MULTILAYERED CRYPTOGRAPHIC ALGORITHM FOR THE SECURITY ENHANCEMENT OF INFORMATION

Dr.G.Kameswari[1],Y.Amrutha[2],T.Pranathi[3],T.Jyothsna[4],R.Sudheer[5]
Associate Proffessor[1],Students[2,3,4,5] Electronics and Communication Engineering
N.B.K.R Institute of Science and Technology, Andhra Pradesh, India

Abstract: The increasing need for protecting data communication in computer networks has led to development of several cryptography algorithms. The Advanced Encryption Standard (AES) is a computer security standard issued by the National Institute of Standards and Technology (NIST) intended for protecting electronic data. The AES cryptography algorithm can be used to encrypt/decrypt blocks of 128 bits and is capable of using cipher keys of 128 bits wide (AES128).

This paper represents the security enhancement of using the multilayer linear feedback shift register (LFSR) cryptographic technique in order to overcome data hacking. A hardware implementation of the AES128 encryption algorithm was proposed. A unique feature of the proposed pipelined design is that round keys, which are consumed during different iterations of encryption, are generated in parallel with the encryption process.

Keywords: Cryptography, Encryption, LFSR, AES, Pipelined

I INTRODUCTION

In today's world, hacking has become a great problem which causes the loss of information during the process of transmitting the data. This hacking creates a sense of insecurity among the users who are transmitting the data. Over the years in order to protect the data security we are inhibiting various types of algorithms, out of which the most familiar is Cryptography. Through centuries Cryptography has an interesting history which helps us to understand the encryption and decryption process in detail. Cryptography is a study of science that deals with secret writing. Cryptography provides data integrity usually means avoiding unintended users to get the information. For symmetric cryptography only one key is used in both the process of encryption and decryption whereas in asymmetric cryptography different type of keys are used. AES is short for Advanced Encryption Standard and is a United States encryption standard defined in Federal Information Processing Standard (FIPS). AES is a symmetric encryption algorithm processing data in block of 128 bits. A bit can take the values zero and one, in effect a binary digit with two possible values as opposed to decimal digits, which can take one of 10 values. Under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for security is the key.

II LITERATURE SURVEY

[1] Ritu Tripathi, Sanjat Agarwal proposed that symmetric Key Cryptography, Asymmetric Key Cryptography uses two separate keys to prevent any unethical access to the data. The public key remains public and the private key is not shared. Moreover, the use of Digital Signatures in case of Asymmetric Key Cryptography provides high data confidentiality and non-repudiation.

[2] Mitali, Vijay Kumar, Arvind Sharma proposed the classical cryptography approach as well the modern ones. Cryptography along with cryptanalysis are very useful tools that make a huge difference and as such should be used with the utmost care.

[3] Babitha P.K, Thushara T, Dechakka M. P , proposed that there is a simulation problem for long bit LFSR when it is targeting to FPGA for rapid prototyping development. Definitely n bit LFSR with maximum length feedback polynomial will generate large sequence which is more secure than other but because of simulation difficulties modification in long bit LFSR needed.

[4] Dr.A.Albert Raj , Dr.Beno , R.Jaisakthi proposed that, The first layer and second layer of cryptography are completed with the help of the LFSR cryptographic technique. The ciphertext for the LFSR cryptography is generated.The work focussed on the design of effective single-layered cryptography as well as multilayer cryptography using the LFSR cryptographic technique**.**

III ADVANCED ENCRYPTION STANDARD

AES is a popular and efficient algorithm that is used in cryptography. It is a specification for the encryption of electronic data. AES is a symmetric encryption algorithm processing data in block of 128 bits. A bit can take the values zero and one, in effect a binary digit with two possible values as opposed to decimal digits, which can take one of 10 values. Under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. . AES may configured to use different key-lengths, the standard defines 3 lengths and the resulting algorithms are named AES-128, AES-192 and AES-256 respectively to indicate the length in bits of the key. Each additional bit in the key effectively doubles the strength of the algorithm, when defined as the time necessary for an attacker to stage a brute force attack, i.e. an exhaustive search of all possible key combinations in order to find the right one.

AES is the name of the standard, and the algorithm described is a variant of '**Rijndael'**. However, in practice the algorithm is also referred to as "AES".

A. Existing AES Algorithm:

Rijndael algorithm consists of encryption, decryption and key schedule algorithm. The main operations of the encryption algorithm among the three parts of Rijndael algorithm include: bytes substitution (Sub Bytes), the row shift (Shift Rows), column mixing (Mix Columns), and the round key adding (Add Round Key).

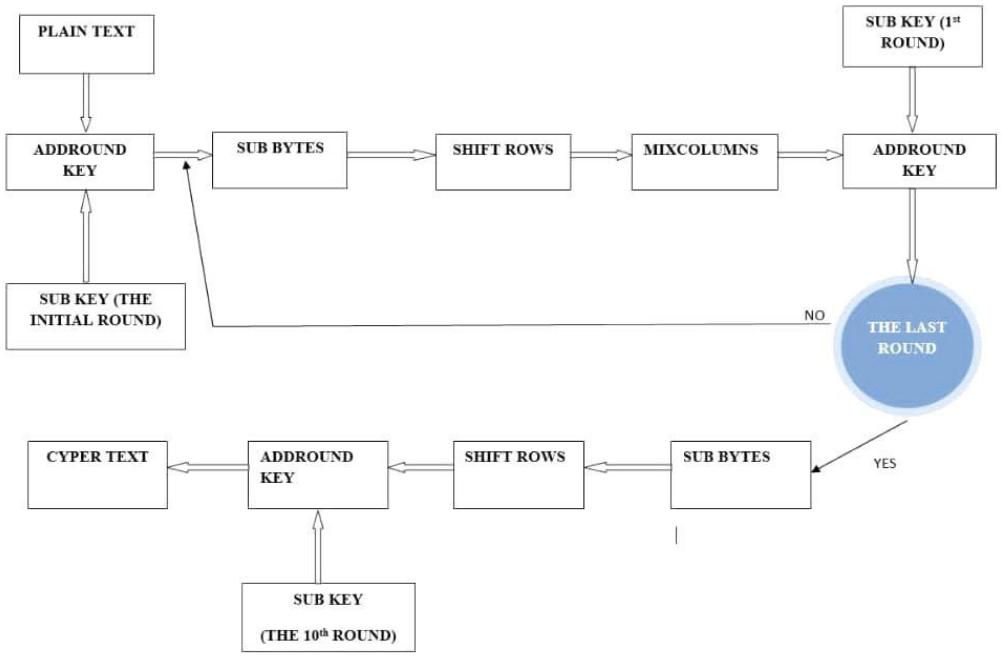

Figure 1: Basic AES Algorithm

Encryption algorithm processes Nr+1 rounds of transformation of the plaintext for the cipher text. The value of Nr in AES algorithm whose packet length is 128 bits should be 10, 12, or 14 respectively, corresponding to the key length of 128,192,256 bits. In this paper, only the (AES-128) encryption scheme with 128-bit keys is considered.

- The existing method has the following disadvantages:

i. When some of the bits in both plain text and cipher text are known then it would be very easy to hack the data.
ii. Security is very less.

B. Proposed AES Algorithm:

The AES encryption algorithm can be divided into two parts, the key schedule and round transformation. Key schedule consists of two modules: key expansion and round key selection. Key expansion means mapping Nk bits initial key to the so-called expanded key, while the round key selection selects Nb bits of round key from the expanded key module. Round Transformation involves four modules by Byte Substitution, Byte Rotation, Mix Column and Add Round Key.

Take the independent and reversible bytes substitution operation of S-box as example. Firstly, the state matrix is divided into four columns. And then byte replacement is achieved by the operation of look-up table.

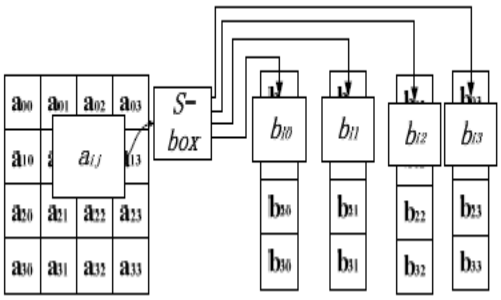

Figure2: Bytes segmentation and replacement processing

Therefore, the original 128-bit input of plaintext and key will be replaced with four consecutive 32-bit input sequences respectively. In order to decrease the output ports, four continuous 32-bit cipher text sequences have taken place of the original 128-bit output by adding a clock controller. The improved structure is also divided into these two major processes. The initial key will be sent to the two modules: Key expansion and Key selection, while the plaintext is to be sent

to the round transformation after the round key is selected. But the operand of data transmission is turned into a 32-bit unit. The function of Mix Column can be achieved. It is a block diagram for the introduction of pipelining technology used in the round transformation.

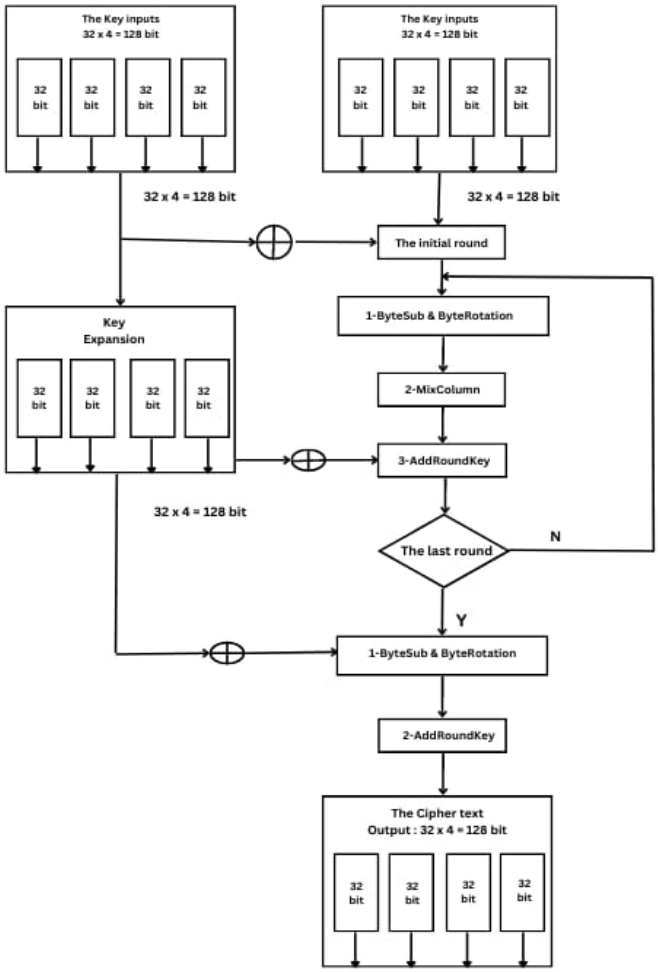

Figure3: The new improved structure of AES algorithm

The function of Mix column can be achieved. It is a block diagram for the introduction of pipelining technology used in the round transformation. In the process of pipelining, the 128-bit data is divided into four consecutive 32-bit packets that take round transformation independently. The operation of the above four groups of data can be realized in pipelining technology. The operation of the above four groups of data can be realized in pipelining technology. In brief, it can be described as follow: store the unprocessed data in the 128-bit register, and control the clock for re-starting the 128-bit register to read the new data when the four group's operations have been overcome. Thus the 128-bit round-operating unit has been transformed into four 32-bit round-operating elements. The internal pipelining processing should be implemented during the whole nine intermediate Round Transformations of the four packets before achieving the 128-bit cipher text.

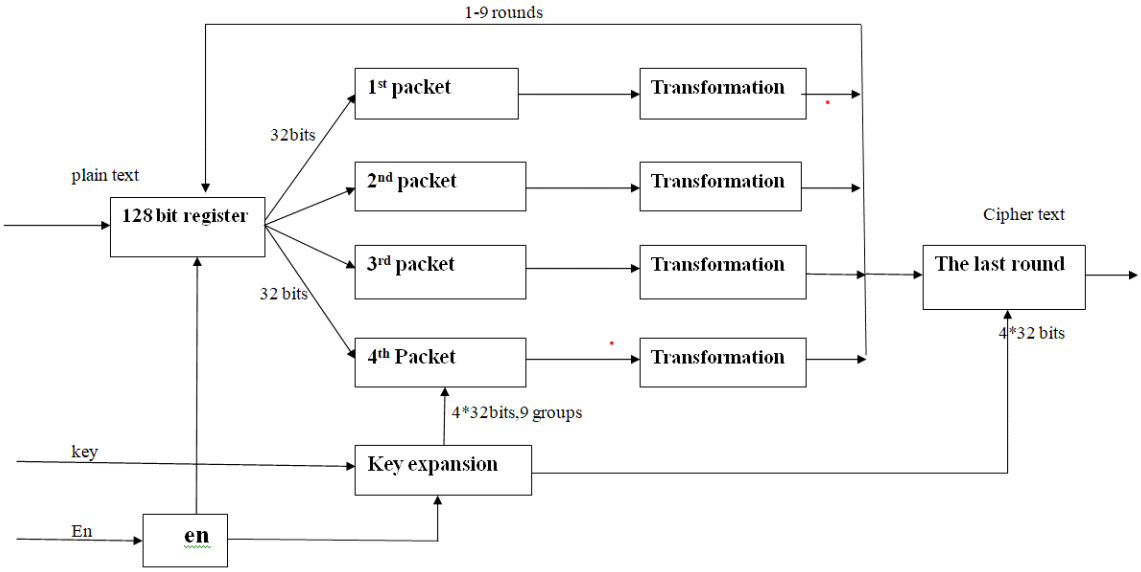

Figure4: The round processing with pipeline technology

III. STIMULATION:

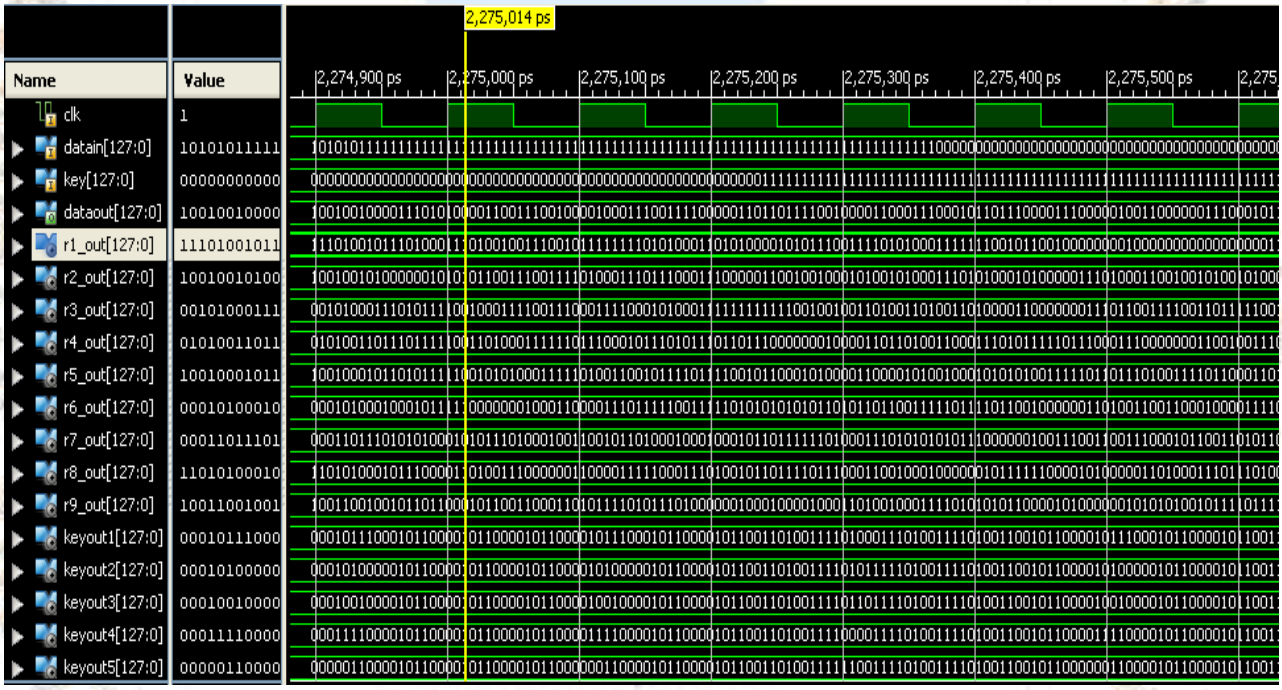

Figure5: Stimulation for AES

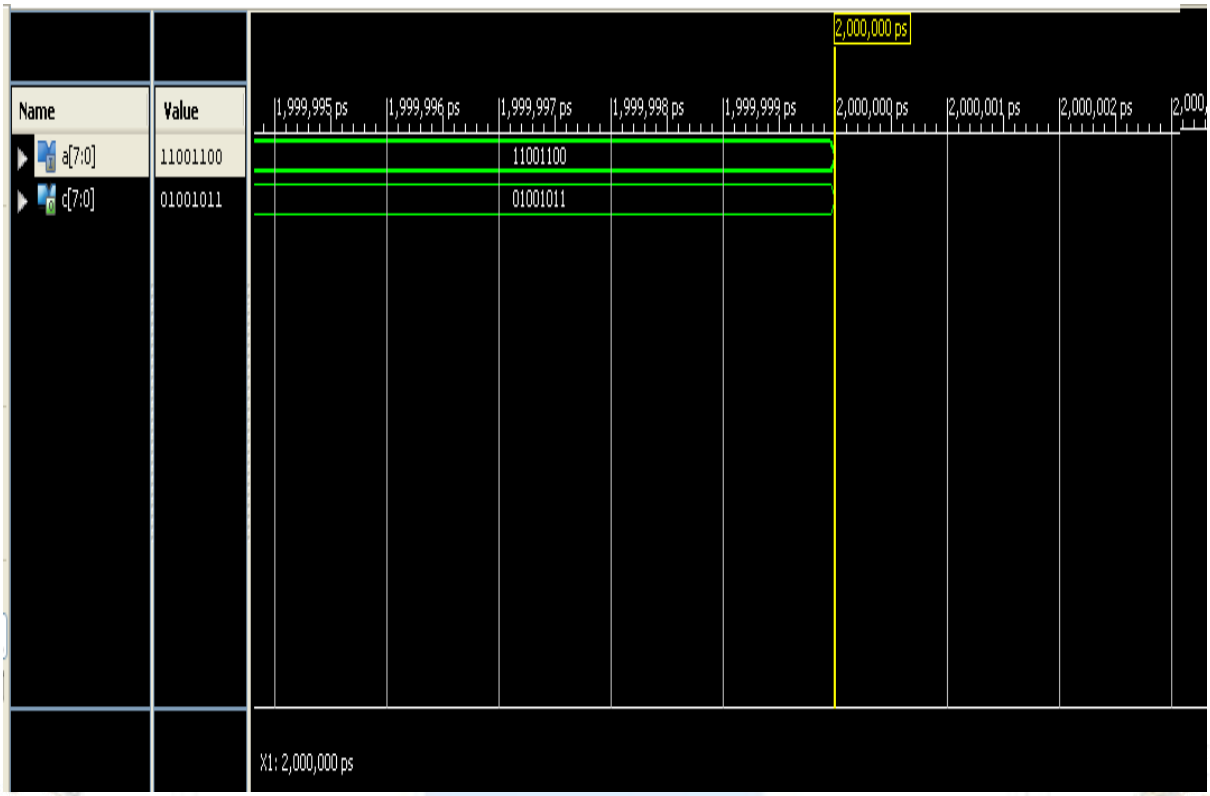

Figure6: AES with S box

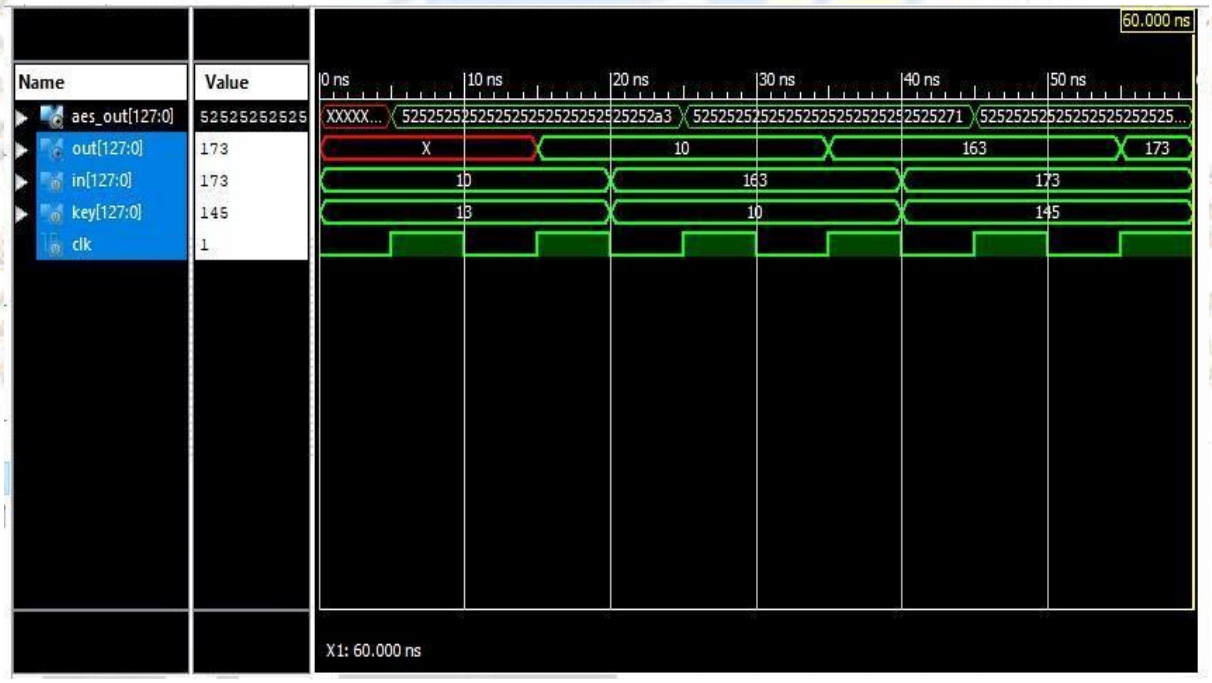

Figure7: Both AES and DES without S-box

Comparison factors	Total Availability	AES with S-Box	DES with S-Box	AES & DES without S-Box
AREA	84,352	27,789	32,281	1,872
TOTAL DELAY	-	3.793ns	74.51ns	3.874ns
TOTAL TIME	-	177.36sec	247.75sec	11.97sec

Figure8: Comparison table of different factors

IV.CONCLUSION:

A FPGA implementation of area-optimized AES algorithm which meets the actual application is proposed in this paper. After being coded with VHDL, the waveform simulation of the new algorithm was taken in the Model Sim SE PLUS 6.0 and Quartus7.2 platform. Ultimately, a synthesis simulation of the new algorithm has been done. The result shows that the design with the pipelining technology and special data transmission mode can optimize the chip area effectively. This design reduces power consumption to some extent, the power consumption is directly related to the chip area. Therefore the encryption device implemented in this method can meet some practical applications. As the S-box is implemented by Look Up Table in this design, the chip area and power can still be optimized. So the future work should focus on the implementation mode of S-box. Mathematics in Galois field can accomplish the bytes substitution of the AES algorithm, which could be another idea of further research.

V. REFERENCES:

[1]J.Yang, J.Ding, N.Li and Y.X.Guo, "FPGA-based design and implementation of reduced AES algorithm" IEEE Inter.Conf. Chal Envir Sci Com Engine(CESCE).,Vol.02, Issue.5-6, pp.67-70, Jun 2010.

[2] A.M.Deshpande , M.S.Deshpande and D.N.Kayatanavar,"FPGA Implementation of AES Encryption and Decryption"IEEE Inter.Conf.Cont,Auto,Com,andEner.,vol.01,issue04, pp.1-6,Jun.2009.

[3]Hiremath.S. and Suma.M.S.,"Advanced Encryption Standard Implemented on FPGA" IEEE Inter.Conf. Comp Elec Engin.(IECEE),vol.02,issue.28,pp.656-660,Dec.2009.

[4]Alessandro Cilardo "Exploring the Potential of Threshold Logic for Cryptography-Related Operations" In IEEE Transactions On Computers, Vol. 60, No. 4, (April 2011).

[5]Babitha P. K, Thushara T, Dechakka M. P. "FPGA based N-bit LFSR to generate random sequence number" in International Journal of Engineering Research and General ScienceVolume 3, Issue 3, Part- 2 , May-June, 2015, ISSN 2091-2730.

6]Divya Jenifer D' Souza, Minu P Abraham "A multilayered Secure for Transmission of Sensitive Information based on Steganalysis" in ELSEIVER, Procedia computer science 78 (2016).

[7]HuiXua, Xiaojun Tonga, Xianwen Menga, "An efficient chaos pseudo-random number generator applied to video encryption" in ELSEIVER, OPTIK 127 (2016).

[8]IrithPomeranz "Computing Seeds for LFSR-Based Test Generation From Nontest Cubes" in IEEE transactions on very large scale integration (vlsi) systems, vol. 24, no. 6, june 2016.