NOVEL APPROACH FOR DESIGNING OF S-BOX WITH MULTIBIT PARITY DETECTION SCHEME

Pendyala Siva Prasad[1], A.Shyam Kumar[2], L.Srinivas Reddy[3]

[1] *M.Tech Scholar (VLSI), Asst.professor (ECE), Assistant. Professor (ECE)*
Nalanda Institute of Engineering and Technology (NIET), Siddharth Nagar, Guntur,A.P. (India)

ABSTRACT

This paper presents novel approach for designing of AES S-box using combinational logic using Verilog and simulated in Xilinx ISE 13.2.AES is data encryption standard which uses same at Encryption as well as for decryption. AES uses Substution box was divided into five blocks and are designed by Combinational blocks. So that we can easily analyse faults which are caused by natural/malfunctioning faults.

Keywords: ROM Based S-Box, Combinational Design Of S-Box, Affine Transformation, Isomorphic Trannsformation

I. INTRODUCTION

Encryption is the process of converting normal text to unknown format by using algorithm called cipher. The format can be understood for those who having knowledge of encryption and key. There are two types of encryption standards are existed. Those are Data Encryption standard (DES) and Advance encryption standard (AES). The data encryption standard was proposed in November 1967. DES has plain text encrypted into 64 bit blocks with the 56 bit key. The input for the encryption is 64 bit input and 56 bit key and managed to 64 bit blocks to get 64 bit output. Faults which were caused by natural /malfunctioning can be complex to analyse.

AES is advance data standard was proposed in the year 26th November 2001 by Joan Daemen and Vincent Rijmen (originally called Rijindael). It normally having bit size 128bits and key size varies from 128,192 and 256 bits. AES algorithm will use same key at encryption as well as for decryption. AES will convert normal text to cipher text after 10 rounds in which encryption will take 4 rounds namely as transformation , sub bytes , shift rows and mixed columns after 10 rounds plain text can be converted to cipher text. This cipher text can be reverse processed in the decryption to get plain text. Sub bytes known as S-box stage in Encryption and Inverse S-box in decryption are nonlinear except all blocks are similar in the Encryption and Decryption. Receiver which is using AES must have to know the key otherwise it will not know how to decrypt the data. Implementation of AES hardware may relts in fault. Data thieves can also try to hack which also results in fault. AES conventional one uses the approach of single bit parity check it has less coverage of fault.

II. AES ALGORITHM

The proposed AES is similar to the conventional AES but the difference is in construction of S-box which was made by combinational gates. AES algorithm works on 4*4 matrix element called states. It works on states which is of 8bit length.

The state will undergo following stages namely sub bytes and inverse sub bytes, shift rows, and mix columns, transformations. The AES algorithm represented pictorially as below

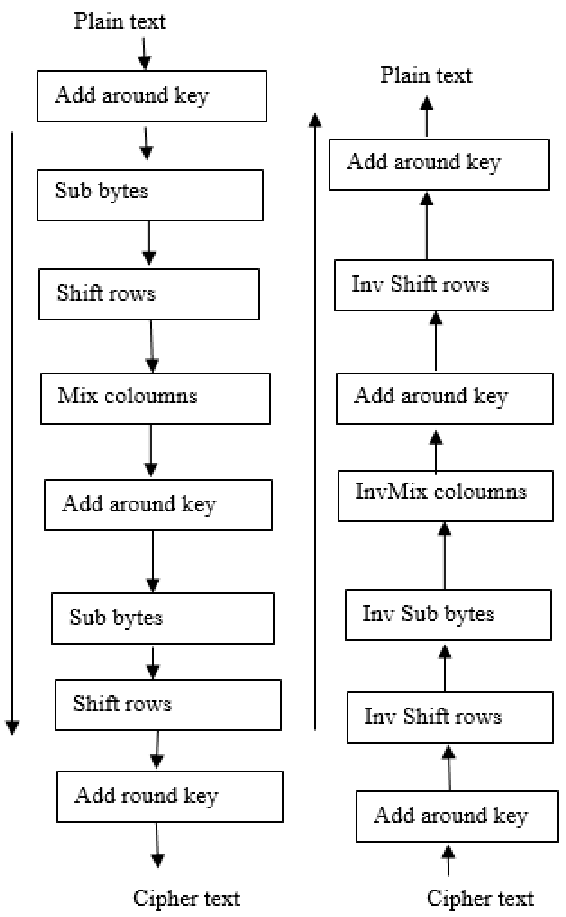


Fig 2.1 AES Algorithm

2.1 Sub Bytes And Inverse Sub Bytes

These 2 stages are first transformations in their respective round which was performed by byte substitution called sub bytes with 16 s-boxes. In this step each byte in the matrix was replaced by the byte specified in the look up table. The look up table is already with preloaded data

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
	0	63	7c	77	7b	F2	6b	6f	C5	30	1	67	2b	fe	D7	ab	76
	1	Ca	82	C9	7d	Fa	59	47	F0	ad	D4	A2	af	9c	A4	72	C0
	2	B7	Fd	93	26	36	3f	F7	Cc	34	A5	E5	F1	71	D8	31	15
	3	4	C7	23	C3	18	96	5	9a	7	12	80	E2	eb	27	B2	75
	4	9	83	2c	1a	1b	6e	5a	A0	52	3b	D6	B3	29	E3	2f	84
	5	53	D1	0	Ed	20	Fc	B1	5b	6a	Cb	Be	39	4a	4c	58	cf
	6	D0	Ef	Aa	Fb	43	4d	33	85	45	F9	2	7f	50	3c	9f	A8
	7	51	A3	40	8f	92	9d	38	F5	Bc	B6	da	21	10	ff	F3	D2
x	8	Cd	0c	13	Ec	5f	97	44	17	C4	A7	7e	3d	64	5d	19	73
	9	60	81	4f	Dc	22	29	90	88	46	Ee	B8	14	de	5e	0b	db
	a	E0	32	3a	0a	49	6	24	5c	C2	D3	Ac	62	91	95	E4	79
	b	E7	C8	37	6d	8d	D5	4e	A9	6c	56	F4	ea	65	7a	ae	8
	c	Ba	78	25	2e	1c	A6	B4	C6	E8	Dd	74	1f	4b	bd	8b	8a
	d	70	3e	B5	66	48	3	F6	0e	61	35	57	ba	86	C1	1d	9e
	e	E1	F8	98	11	69	D9	8e	94	9b	1e	87	ca	ce	55	28	df
	f	sc	A1	89	0d	bf	E6	42	68	41	99	2d	0f	B0	54	bb	16

Fig 2.2 s-box

2.2 Shift Rows and Inverse Shift Rows

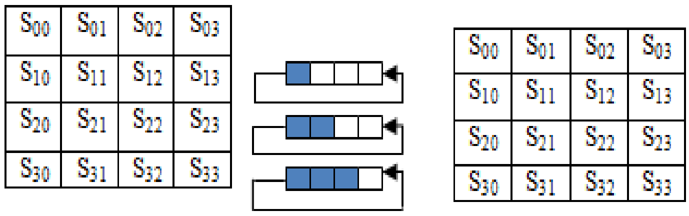


Figure 2.3 Shift Rows

In this step encryption side first row left unchanged and second row shifted left to one position and third row shifted by 2 positions similarly last row shifted by three position. At decryption side inverse shift rows were performed as last row shifted by three positions to right, second row shifted by two positions to right, first row is unchanged

2.3 Mix Columns and Inverse Mix Columns

In this stage input state byte is multiplied by the fixed polynomial over Galois field and the product value is replaced in output state

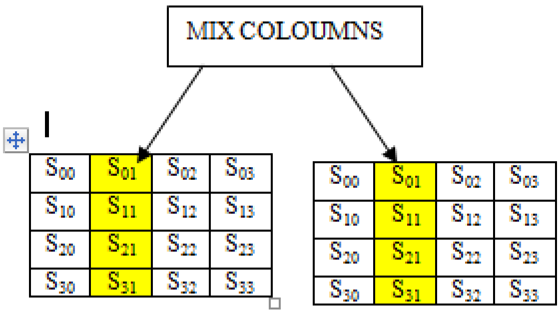


Figure 2.4 Shift Mix Columns

2.4 Add Round Key

Here it was derived from the cipher key using key schedule .each byte in the state matrix is combined with the add round key using Ex-or operation

2.5 AES Key Expansion

Aes key takes 4word key as input and produces array of 44 word, each round uses 4 of these words and each word has 32 bytes which means that each sub key is 128 bit long

III.PROPOSED S-BOX DESIGN

In proposed S-box designion we have designed 5 blocks of hardware. In which 3 blocks represent multiplicative inversion and remaining blocks performs affine transformation. This design also has multi bit parity fault detection scheme. It will replaces the each single byte in the state matrix so that at time it process a single byte it has 8 bit input and 8 bit output.following block diagram shows the hardware implementation s-box was construted by following formuales of multiplicative inversion and affine transformation for inverse s-box invere multiplicative and inverse affine transformation

3.1 Isomorphic and inverse Iso morphic transformations

Multiplicative inverse of an element in GF(8) can be found by decomposing the element in galosifield intto smaller order elements of GF(2), GF(2^1) and GF(2^2). Multiplicative inverse of an element composite field can be found by mapping an element using isomorphic function then we find multiplicative inversion and again converted back to composite field by using inverse isomorphic function which was denoted by δ is an 8*8 matrix and multiplication is AND operation, addition is modulo-2 addition

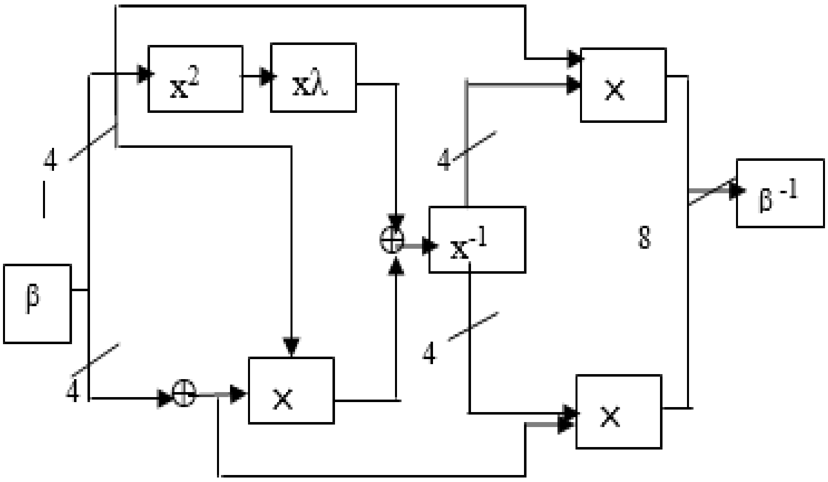


Fig 3.1 Block diagram of s-box

β ⟶ iso morphic transformation
× ⟶ multiplication
xλ ⟶ multiplication with lambda
x^2 ⟶ squarer
δ^{-1} ⟶ inverse iso morphic transformation
X^{-1} ⟶ Multiplicative inversion

I .Isomorphic and inverse Iso morphic transformations

Multiplicative inverse of an element in GF(8) can be found by decomposing the element in galosifield intto smaller order elements of GF(2), GF(2^1) and GF(2^2). Multiplicative inverse of an element composite field can be found by mapping an element using isomorphic function then we find multiplicative inversion and again converted back to composite field by using inverse isomorphic function which was denoted by δ is an 8*8 matrix and multiplication is AND operation, addition is modulo-2 addition.

Where q is 8 bit incoming data

$$\beta \times \mathbf{q} = \begin{pmatrix} 1&0&1&0&0&0&0&0 \\ 1&1&0&1&1&1&1&0 \\ 1&0&1&0&1&1&0&0 \\ 1&0&1&0&1&1&1&0 \\ 1&1&0&0&0&1&1&0 \\ 1&0&0&1&1&1&1&0 \\ 0&1&0&1&0&0&1&0 \\ 0&1&0&0&0&0&1&1 \end{pmatrix} \times \begin{pmatrix} q7 \\ q6 \\ q5 \\ q4 \\ q3 \\ q2 \\ q1 \\ q0 \end{pmatrix} \qquad \beta^{-1} \times \mathbf{q} = \begin{pmatrix} 1&1&1&0&0&0&1&0 \\ 0&1&0&0&0&1&0&0 \\ 0&1&1&0&0&0&1&0 \\ 0&1&1&1&0&1&1&0 \\ 0&0&1&1&1&1&1&0 \\ 1&0&0&1&1&1&1&0 \\ 0&0&1&1&0&0&0&0 \\ 0&1&1&1&0&1&0&1 \end{pmatrix} \times \begin{pmatrix} q7 \\ q6 \\ q5 \\ q4 \\ q3 \\ q2 \\ q1 \\ q0 \end{pmatrix}$$

$$\delta \times \mathbf{q} = \begin{pmatrix} q7 \oplus q5 \\ q7 \oplus q6 \oplus q4 \oplus q3 \oplus q2 \oplus q1 \\ q7 \oplus q5 \oplus q3 \oplus q2 \\ q7 \oplus q5 \oplus q3 \oplus q2 \oplus q1 \\ q7 \oplus q5 \oplus q3 \oplus q2 \\ q7 \oplus q6 \oplus q2 \oplus q1 \\ q7 \oplus q4 \oplus q3 \oplus q2 \oplus q1 \\ q6 \oplus q4 \oplus q1 \\ q6 \oplus q1 \oplus q0 \end{pmatrix} \qquad \delta^{-1} \times \mathbf{q} = \begin{pmatrix} q7 \oplus q6 \oplus q5 \oplus q1 \\ q6 \oplus q2 \\ q6 \oplus q5 \oplus q1 \\ q6 \oplus q5 \oplus q4 \oplus q2 \oplus q1 \\ q5 \oplus q4 \oplus q3 \oplus q2 \oplus q1 \\ q7 \oplus q4 \oplus q3 \oplus q2 \oplus q1 \\ q5 \oplus q4 \\ q6 \oplus q5 \oplus q4 \oplus q2 \oplus q0 \end{pmatrix}$$

3.2 Affine Transformation

Affine transformation and its inverse was found after finding multiplicative inverse since its inputs are multiplicative inverse of 8 bit input byte in stste matrix ,both affine and its inverse was using same multiplicative inverse and is denoted by matrix “a”

$$AT(a) = \begin{pmatrix} 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \\ 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \end{pmatrix} \times \begin{pmatrix} a7 \\ a6 \\ a5 \\ a4 \\ a3 \\ a2 \\ a1 \\ a0 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \qquad AT^{-1}(a) = \begin{pmatrix} 0&1&0&1&0&0&1&0 \\ 0&0&1&0&1&0&0&1 \\ 1&0&0&1&0&1&0&0 \\ 0&1&0&0&1&0&1&0 \\ 0&0&1&0&0&1&0&1 \\ 1&0&0&1&0&0&1&0 \\ 0&1&0&0&1&0&0&1 \\ 1&0&1&0&0&1&0&0 \end{pmatrix} \times \begin{pmatrix} a7 \\ a6 \\ a5 \\ a4 \\ a3 \\ a2 \\ a1 \\ a0 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

3.3 Airthemetic Operations In Galoisi Field

i. Multiplication with constant, λ

Here the input is 4 bit and and constant is denoted by λ={1100} we will multiply the isomorphic output was firsr squred then that 4 bit output fed multiplier unit that can be performed by following formuales.

$k3 = q2 \oplus q0;$

$k2 = q3 \oplus q2 \oplus q1 \oplus q0;$

$k1 = q3;$

$k0 = q2;$

ii. Squaring in GF(2^4)

we can calculate squaring by letting $k=q^2$,where k and q are elements in GF(2^2) and k,q are denoted by binary numbers {k3k2k1k0},{q3q2q1q0} respectively and squaring can be found by using following formulaes which are deduced by using decomposition

$k3 = q3$

$k2 = q3 \oplus q2;$

$k1 = q1 \oplus q2;$

$k0 = q3 \oplus q1 \oplus q0;$

iii. GF (2^2) Multiplication

Let $k = qw$, where $k = \{k1\ k0\}2$, $q = \{q1\ q0\}2$ and $w = \{w1\ w0\}2$ are elements of GF(2^2).

$k1 = q1\ w1 \oplus q0\ w1 \oplus q1 w0;$

$k2 = q1\ w1 \oplus q0\ w0;$

iv. Multiplication with constant φ

Let $k = q\varphi$, where $k = \{k1\ k0\}2$, $q = \{q1\ q0\}2$ and $\varphi = \{10\}2$ are elements of GF(2^2).

$K1=q1 \oplus q0;$

$K0=q0;$

3.4 Multiplicative Inversion

The multiplicative inverse of q (where q is element of GF(24)) such that $q\text{-}1= \{q3\text{-}1,q2\text{-}1,q1\text{-}1,q0\text{-}1\}$.

$q3^{-1} = q3 \oplus q3q2q1 \oplus q3q0 \oplus q2;$

$q2^{-1} = q3q2q1 \oplus q3q2q0 \oplus q3q0 \oplus q2 \oplus q1;$

$q1^{-1} = q3 \oplus q3q2q1 \oplus q3q1q0 \oplus q2 \oplus q2q0 \oplus q1;$

$q0^{-1} = q3q2q1 \oplus q3q2q0 \oplus q3q1 \oplus q3q1q0 \oplus q3q0 \oplus q2 \oplus q2q1 \oplus q2q1q0 \oplus q1 \oplus q0;$

IV. FAULT DETECTION METHOD

In prior designs of AES have fault detection schemes of single bit in this proposed design of s-box and inverse s-box was devided into 5 blocks. parity of each block was identified from the input bits of the blocks.we can evaluate the parities of each block is as follows

For block 1 & block 5

Let z be an input of s-box.The intial block of s-box consisting of transformation of matrices. Which was done by using isomorphic tradnsformation its predicted parity calculated as follows and denoted by p1, block 5 having inversetransformation of the matrices which is inverse isomorphic transformation and its parity denoted as p5 and its input denoted by V

P1 = Z[0]+Z[2]+Z[4]+Z[5];

P5 = V[0]+V[1]+V[2]+V[4]+V[6];

For block 2 &4

Block 2 and 4 comprises of modulo-2 adder ,multiplication with lambda and multiplier and squarer each having 4 bit and 8 bit input according to their role their parities are denoted by p2,p4 respectively

P2 = E[4] + E[3] ((~Ph) + E[6]) + (~E[2] (ph+e[6]) + e[1] e[6] + e[4]) + E[0] (~ph) ;

P4 = e[3] (s[0] + s[2] + e[2] s[0] + s[1] + s[3]) + e[1] (s[6] + s[4] + e[0] s[0] + s[1] + s[2] + s[3]);

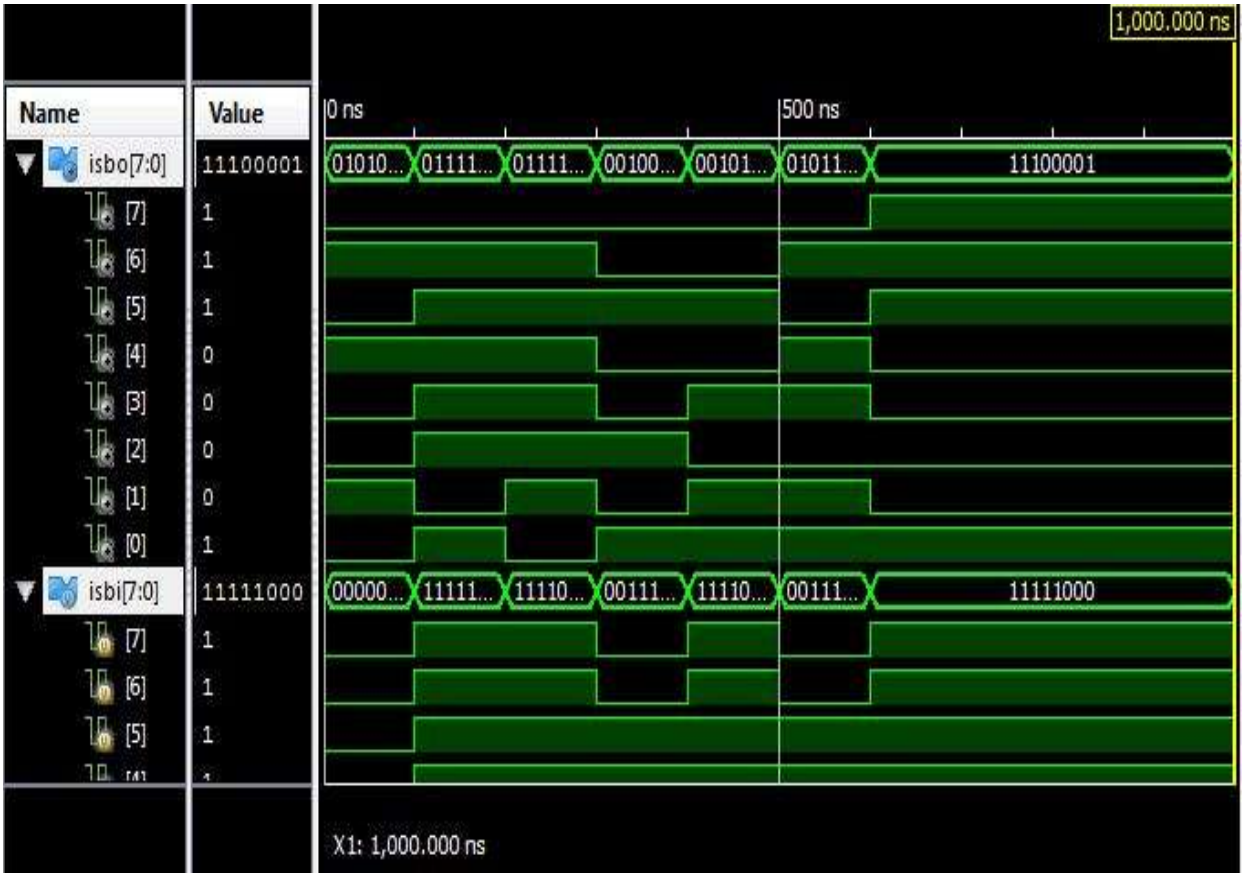
Block 3

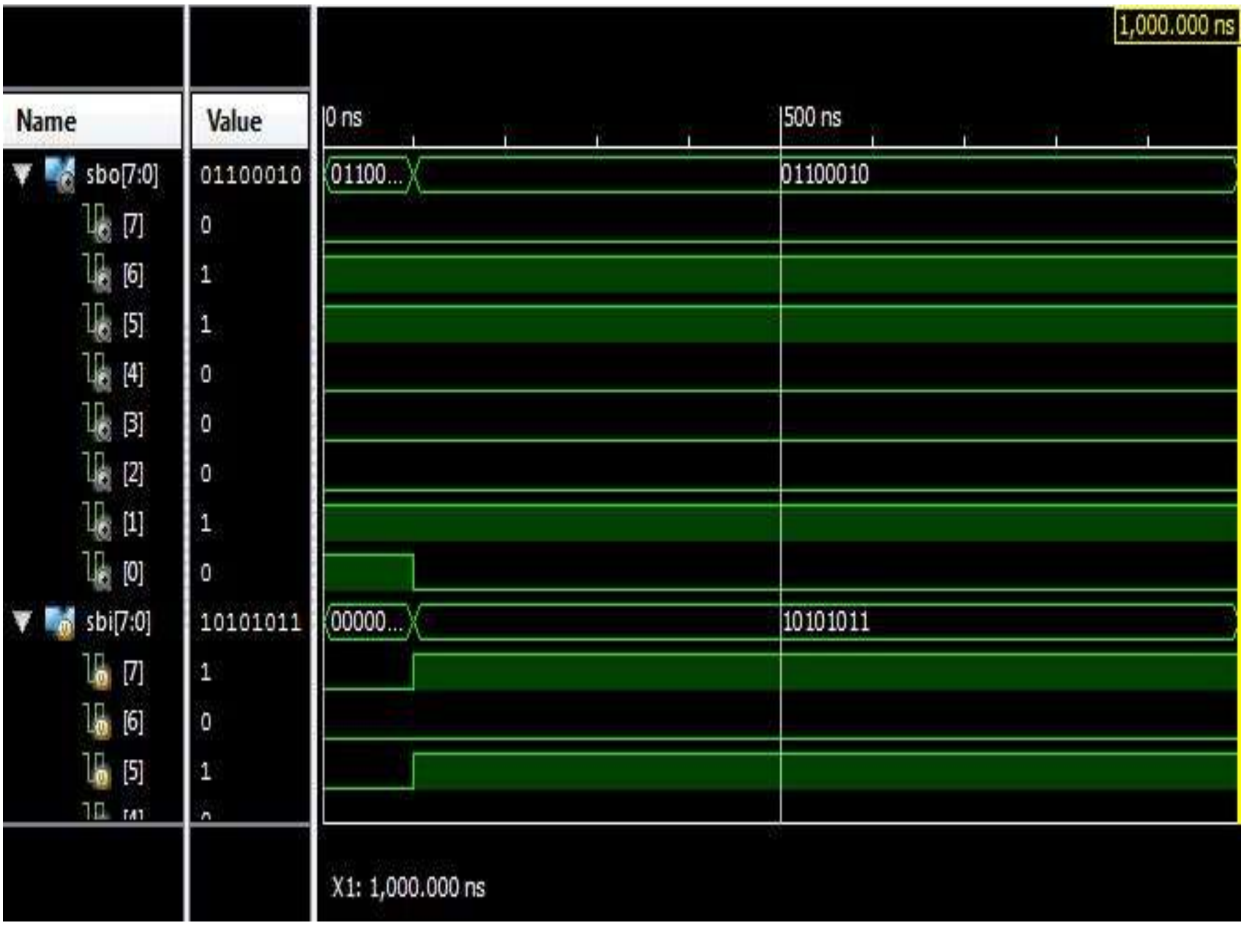
This block performs multiplicative inverse on the given input data.it accepts 4bit input and perform multiplicative inverse and produce 4 bit output. This block parity can be found by given formulae

P3 = (r1 + r0) r3 +(~r2 | r1) r0;

V. SIMULATION RESULTS

The S-box is designed in Verilog HDL and simulated in the Xilinx ISE13.2I. This design is combainational design which reduces the hardware design complexity. Which enhances the speed. The complexity less.


1,000.000 ns
Name
Value
0 ns
500 ns
isbo[7:0]
11100001
01010...
01111...
01111...
00100...
00101...
01011...
11100001
[7]
[6]
[5]
[4]
[3]
[2]
[1]
[0]
isbi[7:0]
11111000
00000...
11111...
11110...
00111...
11110...
00111...
11111000
X1: 1,000.000 ns


1,000.000 ns
Name
Value
0 ns
500 ns
sbo[7:0]
01100010
01100...
01100010
[7]
[6]
[5]
[4]
[3]
[2]
[1]
[0]
sbi[7:0]
10101011
00000...
10101011
X1: 1,000.000 ns

VI. CONCLUSION

This type of novel design of s-box using combinational logic with the multi 0bit fault detection scheme was designed using Verilog hardware description language with 8bit input and simulated in Xilinix ISE 13.2 found that novel design giving better performance and reduced area due to galosifield operations in combinational design.

REFERENCES

[1] Akashi Satoh, Sumio Morioka, Kohji Takano and Seiji Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization.", Springer-Verlag Berlin Heidelberg, 2001.

[2] Vincent Rijmen, "Efficient Implementation of the Rijndael S-Box.", Katholieke Universiteit Leuven, Dept. ESAT. Belgium.

[3] Xinmiao Zhang and Keshab K. Parhi, "High-Speed VLSI Architectures for the AES Algorithm.", IEEE Transactions on Very Large Scale Integration(VLSI) Systems, Vol. 12, No. 9, Septemper 2004.

[4] "Advanced Encryption Standard (AES)" Federal Information Processing Standards Publication 197, 26th November 2001.

[5] Tim Good and Mohammed Benaissa, "Very Small FPGA Application-Specific Instruction Processor for AES.", IEEE Transactions on Circuits and Systems – I: Regular Papers, Vol. 53, No. 7, July 2006.

[6] The Advanced Encryption Standard http://en.wikipedia.org/wiki/Advanced_Encrypti

[7] Subashri T, Arunachalam R, Gokul Vinoth Kumar B, and Vaidehi V, "Pipelining Architecture of AES Encryption and Key Generation with Search Based Memory," International journal of VLSI design & Communication Systems (VLSICS), YoU, No.4, December 2010.

[8] J. Vijaya and M. Rajaram, "High Speed Pipelined AES with Mix Column Transform," European Journal of Scientific Research, ISSN 1450-216X Vol.61 No.2 (2011), pp. 255-264.

[9] Priyanka Pimpale, Rohan Rayarikar, Sanket Upadhyay, "Modifications to AES Algoritlun for Complex Encryption," IJCSNS International Journal of Computer Science and Network Security, Vol.11 No.1 0, October 2011.

[10] Aluned. H. Sawahneh, "Hardware Design of AES S-box using pipelining structure over GF((24i)".

[11] K.Rahimwmisa, Dr. S. Sureshkumar, and K.Rajeshkumar,"Implementation of AES with New S-Box and PerformanceAnalysis with the Modified S-Box," International Conference on VLSI, Communication & Instrumentation (ICVCI) 20J J Proceedings published by International Journal of Computer Applications® (IJCA).

[12] MooSeop Kim, Juhan Kim, and Yongje Choi, "Low Power Circuit Architecture of AES Crypto Module for Wireless sensor Network," World Academy of Science, Engineering and Technology 8, 2007.

[7] M.Pitchaiah, Philemon Daniel, and Praveen, "Implementation of Advanced Encryption Standard Algorithm," International Journal of Scientific & Engineering Research, Volume 3, Issue 3, March -2012 1 ISSN 2229-5518.

[8] Zine EI Abidine, Alaoui Ismaili, and Aluned MOUSSA, "Self-Partial and Dynamic Reconfiguration Implementation for AES using FPGA," IJCSI International Journal of Computer Science, Issues, Vol. 2, 2009 ISSN (Online):1694-0784 ISSN (Print): 1694-081456

AUTHOR DETAILS

	**PENDYALA SIVA PRASAD**, Pursuing M.tech (VLSI) from Nalanda institute of Engineering and Technology(NIET), Siddharth Nagar, Kantepudi village, satenepalli Mandal Guntur Dist.,A.P, INDIA.His area of interest includes VLSI system design, CMOS digital Ics, Digital system design, CMOS mixed signal anlaysis.
	**A.SHYAM KUMAR**, He received his master degree in DECS. His area of interest includes digital communication, digital electronics and communication systems . currently he is working as Asst. professor (ECE) from Nalanda institute of Engineering and Technology (NIET), Siddharth Nagar, Kantepudi village, satenepalli Mandal, Guntur Dist.,A.P,
	**L.SRINIVAS REDDY**, He completed his post graduation in DECS. His area of interest includes digital electronics, digital communication, digital system design and VLSI technology and design. His research areas are optimal communication technology. He is currently working as Asst.professor (ECE) from Nalanda institute of Engineering and Technology (NIET), Siddharth Nagar,Kantepudi village, Satenepalli Mandal. Guntur Dist.,A.P,