DESIGN AND IMPLEMENTATION OF MODIFIED AES ALGORITHM FOR IMPROVING EXECUTION SPEED USING VERILOG

B.Anil kumar[1], T.Pradeep Reddy[2], K.Samatha[3]

[1] *Assistant Professor, Dept of ECE, Malla Reddy Institute Of Engineering And Technology, Hyd., TS, India.*

[2] *B.Tech Student, Dept of ECE, Malla Reddy Institute Of Engineering And Technology, Hyd., TS, India*

[3] *B.Tech Student, Dept of ECE, Malla Reddy Institute Of Engineering And Technology, Hyd., TS, India*

Abstract **-** An implementation of Modified AES Algorithm For Improving Computing Speed Using Verilog high is presented in this paper in order to improve the safety of data in transmission. The mathematical principle, encryption process and logic structure of AES algorithm are introduced. So as to reach the purpose of improving the system computing speed, the Encryption and Decryption processing methods were used. This research investigates the AES algorithm with regard to the Very High Speed Integrated Circuit Hardware Description Language (VHDL). Software is used for simulation and optimization of the synthesizable VHDL code. All the transformations of both Encryption and Decryption are simulated using an iterative design.

Keywords— Encryption, Decryption, Xilinx, Verilog.

I. INTRODUCTION

VLSI stands for "Very Large Scale Integration". This is the field which involves packing more and more logic devices into smaller and smaller areas. Simply we say Integrated circuit is many transistors on one chip.Design/manufacturing of extremely small, complex circuitry using modified semiconductor material. Applications wide ranging: most electronic logic devices. The **Advanced Encryption Standard** (**AES**), also known by its original name **Rijndael Algorithm**.AES is formal encryption method adopted by the National Institute of Standards and Technology of the US Government, and is accepted worldwide. This paper introduces AES and key management, and discusses some important topics related to a good data security strategy. The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

II. LITERATURE SURVEY

Arithmetic coding implemented in traditional way is not secure. Applications like internet, digital cameras and portable music players demand security in addition to compression. One approach is to use the encryption engine like Advanced Encryption Standard (AES) in addition to arithmetic coder. But this approach is in efficient since it doesn't explore the commonalities of Encryption and Decryption. However, while this will certainly meet both goals, it fails to take advantage of the additional design flexibility and potential computational simplifications that are available if the coding and encryption are performed jointly. A new method is proposed in this project that is secure against a chosen plaintext attack.

III. BLOCK DIAGRAM

TRANSMITTER:

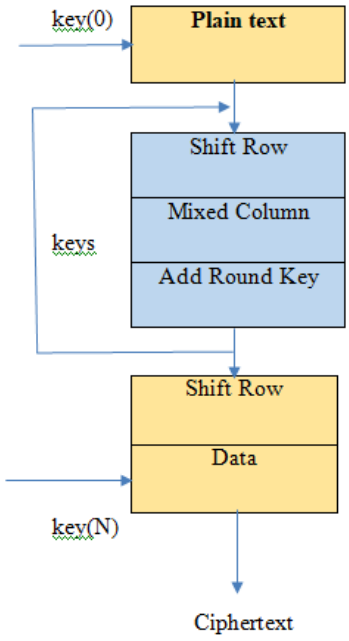


Figure 1: Encryption Block Diagram

The AES encryption and decryption processes for a 200-bit plain text block are shown in Fig. 1 and 2. The AES Algorithm specifies three encryption modes: 200-bit, 192-bit, and 256-bit. Each cipher mode has a corresponding number of rounds Nr based on key length of Nk words .The state block size, termed Nb, is constant for all encryption modes. This 200-bit block is termed the state. Each state is comprised of 4 words. A word is subsequently defined as 4 bytes. Table1 Shows the possible key/state block/round combinations.

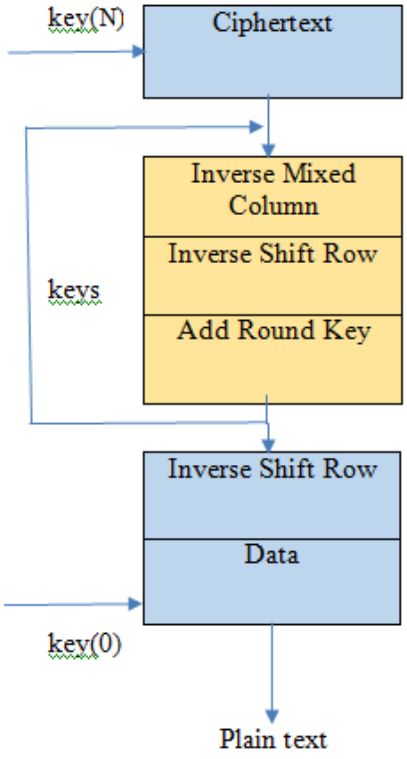


Figure 2: Encryption Block Diagram

IV. DESCRIPTION

ENCRYPTION PROCESS:

The Encryption and decryption process consists of a number of different transformations applied consecutively over the data block bits, in a fixed number of iterations, called rounds. The number of rounds depends on the length of the key used for the encryption process. For key length of 200 bits, the number of iteration required are10. (Nr = 10). As shown in Fig. 2, each of the first Nr- 1 rounds consists of 3 transformations: Shift Rows (), Mix Columns () & Add Round Key ().

SHIFTROWS:

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows :

1. First row is not shifted.
2. Second row is shifted one (byte) position to the left.
3. Third row is shifted two positions to the left.
4. Fourth row is shifted three positions to the left.
5. The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

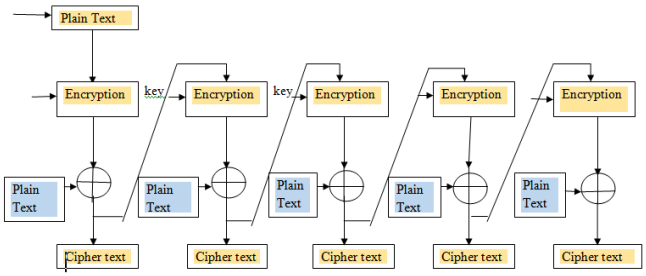
MIXCOLUMNS:

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

ADDROUNDKEY:

The 25 bytes of the matrix are now considered as 200 bits and are XORed to the 200 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 200 bits are interpreted as 16 bytes and we begin another similar round.

ENCRYPTION BLOCK DIAGRAM:



Plain Text Input: TABLE 1

V	E	R	Y	L
A	R	G	E	S
C	A	L	E	I
N	T	E	G	R
A	T	I	O	N

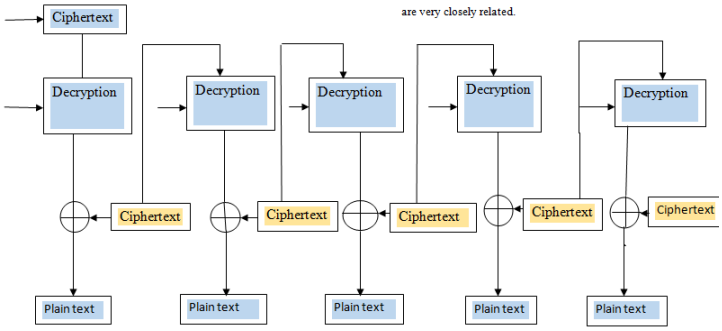
Cipher Text Output: TABLE 2

L	V	E	R	Y
G	E	S	A	R
E	I	C	A	L
E	G	R	N	T
O	N	A	T	I

DECRYPTION PROCESS:

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. This process is direct inverse of the Encryption process. All the transformations applied in Encryption process are inversely applied to this process. Hence the last round values of both the data and key are first round inputs for the Decryption process and follows in decreasing order. Each round consists of the three processes conducted in the reverse order −

DECRYPTION BLOCK DIAGRAM:



1) TRANSMITTER Input Plaintext : -

“ VERYLARGESCALEINTEGRATION “

2) TRANSMITTER Output Cipher text:-

“ LVERYGESAREICALEGRNTONATI “

3) RECEIVER Input Cipher text:-

4) **“ LVERYGESAREICALEGRNTONATI “**

5) RECEIVER Output Plaintext:-

“ VERYLARGESCALEINTEGRATION “

1. Add round key
2. Mix columns
3. Shift rows

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related. The Key Expansion step is performed using key schedule. The Initial Round consists only of an Add Round Key operation. The Rounds step consists of a Bytes, Shift Rows, Mix Columns, and an Add Round Key operation. The number of rounds in the Rounds step varies from 10 to 14 depending on the key size. Finally, the Final Round performs a Bytes, Shift Rows, and an add Round key operations.

Plain Text Output: TABLE 3

V	E	R	Y	L
A	R	G	E	S
C	A	L	E	I
N	T	E	G	R
A	T	I	O	N

Cipher Text Input: TABLE 4

L	V	E	R	Y
G	E	S	A	R
E	I	C	A	L
E	G	R	N	T
O	N	A	T	I

V. SIMULATION RESULT

Figure 3: Simulation Waveforms of final round of

Encryption process

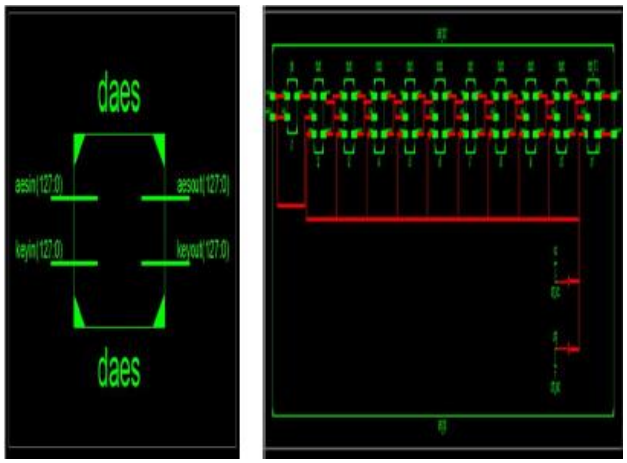


Figure 4: RTL Schematic of Encryption Process

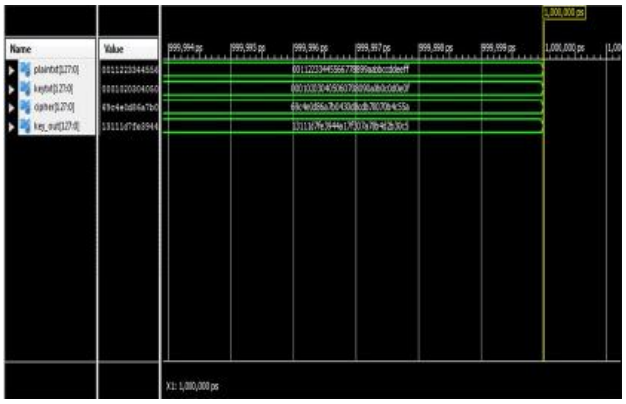


Figure 5: Simulation Waveforms of final round of Decryption process

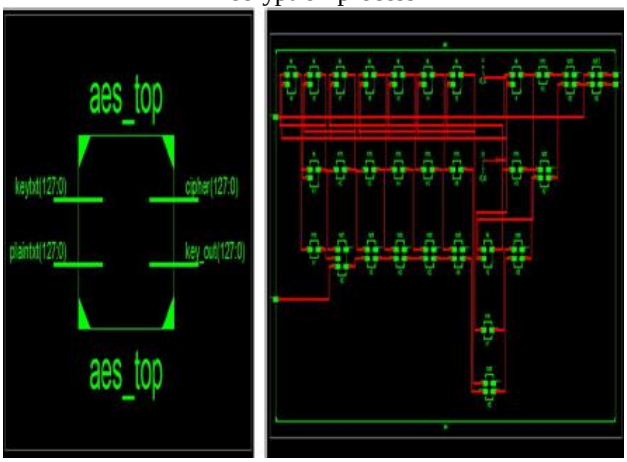


Figure 6: RTL Schematic of Decryption Process

VI. CONCLUSION AND FUTURE SCOPE

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing'. The Advanced Encryption Standard algorithm is an iterative private key symmetric block cipher that can process data blocks of 200 bits through the use of cipher keys with lengths of 200, 192, and 256 bits. An efficient FPGA implementation of 200 bit block and 200 bit key

AES cryptosystem has been presented in this Paper. Optimized and Synthesizable Verilog code is developed for the implementation of both 200 bit data Encryption and decryption process & description is verified using ISE 18.1 functional simulator from Xilinx. All the transformations of algorithm are simulated using an iterative design approach in order to minimize the hardware consumption. Each program is tested with some of the sample vectors provided by NIST.

VII. REFERENCES

[1] Marko Mali, Franc Novak and Anton Biasizzo "Hardware Implementation of AES Algorithm" – Journal of ELECTRICAL ENGINEERING, Vol. 56, No. 9-10, 2005, 265-269.

[2] Beerhouse A. Forouzan and Debden Mukhopadhyay "Cryptography

[3] FIPS 197, "Advanced Encryption Standard (AES)", November 26, 2001.

[4] L.Thulasimani,"A Single Chip Design and Implementation of AES -200/192/256 Encryption Algorithms"- International Journal of Engineering Science and Technology, Vol. 2(5), 2010, 1052-1059.

[5] Nation Institute of Standards and Technology (NIST), Data Encryption Standard (DES), National Technical Information Service, Springfield, VA 22161, Oct. 1999.

[6] J. Daemen and V. Rijmen, "AES Proposal: Rijndael", AES

[7] J Algorithm Submission, September 3, 1999. Nechvatal et. al., Report on the development of Advanced Encryption Standard, NIST publication, Oct 2, 2000.

[8] FIPS 197, "Advanced Encryption Standard (AES)", November 26, 2001.

[9] K. Gaj and P. Chodowiec, Comparison of the hardware performance of the AES candidates using reconfigurable hardware, in The Third AES Candidates Conference, printed by the National Institute of Standards and Technology.

Mr. **B. ANIL KUMAR** , M.Tech working as Assistant professor ,in the **Department of Electronics and communication , Mallareddy Institute of Engineering and Technology, Hyderabad**. He studied **B.Tech** in **Electronics and Communications Engineering** from JNTU college of Engineering, JNTUH, Hyderabad, Telangana and **M.Tech** in **VLSI SYSTEM DESIGN From Aurora college of engineering**, JNTUH, Hyderabad, Telangana.

T.PRADEEP REDDY is studying B.Tech in (Electronics & Communication Engineering) at Mallareddy Institute of Engineering & Technology (MRIET), Hyderabad. Telangana.

K.SAMATHA is studying B.Tech in (Electronics & Communication Engineering) at Mallareddy Institute of Engineering & Technology (MRIET), Hyderabad. Telangana.