Journal of Nonlinear Analysis and Optimization
Vol. 11(7) (2020), July 2020
https://ph03.tci-thaijjo.org/
ISSN : 1906-9685

J.Nonlinear Anal. Optim

An On-Chip Delay Measurement Technique for Small-Delay Defect DetectionUsing Signature Registers

Dr.T.Krishnamoorthy
Associate Professor, Department of ECE
Sri Sai Institute of Technology and Science, Rayachoti
Email: krishnamoorthyphd@gmail.com

***Abstract*-With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. In data and telecommunications, cryptography is necessary when communicating over any unreliable medium, which includes any network particularly the internet. The Advanced Encryption Standard (AES) is the newly accepted symmetric cryptography standard for transferring block of data securely. The AES algorithm defined by the National Institute of Standard and Technology (NIST) of United States has been widely accepted. AES involves the sequence of four primitive functions: Sub Bytes, Shift Rows, MixColumn and Add Round Key. This paper presents the design of a 128 bit encryptor using AES Rijndael Algorithm for 128 bit data encryption. These designs were described using VerilogHDL. Xilinx ISE 14.2 software is used for synthesis.**

Keywords- AES, Cryptography, Encryption, S-box.

I. INTRODUCTION

Information is significant in every aspect of human life. Like any other property, it needs protection. There are different cryptographic algorithms available to secure information. However, most of them are computationally intensive, either deals with huge numbers and complex mathematics or involves several iterations [7]. There are mainly two types of cryptographic algorithms: symmetric and asymmetric algorithms. Symmetric systems such as Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) use an identical key for the sender and receiver; both to encrypt the plain text and decrypt the cipher text. Asymmetric systems such as Rivest-Shamir- Adelman (RSA) & Elliptic Curve Cryptosystem (ECC) uses different keys for encryption and decryption. Symmetric cryptosystems is more suitable to encrypt large amount of data with high speed. To replace the old Data Encryption Standard, in September 12 of 1997, the National Institute of Standard and Technology (NIST) required proposals to what was called Advanced Encryption Standard (AES).Many algorithms were presented originally with researches from 12 different nations. On October 2nd 2000, NIST has announced the Rijndael Algorithm is the best in security, performance, efficiency, implement ability & flexibility. The Rijndael algorithm was developed by Joan Daemen of Proton World International and Vincent Rijmen of Katholieke University at Leuven [3].AES is a simple design, a high speed algorithm, with low memory costs. AES is a symmetric block cipher. The same key is used to encrypt and decrypt the data. The plain text and the cipher text are the same size. AES is an algorithm for performing encryption (and the reverse, decryption) which is a series of well-defined steps that can be followed as a procedure. The original information is known as plaintext, and the encrypted form as cipher text. The cipher text message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it; it should resemble random gibberish to those not intended to read it. The encrypting

procedure is varied depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher cannot be used to encrypt or decrypt. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits [2].

A symmetric cryptosystem is shown in Fig.1 and has five ingredients:

a. Plain text: this is the original message or data that fed into the algorithm as input.
b. Encryption algorithm: the algorithm performs various substitutions and transformations on the plaintext.
c. Secret key: this is also an input to the algorithm and its value is independent of the plaintext. The algorithm will produce a different output depending on the specific key.
d. Cipher text: this is the scrambled message produced as output. It depends on the plaintext and the secret key.
e. Decryption algorithm: this is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext [3].

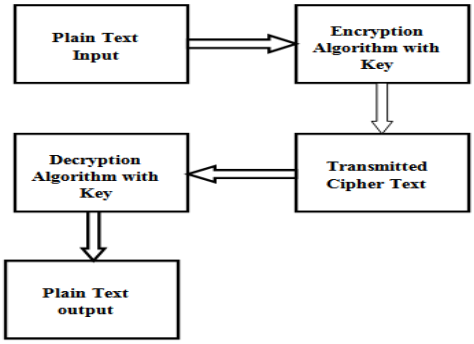

Fig.1 General Block diagram of symmetric cryptosystem

II. LITERATURE SURVEY

With the use of more handheld wireless devices and increasing networking and wireless data transfer, the issue of security is being addressed from many different directions. The National Institute of Standards and Technology (NIST) selected the Rijndael algorithm as a new Advanced Encryption Standard (AES) [1] in 2001. This standard was first developed for secure data encryption/decryption for high-end applications. In [2] [7] authors used AES algorithm for a high speed and low power consumption hardware implementation to encrypt the image. For increase speed he used 4 pipeline stages and also for reducing power consumption resource sharing, pipelining and signal gating techniques used. Paper [3] presents the design of a 128 bit encoder using AES Rijndael Algorithm for image encryption to protect the confidential image data from unauthorized access. The paper [4] compares the hardware efficiency of different AES implementations with respect to their area, speed and power performance especially in two different styles – one using controller based design can infer that power dissipation is more and the other one is iterative method and can infer that iterative method utilizes less number of hardware units compared to the controller method. In [5] authors show how the AES can be programmed in software or built with hardware. Software is used for simulation and optimization of the synthesizable VHDL code and all the transformations of algorithm are simulated using an iterative design approach in order to minimize the hardware consumption. In [6] author introduces new efficient hardware implementations for the Advanced Encryption Standard (AES) algorithm. Two main contributions are presented in this thesis to achieve higher FPGA (Throughput/Area) efficiency comparing to previous loop unrolled designs. The first one is a high speed 128 bits AES encryptor, and the second one is a new 32 bits AES design. In [8] paper mainly focused in implementation of AES encryption and decryption standard AES-128. All the transformations of both Encryption and Decryption are simulated using an iterative design approach in order to minimize the hardware consumption.

III. THE ORIGINS OF AES

The principal drawback of 3DES (which was recommended in 1999, Federal Information Processing Standard FIPS PUB 46-3 as new standard with 168-bit key) is that the algorithm is relatively sluggish in

software. A secondary drawback is the use of 64-bit block size. For reasons of both efficiency and security, a larger block size is desirable.

In 1997, National Institute of Standards and Technology NIST issued a call for proposals for a new Advanced Encryption Standard (AES), which should have security strength equal to or better than 3DES, and significantly improved efficiency. In addition, NIST also specified that AES must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits.

In a first round of evaluation, 15 proposed algorithms were accepted. A 2nd round narrowed to 5 algorithms. NIST completed its evaluation process and published a final standard (FIPS PUB 197) in November, 2001. NIST selected Rijndael as the proposed AES algorithm. The 2 researches of AES are Dr. Joan Daemon and Dr. Vincent Rijmen from Belgium.

1. AES Evaluation

i. Security – 128 minimal key size provides enough security
ii. Cost – AES should have high computational efficiency

i. Security: This refers to the effort required to cryptanalyze an algorithm. The emphasis in the evaluation was on the practicality of the attack. Because the minimum key size for AES is 128 bits, brute-force attacks with current and projected technology were considered impractical. Therefore, the emphasis, with respect to this point, is cryptanalysis other than a brute-force attack.

ii. Cost: NIST intends AES to be practical in a wide range of applications. Accordingly, AES must have high computational efficiency, so as to be usable in high-speed applications, such as broadband links [5].

2. The AES Cipher

The AES Algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits, while the length can be 128, 192, or 256 bits. In addition, the AES algorithm is an iterative algorithm. Each iteration can be called a round, and the total number of rounds is 10, 12, or 14, when key length is 128,192, or 256, respectively. The 128 bit data block is divided into 16 bytes. These bytes are mapped to a 4x4 array called the State, and all the internal operations of the AES algorithm are performed on the State [2][3][4][1].

Table I :AES Parameters

Algorithm	Key length (Nk words)	Block size(Nb words)	Number of rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

IV. DESIGN OF 128 BIT ENCODER

1. Methodology

The encryption process is iterative in nature. Each iteration is known as rounds. For each round 128 bit input data and 128 bit key is required. That is, need 4 words of key in one round. So the input key must be expanded to the required number of words, which depends upon the number of rounds. The output of each round serves as input of next stage. In AES System, same secret key is used for both encryption and decryption. So it provides simplicity in design.

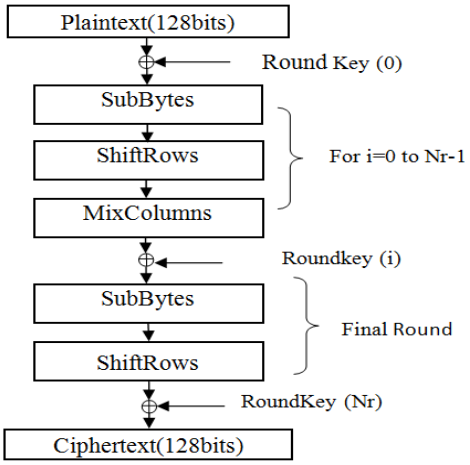

Fig.2 Detailed Block diagram of an encryption

In the encryption of the AES algorithm (Fig.2), each round except the final round consists of four transformations: The four stages of AES encryption transformation are as follows:

i. SubBytes: Operates in each byte of the State independently. Each byte is substituted by corresponding byte in the S-box.
ii. Shift Rows: Cyclically shifts the rows of the State over different offsets.
iii. MixColumns: In this operation the column of the State are considered as polynomials over GF (2^8) and are multiplied with a fixed polynomial. The MixColumn component does not operate in the last round of the algorithm.
iv. AddRoundKey: Involves bit-wise XOR operation [3].

2. DESIGN STEPS AES ALGORITHM

2.1 SubBytes Transformation

AES defines a 16 x 16 matrix of byte values called an S-box, that is a pre calculated substitution table contains 256 numbers (from 0 t0 255) and their corresponding resulting values. S-box table is as shown in Table II. Each byte of State array is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the right most 4 bits are used as a column value [3] [8]. These row and column values serve as indexes into the S-box to select a unique 8-bit output value as shown in Fig.3.

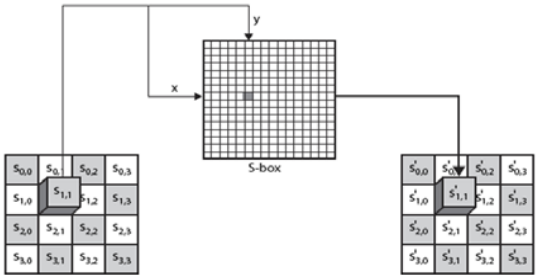

Fig.3 S-box transformation

Table II: S-box table

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

2.2 Shift Rows Transformation

Every row in the state is shifted a certain amount to the left. In this operation, each row of the state is cyclically shifted to the left, depending on the row index. The first row is not shifted, the second shifted 1 byte position, the third 2 byte and the fourth 3 byte position [1]. A graphical representation of shiftrows transformation is shown Fig.4.

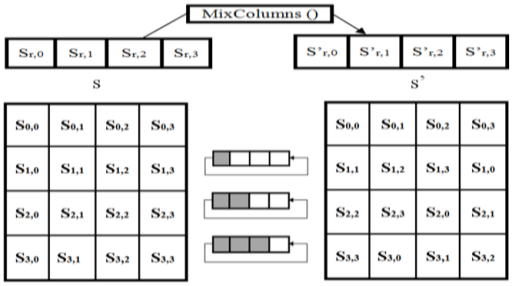

Fig.4 Shift Rows transformation

2.3 MixColumns Transformation

MixColumn operation (Fig.5) performs on the state column by column, and each column is treated as a four term Polynomial over GF (2^8) As a result of this multiplication, the new four bytes in a column are generated as follows [4]:

$$A' = (\{02\}.A)\wedge(\{03\}.B)\wedge\{01\}.C)\wedge(\{01\}.D)\quad B' = (\{01\}.A)\wedge(\{02\}.B)\wedge(\{03\}.C)\wedge(\{01\}.D)$$
$$C' = (\{01\}.A)\wedge(\{01\}.B)\wedge(\{02\}.C)\wedge(\{03\}.D)\quad D' = (\{03\}.A)\wedge(\{01\}.B)\wedge(\{01\}.C)\wedge(\{02\}.D)$$

…..... (1)

The operation of '^' is XOR operation modulo 2 and the '.' is a multiplication of polynomials modulo an irreducible polynomial $m(x) = x8 + x4 + x3 + x + 1$.The operation of $\{02\}.X$ can be computed using VerilogHDL HDL language:

$$\{02\}.X = \{X[6:0],1'b0\}\wedge(8'h1B \,\&\, \{8\{X[7]\}\}) \qquad \text{..... (2)}$$

So $\{03\}\_X$ can be generated as follows [4]:

$$\{03\}.X = (\{02\}.X) + \{01\}.X \,(3)$$

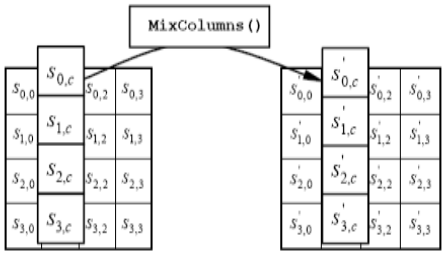

Fig.5 MixColumns transformation

2.4 AddRoundKey Transformation

AddRoundKey operation is only a simple logical XOR of the state using a round key which is produced by the key expansion operation [4] [1]. The action of this transformation is shown in Fig.6.

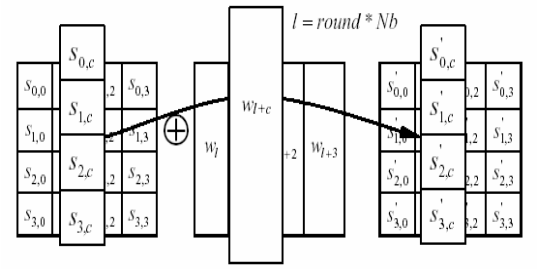

Fig.6 AddRoundKey XORs each column of the state with a word from the key schedule

2.5 Key Expansion

The AES algorithm takes the Cipher Key and performs a Key Expansion routine to generate a key schedule [3]. This process, as shown in Fig.6, consists of the following sub-functions:

- RotWord performs a one-byte circular left shift on a word.
- SubWord performs a byte substitution on each byte of its input word using the S-box.
- The result of steps i and ii is XOR-ed with a round constant RC[j] is shown in Table III.

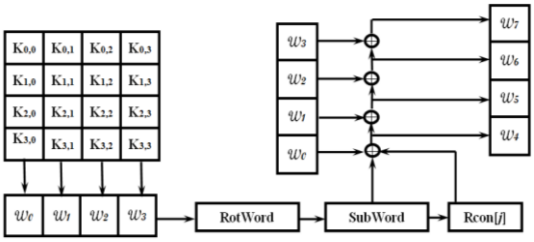

Fig.7 Key Expansion process

Table III: The value RC[j] in Hexadecimal

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

V. SIMULATION RESULTS

Each round has 4 operations and it is iterative in nature. So the output of first round is fed to the second round as input data and performs the same operations with another set of keys. This process continued until the last round reach. In the last round, there is no MixColumn operation. The State array obtained after the last round is the required cipher text for transmission (Fig.8) and Simulation Results For Different Combination Of Input Data is as shown in Table IV.

Encryption Process (Cipher):
AES block length/Plain Text = 128bits (Nb = 4)
Key length = 128 bits (Nk = 4);
No. of Rounds = 10(Nr = 10)
Input data
[11223344aabbccddeeffaabbccddeeff]
Input key
[000102030405060708090a0b0c0d0e0f]
Output/Cipher text
[5c5c68c3db976831d7785e924ae986c0]

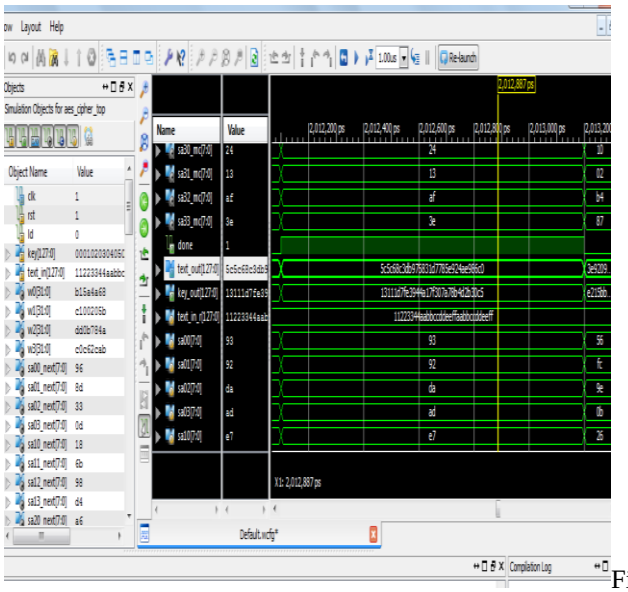

Fig.8 Simulation Waveform of Encrypted data

Table IV Simulation Results For Different Combination Of Input Data

Sr No	Input data	128 Bit key	Encrypted data
1	00112233445566778899aabbccddeeff	aabbccddeeffaabbccddeeffaabbccdd	d2acdc78b8ebace37f2df83a37c75062
2	11223344aabbccddeeffaabbccddeeff	000102030405060708090a0b0c0d0e0f	5c5c68c3db976831d7785e924ae986c0
3	AABBCCDDEEFFaabbccdd001122334455	0011223344aabbccddeeAABBCCDDEEFF	8f7ec00c1f99cc3c8ee48fa4d1e8b868
4	00010203040506070809101112131415	00010203040506070809101112131415	e08c969f6ca83fd3c12304f373cd3a83
5	00112233445566778899AABBCCDDEEFF	aabbccddeeff11223344556677889900	5a9a59a38c56e11ed6846660dcac247c

VI. CONCLUSION

In this paper software implementation of Advanced Encryption Standard (AES) algorithm is used for data encryption that can process with the data block of 128 bit and cipher key length of 128 bit. The usage of 128 bit cipher key to achieve the high security, because 128 bit cipher key is difficult to broken. As result of this secure transmission of data is occurred in encryption. While computing the existing AES, the SubBytes transformation consumes the more memory in AES so to overcome this affine transform is used in AES flow.

VII. ACKNOWLEDGMENT

It is a great pleasure to express sincere and humble gratitude to the guide Prof. Mala L M. for valuable guidance and encouragement given during the course of work and also author would like to thank the Principal, HOD and to all teaching and non-teaching staff E&CE department of Sri Dharmasthala Manjunatheshwara College of Engineering and Technology, Dhavalagiri, Dharwad, Karnataka, India for their constant support.

REFERENCES

[1] Advanced Encryption Standard (AES), FIPS PUB 197, Nov. 26, 2001, Federal Information Processing Standards publication 197. Federal Information Processing Standards Publication 197.

[2] K.Rahimunnisa, m. Priya Zach, s. Suresh Kumar, j.jayakumar "Architectural optimization of aes Transformations and key expansion", Sept 2012.

[3] P.Karthigaikumar, Soumiya Rasheed "Simulation of Image Encryption using AES Algorithm", 2011.

[4] Vasamsetti Ramoji, P.Ganesh, Ch.Appala Swamy, "Highly Secured High Throughput Efficient VLSI Architecture for AES Implementations, 2012.

[5] William Stallings. Cryptography and Network Security Principles and Practices, Fourth Edition: Prentice-Hall, Pub Date: November 16, 2005.

[6] Issam Mahdi Hammad, Efficient Hardware Implementations for the Advanced Encryption Standard (AES) Algorithm, Dalhousie University Halifax, Nova Scotia October 2010.

[7] G. H. Karimian, B. Rashidi, and A.farmani "A High Speed and Low Power Image Encryption with 128 Bit AES Algorithm", 2011.

[8] P. Aatheeswaran, Dr.R.Suresh Babu "FPGA can be Implemented by using Advanced Encryption Standard Algorithm "Jan 2013.