International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 3, No. 2, July 2014, pp. 49~53
ISSN: 2089-4864

Design of AES Algorithm for 128/192/256 Key Length in FPGA

Pravin V. Kinge[1], S.J. Honale[2], C.M. Bobade[3]
[1]Department of Electronics and Telecommunication Engineering
G.H. Raisoni College of Engineering, Amravati, India
[2,3]Faculty of Electronics and Telecommunication Engineering
G.H. Raisoni College of Engineering, Amravati, India

Article Info

Article history:

Received Feb 22, 2014
Revised May 5, 2014
Accepted May 20, 2014

Keyword:

AES
Ciphertext
FPGA
Plaintext
VHDL

ABSTRACT

The cryptographic algorithms can be implemented with software or built with pure hardware. However Field Programmable Gate Arrays (FPGA) implementation offers quicker solution and can be easily upgraded to incorporate any protocol changes. The available AES algorithm is used for data and it is also suitable for image encryption and decryption to protect the confidential image from an unauthorized access. This project proposes a method in which the image data is an input to AES algorithm, to obtain the encrypted image, and the encrypted image is the input to AES Decryption to get the original image. This project proposed to implement the 128,192 & 256 bit AES algorithm for data encryption and decryption, also to compare the speed of operation, efficiency, security and frequency. The proposed work will be synthesized and simulated on FPGA family of Xilink ISE 13.2 and Modelsim tool respectively in Very high speed integrated circuit Hardware Description Language (VHDL).

Corresponding Author:

Pravin V. Kinge,
PG Student, Department of Electronics and telecommunication Engineering,
G. H. Raisoni College of Engineering, Amravati.
Email: Kinge.p.v@gmail.com

1. INTRODUCTION

In communication security is the most important factor during 19 century. The data security is the big issue in various field so us government invited the new cryptography concept. For secure communication instead of DES algorithm, the disadvantage of DES algorithm is only 56 bit key. Its length easy to break so the new AES algorithm is developed by Joan Daemen and Vincent Rijmen this algorithm is approved by us national institute of standard & technology in October 2000. The basic of AES Rijndael are in a mathematical concept called as Galois field theory. Similar to the way DES function, Rijndael also used the basic techniques of substitution and transposition (i.e. permutation). The key size and the plain text block size decide how many rounds need to be executed. The minimum number of rounds is 14. One key differentiator between DES and provides for more optimized hardware and software implementation of the algorithm. AES algorithm has fix block size 128 bit and key size 128,192 and 256 bit. AES algorithm implemented by using hardware and software by using software it is easy to implemented the AES algorithm and it is easy low cost but it is not fully secured most secure. AES algorithm is applied data as well as image every image define in pixel concorn intensity value (digitel number) and location address in the form of row and column. The applications of the image processing have been commonly found in the Military communication, Forensics, Robotics, Intelligent systems etc. In this project, the AES algorithm is proposed which is an efficient scheme for both hardware and software implementation.

AES algorithm

An encryption algorithm converts a plain text message into cipher text message which can be recovered only by authorized receiver using a decryption technique. The AES-Rijndael algorithm [4] is an iterative private key symmetric block cipher. The input and output for the AES algorithm each consist of sequences of 128 bits (block length). Hence Nb = Block length/32 = 4. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits (Key length). In this implementation, the key length is 128. Hence Nk = Key length/32 =4.

Encryption Process

The Encryption and decryption process consists of a number of different transformations applied consecutively over the data block bits, in a fixed number of iterations, called rounds. The number of rounds depends on the length of the key used for the encryption process. For key length of 128 bits, the number of iteration required are10. (Nr = 10). As shown in Figure 1, each of the first Nr-1 rounds consists of 4 transformations: SubBytes(), ShiftRows(), MixColumns() & AddRoundKey().

Figure 1. AES Rijndael Describe step

There are four different transformations are described in detail below.

a) *Sub Bytes Transformation*:

It is a non-linear substitution of bytes that operates independently on each byte of the State using a substitution table (S box). This S-box which is invertible is constructed by first taking the multiplicative inverse in the finite field GF (2^8) with irreducible polynomial m(x) = x8 + x4+ x3 + x + 1. The element {00} is mapped to itself. Then affine transformation is applied (over GF (2)).

b) Shift Rows Transformation:

Cyclically shifts the rows of the State over different offsets. The operation is almost the same in the decryption process except for the fact that the shifting offsets have different values.

c) Mix Columns Transformation:

This transformation operates on the State column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF (2^8) and multiplied by modulo x4 + 1 with a fixed polynomial a(x) = {03} x3+ {01} x2+ {02} x.

d) Add Round Key Transformation:

In this transformation, a Round Key is added to the State by a simple bitwise XOR operation. Each Round Key consists of Nb words from the key expansion. Those Nb words are each added into the columns of the State. Key Addition is the same for the decryption process.

Key Expansion:

Each round key is a 4-word (128-bit) array generated as a product of the previous round key, a constant that changes each round, and a series of S-Box lookups for each 32-bit word of the key. The Key schedule Expansion generates a total of Nb (Nr + 1) words.

The decryption process is direct inverse of the encryption process. All the transformations applied in encryption process are inversely applied to this process. Hence the last round values of both the data and key are first round inputs for the decryption process and follows in decreasing order.

2. RELATED WORK

The system uses AES key expansion which is used to generate multiple non-linear keys for the encryption process. This algorithm is suitable for image encryption in real time applications [1]. The data can be encrypted by 128 bit cipher key, through the use of cipher key with length 128, an efficient FPGA implementation of 128 bit block and 128 bit key AES algorithm has been presented [2]. They presented a low cost effective area cipher for encryption /decryption using 128 bit iterative architecture, after found that the amount of hardware resources has been optimize, One of the important Implementation of AES algorithm has been presented by Raneesha K, Rema Vellody and R nanda Kumar They compared two type of algorithm for speed of operation and observed that controller base approach [4]. Mg Suresh, Nataraj. K.R, concluded that the concept of Pipelined AES architecture can be practically implemented. It has been observed that the implementation of AES Encryption on the FPGA is successful and several data input. The AES algorithm is an iterative private key symmetric block cipher that can process data block of 128- bits through the use of cipher keys with key length 128,192 and 256 bits. An efficient FPGA implementation of 128 bit block and keys 128, 192 and 256 bits of AES –Rijindael algorithm has been presented [5].

3. WORKING

The proposed work implemented with Field Programmable Gate Arrays (FPGA), which offers quicker solution and can be easily upgraded to incorporate any protocol changes. The available pipelined AES algorithm is used for image and suitable for image encryption and decryption to protect the confidential image from an unauthorized access. This project proposes a method in which the image is an input to pipelined AES algorithm to obtain the encrypted image, and the encrypted image is the input to pipelined AES Decryption to get the original image, as Figure 2. In this project, implement the 128,192 & 256 bit pipelined AES for image encryption and decryption and compare the speed of operation and efficiency, security & frequency.

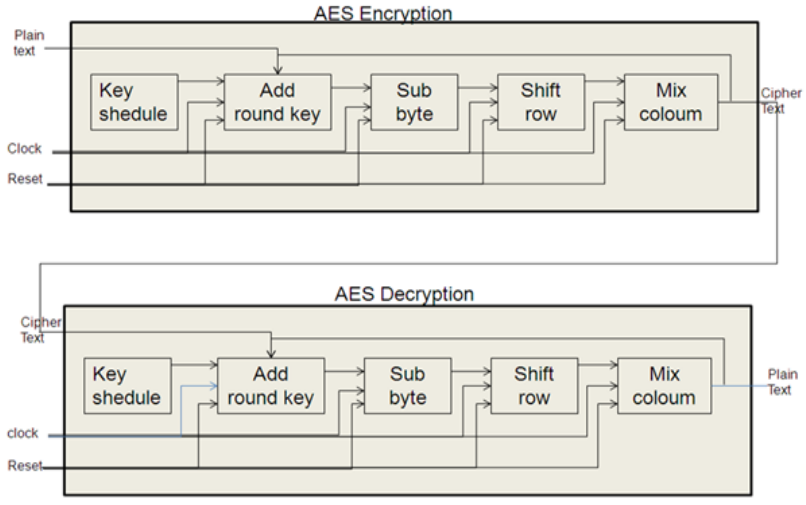

Figure 2. AES encryption/Decryption module in VHDL

4. SIMULATION RESULTS

The design has been coded by VHDL. All the results are synthesized and simulated basing on the Xilinks 3E, the Model Sim.The results of simulating the AES 128/192/256 encryption/decryption algorithm from the ModelSim simulator are shown in Figure 3, Figure 4 and Figure 5. We have generated a Generic code which can be use for all the three AES key.

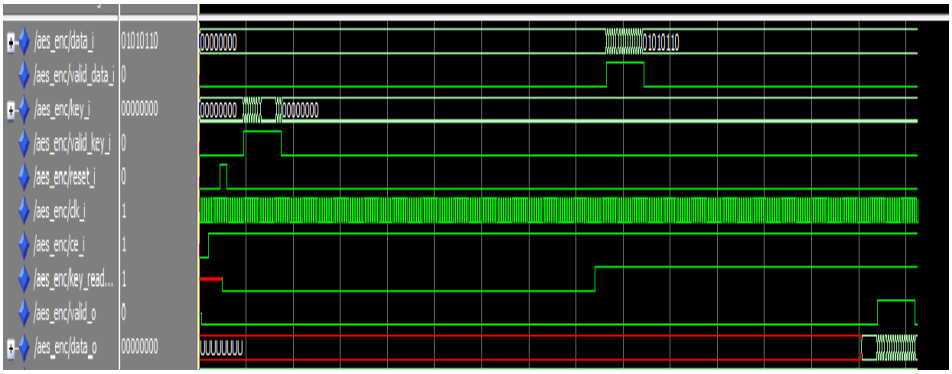

Figure 3. Timing simulation of AES128 encryption algorithm

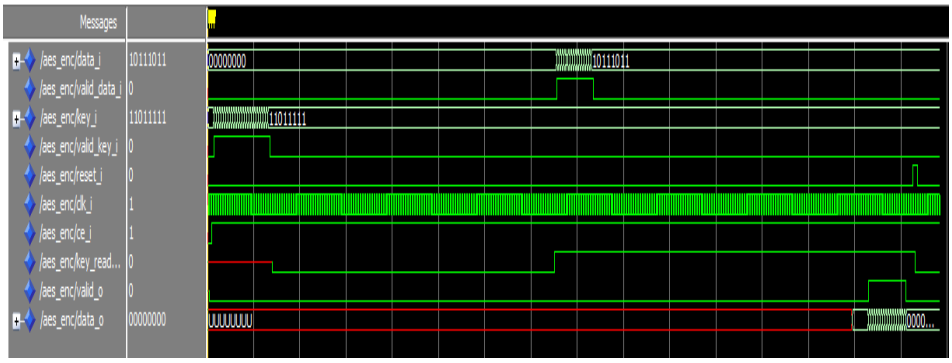

Figure 4. Timing simulation of AES192 encryption algorithm

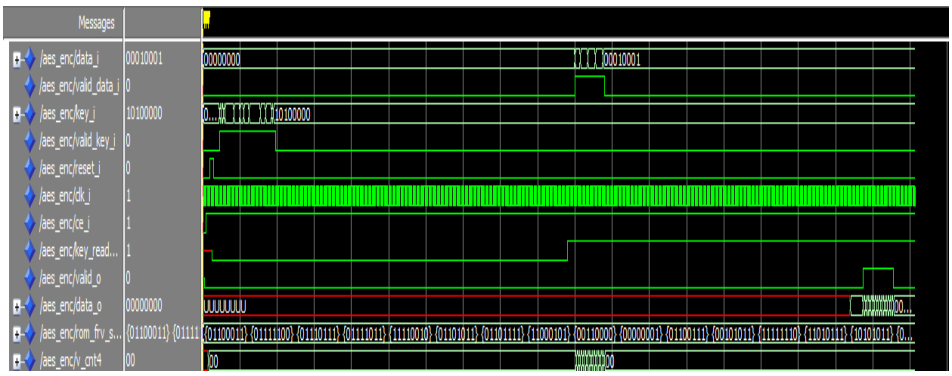

Figure 5. Timing simulation of AES256 encryption algorithm

They are showing a low latency. Hence, the practical results are in accordance to theoretical predictions and satisfy the encryption and decryption methodology. To test the system, a test bench is used. The test bench applies encryption/decryption input pulse to trigger the system. The output result of the encryption was found accurately after 99 clock cycles from the starting of encryption process. So the latency of encryption is only 99 clock cycles. Similarly, the latency of decryption is 99 clock cycles.

AES KEY Size	128 bit	192 bit	256 bit	Existing Result 128 bit
Maximum Operating Frequency	112.790MHz	123.712MHz	114.877MHz	140.390MHZ
Number of Slices	869 out of 4656	854 out of 4656	875 out of 4656	1853 out of 6912
Number of Slice Flip Flops	330 out of 9312	332 out of 9312	330 out of 9312	512 out of 13824
Number of 4 input LUTs	1725 out of 9312	1699 out of 9312	1737 out of 9312	3645 out of 13824
Number of bonded IOBs	31 out of 232	31 out of 232	31 out of 232	391 out of 408
Encryption/Decryption Throughput	145.83 Mbps	199.6Mbps	211.57Mbps	352Mbits/sec
Total memory usage	212220 KB	213244 KB	212220 KB	130248 KB
CLOCK Required for encryption/decryption	99	119	139	223

5. CONCLUSION

The Advanced Encryption Standard algorithm is a symmetric block cipher that can process data blocks of 128 bits through the use of cipher keys with lengths of 128, 192, and 256 bits. An efficient FPGA implementation of 128 bit block and 128 bit key AES algorithm has been presented in this paper. The design is implemented on XILINKs using Spartan 3E FPGA which is based on high performance architecture. Our architecture is found to be better in terms of latency, throughput as well as area. The design is tested with the sample vectors provided by FIPS 197.

REFERENCES

[1] B. Subramanyan, Vivek. M. Chhabria, T.G. Sankar babu, "Image Encryption Based On AES Key Expansion", *Second International Conference on Emerging Applications of Information Technology, DOI 10.1.109/EAIT.2011.60,* IEEE, 2011.

[2] Hoang Trang, Nguyen Van Loi, "An efficient FPGA implementation of the advanced Encryption standard algorithm", *978-1-4673-0309-5/12, IEEE,* 2012.

[3] A. Amaar, I. Ashour and M Shiple, "Design and implementation a compact AES Architecture for FPGA Technology", *World Academy of science, engineering and technology,* 59, 2011.

[4] Raneesha K, Rema Vellody and R nanda Kumar, "Hardware efficiency comparion of AES implementation", *international conference on communication system and network technology. DOI 10.1109/CSNT.2012.187, IEEE,* 2012.

[5] Mg Suresh, Dr. Nataraj. K.R, "Area Optimized and Pipelined FPGA Implementation of AES Encryption and Decryption", *International Journal of Computational Engineering Research,* Vol. 2 Issue 7, Nov 2012.

[6] National Institute of Standards and Technology (U.S.), "Data Encryption Standard (DES)", *FIPS Publication 46-3, NIST, 1999. Available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf*

[7] J. Yang, J. Ding, N. Li and Y.X. Guo, "FPGA-based design and implementation of reduced AES algorithm" *IEEE Inter. Conf. Chal Envir Sci Com Engin (CESCE).* Vol. 02, Issue. 5-6, pp. 67-70, Jun 2010.

[8] National institute of standard and technology, "Federal information Procesing standaed publication 197, *the AES"*, Nov 2001.