MODIFIED AES APPROACHES IN ENCRYPTION AND DECRYPTION FOR INSECURE ENVIRONMENT

DR.V.DEVARAJAN **Mr.S.NIRESH KUMAR** **JEEVANAND D**
ASSOCIATE PROFESSOR **ASSISTANT PROFESSOR** **STUDENT**
DEPARTMENT OF ECE **DEPARTMENT OF CSE**
DHANALAKSHMI SRINIVASAN COLLEGE OF ENGINEERING AND TECHNOLOGY, CHENNAI

ABSTRACT
The security of video applications such as commercial videos, military videos and others have become an important field of research recently. One of the most secure algorithms is Advanced Encryption Standard (AES) algorithm;however this algorithm is inefficient for dealing with video encryption due to its slowness property. This paper proposes a new modified of AES to make it more suitable for encrypting digital video. The Modification focuses on the slowest transformations in original AES which is mix columns transformations and replace them with new Henon map chaotic based mask and one mix columns transformation. Resulting in a significant reduction in encryption and decryption time and enhance the security level of AES algorithm, and also the key space is increased as observed in the simulation results of proposed system.
Keywords: AES-128, Chaotic mask, Henon map, Sub-Byte, Mix columns

INTRODUCTION

Internet communication is playing the important role to transfer large amount of data in various fields. Some of data might be transmitted through insecure channel from sender to receiver. Different techniques and methods have been using by private and public sectors to protect sensitive data from intruders because of the security of electronic data is crucial issue. Cryptography is one of the most significant and popular techniques to secure the data from attackers by using two vital processes that are Encryption and Decryption. Encryption is the process of encoding Data to prevent it from intruders to read the original data easily.

Modern cryptography provides the confidentiality, integrity, no repudiation and authentication. These days, there are a number of algorithms have been available to encrypt and decrypt sensitive data which are typically divided into three types.

[1] present MAES, a lightweight version of Advanced Encryption Standard (AES) which meets the demand. Efficiency rate of MAES is around 18.35% in terms of packet transmission which indicates MAES consumes less energy than AES and it is applicable for Resource Constraint Environments. There are very less powered and experiment cost

of challenges in usage communication medium. The [2] proposes for a modified version of the AES algorithm using multiple S-boxes. Based on simulation testing conducted, it was found out that the modified AES algorithm using multiple S-Boxes has better speed performance compared to the original cipher. However, when tested using the avalanche effect, the changes in the output bits were below the minimum expected rate. Here multiple s-box is generated so number of hardware increased and the less power consumption

In [3] initially the optimization was mainly on area and power consumption, but, nowadays the attention is more on the energy consumption. In this paper, for the first time, we look at energy consumption of lightweight block ciphers implemented in reconfigurable devices, and we analyze the effects that round unrolling might have on the energy consumed during the encryption. In exploring the energy consumption of light weight block cipher in FPGA is that more energy consumption and number of parallel encryption varies in each algorithm and the amount of unrolled rounds also high.

Security is always a major concern in the field of communication. In [4] Advanced Encryption Standard (AES) and RSA algorithms are the two popular encryption schemes that guarantee confidentiality and authenticity over an insecure communication channel. It also includes several computational issues as well as the analysis of AES and RSA security aspects against different kinds of attacks including the countermeasures against these attacks.Performance of security issue AES and RSA cryptography it includes several computational issues as well as the analysis of AES and RSA security aspects against different kinds of including the counter measures against their attacks, data security is low.

Data transferred in an electronic way is vulnerable to attacks. With an aim to protect data for secure communication, [5] a new Hybrid non-pipelined Advanced Encryption Standard (AES) algorithm based on traditional AES algorithm with enhanced security features is proposed in this work. The design is synthesized on various Field Programmable Gate Array (FPGA) device and compare to the existing designs resulting in significant improvement in throughput. The proposed design is implemented on Spartan6 FPGA device.

2. EXISTING SYSTEM

The Advanced Encryption Standard (AES), a symmetric key block which is published by the National Institute of Standards and Technology (NIST). It is a non-Festal block cipher that encrypts and decrypts a fixed data block of 128-bits. There are three different key lengths. The encryption or decryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

AES performs several rounds where each round is made of several stages. A data block is transformed from one stage to another. Before and after each stage, the data block is referred to as a state. Each round, except the last, performs four transformations which are invertible. The last round implements the rest three transformations except the Mix Columns stage.

2.1. EXPLANATION

2.1.1. SUB BYTES

In the Sub Bytes step, each byte in the matrix is updated using an 8-bit substitution box, the Rijndael S-box. This operation provides the non-linearity in. The S-box used is derived from the multiplicative inverse over GF (2^8), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen to avoid any fixed points (and so is a derangement), and also any opposite fixed points.

2.1.2. SHIFT ROW

The Shift Rows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively.

2.1.3. MIX COLUMN

During this operation, each column is multiplied by the known matrix that for the 128-bit key. The multiplication operation is defined as: multiplication by 1 means no change, multiply by 2 means shifting to the left, and multiplication by 3 means shifting to the left and then performing XOR with the initial un shifted value. After shifting, a conditional XOR with 0x1B should be performed if the shifted value larger than0xFF.

2.1.4 ADD ROUND KEY

In the Add Round Key step, the sub-key is combined with the state. For each round, a sub-key is derived from the main key using Rijindael key schedule; each sub-key is the same size as the state. The sub-key is added by combining each byte of the state with the corresponding byte of the sub-key using bitwise XOR

2.2. PROBLEMS IN EXISTING SYSTEM:

1. S-Box in AES consumes more time and more area

2. Replacement of S-Box value with 256 different possibilities is difficult.

3.PROPOSED SYSTEM

3.1 NEW S-BOX ALGORITHM:

According to previous research observation, we have found out that S-Box and Mix Columns are the most energy consuming stages in encryption and decryption process. We have analyzed the S-Box generation process of the Rijndael AES. The 16x16 2-dimensional lookup tables are formed through the multiplicative inverse phase and affine transformation phase in the original AES. We are proposing a new 1-dimensional lookup table as S-Box. It also follows the same generation process as the original one. However, substitution of one complete byte requires two times substitution from the S-Box. First four bits of the state byte is replaced first then there four bits are substituted from the S-Box.

3.1.1. Rijndael S-Box Generation Method

The Rijndael S-Box is a square matrix which is used in the Rijndael cipher. The S-Box serves as a lookup table. It is generated by determining the multiplicative inverse for a given number in GF (2^8) and then transforming the multiplicative inverse using affine transformation.

1) Multiplicative Inverse Phase: In multiplicative inverse phase, the input byte is inversed by substituting value from multiplicative inverse table.

2) Affine Transformation: Selection of the irreducible polynomial and the designated byte are the two most important factors of affine transformation phase. In RijndaelAES,**x^8 + x^4 + x^3 + x + 1** is used. Basically, the affine transformation consists of two operations. Firstly, 8x8 square matrix's multiplication and secondly, 8x1 constant column matrix addition .

3.1.2. Modified AES S-Box Generation

Our modified AES S-Box generation process follows the construction procedure of the original AES. The whole process differs only in the selection of the irreducible polynomial and specially designated byte.

1) Multiplicative Inverse Table: In the Rijndael AES, all the arithmetic operations are performed over the Galois Field (2^8). In our work, the Galois Field (2^4) is considered. The number of irreducible polynomials of degree 4 over GF (2) are x^4 + x + 1, x^4+x^3+x^2+x+1 and x^4 + x^3+1. All the generated values of the multiplicative inverse table and substitution box depend on the selection of irreducible polynomial. Following the Extended Euclidean Algorithm, 1-dimensional multiplicative inverse table is formed. Figure illustrates the multiplicative inverse table of the proposed algorithm.

2) Affine Transformation: This affine transformation process also follows two phases. Firstly, 4x4 square matrix's multiplication and secondly, 4x1 constant column matrix addition.

4. RESULT

4.1. TOP MODULE:

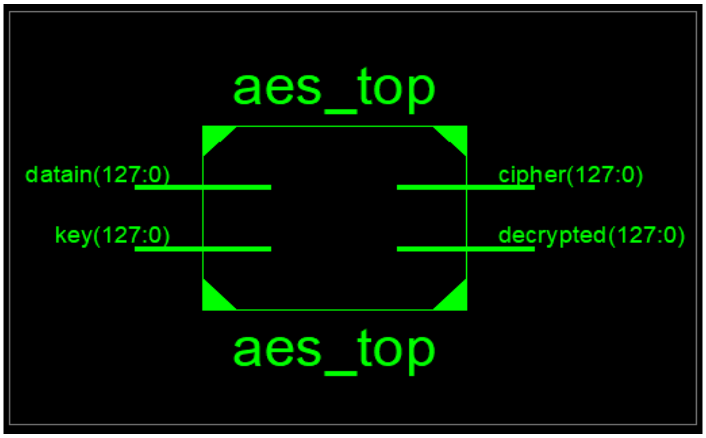


Fig.3.4.Top level

4.2. RTL SCHEMATIC:

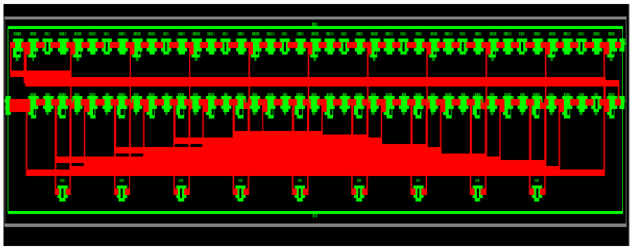
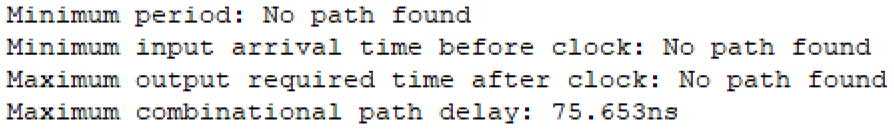


FIG3.5.RTL SCHEMATIC

4.3. TIMING ANALYSIS:



```
Minimum period: No path found
Minimum input arrival time before clock: No path found
Maximum output required time after clock: No path found
Maximum combinational path delay: 75.653ns
```

4.4. OUTPUT WAVEFORM OF PROPOSED SYSTEM:

	EXSTING SYSTEM	PROPOSED SYSTEM
Number of slice LUTs	18969	8740

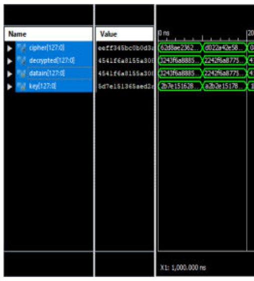


FIG 3.6 Output waveform of proposed system

In MAES algorithm is highly efficient and source when compared to AES algorithm. The number of hardware used in AES is reduced by modified S-Box and mix column used in AES algorithm so, the data security is improved and the hardware is reduced.

5. CONCLUSION

In this paper, we present a modified version of AES for Resource-Constraint Environments. A new Substitution Box is proposed which works over the Galois Field (2^4) by constructing a unique affine transformation equation. One notable feature of MAES is extending the battery life of low powered devices by consuming less amount of energy. In future, the security issue and space complexity will be considered to make the proposed modification more applicable. Also, we plan to investigate multipath routing scheme while transmitting the encrypted data to the sink node. We will further delve to integrate Public Key Cryptosystem, especially Elliptic-Curve cryptography (ECC) to achieve comparable efficiency in terms of number of packet transmission and latency with better security.

REFERENCES

[1] [Chunking Sun. Application of RFID Technology for Logistics on Internet of Things [J]. AASRI Proscenia, 2012(1):106 – 111.

[2] AlmudenaD´ıaz-Zayas, Cesar A. Garc´ıa-Pe´rez, A´ largo M.Recio-Pe´rez. 3 GPP standards to deliver LTE connectivity for IOT [C]. 2016 IEEE First International Conference on Internet-of-Things Design and Implementation
(IOTDI), 2016, 283-288.

[3] Wang Ying. Improvement of Mix Column () function in advanced encryption standard AES [D]. Shaanxi Normal University, 2011.

[4] Christ of Pear, Jan Pell. Exploring cryptography in depth -Principles and applications of commonly used encryption techniques [M]. Beijing: Tsinghai UniversityPress,2012.51-111.

[5] Mary James, Deeps S Kumar. An Implementation of Modified Lightweight Advanced Encryption Standartion FPGA [J].ProcediaTechnology, 2016(25):582–589.

[6] Xiao Xiaocao, Li Shogun. An Expression Method of S-Box and Inverse S-Box Replacement in AES Algorithm [J] Microelectronics Computer, 2014, 31(1):112-115.

[7] Mo Xinhua. Research on an encryption algorithm for WSN data security [D].Zhejiang University of Technology, 2010.

[8] Montalba Alidade, Wan Hassling Hassan, Mazda Zama, et al .Implementation and Evaluation of Lightweight Encryption Algorithms Suitable for RFID