ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

MODIFIED ADVANCED ENCRYPTION STANDARD WITH ADDITIONAL ROW TRANSFORMATION

Sathya Sankaran, Sneha Ambhore, P.M.Durai Raj Vincent*
[1,2]14PHD0483, Vellore Institute of Technology, Vellore.
Associate Professor, SITE School of Information Technology and Engineering, VIT University, Vellore, Tamilnadu.
Email: pmvincent@vit.ac.in

Received on 06-08-2016 *Accepted on 27-08-2016*

Abstract

AES is one of the significant encryption algorithms available till date. Several studies have been made on the efficiency and performance of AES. This paper is a study of the various research work on AES. The studies help us understand the advantages of the encryption algorithm and gives us a better understanding of its working. Some introduce a new technology in the implementation; some introduce a new environment in which to do the implementation. The information gathered from all will be of use in further modifications to AES.

Introduction

Over ages, there has been a necessity to transmit confidential information from one part of the globe to the other. Simultaneously, there has been a growth to tap this information by introducing several types of attacks called security attacks. Security mechanisms and security services have been introduced to handle these security attacks and to ensure the security of the information transferred from one place to another. Cryptographic algorithms have been used to protect data from the intruders. Cryptography is used to transform the message sent into a form that cannot be understood by the hackers. At the receiving end, the transformation is reversed thereby yielding the original message that was sent by the sender to the receiver. Some of the cryptographic algorithms available are (Rivest – Shamir – Adlemen) , DES and AES algorithm. All the algorithm available have their own advantages and disadvantages. In this paper, we are doing a survey on AES algorithm and try to improve it.

Basic Flow of AES: The basic flow of advanced encryption standard is given below which involves substitution of bytes, shifting rows and mixing columns which is shown in the diagram.

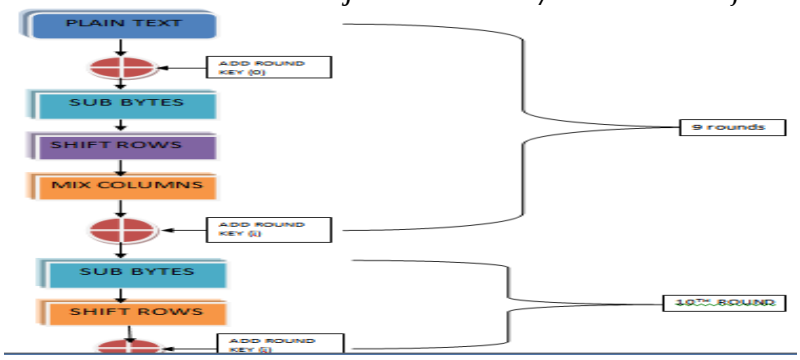


Fig 1: AES

Literature survey

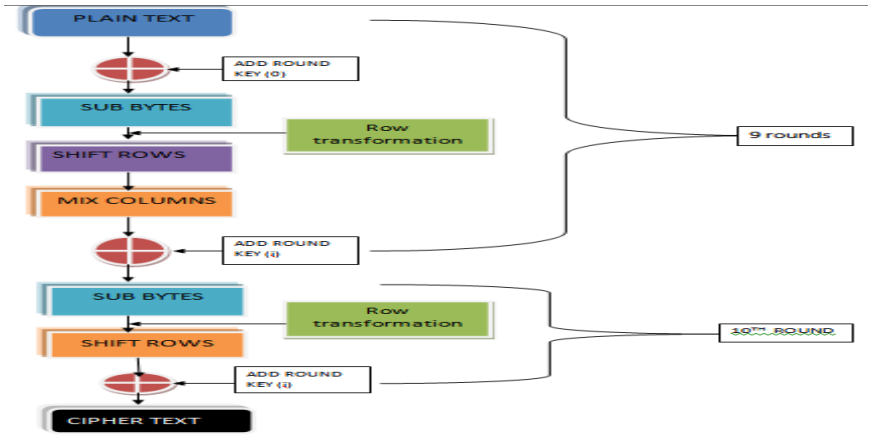
DFA techniques were used modified in this Paper[1] which were originally being used on AES-128 so as retrive the entire key of AES-192 and AES-256. This paper proposed the attack possible on the key expansion of AES-192 and AES-256. and this paper has also analyzed that the modification of differential fault analysis on key expansion is difficult than that on DFA state using the mentioned technique

To increase the efficiency of the execution, hardware realization of AES was in research those days. The paper[2] developed a dedicated processor which is based on Electronic System Level which is an optimized processor. The designs were compared with FPGA and ARM ISA and it was been concluded that by using FPGA the cycle count can be reduced by 40.8% using 38% percent of memory. The performance evaluation of AES-128 bit has been carried out in Paper[3]. Hardware models were being used to evaluate the performance of the algorithm named HDL and IP core. The comparison included the encryption time and performance metrics such as size, speed and memory were also been considered. In paper[4] the architecture with low cost error detection was being developed. The method implemented in this paper offers basis for BIST implementation. A technique was being implemented for masking of AES in[5]. It was represented using tower field. And it was realized that this technique is optimal with less cost as well as resources and high performance when compared to other techniques out there. And it was compared with other techniques with respect to security with the simulator named modelsim. A hardware implementation of 8-bit AES was implemented using CFB/OFB in[6] without using block RAM. Where BRAM occupies low area, higher slice count and gives less throughput. To enhance the security performance the 8-bit AES is added to our wireless device i.e Bluetooth. A high performance as well as time cost efficient Advanced Encryption System is being presented in[7]. The system proposed here can be used in various embedded application. A compact architecture of Mix Columns is presented in[8]. The architecture is then further compared with the existing architecture and it was being found that the number of gates used here is reduced by 14% of

the original and also the complexity of algorithm is being reduced by using the proposed architecture. In paper[9] C++ implementation of AES algorithm is done and different hardware micro architecture of the same is done using HLS solution. A baseline software was being implemented first and then the hardware realization of the same was done by analyzing which constraints to satisfy inorder to get a C++ code out of it. Keeping the same roboustness and security of the standard algorithm a algorithm on DNA Cryptography was being proposed in[10]. In comparison to previous algorithms the proposed algorithm consists of less mathematical and theoretical basis and giving the same results as in binary based AES. In Location based data encryption methods and applications[11] geo-encryption is the application of a mobile user's location. These encryption methods are called Location based Encryption Methods. It is used to improve the security of applications by the name Location based Services. It includes geographical position and time data for the encryption and decryption. Better throughput and higher security is possible. In, A secure and efficient file protecting system based on SHA3 and parallel AES[12]AES is combined with Secure Hash Algorithm 3. It introduces high performance using the Graphics Processing Unit and parallelism at the CPU level or GPU level. For efficient implementation of Advanced Encryption Standard on hardware which can be reconfigured, a pipelined as well as parallel architecture was being proposed in [13], by increasing the rounds the strength of AES is improved. The overall efficiency of the algorithm reduces inversely to the number of rounds.

Proposed System

The proposal is to include another Row Transformation before the shift row activity for each round. The number in row is considered to be decimal number, modulus of a 10 gives last digit and then this digit will be substracted from the other digits of row. This will make it more complex . In decryption the opposite operations will be carried out i.e the number will be added from the numbers in the row except the last number .



Result and Analysis

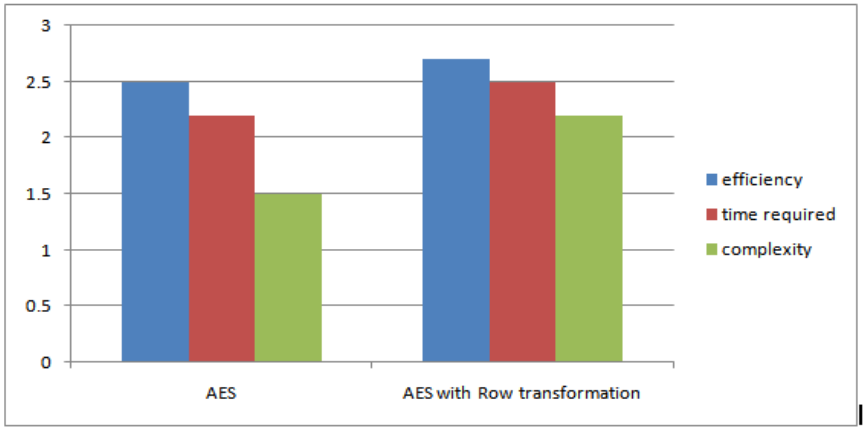


Figure 1: comparison of AES algorithm to AES with Additional row transformation

AES till date is the fastest security algorithm and researches are still carried out on it to make it more efficient so that it can be used in almost all fields. Also AES was being combined with RSA,ECC to make it more complex and efficient. due to the advancements in AES it will be easy to crack the AES algorithm in near future In such case an additional row transformation like the above will increase the stability of AES .moreover the transformation suggested can be reversed during decryption.

Conclusion

The aim of the proposed system was to make AES more acceptable by increasing its efficiency and complexity. The results above shows that the difference by using only AES and AES with Additional Row Transformation i.e. it not only increases the efficiency but also the complexity of a system also the time required is more since an extra round is added to the existing system. But, the efficiency offered additionally is an advantage.

References

1. Noemie Floissac, Yann L' Hyver, "from AES -128 to AES-192 and AES-256, how to adapt differential fault analysis attack on Key Expansion", 2011 workshop on Fault diagnosis and Tolerence in Cryptography.
2. Renhai Chen, Zhipinh Jia *, Yibin Li, Hui Xia, Xin Li, "The Application Specific Instruction processor for AES" Shandong University.
3. Mona Sabry, Mohamed Hasem, Taymoor Nazmy, Mohamed Essam Khalifa, "Design of DNA- based Advanced Encryption Standard(AES)",2015 IEEE 7th International Conference on Intelligent Computing and Information Systems.

4. Jyothi Yenuguvanilanka, Omkar Elkeelany, ”Performance Evaluation of Hardware Models of Advanced Encryption Standard (AES) Algorithm”, Tennessee Tech University.
5. Jayashri Patil ,”On-Line Error Detection and testing of AES”, 2009 international conference on computers and devices for communication.
6. Wei Wi[1],Xiaoxin Cui[1],Di Wu[1],Rui Li[1], Kaisheng Ma, Dunsh An yu[1],Xiaole Cui[2],”A Compact Implementation of Masked AES S-Box”, PeKing University Beijing, PeKing University Shenzhen Graduate School.
7. Chi-Wu Huang, Shao wei kuo, Chi-Jeng Chang, ”Embedded 8-bit AES in Wireless Bluetooth Application”, ICSSC 2013.
8. Mehrdad Biglari[1], Ehsam Quasam[2], Behnaz Pourmohseni[2],”Maestro : A High Performance AES Encryption/Decryption System”, Sharif University of Technology, University of Tehran.
9. Hua Li, Zac friggstad,”An Efficient Architecture for the AES Mix Column Operation”, Department of Mathematics and Computer Science, University of lethbridge Canada.
10. Rodrigo Schmitt Meurer, Tiago Roigerio, Antaneo Augusto Frohlich, ”An Implementation of the AES Cipher using HLS”, Federal University of Santa Catarina,Brazil,2013 Brazilian Symposium on Computing Systems Engineering.
11. Kolapwar.P.G., Ambulgekar.H.P., ”Location based data encryption methods and applications”, SGGS Institute of Engineering and Technology, Nanded, India.
12. Fei, Xiongwei, et al. "A Secure and Efficient File Protecting System Based on SHA3 and Parallel AES."*Parallel Computing* 2016.
13. Nedjah, Nadia, Luzia de Macedo Mourelle, and Chao Wang.”A Parallel Yet Pipelined Architecture for Efficient Implementation of the Advanced Encryption Standard Algorithm on Reconfigurable Hardware.”,(IJPP) International Journal of Parallel Programming 2016.

Corresponding Author:

P.M.Durai Raj Vincent*,

Email: *pmvincent@vit.ac.in*