ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 6, Issue 10, October 2017

VDAAESA: VLSI Based Design and Analysis of Advanced Encryption Standard Algorithm

M. Shoukath Ali[1], P.V. Sai Ramji[2], M. Harsha[3], N. Yugendher Reddy[4]

Associate Professor, Dept. of ECE, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana State, India[1]

IV B.Tech Student, Dept. of ECE, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana State, India[234]

ABSTRACT: In the contemporary world most of the communication is done using electronic media. Hence, there is a need to protect data from malicious attacks. Data Security plays a vital role in such communication. Advanced Encryption Standard (AES), also known as Rijndael, is an encryption standard algorithm used for securing information. AES was published by NIST (National Institute of Standards and Technology). AES is a block cipher algorithm that has been analysed extensively and is now used widely. AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. The main purpose of this paper is to make everyone aware of the functionality of advanced encryption standard algorithm.

KEYWORDS: Advanced Encryption Standard, Cipher Text, Encryption, Decryption, Rijndael algorithm.

I. INTRODUCTION

AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts plain text into an unintelligible form called cipher-text and decrypting the cipher-text converts the data back into its original form, called plaintext.
The Advanced Encryption Standard, after the Data Encryption Standard was found too weak because of its small key size and the technological advancements in processor power. Fifteen candidates were accepted and based on public comments the pool was reduced to five. One of these five algorithms was selected as the standard algorithm.

The Rijndael, whose name is based on the names of two Belgian inventors, Joan Daemen and Vincent Rijmen. It is a Block cipher that works on fixed length of bits, which are called blocks. It takes an input block of a certain size, usually 128 bits, and produces a corresponding output block of the same size. The transformation requires a second input, which is the secret key whose length can be of 128, 192 and 256 bits. Unlike DES, which is based on Feistel network, AES is a substitution-permutation network, which is a series of mathematical operations that use substitutions (also called S-Box) and permutations (P-Boxes) .When a block cipher algorithm is used for encryption and decryption purposes, the message is divided into blocks of bits. These blocks are then put through substitution, transposition, and other mathematical functions. The algorithm dictates all the possible functions available to be used on the message, and it is the key that will determine what order these functions will take place. Cipher text contains confusion and diffusion. Different unknown key values cause confusion and diffusion is accomplished by putting the bits within the plaintext through many different functions so that they are dispersed throughout the algorithm. Block ciphers use diffusion and confusion in their methods.

The main objectives of AES are high level security, adoptable to diverse application, efficient and exportable. 128 bits is given as input to encryption block in which encryption of data is made and the cipher text of 128 bits is throughout as output. The key length of 128 bits is used in process of encryption. The AES algorithm is a block cipher that uses the same binary key both to encrypt and decrypt the data. Therefore it is called as a symmetric key cipher.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 6, Issue 10, October 2017

II. PROPOSED METHODOLOGY

The AES is an iterated block cipher with a fixed block size of 128 and a variable key length. The different transformations operate on the intermediate results, called state. The state is a rectangular array of bytes and since the block size is 128 bits, which is 16 bytes, the rectangular array is of dimensions 4x4. The basic unit for processing in the AES algorithm is a byte**,** a sequence of eight bits is treated as a single byte. The input, output and Cipher Key bit sequences which are processed as arrays of bytes that are formed by dividing these sequences into groups of eight contiguous bits to form arrays of bytes.
In the Rijndael version with variable block size, the row size is fixed to four and the number of columns varies. The number of columns is the block size divided by 32 and denoted Nb. The cipher key is a rectangular array with four rows. The number of columns of the cipher key, denoted as Nk, is equal to the key length divided by 32.

Encryption:
AES algorithm uses a round function that is composed of four different byte-oriented transformations:

1. Byte substitution using a substitution table (S-box)
2. Shifting rows of the State array by different offsets
3. Mixing the data within each column of the State array
4. Adding a Round Key to the State

Above mentioned functions are carried out for every individual round and in the last round the third function, that is, Mixing the data within each column of the State array will not be performed. Hence the last round is carried out separately. Based on the key provided, the new set of keys will be generated in the Key Expansion block and is given to the each round as input.

Decryption:
The cipher text of 128 bits and the same key of 128 bits will be given as the input to the decryption block. The encrypted data will be decrypted and the original plain message will be achieved as the output of the decryption block. The Cipher transformations can be inverted and then implemented in reverse order to produce a straightforward Inverse Cipher for the AES algorithm.
The transformations used in the Inverse Cipher are as follows.

1. Inverse Shift Rows
2. Inverse Sub Bytes
3. Inverse Mix Columns
4. Add Round Key

Here also 10 rounds will be carried out and the only difference in the decryption block with respect to the algorithm flow is that the result of the Key Expansion of each round will also be given to the Mix Columns operation after which the Add Round Key transformation should be carried out.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 6, Issue 10, October 2017

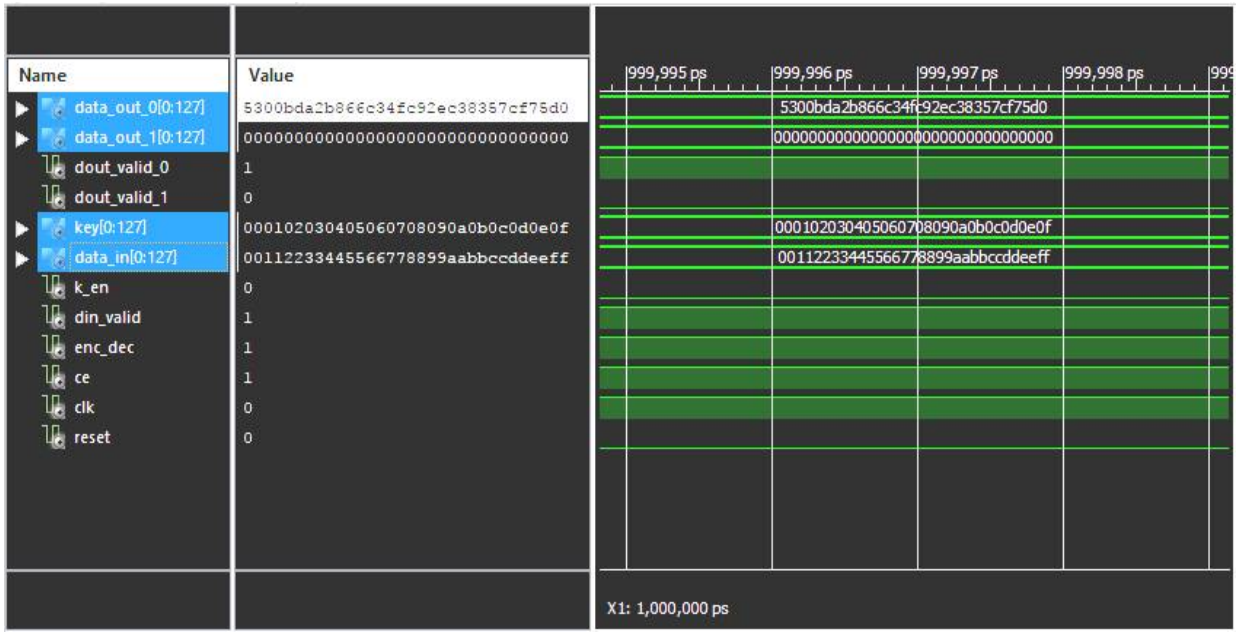
III. EXPERIMENTAL RESULTS

Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Flip Flops	1,626	93,184	1%
Number of 4 input LUTs	161,979	93,184	173%
Logic Distribution			
Number of occupied Slices	81,991	46,592	175%
Number of Slices containing only related logic	66,234	81,991	80%
Number of Slices containing unrelated logic	15,757	81,991	19%
Total Number 4 input LUTs	162,232	93,184	174%
Number used as logic	161,979		
Number used as a route-thru	253		
Number of bonded IOBs	391	1,108	35%
IOB Flip Flops	381		
Number of GCLKs	1	16	6%
Total equivalent gate count for design	1,055,595		
Additional JTAG gate count for IOBs	18,768		

Figure 1: Device utilization summary

The device utilization summary is shown in figure-1. It gives the details of number of devices used from the available devices and percentage of utilization.

Encryption:



Data before encryption:
Input: 00112233445566778899aabbccddeeff
key: 000102030405060708090a0b0c0d0e0f
Data after encryption:
Output:0[0:127] 5300bda2b866c34fc92ec38357cf75d0

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

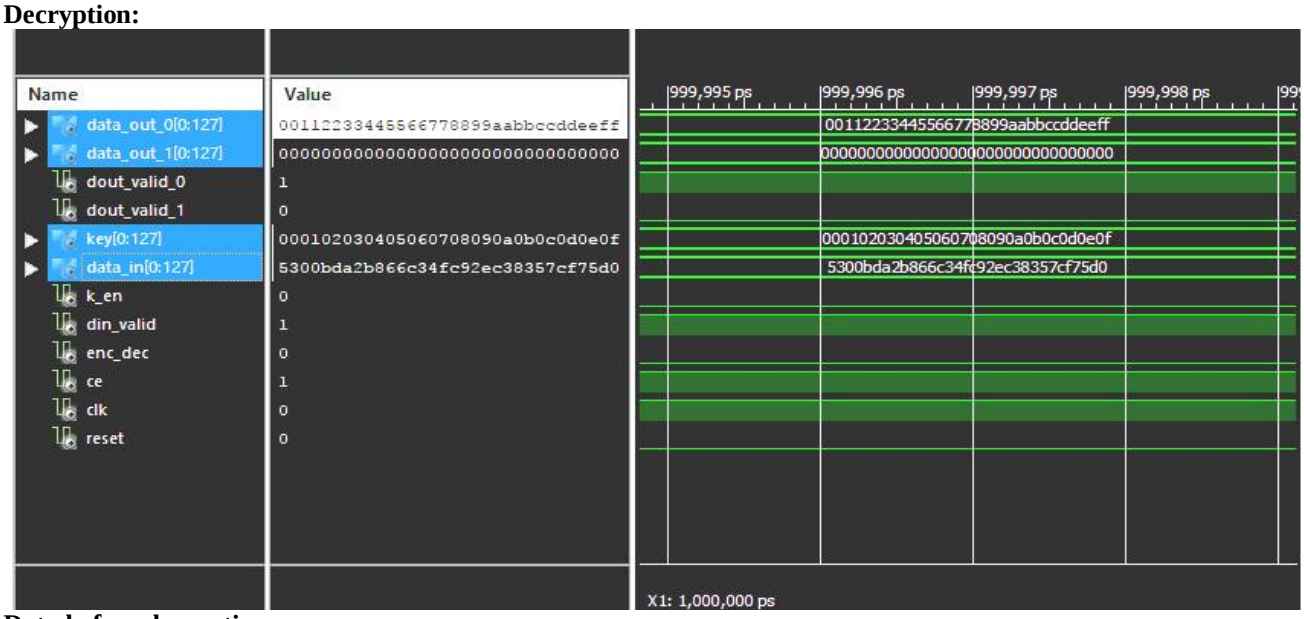
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 6, Issue 10, October 2017

1[0:127]00000000000000000000000000000000

Decryption:



Data before decryption:
Input: 5300bda2b866c34fc92ec38357cf75d0
Key: 000102030405060708090a0b0c0d0e0f
Data after encryption:
Output:0[0:127] 00112233445566778899aabbccddeeff
1[0:127]00000000000000000000000000000000

.

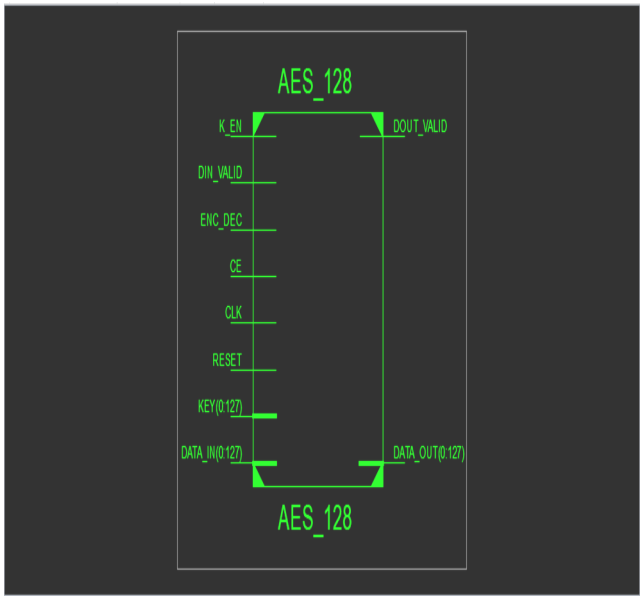


Figure 4: RTL schematic of AES-128

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 6, Issue 10, October 2017

IV. CONCLUSION

The Rijndael algorithm is chosen as the new Advanced Encryption Standard (AES) for several reasons. The algorithm is resistant to known attacks and is quick to code. The inverse of the addition operation is itself, making much of the algorithm easy to do. In fact, every operation is invertible by design. In addition, the block size and key size can vary making the algorithm versatile. AES was originally designed for non-classified U.S. government information. Later on AES-256 was being used for top secret government information. As of recent findings, no practical attacks have been successful on AES.

REFERENCES

[1] J. Daemen and V. Rijmen, "AES Proposal: Rijndael. NIST AES Proposal," June 1998. Available at http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf.
[2] National Institute of Standards and Technology (U.S.), "Advanced Encryption Standard (AES)," Available at http://csrc.nist.gov/publications/drafts/dfipsAES.pdf.
[3] J. Daemen, V. Rijmen, " AES proposal: The Rijndael Block Cipher, " Version 2 (Sept. 1999) pp. 1–45.
[4] Leelavathi.G, Prakasha S, Shaila K, Venugopal K R, L. M. Patnaik "Design and Implementation of Advanced Encryption Algorithm with FPGA and ASIC", International Journal of Research in Engineering & Advanced Technology (IJREAT), Volume 1, Issue 3, June-July, 2013
[5] Ali, M. Shoukath & Singh, R.P.. (2017). QoS-aware protocol using priority packet scheduling scheme for wireless sensor networks. International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST). 3. 57-65. 10.20238/IJARBEST.2017.0304008.
[6] Mr. Atul M. Borkar, Dr. R. V. Kshirsagar and Mrs. M. V. Vyawahare, "FPGA Implementation of AES Algorithm", International Conference on Electronics Computer Technology (ICECT), pp. 401-405, 2011.
[7] Ai-Wen Luo, Qing-Ming Yi, Min Shi, "Design and Implementation of Area-optimized AES-Based on FPGA" in , IEEE.
[8] jalal ahmad, Syed & Ali, M. Shoukath & Noor Mohammad, Shaik. (2017). Multimedia Transmission Over Mobile Adhoc Networks (QoS).
[9] Samiee, H., Atani, R.E. and Amindavar, H. (2011) A Novel Area Throughput Optimized Architecture for AES Algorithm. International Conference on Electronic Devices, Systems and Applications (ICEDSA), Kuala Lumpur, 25-27 April 2011, 29-32. http://dx.doi.org/10.1109/ICEDSA.2011.5959055
[10] Liberatori, M., Bonadero, J.C.:"Minimum Area, low cost FPGA implementation of AES. VIII International Symposium on Communications Theory and Applications, UK, Julio 2005.pp 461-466.
[11] Ali, M. Shoukath. (2016). Priority Based Packet Scheduling Scheme in Wireless Sensor Networks.International Journal of Advanced Research Foundation. 3. 32-35.

BIOGRAPHY

M. Shoukath Ali is working as Associate Professor in the Department of Electronics & Communication Engineering at Guru Nanak Institutions Technical Campus (GNITC), Hyderabad, Telangana State, India. His areas of interest are Wireless sensor networks, VLSI Design and Communication system design. His Publications includes 7 research articles in International Journals / conferences and a book on Mobile adhoc networks.

P V Sai Ramji , Pursuing IV Year B.Tech in the specialization of Electronics and Communication Engineering from Guru Nanak Institutions Technical Campus (GNITC), Hyderabad. His area of interest is Chip Designing in VLSI.

M Harsha, Pursuing IV Year B.Tech in the specialization of Electronics and Communication Engineering from Guru Nanak Institutions Technical Campus (GNITC), Hyderabad. His area of interest is Chip designing in VLSI.

N Yugendher Reddy , Pursuing IV Year B.Tech in the specialization of Electronics and Communication Engineering from Guru Nanak Institutions Technical Campus (GNITC), Hyderabad. His area of interest is Chip Designing in VLSI.