International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 11047-11058

http://www.ripublication.com

Secured High Throughput of 128-Bit AES Algorithm Based on Interleaving Technique

Litty M Raju[1], M.Sumathi[2]
[1]M.Tech (VLSI Design),
Sathyabama University, Chennai-119, India
littyraju9@gmail.com
[2]Professor
Department of Electronics & Control Engineering
Sathyabama University, Chennai-119, India
sumagopi206@gmail.com

Abstract

This paper describes the 128-bit AES algorithm based on interleaving technique in order to reduce the logic elements used in encryption and decryption. The logic elements reduced from 38386 of the existing AES to 6386. AES is one of the widely used security algorithm for Network Security. Due to the presence of brute force attack, there is chance of hacking the data during transmission and reception. In order to improve security and performance, this paper discusses about hiding the data in an image after encryption. The image is processed using MatlabR2009b. The software implementation of AES has been made using Verilog HDL and ModelSim 6.3g_p1. The performance factors of Throughput, Power consumption and Operating frequency have been observed using Quartus II software. Implementation of proposed AES increases the throughput and reduces the power.

Keywords: Cryptography, AES algorithm, Encryption, Decryption, Interleaver, Data hiding

Introduction

The increase in the usage of internet and growth in wireless communication has led to a situation where security should be given importance. In order to improve security cryptographic algorithms has been developed. In all the cryptographic algorithms encryption and decryption takes place. Cryptography is the art of transforming the data into another form which cannot be read by the persons for whom the data is not intended. This procedure is known as encryption. The data which we get after

encryption is known as cipher text. The cipher text along with the key is decrypted to retain the original data. This decryption procedure can be done only by the persons for whom the data is intended. Advanced Encryption Standard (AES) algorithm is one of the cryptographic algorithms. AES has been developed to replace all the previous cryptographic algorithms.

AES Algorithm

The National Institute of Standards and Technology (NIST) have issued a call for an Advanced Encryption Standard (AES) algorithm which can overcome the drawbacks of 3DES in the year 1997. In the span of 5 years NIST received 15 algorithms. In the year 2001, NIST selected Rijndael as the proposed AES algorithm. Rijndael was proposed by Dr Joan Daemen and Dr Vincent Rijmen. Both of them are cryptographers from Belgium. The AES algorithm is having a block length of 128 bit data with different key sizes as 128 bit, 192 bit and 256 bits. The 128 bit requires 10 rounds of operation, 192 bit requires 12 rounds of operation and 256 bit requires 14 rounds of operations. [1]-[5]. AES uses a symmetric key and a block cipher. Symmetric key is the key which is same for encryption and decryption. Block cipher acquires outsized number of bits and encrypt them as a single unit. AES is not a feistel structure. In feistel structure half of the data is used to modify the other half and then the halves are swapped. The overall structure of AES in shown in figure.1

The structure is simple.Both encryption and decryption starts with add round key. It is followed by 9 consecutive rounds. Each round consists of all the four stages. The last round consists of 3 stages.Mix columns will not be there in last round.There are four stages in each round of AES algorithm. The four stages are given below

1. 1.Substitute bytes
2. 2.Shift rows
3. 3.Mix columns
4. 4.Add round key

The structure is simple.Both encryption and decryption starts with add round key.It is followed by 9 consecutive rounds. Each round consists of all the four stages. The last round consists of 3 stages.Mix columns will not be there in last round.

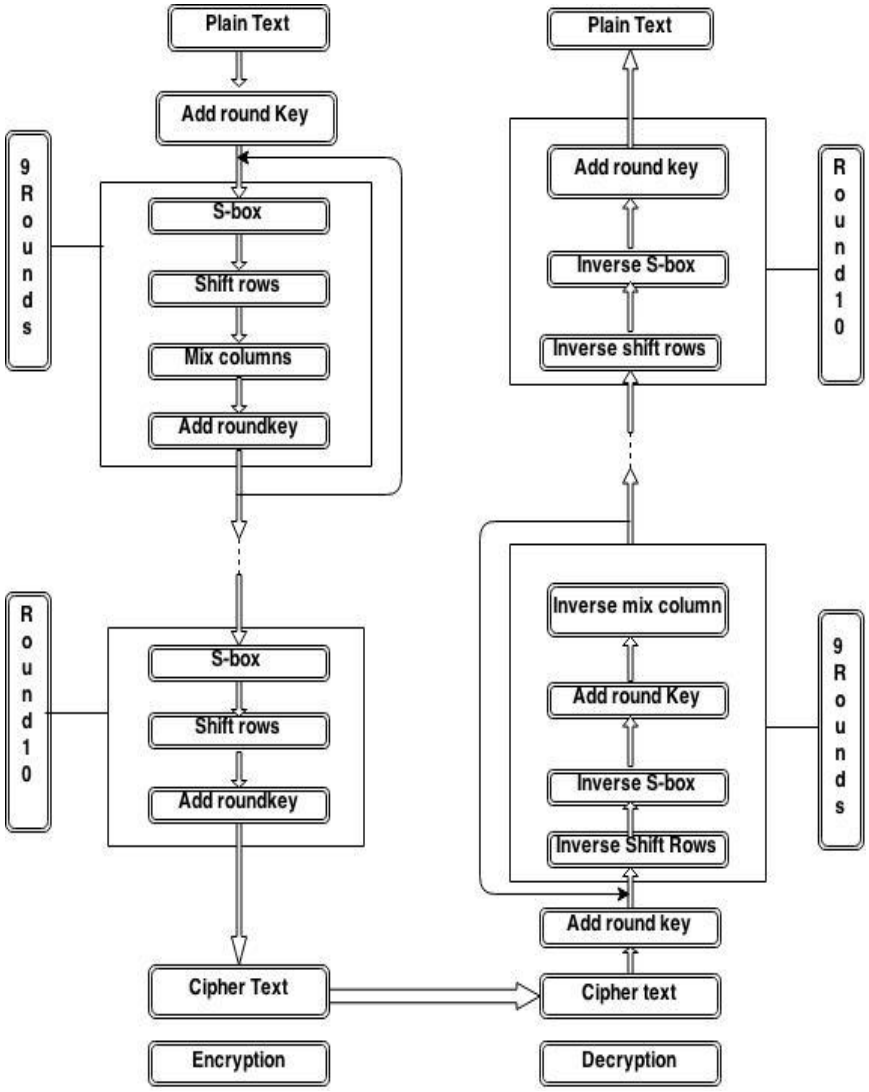
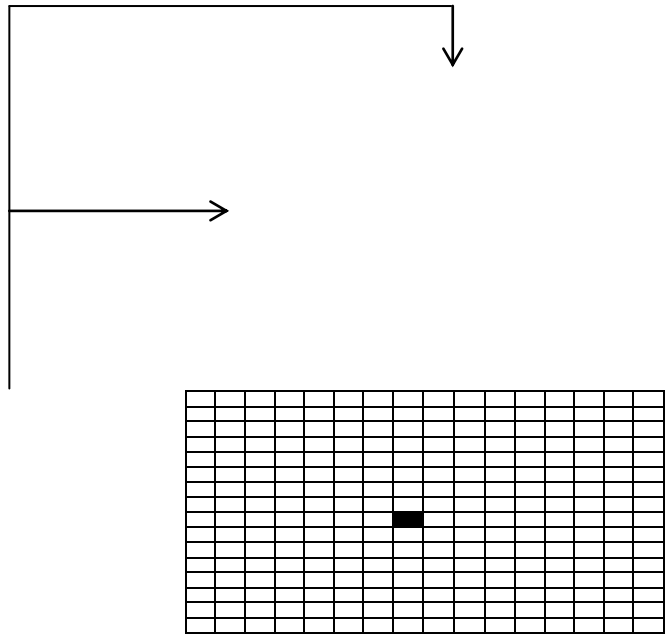


Figure 1: AES Encryption and Decryption

(A) Substitute bytes transformation

The substitution bytes which is also known as subbytes, is a simple look up table. It is shown in figure.2.AES defines a 16*16 matrix of byte values, which is called s-box. It contains a permutation of all possible 256, 8-bit values. In the given state each individual byte is transformed into new byte in the following way- the left most 4 bits are used as row value and the right most 4 bits are used as column value. The subbyte transformation is shown in following figure 2. In the given example B is considered as the right most 4 bits and I is considered as the left most 4 bits. Each of A and B are mapped with the s-box and we will get BI' as the output.



AE	BI	CM	DA
EI	FM	GC	HV
TI	JH	KG	LW
MJ	NG	OH	PI

AE’	BI’	CM’	DA’
EI’	FM’	GC’	HV’
TI’	JH’	KG’	LW’
MJ’	NG’	OH’	PI’

Figure 2: Substitute byte transformation

(B) Shift rows transformation

In shift rows,the rows are shifted. The first row will not be shifted. Second row will be shifted by one byte circularly in left direction, third row is shifted by two bytes circularly in left direction and fourth row is shifted by 3 bytes. It is shown in figure 3.

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

NO SHIFT

A	B	C	D
F	G	H	E
K	L	I	J
P	M	N	O

Figure 3: Shift row transformation

In inverse shift rows, the rows are shifted circularly in opposite direction. The first row will not be shifted. Second row is circularly shifted by one byte in right direction. For third row, a 2-byte circular right shift is performed. For fourth row, a 3-byte circular right shift is performed [6]-[10].

(C) Mix columns transformation:

In mix column, the transformation is performed on columns of the matrix. The first column will not be changed. The remaining columns will be changed in the following format. It is shown in figure 4.

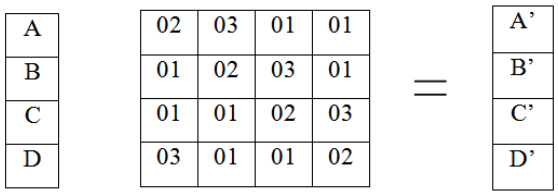


Figure 4: Mix columns transformation

A' = (A*02) xor (B*03) xor (C*01) xor (D*01) [1]

B' = (A*01) xor (B*02) xor (C*03) xor (D*01) [2]

C' = (A*01) xor (B*01) xor (C*02) xor (D*03) [3]

D' = (A*03) xor (B*01) xor (C*01) xor (D*02) [4]

The multiplication with (02) can be performed as, 1 bit left shift of the given 8 bit data and then a bitwise xor operation with (0001 1011). Bit wise xor operation should be performed only if the leftmost bit of the original value is 1 before the shift. If the leftmost bit is not 1 before the shift then the value should be left as it is after the shift. The multiplication of x with (03) is performed as {x xor (x*02)}.

The inverse mix columns are performed by using the following formulae. Inverse mix column transformation is shown in figure 5.

A' = (A*0B) xor (B*0B) xor (C*09) xor (D*0E) [5]

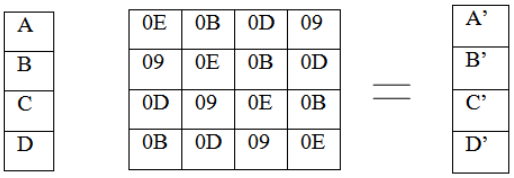


Figure 5: Inverse mix column transformation

(D) Add round key transformation:

In add round key transformation, the 128 bits are XORed with 128 bits of the round key.

S' = S xor R [6]

Where S' = state after adding round key
S = state before adding round key
R = round key

Existing Methodology

Advanced Encryption Standard (AES) uses a symmetric block cipher for encryption and decryption of data. Block cipher acquires an outsized number of bits and encrypt them as a single unit. In the existing methodology hardware implementation of AES has been done. The architecture of existing methodology is shown in the below figure 6.

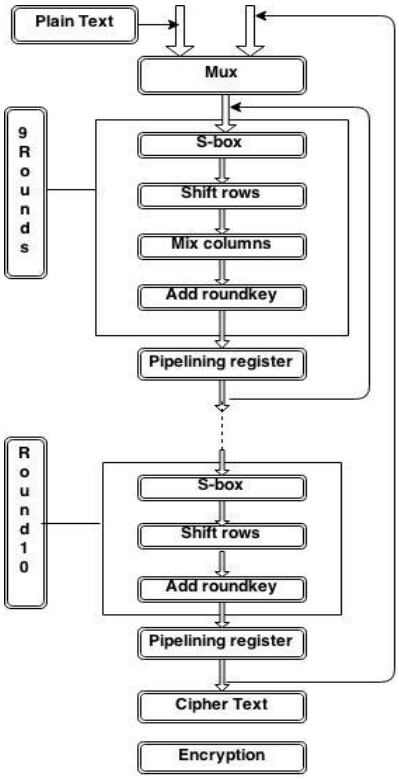


Figure 6: Pipelined architecture of AES

In the pipelining architecture of AES, multiplexer is used for selection between plain text, key and output from the previous round. If selection line is high, then the multiplexer selects the plain text and key. If the selection line is low then the output of the previous round will be selected. The output from multiplexer is given to s-box which uses a look up table for its operation. The output from s-box is given to shift rows. The output from shift rows is given to mix columns. The output from mix columns is given to add round key. The final output from add round key has been given to pipelining registers. This completes the first round. [11]-[15]

Likewise nine more rounds will be performed. Last round will not have mix column transformation. Speed is an important factor in most of the applications. In order to increase the speed of AES algorithm, pipelining register has been used after each round. The drawbacks can be stated as, use of pipelining architecture increase

the hardware architecture of AES. So the pipelining registers need to be used very carefully without increasing the size of hardware.Use of look up table in s-box increases the area and security is not high.

Proposed Methodology

In proposed methodology, interleaver has been used instead of look up table in substitute box. Interleaver is the technique of interchanging the data. Use of interleaver increases the performance of substitute box. Use of interleaving tecchnique decreases the power consumption.

AES is a secured algorithm, but with the effect of attacks like brute force attack and dictionary attack, there are chances of hacking the data. If the length of the key is small then one can hack the data using brute force attack. If the length of key is large then the data can be hacked using dictionary attack. So in order to make the AES more secure, a new method has been used in this paper. The method is to hide the cipher text in an image. By mixing the data with image it will be difficult to identify which one is data and which one is pixel. By doing this security will be increased. The diagrammatical representation of the proposed methodology is shown in figure 7.

As shown in the figure, the output from multiplexer is given to s-box which uses an interleaver for its operation. The output from s-box is given to shift rows. The output from shift rows is given to mix columns. The output from mix columns is given to add round key. The final output from add round key has been given to pipelining registers. This completes the first round. Likewise nine more rounds will be performed. Last round will not have mix column transformation. Thus the cipher text which has been obtained from encryption is hidden in an image. After hiding the cipher in image, it is extracted and is given for decryption. In decryption the inverse of s-box, inverse of shift rows, inverse of mix columns and add round key operation will be performed.

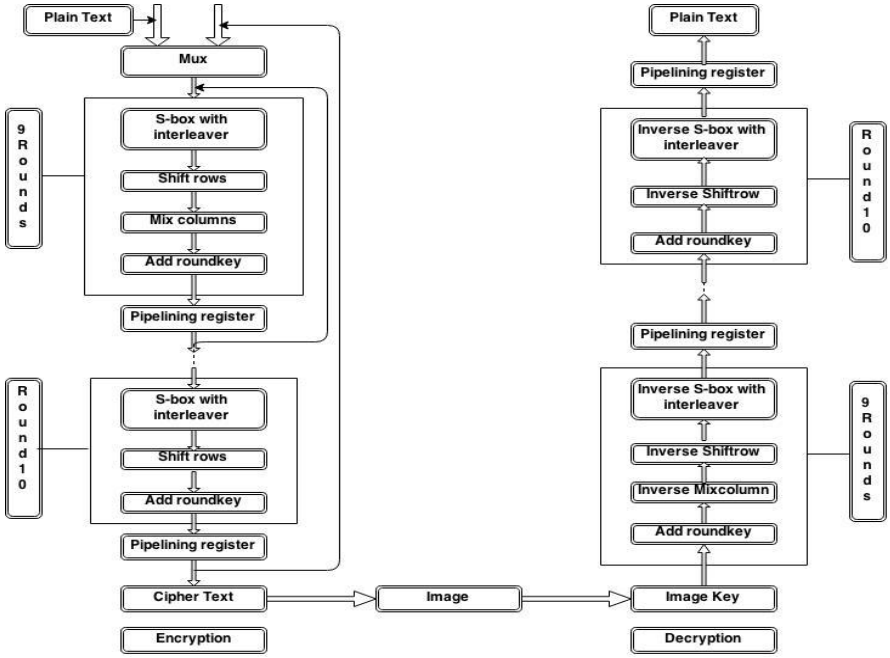


Figure 7: AES Encryption and Decryption with Interleaver

Implementation Results

The AES algorithm is implemented using Verilog and simulated using model sim 6.3g. Simulation of 128 bit AES encryption and decryption has been done. AESALGORITHM is a 128 bit data which is considered as the plain text. A 128 bit key is taken. Both the plain text and key are given as input to the encryption procedure. The simulation graph is shown in figure 8.

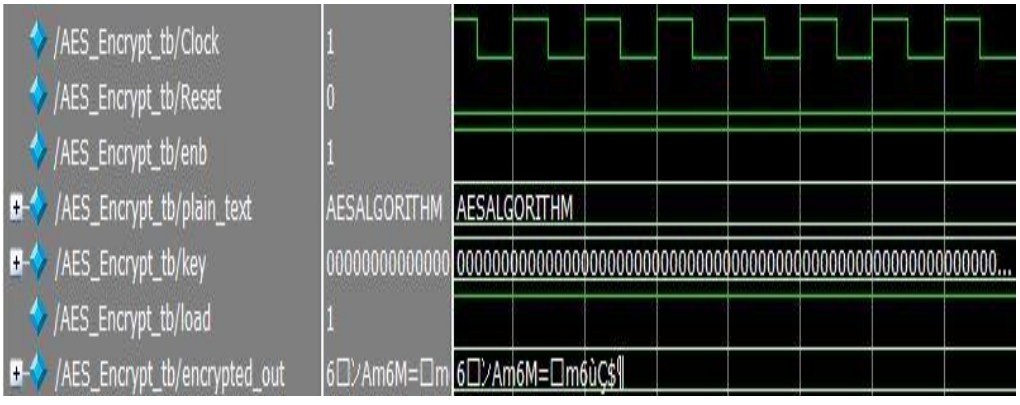


Figure 8: Encryption Simulation

The output of the encryption procedure, cipher text is hided in an image to increase the security. The image in which the data is hidden is shown in figure 9. It is done using MATLAB.

Figure 9: Data hidden image

The decryption is implemented using Verilog HDL and model sim. The cipher text which is extracted from the image is given as input to the decryption. The decryption simulation is shown in figure 10.

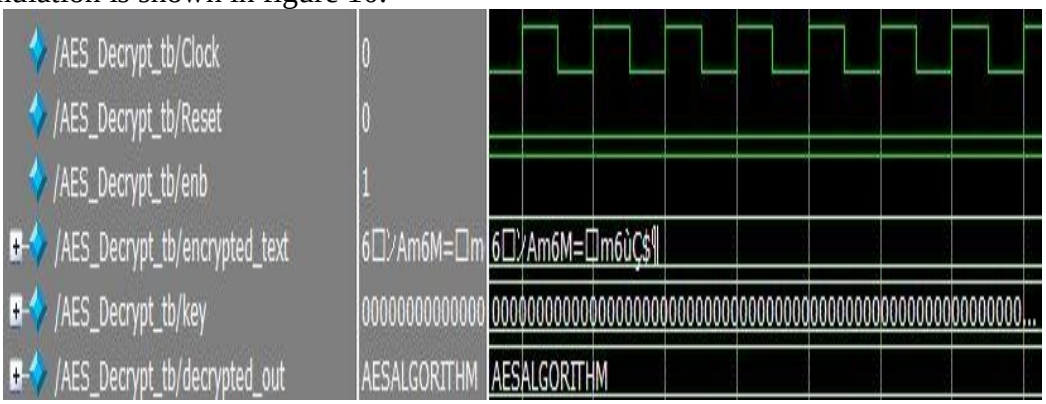


Figure 10: Decryption simulation

The performance parameters like area, power consumption, frequency throughput are observed using quartus software. It is tabulated in table 1.

Table 1: Performance parameters

Performance parameters	Existing AES	Proposed AES
Total logical elements	38,386	6386
Power dissipation	1074.11mW	225.38mW
Frequency	194.74Mhz	460.41Mhz
Throughput	800Mbytes/sec	980Mbytes/sec

Throughput of the proposed AES is higher than the existing AES which is shown in table 1. It is calculated using the formula

$$\text{Throughput} = \frac{\text{Number of bits} * \text{Clock frequency}}{\text{Clock cycle}} \quad [7]$$

When compared to reference paper [7] and existing AES, the proposed AES utilised more frequency. It indicates that operation requires only less time for simulation. Throughput is also high for proposed AES when compared with existing AES. The graphical representation is shown in figure 11 and figure 12.

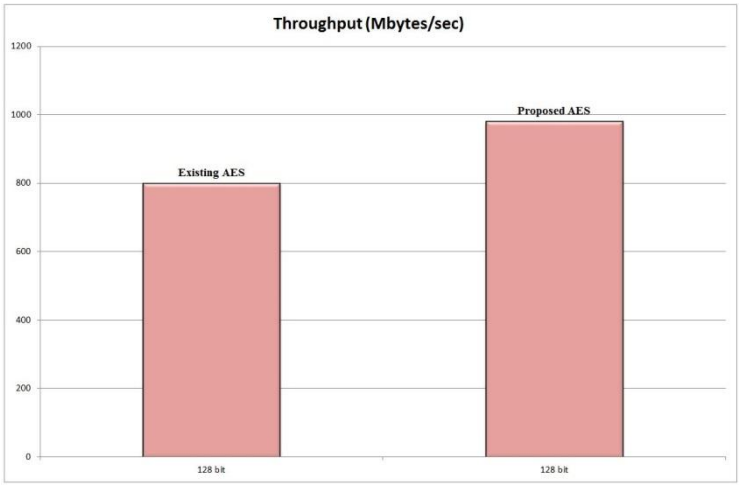


Figure 11: Comparison of throughput

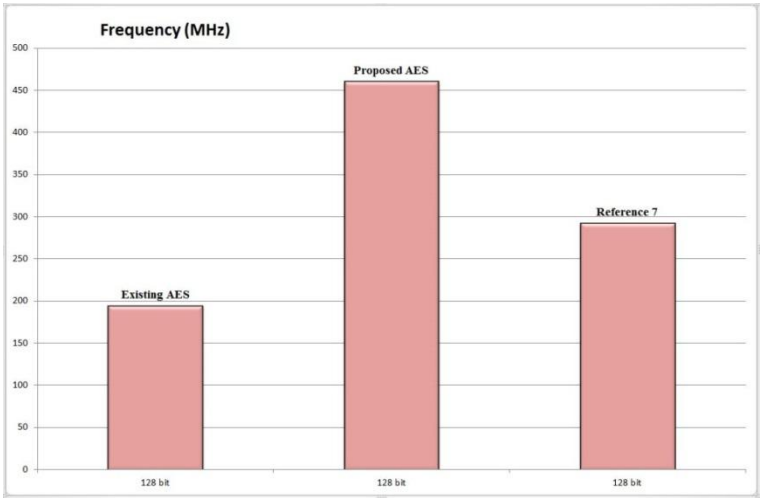


Figure 12: Comparison of frequency

Conclusion

This paper presented a new structure of AES algorithm which makes use of interleaving technique in s-box. The cipher text has been hided in an image in order to increase security. The encryption and decryption are designed using Verilog HDL and simulated using ModelSim. Image has been designed using MATLAB. Performance parameters are analysed using Quartus -II software. From this study, it has been observed that enhanced AES algorithm used only 6386 logic elements instead of 38386 in pipelined AES algorithm. It requires only less area in hardware implementation. The proposed algorithm can be used and suitable for high speed applications by the improved results of throughput and power dissipation.

References

[1]. M. Vanitha, R. Sakthivel, Subha, "Highly Secured High Throughput VLSI Architecture for AES algorithm", IEEE, vol. 1, issue 7, 2012

[2]. Xinmiao Zhang, Keshab K Parhi, "High-Speed VLSI Architectures for the AES Algorithm", IEEE, vol. 12, no. 9, 2004

[3]. B. Santhi, K. S. Ravichandran, A. P. Arun and L. Chakkrapani, "A Novel Cryptographic Key Generation Method Using Image Features", Research Journal of Information Technology 4(2): 88-92, 2012. ISSN: 2014-3114, 2012

[4]. Mr. Vikas Tyagi, "Data Hiding in Image Using least significant bit with Cryptography", IJARCSSE, vol. 2, no. 4, pp. 120-123, 2012.

[5]. Ritu Pahal, Vikas Kumar, "Efficient Implementation of AES", IJARCSSE, vol. 3, Issue 7, pp.290-295, 2013

[6]. Mostafa Abd-El-Barr, Altaf Al-Farhan, "A Highly Parallel Area Efficient S-Box Architecture for AES Byte-Substitution", IACSIT International Journal of Engineering and Technology, Vol. 6, No. 5, 2014, pp. 346-350

[7]. M. Narasimhulu, S. Mahaboob Basha, P. Chandra Sekhar, "Hardware Implementation of High Performance AES using Minimal Resources", IJER, ISSN: 2319-6890, vol. 3, issue no: special 2, pp: 68-72, 2014

[8]. Mr. Shelke R.B, Mrs. Patil A.P, Dr. (Mrs) Patil S.B, "VLSI Based Implementation of Single Round AES Algorithm", IOSR-JECE, ISSN: 2278-2834, ISBN: 2278-8735, pp: 63-67

[9]. Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande, "Modified Advanced Encryption Standard", IJSCE, ISSN: 2231-2307, vol. 6, issue 1, 2014

[10]. Manjesh K N, R K Karunavathi, "Secured High Throughput Implementation of AES Algorithm", IJARCSSE, vol. 3, issue 7, 2013

[11]. T. Rahman, S. Pan, Q. Zhang, "Design of a High Throughput 128-bit AES (Rijndeal Block Cipher)", in Proc. International Multi Conference of Engineers and Computer Scientist, vol. 2, 2010

[12]. Shtewi A.M, "An Efficient Modified Advanced Encryption Standard adapted for image cryptosystems", IJCSNS International Journal of Computer Science and Network Security, vol. 10 no. 2

[13]. Stallings W., Cryptography and Network Security, Third Edition, Pearson Education, 2003

[14]. Julia Juremi, Ramlan Mahmod Salasiah Sulaiman Jazrin Ramli, "Enhancing AES s-box generation based on Round key", International Journal of Cyber-Security and Digital Forensics,vol.1,no.3,pp.183-188,2012.

[15]. M.Gnanambika, S.Adilakshmi, Dr.Fazal Noorbasha, "AES-128 Bit Algorithm Using Fully Pipelined Architecture for Secret Communication", International Journal of Engineering Research and Applications 2248- vol. 3, no.2, pp.166-169,2013.