Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 540 – 547

Procedia
Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

Hardware Efficient Parallel Substitution Box for Block Ciphers with Static and Dynamic Properties

Jithendra.K.B[a,*], Shahana.T.K[b]

[a] *Dept. of ECE, College of Engineering, Vadakara,Kerala-673105,INDIA*
[b] *School of Engineering, Cochin University of Science and Technology, Kochi-682022, INDIA*

Abstract

Security aspects in communication systems are becoming more and more significant day by day. New methods for improved security are to be introduced since the security attacks also forms new shapes and expressions. Generally the security of a hardware system is directly proportional to the hardware complexity. It is a challenge to enhance or at least maintain the security level with reduced hardware complexity. In this paper an attempt is made to design a part of secure communication system, diverting from the conventional methods. This paper focus on hardware efficient design of Substitution Box (S Box), as S Box is the most significant part of a block cipher. The proposed design incorporates the concept of both static and dynamic S Boxes.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

*Keywords:*Block Cipher; S Box; Nonlinearity; Confusion; Diffusion; LFSR; Security; Hardware Complexity

1. Introduction

Substitution Box is the heart of a Block Cipher in which the process substitution is done, introduced by Shannon[1]. A message or a part of it is substituted by some other letters or bits. Now the substituted bits are processed instead of the original message. This process kept on continuing until the original message becomes really hidden so that no cryptanalysis can recover the original message. The decryption of the ciphered message is done just by reversing the process that used to encrypt the message.

* Corresponding author. Tel.: +91-944-747-432.
E-mail address: jithendrakb@yahoo.com

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.02.085

Security is the most important aspect of any crypto system. It is proved that nonlinearity contributes significantly to security. Since S Box is the only non linear part of the Block Ciphers, it plays the most important role in making the system secure. The cryptographic strength and resistance to cryptanalysis of block ciphers directly depends on the properties of S Box. Weakness of S Box leads to information or/ and power leakage. An S Box can be static or dynamic in nature. In static S Boxes, the data to be substituted is fixed as in the case of AES. In dynamic S Boxes like Blow fish or Two fish, the substitution data is generated at run time.

A new S Box is introduced here with lesser hardware complexity, but at the same time difficult to cryptanalyze. The higher security level is achieved with the introduction of additional key bits. The new design combines the properties of both static and dynamic S Boxes. Both confusion and key based diffusion are introduced within the S Box to get the expected results.

The paper is organized as follows: Section 2 mentions the functioning of conventional S Box and the properties expected. Since AES is the most widely used block cipher, focus is given to AES S Box. Section 3 describes the architecture and functioning of the proposed S Box. Decryption process which is slightly different from that of the conventional S Box of AES is also mentioned. Section 4 demonstrates the experimental results and verifies that the properties required for S Box are achieved with the proposed design. The security enhancement and resistance achieved towards both linear and differential cryptanalysis with the proposed design are also detailed. Section 5 shows the synthesis report and compares the hardware complexity of the proposed S Box with that of the conventional design. Section 6 concludes the paper.

2. Conventional S Box and properties

In conventional S Box, designed for the most widely used block cipher AES, the total number of message bits is split into a sequence of bits groups, each with 8 bits. In the substitution process, the input byte will be substituted by another byte from a look-up table. The look-up table consists of 256 data bytes so that there is a one to one mapping between any input and the substituted data[2]. The 8 bit message is split into upper 4 bits and lower 4bits. The data in the location pointed by the upper and lower nibbles is substituted for the original data. The same procedure is used for reverse substitution in decryption process. Properties requires for a good S Box are given below.

- *Nonlinearity:* When there are linear relations between input and output vectors, simple mathematics can easily find the mapping. So input to output nonlinear mapping is an essential requirement for a good S Box. This property safeguards the S Box from attacks.
- *Bijection:* For an $n \times n$ S Box, Bijection requires each data to be substituted by a unique data[3].
- *Balance:* When the truth table of a function carries equal number of zeros and ones, then the function is said to be balanced. An S Box S:$\{0,1\}^n \rightarrow \{0,1\}^m$is balanced if and only when all the m output columns are balanced.
- *Bit independent criteria or Correlation Immunity:* To satisfy this criterion, the output bits should act independently from each other. That means there should not be any statistical dependencies between output bits of the output vectors[3,4].
- *Completeness:* A Boolean function f: $\{0,1\}^m \rightarrow \{0,1\}$ is complete if its output depends on all input bits. For an S Box to be complete each bit of output should be a function of all bits of input.
- *Strict Avalanche Criteria (SAC):* The Strict Avalanche Criteria (SAC) was introduced by Webster and Tavares[5]. The concept behind this criterion is, if there is a slight change in the input vector, there should be a significant change in the output vector. If a function is to satisfy SAC, whenever a single input bit is complemented the output vector should change with a probability of one half. The purpose here is to introduce maximum confusion.
- *Extended Properties- Static and Dynamic:* Dawson and Tavares[6] proposed an extended set of desirable properties of S Boxes using information theory and previous works. S Boxes can be viewed in two ways: static and dynamic. In static view, the input and output vectors are considered to be static. On the contrary, in dynamic view changes happening in input and output vectors are correlated. Sivabalan et al.[7] proposed their own extended criteria. This proposes the design criteria at multiple bits level. The reduction in uncertainty due to the dependency between output bits and input bits or one or more output bits and the rest of the output bits are focused here. The information leakage is classified as Static Input Output Information leakage – SL[I,O],

Dynamic Input Output Information leakage – DL[I,O] and Dynamic Output Output Information leakage – DL[O,O].

3. New Design: Hardware Efficient S Box

Achieving reduced hardware complexity with enhanced security level is always a tough task. The new S Box design is carried out with the same intension. The approaches used here are:

- Increase the key size to enhance the security.
- Instead of conventional 1 to 1 substitution (Bijection), here 1 to p substitution is suggested where p is decided by the hardware.
- Reduced number and size of data stored in LUTs for substitution, which reduces the hardware complexity.
- Key based permutation to resist both linear and differential cryptanalysis.

Fig. 1. represents the block diagram of the new design. Here block B deals with substitution of data while block A and C perform additional operations to provide better security. Block D acts as control element which generates and applies random key bits in order to control the operation and enhance the uncertainty. Fig. 2. shows the proposed implementation of block B where substitution is carried out. Here the n bit message is divided into two $n/2$ bit segments. Each $n/2$ bit message is connected with one of the two Data banks, each having m number of Look Up Tables (LUT). The trade-off between randomness of substitution and hardware complexity depends on the value of m. Each LUT carries $2^{n/2}$ number of $n/2$ bit data for substitution. Each $n/2$ bit message can now be substituted by any of the $n/2$ bit data residing in the connected Data bank. How the message bits are connected with the LUTs in the data banks is shown in Fig. 2.

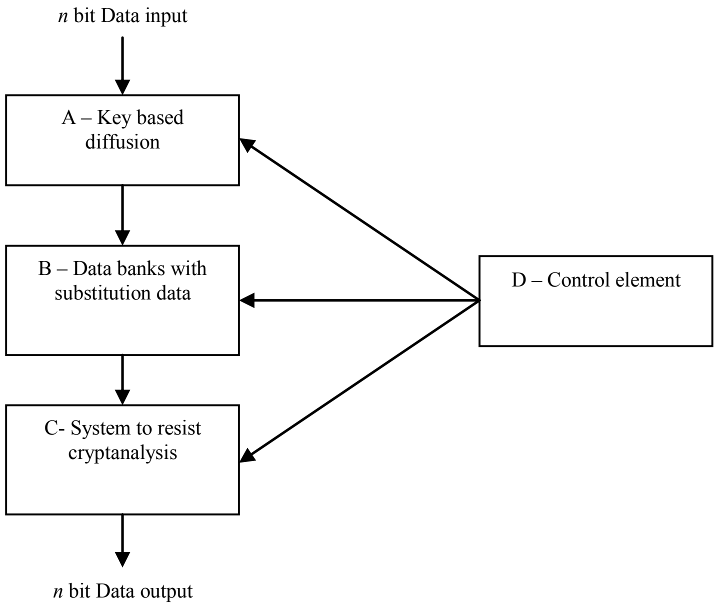
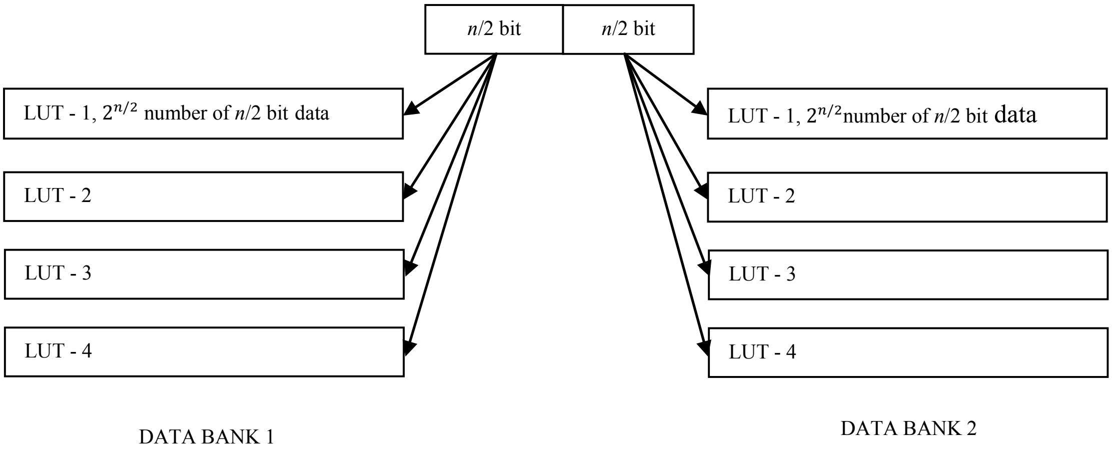


Fig. 1. Block Diagram of Secure hardware efficient S Box

Selection of LUT is decided by the status of the control element in Fig. 1, shown as block D. A Linear Feedback Shift Register (LFSR) is used as a control element. An LFSR with log_2m bits can select the LUTs of each bank, where m is the number of LUTs within the bank. The total number of $n/2$ bit data in bank 1 and bank 2 is $2m\times2^{n/2}$. All $2m$ LUTs contain totally different data at same address locations in order to maximize randomness of selection.

The number of data that can be substituted for a single *n* bit message is m^2, since each *n*/2 bit message has a one to one mapping with each LUT.

The limitation of the above circuit is, it is easy to understand which data bank is connected to upper and lower *n*/2 bits, which makes the cryptanalysis easier. The remedy is to introduce block A, which can diffuse the input data so that the direct relation between the upper or lower *n*/2 bits of message and data banks is broken. Further, this can increase the number of data that can be substituted for a single *n* bit message from m^2 to $2m^2$. Fig.3 represents a simple strategy for key based diffusion using multiplexers. An LFSR bit is used as the control signal to randomly interchange upper and lower *n*/2 message bits of the message.



n/2 bit
n/2 bit
LUT - 1, $2^{n/2}$ number of *n*/2 bit data
LUT - 2
LUT - 3
LUT - 4
LUT - 1, $2^{n/2}$number of *n*/2 bit data
LUT - 2
LUT - 3
LUT - 4
DATA BANK 1
DATA BANK 2

Fig. 2. Arrangements of LUTs for substitution

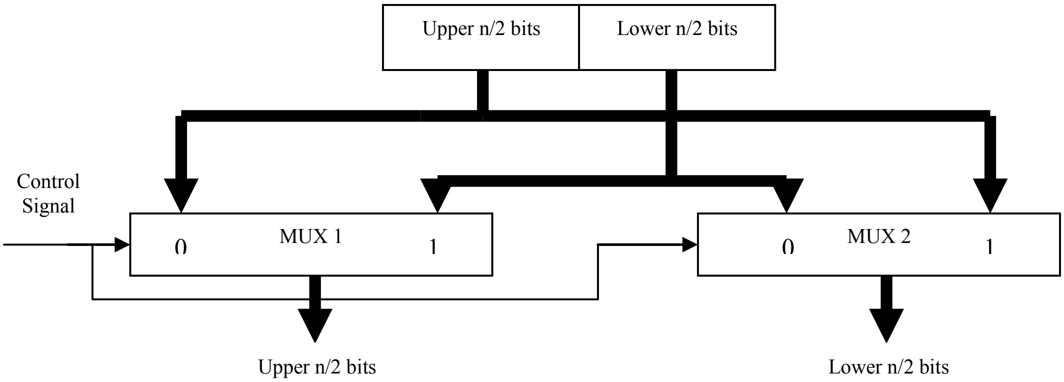


Fig. 3. Implementation of Block A-Key based Diffusion

Even if Block A is introduced between input message and block B, the output from the data banks will be changing only in *n*/2 bit blocks. Definitely the strict Avalanche Criteria (SAC) will not be satisfied here. Block B of Fig.1 performs another key based diffusion to satisfy the SAC and to resist cryptanalysis. Fig.4 shows a multiplexer based approach for achieving the same.

It uses *n* number of n:1 multiplexers to give *n* bit output. The input bits of each multiplexer are interleaved in such a way that, for each value of control signal, all the *n* output bits of data bank 1 and 2 reaches the final output vector, but permuted differently. So for different control signals the substituted data will appear in differently permuted combinations so that there can be *n* number of combinations. Here also an LFSR provides the control bits for multiplexers where the number of bits required is $log_2 n$. Cryptographic strength enhancement of the S Box using this circuit is explained in section 4.

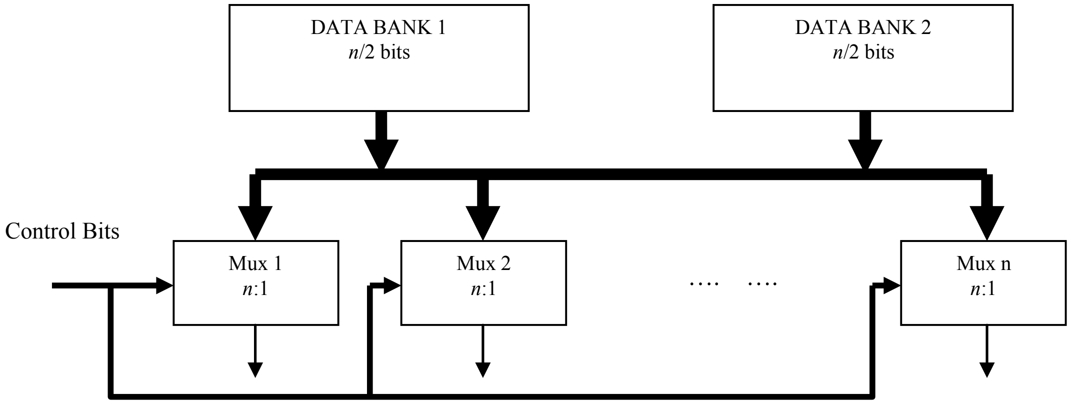


Fig. 4. Block C - Circuit to break Cryptanalysis

The decryption process is as follows: For an AES system, the number of rounds is fixed. Since AES is a symmetric cipher, the same key is used for both encryption and decryption of the message. For maximum security of the proposed design, the additional keys are varied in each round. Since the decryption process is in the reverse direction of encryption, one constrain here is to generate the key bits in the reverse direction. It is possible to reverse the sequence of LFSR by changing the polynomials. So the decryption circuit will have to find the initial value of key by advancing the LFSR polynomial used in the encryption side by r times where r is the number of rounds of AES. After calculating the initial value of key for decryption, the polynomial will have to change for reverse sequencing. The reciprocal polynomial is given by, $P^*(x) = x^k P(1/x)$, where P(x) is the Primitive polynomial of an LFSR and k is the number of LFSR bits. To get the reverse sequence, an LFSR having a reciprocal polynomial is to be designed with the rotation of data in opposite direction.

4. Properties, Security and Cryptanalysis

The degree of achievement of the desirable properties of S Box explained in section 2 is discussed here. Also the reason why the cryptanalysis fails is explained in this section.

4.1 Properties: Achieved with the new design

- *Nonlinearity:* The number of data that can be substituted for a single n bit data is $2m^2$. It is obvious that there cannot be a linear relation between all the numbers. The designer should select the S Box data carefully based on the usual criteria and conventions.
- *Bijection*: The conventional meaning is not satisfied here. However, a one to many ($1{:}2m^2$) mapping is achieved. There is considerable difference in the size of LUTs in comparison with conventional S Box. This design combines the property of static and dynamic S Boxes and gives more security with lesser hardware complexity.
- *Balance*: Better balance is possible since number of Substitution data are less. More over the system to resist cryptanalysis shown in Fig. 5, does not change the hamming weight of substituted data.
- *Bit independent criteria or Correlation Immunity*: There will not be any statistical dependency for output bits with output vector. Some results are given in Table 1 to shows this.
- *Completeness*: From the Fig. 3 it is seen that completeness is not obtained because each halves of the message are substituted separately. But the presence of block C in Fig. 5 ensures completeness by interleaving the bits in such a way that each bit of the output depends really on all the input bits.
- *Strict Avalanche Criteria(SAC)*: Experimentally it is proved that SAC is satisfied but is not merely contributed by substitution. Fig. 5 shows how the bits of substituted data are permuted to achieve SAC and the combinations are

given in Table 2. Table 1 gives the number of output bit changes in output vector due to change in single input bit.

- *Extended Properties :Static and Dynamic*: SL[I,O] :- Partial information about the input bits will not reduce the uncertainty in the unknown output bits because the message is substituted and permuted randomly based on the secret key. DL[I,O]:- Information about any changes in the input bits does not reduce the uncertainty in the change in the output bits. Table 1 shows the data substituted for consecutive data at input which shows that there is no relation with change in input vector and change in output vector. DL[O,O]:- Partial information about any changes in the output bits does not reduce the uncertainty in the changes of another output bits, because the output is derived only from input and SL[I,O] is satisfied.

4.2 Experimental results

Simulation is carried out for the proposed design for n = 8 and m = 4. Table 1 shows that SAC, correlation immunity, Completeness, Nonlinearity, SL[I,O], DL[I,O], DL[O,O] etc are satisfied. Choosing value for n and m: For the proposed S Box, the total number of 4 bit substitution data is $2m\times2^{n/2}$ = 128. In conventional S Box 256 numbers of 8 bit data are stored. As far as number of LUTs (m) are concerned, the relation 1<m< 8 holds well. Mathematically the best combination is n= 8 and m = 4.

Table 1. Substituted data and its properties

Message (1 bit change for consecutive inputs)	Data substituted	SAC (no. of bit change – minimum 4)	Hamming Weight
B0	4B		4
B1	21	4	2
B3	CA	6	4
B7	26	5	3
BF	13	4	3
BE	62	4	3
BC	89	5	3

4.3 Security and key length

Key length has a significant role in security. Greater the key length of the system, tougher the cryptanalysis to break it. In the proposed hardware efficient design, the key length is extended as given below

- For block A in Fig. 1, the required key length minimum is log_2k, where k is the number permutations possible for the diffusion system
- For block B in Fig. 1, the required key length is 2 log_2m, where m is the number of LUTs in each data bank.
- For block C in Fig. 1, the required key length is log_2n, where n is the number of bits in the group to be substituted.
  The total number of additional key bits, K = log_2k + 2 log_2m+ log_2n
  Hence the simulated system with k = 2, m = 4, and n = 8 have additional number of key bits K = 8.

Any S Box should be able to withstand both Linear and Differential cryptanalysis. The achievement of enhanced resistance to cryptanalysis offered by the proposed design is detailed below.

4.4 Linear Cryptanalysis

Linear cryptanalysis fails because of the presence of the system specially designed shown as Fig. 5 (block C in Fig. 2). The Table 2 shows how the positions of substituted data bits are interchanged to meet SAC. Unless the control bits generated by LFSR are known, the linear relation between input and output bits cannot be found out. Since the LFSR bits do not appear directly, finding this will be too difficult.

4.5 Differential Cryptanalysis

Suppose x is the input and y is the output of a system when mixed with a key K.

$y = x \oplus K$

when x is changed by Δx to x'

$x' = x \oplus \Delta x$

Correspondingly,

$y' = x' \oplus K$

$= x \oplus \Delta x \oplus K$

$= x \oplus K \oplus \Delta x$

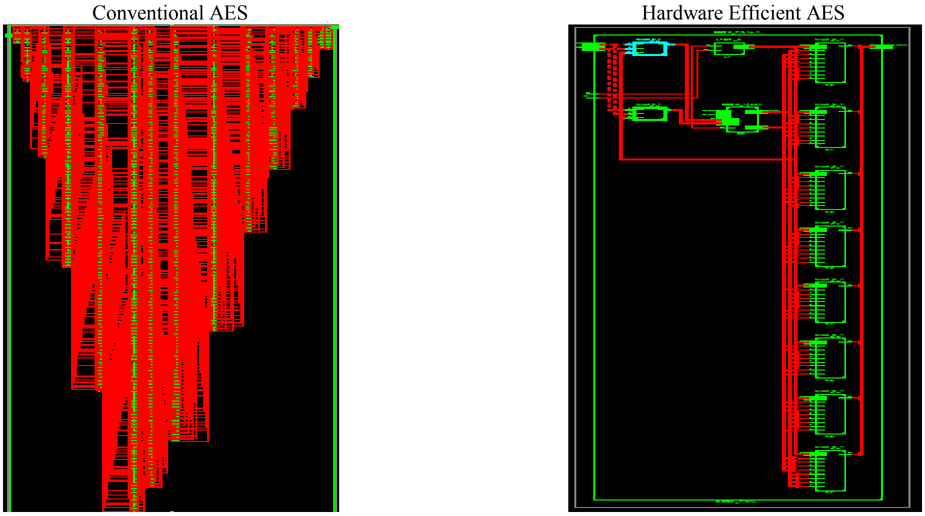
$=$ y$\oplus \Delta x$

So in differential analysis, key has no effect on Δx. But in the proposed design, the differential cryptanalysis can be overcome by the presence of block C shown in Fig. 5. Table 2 gives the different input combinations of Multiplexers of block C given for an n=8 bit system, chosen for simulation. Each column represents the order of output bits corresponding to the different control bits status.

Table 2. Position of output bits for different keys

Control status	000	001	010	011	100	101	110	111
Mux 1	6	2	4	2	7	0	3	4
Mux 2	0	7	2	3	5	6	2	1
Mux 3	4	0	6	1	3	7	5	7
Mux 4	1	3	5	4	0	1	6	3
Mux 5	3	6	7	0	2	4	1	5
Mux 6	7	4	0	6	1	3	7	2
Mux 7	5	1	3	7	4	2	0	6
Mux 8	2	5	1	5	6	5	4	0

An LFSR can be used to generate the control signal which acts as key bits. With differential cryptanalysis, this key cannot be eliminated because the key does not appear directly in the output. Instead of performing some mathematical operations, the keys are used for permutation. Calculation of difference in consecutive outputs will not do the expected job.


Conventional AES

Hardware Efficient AES

Fig. 5. RTL diagrams for Conventional and new S Box

4.6. Synthesis report and comparison

The conventional AES SBox and the proposed hardware efficient S Box are coded in Verilog and synthesized using Xilinx ISE Design Suite 12.1. Fig. 5 shows the RTL diagrams for both obtained. Table 3 shows the comparison of hardware complexity for conventional and newly designed S Boxes. From the table it is clear that the hardware requirement of conventional AES S Box is far greater than the proposed S Box.

Table 3. Comparison of hardware complexity

Components	Conventional AES	Hardware Efficient AES
IOs	17	18
Cell Usage		
BELLs	1704	265
AND2	559	128
AND3	129	0
AND4	4	0
AND5	1	0
INV	642	72
OR2	314	64
OR3	52	0
OR4	2	0
XOR2	1	1
FLIP FLOP/LATCHES	8	11
FD	8	8
FDP	0	3
IO BUFFERS	17	18
IBUF	9	10
OBUF	8	8

6. Conclusion and future scope

Here a new S Box is designed with lesser hardware complexity and improved security. Differing from conventional S Box, some key based operations are performed which enhances the security by defeating all kind of cryptanalysis. Strategy for resisting linear and differential cryptanalysis is also explained here. The increase in number of key bits really contributes to the level of security

An in depth research can be conducted in this area for enhancing the cryptographic features. Cryptographic functions can be clubbed in a single module by time sharing basis. This may further lead to low hardware complexity and power consumption.

References

1. C. Shannon, Communication theory of secrecy systems, *Bell Systems Technical Journal*, vol.28, 1949
2. W.Stallings*, Cryptography and Network Security, Principles and Practices*, Prentice Hall, 2006
3. C Adams and S Tavares, The structured design of good S Boxes, *Journal of Cryptology*, 3(1):27-41,1990
4. J.Cobas and J.Brugos. Complexity –theoretical approachesto the design and analysis of cryptographical Boolean functions. In Computer Aided Systems Theory-*EUROCAST 2005, LNCS. Springer- Verlag, Berlin*, Germany, 2005
5. A. Webster, S.Tavares, On the Design of S Boxes, *Advances in Cryptology –CRYPT0 1985, LNCS 218, Springer-Verlag*, 1985
6. M.Dawson,S.Tavares, An Expanded Set of S Box Design Criteria Based on Information Theory and its Relation to Differential-like Attacks, *Advances in Cryptology – EUROCRYPT 1991, LNCS 547, Springer- Verlag* 1991
7. M Sivabalan, S.Tavares, L.Peppard, On the design of SP networks from an information theoretic point of view, *Advances in Cryptology – CRYPTO 1992, LNCS 740, Springer Verlag 1993*