A New Encryption and Decryption Algorithm for Block Cipher Using Cellular Automata Rules

Sirgamalla Vasantha [1], N. Shivakumar [2], Dr. D Subba Rao [3]

[1]*Department of ECE, Siddhartha Institute of Engineering and Technology, Hyderabad, India (PG Scholar)*
[2]*Department of ECE, Siddhartha Institute of Engineering and Technology, Hyderabad, India (Assistant Professor)*
[3]*Department of ECE, Siddhartha Institute of Engineering and Technology, Hyderabad, India (Head of the Department for Electronics and Communication Engineering)*

ABSTRACT

A novel cryptographic algorithm mainly depends on the cellular automata .In order to get the randomness using cellular automata concept. In this algorithm we have mainly concentrated on cellular automata module we have 8 different rules for different rounds .In previous algorithm the message and key size was 128bit, but in this project we have increased the message and key bit size to 256bit and performed 16 Rounds of operation. This increases the security. We have increased complexity by implementing different modules such as bit-permutation, inverse bit-permutation NRCA, RCA.

Keywords: RCA. NRCA, bit permutation, RBP.

INTRODUCTION

Cryptography is the art and science of keeping messages secure. the basic objective of network security and cryptographic algorithms is to communicate securely over an insecure medium. The security to the data is provided by the cryptographic algorithms. The word cryptography has come from a Greek word, which means secret writing. The message to be sent through an unreliable medium is known as plaintext, which is encrypted before sending over the medium. The encrypted message is known as cipher text, which is received at the other end of the medium and decrypted to get back the original plaintext message. Cryptographic algorithm is a mathematical function used for encryption and decryption. Cryptographic algorithms are broadly classified into three types:- i.e. symmetric algorithm, asymmetric algorithm and authentication. As per the symmetric algorithm, same key is used for encryption and decryption. In asymmetric algorithm, different keys are used for encryption and decryption. Authentication algorithms mean that the receiver should be sure about sender's identity. The cellular automata (CA) have been used since the forties of last century. It was used in many physical applications. The applications of Cellular Automata extended to fields such as biological models, image processing, language recognition, simulation, Computer architecture, cryptography etc. The Cellular Automata is also one of the modern methods used to generate binary pseudo–random a Sequences using registers. The concept of CA was initiated by J. Von Neumann and Stan Ulam in the early 1940's. He devised a CA in which each cell has a state space of 29 states, and showed that the devised CA can execute any computable operation. He studied the 1 dimensional rules of Cellular Automata. However, due to its complexity, in the 1970, the mathematician John Conway proposed his now famous game of life which received widespread interest   among   researchers.   His research was based on 2D Cellular Automata rules. Stephen Wolfram studied in much detail and showed that a family of simple one-dimensional cellular

automata rules (now famous Wolfram rules) and are capable of emulating complex behavior .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 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.

Cellular Automata has following inherent Properties

- Parallelism means that the individual cell updates are performed independently of each other. That is, we think of all of the updates being done at once

- Homogeneity means that each cell is updated according to the same rules.

In this paper a new algorithm for encryption and decryption is introduced. Here, we have mostly concentrated on securing the key, by using the concept of cellular automata. In cellular automata, we have different rules based on each rule we generate the random key for each round. By using these keys, we are performing encryption and decryption operation. In encryption, we have xormodule, bit permutation, non reversible cellular automata. In decryption, we have xormodule, reverse bit permutation, non reversible cellular automata.

The structure of the paper is as follows: Section 1 describes introduction, Section 2 describes key generation, Section 3 describes encryption and Section 4 describes decryption, Section 5 describes simulation waveforms, Section 6 describes conclusion, Section 7 describes references.

KEY GENERATION

The input key is 256 bit. It is divided into 2 blocks of 128 bit. Each block is given to RCA module. First block is further divided into sixteen 8 bit blocks then given to rule 30 then we xor k1 with k16 to get the k16 of next block. Likewise k15 is xored with old k16 to get new k15 and so on. After completion of this operation we generate the random key for second round. As for first round the input key itself serves as the round key. In a similar manner, we apply rule 45,rule 86,rule 90,rule 105,rule 150,rule 165,rule 218,rule 30,rule 45, rule 86,rule 90,rule 105,rule 150,rule 165 for the further rounds. The same procedure follows for the second block as well.
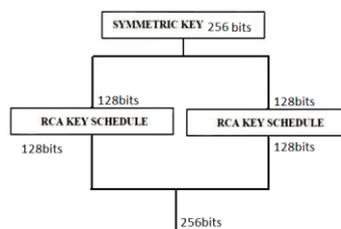

Fig1
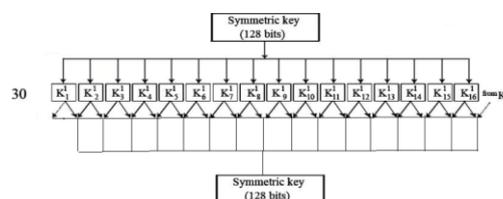
Fig2

ENCRYPTION

In encryption, we have three blocks i.e. xorblock, bit permutation, NRCA. The input to encryption is 256 bit plain text. This is divided into two 128 bit blocks. For the first block, we are passing 128 bit plaintext and 128 bit key, then the plaintext and key is further divided into sixteen 8 bit blocks. All these blocks of plaintext and key are given as input to xor block. Then we get sixteen 8 bit blocks as output from xor block. This output is clubbed such that we get 4 blocks of 32 bit. This serves as input to bit permutation block. In bit permutation the bits are arranged in different order based on the formula $(9*I \bmod 31) +1$. The permuted output from bit permutation block is divided into sixteen 8 bit blocks and given to NRCA block along with input key. One of the inputs to the NRCA is the 8 bit input key. Each bit of this 8 bit input key is applied with one particular rule. Then the above output along with bit permutation output is xored. The same operation follows for 2nd block also. These operations are performed for 15 more rounds.
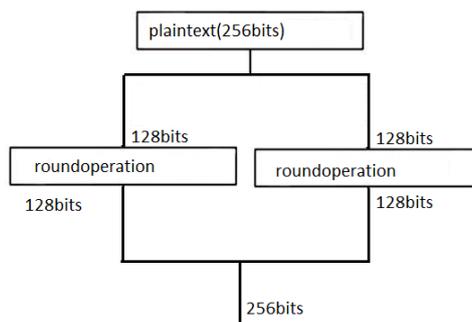
Fig3. *XOR module*
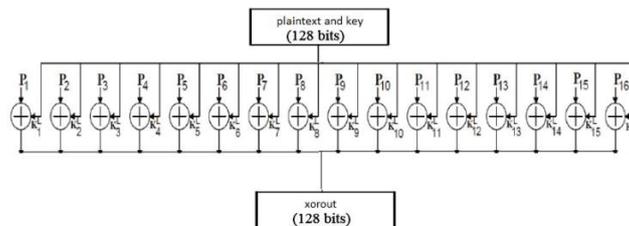
Fig4. *BIT PERMUTATION*
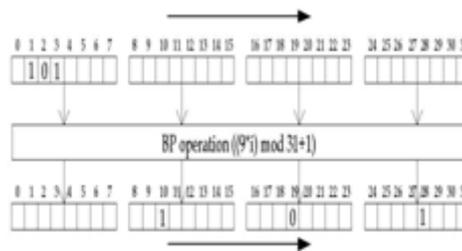
Fig5
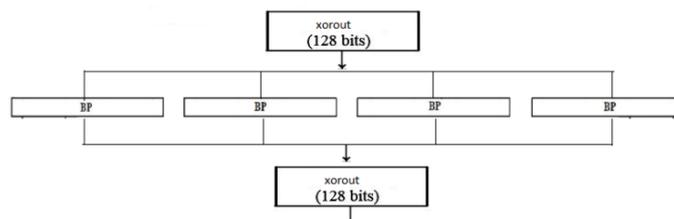
Fig6. *NRCA*
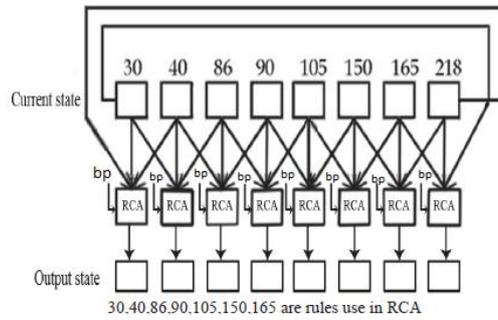
Fig7
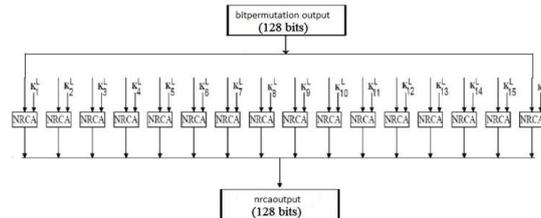
Fig8

DECRYPTION

In decryption, we have three blocks i.e. xor block, Reverse bit permutation, NRCA. The input to decryption is 256 bit cipher text. It is divided into two 128 bit blocks. For the first block, we are passing 128 bit cipher text and 128 bit key, then the cipher text and key is further divided into sixteen 8 bit blocks. All these blocks of cipher text and key are given as input to NRCA block. Then we get sixteen 8 bit blocks as output from xor block. This output is clubbed such that we get 4 blocks of 32 bit. This serves as input to reverse bit permutation block. In reverse bit permutation the bits are re organized into the original position. The output from Reverse bit permutation block is divided into sixteen 8 bit blocks and given to xor block along with input key. The same operation follows for 2nd block also. These operations are performed for 15 more rounds.
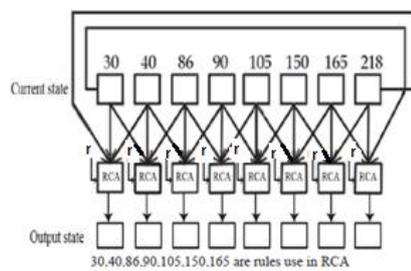

Fig9. *NRCA*
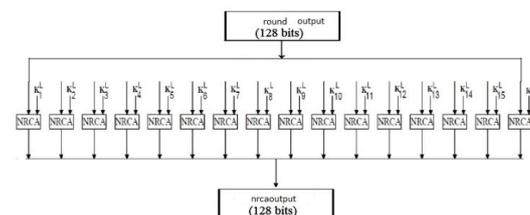
Fig10
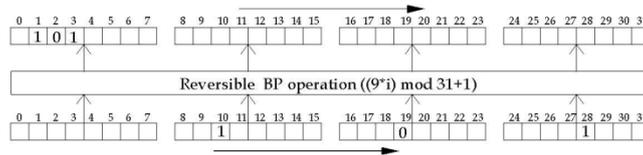
Fig11. *Reverse bit permutation*
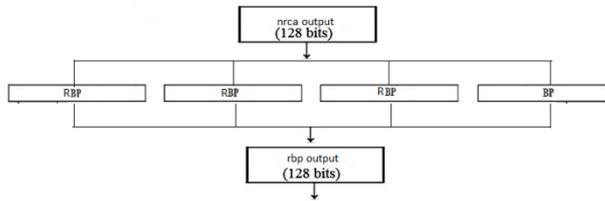

Fig12. *XORmodule*
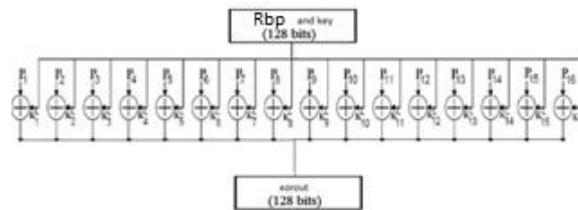
Fig13

SIMULATION WAVEFORMS

Encryption
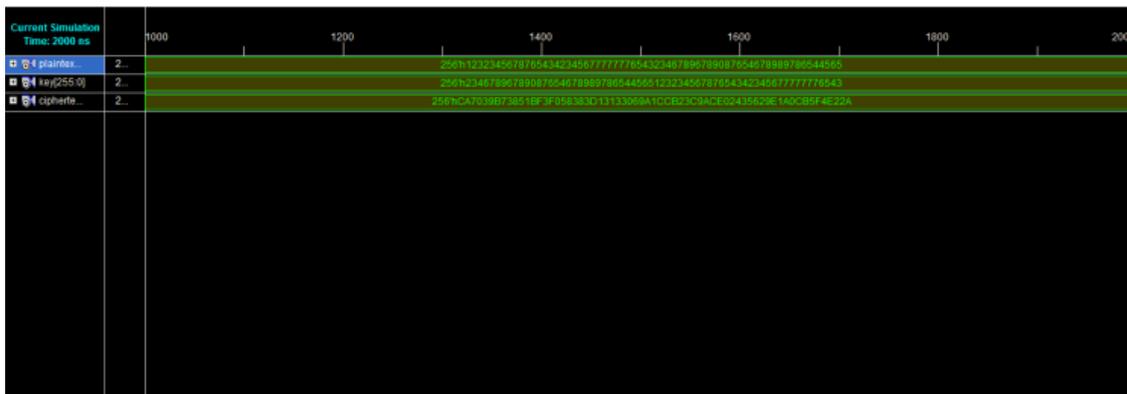
Decryption
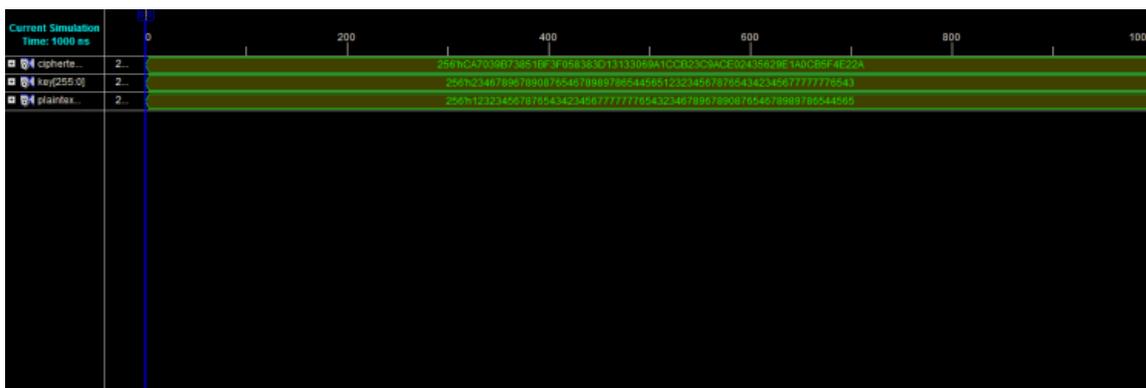
CONCULSION

In this paper, the 256 bit cellular automata encryption and decryption is designed and synthesized using vhdl codes in Xilinx ise 13.2i

REFERENCES

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

[2] S Tripathy and SIRGAMALLA VASANTHA received B.Tech degree from SRIDEVI WOMEN'S Engg College in ECE branch. M.Tech degree from SIDDHARTHA INSTITUTE OF ENGINEERING AND TECHNOLOGY with VLSI System Design IBRAHIM PATNAM.

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

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

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

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

[7] 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.

[8] 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.

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

AUTHORS' BIOGRAPHY

Sirgamalla Vasantha

Department of ECE, Siddhartha Institute of Engineering and Technology, Hyderabad, India (PG Scholar)

N. SHIVAKUMAR is an Assistant Professor at Siddhartha Institute of Engineering and Technology, Hyderabad in ECE Department. He received his B.Tech degree in Electronics and Communication Engineering from Swarna Bharathi Institute of Science and Technology, Khammam and M.Tech degree in VLSI System Design from Narayana Engineering College, Hyderabad. He attended many workshops and conferences related to VLSI and Low power VLSI. His research interest is VLSI Technology and Design, communication systems and antennas.

DR. D SUBBA RAO is a proficient Ph.D person in the research area of Image Processing from Vel-Tech University, Chennai along with initial degrees of Bachelor of Technology in Electronics and Communication Engineering (ECE) from Dr. S G I E T, Markapur and Master of Technology in Embedded Systems from SRM University, Chennai. He has 13 years of teaching experience and has published 12 Papers in International Journals, 2 Papers in National Journals and has been noted under 4 International Conferences. He has a fellowship of The Institution of Electronics and Telecommunication Engineers (IETE) along with a Life time membership of Indian Society for Technical Education (ISTE). He is currently bounded as an Associate Professor and is being chaired as Head of the Department for Electronics and Communication Engineering discipline at Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, Hyderabad.