A Review paper on Design of Pipelined Architecture for implementation of AES key encryption/decryption module

Mr. Pravin V Kinge
Student of M. E. Electronics & Telecommunication

Mr. Ravi H Bailmare
Student of M. E. Electronics &Telecommunication

Prof. S.J.Honale
Faculty of Electronics & Telecommunication

Department of Electronics & Telecommunication Engineering
G.H.Raisoni College of Engineering, Amravati, Maharashtra.

Abstarct:- The cryptographic algorithms can be implemented with software and 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 image encryption and decryption to protect the important image from an unauthorized access. This project proposes a method in which the image data 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. This project proposed to implement the 128,192 & 256 bit Pipelined AES algorithm for image 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 9.2 and Modelsim tool respectively in Very high speed integrated circuit Hardware Description Language (VHDL).

Keywords: ***AES, FPGA,VHDL,Plaintext,Ciphertext***

I. 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 128,192and 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 Pipelined 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 to 128. Hence Nk = Key length/32 =4

initialization processes

- Expand the 16-byte key to get the actual key block to be used.
- Do one time initialization of the 16-byte plain text block(called as state).
- XOR the state with the key block.
- Apply s-box to each of the plain text bytes.
- Rotate row k of the plain text block(i.e. state) by k bytes.
- Perform a mix columns operation.
- XOR the state with the key block.

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 Fig. 1, each of the first Nr-1 rounds consists of 4 transformations: SubBytes(), ShiftRows(), MixColumns() & AddRoundKey().

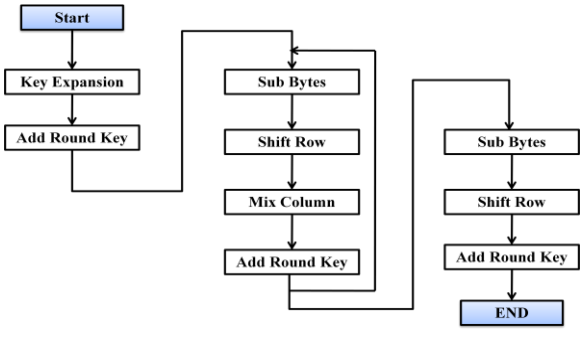

Figure 1:- AES Rijndael Describe step.

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.

II. RELATED WORK

In [1] paper makes use of AES Key Expansion which is used to generate multiple non-linear keys for the encryption process. Based on the experimental results it can be observed that the proposed algorithm offers high encryption quality with minimal memory requirement and computational time.. The above mentioned features make the algorithm suitable for image encryption in real time applications [1].

In paper [2] 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. Encryption /decryption algorithm was synthesized, implemented by Altera Tool and achieve Low Latency and the Throughput reaches the value of 1054Mbit/sec for encryption and 615Mbit/sec for Decryption [2].

This paper [3] presents a low area cost effective area cipher for encryption /decryption using 128 bit iterative architecture, after found that the amount of hardware resources has been optimize with respective to various proposed design on alternative platform Spartan 3 and Virtex E. The cipher text has been synthesize using Xilink 6.2 simulated using Modelsim SE6.2 [3]

One of the important Implementation of AES algorithm has been presented by Raneesha K , Rema ellody and R nanda Kumar [4]. They compare two type of algorithm for speed of operation and observe that controller base approach took at list 505 clock cycle each to perform encryption and decryption [4].

In paper [5] Mg Suresh, Dr.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 cipher key can be changed with respect to the user requirements. The result shows that the design with the pipelining technology and special data transmission mode can optimize [5].

III.CONCLUSION

From review of various papers concluded that AES algorithm is base suited for protection of data/images(i.e.encryption and Decryption),using different key length. Because protection of data is much more important in application like Military communication, Forensics, Robotics, Intelligent systems. If key length increase security increase but speed of operation decrease.

Hear we use AES with different key length for encryption and use of pipeline architecture of AES algorithm, we will try to find better result as compare to various research in field of speed/area/power.

IV.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, IEEE2011*.

[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.*