© 2017 IJSRST | Volume 3 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X

National Conference on Advances in Engineering and Applied Science (NCAEAS)
16th February 2017
In association with
International Journal of Scientific Research in Science and Technology

Fault Detection Countermeasures using AES

Priyanka Dhok, Sneha Barwad, Kalyani Patil, Vikram Deshmukh

Electronics and Telecommunication, Smt. Rajashree Mulak Collage of Engineering for Womens, Affiliated to RTM University, Maharashtra India

ABSTRACT

For security purpose, cryptography method is implemented through which communicated data is secured. Advanced Encryption Standard (AES) is the first choice for many critical applications. Federal Information Processing Standard (FIPS) consisting AES tool which is cryptographic algorithm used to secured electronic data. Implementations of the Advanced Encryption Standard (AES) has been used in various applications data-telecommunications, finance and networks that require low power consumptions, low cost design, less delay and specially it should be more secured. In this paper, the implementation details of the AES 128-bit Encryption and Decryption is presented. We will conduct a fault injection attack against the unprotected AES. Moreover we proposed a fault detection scheme for the AES. AES can be programmed in software or built with pure hardware. However Field Programmable Gate Arrays (FPGA) offer a quicker, more customizable solution. The protected AES has been implemented on Xilinx Nexus-3 FPGA. Its fault coverage, area overhead, frequency degradation, power and throughput have been compared. and it is shown that the proposed fault detection scheme allows maximum fault coverage and implemented design have low area, less hardware requirement and is more power efficient.

Keywords: AES, FIPS, FPGA, NIST, WiMAX, AES Encryption, SubByte Transformation, Inversion, GF Linear Mapping, Sbox Table, ShiftRows Tranformation, AddRoundKey, AES Decryption, InvShiftRows Transformation

I. INTRODUCTION

The National Institute of Standards and Technology (NIST) standardized the Advanced Encryption Standard. The AES is Federal Information Processing Standard which is cryptographic algorithm used to protect electronic data.

The algorithm described by AES is a symmetric key algorithm that can encrypt,(encipher), and decrypt, (decipher), data. Encryption converts data to an unintelligible form called cipher-text. The decrypt cipher-text converts the data back into its original form, which is called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data. Symmetric key cryptography uses a shared key in both sender and receiver ends during encryption and decryption for secure communications. [1]

For the drawbacks of the previous symmetric-key cryptographic standards such as the DES and the 3DES, they have been replaced by the Advanced Encryption Standard (AES). In particular, the AES has overcome the drawbacks of the previous standards has overcome by AES in terms of vulnerability to brute symmetric-key cryptographic standards such as the DES and the 3DES, they have been replaced by the Advanced Encryption Standard (AES) . [2]

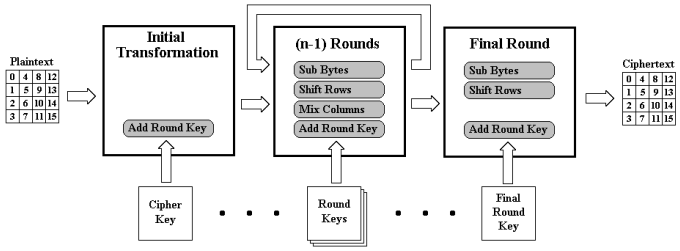
The AES was accepted in 2001 by the National Institute of Standards and Technology (NIST) and since its acceptance, it has been utilized in a variety of security-constrained applications. For instance, it has been included in wireless standards of Wi-Fi as well as WiMAX and many more other applications, ranging from the security of smart cards to the bit stream security mechanisms in FPGAs. Various hardware implementation architectures of AES algorithm have been proposed and their performances are evaluated.[3,4]

In this paper, Encryption and Decryption process of AES algorithm is implemented a fault attack is conducted and fault detection scheme is applied. Maximum fault coverage is achieved through this detection scheme and then different parameters like Area, Hardware requirement is to be compared. Power analysis is to be performed to show that proposed design is more power efficient.[5,6]

The rest of the paper is organized as follows: The basic structure of AES is given in section II. The Encryption process of AES is explained in section III. The Decryption process of AES is explained in section IV. The experimental synthesis results as well as the performances report of the AES encryption and decryption are discussed in section V. Section VI concludes the paper.

II. AES ALGORITHM

In AES algorithm, Data is encrypted or decrypted in blocks of 16 bytes. The state is manipulated internally during a variable number of rounds. There are 10,12, or 14 rounds needed for cipher keys of length 128, 192, or 256 bits respectively.



1. AES Encryption

AES encrypt information by repeatedly using four kinds of data transformations: SubBytes, ShiftRows, MixColumns and AddRoundKey while the final round does not have the MixColumns transformation. Each round contain four transformations (linear and non linear) called Layers. Each round has round key derived from original key. Round transformation and its steps generate intermediate data called States. State considered as rectangular array of bytes with four rows and no. of columns that depend on size of key length.

Key length: 128 bit
Key arranged in 4*4 matrix
Each element is byte.

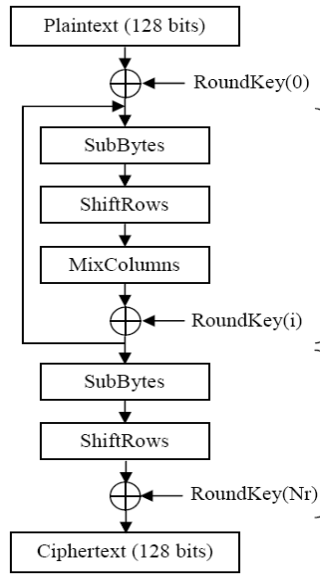
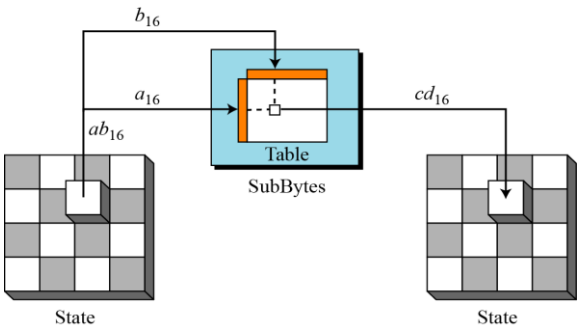


Figure 1. AES Encryption Structure

A. SubByte Transformation

This is the only non linear part of algorithm assures resistance to differential and linear cryptanalysis attacks this transformation consist of S-box which is applied to each byte element of state (16 byte block) independently and has 3 different steps:

1. Inversion
2. A Galois field linear mapping
3. S-box constant



B. Inversion

In this operation of s-box, inverse is computed in 8bit Galois field, GF (2^8).the byte 00000000 has no inverse and 00000000 is used in place of its inverse.

Assume $x_7x_6x_5x_4x_3x_2x_1x_0$ byte which comes up from inversion $y_7y_6y_5y_4y_3y_2y_1y_0$ represent 8 element column vector with rightmost binary bit y_0 in top position this operation provides resistance against linear and differential cryptanalysis attack.

2. GF Linear Mapping

At this pt. y vector is multiplied by constant matrix and column vector (0,1,1,0,0,0,1,1) is added yielding vector $z_7z_6z_5z_4z_3z_2z_1z_0$.

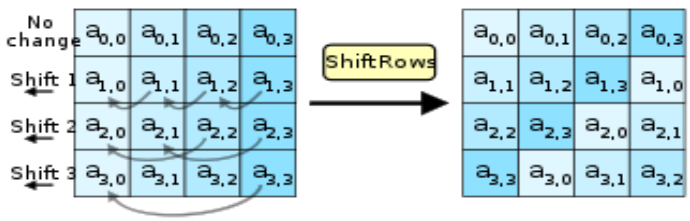
3. Sbox Table

It is basic component of symmetric key algorithms. It performs substitution S box often implemented as lookup table. Each of 256 possible byte values is transformed to another byte value with the sub bytes transformation, which is full permutation meaning that every element gets changed and all 256 possible elements are represented a result of change so that no two different bytes are changed to same byte. The sub byte transformation carried out by s-box is most time consuming procedure in AES. The strength of cryptographic algorithms is determined by non linear s boxes.

x \ 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
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

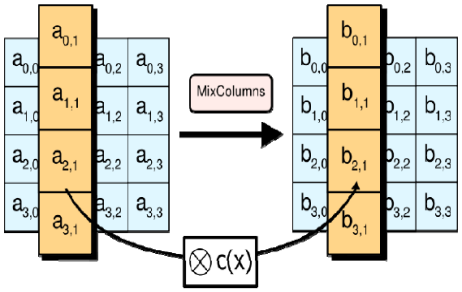
A. ShiftRows Tranformation

It is linear transformation. This provides resistance against truncated differential and saturation attacks. The ShiftRows transformation is a circular shifting operation on the rows of the state with various numbers of bytes. The first row of the state is kept as it is, while the second, third and fourth rows cyclically shifted by one byte, two bytes and three bytes to the left respectively.



B. MixColumn Tranformation

This transformation operates on each 4 byte column separately and is omitted in last round. Columns of state are considered as polynomials over GF (2^8) which are multiplied by fixed polynomial c(x) modulo (x^4+1) .

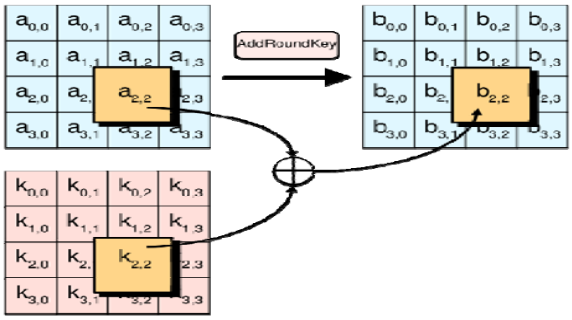


Fixed polynomial c(x) is given by
$c(x)= \{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$
In matrix form, the MixColumns transformation can be expressed as:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

C. AddRoundKey

The add round Key is a XOR operation that adds a round key to the state in each iteration, where the round keys are generated during the key expansion phase .Key consisting of 128 bits which are arranged in 4*4 byte matrix is added to output of mix column transformation. A different round key is added to state at end of each round.



4. AES Decryption

The transformations in the decryption process perform the inverse of the corresponding transformations in the

encryption process. In the AES decryption rounds, four transformations are used : InvShiftRows, InvSubBytes, AddRoundKey and InvMixColumns.

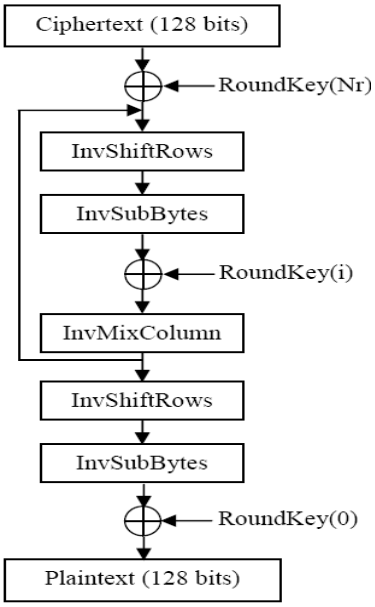


Figure 2. AES decryption Structure

A. InvByteSub Transformation

It consist of inverse S-box. The inverse transformation of equation that was made in ByteSub transformation is performed. For linear mapping:

$$\begin{bmatrix} 0&1&0&1&0&0&1&0\\ 0&0&1&0&1&0&0&1\\ 1&0&0&1&0&1&0&0\\ 0&1&0&0&1&0&1&0\\ 0&0&1&0&0&1&0&1\\ 1&0&0&1&0&0&1&0\\ 0&1&0&0&1&0&0&1\\ 1&0&1&0&0&1&0&0 \end{bmatrix} \times \begin{bmatrix} a_7\\ a_6\\ a_5\\ a_4\\ a_3\\ a_2\\ a_1\\ a_0 \end{bmatrix} \oplus \begin{bmatrix} 0\\ 0\\ 0\\ 0\\ 0\\ 1\\ 0\\ 1 \end{bmatrix} = \begin{bmatrix} b_7\\ b_6\\ b_5\\ b_4\\ b_3\\ b_2\\ b_1\\ b_0 \end{bmatrix}$$

Following is the inverse S-box used in the decryption process:

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

B. InvShiftRows Transformation

In this transformation opposite shifting operation applied. Therefore rows are shifted to right instead to left, which takes place at shiftrows transformation.

C. InvMixColumn Transformation

In this transformation, every column is multiplied by inverse polynomial of c(x)(mod x^4+1) which is

d (x)= {0B}.x^3 +{0D}.x^2+{09}.x+{0E}

The inverse matrix multiplication of equation which was used in mixcolumn transformation:

$$\begin{bmatrix} b_0\\ b_1\\ b_2\\ b_3 \end{bmatrix} = \begin{bmatrix} 0E&0B&0D&09\\ 09&0E&0B&0D\\ 0D&09&0E&0B\\ 0B&0D&09&0E \end{bmatrix} \times \begin{bmatrix} a_0\\ a_1\\ a_2\\ a_3 \end{bmatrix}$$

This transformation is omitted in last round.

D. InvAddRoundKey Transformation

This transformation applies keys that were used in encryption process in reverse order. The AddRoundKey is the same for both encryption and decryption.
Block diagram of AES encryption and decryption is shown in Fig.1 and Fig.2 respectively.
In this paper, we consider the implementation of 128bit key system only, as this is the most commonly implemented form of AES.

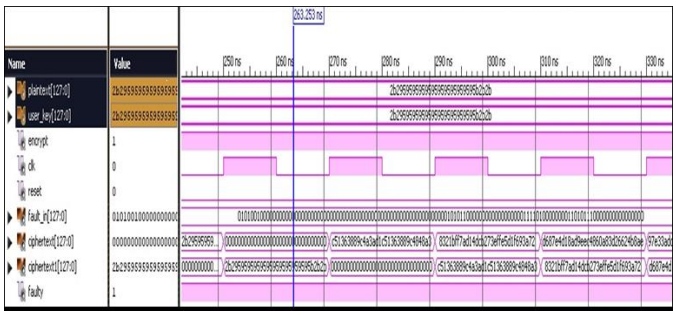
5. AES Implementation: Results and Conclusion

The AES Encryption and decryption have been described using VHDL and simulated using Model Sim and synthesized using Xilinx ISE13.1.

As seen in the table, the number of occupied slices, frequency, the throughput, efficiency and the power required for AES encryption and decryption are presented.

AES Design	Area	Frequency	Throughput	Efficiency	Power
Conventional Encryption	250	3.356ns	3.806 W	297.97 MHZ	3814.06 Mbps
Proposed Encryption	270	3.343ns	3.3809 W	299.155 MHZ	3829.12 Mbps

III. RESULT



IV. CONCLUSION

In this paper, in order to improve the security of the AES. AES algorithm in encryption and decryption is implemented. And the parameters like Area, Frequency, Throughput, Efficiency and power analysis is performed. From the above paper we see that after injecting and detecting the fault in any signal, the throughput of the signal decreases.

AES Design	Area(Slice)	Frequency	Throughput
Encryption without countermeasure	270	299.15MHz	3829.12Mbps
Encryption with countermeasure	430	218.98MHz	2802.944Mbps

V. REFERENCES

[1]. Paolo Maistri And Regis Leveugle "Double-Data-Rate Computation As A Countermeasure Against Fault Analysis" Ieee Transactions On Computers, Vol. 57, No. 11, November 2008.

[2]. Hassen Mestiri, Noura Benhadjyoussef, Mohsen Machhout And Rached Tourki "An Fpga Implementation Of The Aes With Fault Detection Countermeasure"Ieee Conference 2013.

[3]. Mehran Mozaffari-Kermani, ,Arash Reyhani-Masoleh "Concurrent Structure-Independent Fault Detection Schemes For The Advanced Encryption Standard" Ieee Transactions On Computers, Vol. 59, No. 5, May 2010

[4]. Mao-Yin Wang, Chih-Pin Su, Chia-Lung Horng,Cheng-Wenwu,And Chih-Tsun Huang"Single- And Multi-Core Configurable Aes Architectures For Flexible Security" Ieee Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 18, No. 4, April 2010.

[5]. Kaijie Wu Ramesh Karri,Grigori Kuznetsov,Michael Goessel"Low Cost Concurrent Error Detection For The Advanced Encryption Standard", Itc International Test Conference 2004.

[6]. Mehran Mozaffari-Kermani Arash Reyhani-Masoleh "A High-Performance Fault Diagnosis Approach For The Aes Subbytes Utilizing Mixed Bases" 2011 Workshop On Fault Diagnosis And Tolerance In Cryptography.