMATA

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 [12], and later by Tomassini& Perrenoud [10], many researchers had explored several possible methods based on them.Fig.1. shows an example of CA next state generation. Here we will only consider boolean automata for which the cellular state $s \in \{0, 1\}$. The state of a cell at the next time step is determined by the current states of a surrounding neighborhood of cells. The cellular array (grid) is d-dimensional, where $d = 1, 2, 3$ is used in practice. In this paper we shall concentrate on $d = 1$ that is, one-dimensional

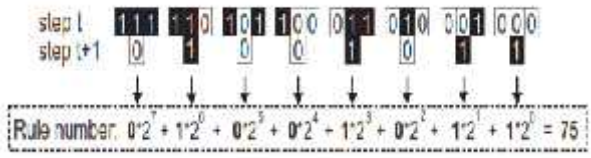


Fig.1:CA next state generation.

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) 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. Finding of Next State by CA Local Update rules

The next state of local update 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	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	1	0	0	1	105
Next State :	1	0	0	1	0	1	1	0	150
Next State :	1	0	1	0	0	1	0	1	165
Next State :	1	1	0	1	1	0	1	0	218

B. Dynamic RCA key schedule

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 .

ξ = RCA (Y, X); Y = RCA (ξ, X).

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.

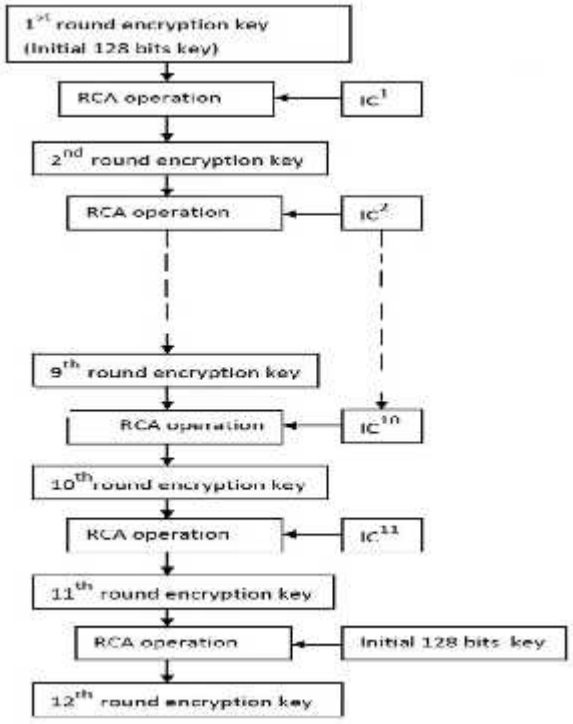


Fig 2. Dynamic RCA key schedule.

C. Bit permutation

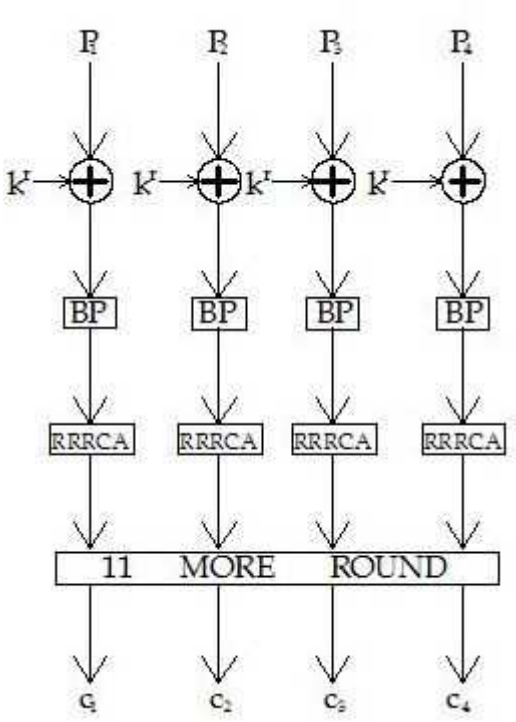
The Bit-Permutation (BP) operation permutes the i^{th} bit into $((9* i) \bmod 31 + 1)^{th}$ bit. The idea behind this permutation is to place the three neighborhood bits into three different bytes. This increases the rate of diffusion and makes differential cryptanalysis difficult. Moreover implementation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

D.Random Rules RCA

Random-rules RCA (RRRCA) is a RCA operation in which we applied random rule for each RCA operations. The rules for RRRCA 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, RRRCA and dynamic RCA key schedule.



P_i32 bit plain text k^r:encryption key for r^{th} round
$\oplus$:XOR operation C_i: final cipher text
Fig: 3.128 key bits Encryption scheme applying CA rules

V.PERFOMANCE ANALYSIS

The necessary requirement of good cryptography is based on the generation of pseudo random number. This relation is measure in term of bits changes between the plain text and the cipher text. 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.

B.Pseudorandom number.

The graph shown in Fig.4 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 80.25 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 plain text. Hence our proposal scheme further increased the diffusion level.

Table 2
Execution Time for Block Encryption

Key size	Proposed scheme	AES
128 bit	0.1.4micro second	1.8micro second

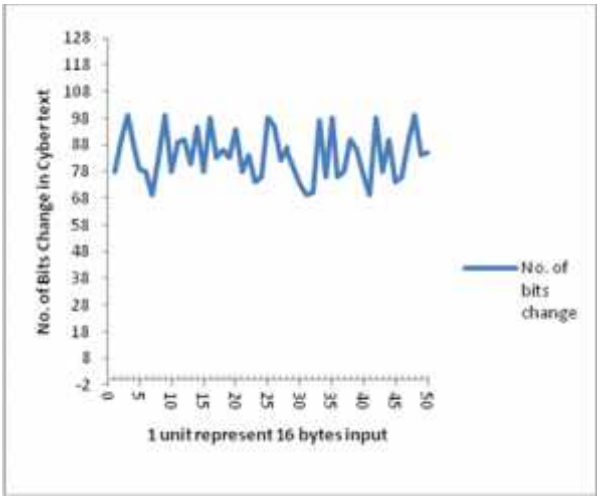


Fig.4.Bits change between cipher text and plain text.

VI. CONCLUSION

We have tested our proposed system, we have comparable result with the standard AES. In this paper we have tried a new cryptographic algorithm based on symmetric key based on random rule reversible cellular automata and dynamic RCA key schedule. This approach generate a highly pseudo random number based on the plain text and the cipher text. 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.

References

[1] N. A. Moldovyan, P. A. Moldovyan, and D.H. Summerville, "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] G.Marsaglia,Diehardhttp://stat.fsu.edu/~geo/diehard.html, 1998
[8] B. Schneier, Applied Cryptography, Wiley, New York, 1996
[9] Franciszek Seredynski, Pascal Bouvry, and Albert Y. Zomaya. Cellular automata
[10] 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. 722-731
[11] 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. 1140-1151
[12] S. Wolfram, Cryptography with Cellular Automata, in Advances in Cryptology: Crypto '85 Proceedings, LNCS 218, Springer, 1986, pp. 429-432