ISSN: 2278-4632
Vol-13, Issue-11, November 2023

# MAES: MODIFIED ADVANCED ENCRYPTION STANDARD FOR RESOURCE CONSTRAINT ENVIRONMENTS

[1] G. HARITHA, B. Tech, M.Tech. LALITH ASHISH REDDY MARAM [2], BABU ALAKUNTLA [3],

SAHITHI ALUGALA [4], NARASIMHA DHARMAPURI [5].

[1] ASSISTANT PROFESSOR OF ECE IN MALLA REDDY INSTITUTE OF TECHNOLOGY & SCIENCE, MAISAMMAGUDA, MEDCHAL (M), HYDERABAD-500100, T. S.

[2,3,4,5.] FINALYEAR STUDENTS FROM DEPT OF ECE IN MALLA REDDY INSTITUTE OF TECHNOLOGY & SCIENCE, MAISAMMAGUDA, MEDCHAL (M), HYDERABAD-500100, T. S.

Abstract: Now a day's data hacking is the main issue for cloud computing, protecting a data there are so many methods in that one most usable method is the data Encryption. Process of Encryption is the converting a data into an un readable form using encryption key, encoded version that can only be read with authorized access to the decryption key. This paper presenting a simple, energy and area efficient method for endurance issue in secure resistive main memories. In this method, by employing the random characteristics of the encrypted data encoded by the Advanced Encryption Standard (AES) as well as a rotational shift operation. Random Shifter is simple hardware implementation and energy efficient method. It is considerably smaller than that of other recently proposed methods. Random Shifter technique used for secure memory with other error correction methods. Rand Shifter consumes less power compare to the other techniques, Random Shifter Consisting of Barrel Shifter, Row Verifier, Checker, and Multipliers. As Enhancement to this Paper, designing AES with Pipelining and Random shifter in one System on Chip (SOC). When compared to AES without pipelining technique decrease the power and delay. In this paper discussed about Introduction, Problem definition, Pipe lining AES, and lastly Result. This Paper is implemented using model sim and Xilinx 14.5 version. This project can used in Communication and Networking and protecting a data in memory devices, Wi-Fi (can be used as part of WPA2), Mobile apps (such as WhatsApp and LastPass), Native Processor Support, Libraries in many software development languages, VPN Implementations.

**Index Terms- Advanced Encryption Standard (AES), Memory, Pipe lining.**

## INTRODUCTION:

Network security has three major security goals: confidentiality, availability and message integration between senders and receivers. Many algorithms are available in each of these three

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

goals of security. One of the frequently used security algorithms in block cipher is the AES algorithm [1]. Cryptography is the study of mystery codes, as a rule, it utilizes a cryptographic framework to change a plaintext into cipher text, it can't be open without a key Which is in 4X4 matrix. There are two classes of algorithm in encryption, they are asymmetric key and symmetric key. In an asymmetric key algorithm, the key is different at encryption process and decryption process. some examples are Diffie-hell man, Elliptic curve cryptography (ECC), El Gamal, Digital signal algorithm (DSA), Rivest Shamir Adelman (RSA). a Symmetric key algorithm uses same key at both encryption and decryption process, through that more security for the data. [2] This process is very fast and more secure compared to the asymmetric key algorithm. Some examples are Advanced Encryption Standard (AES), Data Encryption Standard (DES), RC4, 3DES. The Advanced Encryption Standard, or AES, is an encryption algorithm created by the National Institute of Science and Technology (NIST) in 2001. The cipher utilized in AES is a block cipher from the Rijndael cipher family. When AES was created, three different Rijndael block ciphers were selected for use, to make AES even more secure. All three ciphers used were 128 bits, but the keys they each used were of different sizes: 128, 192, and 256 bits. [3] This is considered a symmetric block cipher, as only one key is used in the encryption process. Pipelining is an approach to increase the throughput of AES encryption and decryption algorithm. Speed of AES encryption depends on the number of rounds and the key generation involved in the algorithm. [4] AES uses its own key expansion algorithm. Pipelined AES encryption and key pipelining in AES algorithm can increase the throughput of the algorithm. Like encryption and decryption module another important component of AES algorithm is its key expansion module. This key expansion algorithm is based on iterative looping architecture [7]. If the architecture for AES with basic iterative architecture and partial loop unrolling is compared, the loop unrolling increases the speed of rounds implementation than the single round implementation in AES key expansion algorithm [4]. Memory Computational processing has increased in cloud servers, requiring larger core counts and higher memory densities. The number of processor cores doubles every two years, while the DRAM (Dynamic Random-Access Memory) DIMM (Dual in Memory Module) capacities double every three years. This causes a large gap between the core count and the memory density. On the other hand, traditional DRAM chips consume more than 40% of power of the servers. [17] Also, DRAM scaling to reach a higher memory density has some challenges such as high leakage current, reduced memory cell reliability, and more complex fabrication processes.

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

1. To protect memory from Hackers, need to secure our data by using Encryption Standards. [1]
2. Need to Increase the speed by using Pipelining Technique, through that the speed will be increased.

AES is short of the Advanced Encryption Standard and is a US Federal Information Processing Norm (FIPS) 192 Encryption Standard, published in November 2001. It was ratified in May 2002 as a federal standard. AES has been approved for federal us in the United States the latest of four current algorithms. Another standard algorithm, as RSA is a different algorithm category, should not be compared with RSA. RSA.RSA is rarely used as bulk encoding to transfer other encryption keys for AES and digital signatures, for example. AES is a symmetrical 128-bit block encryption algorithm. Sometimes a binary digit with two possible values as opposed to decimal digits can take one of the 10 values and one can take values zero and one. A 128-bit block is encrypted under the influence of a key and converted into a new block of the same size in a unique way. AES is symmetrical because the same key is used to encode and decrypt the reverse transformation. The only secret that is needed to maintain security is the key. The standard sets the 3 lengths and results algorithms AES-128, AES-192 and AES-256 are named, respectively, to set the length in bits. The resulting algorithms may be configured to use different key longs. When defined as time necessary to launch a brute force attack for the attacker, each additional bit of the key effectively doubles the strength of the algorithm i.e. an exhaustive search of the various key combinations to find the right one.

**Some background on AES:**

- In 1997, a call was made to candidates to replace the old data encryption standard, DES, by the US National Institute for Standards and Technology. 15 applicants were accepted for further consideration and the number of candidates was reduced to 5 following a fully public process and three open international conferences. The final candidate was announced and observations requested in February 2001. Comments were submitted by 21 organisations and individuals. Nobody had a doubt about the algorithm suggested. AES is based on well-publicated and solid mathematics and seems to be well resistant to any known attacks. There has been strong evidence that since published for a very long time now, there is no back door weakness or known weakness that is under intense scrutiny by researchers all over the world, and that the AES is already successfully protecting

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

enormous amounts of economic value and information. It is designed by Belgian researchers in Belgium and therefore does not convey the conspiracy theories sometimes spoken concerning a standard of encryption developed by a government agency from the United States. Only single main criteria must be met with a strong encryption algorithm:

## RELATED WORK

Literature research work by Chodowiec et al. (2001) has been presented on AES algorithms that use FPGA and by Sklavos et al (2002). The efficiency of AES architecture was addressed by Mr Karri and others (2002) and therefore errors in the circuit are desirable.. Schneier (1996) has considered that the following benefits of programme deployment include ease of usage, simplicity of uploading, portability and versatility and has only minimal physical protection for key storage. However, cryptographic algorithms enforced by hardware have further physical protections, which the intruder cannot easily access. The duplication of multiple functional units suggested by Rodriguez et al., achieves high performance; (2007).

Elbirt et al. (2001) utilised methods such as escape loops and pipelines. Ses methods have been extended to algorithms such as Serpent, Twofish, RC6, and AES. Finally all these algorithms were measured and Serpent became the best. Authors like Mcloone and McCanny (2001) have demonstrated that AES is a far quicker hardware application than the software. You indicated that shiftrow and mixcolumn may also be used as LUT. Typically a boolean feature representation can be implemented using the LUT method and the Sbox (BFR). This technique is used to introduce the Sbox as a mixed circuit. Jarvinen et al. (2003) used the Unified Circuit to enforce the Sbox and so no internal memory was needed. If Sbox is used as LUT, you would require a memory of 28 x 8 = 2048 bits. It needs a random access memory for half a block (BRAM). In dual port mode, BRAM is possible to divide between two Sboxes. For one round, ten BRAMs are required, and hundred BRAMs are essential for the ten rounds. In a big heavy pipeline configuration, the amount of internal memory may also be a bottleneck. Any step of the pipeline therefore requires a separate unshared memory block. A smaller and less costly aim computer needs a completely combined architecture without touching the memory. A high speed, low cost, AES processor has been built by Su et al. (2003). Zhang et al. (2004) also applied the combined logic Sbox and arithmetic field is used in order to minimise the domain. In their work they avoided the LUT and recommended a composite field in the AES algorithm for replacement bytes and reciprocal replacement bytes. In

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

the stage SubBytes and InvSubBytes, they decompose the GF inversion (28) into GF (( ((22) 2)). They suggested in their work a decomposition of the reverse to GF ((24)2, which results in a successful design with lower paths and narrower regions. The iterative loop technique is used by Hoang (2012) and the LUT procedure has been used for SBX. A reciprocal algorithm has been offered by Hussain and Gondal (2014). It offers a low convolution model and it quickly achieve high rate and low latency.

There are several books on the software-oriented implementation of the AES algorithm. Open MultiProcessing (OpenMP) programme helps you to parallel code. Memory Controller AES Processor was introduced by Wang et al. (2010). The overlap between data sharing and encryption has been resolved. This helps reduce the demand of the host processor disrupted handling. Its separate data paths minimise the latency issue and feedback dramatically. In their work, Alam et al. (2002) enhanced across parallel cores and pipelines. Pipelines are however, restricted for cypher block chaining (CBC) mode. Swankoski et al. (2004) suggested an N-encrypted parallel architecture for several symmetric encryption algorithms with N being the number of block cypher rounds. This thesis centred on the efficiency of the AES algorithm utilising software and hardware parallel techniques.

## PRELIMINARIES

The ASE [13], a symmetrical main block published in December 2001 by the National Institute of Norms and Technologies (NIST). It is a block cypher non-Feistel that encrypts and decrypts a 128-bit set database. Three separate lengths are available. The encryption consists of 10 processing rounds on 128-bit keys, 12 processing rounds on 192-bit keys, 14 processing rounds on 256-bit keys. In each stage, AES runs numerous rounds in which there are several phases. From one point to another a data block is modified. The data block is referred to as a state before and after each step. With the exception of the third, each round carries out four invertible transformations. The remaining three transformations arise in the last round with the exception of MixColumns. The AES cypher structure as shown in Figure 1.

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

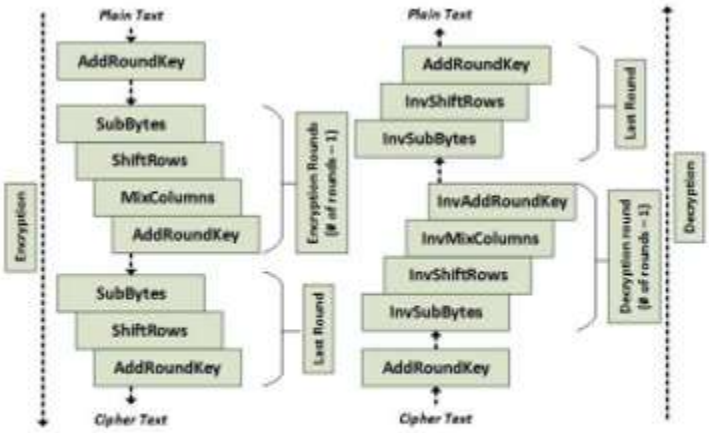



**Fig. 1. General design of AES encryption and decryption**

**Substitute Bytes:** On this encryption site, the first transition is Sub Bytes. It is an independent non-linear byte substitution that it regulates using a substitution table on any byte of the state (S-Box). The identical values from the search table overwrite all 16 bytes of the state. The Inv Sub Bytes can be used at decoding. Inv Sub Bytes table substitutes bytes of a state. The sub bytes process is seen in Figure 2.

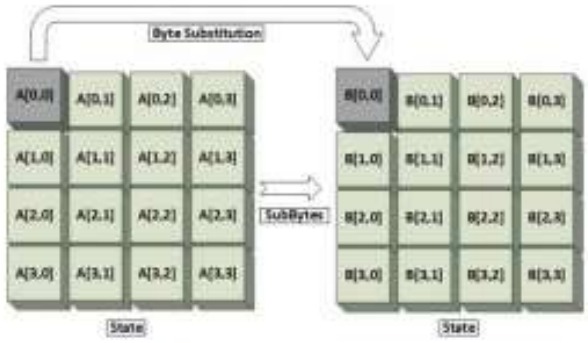



**Fig. 2.** Sub Bytes

**Shift Rows:** The status bytes in Figure 3 appear in each row to be moved to the left. It is referred to as Move Line. The amount of changes depends on the state matrix's row number (0, 1, 2 or 3). Row 0 bytes shall not be transferred, Row 1, 2, 3 shall be moved to 1, 2, 3 bytes shall be allocated accordingly. The map displays the activity Change Rows.

ISSN: 2278-4632
Vol-13, Issue-11, November 2023


**Fig. 3.** ShiftRows

**Mix Column:** The transition of the Mix columns is at the stage of columns. It transmits each state column to a new column. In truth, the transformation is the multiplication by a stable square matrix of a column. The Galois field performs all the arithmetic operations (Finite Field). The bytes are not numbers but polynomials. The Mix Columns process is shown in Figure 4.

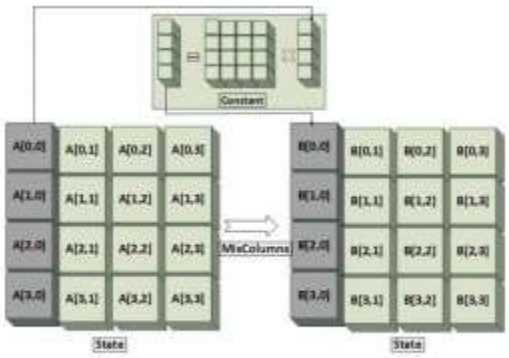



**Fig. 4.** MixColumns

**Add Round Key:** . Attach Circular Key continues from one column to the next. As a consequence, It's close to Mix Column. Attach Round Key to each matrix for columns adds a round keyword. In the Add Round Main point, the matrix addition operation is done. The Add Round Key activity is shown in Figure 5. In encryption, all rounds except in the last round, contain sub bytes, move rows, mix columns and add round keys.

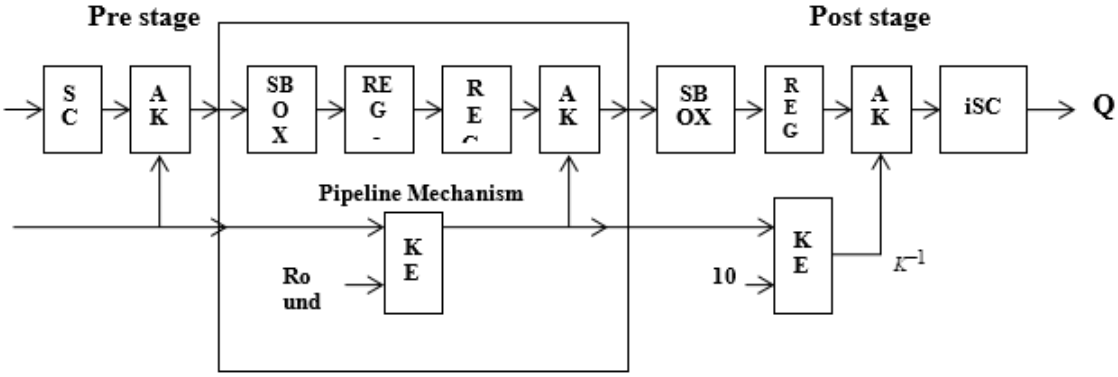
Transformation of Mix Columns in the last encryption round shall not be done. In addition to the nine rounds of Inverse Move Rows, Inversal Sub Bytes, Inverse AddRoundKey and Inverse Mix Columns Transition, the decryption process effectively assumes the same structure as the encryption. The Inverse Mix Columns are no longer carried out in the final round.

## PROPOSED METHOD

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

# MODIFIED-ADVANCED ENCRYPTION STANDARD

Encrypting data is a way to protect the data or to prevent the unauthorized access of data by others and these data can be text, image audio, video or anything. In order to protect data from unauthorized access a new concept is introduced and this is based on linear feedback shift register method. In this method two step encryption is provided to give more security to the data. The encrypted image can be decoded in the decryption stage. In the encryption stage the LFSR will generate random numbers to reorder positions of each pixels in the row of the image . After row encryption, column need to be encrypted by again generating random numbers using LFSR to reorder each pixels in the column of the image . Then we use XOR operation to shuffle all pixels to get the final encrypted image. To decrypt the image , reverse operation of encryption is performed . First step in the decryption process is XOR execution and then decrypt the column encrypted image and finally decrypting row encrypted image to reconstruct the original image.

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

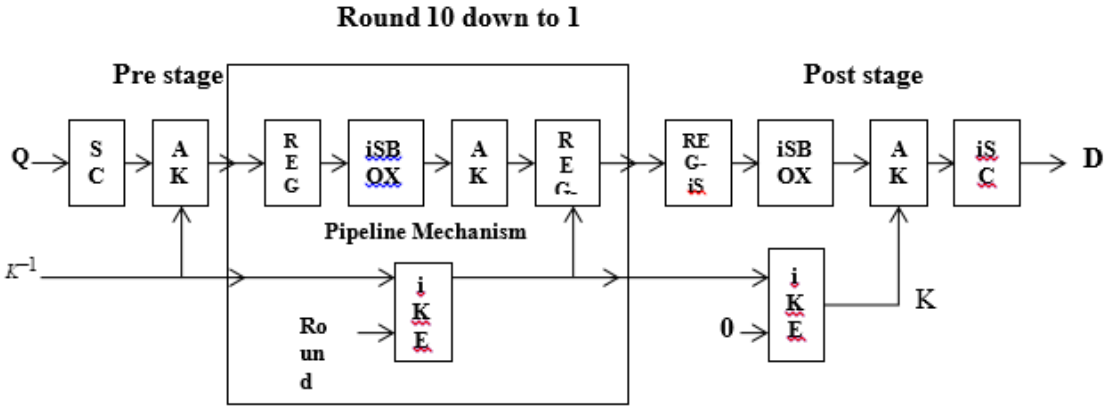



**FIG: 6. DESIGN OF AES SYSTEM WITHOUT S BOX USING REGISTER FOR COMMUNICATION SYSTEM**

**Two main processes of AES encryption algorithm:**

It is possible to break the AES encryption algorithm into two sections, the main timeline and Round Shift. Two major planners are the main extension and the collection of the round key. Key expansion involves mapping Nk bits initial key to the expanded key when choosing round key Nb bits from the expanded key module. Key expansion

The transition round consists of four substitution bytes, byte rotation, combine column and AddRoundKey units.

The ByteRotation, MixColumn and AddRoundKey all are linear transformations except ByteSub in the share information modules of round transformation.

### A. Take analysis of the AES algorithm principle and we can find:

Byte The 128-bit input plaintext portion substitutes the inverse element corresponding to the Galois field GF (28) which has 8 bits/group on its smallest operating segment. Byte Rotation is achieved by cyclically moving the 128-bit state matrix of which the smallest operand is a row (32 bits).

The process of the Mix Columns involves multiplication and add-on operation byte rotation results with the required x8 + x4 + x3 + x 1 irreducible GF(28) polynomial with an operating unit minimum of 32 bit. Adding round key operation requires a basic 8-bit XOR operation.

The plaintext inputs and first-key inputs and intermediate translation outputs are all saved into state matrices and processed in one byte or one phrase in the AES Algorithm. In addition, cypher text output is stored in a state matrices. Therefore the initial 128-bit data could be segmented in

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

order to take operations at least in bits. In the new algorithm we design several external controls to enforce the information transfer and processing on each column of the state matrix (32bit).

### B. That means the data should be packed and put into further operations.

Take S-box as an example for separate and reversible bytes replacement. First of all there are four columns in the State matrix. The process of the lookup table displayed as figure then replaces byte. 7.

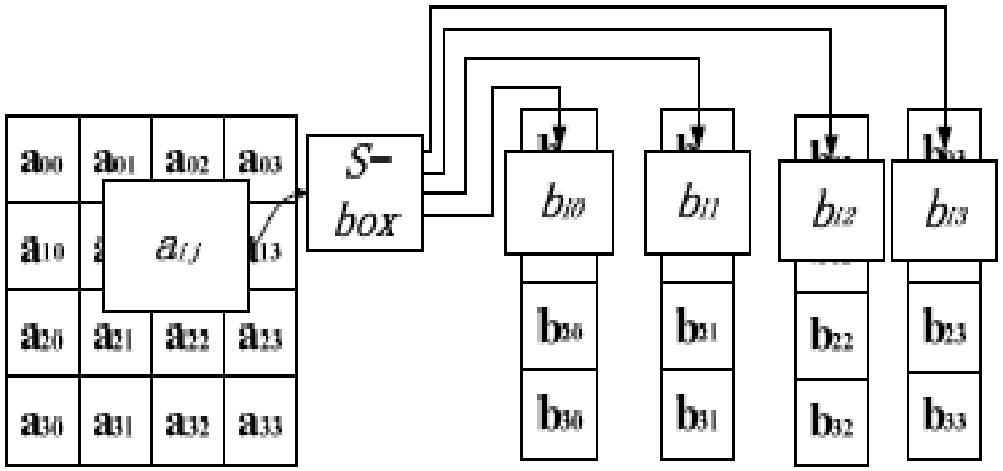



**Figure 7. Bytes segmentation and replacement processing**

Consequently, the real 128-bit data with plain text and input with a key would be augmented by up to four 32-bit strings. To minimise the display ports, the initial 128-bit output was fitted with the inclusion of a clock controller with four continuous 32-bit ciphertext sequences. Before the pipelination process, the 128-bit data in the round transition is separated into four classes of 32-bit data.

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

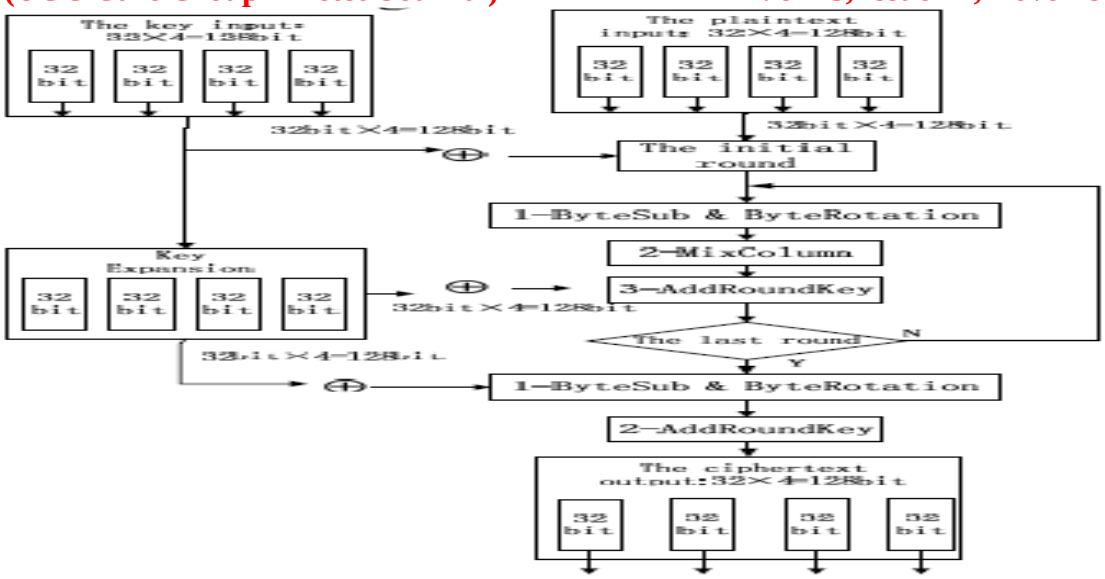



**Figure 8. The new improved structure of AES algorithm**

In the analysis above, it can be seen that the AES encryption method can mainly be split into two parts: the key software and the round transformation process. These two primary processes are both separated by the enhanced framework. The first key is to be sent to the two modules: key expansion and key collection, when after the round key is chosen, the plaintext would be sent to round transformation. However the data processing process is converted into a 32-bit device. The latest algorithm technique is shown in Fig. 8.

The work of Subbytes and MixColumns with 32-bit columns is mostly carried out in a round transformation. Four packets are processed separately in the circular transition. Then MixColumn effects and Keyexpansion 32-bit keys are paired with XOR operators. The round transformation is a module with sixy-four input ports and three-four output ports (32-bit plaintext+32 bit key).

Look-Up Table feature is done by SubByte (LUT). This ensures that all replacement units are saved into a memory (256 TEXTRA 88bit=1024 bit), and are finalised via Locate and Replace.

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

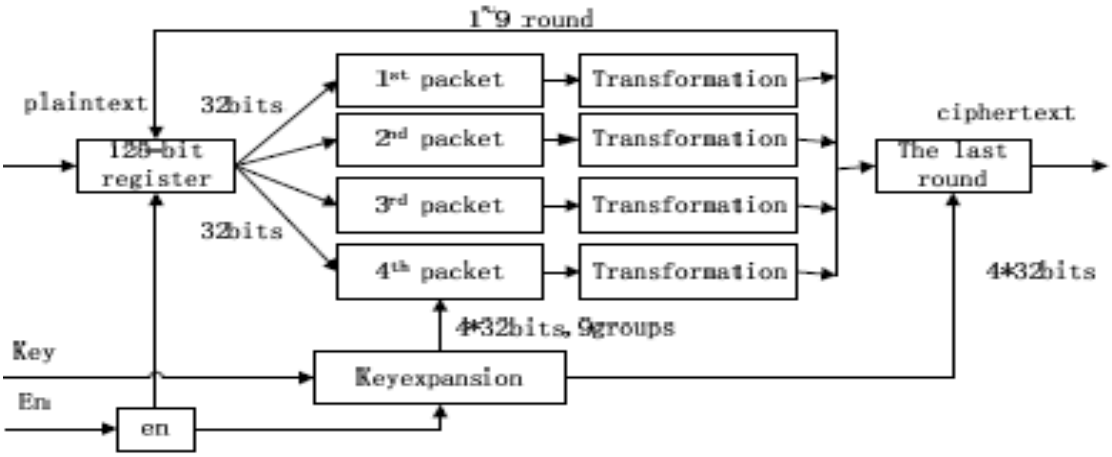



**Figure 9. The round processing with pipeline technology**

A 128-bit processor is the final round. The 128-bit intermediate encrypted data can be used in XOR after nine rounds of operations including Shiftrows, SubByte and Mixclumns.

Final extended key (4*32bit), the key expansion module is given. The final processor round performance is the 128-bit ciphertext desired. Similarly, an external allow signal divides the ciphertext into four paquets of 32-bit details.

This module is essentially the same as other component of the AES encryption algorithm, which is conventional. Just the method of propagation is the difference. THIS Until removing the original key and the extended key, four 32-bit data are separated.

All of these modules may be split down into the fundamental quest and XOR operations if FPGA applies the AES algorithm. Thus the fundamental processing machine (look-up table) Can be worked with FPGA. The Add Round Key procedure is done first. The programming module begins to operate when the plaintext and initial key are entered.

Stored keys are simultaneously in the registers. This approach is independent of a single FPGA.

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

## THE DECRYPTION MODEL

Parallel decryption may be conducted on two occasions during the encryption. The decryption process takes place as the encryption activity at the first parallel stage (pipelines in separate rounds). The number of databases (1 = I = L), D, Ci, and Bi may be defined as following for each of the blocks to be decrypted as "L"

$$C_i = \begin{bmatrix} c_{i,1} & c_{i,2} & c_{i,3} & c_{i,4} \\ c_{i,5} & c_{i,6} & c_{i,7} & c_{i,8} \\ c_{i,9} & c_{i,10} & c_{i,11} & c_{i,12} \\ c_{i,13} & c_{i,14} & c_{i,15} & c_{i,16} \end{bmatrix} \quad \text{and} \quad D = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

$$B_i = D * C_i$$

$$\begin{bmatrix} b_{i,1} & b_{i,2} & b_{i,3} & b_{i,4} \\ b_{i,5} & b_{i,6} & b_{i,7} & b_{i,8} \\ b_{i,9} & b_{i,10} & b_{i,11} & b_{i,12} \\ b_{i,13} & b_{i,14} & b_{i,15} & b_{i,16} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} * \begin{bmatrix} c_{i,1} & c_{i,2} & c_{i,3} & c_{i,4} \\ c_{i,5} & c_{i,6} & c_{i,7} & c_{i,8} \\ c_{i,9} & c_{i,10} & c_{i,11} & c_{i,12} \\ c_{i,13} & c_{i,14} & c_{i,15} & c_{i,16} \end{bmatrix}$$

Inv_Mix_Column is then represented by the following set of equations and illustrated

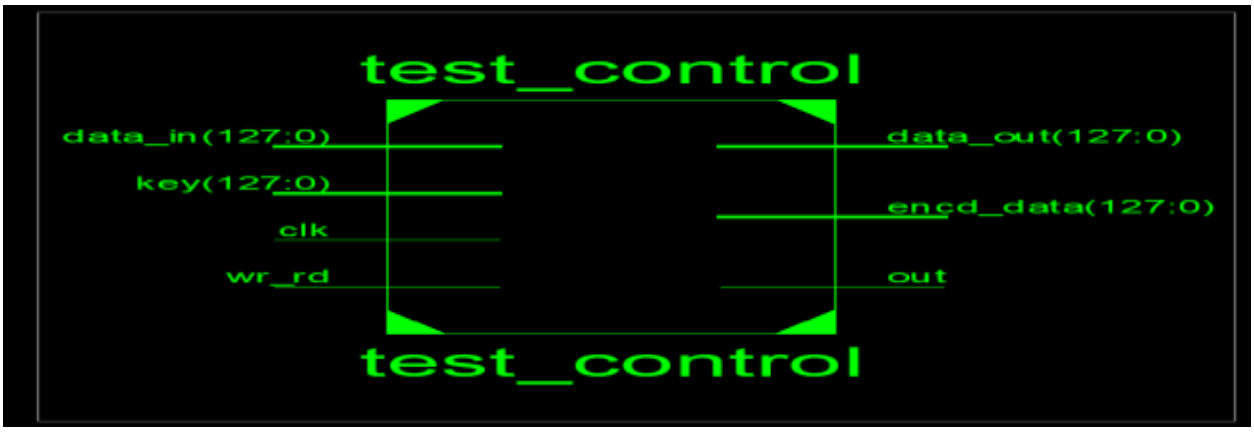
$$b_{i,1} = (0E \bullet c_{i,1}) \oplus (0B \bullet c_{i,5}) \oplus (0D \bullet c_{i,9}) \oplus (09 \bullet c_{i,13})$$
$$b_{i,5} = (09 \bullet c_{i,1}) \oplus (0E \bullet c_{i,5}) \oplus (0B \bullet c_{i,9}) \oplus (0D \bullet c_{i,13})$$
$$b_{i,9} = (0D \bullet c_{i,1}) \oplus (09 \bullet c_{i,5}) \oplus (0E \bullet c_{i,9}) \oplus (0B \bullet c_{i,13})$$
$$b_{i,13} = (0B \bullet c_{i,1}) \oplus (0D \bullet c_{i,5}) \oplus (09 \bullet c_{i,9}) \oplus (0E \bullet c_{i,13})$$

For the three other columns of the matrix, this is replicated. As stated before, transformations can all be done in parallel with Inv Mix Column and Add Round key. Transformation Inv Mix Column contains 160 XOR transactions and 192 move transactions. The elements of the matrix Inv Mix Column can be determined separately, equivalent to the Mix Columnu matrix. At most 64 processors will perform the Inv Mix Column transformation in each point. When utilising 16 processors, calculation of each matrix product in parallel. Four processors will function with one or more variable bi,j as seen in this figure.

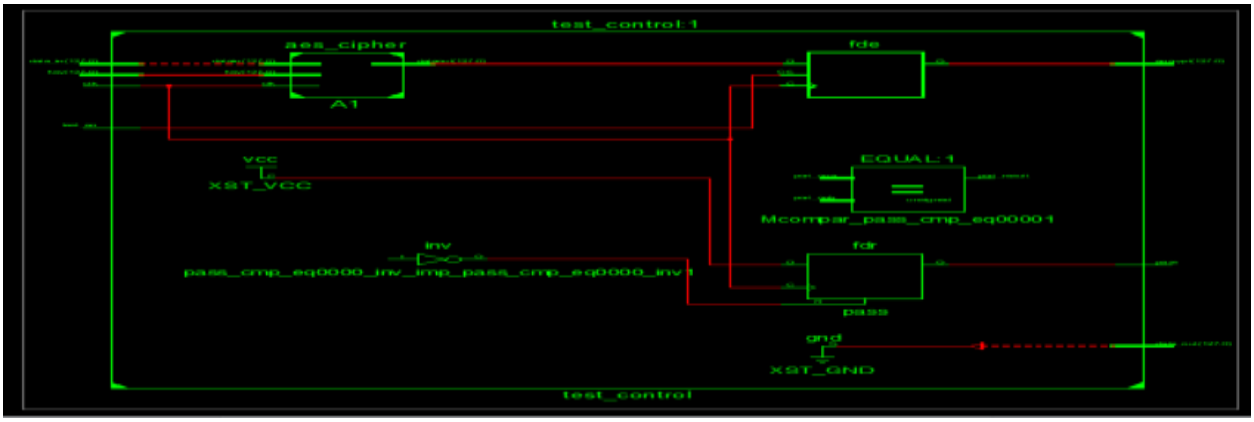
## RESULTS

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

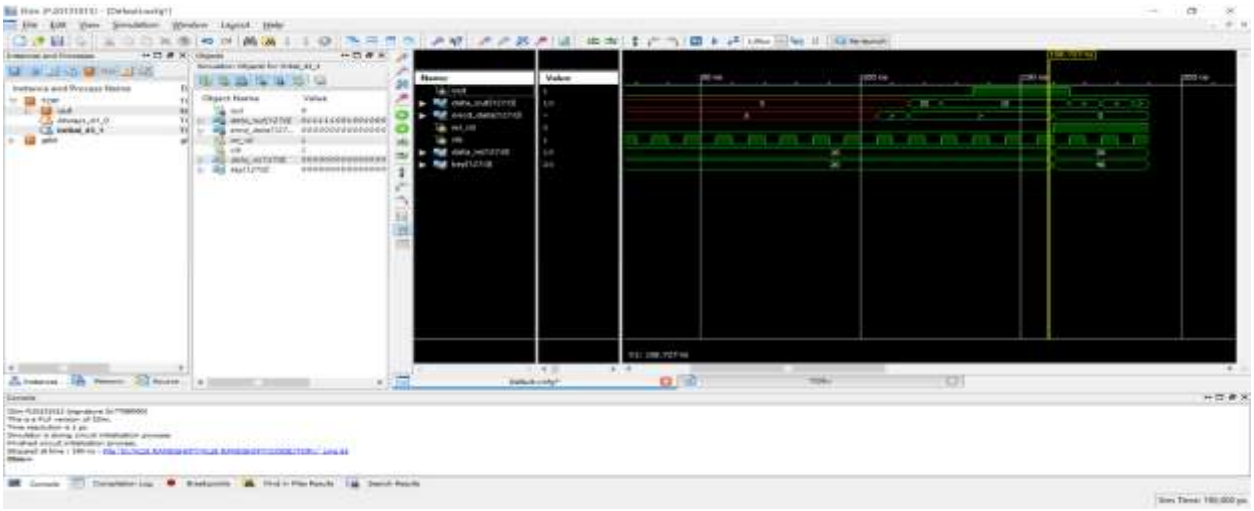
**RTL**




**INTERNAL BLOCK DIAGRAM**




**SIMULATION RESULTS**



**COMPRESSION TABLE -1**

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

| | | | |
|---|---|---|---|
| **EXISTING METHOD** | **AREA 64050 LUTS** | **DELAY 5.925nS** | **POWER 1.271 mW** |
| **PROPOSED METHOD** | **AREA 20,589 LUTS** | **DELAY 3.793nS** | **POWER 1.271 mW** |

## CONCLUSION

In this paper implemented the randomness feature of Pipelined AES encryption as well as rotational shift operation in memory cells. This method, which was called Rand Shift, is simple hardware implementation and low energy consumption. This paper implemented Advanced Encryption Standard by using pipelining technique to reduce the delay and area.

**FUTURE SCOPE:** AES is a block cipher and the most popular algorithm used in symmetric key cryptography. Selection of larger key size which would make the algorithm more secure. The strength of the AES algorithm may enhance by increasing the key length from 128 bits to 256 bits and there by the number of rounds is increased in order to provide a stronger encryption method for secure communication. This paper can be implemented by a Pipelining Rand Shifter with Pipelining AES for better Result as compare to Area, delay and Power delay product.

## REFERENCES:

[1] M. Soltani, M. Kamal, and A. Afzali-Kusha are with the school of Electrical and Computer Engineering, University of Tehran, “RandShift: An Energy-Efficient Fault-TolerantMethod in Secure Nonvolatile Main Memory”, Manu script received February 23,2019, received June 20,2019 and August 17,2019, accepted September 3,2019.

[2] Anane Nadjia CDTA (Centre de Développement des Technologies Avancées) Algiers, Algeria Anane Mohamed ESI (Ecole nationale Supérieure d’Informatique) Algiers, Algeria/2015

[3] Liting Yu, Dongrong Zhang, Liang Wu, Shuguo Xie, Donglin Su, Xiaoxiao Wang Beihang University. 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering.

ISSN: 2278-4632
Vol-13, Issue-11, November 2023

[4] Anane Nadjia CDTA,Algiers, Algeria Anane Mohamed ESI "AES IP for Hybrid Cryptosystem RSA-AES" 2015 12th International Multi-Conference on Systems, Signals & Devices.

[5] K.Sandyarani "Design And Analysis Of AES-CM With Non- Linearity S-Box Architecture"/July/2013/3

[6] Guang-liang Guo, Quan Qian*, Rui Zhang "Different Implementations of AES Cryptographic Algorithm"/2015.

[7] Rozita Borhan, Mohd Fuad Tengku Aziz "Successful Implementation of AES Algorithm in Hardware"/2012/85

[8] M0nica Liberatori, Fernando Otero J. C. Bonadero, Jorge Castifieira "AES-128CIPHER.HIGHSPEED,LOW-COSTFPGA IMPLEMENTATION"/2017/98.

[9] Zhiyong Guo, Guangjun Li, Yang Liu "Dynamic Reconfigurable Implementations of AES Algorithm Based on Pipeline and Parallel Structure" /2010/156.

[10] JINN-TSONG TSAI1 , KAI-YU CHIU2 , AND JYH-HORNG CHOU2,3,4.