VHDL Based Implementation of AES system using FPGA

Mr.Abhilash Donge[1], Mr.Pankaj kumar[2], Mr.Sushant kumar[3], Mr.Swapnil Ghodke[4].
[5]prof. J. Shelke,

[1234]Dept. of Electronics and Telecommunication Engineering, PJLCE, Maharashtra, India.

[5]Professor, Department of Electronics & Telecommunication Engineering, PJLCE, Maharashtra, India.

Abstract- *This project is basically designed to implement an encryption and decryption unit based on Advanced Encryption standard on a single chip by using VHDL algorithm. The basic working contains the encryption of plain text using a keyword of 128 bits as a input. Both the inputs are EX-OR and converted into state matrix of 4*4.The encryption process consist of Shifting of rows, mixing of columns for 7 rounds. After this the resultant output is EX-OR with another Keyword. This results in Cipher text of 128 bits. During Decryption, the process get reversed. Data path and control unit are designed for both cipher and decipher block, after that respective data path and control unit are integrated using structural modeling style of VHDL. Xilinx_ISE_14.2 software is being used for the purpose of simulating and optimizing the synthesizable VHDL code. The working of the implemented algorithm is tested using VHDL test bench wave form of Xilinx ISE simulator and resource utilization is also presented for a targeted Spartan3e XC3s500e FPGA*

Key Words: S-Box, Shift Row, Mix Column, Add-Round key, Inv-Sbox, Inv-Shift Row, Inv-Mixed Column, Sub bytes, Key Schedule, Control Unit.

1.INTRODUCTION

Cryptographic algorithms are utilized for security services in various environments in which low cost and low power consumption are key requirements. Wireless Local Area Networks (WLAN), Wireless Personal Area Networks (WPAN), Wireless Sensor Network (WSN), and smart cards are example of such technologies. In January 1997, The National Institute of Standards and Technology (NIST) invited proposals for new algorithms for the advanced encryption standards (AES) to replace the old data encryption standards (DES). After two round of evaluation on the 15 candidate algorithms, NIST selected the Rijendael as the AES algorithm [1] in October 2000.

1.1 ENCRYPTION

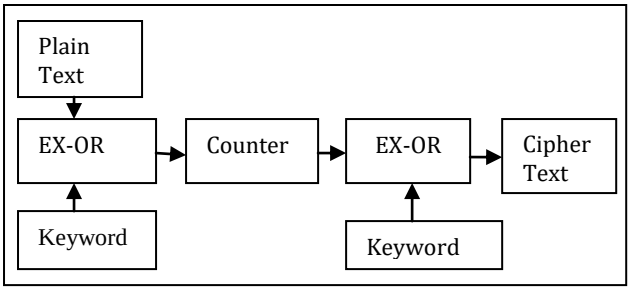


Fig-1: Block diagram of AES System

The Basic block diagram of AES System shown above explains about the working of the system. In this the two inputs plain text of 128 bits and keyword of 128 bit size are EX-OR with each other and the resultant output is replaced with the standard algorithm (Look Up Table). The encryption process is performed on this State matrix and a counter of 7 is performed. The Resultant Output is again EX-OR with the another keyword and a cipher Text is generated.

1.2 FLOW CHART

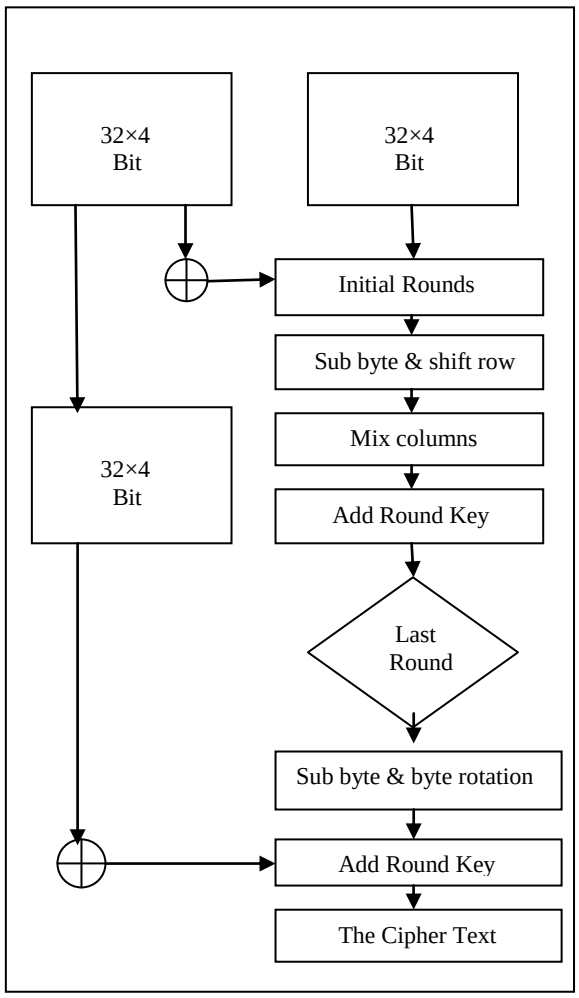


Fig-2: Flow chart of AES System.

1.3 DECRYPTION

The principle design of Advanced Encryption Standard (A (AES) is based on substitution permutation network, hi take a block of the plain text and the key as input.

The plain text is of 128 bit (32bit×4) and the cipher key is also of 128 bit. Initially the user keys are XOR with the plain text This round is called as initial round thus gives State Matrix of 4×4. On this Matrix various Operations are performed that are Sub byte and Shift row, Mix Columns and Add round key. These process are continue up to 10 rounds, The Expanded key is EX-OR with the result of tenth round. After that we get the Cipher Text.

2.1 S-BOX TRANSFORMATION

The Sub-byte transformation is a non-linear byte substitution that operates independently on each byte of the state using a substitution table.

	0	1	2	3	4	5	6	7	8	9	A	b	c	d	E	F
0	63	7c	77	7b	f2	6b	b6	c5	30	01	67	2b	fe	d7	Ab	76
1	Ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	d7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	a2	eb	27	b2	75
4	09	83	2c	1a	1d	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	Cf
6	d0	ef	aa	fb	43c	4d	33	85	45	f9	07	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	Cd	0c	13	ec	5f	97	44	17	c4	a7	79	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	Db
A	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
B	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	Ae	08
C	Da	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
D	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
E	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	Df
F	8c	a1	89	0d	bf	e6	42	684	411	99	2d	0f	b0	54	Bb	16

Fig-3: Look up table.

For example, if s1,1={53}, then substitution value would be determined by the intersection of the row with index '5' and the column with index '3' in figure 3. This result in s'1,1 having a value of {ed}.

2.2 SHIFT ROW TRANSFORMATION

In the shift row transformation, the byte in the last three rows of the state are cyclically shifted over different number of byte (offset).the first row, r=0, is not shiftedThe shift row transformation is proceed as follows:

S'r,c = Sr,(c+shift(r,Nb))mod Nb for 0<r<4 and 0≤c≤Nb.

s S

S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3
S2,0	S2,1	S2,2	S2,3
S3,0	S3,1	S3,2	S3,3

Fig 4:- Original Matrix

This has the effect of moving bytes to "lower" position in the row (lower value of C), while the "lowest" bytes wrap round into the "top" of the row (higher value of 'C' in a given row).

S'

S0,0	S0,1	S0,2	S0,3
S1,1	S1,2	S1,3	S1,0
S2,2	S2,3	S2,0	S2,1
S3,3	S3,0	S3,1	S3,2

Fig 5:- After shifting cyclically.

2.3 MIX COLUMNS TRANSFORMATIONS

The Mixed columns transformation operates on the state column by column as a four term polynomial. The column are consider as polynomials over GF(2^8) and multiplied modulo x^4+1 with a fixed polynomial a(x), given as follows.

a(x) ={03}x^3 +{01}x^2 +{01}x +{02}.

This can be written in matrix form as follows.
S'(x) = a(x) XOR s(x)

$$\begin{bmatrix} S'0,c \\ S'1,c \\ S'2,c \\ S'3,c \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S0,c \\ S1,c \\ S2,c \\ S3,c \end{bmatrix}$$

The Mix-column transformation is as follows,

S

S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3
S2,0	S2,1	S2,2	S2,3
S3,0	S3,1	S3,2	S3,3

S'

S'0,0	S'0,c	S'0,2	S'0,3
S'1,0	S'1,c	S'1,2	S'1,3
S'2,0	S'2,c	S'2,2	S'2,3

S'3,0	S'3,c	S'3,2	S'3,3

For $0 \leq C < Nb$ (Nb = 4 for 128 -bit)s

2.4 ADD ROUND KEY TRANSFORMATION

In this transformation, a round key is added to the state by a simple XOR operation. Each Round key is consist of Nb words from the key schedule and this words are each added into the columns of state, such that,

For example,

Round 0 = (output of mix column) XOR (round key)

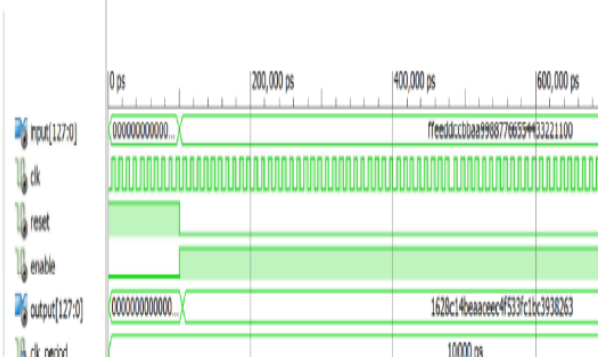
This process is continues up to the 10th round.

2.5 KEY EXPANSION

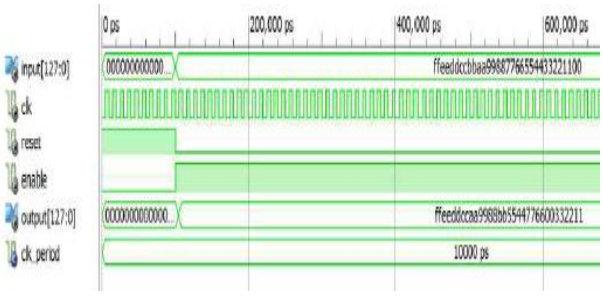
The AES algorithm takes the cipher key, k and performs a key routine to generate a key schedule. The key expansion generates a total of Nb (Nr+1) words: The algorithm requires an initial set of Nr rounds requires Nb words of key data. The resulting key schedule consists of a linear array of 4-byte words.

3. OUTPUT:

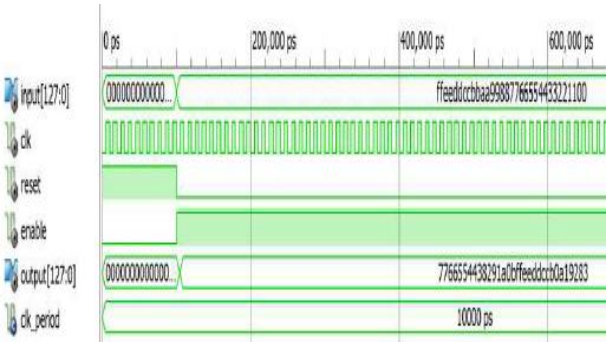
3.1 BYTE SUBSTITUTION-



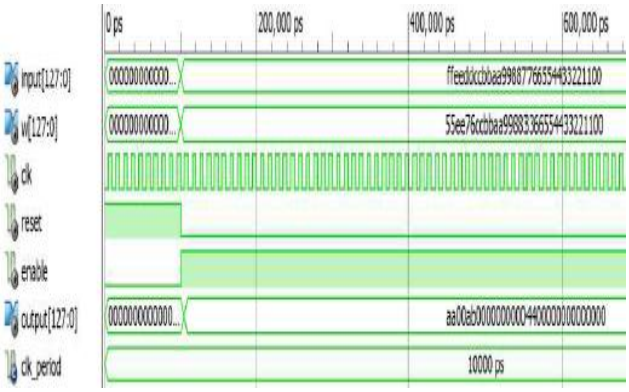
3.2 SHIFT ROW-



3.3 MIX COLUMN-



3.4 ADD ROUND KEYS-



4. CONCLUSIONS

Here, the development of AES encryption part has been performed using VHDL code and the resultant outputs are given above. The physical implementation of the design is conducted using FPGA ALTERA MAX300A device. The main advantage of encryption part is saving of area by reordering of sub bytes and shift rows which are the process of calculating 4 bytes of data.

REFERENCES

1. ADVANCED ENCRYPTION STANDARD, Federal Information Processing Standards Publication 197, November26,2001

2. FIPS 197, "Advanced Encryption Standard" http://www.ratchkov.com/vpn/aes/aes.html RIJNDAELhttp://www.cs.mcgill.ca/~kaleigh/computers/crypto_rijndael.html The Laws of Cryptography http://www.cs.utsa.edu/~wagner/laws/

3. Computer Security Objects Register (CSOR): http://csrc.nist.gov/csor/

4. A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 1999.

5. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York,1997,p.81-83

6. J. Nechvatal, et. al., Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.