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

Design Enhance AES Data Encryption and Decryption

Shraddha Wade, Ashmika Gadikar, Aafreen Khan, Vikram Deshmukh

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

ABSTRACT

Advance Encryption Standard (AES), it is used to specify a Federal Information Processing Standard (FIPS) approved cryptographic algorithm that can be used to protect our electronic data. This paper present the AES algorithm with regard to Field Program Gate Array (FPGS), offers a very fast method and most customizable solution. The approach in order to minimize the hardware consumption for the transformation of Encryption and Decryption are simulated using an iterative design. Implementation of code carried out in Xilinx ISE 9.2i. In this paper, we present the implementation of the AES 128-bit encryption and decryption. AES Encryption is a method for scrambling data. A key is used to mix up data such that it can be securely stored or transfer over a network. The design is based on substitution and permutation network. In this system we have message, a plain text and a secret key. The 128 bits cipher text block is produce after the round function is processed plaintext block.

Keywords : AES, FPGA, VHDL, Encryption, Decryption.

I. INTRODUCTION

The Advanced Encryption Standard was launched in 2001 by the National Institute of Standards and Technology (NIST).It is now the most widely used symmetric key encryption algorithm in the world. AES algorithm have been proposed for different applications and their performance have been evaluated by using ASIC libraries and FPGA.[1]

Cryptographic algorithm AES is currently used in a very large variety of scenarios. The common examples: e-commerce and financial transactions, which have strong security requirements. The Advance Encryption Standard (AES) is a standard for the encryption of electronics data. The AES 192-bits algorithm includes the following function i.e. 192-bit key size, Automatic Round key calculation and Encryption or decryption functions. In this paper, we design the 192 bit AES algorithm in encryption and decryption process. We conduct a fault attack against the unprotected AES by using VHDL code. 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.[2,3]

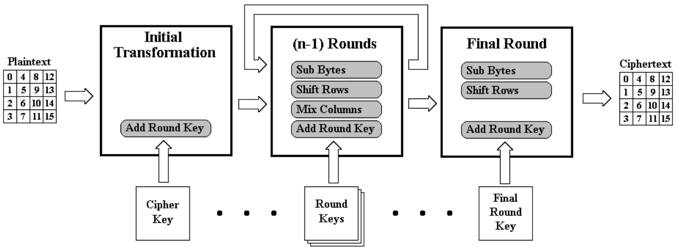
In this paper, Encryption and Decryption process of AES algorithm is implemented. A fault attack is conducted and fault detection scheme is applied. Maximum fault coverage is achieved through this detection scheme and then different parameters like Area; Hardware requirement is to be compared. Power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

II. METHODS AND MATERIAL

1. AES Algorithm

To encrypt a message, we supply the message along with the key. The AES Encryption algorithm scrambling the message and the output unrecognisable data. A key is used to mix up data that it can be securely stored or transferred over network, and only with the key can unscramble the data. It is symmetrical key algorithm. This means that the same key is used to scramble the data and unscramble it.

The 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.



2. Block Cipher

AES is a block cipher which encrypts 128 bits of data at a time. It treat a 16-bytes as a grid of 4*4. Messages which are longer than 128 bit are broken into block of 128 bits. Each block is encrypted separately using exactly the same steps.

3. Key Lengths

When using AES we can select a key length.The keys can be 128-bits, 192 bits or 256 bits. The size of the key dictates how many round or cycle of scrambling we have to perform. With large keys corresponding to more round, And, in theory, more secure but slower encryption.

4. 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 nonlinear) 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.

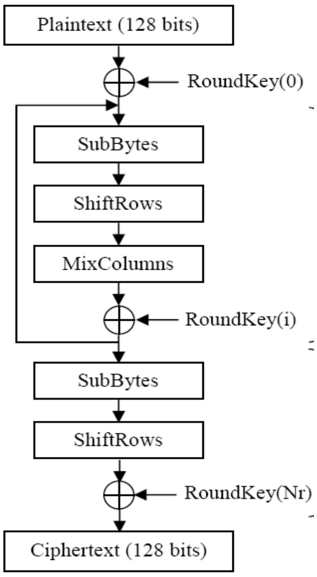
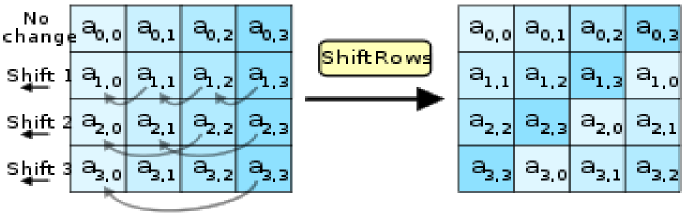


Figure 1. AES Encryption Structure

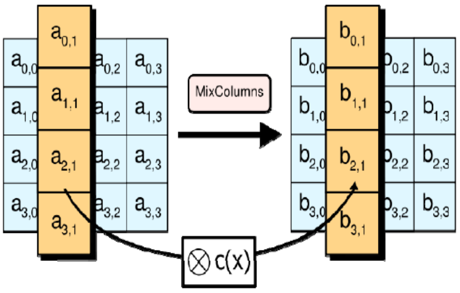
A. ShiftRows Tranformation

It is linear transformation. This provides resistance against truncated differential and saturation attacks. The Shift Rows 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 $(x^4 +1)$.

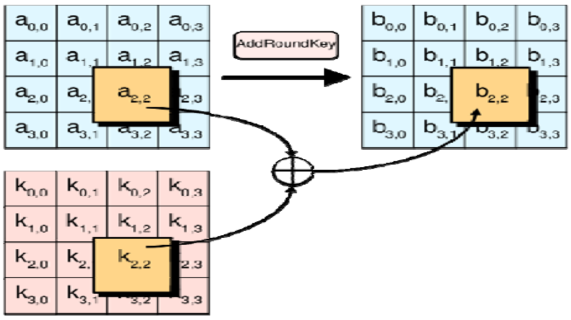


Fixed polynomial c(x) is given by
$c(x)= \{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$
In matrix form, the MixColumns transformation can be expressed as:

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

C. AddRound Key

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.



D. 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.

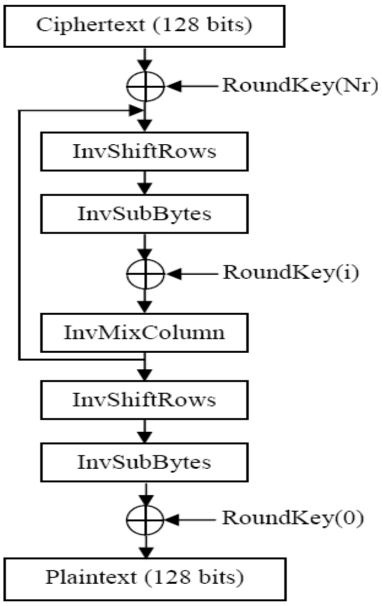


Figure 2. AES decryption Structure

III. CONCLUSION

In order to improve the security of the AES, AES algorithm in encryption and decryption is implemented. In this paper, we propose the Encryption and Decryption of Plain text. Initial Transformation, Rounds and Final rounds are the transformation which is being used in this project.

AES Design	Area(Slice)	Delay	Power	Frequency	Throughput
Conventional Encryption	250	3.356ns	3.806W	297.97 MHz	3814.06 Mbps
Conventional Decryption	3712	3.808ns	3.577W	382.77 MHz	4899.328 Mbps

IV. REFERENCES

[1]. National Inst. of standard and technology,"Federal Information Processing Standard publication 197, the Advance Encryption Standard (AES)," Nov.2001

[2]. William Stalling, Cryptography and Network Security, Principle and Practices, 4th ed. Pearson Education pp.134-161, 2006

[3]. J.Daemen and V.Rijmen , "AES Proposal: Rijndael," Aes Algorithm Submission, Sept. 1999.