International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Modified Encryption Standard with High Performance through Secure Protocol

M L N Swamy, B S Sridevi

Abstract: ***The Advanced Encryption Standard (AES) has been accepted worldwide as a desirable algorithm to encryption and decryption sensitive information. In cryptography the unencrypted information referrers to as plaintext it is encrypted into cipher-text, which will in turn be decrypted back into the usable plaintext. The encryption and decryption are based on the type of cryptography system and secret keys. The secret key is responsible for preparing the input key to be used by the cipher in each round. AES with one-stage pipeline producing minor reduction of delay but does not show any improvement in area and power consumption. To overcome the above drawbacks, the basic architecture of AES, which includes encryption and decryption can be modified with one stage pipeline architecture by using one- dimensional Substitute Box (SBOX). Advanced Microcontroller Bus Architecture (AMBA) describes level of an on-chip communication standards for elevated performance embedded microcontrollers. AMBA AHB (Advanced High Performance Bus) is intended for elevated performance and high-frequency clocks. AHB has unique characteristics such as burst transfer, split transaction and single-cycle master bus transfer. 128 bit plain text is guided by AMBA-AHB requirements and can be used to send a plain text block to the cypher per clock cycle.. Plain text of 128 bit is driven by AMBA-Advanced High-performance Bus. AMBA-AHB specifications and supports the transmission to the cipher of a plain text block per clock cycle i.e., Modified Encryption Standard will be implemented with AMBA –AHB driven by input, which provides on-chip communication, increasing security of encryption standard. Propositioning methodology, Modified Encryption Standard will be simulated and synthesized by using Xilinx ISim 14.7 FPGA.***

Keywords-Cryptography, AES (Encryption &decryption), MAES, AMBA-AHB, Pipe-lining.

I. INTRODUCTION

The Advanced Encryption Standard (AES) was the result of an effort launched by the National Institute of Standards and Technology. Originally, AES was intended to protect sensit ive data in government organizations in the United States.A ccording to the research observation of the AES,

it is observed that the Substitutional -Box (S-Box) and Mix-Columns are the more space occupying phases of encryption and decryption process We evaluated the Rijndael Advanced Encryption Standard's S-

Box generation method.The twodimensional 16x16 look up table is created in the initial AES through the multiplicat ive inverse and affine transformation stage.It proposes as S-Box a unique one-dimensional lookup table.

It also uses the same process of generation as the initial method. However, to replace the entire byte, the S-Box needs to replace it twice. First, substitute the 4 bits of the state byte and then extract the remaining 4 bits of the approach to generating S-Box Rijndel S-Box. The Rijndel S-Box is a rectangular matrix used as a lookup table in the Rijndael block cipher. It is produced by using affine transformation to determine t he multiplicative inverse for a specified amount in GF(2^8) and then transform the multiplicative inverse. AES is regarded one of the strongest and most efficient algorithms in terms of the security aspect and the complexity of execution. Despite that the secret key allocation is still regarded as a critical problem, like other symmetric encryption algorithms. Again, a single block (128-bits) of information needs to be encrypted or decrypted, an important quantity of computational processing that occupies less area and producing less delay.

The impact of the proposed work can be explained as follows:

The existing AES, which includes encryption and decryption can be modified with one stage pipeline architecture by using one dimensional Substitute Box (S-BOX). One-Dimensional Substitution Box (S-Box) created by formulate a new equation for the construction of a square matrix in the Modified-AES transformation stage. Modified Advanced Encryption Standard (MAES) implemented with AMBA –AHB. After analyzing the results of our experiment we conclude that MES is well effective in terms of area and delay than AES.

II. RELATED WORK

A lot of research work has been done in latest years, and many famous scientists have achieved important results in terms of high-performance algorithms. However, most of them focus on optimization of area and delay as their respective aspects and are hardware-oriented. [1]

Manuscript published on November 30, 2019.
* Correspondence Author
M L N Swamy*, M.Tech in VLSI Design Department of ECE M.Tech student Aditya Engineering College Surempalem, India E-mail: swamy121993@gmail.com
B S Sridevi M.Tech, (Ph.D.) Department of ECE Associate professor Surempalem, IndiaE-mail: sridevibaddireddy@aec.edu.in

The Advanced Encryption Standard (AES), a symmetrical k ey block released in December 2001 by the National Institut e of Standards and Technology (NIST) 2001.
[2]In addition, it has been shown that the maximum area occupying the circuit during encryption method has approximately an algebraic relationship with the extent of unrolling, and that the majority of the area occupying the part is a 2-round unrolled Substitution Box (S-Box). In [3] and [4] the development of the AES has been suggested and fundamental changes (such as the Substitutional Box) are targeted at a reduced area and a less delay. Most of the applications are hardware-oriented. In [5], a comparative analysis of various area-based algorithms and hardware complexity was provided and state-of - the-art methods were implemented to reduce delay and area. In [6] a research investigated on reduce the hardware complexity and delay in different newly developed lightweight variants of block ciphers consider feasible optimizations for a non-linear transformations. Detailed in [7], Advanced Encryption Standard research. Two Substitution Boxes have been proposed.
In [8]study the 1st S-Box is the Rijndel S-Box and the 2nd S-Box that replaces the Mix Columns procedure of the original AES, the XOR operation and an affine transformation are constructed. It is discovered that the altered AES algorithm using various S-box's enhanced speed performance compared to the initial cipher. In [9], a modified AES was proposed using state-of - the-art methods to reduce the computational operating costs of the original AES algorithm by encrypting large-scale data such as multimedia data. In [10] "Modified Advanced Encryption Standards." International Journals of Soft Computing and Engineering.

III. PRELIMINARIES

The
Advanced Encryption Standard (AES), a symmetric key
Block released in December 2001 by the National Institute o f Standards and Technology (NIST).
It is a block cipher that encrypts and decrypts a 128-bit information block set. There are three distinct primary lengths available. It gives 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Decryption consists of 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. AES carries out many rounds where there are several phases in each round. A block of information is converted from one point to the next. The block of information is referred to as a state before and after each phase. Each round carries out four transformations, except the last one. The last round uses the remaining three transformations except the phase of the mix columns.

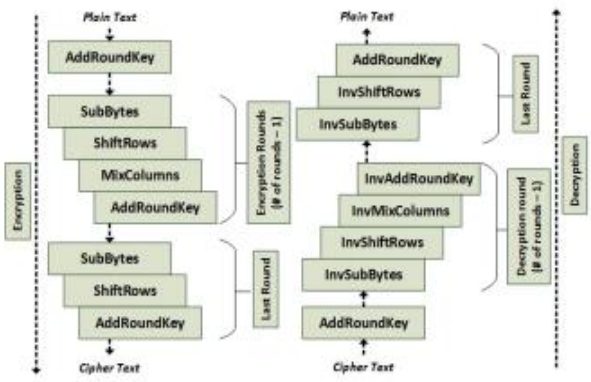

Fig. 1. AES basic encryption and decryption design

4 stages of each round have:

Substitute Bytes: Only encryption sites use the first transformation, Sub Bytes. All of the state's sixteen (16) bits are replaced by the respective numbers from the lookup table.

Inverse sub bytes are used for decryption. Bytes of a state are replaced from the list of Inverse Sub Bytes.

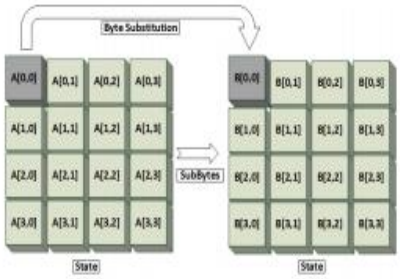

Fig. 2. Sub Bytes

Shift Rows: In the encryption process, the states bytes are rotational left shifted in each row. The number of changes is based on the number of rows of the state matrix (0, 1, 2 or 3). Row 0 bytes is not moved and row 1, 2, 3 is moved to 1, 2, 3 bytes. Row 0 bytes is not moved.

Fig. 3. Shift Rows

MixColumns:

The conversion of the mix columns works at the stage of th e column. It converts every state column into a fresh column. The transformation is in fact a steady square matrix multiplications of a state column. All arithmetic operations are carried out in the Galois Field. The bytes are regarded as polynomials rather than numerals.

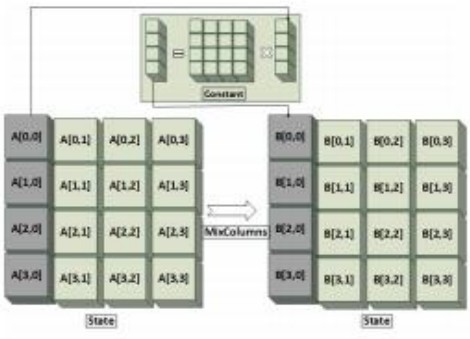

Fig. 4. Mix Columns

Add Round Key Add Round Key at a moment precedes one column. In this regard, it is comparable to mixing columns. Add Round Key to each column matrix adds a round keyword. In the Add Round Key stage, the matrix addition procedure is conducted. Figure 5 demonstrates the procedure of the Add Round Key.

In encryption, Sub Bytes, Shift Rows, Mix Column and Add Round Key are used in all rounds except the final round.

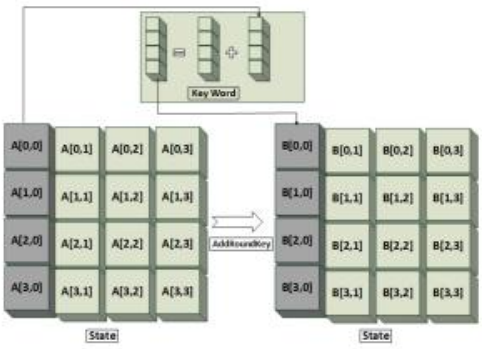

Fig. 5. Add Round Key

The conversion process of Mix Columns is not carried out in the final round of encryption.

The decryption method mainly performs the same procedures as the algorithm, in addition to the 9 steps of Inverse Shift Rows, Inverse Sub Bytes Inverse Add Round Key and Inverse Mix Columns Transformation, the decryption method mainly uses the same structure as the encryption algorithm. In the last round, the Inverse-Mix Column did not performed.

IV. MODIFIED-ADVANCED ENCRYPTION STANDARD

According to previous research studies, it have been observed that S-Box and Mix Columns are the more complex hardware and consume more delay and area in the encryption and decryption methods. We have examined the Rijndael AES S-Box generation method.. The 2-dimensional 16x16 lookup tables are created in the initial AES through the multiplicative reverse stage and affine transformation phase. We are putting forward as S-Box a fresh1-dimensional lookup table. It also uses the same generation technique as the initial one. However, replacing a complete byte requires changing the S-Box twice. First remove four elements of the state byte first then add the S-Box's remaining four bits.

S-Box Generation Methods:

The S-Box is used as a lookup table. It is created using the affine method to evaluate the multiplicative inverse for the given amount in GF (28) and then transform the multiplicative inverse.1) The multiplicative inverse phase: the input byte is reflected in the multiplicative inverse table by changing the value.2) Affine transformation: the selection of the irreducible polynomial and the assigned byte are the two main variables in the stage of affine transformation. In AES Rijndael, Fig. six, Generation of initial S-Box Modified AES S-Box Generation Our modified S-Box AES,

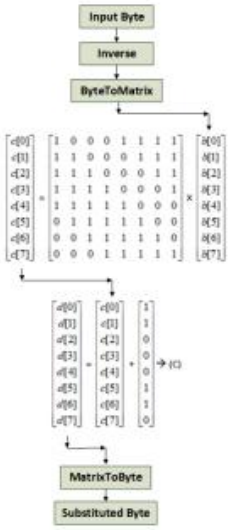

Fig. 6. S-Box generation process

Modified AES S-Box Generation

The altered AES S-Box generation technique follows the initial AES building process. In choosing the irreducible polynomial and one-dimensional S-Box, the entire method differs only. 1) Multiplicative Inverse Table: All arithmetic operations on the Galois Field (28) are conducted in the Rijndael AES. The Galois Field (24) is being regarded in our job. The number of degree 4 irreducible polynomials over GF (2)

$$x^4 + x + 1,\ x^4 + x^3 + x^2 + x + 1 \text{ and } x^4 + x^3 + 1.$$

the selection of irreducible polynomial relies on all the multiplicative inverse table and replacement box values generated. For our experimental purpose, it select x 4+x+1 as our irreducible vector, but it can choose any of the above described irreducible polynomials. The 1-dimensional multiplicative inverse table is developed by the Extended Euclidean Algorithms.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	9	E	D	A	7	6	F	2	C	5	A	4	3	8

Fig. 7. Multiplicative inverse table

2) Affine transformation: two stages also follow this affine transformation method. First, the multiplication of the 4x4 s

quare matrix and second, the addition of the 4x1 continuous column matrix matrix. Following equation 1 the 4x4 square matrix is built and equation 2 relates to the di value

$$d_i = b_i \oplus b_{(i+2)\%4} \oplus b_{(i+3)\%4} \oplus C_i$$

$$C_i = i^{th}\ bit\ of\ a\ specially\ designated\ byte\ which\ is\ hexadecimal\ of\ 3, 8, 10, 13, 15\ as\ they\ don't\ generate\ any\ fixed\ points.$$

Since we calculate over the GF (24) where the continuous columns matrix value ranges from 0x00 to 0x0F, it can pick 5 values from 3 because after conversion these values don't produce a fixed point. The fixed point referred to the value of the product produced just like the price of the entry. Figure 8 shows the proposed MAES generation process.

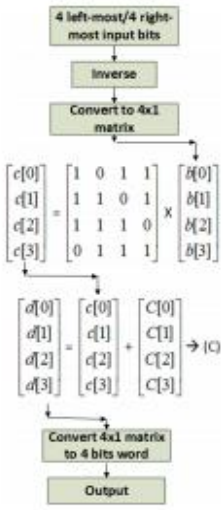

Fig. 8. Proposed Modified AES S-Box generation method

Several S-Boxes and inverse S-Boxes are shown below from figure 9 to 13 for distinct values of steady quality C:

Case-1: When C = 0x03

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3	4	F	B	2	1	7	0	C	D	5	9	6	E	A	8

Inverse S-box:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
7	5	4	0	1	A	C	6	F	B	E	3	8	9	D	2

Fig. 9. Case-1: When C = 0x03

Case-2: When C = 0x08

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
8	F	4	0	9	A	C	B	7	6	E	2	D	5	1	3

Inverse S-box:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3	E	B	F	2	D	9	8	0	4	5	7	6	C	A	1

Fig. 10. Case-2: When C = 0x08

V. PERFORMANCE ANALYSIS

It have gone through different cases S-Boxs are available, to evaluate our experiment.

Case-3: When C = 0x0A

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
A	D	6	2	B	8	E	9	5	4	C	0	F	7	3	1

Inverse S-box:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
B	F	3	E	9	8	2	D	5	7	0	4	A	1	6	C

Fig.11. Case-3: When C = 0x0A

Case-4: When C = 0x0D

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
D	A	1	5	C	F	9	E	2	3	B	7	8	0	4	6

Inverse S-box:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
D	2	8	9	E	3	F	B	C	6	1	A	4	0	7	5

Fig. 12. Case-4: When C = 0x0D

Case-5: When C = 0x0F

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
F	8	3	7	E	D	B	C	0	1	9	5	A	2	6	4

Inverse S-box:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
8	9	D	2	F	B	E	3	1	A	C	6	7	5	4	0

Fig. 13. Case-5: When C = 0x0F

Implementation

As it's suggest a lightweight version of AES for elevated efficiency, first assess the existing AES method and implement AES in a structured programming language before applying it in MES. The same technique is pursued for the suggested modified AES. Both algorithms (AES and MES) have been introduced in a single-stage pipeline architecture. It can be implement the original AES in a single-stage pipeline architecture in the first phase and generate two sets of data packets that have been transferred. The first information set is based on the transmission of encrypted information packets using the initial AES encrypted methods, while the second information set consists of unencrypted information packets. In the second phase, both the original AES and the proposed modified AES are implemented in a single-stage pipeline input (i.e. plain text) driven by AMBA-AHB.

VI. AMBA INTERFACE

Wrappers that can be added to the suggested AES architectures have introduced the AMBA AHB interface. Wrappers have 32-bit data path (HRDATA and HWDATA buses in AMBA) for fundamental and compact architectures. 128-bit buses have been introduced for the pipeline. The AMBA AHB specification accepts this bus width and promotes sending a plain text block to the cipher per clock cycle If the architecture of the pipeline uses smaller information routes, its peak output can never be achieved. AHB Master sends information (plain text and secret key) to the cipher by registers.

These registers must be written in a specific order by AHB Master in 32-bit data path wrappers as the data is transferred to AES cipher once the least significant word register is written. HREADYOUT signal is sets to a low value in basic architectures while encryption or key expansion processes are performed on, indicating that new information or data can't be obtained.

Due to its pipeline structure, which simultaneously encrypts different information, HREADYOUT is placed at a low cost in pipeline architecture only while conducting significant design procedures. The 2 architectures store the resulting cipher text in registers after the encryption process (four basic and compact 32-bit registers and one 128-bit pipeline register). Before writing a new cipher text section, the AHB Master should read these registers. Since AMBA AHB Master is unable to write and read Slaves at the same moment, storing cipher blocks of text in a FIFO or Other memory structures may be critical to avoid data loss in order to obtain complete pipeline latency.

Comparison of parameters

DELAY_COMPARISION	WITHOUT_AHB	WITH_AHB_PIPELINE
AES	10.371ns	9.30ns
MAES	8.85ns	7.704ns

AREA_COMPARISION	WITHOUT_AHB	WITH_AHB_PIPELINE
AES	8 /8672 (0%)	33662/8672 (388%)
MAES	6896/8672(79%)	6614/8672(76%)

AES(with_AHB) vs MAES(with_AHB)

AES: Advanced Encryption Standard
MAES: Modified Advanced Encryption Standard
Modified Encryption Standard shows an improved results when compared to Existing AES

VII. CONCLUSION & FUTURE WORK

In that research work, we presents proposed architecture of Modified Encryption Standard (MES)for High performance, a new Substitution Box is proposed which works over the Galois Field (2^4) by constructing an unique affine transformations equations. One notable feature of Modified Encryption Standard is, occupied less area and reduces the delay. The proposed method shows efficient area and delay when compare to existing Advanced Encryption Standard. MAES driven by AMBA-AHB, provide on-chip communication, increasing security of encryption standard. In future scope will further increase security by increasing the key size and further delve to integrate mixing of Symmetric and Asymmetric key Cryptosystem.

ACKNOWLEDGMENT

The researchers of this paper are highly grateful to independent reviewers for their strict condemnation of this work, which helps the writers to reorganize the work in excellence.

REFERENCES

1. Daemenn, Joan and Rijmens, Vinceent. "The design of Rijndel AES-the advanced encryption standards." Springers Science & Business Media, 2013.
2. Banek, Subhadeeps, Andrey Bogdanoov, and Francesco Regazzoni. "Exploring energy efficiency of lightweight block ciphers." International Conference on Selected Areas in Cryptography. Springer, Cham, 2015.
3. Feldhofer, Martinn, Johannes Wolkerstorfer, and Vinceent Rijmans. "AES implementations on a grain of sande." IEE Proceeding's-sInformation of Security 154, no. 1 (2005): p.14-21
4. Moradis, Ameir, Axel Poschmsan, San Ling, Christoof Parr, and Huaxiongs Wang. "sPushing the limits: a very compact and a threshold implementation of AES." In Eurocryption, vol. 6631, pp. 65-90. 2011
5. Kerckhofs, Stphaniee, Franois Durvaunx, Cdric Hocquest, David Bols, and Franois-Xavier Standaerts. "A comparison of lightweight ciphers from the perspective of the region. "Cryptographic Hardware and Embedded Systems CHES 2012: p.376-420..
6. Baatina,Leejles, et al. "Dietarry recommendations for lightweight block ciphers: power and area analysis of recently developed architecture." International Workshop on Radio Frequency Identifier: safety and privacy problems. Berlin,Heidelbberngs, Springer, 2013
7. Konng, Jian Hao, Li-Minns Angs, and Kah Phoeoi Seing. "A detailed survey of present cryptographic symmetric solution for restricted resources and parameters." Journal of Networks and Computer Applications 49 (2015):
8. pdf of AMBA Specifications (Rev 2.0).
9. M. Duboois, Y. Savariae, "A generic AHB bus for implementations, high- speed locally synchronous islands".
10. Yi-Ting Lin, Chienn-Chou Wang, "AMBA AHB bus protocols checker with efficient debugging mechanism", IEEE International Symposium on Huangan Circuits and Systems, Page(s). 928 – 93, 2008.
11. study of "Design and Implementation of superior Master/Slave Memory Controller with Microcontroller Bus design", IEEE International Conference on Instrumentation and Measurement Technology (I2MTC) Proceedings, pp. 10 – 15, May 2014

AUTHORS PROFILE

M L N Swamy M.Tech in VLSI Design Department of ECE M.Tech student Aditya Engineering College Surempalem, India E-mail: swamy121993@gmail.com

B S Sridevi M.Tech, (Ph.D.) Department of ECE Associate professor Surempalem, India
E-mail: sridevibaddireddy@aec.edu.in