2018 4th International Conference for Convergence in Technology (I2CT)
SDMIT Ujire, Mangalore, India. Oct 27-28, 2018

Designing of AES Algorithm using Verilog

SOUMYA V H
VLSI design and Embedded System
Visvesvaraya Technological University,
PG centre, Belgavi, India
soumyahudge@gmail.com

MAHESH B. NEELAGAR
Assistant professor
Dept.VLSI Design& ES,
Visvesvaraya Technological University,
PG centre, Belgavi, India
neelagarmahesh@gmail.com

K V KUMARASWAMY
Senior Technical Manager,
Trident TechLabs Pvt Ltd,
Banglore, India
kvkswamy@yahoo.com

***Abstract*— One of most popular algorithm of cryptography is AES, which has data block of 16bytes and key size is variable of 128bits, 192bits and 256bits. In proposed design, AES method implemented by the use of Verilog using Xilinx ISE 14.7, which reduces operation time and clock cycles needed for encode and decode the message, if compared with implementation using VHDL. AES has more private compared with DES, because of its key size. It includes two main modules, in which all the sub modules are called by module call method. In application of embedded system it improves security measures.**

***Key words*— AES, Verilog, Xilinx ISE, plain text, cipher text.**

I. INTRODUCTION

Data transfer in internet security and other applications is the main role of cryptography. It is used for secure communication and information security. In wireless communication, several security issues like privacy of data over insecure networks. Thus, it became one main method to overcome the attacks and secure the user's data. Any cryptographic algorithm performs two processes one is encryption process and other one is decryption process. Encryption process, it converts original message (plain text) into coded message (cipher text). Decryption process, it converts coded message into original plain text. Most preferred algorithm is symmetric key because it has faster execution time than asymmetric key.

Cryptography is divided in 2 categories and those are,

i) Symmetric key cryptography, in which same key is used for encryption and decryption shown in figure 1.

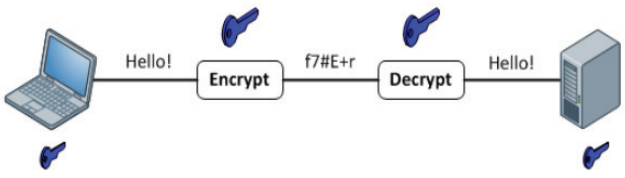

Fig. 1. Symmetric cryptographic method

ii) Asymmetric key cryptography, here different keys, private and public key are required for encryption and decryption shown in figure 2.

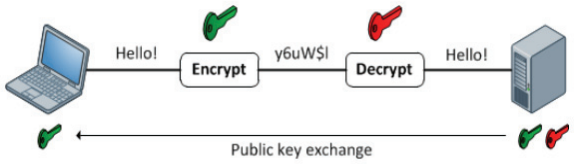

Fig. 2. Asymmetric cryptographic methods

Main advantage of AES is higher key size, which are 128bits, 192bits and 256bits. If key is 128bits, very complicated to corrupt because it attempts 2^{128} combinations to hack message therefore AES is safe protocol. Each block uses same way of operation to encrypt and decrypt and implementation on software is difficult.

It is commonly used for privacy in internet, wireless applications, economical transactions and storage of message or data or voice or image.

Paper organised into different sections given by, Section I gives, importance and types of cryptography and AES benefits, limitations and applications. Section II gives, history and review of AES. Section III gives, previous methodology of AES and Section IV gives, design which is proposed and implementation using Verilog. Section V gives, simulation results and comparison table. Section VI defines conclusion and future scope and then references.

II. LITERATURE OVERVIEW

An older standard was DES used for privacy in internets. It has 56bits and 64bis as size of key and data block, 16 operations of round are present. DES can easily breakable by third party, reason is minimized key size. Hence NIST announced different algorithms for protecting data [1].

It summarizes tradeoffs between power, area and throughput design of AES. Area and power minimised by iterative looping and expansion key module. It provides best throughput by the use of pipeline register. These optimization helpful for secure applications like low power ES applications [3]. It is implemented on micro controller 8-bit chip for security improvement [5]. Design with low power and area applicable for real time [6].

978-1-5386-5232-9/18/$31.00 ©2018 IEEE

III. METHODOLOGY

AES has different block size, expanded key size, and round operations for different key size of 128bits, 192bits, 256bits with data of 128bits, whose specifications shown below.

TABLE I. DIFFERENT SPECIFICATIONS OF AES WITH VARIABLE KEY

AES(bits)	Size of block, Nb(words)	Key size, Nk(words)	Number of rounds (Nr)	Expanded key size(words)
128	4	4	10	44
192	4	6	12	52
256	4	8	14	60

AES provides 10 round operations for both processes shown in figure 3. Each round has particularly steps of operations which are repeated for all rounds. 10 round keys are calculated for each round by key expanding method.

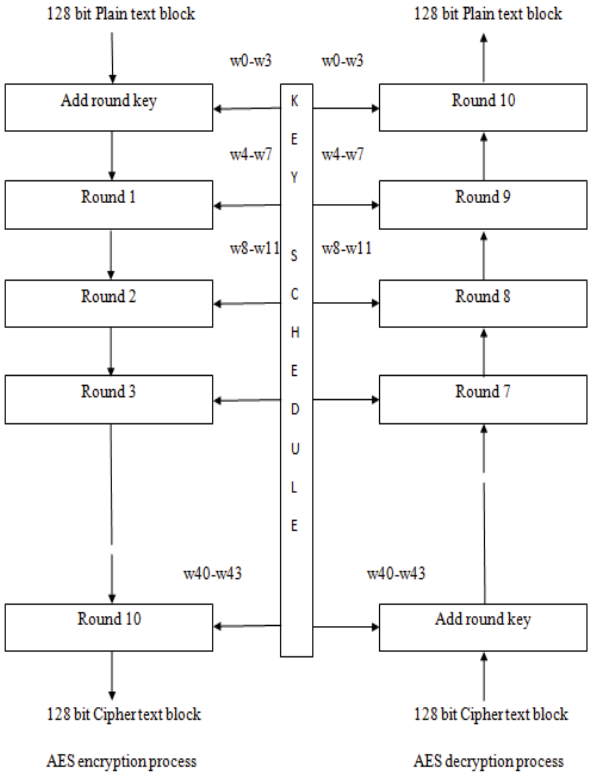

Fig. 3. Complete block diagram of AES

During encryption, each round will take 4 transformations shown in figure 4. Each transformation has array of 16bytes of state with 4x4 matrixes, which are given below.

i) Substitute byte: It performs on each and individual state. Substitution can done from standard box (S-Box) shown in figure 5. Example, substitute b14 from S-Box by replacing a14. It consist total 256 numbers in table. It uses LUT's for substitution. Different types are available to calculate S-Box value. LUT provides less usage of hardware, it reduces latency with computation time.

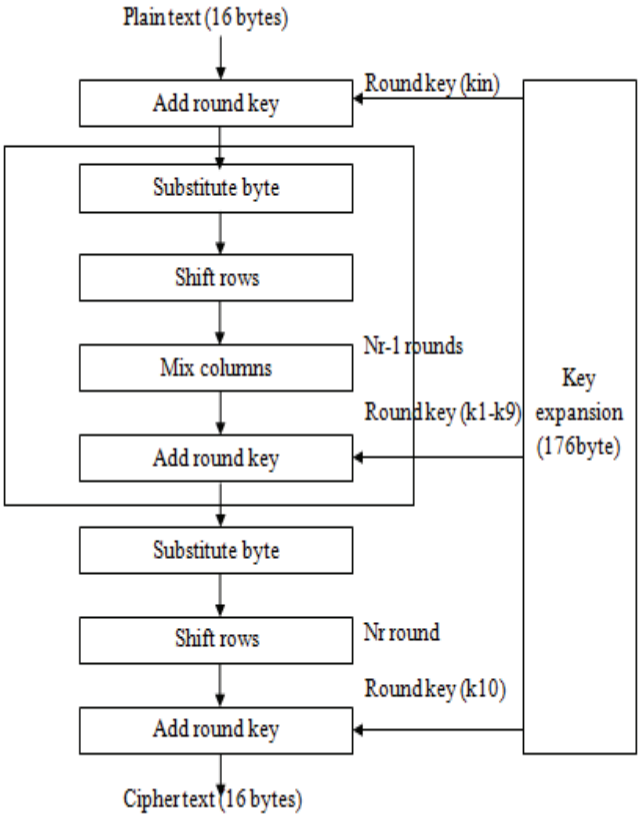

Fig. 4. Round operations during encryption

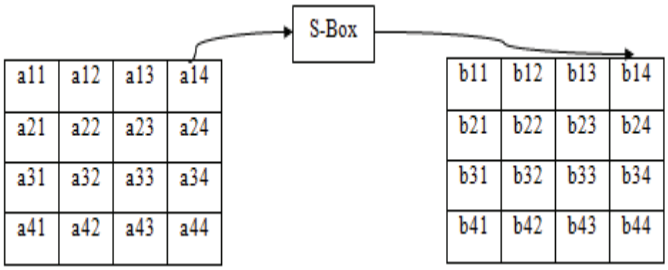

Fig. 5. Substitute byte operations

ii) Shift rows operation: On matrix rows, operation will be performed. Here first row kept same, 2nd, 3rd and 4th row shifted cyclically left by 1 byte, 2 byte and 3 byte given in figure 6.

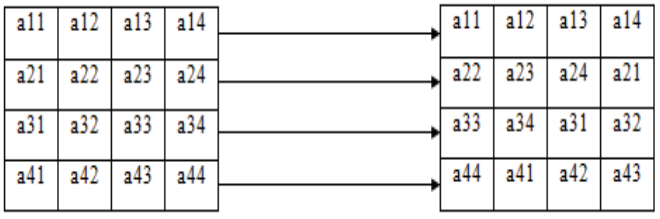

Fig. 6. Shift rows operation on states

iii) Mix column operation: Current state matrix and standard matrix obtained from polynomial multiplied, evaluated in figure 7. Multiplication can be done on matrix of shift row output.

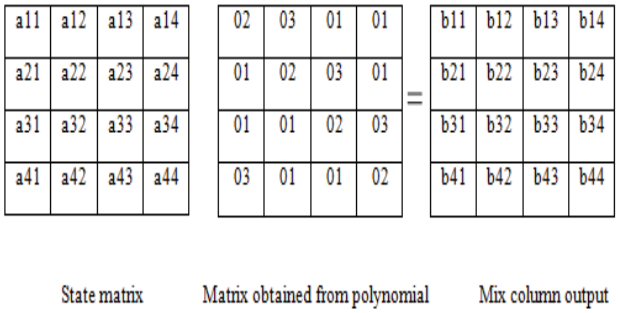

Fig. 7. Mix column operations

iv) Add round key: XOR operation performed on each state of matrix. Hence, each byte of round key and current state matrix is XORed.

$$\text{Add round key} = \text{State matrix} \oplus \text{Round key}$$

Key expansion operation: key expansion consist an array of 176-byte (44 words) key, called as expanded key. In this expansion combination of four bytes is 'word'.

For generating round key, 'g' is function created by performing 3 different operations on word w3 shown in figure 8. 1st operation is rotate word cyclic left by 1 byte, 2nd
operation is substitute byte from S-Box, and last operation is 1st and 2nd operation result XORed with round constant (RCON).

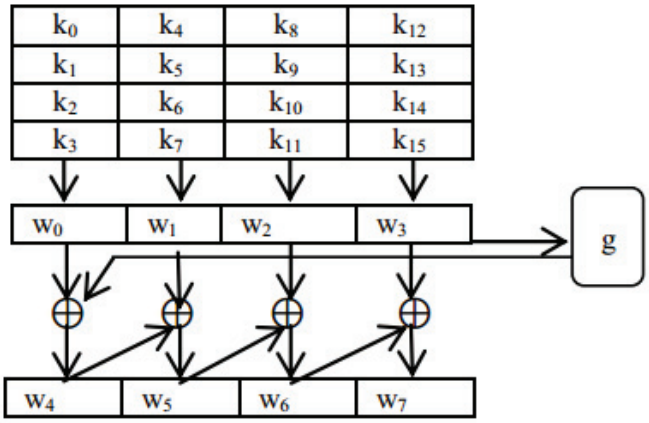

Fig. 8. Key expanding algorithms

During decryption, 4 steps of operations are there. Decryption is inverse of encryption. At end of decryption final round, cipher text converted into plain text. Both processes have different steps but similar key. They are,

i) Inverse substitute byte: It performs on each state of matrix. Substitution can done from inverse standard box (Inverse S-Box).

ii)Inv shift rows operation: In this operation, first row kept same, 2nd, 3rd and 4th row shifted cyclically right by 1 byte, 2 byte and 3 byte.

iii)Inv add round key: XOR operation performed on each state of matrix. Hence, each byte of round key and current state matrix obtained from inv shift rows is XORed.

iv)Inv mix column operation: Current state matrixes obtained from inv add round key and standard matrix obtained from polynomial multiplied.

IV. DESIGN AND IMPLEMENTATION

In designing of AES, data block of 16bytes is encoded using Verilog; top module is aes_128_encryption whose Verilog code is shown in figure 9.

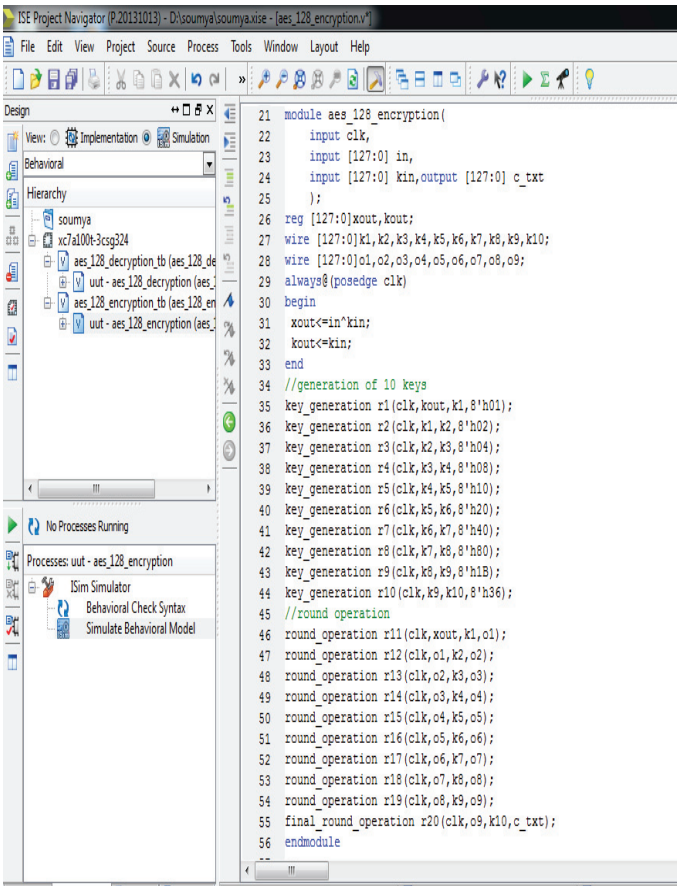

Fig. 9. Verilog code of encryption

Fig. 10. RTL schematic of AES encryption

In encryption, key generation, round and final round operation will be performed according to steps, if there is an existence of clock. RTL schematic generated using Verilog code shown in figure 10.

In decryption process, data block of 16bytes is decoded using Verilog; top module is aes_128_decryption whose Verilog code is shown in figure 11.

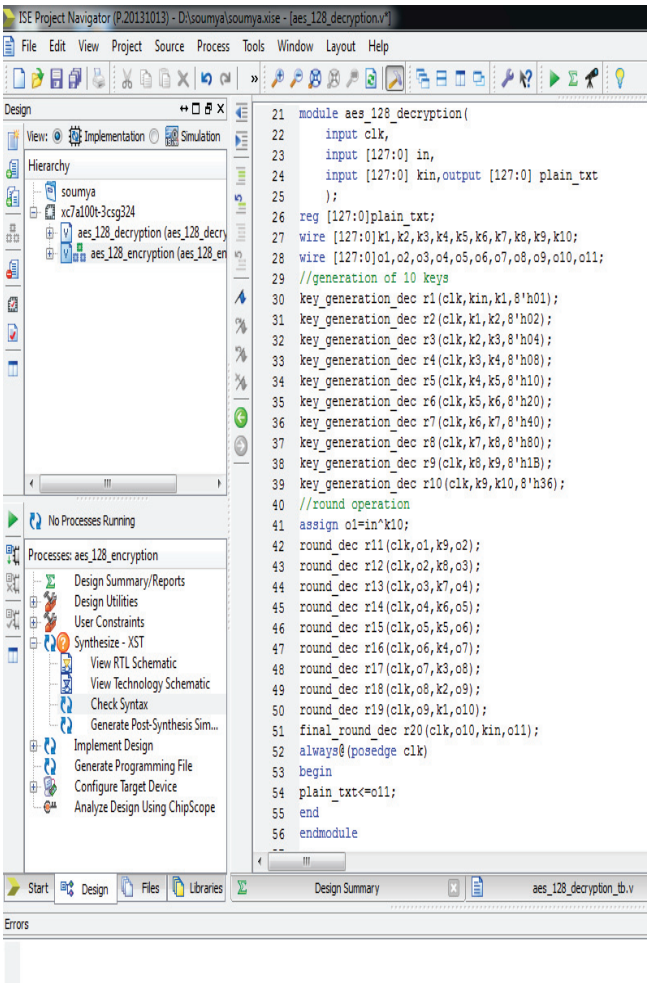

Fig. 11. Verilog code of decryption

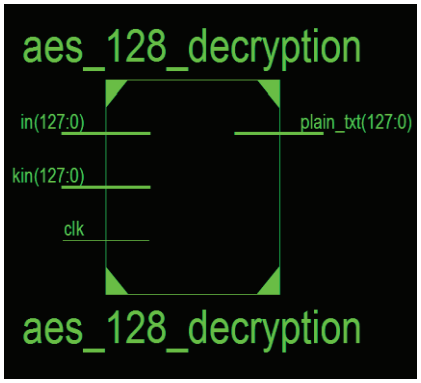

Fig. 12. RTL schematic of AES decryption

In decryption, after performing key generation, round and final round operation, if there is clock then output generated at final round will assigned to plain text. RTL schematic generated using Verilog code shown in figure 12.

V. RESULTS AND OBSERVATIONS

Simulation result of encryption shown in figure 13.

Inputs:
in=128'h54776F204F6E65204E696E652054776F, clk=1 and kin=128'h5468617473206D79204B756E67204675

Output:
c_txt=128'h29C3505F571420F6402299B31A02D73A

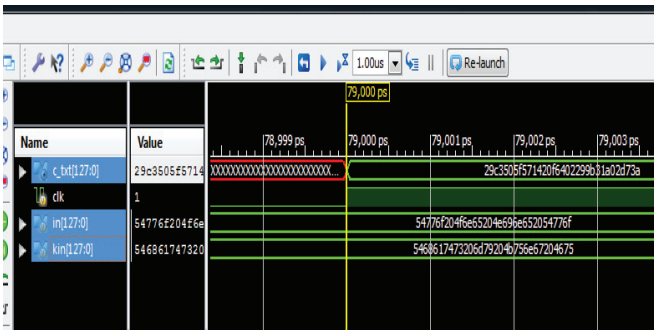

Fig. 13. Encryption simulation result

Simulation result of decryption shown in figure 14.

Inputs:
in=128'h29C3505F571420F6402299B31A02D73A (encrypted data), clk=1,
kin=128'h5468617473206D79204B756E67204675

Output:

plain_txt=128'h54776F204F6E65204E696E652054776F

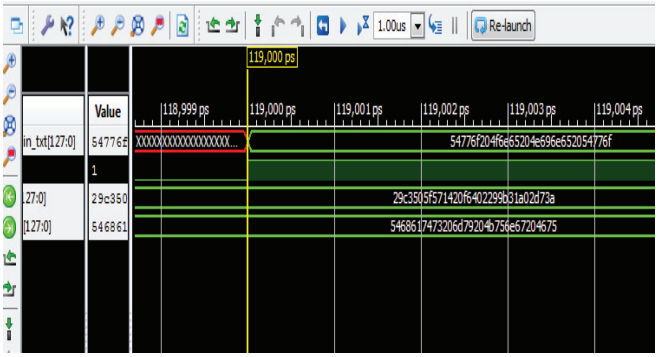

Fig. 14. Decryption simulation result

TABLE II: COMPARISON OF AES AND DES METHODS

Parameter	DES method	AES method
Key size	56bits	128bits
Data block size	64bits	128bits
Number of round operations	16	10
Number of round keys	16	10

TABLE IIII. COMPARISON OF IMPLEMENTATION OF AES-128 USING DIFFERENT PLATFORMS

Parameters	AES-128 using platform 'C' (previous work)	AES-128 using platform 'VHDL' (previous work)	AES-128 using 'Verilog' (proposed work)
Time for encryption and decryption	1792120nsec	558nsec	200nsec
Number of clock cycles required	89606	558	100

VI. CONCLUSION AND FUTURE SCOPE

In proposed AES, which is designed using Verilog results with minimised Clock cycles and operation time required for both processes, which is tabulated in comparison table.

From results its clear that, clock cycles and time are reduced using Verilog compared with VHDL. Reduced clock cycles minimises power consumption.

AES is difficult to corrupt or hack because of number of operations of round are more compared with DES. DES has only 56bits of key size than AES.

Using system Verilog, AES can be implemented for verification; compared to Verilog it has more advantages. Hardware implementation is more beneficial for high speed real time applications. It improves the flexibility.

REFERENCES

[1] J. Orlin Grabbe, "The DES algorithm illustrated".

[2] Zabina Kouser, Manish Singhal, and Amit M.Joshi,"FPGAimplementation of Advanced encryption standard algorithm", IEEE international conference on Recent advances and innovations in Engineering, (ICRAIE-2016).

[3] Shady Mohamed Soliman, Baher Magdy and Mohamed A. Abd E1 Ghany, "Efficient implementation of the AES algorithm for security applications", IEEE 2016.

[4] Mohini Mohurle and Vishal V. Panchbhai, "Review on realization of AES encryption and decryption with power and area optimization",1st IEEE Conference on power electronics, intelligent control and energy system (ICPEICES-2016).

[5] Yehya A. Nasser, Mohammad A. Bazzoun, Samih Abdul Nabi, "AES algorithm implementation for a simple low cost portable 8- bit microcontroller", IEEE 2016.

[6] Hrushikesh S. Deshpande, Kailash J. Karande, Altaaf O. Mulani, "Efficient implementation of AES algorithm on FPGA",International conference on communication and signal processing, 2014.

[7] Noura BEN HADJY YOUSSEF, Wajih EL HADJ YOUSSEF, Mohsen MACHHOUT, Rached TOURKI, and Kholdoun TOURKI, "Instruction set extensions of AES algorithms for 32-bit processors", IEEE 2014.

[8] Ayushi, "A symmetric key cryptographic algorithm", International journal of computer applications (0975-8887),Volume 1-no.15,2010.

[9] "AES 128- A C implementation for encryption and decryption", SLAA397A-July 2009.

[10] Pradhya Katkade, Dr. Mrs G. M Phade, "Application of AES algorithm for data security in serial communication".