IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Analysis of the Effective Advanced Encryption Standard Algorithm

Umalaxmi Sawant[1], Prof. Kishor Wane[2]

Student, Electronics and Telecommunication, DPCOE, Pune, India [1]

Professor, Electronics and Telecommunication, DPCOE, Pune, India[2]

Abstract: Now a day's civilization is hugely dependent upon electronic and communication system. In this electronic world, increasing need of data protection in computer networks is necessary for the development of several cryptographic algorithms and to send data securely over a transmission link from one person to another person.AES is one of the better algorithms for secured transmission than the traditional algorithm. In this AES algorithm, various steps are required to encrypt and decrypt. The AES algorithm uses cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data on block size of 128 bits. The algorithm is synthesized and simulated using Xilinx ISE and Model Sim software and results are compared with previous work.AES algorithm is implemented on hardware as well as software which provide higher security.

Keywords: AES **(**Advanced Encryption Standard), DES (Data Encryption Standard), Encryption, Decryption, Cryptography, FPGA, cipher text.

I. INTRODUCTION

In today's life people generates and interchange large amount of information in various fields such as defences, medical reports, and bank services via Internet [1].To utilize the channel resources completely encryption algorithm must have a speed at least equal to data transmission speed. Achieving high throughput for encryption algorithm for a communication channel of high data rate is a challenging task.

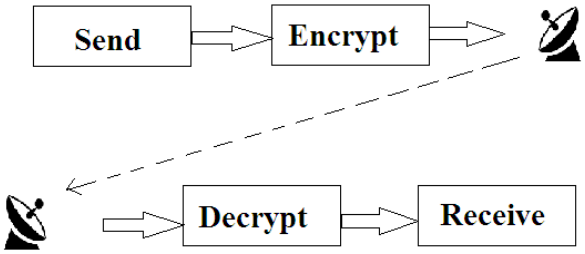

Fig. 1 General Diagram of Information Transmission

To secure the access of unauthorized data from hackers Cryptography is used [1].Cryptography is nothing but "hidden or secret codes" to encrypt the data before transmission. In 1977 the DES(Data Encryption Standard) issued for the encryption by FIPS (Federal Information Processing Standard). This scheme was considered as more secured scheme in 1998, due to the small key length of DES it is replaced by the Rijndael algorithm. The later Rijndael algorithm was selected as AES algorithm [2].

AES algorithm is based on software implementation as well as hardware implementation. Generally high security with high speed cannot be provided by the only Software implementation, so hardware implementation is used. Which provides today's requirement that is high speed, high volume secure communication combined with physical security [3].

Basically, to change original form of data (plaintext) to unreadable form or with coded form(cipher text) is known as encrypted information. AES algorithm has various steps which are required to encrypt and decrypt. The AES algorithm uses cryptographic key lengths of 128, 192, and 256 bits to encrypt and decrypt data in block size of 128 bits [4].Cryptography has two types Symmetric and Asymmetric. Symmetric (Private Key) Cryptography is nothing but the same key is used for encryption &decryption. Asymmetric (Public) Cryptography means the Different keys are used for encryption &decryption. The symmetric key is much effective and has fast approach as compared to asymmetrical key cryptography. So that Advanced Encryption Standard (AES) is a private key algorithm [5].

The AES algorithm is used in various application fields like automated teller machines (ATMs), cellular phones, digital video recorders as well as WWW servers [6].

II. RELATED WORK

Ashwini R. Tonde, Akshay P. Dhandproposed that Advanced Encryption Standard (AES) algorithm implemented on FPGA is presented in this paper. The design has been coded by Very high speed integrated circuit Hardware Description Language. All the results are synthesized and simulated using Xilinx ISE and Model Sim software respectively [1].

Hoang Trang, Nguyen Van Loi, Said that, an efficient FPGA implementation of 128 bit block and 128 bit key AES algorithm is proposed. In this the encryption /decryption algorithm is synthesized and 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].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Z. Yuan, Y. Wang, J. Li, R. Li and W. Zhao proposed that masking method are used to defend against power analysis attacks in embedded systems. Masking techniques are Boolean masking, Additive masking, Multiplicative masking, mixed masking, Algorithmic level masking is used. To resist against DPA (Differential Power Attack) is optimized AES implementation with 32-bits and 128-bits data path separately [3].

Ms. Ruchi R. Vairagade Prof. Shubhangini Ugale Prof. Prachi Pendke proposed that it is 128 bits AES algorithm since it will accept 128 bits plaintext and 128 bits master key. The 128 bit cipher text block is produced after plaintext block which is processed by round of times. This algorithm uses a combination of Exclusive-OR operation (XOR), Substitution with S-Box, Row and Column rotation and a Mix column. Plaintext, cipher text and intermediate state block can be depicted as 4*4 matrix form. In this paper, the proposed work presents the details of 128 bits AES Encryption and Decryption structure and conducts a fault injection attack against the unprotected AES. The methodology is based on VHDL [4].

Saurabh Kumar, V. K. Sharma, K. K. Mahapatrapaper presents and proposed that delay improved VLSI architecture of S-box for Advance Encryption Standard (AES) algorithm. The architecture is implemented in FPGA. By using constant area in terms of FPGA slices, delay is improved along with low power consumption. This architecture is implemented with FPGA and ASIC. ASIC is implemented using 0.18 µm standard cell technology library which shows delay improvement of about 16 percent [5].

Vishal Pachori, Gunjan Ansari, Neha Chaudhary proposed that Most of the research for performance improvement, AES is based on hardware implementation. This paper presents the parallel implementation of AES using JPPF (Java Parallel Programming Framework) which provides flexibility & performance improvement in terms of speed-up. In this implementation there are two approaches data parallelism and control parallelism[6].

III.PROPOSED WORK

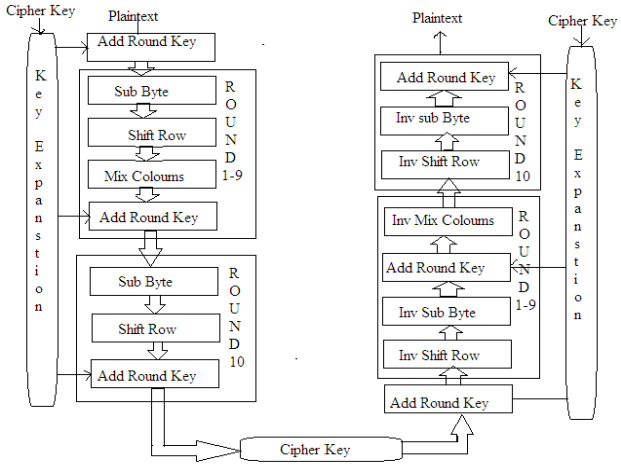

Fig.2 AES standard encryption & decryption Algorithm

Advanced Encryption Standard (AES) is published under the name of FIPS-197 (Federal Information Processing Standard number197) which is adopted by National Institute of Standards and Technology (NIST).

The AES algorithm uses symmetric block cipher. It encrypts data of block size 128 bits. It uses three key sizes, 128 bits, 192 bits and 256 bits. In three versions no of rounds are 10, 12 and 14respectively.
AES encryption and decryption algorithm has subsequent steps as following:

A. Sub Bytes
The first transformation is sub byte transformation. Sub Bytes transformation is Cipher that processes the State using a nonlinear byte substitution Table (S-box) that operates on each of the State bytes independently. It has two types

1. Conventional BRAM
2. Combinational Logic

A. Conventional BRAM
All pre-computed 256 value stored in ROM based lookup table and input byte wired to ROM's address bus, but there is disadvantage.
Disadvantage- This method suffers from unbreakable delay as fixed access time for read and writes operation as well as low latency due to ROM access time. Parallel ROMs were leading to large size of chip area which requires high amount of memory and it increases the throughput.

B. Combinational Logic
Therefore S-box transformation through composite field arithmetic is more appropriate for low latency with decrease in area. A more suitable second method is to implement S-Box by using combinational logic. It has benefit like small area occupancy and pipelined for increased performance in clock frequency. In this paper S-Box architecture based on combinational logic is proposed. It is computed by multiplicative inverse in GF(2^8) followed by an affine transformation. In this Inverse Sub Byte transformation, firstly applied inverse affine transformation and then multiplicative inverse.

B. Shift Rows
Shift Rows transformation is Cipher that processes the State by cyclically left shifting the last three rows of the State by different byte. First row is not shifted, second row is circularly left shifted by one byte position, third row is circularly left shifted by two byte position, and last row circularly left shifted by three bit positions

C. Mix Columns
In Mix Columns transformation, the four bytes of each column from state are combined using an invertible linear transformation. Here only Colum-wise operation is done, where 4 bytes input process at the same time and gives 4 bytes outputs. Mix Column transformation in Cipher that takes all of the columns of State and mix their data individually of one another to produce new columns using GF (2^8) polynomial.

DOI 10.17148/IJARCCE.2016.53227

D. Add Round Key

In this Add Round Key operation bitwise exclusive-or (XOR) operation is used and performing the XOR operation between outputs from mix column and round keys. For AES 128,128 bit XOR operations are performed.

E. Key Expansion

In Key Expansion, parallelism concept is used. Key Expansion routine is used to perform key scheduling, which generate a series of Round Keys from cipher key. Advantage of Parallelism is to increase speed and decrease time of key generation. In Key Expansion routine Sub Word is present that takes a 4-byte input word applies to S-box each of 4-bytes to produce an output word. Before that rot word is present which takes input word and performs a cyclic permutation where 4 byte word cyclic right shifted with 1 bytes increment. Rcon is array of bytes in a word having permanent logical value having size of 128 bit.

Cipher key computed for each round of operation for that temporal storage Key register is used.

Here input to key expansion module is 128 bit cipher generates 10 number of 128 bit size of RAM or Partial key for each round of operation. The pipeline structure for repeated computation become lower down speed up to nine times as well as data rate A combinational logic of Key Expansion reduce period by nine time for key generating.

In the AES decryption side Inv Sub byte, Inv Shift Rows Inv Mix columns, Inv add round key operation are performed just opposite operation to the encryption side.

IV. RESULT

Xilinx ISE tool is used for the synthesis and the for testing and verification purpose Xilinx ISE and Model SIM tool is used. In this the Comparative result are shown between implemented AES algorithm and the Standard algorithm. The various performance parameters of the design like throughput, latency, area, power, etc are calculated and compared with the previous work.

TABLE 1 Proposed work AES Encryption design utilization

Parameter	AES128	AES128 regular
Data path(bit)	128	128
LUT FF	459	40
Slice LUTs	3559	24999
Slice Register	564	4800
No. of Round	10	10
Block RAM	4	11
Max.Operating Frequency(MHz)	273.997	102.990
Area Constraint Ratio	50%	>100%
Throughput(Mbps)	855.61	13183.6
Combinational Delay(Ns)	0	11.992

V. CONCLUSION

Advanced encryption standard algorithm is the efficient algorithm and analyzes the result in term of speed, area, power consumption with the Standard algorithm. This is based on the software as well as hardware system so that security is high as compared to the traditional algorithm. Also the key system is sufficient to encrypt the data and this is suitable for any application where the requirement is strong encryption technology.

REFERENCES

[1] Ashwini R. Tonde, Akshay P. Dhand, "Review Paper On FPGA Based Implementation Of Advanced Encryption Standard Algorithm", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014

[2] Hoang Trang, Nguyen Van Loi, "An efficient FPGA implementation of the Advanced Encryption Standard algorithm", Proc. Computing and Communication Technologies RIVF International Conference, pp.1-4 July 2012

[3] Z. Yuan, Y. Wang, J. Li, R. Li and W. Zhao, "FPGA based optimization for masked AES implementation", Proc. IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), pp.1-4 August 2011.

[4] Ms. Ruchi R. Vairagade Prof. ShubhanginiUgale Prof. PrachiPendke, "Review On 128 Bit Advanced Encryption Standard Algorithm With Fault Detection" International Journal Of Advanced Information And Communication TechnologyVolume 1, Issue 7, November 2014

[5] Saurabh Kumar, V. K. Sharma, K. K. Mahapatra, "Low Latency VLSI Architecture of S-box for AES Encryption", Proc. International Conference on Circuits, Power and Computing Technologies, pp. 694-698 March 2013.

[6] Vishal Pachori, Gunjan Ansari, NehaChaudhary,"Improved Performance of Advance Encryption Standard using Parallel Computing",International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 1,Jan-Feb 2012, pp.967-971