ISSN 2348 – 9928
IJAICT Volume 3, Issue 11, November 2016 Doi:01.0401/ijaict.2014.07.12 Published on 05 (11) 2016

REVIEW ON 128 BIT ADVANCED ENCRYPTION STANDARD ALGORITHM WITH FAULT DETECTION

Ms. Ruchi R. Vairagade
Electronics and Communication Engineering
GHRAET, RTMNU
Nagpur, India

Prof. Shubhangini Ugale
Electronics and Communication Engineering
GHRAET, RTMNU
Nagpur, India

Prof. Prachi Pendke
Electronics and Communication Engineering
GHRAET, RTMNU
Nagpur, India

Abstract— Advanced Encryption Standard (AES) is the standard for secret key encryption. The goal of AES is to achieve secure communication. And it is based on design principle known as substitution and permutation network. as this is 128 bit AES algorithm since it will accepts 128 bits of plaintext and master key of size128 bits. The 128 bits cipher text block is produce after the plaintext block is processed by round function number of times. This algorithm uses a combination of Exclusive-OR operation (XOR), Substitution with S-Box, Row and Column rotation and a Mix column. Plaintext, ciphertext and intermediate state block can be depicted as 4*4 matrix form. In this paper, in the proposed work present the details of the 128 bits AES Encryption and Decryption structure and conduct a fault injection attack against the unprotected AES. The methodology to be employed is VHDL

Keywords- AES, VHDL.

I. INTRODUCTION

The Advanced Encryption Standard (AES) is a standard for the encryption of electronic data. The AES-128 Algorithm includes the following functions i.e. 128-bit key size, Automatic Round key calculation and Encryption or decryption functions. In this paper, we design the 128 bit AES algorithm in encryption and decryption process. We conduct a fault attack against the unprotected AES by using VHDL code.

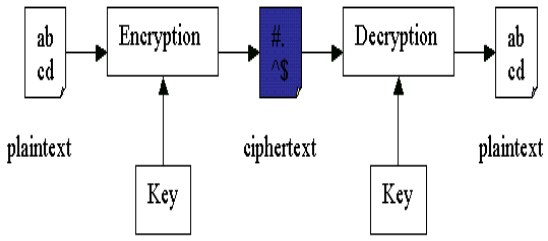


Fig 1: Block Diagram of AES

Plaintext: Plain text is add input Data by using algorithm.

Encryption algorithm: The encryption algorithm performs substitution and permutation values or document or data on input text (Plain text).

Secret Key: The secret key is also input to the encryption algorithm. The exact substitutions and permutations performed depend on the key used, and the algorithm will produce a different output depending on the specific key being used at the time.

Cipher text: This is the scrambled message produced as output. It depends on the plaintext and the key. The cipher text is an apparently random stream of data, as it stands, is unintelligible.

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.

These cryptographic Algorithms are use for protection of the user data so that only the permitted user is allowed to access it and it is a science of information security. Unlike DES, the decryption algorithm differs from the encryption algorithm.

II. THE AES CIPHER

AES is a symmetric block cipher, Like DES. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits i.e diffent AES algorithm. and need not be the same. However, the AES

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.07.12 Published on 05 (11) 2016

standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. As well as these differences AES differs from DES in that it is not a feistel structure.

III. AES ALGORITHM

AES is a symmetric key block with a data block length of 128 bits, which supports different key lengths of 128, 192 or 256 bits. The AES is a round-based encryption algorithm. The number of rounds for key length 128 bits is 10, for key length 192 bits is 12 rounds, and for 256 bits 14 rounds. In the encryption of the AES algorithm, each round performs four transformations namely SubBytes, ShiftRows, MixColumns and AddRoundKey, while the final round does notperform the MixColumns transformation. The key used in each round which is called the round key, this is generated from the initial key by a separate key scheduling module of AES.

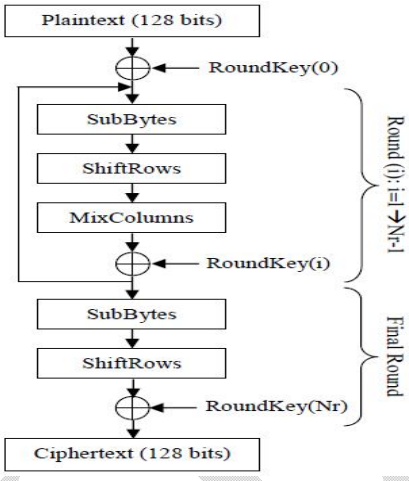


Fig 2a: Encryption Structure

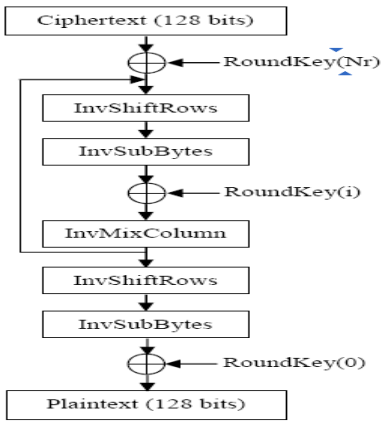
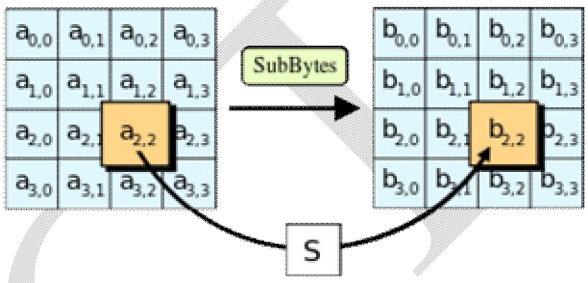


Fig 2b:Decryption Structure

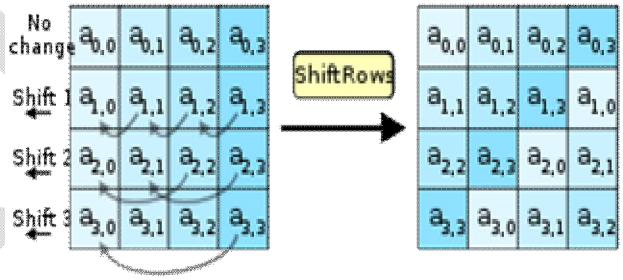
SubBytes transformation: The SubBytes transformation is a non-linear byte substitution, operating on bytes independently. a non-linear substitution step where each byte is replaced with another according to a table. The Sub Bytes is constructed by the composition of the following transformations

Inversion in the GF(28) field, modulo an irreducible polynomial m(x) given by:

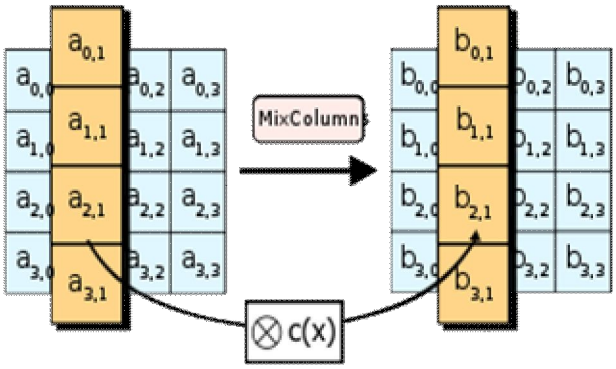
$$a(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$$



ShiftRows transformation: ShiftRows is a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.



Mixcolumn transformation:In MixColumns a mixing operation which operates on the columns of the state, combining the four bytes in each column.



During this operation, each column is multiplied by a fixed matrix which is shown below:

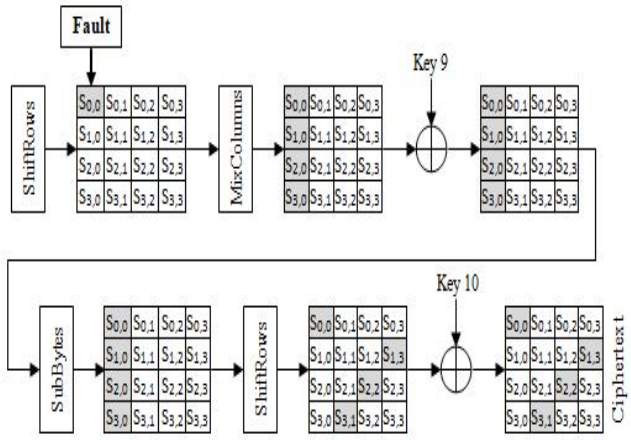
ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.07.12 Published on 05 (11) 2016

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

The matrix operation is perform in following manner, Matrix multiplication is composed of multiplication and addition of the entries, and here the multiplication operation can be defined as this: multiplication by 1 means no change, multiplication by 2 means shifting to the left, and multiplication by 3 means shifting to the left and then performing XOR with the initial unshifted value.

IV. FAULT ANALYSIS

As the second part of this project to determine the result of unprotected AES since to demonstrate the necessity to protect the AES algorithm against the fault Analysis, conduct a attact against the unprotected AES.



V. LITERATURE REVIEW

An exhaustive literature review has been carried out related to the work to find out the current research. Abstracts of some of most relevant research works are reported in the following paragraph

Hassen Mestiri,Noura Benhadjyoussef, Mohsen Machhout and Rached Tourki, "An FPGA Implementation of AES with Fault Detection," IEEE Electronics and micro-Electronics Laboratory(E.U.E.L) CODIC 2013.

In this paper,to improve the security of the AES algorithm, we implemented the AES algorithm in encryption and decryption process. We conduct a fault attack against the unprotected AES.and simulation result is shown on Matlab software.

F. Regazzoni, Y. Wang and, F.X. Standaert, "FPGA Implementations of the AES Masked Against Power Analysis Attacks," Second international workshop on constructive side channel Analysis and Secure Design(COSADE 2011).

In this paper, they introduce a compiler that automatically inserts software countermeasures protect cryptographic algorithms against power based side channel attacks i.e work on power factor.

L. Lan, "The AES encryption and decryption realization based on FPGA", Seventh International Conference on Computational Intelligence and Security (CIS 2011).

In this paper, a method of AES encryption and decryption algorithm implemented on the FPGA is presented,a-128 bit key size mode is implemented. with the development of networking technology.

T. Rahman, S. Pan, and Q. Zhang, "Design of a high throughput 128-bit AES (Rijndael Block Cipher)", Proceedings of the International Multi conference of Engineers And Computer Scientists(IMECS), Vol II,2011.

In this paper, work on speed.presents an efficient FPGA implementation approach of the Advanced Encryption Standard (AES) Algorithm. The architectural optimization method has been incorporated which includes pipelining architecture techniques. speed is increased by processing multiple rounds simultaneously but at the cost of increased area. A 119.954 MHZ clock frequency is achieved which translates to a throughtput of 1.18 Gbps using 6279 slices.

VI. ARCHITECTURE OPTIONS

There are two approaches for the SubBytes/InvSubBytes transformation operation namely:

The first approach usesfor this operation is Look-Up Table (LUT) to get the SubBytes/InvSubBytes value for each input, there are 256 different SubBytes or InvSubBytes operation values in total, and all the values can be stored in a ROM as a table.

The second approach to be used for this operation is calculate the SubBytes or InvSubBytes value by mathematical equations, all the operations are in finite Galois field. But This approach costs a lot of hardware resources and requires a long time execution to transform since cost and time is more. Since look up table is used.

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.07.12 Published on 05 (11) 2016

VII. CONCLUSION

To improve the security of the AES, Design the AES algorithm in encryption and decryption process.and conduct a fault attack against the unprotected AES i.e.comparision of protectected AES against unprotected AES. by using Xilinx and proposed a fault detection scheme for the Advanced Encryption Standard.Its area, frequency and throughput for the AES encryption have been obtained and compared.

References

[1] Hassen Mestiri, Noura Benhadjyoussef,Mohsen Machhout and Rached Tourki, "An FPGA Implementation of AES with Fault Detection",IEEE Electronics and micro-Electronics Laboratory(E.U.E.L) CODIC 2013.

[2] Hoang Trang , Nguyen Van Loi , "An efficient FPGA implementation of the Advanced Encryption Standard algorithm", IC Design Research & Education Center (ICDREC) VietNam National University HoChiMinh City ©2012 IEEE.

[3] Rourab Paul, Sangeet Saha, Suman Sau, Amlan Chakrabarti "design and implementation of real time AES-128 on real time operating system for multiple FPGA communication".

[4] L. Lan, "The AES encryption and decryption realization based on FPGA", Seventh International Conference on Computational Intelligence and Security (CIS 2011).

[5] Tin Lai Win,and Nant Christina Kyaw "Speech Encryption and Decryption",world Academy of Science, Engineering and Technology 48 2008.

[6] Monica Liberatori, FernandoOtero,J.C. Bonadero, Jorge Castifieira, "AES-128 cipher. high speed, low cost FPGA implementation", ©2007 IEEE.

[7] K. Wu, Ramesh Karri, G. Kuznetsov, M. Goessel, "Low cost concurrent error detection for the advanced encryption standard,"ITC International Test Conference, 2004.

[8] P.Dusart G. Letourneux, and O. Vivolo, "Differential Fault Analysis on A.E.S," ACNS 2003, Lecture Notes in Computer Science Vol. 2846, pp. 293–306, 2003.