IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Optimized Mix Column Architecture Design and Fault Detection Scheme for the Advanced Encryption Standard

[1]MANOHAR.C.M, [2]SUDHA.H,

[1]PG Student, [2]Associate Professor
[1]VLSI Design and Embedded Systems,
[1]Banglore Institute of Technology, Bengaluru, INDIA

Abstract: With the evolution of the Internet, there has been a huge spurt in online transactions and also an increase in sharing of private, confidential and sensitive information over the web. This in turn has increased the requirement of highly secure and swift methodologies to protect such data using modern cryptographic techniques such as the Advanced Encryption Standard (AES). AES is an endorsed cryptographic algorithm that can be utilized to secure electronic information. AES was replacing the old Data Encryption Standard (DES) with more security. In order to achieve the same, this project discusses significant and novel modifications to the existing hardware architecture of the mix column step of the AES algorithm. And also implement the fault detect scheme for AES.

Index Terms **- AES, Mix Column, Encryption, Decryption, Fault Detection, VLSI.**

I. INTRODUCTION

The dawn of the 21st century has brought along with it a huge amalgamation of technological breakthroughs and novel inventions. Most of these discoveries cater to easing the life of people in their day to day life activities which include communication, agriculture, transportation and the likes. At the same time, it must be noted that most of these innovations are currently backed by complex algorithms generally setup and executed on servers situated elsewhere using the power of cloud computing and wireless communication. These systems can also be controlled wirelessly through virtual private networks and also remote desktop access solutions. Though this may seem advantageous, it comes along with it a major disadvantage as well. If not vigilant, these systems can unfortunately be also controlled by unauthorized personnel through hacking, obtaining credentials through phishing and other network security breaches. Hence, highly efficient and quick methodologies to secure such systems, becomes the need of the hour.

The past few years has seen a large increase in different methodologies to provide network security to various installations, the most common of these methods being cryptography. Whether it is social networking, online transactions, social security or controlling smart applications through the Internet of Things (IoT), cryptographic methods assist in prevention of data loss or cyber theft. The word Cryptography, which is derived from two Greek words 'krypto' and 'graphene' which mean hidden and writing respectively, is the science of protecting vital information, where the data is encrypted or scrambled in such a way that only the one who possesses the knowledge of deciphering it, can understand it. Amongst the various cryptographic techniques which exist, the most popular methods include the Data Encryption Standard (DES), Triple DES (3DES) and the Advanced Encryption Standard (AES). Amid these, due to the advantages of the AES standard over the rest, it is considered as the most preferred algorithm. Currently, a further advanced variant of the AES – the Rijndael algorithm, is also popularly used, mainly due to its heightened level of security.

II. LITERATURE REVIEW

- The authors [1] explains Cryptography is the art and science of keeping massages secure. It is the study of techniques related to aspects of information security such as information privacy, integrity, authentication and non-repudiation. Cryptography is almost synonymous with encryption i.e. the conversion of plain text to a cryptic text to secure it against unauthorized users.

- The authors [2] have surveyed the traditional algorithms, along with the proposed algorithms based on their pros and cons, related to Symmetric and Asymmetric Key Cryptography. The author have also compared the importance of both these cryptographic techniques. The proposed algorithms proved to be highly efficient in their respective grounds but there are certain areas that remained open, related to these algorithms, and have not yet been thoroughly discussed.

- The authors [3] provide a comparison of two encryption standards, 3DES and AES is presented. It may seem that DES is insecure and no longer of any use, but that is not the case since the DES and 3DES algorithms are still beyond the capability of most attacks in the present day. However, the power of computers is increasing and stronger algorithms are required to face hacker attacks.

- The authors [4] describes a modified version of the Advanced Encryption Standard algorithm is developed here for the aim of security and easier implementation. As the cloud users and communications over the network are increasing tremendously and therefore the users also would like faster storing and access to data on the cloud, it's become the key issue to provide security. Advanced Encryption Standard (AES) is a vastly used technique for providing security.

- The authors [5] explains High throughput AES encryption/decryption is a necessity for many of modern embedded systems. This article presents a high performance yet cost efficient AES system. In the proposed architecture the DMA modules act as interfaces between data sources and data sinks by loading the input data into AES engine and taking encrypted and generated test data to target memories.

- The authors [6] details Implementation of the Encryption algorithm AES under VHDL language In FPGA by using different architecture of mix column. The author then review this research investigates the AES algorithm in FPGA and the Very High Speed Integrated Circuit Hardware Description language.

- The authors [7] proposed and implemented of a one very useful method for area efficient and high performance for AES by using "Mixing of column and Inverse mixing of column operation" which is the one of the major block of operation in AES to implement the high performance of AES. I SIMULATE and SYNTHESIS on XILINX ISE 14.7 and implemented on VIRTEX 4. It is 100% area efficient.

- The authors [8] use FPGA chips to realize high data throughput AES pipelined architecture is proposed by partitioning the ten rounds into sub-blocks of repeated AES modules. In this paper the author have detailed the alternative design of both direct, inverse Mix Column transforms and high secure nonlinear S-box required in the AES hardware implementation and apply the pipeline architecture for high speed application.

- The authors [9] describes AES is one of the widely accepted and used algorithms for ensuring the security of data. The advancements in VLSI technology, both from the point of view of design complexity and increase in the probability of error occurrences, have become a significant problem to consider. However, some faults may occur during the implementation of AES which results in reducing the reliability and may cause leakage of information. In this work, we have implemented AES-128 with fault detection techniques based on parity and interleaved parity generation which does not require any additional hardware.

- The authors [10] describes Advanced Encryption Standard has been built as the first choice for many cryptographic applications because of the high level of security This paper presents a low power and low area design for the Advanced Encryption Standard based on an 8-bit data path. It has significant power-area-latency performance improvements over normal 128-bit data path AES. Such improvements are achieved by the use of resource sharing, simple compact memory architecture, Low Resource Mix Column Circuit, minimizing memory transfers and avoiding unnecessary switching activity. In addition to the performance requirements of the AES, it must be reliable against transient or permanent internal faults.

- The authors [11] explains Cryptographic circuits are used in areas that require confidentiality and a secure information exchange. Thus, these circuits use cryptographic algorithms proven resistant to conventional attacks by certified organizations of the state. For performance reasons, Advanced Encryption Standard (AES) is often physically implemented in cryptographic circuits. This implementation proves make these circuits susceptible to other types of attacks that exploit any kind of information from the system to obtain the secret key. In this paper, the simulation results indicate that error coverage of our proposed countermeasure archive 99.993%.

III. INSIGHTS ON AES

3.1 Advanced Encryption Standard (AES)

The Advanced Encryption Standard is used in order to protect data against unauthorized access and to encrypt this. The cryptographic process key of varying lengths is utilized for this purpose. This is designated AES-128, AES-192 or AES-256 depending on the length. Data security is the key parameter to be taken care to prevent the loss of information and avoid cyber-crimes. Data security assumes imperative job in putting away and transmitting the information. When we transmit interactive media information, for example, sound, video, pictures and so forth over the system, cryptography gives security.

As shown in fig 3.1, it can be clearly seen that the input data is first subjected to the add-round key step and is then made to undergo 10 rounds of AES wherein the first nine rounds involve all the 4 steps i.e., Sub byte operation, Shift row operation, Mix column operation and Add round key operation, the tenth round excludes the mix column step.

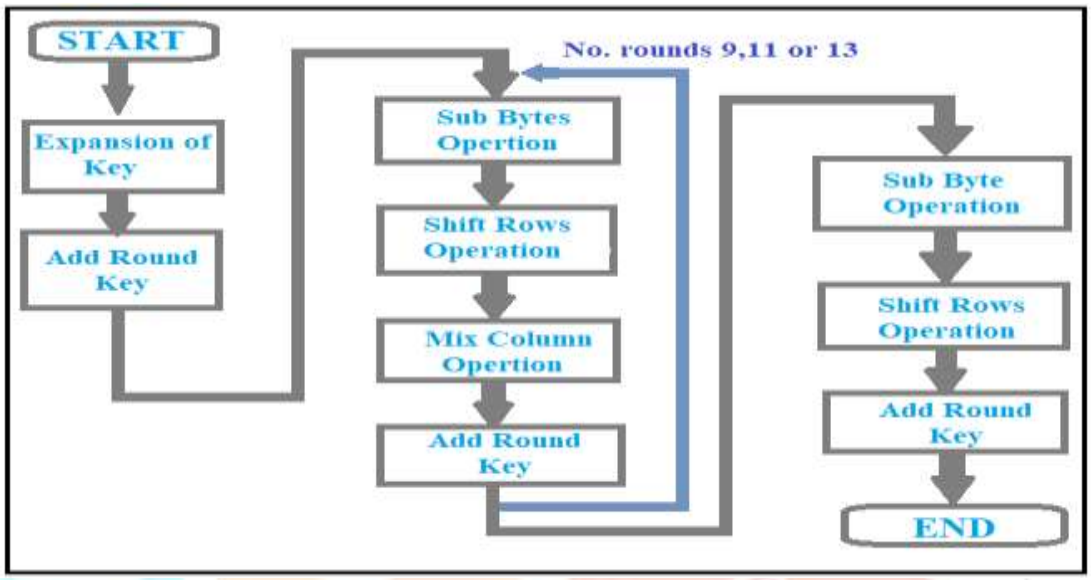

Fig 3.1: Steps involved in the AES algorithm

IV. PROPOSED METHODOLOGY

4.1 FLOW CHART

AES comprises of 128 square lengths of bits and backings 128 bit, 192 bit and 256 bit key length bits. The 128 bit key is sorted out into state framework which measure of 4×4, then the calculation begins with starting change of state grid followed by ten cycles of rounds. A round comprises of four changes byte substitution (sub bytes), row shifting (shift rows), mixing of sections (mix columns) and pursued by expansion of round key called (add round key). From every cycle, a round key is produced by the first key through key blocking process. The final round comprises of sub bytes, shift rows and add round key change.

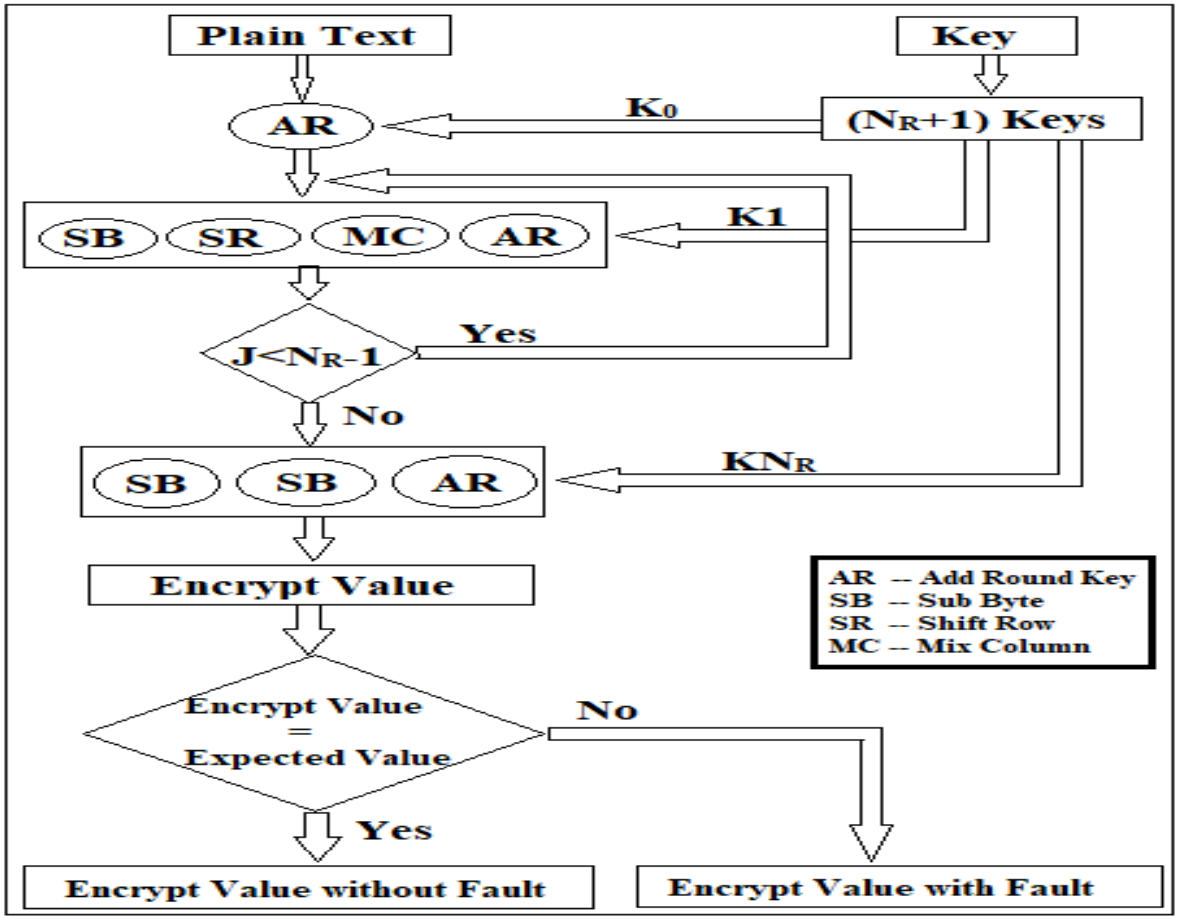

Fig.4.1: Flow chart of the execution

In this project we present a differential fault attack that can be applied to the AES using a single fault. Here, demonstrate that when a single bit fault is induced at the input of the AES inputs. Fault Attacks exploit malicious or accidental faults injected during the computation of a cryptographic algorithm.

4.2 OPERATIONAL BLOCK DIAGRAM

Fig.4.2 represents the block diagram of encryption and decryption of the Advanced Encryption Standard.

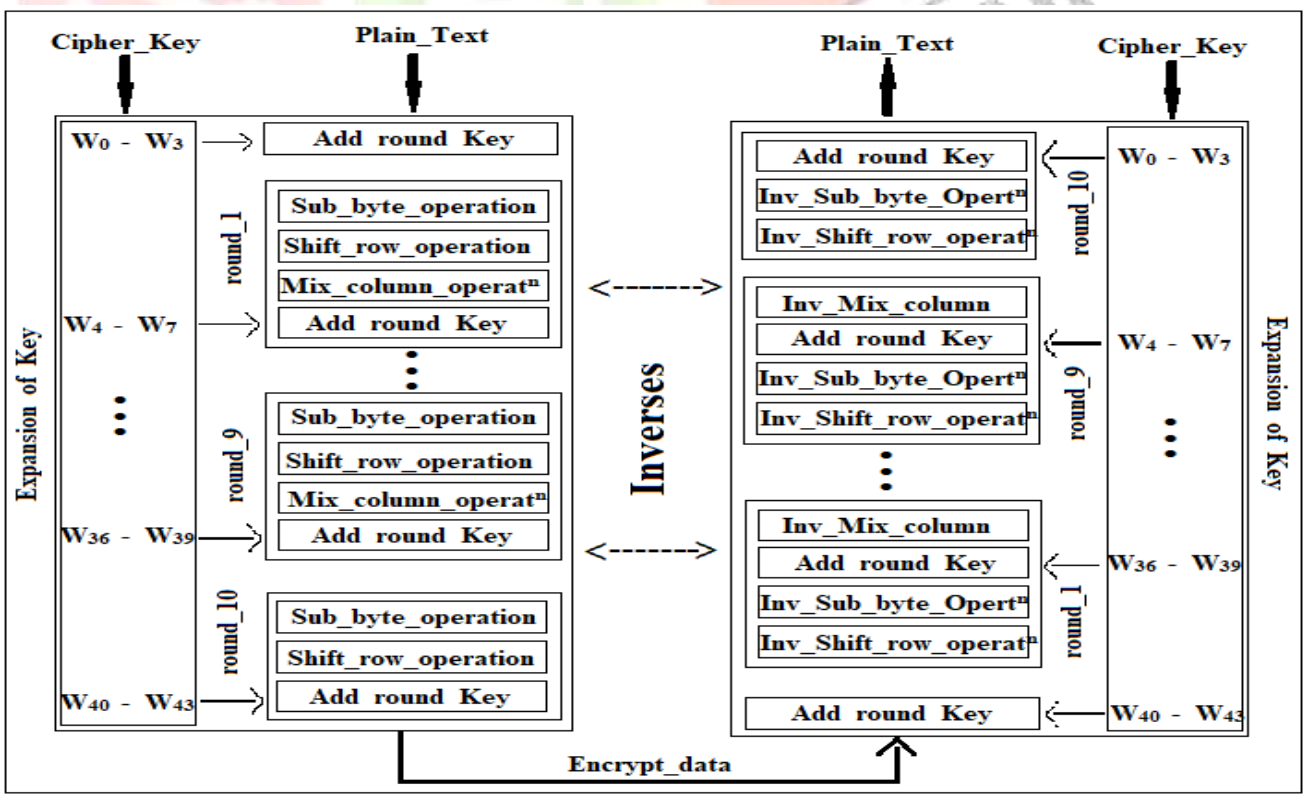

Fig 4.2: Block Diagram of AES

4.3 THE SUB-BYTES OPERATION

Sub bytes transformation is actualized utilizing S-Box. The S-Box is a standout amongst the most tedious procedure since it is required in each round. In substitute byte operation each element in the input state is mapped to an element in the Substitution box. The leftmost 4 bits are used to represent the rows and the rightmost 4 bits are used to represent the columns. This row and column value act as the indexes to the S-box. S-box is a 16x16 matrix which is fixed for an AES algorithm. There is a total of sixteen distinct byte to byte transformations. During the decryption phase inverse substitute byte is carried out by using the inverse S-box.

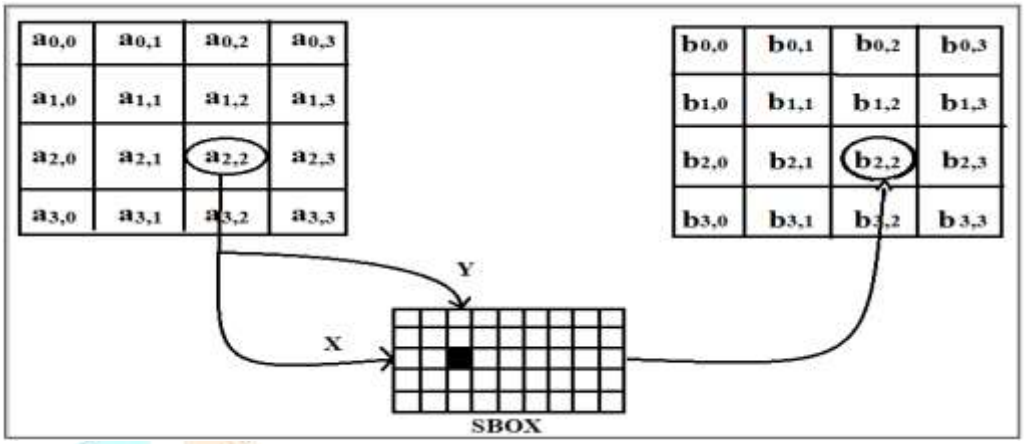

Fig 4.3: The Sub-Bytes Operation

4.4 SHIFT ROW OPERATION

In this operation, each row of the state is cyclically shifted to the left, depending on the row index. The 1st row is shifted 0 positions to the left. The 2nd row is shifted 1 position to the left. The 3rd row is shifted 2 positions to the left. The 4th row is shifted 3 positions to the left.

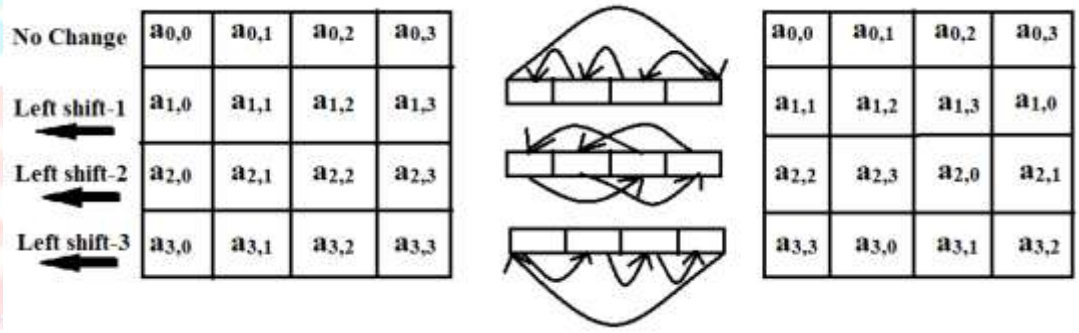

Fig 4.4: Shift Row Operation

4.5 MIX COLUM OPERATION

The Mix Column function operates by taking four bytes as input and it outputs four bytes. Here each of the input byte affects all the four bytes of the output. A fixed matrix is used to transform the state. Each column is considered here as a four term polynomial. The columns are considered as polynomials over GF (2^8) and multiplied modulo (x^4)+ 1 with a fixed polynomial $A(x) = \{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$.

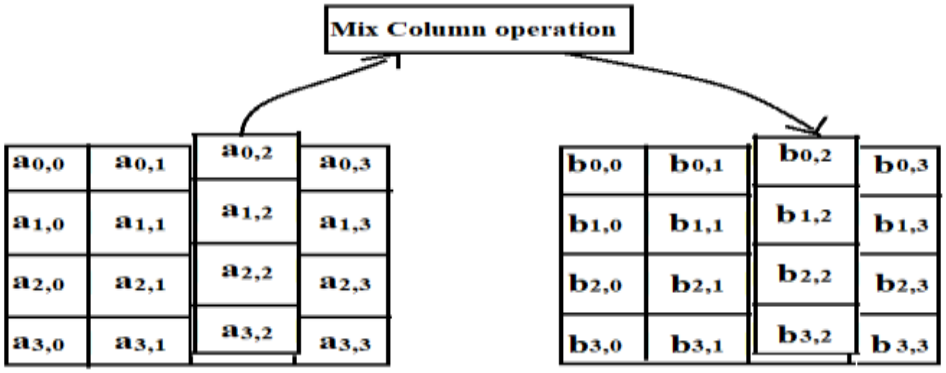

Fig 4.5: Mix Column Operation

4.6 ADD ROUND KEY OPERATION

The primary function of Add Round Key Operation is to associate key expander output generated by key generator Circuit to the AES algorithm. In this operation, a Round Key is applied to the state by a simple bitwise XOR. The Round Key is derived from the Cipher Key by the means of the key schedule. The Round Key length is equal to the block key length (=16 bytes).

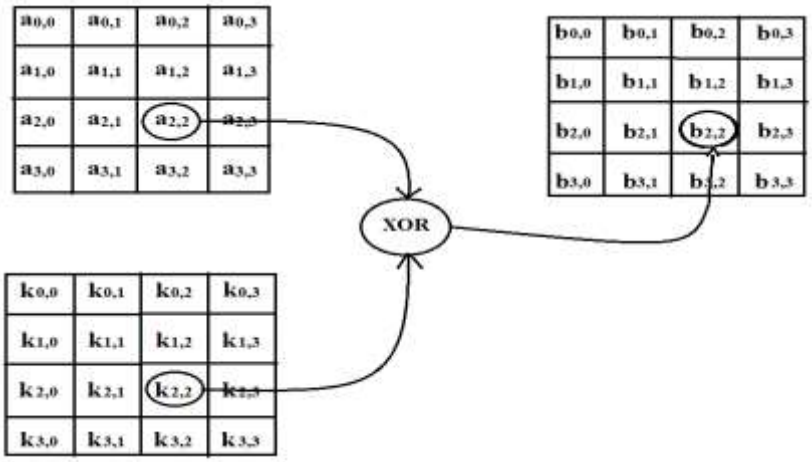

Fig 4.6: Add Round Key Operation

4.8 FAULT DETECTION IN AES

The secret information from the cryptographic system is being extracted with the introduction of different types of attacks. These may result in loss of confidential and secure data. Due to these problems fault detection technique must be employed within the cryptographic system.

The faults can be of varying nature but can be categorized as follows:

1. **Bit Model**: This fault model assumes that the faults is localized to one bit. The fault control is crucial here, as there is a high probability that a random fluctuation of the operating conditions can lead to more than one bit getting affected. Hence attacks based on such models are often unrealistic and may not be practically viable.

2. **Single Byte**: A more practical and most common fault model is the single byte model. This fault model assumes that the faults are spread to bytes and the fault model can be any random non-zero value. This non-specificity of the fault value makes these types of DFAs very powerful and practical techniques.

3. **Multiple Byte**: In this fault model, it is assumed that the faults propagate to more than 1 byte. More often, these models are more practical, in the sense that the DFAs based on them work even with lesser fault control. In context to DFA of AES, we shall observe a special fault model, namely the Diagonal Fault Model which helps to generalize the DFA of AES to a large extent. The fault values are again arbitrary, and hence makes these attacks very powerful.

V. OUTCOMES OF PROJECT

This project presents the encryption and decryption of AES with fault detection mechanism in AES algorithm. Faults may be introduced intentionally so as to extract the secret information. Here we have initially implemented AES-128 bit using GF (2^8) multiplication. The key size used here is also 128 bits.

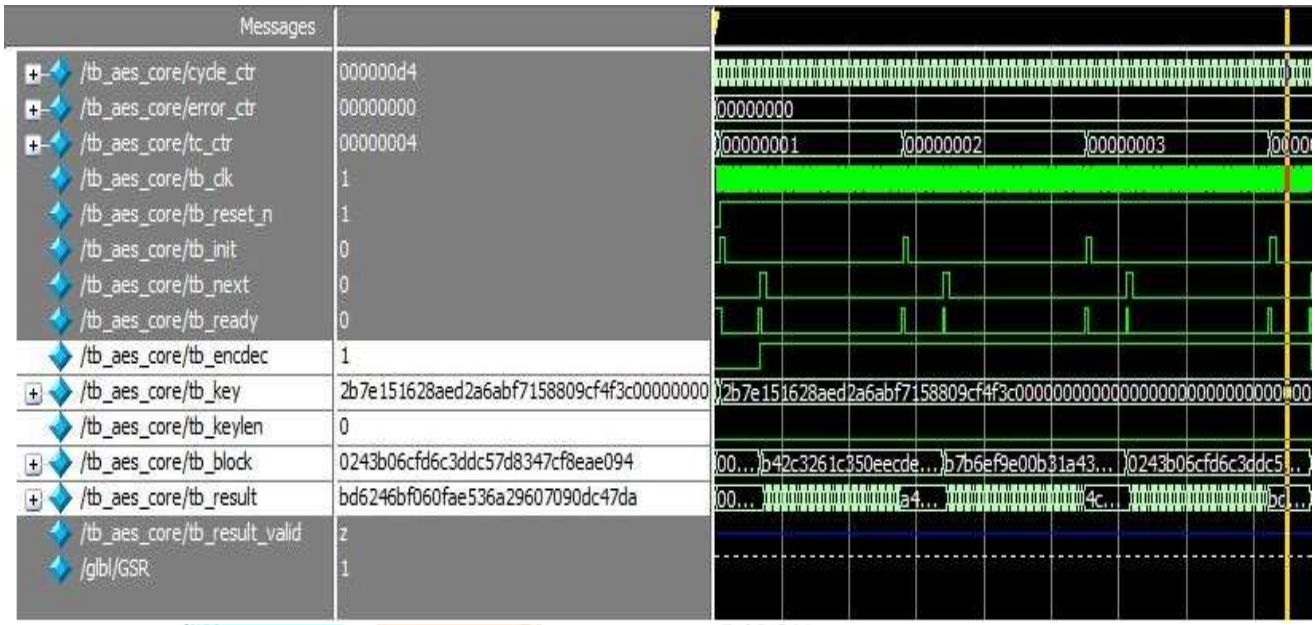

Fig.5.1: Encryption Output without Faults

The fig 5.1 and 5.2 both shows the implementation of encryption and decryption of AES simulation results with fault detection method embedded into the algorithm for enhanced security. Here fault is not introduced into the message (Plain Text). The fault detection is done in such a way that that the result of encrypted value and the known expected value will be compared, if the result is different from each other the fault is detected or else there is no fault.

The fig.5.3 and 5.4 shows the fault detection which is done in the AES algorithm. Here we have intentionally injected fault in the input side. Then the encrypted value and the known expected value will be different from each other so the result is faulty.

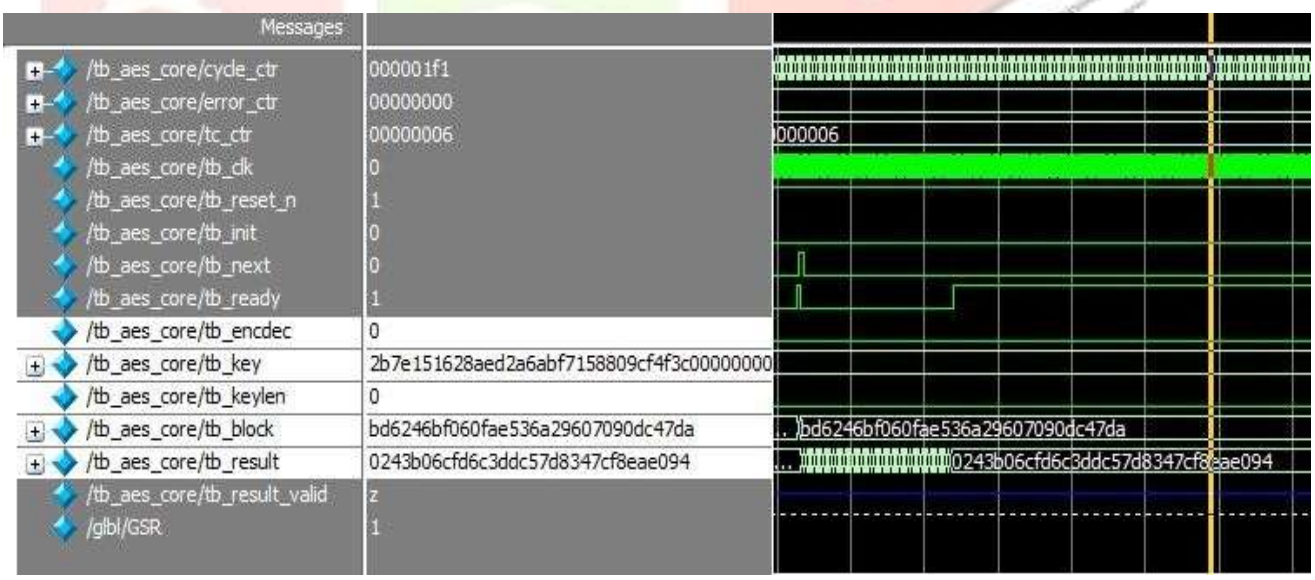

Fig.5.2: Decryption Output without Faults

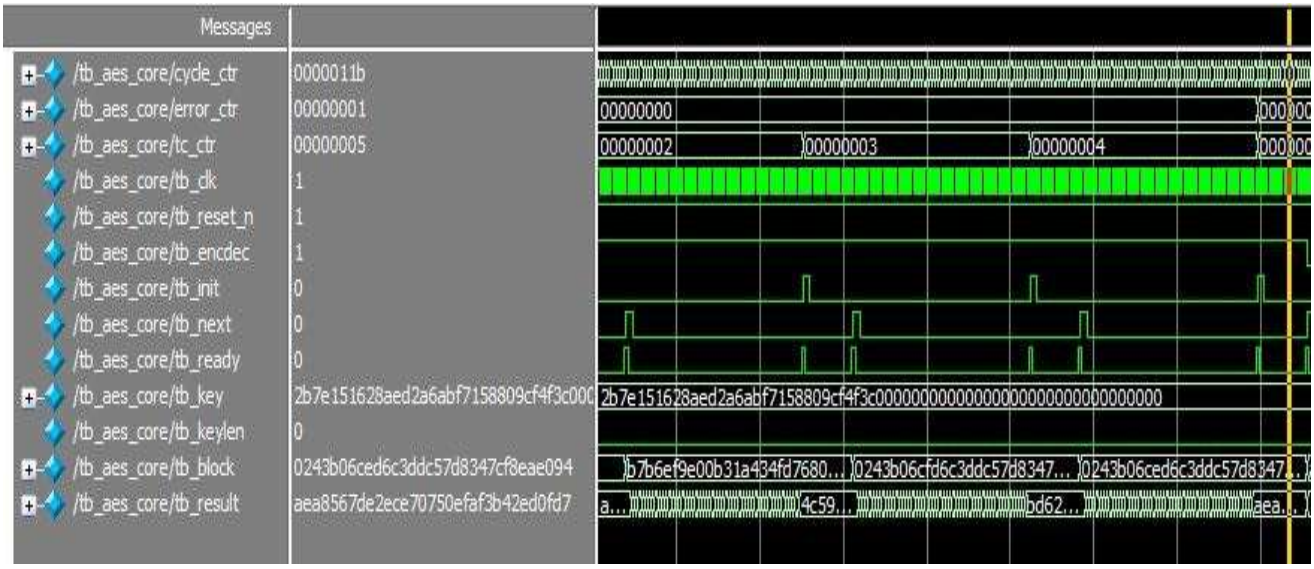

Fig.5.3: Encryption Output with Faults

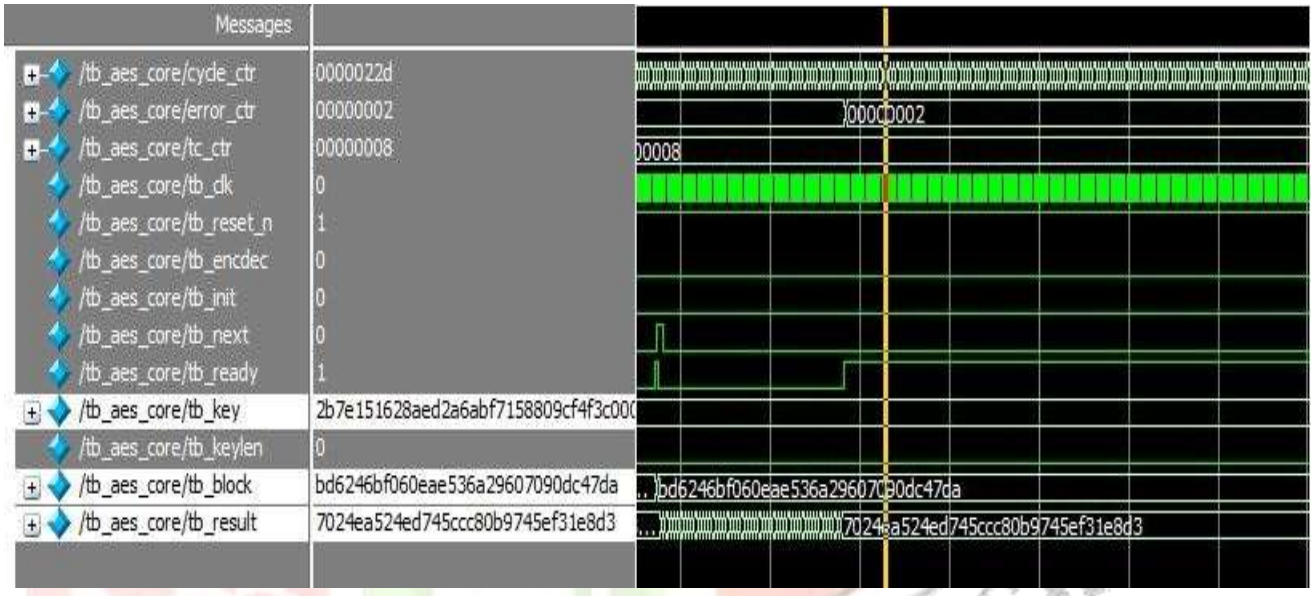

Fig.5.4: Decryption Output with Faults

VI. CONCLUSIONS AND FUTURE SCOPE

In this project work novel approaches were used to perform the Galois Field multiplication (2^8) for the mix column stage of AES, which have been elaborated and explained. In these methods, a significant improvisation in area and speed were obtained and also have an efficient Faults detection scheme for AES. Similar types of methodologies could be explored for the other stages of AES as well. Application of these techniques, to other encryption methods such as visual cryptography, could open up a new paradigm into the world of research in the fields of network security and management.

REFERENCES

[1] M. Meena, A. Komathi, " A Study and Comparative Analysis of Cryptographic Algorithms for Various File Formats", International Journal of Science and Research (IJSR), Volume 5 Issue 8, August 2016, pp. 991 – 995

[2] S. Chandra, S. Paira, S. S. Alam and G. Sanyal, "A comparative survey of Symmetric and Asymmetric Key Cryptography," 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, 2014, pp. 83-93

[3] Aleisa, N. "A Comparison of the 3DES and AES Encryption Standards." International Journal of Security and Its Applications", 2015, vol. 9, issue. 7, pp- 241-246.

[4] W. Stallings, "Advanced Encryption Standard" in Cryptography and Network Security: Principles and Practices, 4th ed., Pearson Education, India, 2006, ch. 5, sec. 2, pp. 140-160.

[5] Aleisa, N. "A Comparison of the 3DES and AES Encryption Standards." International Journal of Security and Its Applications", 2015, vol. 9, issue. 7, pp- 241-246.

[6] M. Biglari, E. Qasemi and B. Pourmohseni, "Maestro: A high performance AES encryption/decryption system," The 17th CSI International Symposium on Computer Architecture & Digital Systems (CADS 2013), Tehran, 2013, pp. 145-148.

[7] S. Arrag, A. Hamdoum, A. Tragha, and S. E. Khamlich, "Design and implementation a different architectures of MixColumns in FPGA", International Journal of VLSI design and Communication Systems, Vol. No. 3, Iss. No. 4, 2012, pp. 11-22.

[8] P. Parikh and S. Narkhede, "High performance implementation of mixing of column and inv mixing of column for AES on FPGA," 2016 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), Chennai, 2016, pp. 174-179.

[9] Gawtham G Dath1 Anu Chalil2 Jasmine Joseph3, "An Efficient Fault Detection Scheme for Advanced Encryption Standard" 2018 3rd International Conference on Communication and Electronics Systems (ICCES),Coimbatore, 2013, pp. 235238.

[10] T. K. Jishamol ; K. Rahimunnisa, "Low power and low area design for advanced encryption standard and fault detection scheme for secret communications",2013 International Conference on Communication and Signal Processing,Coimbatore, 2013, pp. 216-219.

[11] Mouna Bedoui ; Hassen Mestiri ; Belgacem Bouallegue ; Mehrez Marzougui ,"An improved and efficient countermeasure against fault attacks for AES", 2017 2nd International Conference on Anti-Cyber Crimes (ICACC),Chennai, 2016, pp. 174-179.