International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Double Security using Dynamic S-Box inside Aes Algorithm

Ashish Dwivedi , Toushiba Khan, S.R.P. Sinha

Abstract: ***Now a days internet and other electronic devices have become an non removable part of our society. Day by day we are increasing the usage of data for transmission and storage as well. But there is always a problem for our data to be in wrong hands or hacked by someone. In order to ensure our secrecy of data we use bunch of algorithms to secure it. These algorithms comes under the vast section of cryptology, which means an art of hiding the data to make it secure. But as we all know when there is a hacker he would find every possible way to bypass the security algorithms. Some of the attacks are very popular in cryptology like Brute Force Attacks which checks each possible key combination to hack the data message. Due to the arrival of quantum computers in upcoming future hacking time will be decreased about a factor of around 1000 times. Now the best possible solution for enciphering data is Advanced Encryption Standard .This algorithm consists of two basic things static Substitution Box (S-Box) and other register operation. In this paper we have introduced a new technique to ensure a secure communication by using a dynamic S-Box with avalanche value of 58.59% as well as we also improved the overall area, delay (1.227 ns) and optimized the power to possible extents. Our results also approached above the traditional AES security as our modification improves avalanche effect also.***

Index Terms: Avalanche, FPGA, AES, cipher, pipeline, ISIM, ISE Xilinx, throughput, delay, wave, CBC mode.

I. INTRODUCTION

In this era, the internet and different types of electronics correspondence has turned out to be progressively common and furthermore electronic security turns out to be progressively significant component for safe exchanges and change of information experienced. The security administrations incorporate improved validation strategies, information privacy, information respectability, accessibility, non renouncement and gateway regulator. One of the main aspect of assured communication is cryptography [9]. In this cryptographic world the most important type is symmetric key type where key is kept as secret or public. AES is a symmetric type algorithm which ensures a proper secrecy to our data. Further this algorithm consists of a set of operations which are performed in order to convert message into cipher or encrypted text. Starting from detailing about AES calculation operations which are as follows:*addition,subtraction,multiplication, anddivision* on Galois Field (2^8). Goodness of AES algorithm is related to key length. Every round consists of bunch of operations like: *Sub Bytes, Shift Rows, Mix Column, and Add Round Key.* Every conversion consumes only 16 byte of matrix dimension. Next subsection explains the new idea of improving the security. Further simulation of proposed model is done on ISE 14.7. Various AES enhancements have been made in the domain of hardware now days. There is a lot of hardware formation of AES enhancements.

II. LITERATURE REVIEW

In *Federal Information Processing Standards* or (FIPS) report in 2001 the *Advanced Encryption Standard* (AES) indicates a cryptographic calculation used by FIPS that could be applied to safeguard electronically stored and transmitted data and information [2]. The AES calculation is equipped for applying cryptographic keys of 256, 192 and 128 bit to scramble and decode information in blocks of data of 128 bits.

"Sumio morioka et al 2003" [3] proposed to execute the *Low Power based S-box circuit design* by considering multiple arrange positive extremity reed muller based pprm engineering. They had accomplished 29 w of power when contrasted and composite s box at 136 w.

"Xinmiao Zhang et al 2004"[4] proposed to supplant *LUT based S-Box with composite field S-Box* since the LUT form of methodology gives high non breakable deferral than the delay of changes in every round unit of execution. Non LUT form of methodology like combination logic strategy could be utilized to stay away from inflexible deferral.

"Bevan M. Baas and Bin Liu 2013" **[5]** in their work *Parallel AES Encryption Engines for Many-Core Processor Arrays* presented a littlest structure that uses just six centers for disconnected key development along with eight centers for online keys expand, same time the biggest requires 107 along with 137 cores, individually.

"Vishal V. Panchbhai and Mohini Mohurle 2016" **[6]** in their work *Review on Realization of AES Encryption and Decryption with Power and Area Optimization* demonstrates the examination of an equipment usage of the AES-256 encryption and unscrambling calculation. Their proposed AES cryptology calculation can be utilized to encipher and decipher blocks of a 128 bits size and is fit for utilizing figure keys of 256 bits.

"Harshali Zodpe and Ashok Sapkal 2018" **[1]** in their work exhibits another methodology for producing S-box values (an altered S-box) and starting key required for encryption/decryption (improved key age) utilizing pseudo noise Sequence Generator.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Ashish Dwivedi*, Electronics and Communication Engineering Department, Institute of Engineering and Technology, Lucknow
Toushiba Khan, Electronics and Communication Engineering Department, Institute of Engineering and Technology, Lucknow
Dr. S.R.P. Sinha, Electronics and Communication Engineering Department, Institute of Engineering and Technology, Lucknow

"Mangi Han and Youngmin Kim 2017"[7] shown in their work non predicted 16 bits LFSR to form True Random Number Generator that an anticipated randomize number produced by the are deadly to applications.

III. OVERVIEW OF ALGORITHM

The operations are mentioned below:

1. Substitution Bytes
2. Shift Rows
3. Mixed Columns
4. Add Round key

1. Substitution Bytes: Also known as *Sub Byte* operation. In this operation a 128 bit message is converted into a matrix format of *16×16 bytes* then it is exchanged with a static S-box by taking message value as address location of the S-box then use that value in place of message it's like register indirect addressing. The predefined S-Box is given in box format in fig 1.

								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	01	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	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
x	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	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	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig 1: Substitution Box

For example if message part is [4b] then search 4 vertically and b horizontally on S-box then the substituted bit will be [b3].

2. Shift Rows: This operation consists of the shifting the matrix at regular rounds for 1st row no shifting is done, single right shift for 2nd row, double right shift for 3rd row and triple shift for last row. Its process is given in fig 2.

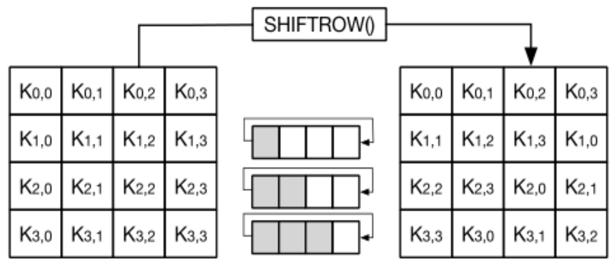

Fig 2: Shift Rows

3. Mixed Columns: Mixed Columns are linear change operation. Every part of message text multiplied with part of multiplication form matrix obtained from the polynomial having coefficient Galois Field (2^8). Further the fig 3 gives the idea of column multiplication. The polynomial used here is given by m(y) below:

$$m(y)= y^8+y^4+y^3+y+1 \quad (1)$$

Above equation tells us that while making polynomial they have used 9th bit, 5th bit, 4th bit, 2st bit and 1st bit for this operation. This is a static polynomial used to design the S-Box also.

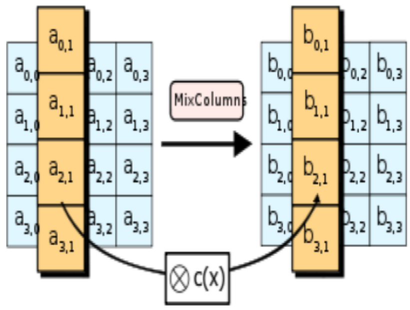

Fig 3: Mixed Columns

4. Add Round key: The operation is also called key addition in which a 16 bytes of the state matrix are bit wise exored through the 16 bytes of given secret round key. The system is noticeable as a column wise strategy among the expression of a state columns and single expression of the mystery round key. This change is as simple as also be reasonable which points of interest in adequacy however it in addition applied to all of the state. Fig 4 shows this operation.

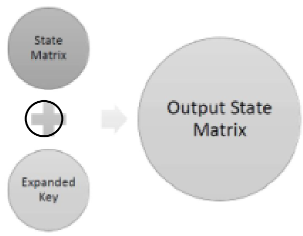

Fig 4: Add Round key

The whole flow process is defined using the explained sets of operations in fig 5. Again the number of rounds is given by using the FIPS data that is 10 for 16 bytes, 12 for 12 bytes and 14 for 16 bytes of data.

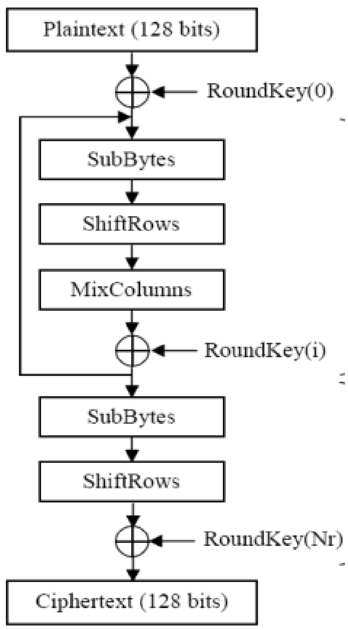

Fig 5: AES Flow Diagram

International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

There are a bunch of modes in AES according to NSIT standard like ECB, CFB, CBC etc. out of these modes the most effective and secure mode is cipher block chaining (CBC) mode. Here initialization vector is used for avoiding the repetition of the data. CBC mode is depicted in the fig 6

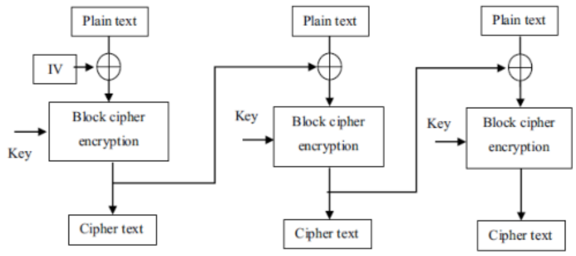

Fig 6: CBC mode of AES

IV. PROPOSED METHEDOLOGY

We have worked on AES model and after reviewing various models in literature we came across a point that using a dynamic S-Box over static S-Box is more effective way of designing the algorithm.

So these are the action plan that is executed in order to obtain the better results:

1. Designing of polynomial modulator for a selective LFSR.
2. Obtaining the required results from selected LFSR.
3. Selecting Wave pipeline method to increase the throughput of the circuit.
4. After that synthesis and simulation on ISE 14.7.
5. Then power and timing analysis is done on the X-power analyzer and timing analyzer.

We have tested a flexible LFSR which is unpredictable as its sample space increases due to presence of multiple polynomials which are selected using a polynomial modulator. This is shown in the DSch schematic in fig 7.

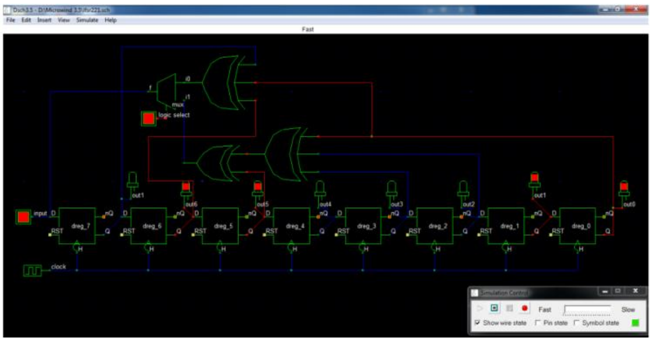

Fig 7: Dynamic LFSR design on DSch

Output waveform is also obtained on DSch which shows the shifting property of LFSR in bit by bit format. The waveform of above given schematic is shown in fig 8.

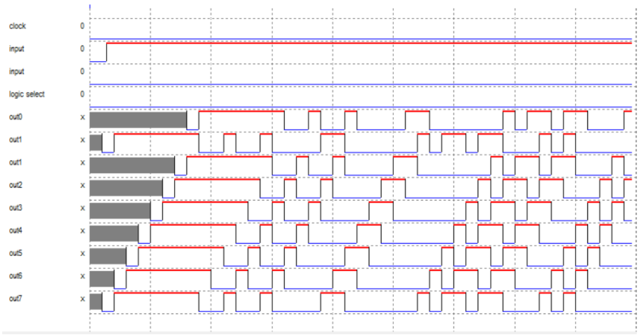

Fig 8: Waveform of Dynamic LFSR on DSch

Further we had worked for improving the throughput, delay, area and other related parameters.

Here parallel model is used which result in an optimized throughput and delay of proposed model. This quality advantage somehow we have to manage a little hike of power due to power delay product. The proposed flow is given in fig 8.

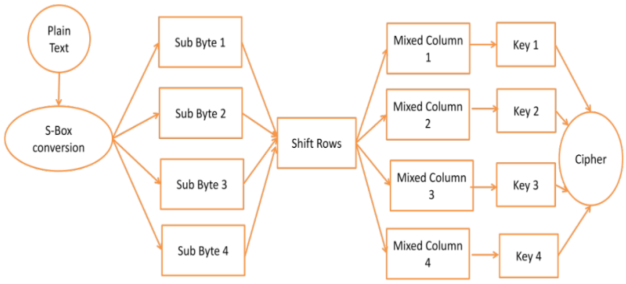

Fig 8: Parallel implementation of Proposed Algorithm

Again with the use of register based pipeling and using wave pipeline model we get a lot of further improvement in our model. Simple pipeline is given below which help us in reducing the latency up to 21 clock cycles.

Here we will introduce the pipelined architecture for reduction of the delay and increment of the throughput of overall circuit. The figure shown in fig 9 tells us how the data is moving through the registers a single key expansion unit is used for various round which saves the time for calculating the round key for each round. Further we can use this technique by this proposed architecture over the rounds to increase the throughput even saving the time.

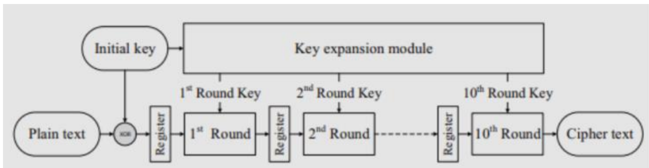

Fig 9: Pipelined proposed model

V. RESULTS

Here we talk about the yields obtained on Xilinx using the programmed codes in VERILOG language by us. Our first aim was to provide security in that order we have used our designed 8 bit LFSR code to obtain the 256 bits of information for designing the S-Box. Both of the S-Box matrixes are given in Table 1 and 2.

Table 1: Modified S-Box 1

80	40	20	10	88	c4	e2	71	38	1c	8e	47	23	91	48	a4
d2	e9	74	3a	1d	0e	07	03	81	c0	b0	30	98	4c	26	93
49	24	92	c9	64	b2	d9	ec	76	3b	9d	4e	27	13	09	04
82	41	a0	50	a8	d4	6a	b5	da	6d	b0	5b	ad	d6	6b	35
9a	4d	a6	d3	69	34	1a	0d	86	c3	e1	f0	f8	7c	be	df
6f	b7	db	ed	f6	7b	bd	5e	af	d7	eb	75	ba	5d	ee	17
8b	45	22	11	08	84	c2	61	b0	d8	6c	36	1b	8d	c6	e3
f1	78	3c	9e	cf	e7	73	39	9c	ce	67	33	19	8c	46	a3
d1	68	64	5a	2d	96	4b	25	12	89	44	a2	51	28	94	4a
a5	52	a9	54	2a	95	e5	72	b9	dc	ee	77	bb	dd	6e	37
9b	cd	e6	f3	79	bc	de	ef	f7	fb	fd	7e	bf	5f	2f	97
cb	65	32	99	cc	66	b3	59	ac	56	2b	15	8a	c5	62	31
18	0c	06	83	c1	e0	70	b8	5c	ae	57	ab	55	aa	d5	ea
f5	fa	7d	3e	9f	4f	a7	53	29	14	0a	85	42	21	90	c8
e4	f2	f9	fc	fe	ff	7f	3f	1f	0f	87	43	a1	d0	E8	f4
7a	3d	1e	8f	c7	63	b1	58	2c	16	0b	05	02	01	8a	4a

Table 2: Modified S-Box 2

1d	0e	07	03	81	c0	60	30	98	4c	26	93	49	24	92	c9
64	b2	d9	ec	76	3b	9d	4e	27	13	09	04	82	41	a0	50
a8	d4	6a	b5	da	00	6d	b6	5b	ad	d6	6b	35	9a	4d	a6
d3	69	34	1a	0d	86	c3	e1	f0	f8	7c	be	df	6f	b7	db
ed	f6	7b	bd	5e	af	d7	eb	75	ba	5d	2e	17	8b	45	22
11	08	84	c2	61	b0	d8	6c	36	1b	8d	c6	e3	f1	78	3c
9e	cf	e7	73	39	9c	ce	67	33	19	8c	46	a3	d1	68	b4
5a	2d	96	4b	25	12	89	44	a2	51	28	94	4a	a5	52	a9
54	2a	95	ca	e5	72	b9	dc	ee	77	bb	dd	6e	37	9b	cd
e6	f3	79	bc	de	ef	f7	fb	fd	7e	bf	5f	2f	97	cb	65
32	99	cc	66	b3	59	ac	56	2b	15	8a	c5	62	31	18	0c
06	83	c1	e0	70	b8	5c	ae	57	ab	55	aa	d5	ea	f5	fa
7d	3e	9f	4f	a7	53	29	14	0a	85	42	21	90	c8	e4	f2
f9	fc	fe	ff	7f	3f	1f	0f	87	43	a1	d0	e8	f4	7a	3d
1e	8f	c7	63	b1	58	2c	16	0b	05	02	01	80	40	20	10
88	c4	e2	71	38	1c	8e	47	23	91	48	a4	d2	e9	74	3a

Next we have obtained RTL schematic of pipelined AES in which all the input and output pins are given on RTL box. And afterward feed plaintext into the encryption module to produce the cipher text. Feed the cipher text into the unscrambling module to create the plaintext, and check that the plaintext that turned out is a similar that was placed in. RTL is shown in fig 10.

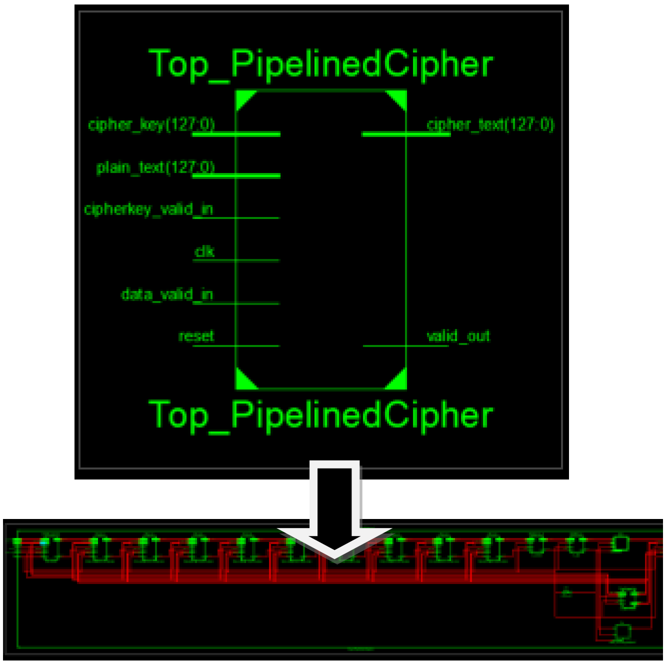

Fig 10: RTL Diagram of proposed AES model

This is the Verilog execution of the symmetric type of block cipher which is non other than AES as specified by NIST [2] FIPS 197. This execution upholds 128 bits of data.

This execution is iterative but support parallel processing also which makes the device faster. In this execution we have selected a powerful FPGA processor *VIRTEX 7 XC7VX330T* with package *FFG1157* and a speed factor of -3.

Now moving to simulation part of our result it contains the cipher text which is obtained by giving the input as well as key along with selecting the S-box matrix.

I-Sim (simulator tool of ISE) gives a total, full-included HDL test system incorporated inside ISE. HDL production presently can be a significantly increasingly essential advance inside your design stream with the tight incorporation of the I-Sim inside your structure condition. So the simulated results are given in fig 11.

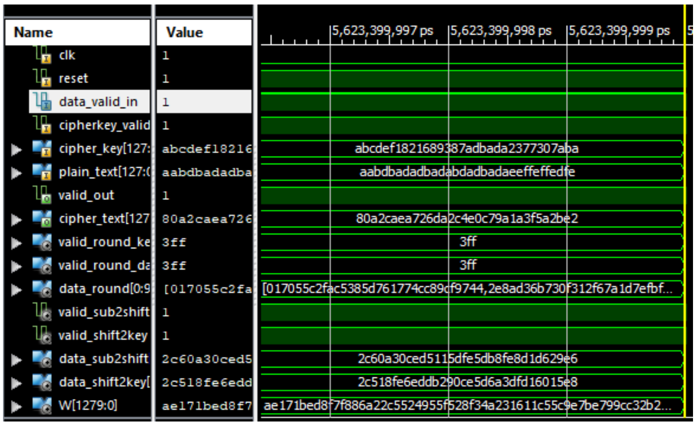

Fig 11: Simulated proposed model on ISIM

Here in the above figure Clk is given with 100ns period reset , valid data in and cipher_key_valid_in all set to the value 1. Cipher key is the password of 128 bit while plain text is input information of 128 bits. The obtained bit of result is given by cipher text as shown in fig 11.

Now finding the power and delay related results, they are obtained using X-Power analyzer and Timing analyzer of ISE 14.7. Timing Summary of the circuit is given by the fig 12.Which shows the delay is reduced from the base paper that is we have obtained a delay of 1.227 ns with a frequency of 814.846 MHz. Also the power results are given in fig 13 which is 0.179 W.

```
Timing Summary:
---------------
Speed Grade: -3

   Minimum period: 1.227ns (Maximum Frequency: 814.846MHz)
   Minimum input arrival time before clock: 1.008ns
   Maximum output required time after clock: 0.515ns
   Maximum combinational path delay: No path found
```

Fig 12: Timing Summary of proposed model

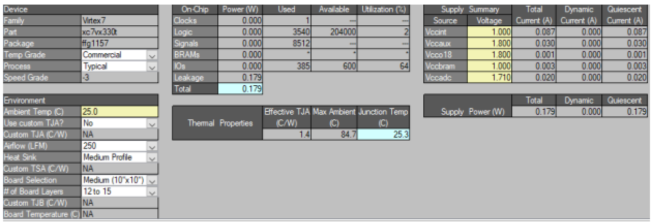

Fig 13: Power of proposed model

Amid HDL synthesis, *XST* breaks down the *HDL* code and endeavors to gather explicit structure building blocks or macros, (for example, *MUXs*, *RAMs*, adders, and subtractors) for which it can make effective innovation executions. So the device utilization report of these defined sub devices is depicted below in fig 14.

```
Advanced HDL Synthesis Report

Macro Statistics
# RAMs                                              : 200
 256x8-bit single-port distributed Read Only RAM    : 200
# Registers                                         : 10769
 Flip-Flops                                         : 10769
# Multiplexers                                      : 144
 8-bit 2-to-1 multiplexer                           : 144
# Xors                                              : 349
 128-bit xor2                                       : 11
 32-bit xor2                                        : 50
 8-bit xor2                                         : 144
 8-bit xor5                                         : 144
```

Fig 14: Advanced HDL of proposed model

VI. DISCUSSIONS

Here in this section we will talk about the analysis that are obtained while calculating results. Talking about *Avalanche Effect* [8] which says that for a single bit change in the input parameter results in abrupt change in output, to satisfy the condition that change must be more than 50 % of the previous output. Obtained analysis of this based on dynamic S-box is shown in fig 15.

Table 2: Avalanche Effect Test Datasheet

Sno.	State Matrix input (plain data) (hexadecimal)	Key used(hexadecimal)	Cipher output(hexadecimal)	Percentage Avalanche Effect
1	abcdef1234567890abcdef1234567890	98074433049807443304abcdef123456	be03e95de89849dc467a52d73738e85b	Test vector
2	bbcdef1234567890abcdef1234567890	98074433049807443304abcdef123456	9976bd8058536d38370968ec1c5a85fc	57.03
3	cbcdef1234567890abcdef1234567890	98074433049807443304abcdef123456	d3469e6499a7ad2eef8f8bcfc8386611	55.46
4	dbcdef1234567890abcdef1234567890	98074433049807443304abcdef123456	ba61c75ebfa0aa16f8da28244cfa7a89	54.69
5	aacdef1234567890abcdef1234567890	98074433049807443304abcdef123456	7e2eb2397e71b868f7d51f2cab5caa9e	58.59

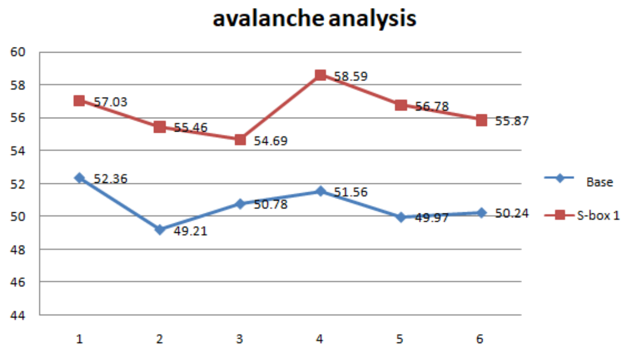

Fig 15: Avalanche Analysis of proposed model

Its clear that our designed S-Box performs better than the base or traditional S-Box so the overall security of the design is improved as well.
Further delay and frequency comparison chart is given in fig 16. This comparison is done on the basis of the base paper [1] vs proposed AES model.

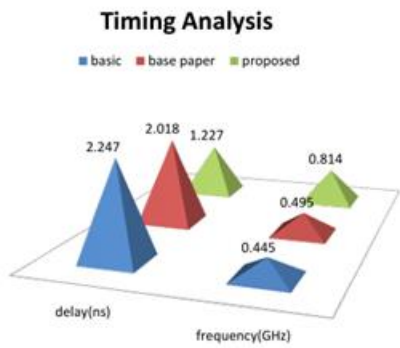

Fig 16: Frequency and time for basic vs. base paper vs. proposed

VII. CONCLUSIONS

The proposed calculation can be connected for any information type at any self-assertive length. This is a particularly attractive component for little organized information. It is basic and simple to actualize. It doesn't require any extra information.
In our design we find that overall delay is reduced by 45.39%, slice area is reduced to about 2.95%, and power is increased a little bit due to delay reduction that is 1.12%. Avalanche effect is improved in proposed design also from 50.78 % to 62.76%. And the most important thing that is throughput which is improved to 10.42 Gbps from 6.34 Gbps.

REFERENCES

1. Harshali Zodpe , Ashok Sapkal, An efficient AES implementation using FPGA with enhanced security features, Journal of King Saud University 2018 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University, 24 july 2018.

2. NIST,―Advanced.Encryption.Standard.‖http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, Nov. 2001.
3. Sumio Morioka and Akashi Satoh, ―An Optimized S-Box Circuit Architecture for Low Power AES Design‖, CHES 2002, LNCS 2523, pp. 172–186, 2003.
4. 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, pp.957-967, September 2004.
5. Bin Liu, Student Member, IEEE, and Bevan M. Baas, Senior Member, IEEE Parallel AES Encryption Engines for Many-Core Processor Arrays IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 3,MARC, March 2013.
6. Mohini Mohurle and Vishal V. Panchbhai Review on Realization of AES Encryption and Decryption with Power and Area Optimization 1st IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES-2016).
7. Han, Mangi & Kim, Youngmin. (2017). Unpredictable 16 bits LFSR-based true random number generator. 284-285. 10.1109/ISOCC.2017.8368897.
8. C.M.Adams and S.E.Tavares. (January 1990) ‗Achieve Higher-Order Strict Avalanche Criterion in S-Box Design'. Technical Report TR 90-013.
9. Francois Morain. (April 1997) ‗A History of Cryptology'. LIX, Ecole polytechnique. summary by Pierrick Gaudry. pp. 1-2.
10. George N.Selimis, Apostolos P.Fournaris and Odysseas Koufopavlou, Applying Low Power Techniques in AES MixColumn/InvMixColumn Transformations‖, ICECS, IEEE Conference Proceedings, pp.1089-1092, 2006.
11. Terence Spies,(2008) Feistel Finite Set Encryption Mode. NIST Proposed Encryption Mode. Available online at ffsem-spec.pdf. pp. 1-10.
12. Balamurugan, J. and Logashanmugam, E., ―Design of Efficient AES using modified Mix Column architecture‖, International Journal of Technology and Engineering Science (IJTES), Vol.1 (7), pp.1054-1059, Oct 2013.

AUTHORS PROFILE

ASHISH DWIVEDI received the B.Tech degree in Electronics and Communication Engineering from Shri Ramswaroop Memorial College of Engineering and Management, Abdul Kalam Technical University Lucknow, India and is currently working towards his M.Tech degree Microelectronics with the research interest in Digital VLSI and Cryptographic Circuit from Institute of Engineering and Technology,Lucknow,UP.

TOUSHIBA KHAN received the B.Tech degree in Electronics and Communication Engineering from Institute of Technology and Management, Gida, Gorakhpur India and is currently working towards her M.Tech degree Microelectronics with the research interest in NCL circuits and the filter designing from Institute of Engineering and Technology,Lucknow,UP.

Dr. S.R.P. Sinha received his B.Sc.(ECE) from B.I.T. Sindri (Ranchi University) in 1982. He had received his M.Tech (ECE) from University of Roorkee in 1984. He had also received his Doctor of Philosophy in field of electronics from Lucknow University in 2004 and currently serving as Professor in Institute of Engineering and Technology, Lucknow.