Design and Implementation of Advanced Encryption Standard Algorithm-128 using Verilog

Vedkiran Saini, Parvinder Bangar

Abstract*— Security has become an increasingly important feature with the growth of electronic communication. The Symmetric in which the same key value is used in both the encryption and decryption calculations are becoming more popular. AES is a symmetric encryption algorithm processing data in block of 128 bits. Under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. In this paper our main concerns is study AES algorithm and implement all modules of AES algorithm on FPGA. This methodology uses verilog HDL implementation of all the modules of AES algorithm Substitution Bytes Transformation, Shift Rows, Transformation, Mix Columns Transformation, Add Round Key Transformation and present power two different frequency 25 MHz. and 50 Mhz. frequency. The codes have been synthesized using Xilinx ISE 9.1i software for a Virtex 5 FPGA device.

Index Terms*— Advanced Encryption Standard (AES), Rinjdael, Cryptography.

I. INTRODUCTION

The art of keeping messages secure is cryptography. Cryptography plays an important role in the security of data. It enables us to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it. The urgency for secure exchange of digital data resulted in large quantities of different encryption algorithms which can be classified into two groups: symmetric key algorithms (with private key algorithms) and asymmetric key algorithms (with public key algorithms).[25,26]Encryption is emerging as a disintegrable part of all communication networks and information processing systems, for protecting both in transit and stored data. Encryption is the transformation of plain data (known as plaintext) into unintelligible data (known as ciphertext) through an algorithm referred to as cipher. Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriate a key. Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data[11].

Security has become an increasingly important feature with the growth of electronic communication. The Symmetric, or secret key algorithms, a cryptography method in which the same key value is used in both the encryption and decryption calculations are becoming more popular. The keys, in practice, represent a shared secret between two or more users that can be used to maintain a private information link. Secret key cryptography uses conventional algorithm that is Advanced Encryption Standard (AES) algorithm. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

Manuscript Received on June 2014.

Ms. Vedkiran Saini, Department of ECE, CBS Group of Institution, Jhajjar, India.
Mr. Parvinder Bangar, CBS Group of Institution, Jhajjar, India.

This standard is based on the Rijndael algorithm.The AES also known as the Rijndael algorithm was selected as a Standard by National Institute of Standards and Technology (NIST).Advanced Encryption Standard (Rijndael Block Cipher) became the new US Federal Information Processing Standard on November 26, 2001[1,23] in order to replace the Data Encryption Standard (DES) which was used for more than 20 years as a common key block cipher for FIPS.Encryption is the transformation of plain data (known as plaintext) into unintelligible data (known as cipher text) through an algorithm referred to as cipher[11]. Symmetric key cryptography due to its use in military application, embedded system design, financial and legal files, medical reports, and bank services via Internet, telephone conversations, smart card, PDA, mobile phone and e-commerce transactions etc[3].

II. ADVANCED ENCRYPTION STANDARD ALGORITHM

The AES algorithm is a symmetric-key scheme. In symmetric key schemes, the encryption and decryption keys are the same. Thus communicating parties must agree on a secret key before they wish to communicate. It is also known as private-key scheme. AES [2] is a symmetric key block cipher published by NIST as FIPS 197. It encrypts as well as decrypts a plaintext blocks of size 128-bits. The number of rounds varies with the key size. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The numbers of cycles of repetition are as follows

Table1. Key-Block-Round Combinations [19]

	Key Length (32-bitword)	Block Size (32-bit word)	Number of Rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Here, The algorithm is used in encrypting data which is stored in blocks of 128-bit (here) and is encrypted with a 128- bit cipher key which is essential to decrypt the information locked in the encrypted data. The Encryption program needs two pieces of inputs one, is the input data which is to be encrypted and the other being the Cipher key with which the information will be locked. The Algorithm is in turn divided into two distinct parts:

a) Encyption
b) Key Generation

We will first look into the Encryption Algorithm then Key generation followed by the Decryption Algorithm.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

i. Substitution Bytes Transformation
ii. Shift Rows Transformation
iii. Mix Columns Transformation
iv. Add Round Key Transformation

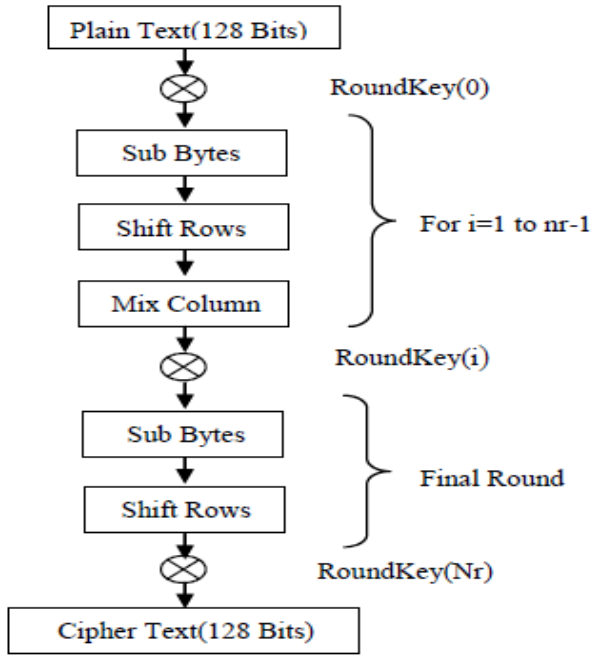


Figure 1. AES Algorithm Encryption Structure [19]

III. TRANSFORMATION IN AES ALGORITHM

A. *Sub Byte Transformation*

This is the first transformation to be done on the input data i.e, the input matrix.This step is also known as SubBytes. In the SubBytes step, each byte in the array is updated using an 8-bit substitution box, the Rijndael S-box. It substitutes all bytes of the state array using a LUT which is a 16x16 matrix of bytes, often called S-box.The sub byte transform is shown in figure 2.In AES algorithm the function of the sub byte is only nonlinear function and that operates independently on each byte of the state using a substitution table (S box). . This operation provides the nonlinearity in the cipher. The S-box used is derived from the multiplicative inverse over $GF^{(2^8)}$, known to have good non-linearity properties.

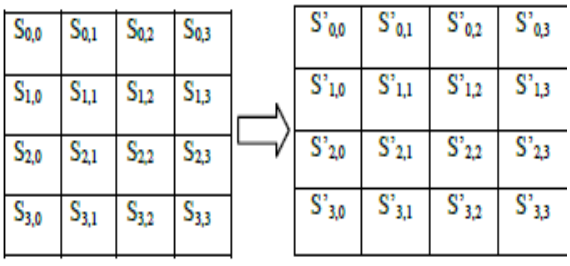


Figure 2. Application of S-Box to the Each Byte of the State

B. *Shift Row Transformation*

This is the Second Transformation in the series of 4 Transformations and is extremely simple to implement. It involves rotating the rows of the input matrix circularly upwards. In the Shift Rows transformation the bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets). It substitutes all bytes of the state array using a LUT which is a 16x16 matrix of bytes, often called S-box. The Shift row transform is shown in figure 4 the shift row transformation. Transformation same as Transformation is almost the same in the decryption process except that the shifting offsets have different values. The main goal of this process is to correlate and scramble the byte order inside each 128-bit block. In the shift the bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets).in this process the row 0 is not shifted, row0 is shifted one byte to the left, row 2 is shifted two bytes to the left and row 3 is shifted three bytes to the left.

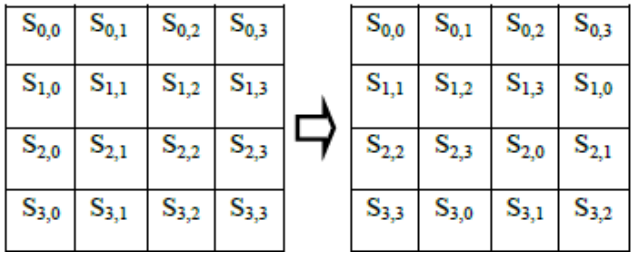


Figure 3. Shift Row Transformation

C. *Mix Column Transformation*

This transformation is based on Galois Field multiplication and third transformation in series 4. Each byte of a column is replaced with another value that is a function of all four bytes in the given column. The Mix Columns transformation is performed on the State column-by column [5].The mix column implementation is shown in figure 5. Each column is considered as a four-term polynomial over $GF^{(2^8)}$ and multiplied by a(x) modulo x4 + 1, Where

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

This Transformation is for mixing up of the bytes in each column separately during the forward process. The corresponding transformation during decryption is denoted Inv Mix Columns and stands for inverse mix column transformation. The goal is here is to further scramble up the 128-bit input block.

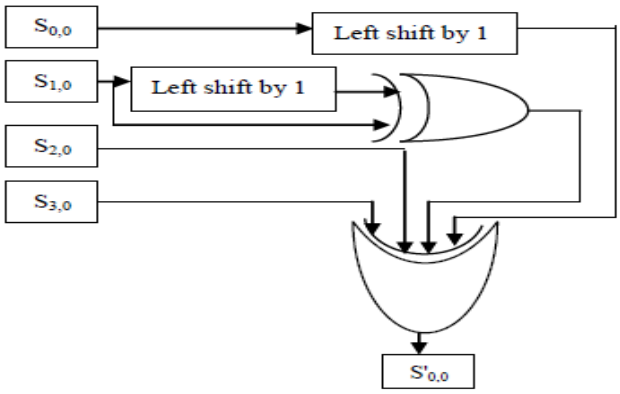


Figure 4. Mix Column Transformations in Matrix Form [19]

D. *Add Round Key and Key Expansion*

In this operation, the round key is applied to the State by simple bit by bit XOR. Key Expansion unit generates the next round key as for three different key size, AES consist of 10, 12 or 14 rounds. After every round a new round key is produced. This process utilizes the concept of shifting the bytes and substitution of bytes which were used in Data processing unit.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

i. Add Round Key

Add Round Key step is applied one extra time comparing to the other encryption steps. The first Add Round Key step is applied before starting the encryption iterations, where in the encryption process the first 128 bits of the input key the whole key in case of using key size of 128 bits are added to the original data block as shown in figure 6. This round key is called the initial round key [4]. It is implemented in hardware as a simple exclusive-or operation of the 128 bit data and key.

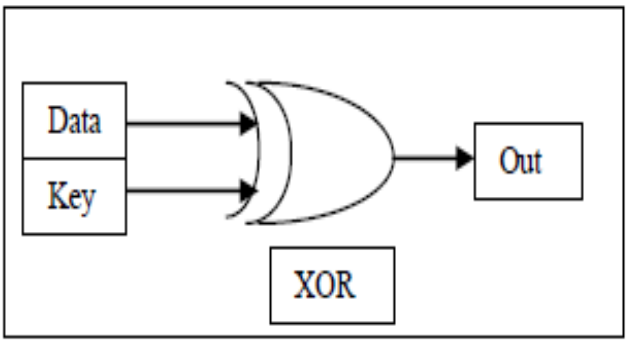


Figure 5. Hardware Implementation of Add Round Key

ii. Key Expansion

The key expansion term is used to describe the operation of generating all Round Keys from the original input key. The initial round key will be the original key in case of encryption the whole operation is shown in figure 7. The key expansion term is used to describe the operation of generating all Round Keys from the original input key. The initial round key will be the original key in case of encryption and the last group of the generated key expansion keys in case of decryption – the first and last 16 bytes in case of key sizes of 192 and 256 bits. As mentioned previously this initial round key will be added to the input initially before starting the encryption or decryption iterations. Using the 128 bits key size, 10 groups of round keys will be generated with 16 bytes size for each.

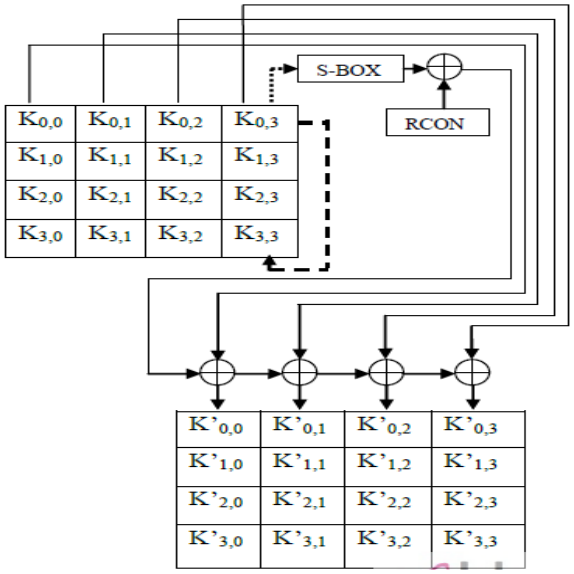


Figure6. Key Expansion[19]

The first 4 bytes column in each group will be generated as follows:

- Taking the S-BOX equivalent to the last column of the previous group (one previous column).
- Perform one cyclic permutation "rotate elements
- Add the round constant.
- Add the result to the first column of the previous group (four previous columns).

IV. SIMULATION RESULT

The AES algorithm is implemented using Verilog HDL coding in Xilinx ISE 9.1i software for a vertex5device. First, the algorithm is tested by encrypting a single 128 bit block. AES block length/Plain Text = 128bits (Nb = 4); Key length=128 bits (Nk= 4); No. of Rounds = 10(Nr = 10).
Tables 2 show the summary of resources utilized by the pipelined AES for a Virtex 5 device 5vlx30ff324-3. Out of available 19200 Slice Registers, 19200 slice LUTs, 15876fully used Bit Slices and 32 BUFG/BUFGCTRLs. Thus %age utilization of resources is 56% Slice Registers, 54% of Slice LUTs,34% of Number of fully used Bit Slices and 6% BUFG/BUFGCTRLs. Table 3 show the power result at 25 Mhz and Table 4 show the power result at 50 Mhz frequency.

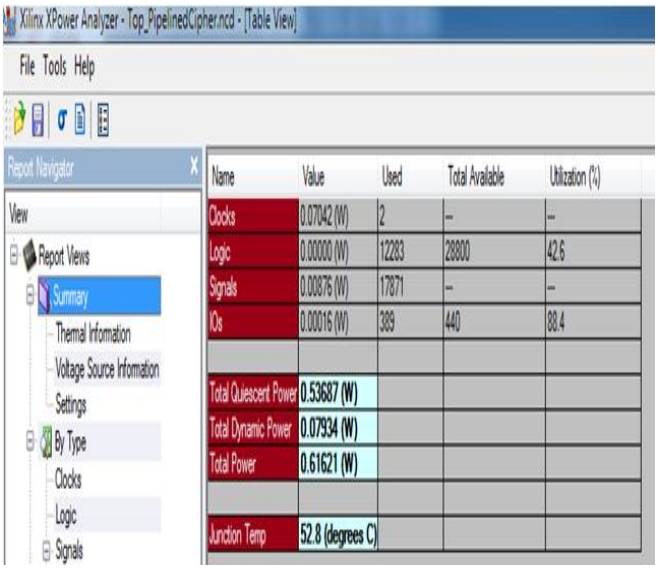
Table 2. The Synthesis & Mapping Results of AES Design

VEDKIRAN_AES Project Status			
Project File:	VEDKIRAN_AES.ise	Current State:	Synthesized
Module Name:	Top_PipelinedCipher	• Errors:	No Errors
Target Device:	xc5vlx30-3ff324	• Warnings:	2 Warnings
Product Version:	ISE 9.1i	• Updated:	Wed Jun 25 06:32:38 2014

VEDKIRAN_AES Partition Summary
No partition information was found.

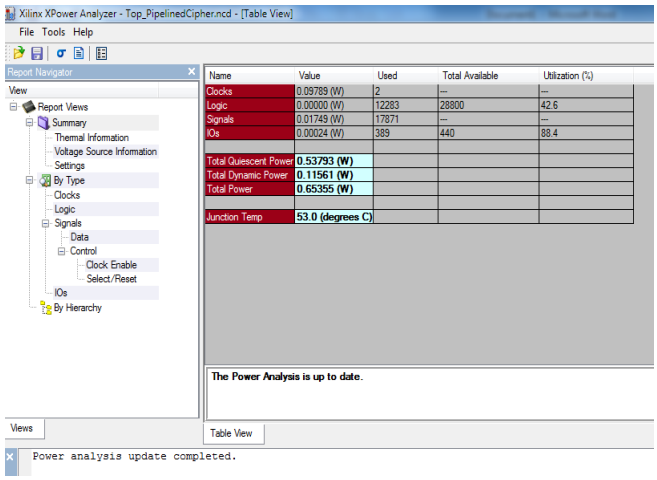
Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slice Registers	10769	19200	56%
Number of Slice LUTs	10558	19200	54%
Number of fully used Bit Slices	5451	15876	34%
Number of bonded IOBs	389		
Number of BUFG/BUFGCTRLs	2	32	6%

Table 3. Power Result of AES Design at 25 Mhz Frequency



Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Table4. Power Result of AES Design at 25 Mhz Frequiency



V. CONCLUSION

As the cryptography is playing the major role in today's world. The Advanced Encryption Standard-Rijndael algorithm is an iterative private key symmetric block cipher that can process data blocks of 128 bits through the use of cipher keys with lengths of 128 FPGA implementation of 128 bit block and 128 bit key AES-Rinjdael cryptosystem has been presented in this paper. In this paper we present the basics of AES algorithm and the implementation of its modules by using verilog HDL. Here the simulations are performed with vertex5device families. The software we have used is Xilinx9.1i and the waveforms are simulated with model sim simulator and power analysis 25 Mhz and 50 Mhz frequency.

REFERENCES

[1] Xinmiao Zhang and Keshab K. Parhi "Implementation Approaches for the Advanced Encryption Standard Algorithm"IEEE 2002

[2] X. Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm,"IEEE Transactions on Very Large Scale Integration Systems, vol.12, issue 9, pp.95 967, Sep. 2004.

[3] Hui QIN, Tsutomu SASAO, Yukihiro IGUCHI "An FPGA Design of AES Encryption Circuit with 128-bit Keys"GLSVLSI'05, ACM 2005.

[4] 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

[5] Chih-Peng Fanand and Jun-Kui Hwang "FPGA Implementations Of High Throughput Sequential And Fully Pipelined AES Algorithm" International journal of Electrical Engineering, vol.15, no.6, pp. 447-455, 2008.

[6] Pachamuthu Rajalakshmi, "Hardware-software co-design of AES on FPGA**"** International Conference on Advances in Computing, Communications and Informatics, Pages 1118-1122, 2010.

[7] Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh "Efficient and High Performance Parallel Hardware Architecture for the AES-GCM" IEEE Transactions On Computers, vol.61, no. 8, August 2012.

[8] Saambhavi Baskaran and Pachamuthu Rajalakshmi "Hardware Software Co-Design of AES on FPGA" ICACCI '12,ACM August 2012.

[9] [9] Pallavi Atha et al, "Design & Implementation Of AES Algorithm Over FPGA Using VHDL", International Journal of Engineering, Business and Enterprise Applications (IJEBEA)", ISSN (Online): 2279-0039,pp. 58-62,2013

[10] [10] M. komala subhadra et al, "Advanced Encryption Standard - VHDL Implementation", International Journal For Technological Research In Engineering, ISSN (Online): 2347 - 4718, Volume 1, Issue 3, pp.132-137 November – 2013.

[11] [11] Archana garg et al, "Implementation of Advanced Encryption Standard Algorithm using VHDL", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 9, pp. 3956- 3961,September 2013

[12] [12] Yoshimura, M. et al, "Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)", IEEE International Symposium on Page(s):278 – 283, 2013

[13] [13] Hui QIN, Tsutomu SASAO, Yukihiro IGUCHI "An FPGA Design of AES Encryption Circuit with 128-bit Keys" GLSVLSI'05, ACM 2005

[14] [14] Chih-Peng Fanand and Jun-Kui Hwang "FPGA Implementations of High Throughput Sequential and Fully Pipelined AES Algorithm" International journal of Electrical Engineering, vol.15, no.6, pp. 447-455, 2008.

[15] [15] Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh"Efficient and High Performance Parallel Hardware Architecture for the AES-GCM" IEEE Transactions On Computers, vol.61, no. 8, August 2012.

[16] [16] Archna Garg et al, "Efficient Field Programmable Gate ArrayImplementation of Advanced Encryption Standard Algorithm using VHDL", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 9, pp. 3956-3961,September 2013

[17] [17] Saambhavi Baskaran and Pachamuthu Rajalakshmi "Hardware Software Co-Design of AES on FPGA" ICACCI '12,ACM August 2012.

[18] [18] 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.

[19] [19] Richa Sharma, Purnima Gehlot, S. R. Biradar, "VHDL Implementation of AES-128, UACEE International Journal of Advances in Electronics Engineering – IJAEE, Volume 3 : Issue 2, [ISSN 2278 – 215X],pp-17-20, 2013

[20] [20] X. Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm,"IEEE Transactions on Very Large Scale Integration Systems, vol.12, issue 9, pp.95 967, Sep. 2004.

[21] [21] Jin Gong ,Wenyi Liu, Huixin Zhang "Multiple Lookup Table-Based AES Encryption Algorithm Implementation" Elseveir- 2012 vol.25 pg no.842 – 847.

[22] [22] Biham, Eli and Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer Verlag, 1993.

[23] [23] National Institute of Standards and Technology, "Federal Information Processing Standards Publication 197", 2001

[24] [24] Jin Gong ,Wenyi Liu, Huixin Zhang "Multiple Lookup Table-Based AES Encryption Algorithm Implementation" Elseveir- vol.25 pg no.842 – 847, 2012.

[25] [25] SCHNEIER, B. : Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 1996

[26] [26] O. Prasanthi ,M. Subba Reddy et al., "RSA Algorithm Modular Multiplication", International Journal of Computer Applications in Engineering Sciences , VOL II, ISSUE II, pp.53-55,JUNE 2012

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.