ISSN:0975-9646

Avalanche Effect of AES Algorithm

Jayant P. Bhoge, Dr. Prashant N. Chatur

Electronics and Telecommunication Department
Government College of Engineering,
Amravati, India.

Abstract— **Efficient implementation of block cipher is important on the way to achieving high efficiency with good understand ability. Numerous number of block cipher including Advance Encryption Standard have been implemented using different platform. However the understanding of the AES algorithm step by step is very complicated. This paper presents the implementation of AES algorithm and explains Avalanche effect with the help of Avalanche test result. For this purpose we use Xilinx ISE 9.1i platform in Algorithm development and ModelSim SE 6.3f platform for results confirmation and computation.**

Keywords: **AES, Avalanche effect, S-Box**

I. Introduction

Cryptography plays major role in information safety. Lots of cryptographic algorithms have been proposed such as the Data Encryption Standard (DES), the Elliptic Curve Cryptography (ECC), the Advanced Encryption Standard (AES) and other algorithms. Lots of researchers and hackers are always trying to break these algorithms using strongest brute force and side channel attacks. Some attacks were victorious as it was the case for the Data Encryption Standard in 1993, where the published cryptanalysis attack could break the DES. Now days as we know Advanced Encryption Standard (AES) are considered as one of the strongest possible cryptographic algorithms in the world, where it was adopted by the National Institute for Standards and Technology (NIST)[1] after the weakening of the Data Encryption Standard. AES is based on the block cipher Rijndael and became the selected successor of the Data Encryption Standard. This has been implemented in a tremendous number of cryptographic modules worldwide since 1977. Even though this implementation is fully operational (i.e. it can be utilized to encrypt illogically chosen plaintext into cipher text and vice versa). For Xilinx implementation of the Advanced Encryption Standard (AES) [6] [8] with Avalanche effect test results of same main consideration is to understand ability and avalanche effect of AES.

In this paper first section contains the introduction of AES algorithm, section 2 contain the internal structure of AES with algorithm, section 3 describes Avalanche effect and Test results and section 4 contains conclusion and last section contains references.

II. Internal Structure Of AES

AES is symmetric key block cipher. It uses a fixed 128-bit block cipher and three variable key lengths 128 bit, 192 bit and 256 bit supported by AES as this was an NIST design requirement. The number of internal rounds of the cipher is functions of the key length according to different key length number of rounds are shown in Table 1[5].

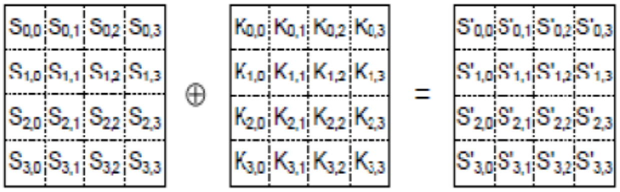
Table 1: Key length and number of rounds of AES

Block size (bits)	Key length (bits)	No. of Rounds
128	128	10
128	192	12
128	256	14

There are three different types of layers to perform AES operation and the function of the different layers is:

1.1 Key Addition Layer:

A 128-bit round key, or sub key, which has been derived from the main key in the key schedule, is XOR with the state[5].



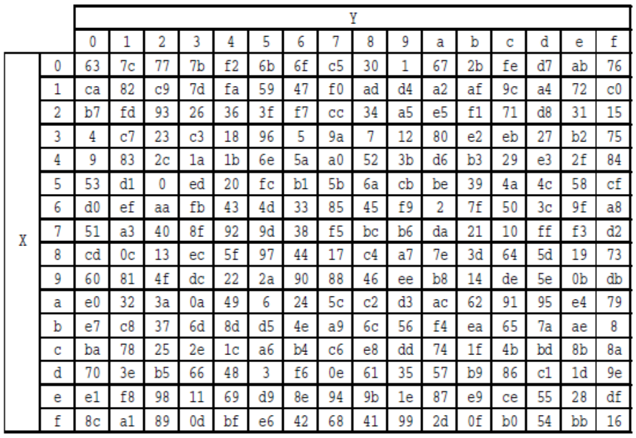
$$\begin{array}{|c|c|c|c|}\hline S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ \hline S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ \hline S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ \hline S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|}\hline K_{0,0} & K_{0,1} & K_{0,2} & K_{0,3} \\ \hline K_{1,0} & K_{1,1} & K_{1,2} & K_{1,3} \\ \hline K_{2,0} & K_{2,1} & K_{2,2} & K_{2,3} \\ \hline K_{3,0} & K_{3,1} & K_{3,2} & K_{3,3} \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ \hline S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ \hline S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ \hline S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \\ \hline \end{array}$$

Figure 1: Key Addition process

1.2 Confusion Layer:

It provides confusion by interchanging content state table of plaintext with other content

Byte Substitution layer (S-Box): Each element of the state is nonlinearly altered using lookup tables called as S-box (figure 1)[5] with special mathematical properties. This introduces confusion to the data plaintext data [1].



		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	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
	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	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	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

Figure 2: *S-Box*

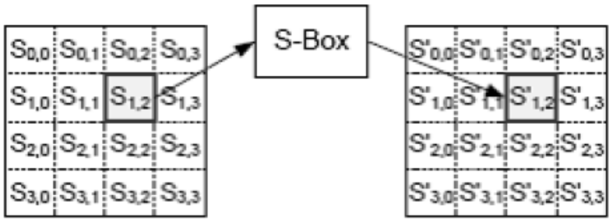

S-Box
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S'_{0,0}$ $S'_{0,1}$ $S'_{0,2}$ $S'_{0,3}$
$S'_{1,0}$ $S'_{1,1}$ $S'_{1,2}$ $S'_{1,3}$
$S'_{2,0}$ $S'_{2,1}$ $S'_{2,2}$ $S'_{2,3}$
$S'_{3,0}$ $S'_{3,1}$ $S'_{3,2}$ $S'_{3,3}$

Figure 3: **Byte Substitution Process**

1.3 Diffusion Layer:

It provides diffusion over all state bits. It consists of two sub layers, both of which perform linear operations:

Shift Rows layer: provides the mechanism for shifting the rows (Figure 4) [5] of the above layer output.

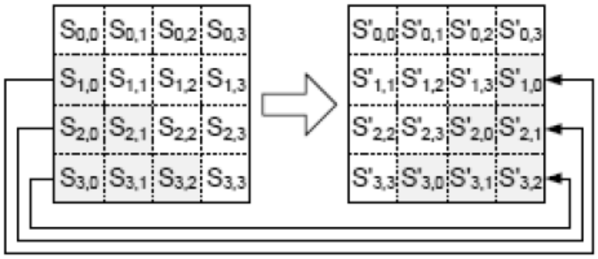

$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S'_{0,0}$ $S'_{0,1}$ $S'_{0,2}$ $S'_{0,3}$
$S'_{1,1}$ $S'_{1,2}$ $S'_{1,3}$ $S'_{1,0}$
$S'_{2,2}$ $S'_{2,3}$ $S'_{2,0}$ $S'_{2,1}$
$S'_{3,3}$ $S'_{3,0}$ $S'_{3,1}$ $S'_{3,2}$

Figure 4: Shift Row Process

Mix Column layer: is a matrix operation where each 4-byte column is considered as a vector and multiplied by a fixed 4×4 matrix. The matrix contains constant entries (Figure 5) [5].

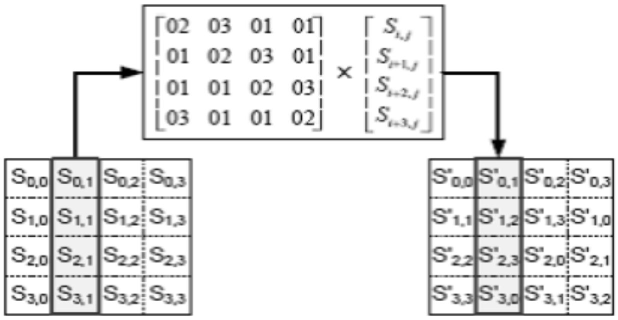

$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} S_{i,j} \\ S_{i+1,j} \\ S_{i+2,j} \\ S_{i+3,j} \end{bmatrix}$
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S'_{0,0}$ $S'_{0,1}$ $S'_{0,2}$ $S'_{0,3}$
$S'_{1,1}$ $S'_{1,2}$ $S'_{1,3}$ $S'_{1,0}$
$S'_{2,2}$ $S'_{2,3}$ $S'_{2,0}$ $S'_{2,1}$
$S'_{3,3}$ $S'_{3,0}$ $S'_{3,1}$ $S'_{3,2}$

Figure 5: Mix Column Process

The complete process of the AES is shown in figure 6 [5]. Last round of the AES does not contain mix column step which makes it stronger. Decryption process is reverse of encryption processes which perform inverse byte substitution operation, inverse shift row and inverse mix column

In this algorithm figure 6.a [5] shows the input plaintext which is the size of 128 bit, key which is 128 bit, 192 bit or 256 bit long, cipher text which is of the length 128 bit long. The number of rounds depends upon the size of the key which varies from 10 to 14. Cipher text output from encryption algorithm is given to the input of the decryption algorithm to recover the original plaintext keeping key constant as given to encryption algorithm.

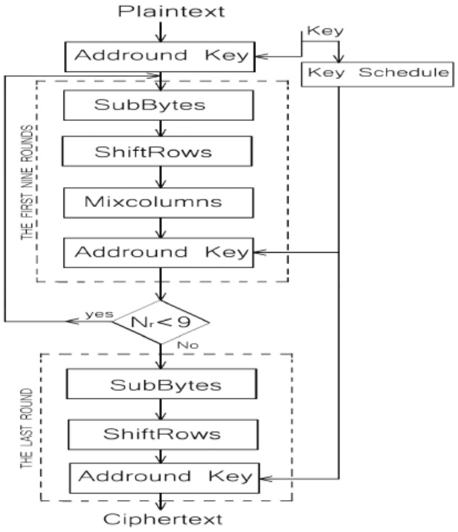


Figure 6.A: Encryption Algorithm

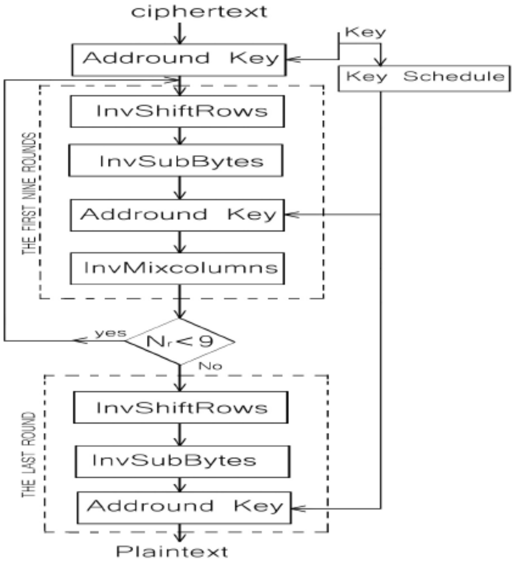


Figure 6.B: Decryption Algorithm

Figure 6: Block diagram of the AES algorithm[5]

III. Avalanche Effect And Test

3.1 Avalanche effect

It is important characteristic for encryption algorithm. This property can be seen when changing some bit in plaintext and then watching the avalanche change in the outcome of the bits in the cipher text [7]. Consider if function $F : \{i,j\}^n$ here $\{i,j\}^n$ satisfy avalanche criteria when one input bit is changed at least half of bit in output bit change. Where i and j are input and output bits, as per avalanche criteria

$$\frac{1}{2^n}\sum_{j=1}^{n} W\left(a_j^n\right) = \frac{n}{2} \qquad (1)$$

Where $W\left(a_j^n\right) = \sum_{j=1}^{n} a_j^n$ all x: $\{0,1\}^n$ (2)

Total change in j^{th} avalanche variable computed over whole input size 2^n in range $0 \leq W(a_j^{e_i}) \leq 2^n$

From equation 1 we can manipulate avalanche parameter of i as

$$K_{avalance}(i) = \frac{1}{n2^n}\sum_{j=1}^{n} W\left(a_j^{e_i}\right) = \frac{1}{2} \qquad (3)$$

With above formula it is proved that probability of change of output bit when only one or i^{th} bit of input is changed is half.

3.2 Avalanche Test

In avalanche test of AES First we start calculate avalanche effect for AES S-box. To perform the test we change plaintext bits keeping key constant "FED4698745232568C789654123569999FED4698745232 568C789654123569999" to all plain text. We use "22" instead of "21" and "77" instead of "71" and "66" instead of "65" the result obtained is .3593, .4921 and .4453 respectively

Plain text	Cipher text	Avalanc-he test results
F222222222222222 2222222222222222	865DE1D46C789FE1 4DEF12C789D4E125	.359375 (46)
F222222222222222 2222222222222221	9457DEC235EDCB75 84DE1245698CEF25	
5555333388887777 5555333388887777	C7D4563E125697CE D456998231457DEF	.492187 (63)
5555333388887777 5555333388887771	E1236845CD4795ED C8965324DC7821EB	
AA11223344556666 AA11223344556666	F1254DCD478C56DE D456987E123D4789	.4453125 (57)
AA11223344556666 AA11223344556665	125478DEC4E1F25C D4698234D7D45DE1	

Observation: From the above result it is clear that cipher text is very strong for very simple plaintext.

IV. Conclusion

The AES provides a reasonably high level of security with efficient implementation, and it is likely to remain a strong algorithm for some time to come. This paper presents the implementation of AES algorithm which also shows the Avalanche effect and understands ability of the AES algorithm. AES is the very strong cipher and impossible to break without knowing the key so the importance of AES algorithm is high security. The complex process of AES algorithm can be comfortably implemented on Xilinx platform and result validated with ModelSim SE 6.3f platform.

Acknowledgment

No words are sufficient to express deep sense of gratitude to my family for support, love and care also I am grateful to my project guide for valuable suggestions, comments and contribution.

References

[1] J. Daemen, and V. Rijmen, "The Design of Rijndael: AES-the Advanced Encryption Standard", Springer-Verlag, 2002

[2] FIPS 197, "Advanced Encryption Standard (AES)", November 26, 2001.

[3] H. Trang, N. V. Loi, "An efficient FPGA implementation of the Advanced Encryption Standard algorithm," IEEE, 978-1-4673-0309-5/12/$31.00, 2012.

[4] W. wai, C. Jie, X. Fei, "An Implementation of AES Algorithm Based on FPGA," 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012), IEEE, pp. 1615-1617, 2012.

[5] N. Bhat, v. Shridhar, "FPGA Implementations of Advanced Encryption Standard: a survey," International Journal of Advances In Engineering & Technology, vol. 3, issue 2, pp. 265-285, 2012.

[6] S. Venkateswarlu, Deepa G. M, G. Sriteja, "Implementation of Cryptographic Algorithm on FPGA," International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 4, pp. 604 – 609, April 2013.

[7] I. Vergili, M. D. Yucel, "Avalanche and bit independent property for the Esembles of randomely choosen NxN S-boxes," EE dept of METU.

[8] A. M. Borkar, Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare, "FPGA Implementation of AES Algorithm", International Conference on Electronics Computer Technology (ICECT), pp. 401-405, 2011 3rd.