A Novel Algorithm for the Generation of Secret-key

V.Kamaraj[#1], K.J.Jegadish Kumar[#2]

[#1]*PG Scholar,* [#2]*Assistant Professor, SSN College of Engineering*
Chennai, India

[1]kamarajtv@gmail.com

[2]jegadishkj@ssn.edu.in

***Abstract*— This paper propose a 64-bit novel subkey generation algorithm which can also be extend to 128,192 and 256-bit keys. The main aim of our algorithm is to increase the computational efficiency by constructing a parallel architecture suitable for hardware implementation for the generation of subkeys. Further, to check the security of the proposed algorithm, a verification is made based on correlation and balance property.**

***Keywords*— Key, Cellular automata, Permutation.**

I. INTRODUCTION

In today`s computing technology there has been a need to protect sensitive information from falling into wrong hands. To achieve this, the message must be encipher by the use of key. Here the key plays a major role to convert the plaintext into ciphertext in such a way that the encrypted text should be resilient against attack.

In this paper, we propose a key generating algorithm of 64-bit key length using cellular automata theory. In future, the proposed algorithm can also be extended to 128, 192 and 256-bit keys. Our algorithm uses the simple operation such as Block Permutation and S-box. The improvement in the performance of the proposed algorithm like security and throughput solely depends on the non-linear S-boxes used to construct the encryption routine.

Here, cellular automata theory based S-boxes are used. A Cellular Automaton is an infinite, regular lattice of simple finite state machines that change their states synchronously, according to a local update rule that specifies the new state of each cell based on the old states of its neighbours.The basic features of cellular automata are highly parallelism in nature, highly complex but simple in structure. This enhances the security level and reduces the implementation cost of the cipher. The detailed description about the cellular automata can be found in [8] [13].

II. RELATED WORK

Seung - Jo Han et al (1996) discussed that the cryptosystem which is most used throughout the world for protecting information is the Data Encryption Standard (DES) which is announced by National Bureau of Standard (NBS). The author described that the DES must be stronger than the other cryptosystems in the security. But, because the process time required for cryptanalysis has lessened, because hardware technique has developed hastily, the DES may be attacked by various kinds of cryptanalysis using parallel procedure. It may be especially vulnerable to attack by the differential cryptanalysis. Hence, the DES will require strengthening to ensure cryptographic security in the days to come. So the author proposed a design of a DES-like cryptosystem called the Improved-DES. The Improved-DES is a new algorithm. They showed that the Improved-DES is stronger than the DES against differential cryptanalysis for cryptographic security. Here, they divide one data block (96 bits) into 3 sub-blocks of 32 bits and then perform different f functions on each of the 3 sub-blocks, and then increase the S1-58 of the S-boxes to 51-516, satisfying the Strict Avalanche Criterion (SAC)and the correlation coefficient (Pij). Finally they increased the key length to 112 bits. The analysis showed that the unicity distance (UD) in the Improved-DES is increased more than the DES's UD[3].

Blowfish et al (2008) describes that the Blowfish cryptosystem is a very fast and useful method, even though it was introduced over a decade ago. This encryption algorithm consists of two different modules, a subkey and S-box generation phase, and an encryption phase. A short introduction to both algorithms is given, along with a few notes about the Ciphertext Block Chaining (CBC) mode. Some common information about attacks are described, along with information about some of the people who have worked to analyze and attempt to break the blowfish. The author presents the encryption scheme clearly to demonstrate how fast the encryption scheme is compared to the sub key and S-Box generation. The secrecy of the encryption routine is explained by using several test files of different types, as well as study of the security with respect to the number of rounds [4].

Ren Fang et al (2009) described KASUMI is a block cipher with the Feistel network. The authors proposed a small and efficient hardware of the KASUMI block cipher, is the core of the 3GPP confidentiality algorithm - f8, and the 3GPP integrity algorithm - f9. In designing the hardware, they focused on optimizing the implementation of FO/FI functions that are the major components of KASUMI. They proposed three methods for this optimization: using a loop-structure in the implementation to reducing the number of the FO/FI function, realizing S7 and S9-boxes in the combinational logic and optimization of extended key's generation [5].

P.Israsena et al (2006) proposed and efficient implementation of algorithm for persistent, ubiquitous applications employing RFID devices, low-cost and secure RFIDs tags. The ICs for such systems have stringent requirements in terms of cost related to area and power consumption, creation conventional encryption unsuitable.

The author discusses the potential of employing the TEA algorithm for medium protected systems. It is found that using the implementation style wished-for, TEA based encryption hardware can be made to meet the necessities. The potential usage of low-cost secure RFID for applications such as secure device tracking is also discussed [6].

P.Israsena et al (2006) signified that the security is an important issue in any communication systems. In exacting, because of their ubiquitous character, additional security services required in wireless pervasive communication systems need efficient hardware clarifications. One of the key requirements is to reduce the circuit's size to lower the cost involved when implementing a security ASIC Core. The author discusses the potential of employing the operationally-lean XTEA-based hash function core for encryption/authentication in medium secure systems. It is found that with the parallel implementation style proposed, the core to be compact and faster [7].

III. Criteria For Good Cryptographic Function

A motivation for applying CA to realize S-boxes streams from potentially very interesting features of CA. CA are computationally universal (see e.g., [9], [10]), that means that such Boolean functions can be realized. Furthermore, CA of a given size and with their rules can potentially realize not one, but a number of S-box functions, that gives a possibility of designing much stronger cryptography systems. CA is a highly parallel system, easy in hardware implementation that results in high efficiency of CA-based cryptographic systems. The quality of S-boxes, also designed with use of CA must be verified by required properties of S-boxes as nonlinearity, autocorrelation, balanced property and strict avalanche criterion. The most important definitions and dependencies related to this issue are recalled from cryptographic literature [11], [12] and are given below

A. Correlation

Correlation defines the linear dependencies between input and output. For Cryptographic functions the correlations should be as low as possible. The formula to find the correlation between two data is given by

$$Corr\ (\rho_{xy}) = \frac{n\sum xy - \sum x \sum y}{\sqrt{\left[n\left(\sum x^2\right) - \left(\sum x\right)^2\right] \times \left[n\left(\sum y^2\right) - \left(\sum y\right)^2\right]}}$$

X – input binary sequence
Y – ouput binary sequence

B. Balanced Property

Balance (regularity) is another important criterion which should be fulfilled by a Boolean function used in ciphering (see, [6]). This means that each output bit (0 or 1) should appear an equally number of times for all possible values of inputs. The balance of a Boolean function is measured using its Hamming Weight. The formula to find out the hamming weight is defined as:

$$\mathbf{HW} = \frac{\mathbf{1}}{\mathbf{2}}(\mathbf{2^n} - \sum_{\mathbf{x \in B^n}} \hat{\mathbf{f}}(\mathbf{x})).$$

When the Hamming weight is equal to 2n-1, the algorithmic Boolean function is balanced.

IV. Algorithmic Description

The input to the key generation algorithm is 128 bit. In order to generate the random subkeys the 128 bit key is subdivided into two 64 bit keys.

A. Key Generation Algorithm

In this section two methods of generating sub keys are described. This algorithm takes 128 bits as key input and generates 64 bits sub keys for each round of encryption.

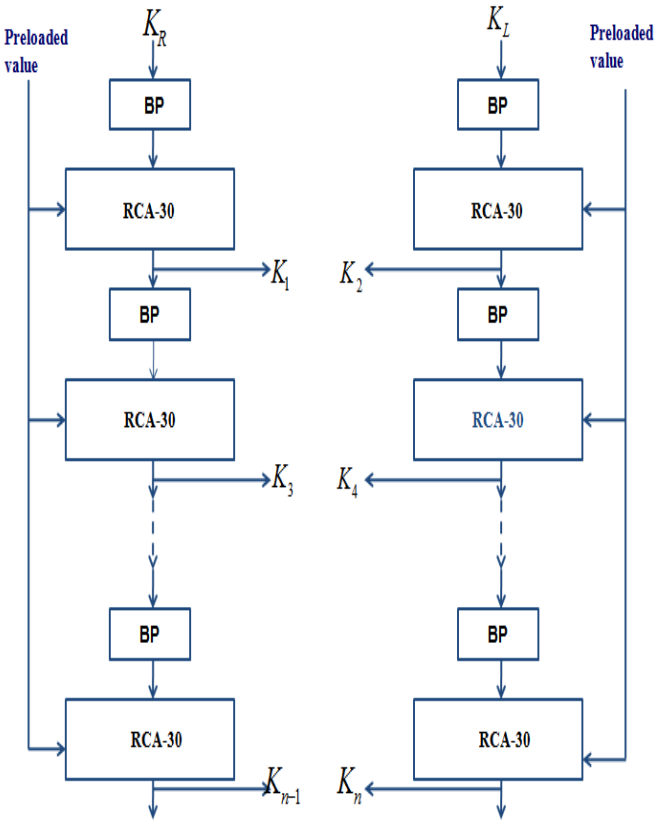

Fig. 1 Key generator representation

To achieve a good balance property and to generate random subkeys for worst case input of all 0's and 1's, we proposed a key scheduling algorithm which has preloaded value 6363636363636363. Here, the 128 bit input key is divided into two half namely KL and KR, where KL and KR are the left and right half of the input key. Both KL and KR is undergone a block permutation before it is given as an input to the RCA-45. Both the right and left hand side output of the block permutation is given to the RCA-45 as input along with the preloaded value.

V. SIMULATION RESULTS AND DISCUSSIONS

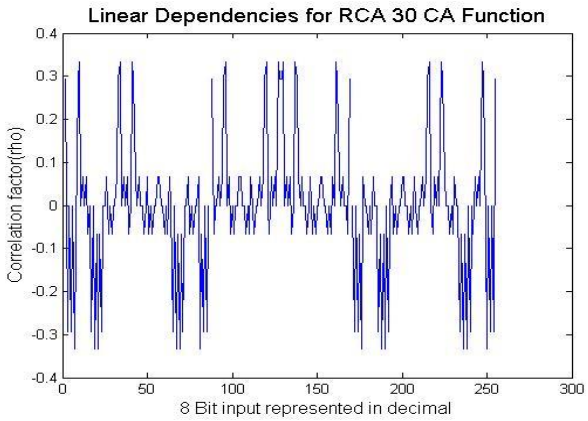

Fig. 2 Linear dependencies for RCA 30 CA function

The figure shows the I/O relationship of all combinations of 8bits for RCA 30 CA Function. From the graph we observed that 75% of value is around zero. The value around zero indicates that the output is highly non linear with the input.

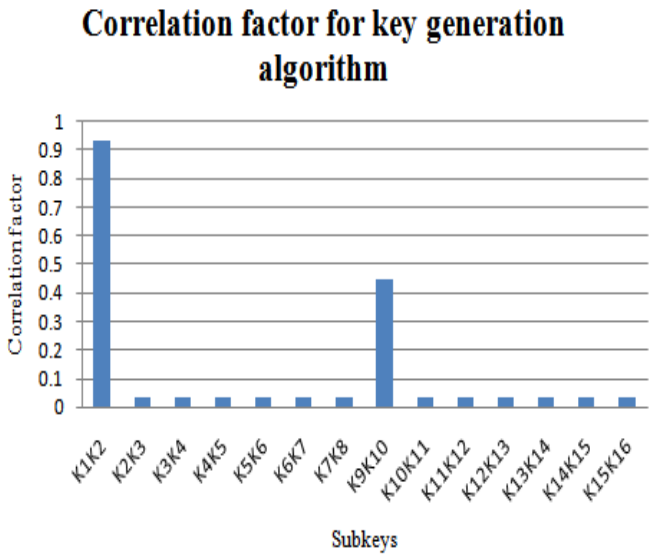

Fig. 3 Linear dependencies of subkeys for proposed algorithm

The figure shows the linear dependencies of subkeys for the proposed key schedule algorithm. The graph clearly tells that the algorithm have good non- linearity property and the values of the correlation factor is nearly around zero except at the 8^{th} and 9^{th} output , due to the parallel processing of the KL and KR.

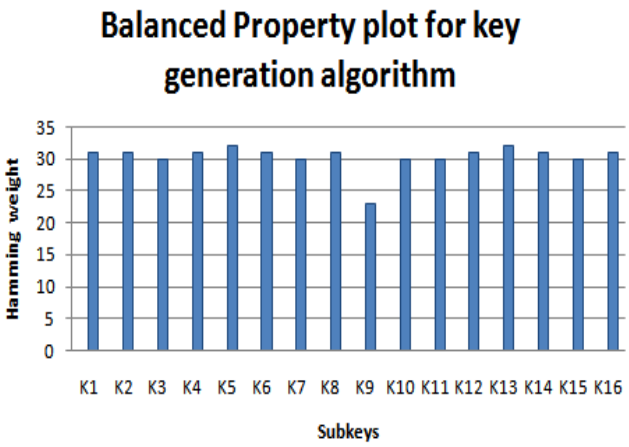

Fig. 4 Balanced property plot for proposed algorithm

The figure shows the balanced property plot for the proposed key schedule algorithm. Balanced property is nothing but the distribution of 1`s and 0`s. From the graph, we observed that the output values of each generating round keys is around 30.

VI. SECURITY ANALYSIS

The proposed algorithm is resistance to exhaustive key search attack, since the length of the key is 128 bit, a complexity of the brute force time estimation is 2^n, where n is the length of the key. The verification of non-linearity property, balanced property, and autocorrelation of the proposed algorithm states its resistance against most common attacks like linear cryptanalysis, differential cryptanalysis, algebraic attacks and correlation attacks.

VIII. CONCLUSION

In this paper we propose a novel key generation algorithm based on reversible CA. The algorithm is based on a particular class of reversible CA. One dimensional CA using radius 1 rule are used. The CA rule 30 S-box function is designed to operate over 128 bit data. Due to a huge key space a brute-force attack appears practically impossible. The algorithm can be easily extended by using larger block size. Because of the parallel nature of CA this algorithm can be implemented on a massively parallel platform. This ensures high encryption/decryption speed.

REFERENCES

1. Chandrasekran, J., Subramanyan, B., Selvanayagam. R., : Global A Chaos Based Approach for Improving Non Linearity in the S-Box Design of Symmetric Key Cryptosystems, International Conference on Computer Science and Information Technology, CCSIT 2011, Bangalore, India.(2011)
2. Bialynicki-Birula., Iwo.Bialynicka-Birula., Iwona., : Modelling Reality: How Computers Mirror Life, Oxford University Press.(2004)

3. Seung – jo Han., Heang – soo oh., Jongan park., : The improved data encryption standard (DES) algorithm,In the Spread spectrum techniques and applications proceedings, vol. 3, pp. 1310-1314.(1996)
4. Russell K. Meyers., Ahmed H. Desoky., : An Implementation of the Blowfish Cryptosystem, IEEE, pp. 346-351.(2008)
5. Ren Fang., Yan Ying – Jian., Fu Xiao –bing., : A small and efficient hardware implementation of the KASUMI, In international conference on information engineering, ICIE '09,vol.2 ,pp. 377-380.(2009)
6. P. Israsena., : Securing Ubiquitous and Low-cost RFID Using Tiny Encryption Algorithm, In Proceedings of International Symposium on Wireless Pervasive Computing.(2006)
7. P. Israsena., : On XTEA-based Encryption/Authentication Core for Wireless Pervasive Communication, Proc Int. Symp. Comm and Information Technologies, Thailand , pp. 59-62.(2006)
8.Wolfram, S., : Cryptography with cellular automata". Proceedings of Advances in Cryptology CRYPTO '85, Lecture Notes in Computer Science 218, Springer-Verlag, pp 429-438.(1985)
9. Smith, A. R III., : Simple computation-universal cellular spaces, Journal ACM, Vol. 18, pp 339 – 353.(1971)
10. Albert, J., Culik, K., II, : A simple universal cellular automaton and its one-way and totalising version, Complex Systems, Vol. 1, pp 1 – 16.(1987)
11. Adams, C., Tavares, S., : Good S-boxes are easy to find , Advance in cryptology, Proc. of CRYPTO'89, LNCS 435, pp 612 -615.(1990)
12. Clark, J., A., Jacob, J., L., Stepney, S., : The Design of S-Boxes by Simulated Annealing, New Generation Computing, Ohmsha and Springer 2005, Vol. 23, No. 3, pp 219 – 231.(2005)
13. Szaban, M, Seredynski, F., "Application of cellular automata to create S-box functions," In IEEE International Symposium on Parallel and Distributed Processing, 2008, pp 1-7

