ISSN No: 2348-4845
International Journal & Magazine of Engineering,
Technology, Management and Research
A Peer Reviewed Open Access International Journal

Prominent Advanced Encryption Standard with High Throughput

V.Tejaswini
M. Tech (ECE),
Department of ECE,
Guntur Engineering College,
Guntur, Andhra Pradesh, India.

Sri V.Santhi Sri
Associate Professor
Department of ECE,
Guntur Engineering College,
Guntur, Andrapradesh, India.

ABSTRACT

Eminent throughput architecture is proposed for an efficacious implementation of the Advanced Encryption Standard (AES) Algorithm. The presented architecture can be adapted for AES Encryption as well as and Decryption with novel integrated AES encryptor/decryptor designs. In our method the 128 bits can be divided in to the two basic parts namely lower and higher parts, apart from the traditional AES in our method we perform the operations only at the lower part. The operations such as Sub Bytes/InvSubBytes substitutionsand XORed at the each stage will get normal AES operation but the computations can be reduced by half. The proposed architecture downplays the critical path delay through the alteration of the SubBytes/InvSubBytes as well as the Key Expansion modules.

INTRODUCTION

Reliable commutations are necessary when the internet, wireless communications and high security communications are increasing in past ten years, for such applications the Advanced Encryption Standard (AES) algorithm is the promising solution. This Advanced Encryption Standard (AES) algorithm can be approved by the National Institute of Standards and Technologies in October 2000 for the more flexible and high security applications.128 to 256 which can be performed the several iteration rounds to provide the novel encryption.

In this process various modifications towards the each level of the AES encryption and decryption right from the byte substation to the end round stage. These are majorly concentrated towards less computation, decreasing the critical path delay and reduction of the area.

This paper organizes as follows.In Section I deal with the introduction, followed by the session II that deals with Advanced Encryption Standard Algorithm, Session III covers proposed method, Results and analysis of our architecture with the proposed techniques is covered in Section IV andfollowed by conclusion and references.

AES ALGORITHM

The term cryptography refers as the converting the data in to the unreadable format for the secure data transmission, that can be done by converting the plane text can be converted into cipher text at the transmission end and that can be transmitted through the channel and the cipher text can be reconverted into the plane text (original text).

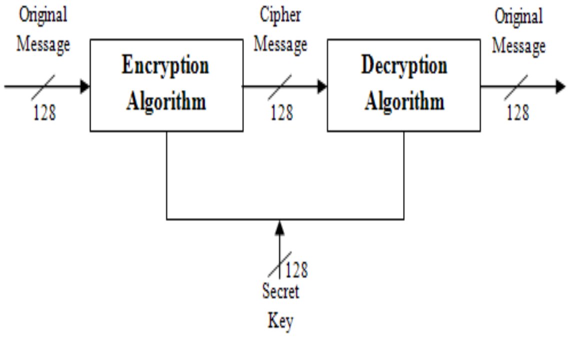


Fig1: Basic Block Level Cryptography

There were different cryptography algorithms can used before like ECC, RSA, DES but there are some drawbacks like less secure and more complex for that the AES can be projected as promising approach. The

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used provide the secure data transmission.

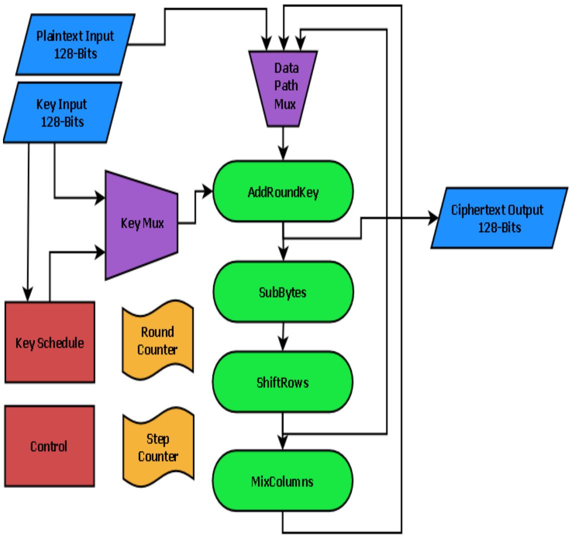


Fig2: AES algorithm

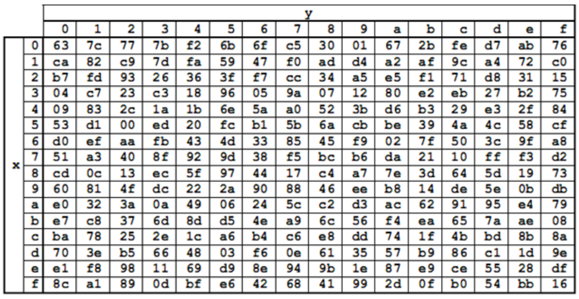
As from the above the plane text and the key can be given to the each stage individually. As per the normal standards 10 to 14 levels can be performed. For the each level operation we need the key for the each level, for that key box can be taken and input key can be XORed to form the specific level keys. Each stage can be cascaded form the first stage to final stage; at the end final end round operation can be performed.

Each stages of the AES encryption and the decryption composeof the basic four different byte-oriented operations:

- Byte substitution using a substitution table (S-box)
- Shifting rows of the State array by different offsets
- Mixing the data within each column of the State array
- Adding a Round Key to the State

Sub byte substitution

In order to perform the sub byte substitution the input data can be divided several sub bytes and that can be given as the input to the each module of the sub byte substitution



		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	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	b7	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	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	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	43	4d	33	85	45	f9	02	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	7e	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	ba	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	68	41	99	2d	0f	b0	54	bb	16

Fig3: S-Box

In substitution module the input can be taken and that will give as the input for the S-Box, this S-Box can be formed by the user defined data bytes. The input data given as the address of this module and this can be given the specified data as the output.

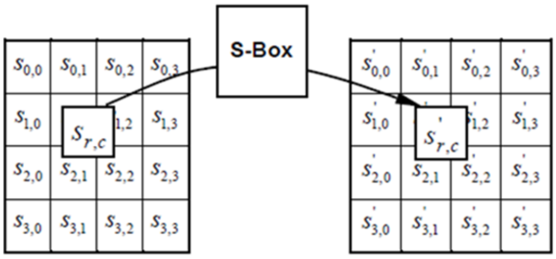


Fig4:Sub byte substitution

Shift Rows Transformation

The data formed in the matrix format the total 128 bit data divided into 8-sub bytes, with that we can forms 8*8 matrix.

In shifting rows first row will not be shifted, second row shifted by one circular left shift, third row shifted by two circular left shifts and last row will be three timescircular left shift.

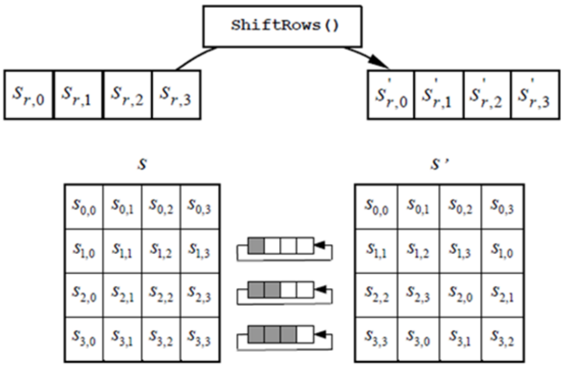

ShiftRows()
$s_{r,0}$
$s_{r,1}$
$s_{r,2}$
$s_{r,3}$
$s'_{r,0}$
$s'_{r,1}$
$s'_{r,2}$
$s'_{r,3}$
s
s'
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,1}$ $s_{1,2}$ $s_{1,3}$ $s_{1,0}$
$s_{2,2}$ $s_{2,3}$ $s_{2,0}$ $s_{2,1}$
$s_{3,3}$ $s_{3,0}$ $s_{3,1}$ $s_{3,2}$

Fig5:Shift Rows Transformation

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Mix Columns Transformation

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

In mix colums the data after shifting rows will be taken and the operations can be performed basedon the below shown. In mix columns majorly multiplication and the XOR can be performed inbetween the internal rows of the matrix.

$S'_{o,c}=(\{02\}*S_{o,c}) \wedge (\{03\}*S_{1,c}) \wedge\ S_{2,c}\wedge S_{3,c}$
$S'_{1,c} = S_{0,c}\wedge (\{02\}*S_{1,c}) \wedge (\{03\}*S_{2,c}) \wedge\ S_{3,c}$
$S'_{2,c} = S_{0,c}\wedge\ S_{1,c} \wedge(\{02\}*S_{2,c}) \wedge (\{03\}*S_{3,c})$
$S'_{3,c} = (\{03\}*S_{o,c}) \wedge\ S_{1,c}\wedge S_{2,c}\wedge (\{02\}*S_{3,c})$

From the above equations the operations can be performed and produces the same bit length there by the novel and more secure cryptography can be achieved.

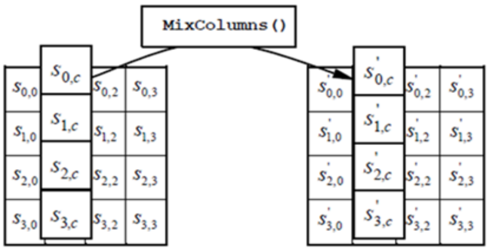


Fig6:Mix columns Transformation

AddRound Key Operation

In the final stage add round operation can be performed in this the data from the Mix column can be taken and that will be XORed with key matrix finally produces the encrypted data for the transmission.

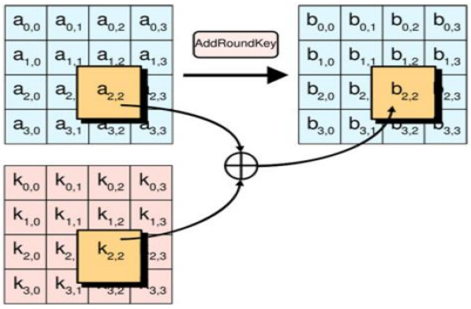


Fig7:Add round operation

PROPOSED METHOD

In normal AES methods the above discussed algorithms can be followed there by the gate count will be increased because when we perform the pipelining operation we require individual S-Boxes will be required, in mix column we perform two multiplication operations.

In order to avoid the drawback of the pervious method we need to reduce the multiplications or the non-pipelining structure can be only alternative but when the multiplications is removed the novelty in security will be reduced where as for non-pipelining consumes the more operation time.

The problems that we discussed in above will be important considerations for all AES methods, for that we proposes new method for the more accuracy, less critical path delay with lesser extent footprint.

In our method the 128 bits can be divided in to the two basic parts namely lower and higher parts, apart from the traditional AES in our method we perform the operations only at the lower part, at each level after completing operation with lower part that will be XORed with the upper part. That will maintain the accuracy and security level. And more over in Mix column we are using the novel method rather than traditional AES. In mix column ADD-XOR operations performed in our method.

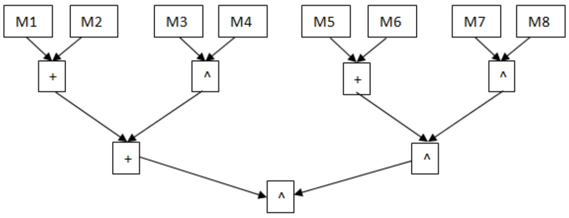
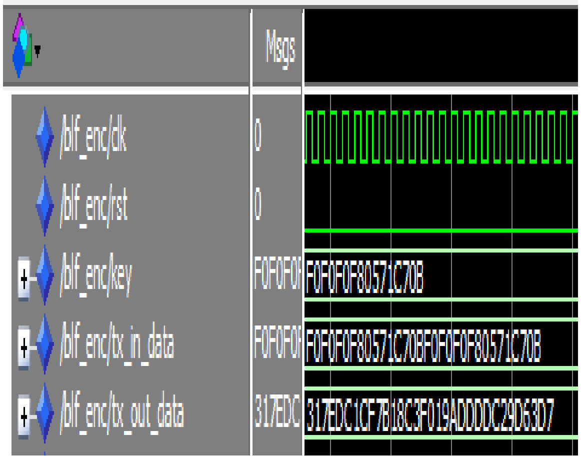


Fig8: proposedMixColumns Transformation operation

RESULTS AND DISUSSION

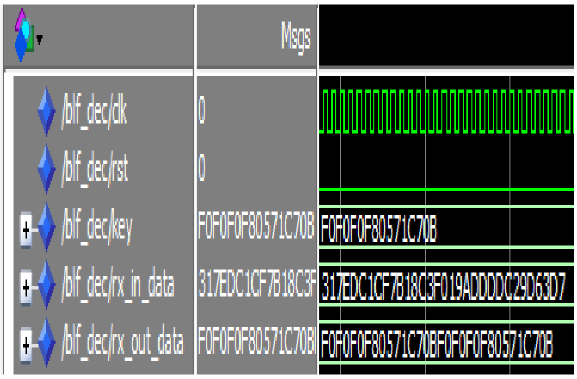
The design of the AES encryptor/decryptor designed using VHDL and logically verified using and MODELSIM.Principally we designed AES encryptor and then AES decryptor block is cascaded to acquire top module. Thesimulation results are as shown in below fig. We applied 128’ h F0F0F0F80571C70BF0F0F0F80571C70B 128 bit data and 64’h F0F0F0F80571C70B key hence our proposed algorithm performs the 16 stage operation then it given the 128’h317E_DC1C_F7B1_8C3F_019A_DDDD_C29D_63D7 output.



```
                          Msgs
/blf_enc/clk              0
/blf_enc/rst              0
/blf_enc/key              F0F0F0F   F0F0F0F80571C70B
/blf_enc/tx_in_data       F0F0F0F   F0F0F0F80571C70BF0F0F0F80571C70B
/blf_enc/tx_out_data      317EDC    317EDC1CF7B18C3F019ADDDDC29D63D7
```

Fig: Encoder output

The output of the encoder applied to the decryptor along with the same key given for the encryptor then we got the original input data before encryption.



```
                          Msgs
/blf_dec/clk              0
/blf_dec/rst              0
/blf_dec/key              F0F0F0F80571C70B   F0F0F0F80571C70B
/blf_dec/rx_in_data       317EDC1CF7B18C3F   317EDC1CF7B18C3F019ADDDDC29D63D7
/blf_dec/rx_out_data      F0F0F0F80571C70B   F0F0F0F80571C70BF0F0F0F80571C70B
```

Fig: Decoder Output

CONCLUSION

In our proposed method AES designed using novel method concentrated on the less utilization of block RAMs for the sub byte substitution and modifications in the Mix column transform.We got normal AES operation but the computations can be reduced by half. The proposed architecture downplays the critical path delay through the alteration of the SubBytes/InvSubBytes as well as the KeyExpansion modules.

REFERENCES

[1] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," 2001.

[2] S. K. Mathew, et al. "53 Gbps native GF(24)2 composite field AES-encrypt/decrypt accelerator for content-protection in 45nm highperformancemicroprocessors,"IEEEJournalOfSolid-StateCircuits,vol.46,no.4,pp.767-776,April2011.

[3] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Efficient highperformance parallel hardware architectures for the AES-GCM,"IEEETransactions on Computers, vol. 61, no. 8, pp. 1165-1178, August2012.

[4] S.-F. Hsiaso, M.-C. Chen and C.-S. Tu, "Memory-free low cost Designs of Advanced Encryption Standard using commonsubexpression elemination for subfunctions in transformations,"IEEETransactions on Circuits and Systems, vol. 53, no. 3, pp. 615-626,March 2006.

[5] X. Zhang and K. K. Parhi, "High speed VLSI architectures for theAES algorithm,"IEEE Transactions on Very Large Scale Integration(VLSI) Systems, vol. 12, no. 9, pp. 957-967, September 2004.

[6] S. K. Reddy S, R. Sakthivel and P. Praneeth, "VLSI implementation of AES crypto processor for high throughput,"International Journal ofAdvanced Engineering Sciences and Technologies, vol. 6, no. 1, pp.022-026, 2011.

[7] J. Chu and M. Benaissa, "Low area memory-free FPGAimplementation of the AES algorithm," in 22nd InternationalConference on Field Programmable Logic and Applications, pp. 623626,August2012.

[8] T. A. Pham, S. H. Mohammad and H. Yu, "Area and powerOptimisation for AES encryption module implmentation on FPGA," in18th International Conference on Automation and Computing, pp. 1-6,September 2012.

[9] J. M. Granado-Criado, M. A. Vega-Rodríguez, J. M. Sánchez-Pérezand J. A. Gómez-Pulido, "A new methodology to implement the AESalgorithm using partial and dynamic reconfiguration,"Integartion, theVLSI Journal, vol. 43, pp. 72-80, January 2010.

[10] K. Rahimunnisa, P. Karthigaikumar, S. Rasheed, J. Jayakumar and S.SureshKumar, "FPGA implementation of AES algorithm for highthroughput using folded parallel architecture," Journal ofSecurity andCommunication Networks, vol. 5, no. 10, October 2012.