International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 2, Issue 4, pp: (96-104), Month: October - December 2014, Available at: www.researchpublish.com

Design of AES Algorithm in Optimized Manner on FPGA

Hrushikesh S. Deshpande[1], Kailash J. Karande[2]

[1]ME Student, [2]Principal, Electronics and Telecommunication Engineering Department,

SKN Sinhgad College of Engineering, Pandharpur, Maharashtra, India

Abstract: **This paper describes a system of AES algorithm in optimized manner. The Advanced Encryption Standard can be programmed in software or built with pure hardware. However Field Programmable Gate Arrays (FPGAs) offer a quicker, more optimized solution. This design includes the AES algorithm with regard to Area optimized software model by using the Very High Speed Integrated Circuit Hardware Description language (VHDL). Xilinx ISE project Navigator 14.1 software is used for simulation and optimization of the synthesizable VHDL code. The National Institute of Standards and Technology (NIST) has initiated a process to develop a Federal information Processing Standard (FIPS) for the Advanced Encryption Standard (AES), specifying an Advanced Encryption Algorithm to replace the Data Encryption standard (DES) the Expired in 1998. All the transformations of both Encryptions and Decryption are simulated using an iterative design approach in order to minimize the hardware consumption. The project is designed by reducing the number of slices in Software AES model, the area optimized AES-128 Bit structure produced by this project which gives most optimized structure as compared with previous results.**

Keywords: **ASIC Application Specific Integrated Circuits, AES Advanced Encryption Standard, ASIP Application Specific Instruction Processor, CLB Configurable Logic Blocks, CBC Cipher Block Chaining.**

1. INTRODUCTION

In today's digital world, data security is most of the common issue in network security domain. The National Institute of Standards and Technology (NIST) proposes a publication of encryption standards by considering Federal Information Processing Standards (FIPS) publications. The presented paper describes AES (Advanced Encryption Standard)-128 algorithms in optimized manner. This paper produces a design of AES-128 system which produces area optimized design by reducing number of slices per area in CLB (Configurable Logic Blocks).This paper produces a design which uses Block RAM (BRAM) as stored memory for S-BOX (Substitution Box).

This reduces the array storing capacity of CLBs.The AES algorithm is a symmetric cipher. In symmetric ciphers, a single secret key is used for both the encryption and decryption, whereas in asymmetric ciphers,.The comparative analysis of these methods is done and overview is given below The NIST standard produces a publiction for cryptographic algorithm.This pubication is based on FIPS security publication details. AES is one of the recent security algorithms which is predecessor of DES algorithm. AES produces 128 bit Encryption while transfering data in online or offline communications [1]. This paper proposes the AES-128 bit SPN Design .The AES design proposed by this paper is based on symmetric 128 bit key variations. This paper describes the area optimized design of AES algorithm in VHDL language with the help of XC3S1400AN device of Spartan Family [5].

2. ASPECTS OF DATA SECURITY

The Network security is critical issues in today's global era of wireless and wired communication topologies. In most of the cases data security is more important than data handling schemes .AES algorithm is most recent SPN algorithm based on

more than 10 round processes of encryption and same for decryption process. The computation power and network attacks both can be minimized completely with the help of this algorithm as it produces 128 Key design which minimizes the security attacks occurred due to DES algorithm .

The cipher text produced during AES algorithm implementation is a type of block cipher mainly it can be either of ECB (Electronic Code Book), CBC (Cipher Block Chain) mode. The cipher key used by Data Security algorithm mainly of Public key or Private Key. AES algorithm uses mainly private key of 128 bit. There are many algorithm were proposes their structure of security like Blowfish, Mars, IDEA, DES and 3DES .Most of these algorithm are based on Fresnel structure in which left part and right part both are shifted together. While in case of AES directly SPN (Substitution and Permutation network) is used in which all values are substituted finally using algorithm constant parameters.

AES algorithm mainly uses 128 bit encryption which is commonly used in most security aspects as, In windows 8 bit locker for bit locking of hard disk drives, ATM transaction ,online banking transaction .windows firewall protection and data transfer ,windows defender, windows fault analysis .

This paper is supposed to propose a basic optimized design of AES algorithm. The optimization done in terms of through put per slices. All the designed results are synthesized and simulated using Xilinx ISE Project Navigator 14.1.and using FPGA device as XC3S1400AN of Spartan family.

This paper is organized as follows. Section 2 Aspects of Data Security, Section 3 basic approach Cryptology that we have found in the literature and references. In Section 4 we describe the AES algorithm methodology. In this section5, we have explained our process and data flow exactly we have implemented the algorithm. Then Section 6 presents Experimental simulation results and section 6, 7 describe conclusion and future scope, it analyzes the final results with the help of that we state our conclusions in the this section

3. CRYPTOLOGY

The cryptology is the combination of cryptography and cryptanalysis. In early days cryptography used to operates on manual schemes. Due to cryptographically techniques a fast and secure data transmission takes place over a communication channel. The Cryptography uses cryptographical algorithms for maintenance of security. The cryptanalysis uses trial and error method for detection of cryptographical attacks. In cryptography it is the process of systematic and well structured use of security algorithm with the help of cryptanalysis process. In which non-readable format back to readable format using decoding and vice versa using encoding techniques.

4. AES METHODOLOGY

AES algorithm basically works on byte as a fundamental element. It uses sequential mathematically operations as linked iterations in 10 rounds. In 1997 NIST issued a request for replacing DES .In September 1997 ,The 15 candidate's algorithm were selected in which only 5 was goes into final round. They produced 5 algorithms for security MARS, RC6, Rijndael, Serpent and Two fish. The Rijndael was the finalist selected by FIPS 197. Thus the AES algorithm development process was started in October 2000.

AES algorithm basically a block cipher operation of 128 bit block. The input to the system is 128 bit plain text and 128 bit cipher key which is symmetric in nature. After performing the encryption operation the output of encryptor is cipher text which is given as input to Decryptor. After AES decryption the original input plain text will be required back. This paper describes symmetric AES structure that's why the cipher key for both encryption and decryption is same.

AES algorithm is previously implemented using Turbo C or C compiler, Matlab. These languages are software languages and are implemented easily in different protocol layer. The purpose of this paper is to implement this design using Hardware description language so that to get hardware layouts and system gate count directly from VHDL coding. The RTL schematic and technical schematic both gives idea of system clocks, memory utilization and RAM details. As FPGA is a reconfigurable device that's why further modification in design flow or design software does not affect on system hardware components. VHDL is a Very High Speed Integrated Circuit HDL which is used for optimized and compact coding of AES Top module called as Mini-AES in this paper. VHDL language coding and synthesis done by using Xilinx device as Xilinx ISE (Integrated Software Environment) Project Navigator 8.1 and 14.1. The simulation is done in Isim

Simulink. The FPGA design can be suited for C and Matlab design using Impulse C compiler and Sysgen tool. The AES algorithm, basic round structure is as follows in Fig 1,

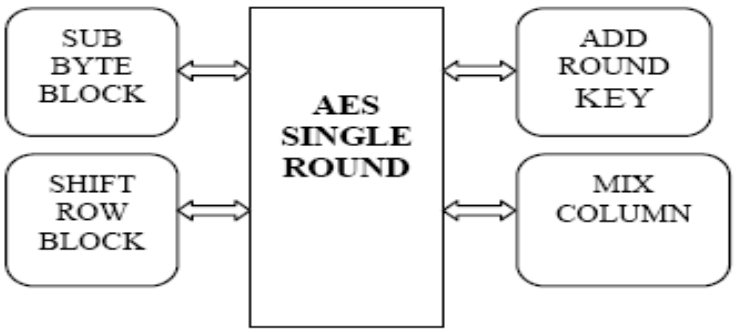

Fig.1. AES Round Structure

As shown in above figure 1, The each round in AES algorithm follows basic 4 sub modules as they are 1.Shift Rows,2.Shift Columns, 3. Add Round Key, 4.Mix columns. According to block cipher structure these rounds and number of block structure ,the number of row count Nr can be implemented as shown in figure 2 below,

AES Structure	Key length (words)	Block Size (words)	Number of Rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Fig.2. AES Block Structure

As shown in this figure the AES algorithm structure is dependence on block size as AES-128 structure forms key length of 4 words means 16 byte structure. Thus it will follows 128 bit forming 4x4 matrix structure each having 1 byte memory allocation. The AES state consists of four rows of bytes and each state has fixed no of rows in which Nb bytes are presents. These Nb is the block length divided by 32(as per no of rounds).As AES is derived from Rijndael it is also called as Rijndael in cryptography to protect sensitive data by converting it into unintelligible form called as a cipher text means coded text. The AES algorithm uses cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

5. DATA FLOW OF AES ALGORITHM

The AES-128 bit algorithm consist of 128 bit block cipher as basic block .Intially 128 bit plain text and 128 bit key is taken as input to the system. Key expansion is the first basic block of AES algorithm which forms expansion of keys in words and producing different key combinations for different rounds.Initially there are 128 bit key means 16 byte key which is converting into 4x4 matrix of 16 byte forming each column element as 1 word of 32 bit of 4 byte. Thus W[0] is formed by first 4 column elements in matrix. Simillary 4x4 matrix forms W[0],W[1],W[2],W[3] keywords now forming such 4 keywords for next rounds is the main task of key expansion unit.For 128 bit there are total 10 rounds are required.thus number of words require for 10 rounds are W[4] to W[43].

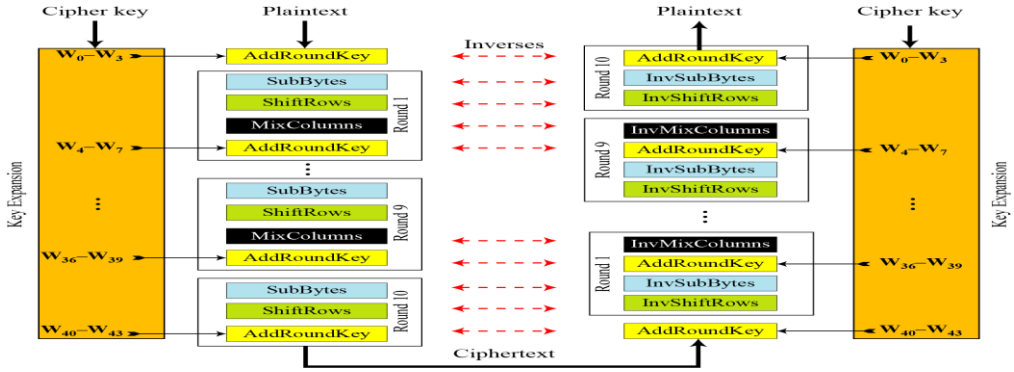

Fig.3. AES Round Structure

The AES basic structure of all round process is as shown in above figure 3.The key expansion block shown in above figure forms key word w[0] to w[43]. The first 4 key word directly formed with the help of 4 x 4 matrices which are called as State. The state is the fundamental unit of AES algorithm. The key Expansion unit is as follows,

```
Key Expansion (byte Cipher Key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
word temp
i = 0
while (i < Nk)
w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
i = i+1
end while
i = Nk
while (i < Nb * (Nr+1)]
temp = w[i-1]
if (i mod Nk = 0)
temp = Sub Word(Rot Word(temp)) xor  Rcon[i/Nk]
else if (Nk > 6 and i mod Nk = 4)
temp = Sub Word(temp)
end if
w[i] = w[i-Nk] xor temp
i = i + 1
end while
end
```

As shown in above pseudo code

1. If w [i] is multiple of 4 i.e. for w [4],w[8],….w [40] then it will follows Substitute, Rotate and Xoring with constant.
2. If w [i] is not multiple of 4 then simple Xoring takes place as w [i]= w [i-1] xor w [i-4].

The AES encryption process is basically depends on 4 modules as mentioned in figure 1. These 4 modules forms cipher text in each round and producing respective round cipher text. The AES encryption flowchart is as shown in following figure,

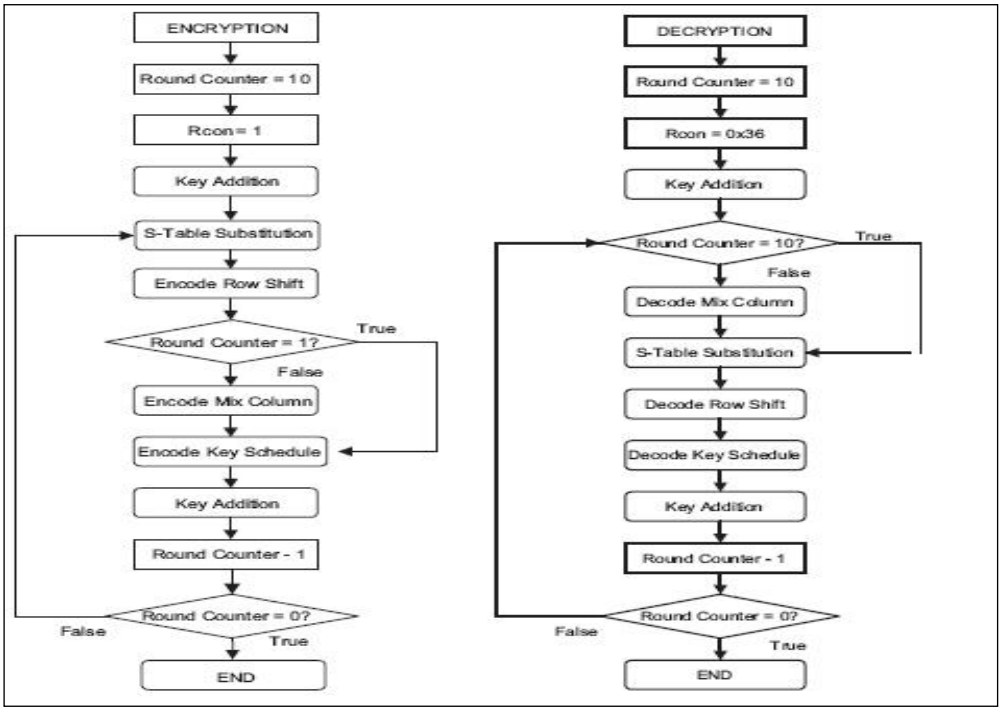

Fig.4.1. AES Round Structure

As shown in above figure 4, AES encryption and decryption basically depends on 4 modules and AES decryption is same as that of AES encryption but it is in reverse order. The four basic modules of AES process is as follows,

SUB-BYTES: It is the SPN process of AES algorithm in which each byte in state replaced by successive byte present in S-BOX. It is the 255 memory location stored in BRAM in our design of AES Top module due to this number of slices reduction takes place. For example, if AF is the element present in state, then it will replaced by Ath column and Fth row in S-Box.

SHIFT-ROW: It is Shift row operations performed cyclically towards Left side each row is shifted towards left side cyclically .For example row at 0^{th} position shifted by 0 bits and 1th by 1 position likewise all the rows in state are shifted after SUB-BYTES.

MIX-COLUMNS: It is the simplest process of multiplication of state with the state formed by using SHIFT-ROW operations. Most of the cases simple matrix multiplication or Galois Field Method is used for such operation and transformations.

ADD-ROUND KEY: It is the transformation in which the Cipher text achieved from above step is xor with this round word key of 4 words i.e.4x4 matrix of key and it will send as input to next round after encryption ,at last round this is used as cipher text giving input to next round.

6. EXPERIMENTAL RESULTS

The AES simulation output is as follows by using Xilinx14.1 ISE software.

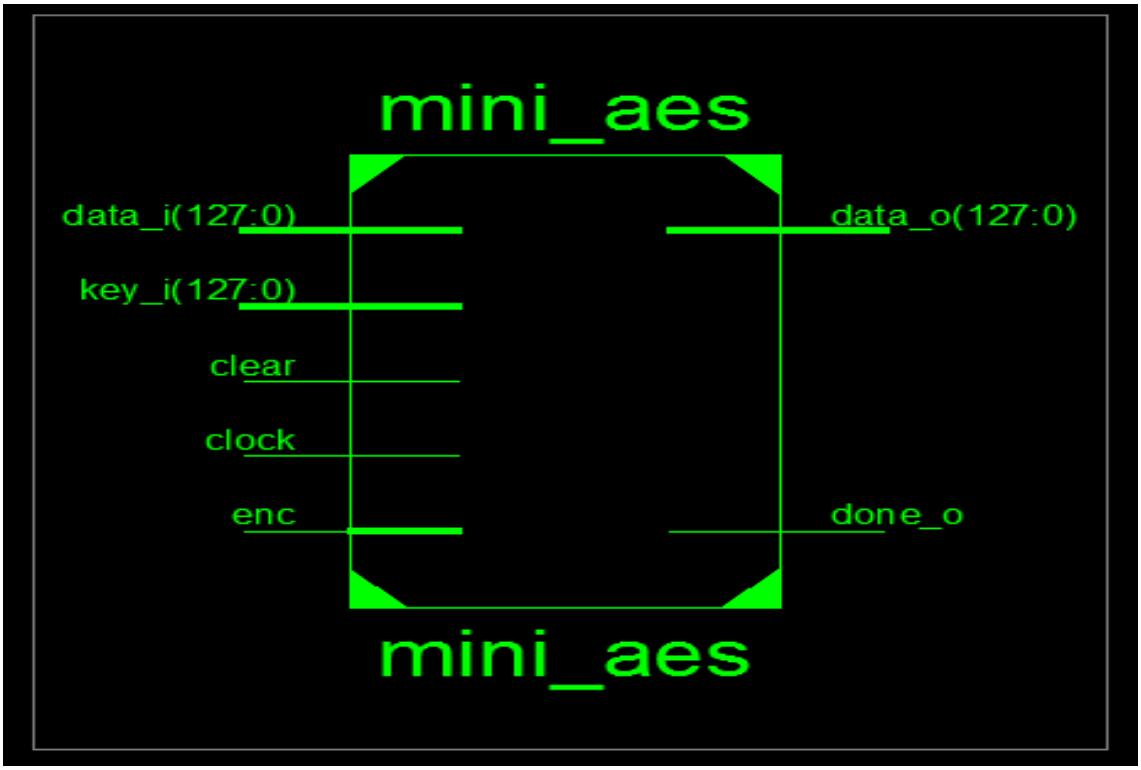

Fig.4.2. AES RTL structure using Xilinx ISE Project Navigator

This simulation result shows in fig 4 that RTL schematic black box design of overall project in which Data in , key acts as basic input for process along with that Clear ,enc ,Clock Enable, Data Input status, Encryption /decryption mode selection respectively acts as system control inputs. DATA_OUT is output either cipher text or plain text depend on status of ENC_DEC mode. All the results are based on simulations from the XILINX ISE 14.1 and ISIM tools using Timing Analyzer and Waveform Generator.

All the individual transformation of both encryption and decryption are simulated using FPGA SPARTAN family and XC3S14001N device. The characteristics of the devices are given as follows in table 1,

Table. 1. SPARTAN Family Features

Device	System Gates	CLBs	Slices	Distributed RAM Bits	Block RAM Bits
XC3S50AN	50K	176	704	11K	54K
XC3S200AN	200K	448	1,792	28K	288K
XC3S400AN	400K	896	3,584	56K	360K
XC3S700AN	700K	1,472	5,888	92K	360K
XC3S1400AN	1400K	2,816	11,264	176K	576K

Sub Bytes Transformation

The following Figure 5 shows the waveforms generated by the 8-bit byte substitution transformation. The inputs are clock of 100ns time period, Active Low reset, and 8-bit state as a standard logic vector, whose output is 8-bit S-box lookup substitution. This overall design utilizes 14 % of the area of XC3S1400AN, around 3376 logic elements are consumed to to implement the complete 128-bit overall process.

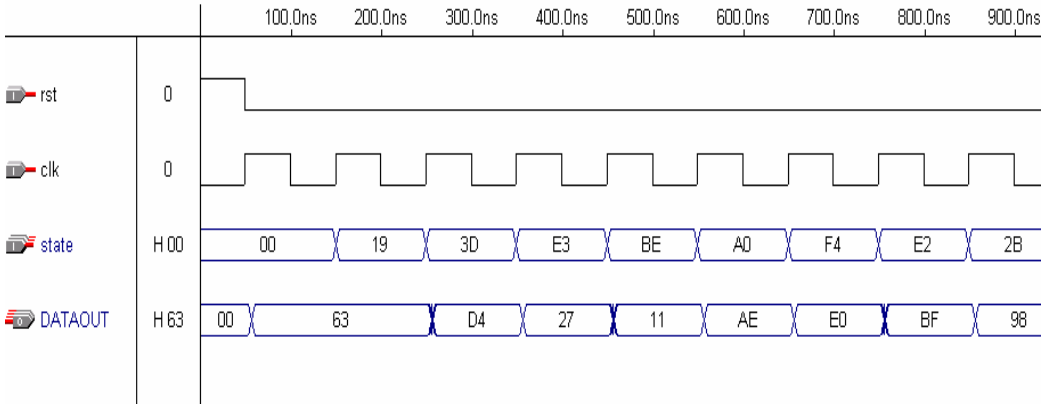

Fig. 5. AES SUB-BYTE Test bench waveform

Shift Row Transformation

The following Figure 6 represents the waveforms generated by the 8-bit byte substitution transformation. The inputs are clock of 100ns time period, Active Low reset, and 128-bit state as a standard logic vector, whose output is shifted as per design flow.

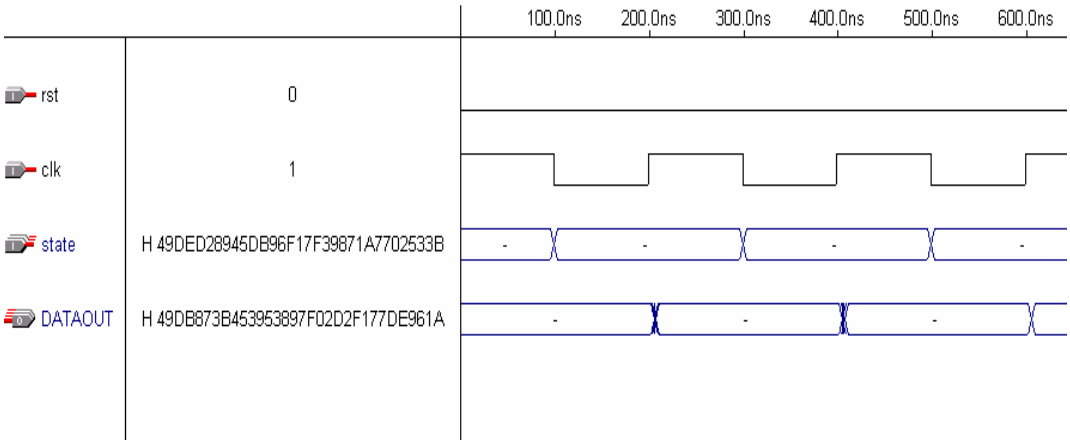

Fig .6 AES SHIFT-ROW Test bench waveform

Mix Columns Transformation

The following Figure 7 represents the waveforms generated by the 128-bit Mix Columns transformation. The inputs are clock of 100ns time period, Active Low reset, and 128-bit state as a standard logic vector, Whose output is mixed by using matrix multiplication as per design flow.

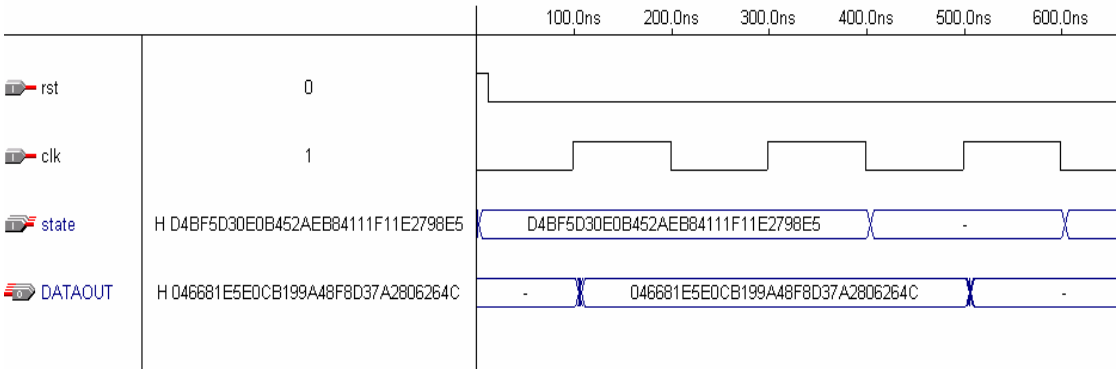

Fig. 7. AES MIX-COLUMN Test bench waveform

AES Encryption Simulation

This is the encryption simulation did in Xilinx ISE Project navigator in which Isim Simulator is used. The simulation consist of,

Input as: - Data in= 128 bit string as plain text, Key=128- bit string, Din_valid=K-en=reset=0, Clk=1, ENC=1.

Output as: - Dout_valid=1, DATA_OUT =Cipher text.

AES Encryption Simulation

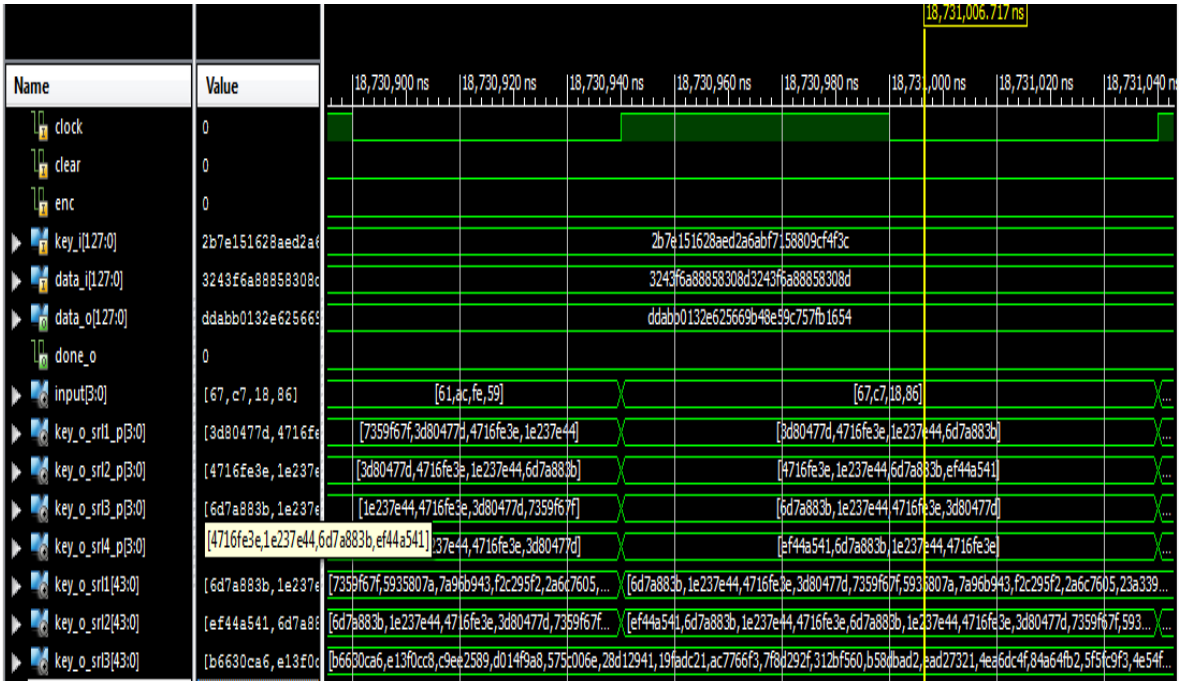

Fig. 8. AES TOP Module Encryption Waveform

AES Decryption Simulation

The decryption simulation result consists of cipher text as input for simulator and as our project is based on symmetric AES design so same key used for decryption also. The final output of overall process is nothing but receiving same DATA OUT(as original plain text input used in encryption) from cipher text.

Input as:-Data in= cipher text output from encryption,

Key in= same used for encryption, K_EN=Din_valid=reset=0.

And at the end of process CLK=0.

Output as:-

Cipher text= original plain text output.

D_OUT VALID = 1

AES Decryption Simulation

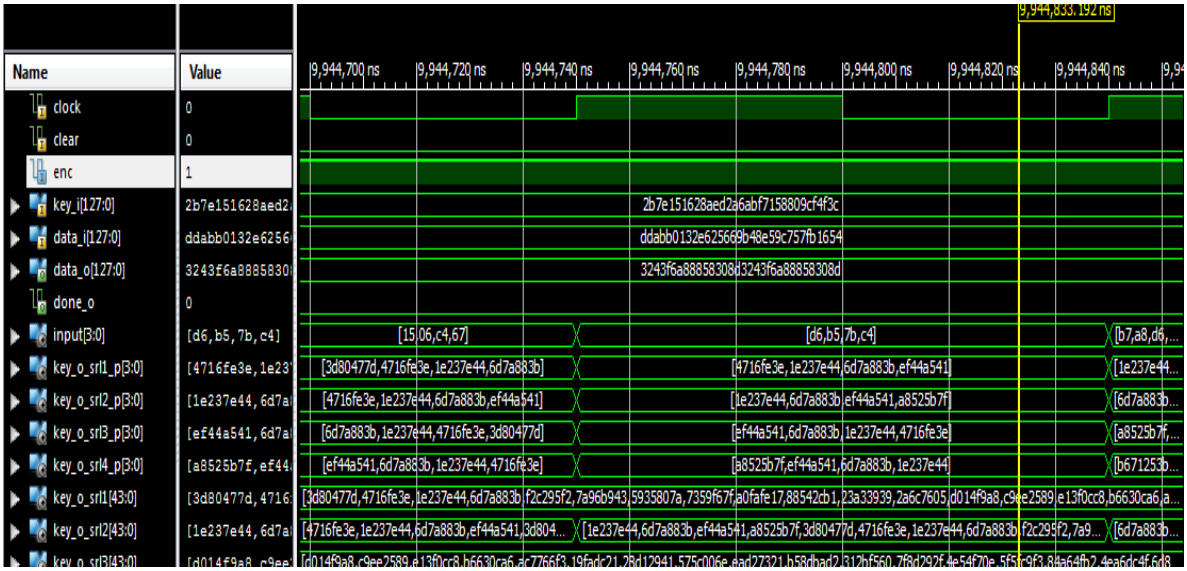

Fig. 9.AES TOP Module Decryption Waveform

AES Synthesis Report

The compact design presented by other researchers where examination of each of the components of the AES algorithm optimized on the basis of throughput per no of slices [1] [5] as shown in table 2,

SR.NO.	DESIGN BY	DEVICE	NUMBER OF SLICES
1	Jarvinen et.al	XCV-1000e-8	11719
2	Zhang And Pahri	XCV-1000e-8	11022
3	Issam et.al	XCV-1000e-8	9104
4	Hodjat	XC2VP20-7	9446
5	Zambreno	XC2V4000	16938
6	Issam et.al	XC2V4000-6	8503
7	Granado et.al	XC2V4000-6	3576
8	Issam et.al	XC2V4000-6	7884
9	Issam et.al	XC2V4000-6	10662
10	Elbirt et.al	XCV1000-4	10662
11	Our Work	XC3S1400AN	3376

7. CONCLUSION

The proposed design produces basic optimized design of AES algorithm in which the use of BRAM for storing memory element of S-BOX is occurred. The proposed design gives compact and optimized design which will optimizes result nearly about 30 per than previous research. This design gives simple design which can be used for further future work.

8. FUTURE SCOPE

Further optimization in area provides better performance for high end applications. The Encryption and the Decryption modules can be combined together in a single chip module instead of separate chips which cause, In future implementation of single chip design called AESTHETIC can be possible which enhances security over AES design's involving Multi-core and many–core processor arrays of Configurable AES architecture's for Flexible Security involving TES strategies.

REFERENCES

[1] Xinmiao Zhang, Student Member, IEEE, and Keshab K. Parhi, Fellow, IEEE "High-Speed VLSI Architectures for the AES Algorithm" IEEE TRANSACTIONS, VOL. 12, NO. 9, SEPTEMBER 2004.

[2] Tim Good, Student Member, IEEE, and Mohammed Benaissa, "Very Small FPGA Application-Specific Instruction Processor for AES" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, VOL. 53, NO. 7, JULY 2006.

[3] Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar,"FPGA Implementation of AES Encryption and Decryption "International Conference on "Control, Automation, Communication and Energy Conservation-2009, 4th-6th June 2009.

[4] Chen-Hsing Wang, Chieh-Lin Chuang, and Cheng-Wen Wu "AnEfficient Multimode Multiplier Supporting AES and Fundamental Operations of Public-Key Cryptosystems "IEEE TRANSACTIONS, VOL. 18 NO. 4, April 2010.

[5] Issam Hammad, Student Member, IEEE, Kamal Sankary, Member "High-Speed AES Encryptor with Efficient Merging Techniques"IEEE EMBEDDED SYSTEMS LETTERS VOL. 2, NO. 3, SEPTEMBER 2010.

[6] Bin Liu, Student Member, IEEE, and Bevan M. Baas, Senior Member, IEEE "Parallel AES Encryption Engines for Many-Core Processor Arrays "IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 3 MARCH 2013.

[7] Chodowiec and Kris Gaj George Mason University, "Very Compact FPGA Implementation of the AES Algorithm" MS1G5, 4400 University Drive, Fairfax, VA 22030, USA

[8] Federal Information Processing Standards Publication 197 November 26, 2001 Announcing the ADVANCED ENCRYPTION STANDARD (AES).

[9] Sliman Arrag, Abdellatif Hamdoun , Abderrahim Tragha and Salah eddine Khamlich, "Design and Implementation A different Architectures of mixcolumn in FPGA"

[10] International Journal of Reconfigurable and Embedded Systems (IJRES), "AES Encryption Algorithm Hardware Implementation: Throughput and Area Comparison of 128, 192 and 256-bits Key" ISSN: 2089-4864 Vol. 1, No. 2, July 2012, pp. 67-74

[11] Adam J. Elbirt, W. Yip, B. Chetwynd, and C. Paar, "An FPGA-Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists" IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 9, NO. 4, AUGUST 2001 545

[12] Mao-Yin Wang, Chih-Pin Su, Chia-Lung Horng, Cheng-Wen Wu, 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 541