FPGA Based Hardware Implementation Of Cryptographic Process Using Sea

M.Gowri, R.Aarthi,G.Bhuvaneswari
Students, Department of Electronics and Communication Engineering Paavai College of engineering, Namakkal, India

P.Gopinathan
M.E/Assistant professor Department of Electronics and Communication Engineering Paavai College of engineering, Namakkal, India

Abstract-The implementation of encryption /decryption algorithm it is provide the more secure communication for the data transform. The triple AES algorithm using encrypts the data for secure communication. The triple AES gives the security of da ta, image, picture and etc. In this paper another plan of cryptographic process and include bit stream compression. The proposed work of the paper it has two process. First process is encrypts the data using SEA and second process is bit stream compression using golomb coding and decode aware placement algorithm for further work. The scalable encryption algorithm using encrypts the information provide the secure communication SEA is suitable for low cost embedded system application like RFID and sensor .SEA is used limited instruction set. Bit stream compression method using reduces the size of bit stream and also reduces the memory constraint. Compression method using achieves the increasing the bandwidth of communication and reduces the reconfiguration time. Golomb encoding using achieves the bit stream compression. It is technique capable of compressing the large size of information in to small size of information. The result of this paper is synthesizing and implementation of the VHDL code carried out on modelsim software.

Keywords – Scalable encryption algorithm, bitmask based compression, golomb coding, VHDL, FPGA

I. INTRODUCTION

SEA is scalable encryption algorithm used to implement the encryption and decryption process for data secure communication.SEA is basically used in cryptography process. Cryptography is the art of protecting information by transforming the original messag e, called plaintext into an encoded message, called a cipher or cipher text.SEA is parametric block cipher for resource constrained system like sensor networks, RFID.It was initially designed low cost encryption /authentication routine (small code size and memory) is targeted for processors with a /limited instruction set. SEA algorithm takes places the plaintext, key and the bus sizes parameters and therefore can be straightforwardly and various implementation contexts and/or security requirements. SEA benefits from a stronger Security analysis derive from in block cipher design/cryptanalysis. Compression block help as reduces the bit stream size.SEA provide efficient solution for embedded software application using micro controllers. Compression is used to reduce the size of one or more files. Therefore, compression is often used to save disk space and reduce the time needed to transfer files over the internet. There are two primary types compressi on. There are lossy compressions and lossless compression. The lossy compression is compressed data is not same as the original data but close approximated of it. Loss less compression is the compression of a file all original data recovered when the file is uncompressed. Data compression is set out to achieve a reduction in file size by encoding data more efficiently. To measure the efficiency of bit stream compression using compression ratio.

Compression ratio=compressed data/original data

FPGA –based embedded system uses decode –aware bit stream compression technique to reduce the memory requirements for storing configuration bit stream which limits the capacity and bandwidth .To compress the configuration bit stream, we introduced a new technique called dictionary, bitmask, and Golomb coding on the compression. After compression, the compressed bit stream in the memory are transferred into decode –aware placement technique. Decode aware placement algorithm is used to place the compressed bit stream into memory Golomb coding is one of the lossless data compression. In this coding cable of reduce the data large size in to small size. Compression mechanisms used to reduce bit stream and increase the bandwidth. It is mainly improve efficiency of communication. Secure and bit stream compression achieve in the proposed work of

the paper. Block diagram of proposed work in fig shown in 1

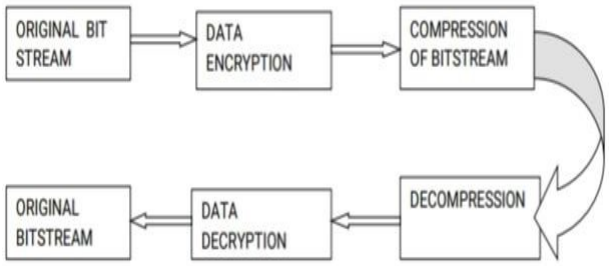


Fig.1 Basic block diagram

In this paper only implement the SEA algorithm process and gives the idea of compression method for future work for further applications.

II LITERETURE REVIEW

AES is an encryption standard is implementation chosen by the national institute of standards and technology (NIST), USA to p rotect the classified information. it has been accepted world wide as a desirable algorithm to encrypt sensitive data. it is a block cipher which operates on block size of 128 bits for both encrypting as well as decrypting .Each round performs same operations. In 1990's the cracking of DES algorithm become possible .NIST is implement new algorithm is Rijndael algorithm. This algorithm designed by Rijment and Daemon in 2001.it is provide the security of data communication.AES basically repeats 4 major functions to encrypt data. It is 128 bit block of data and key and gives a cipher text as output. The functions are:

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

The number of rounds performed by the algorithm strictly depends on the size of key. The following table gives overview of number of rounds performed with the input of variable key lengths.

Key Size	Number of rounds
128-bit	10
192-bit	12
256-bit	14

Substitute bytes transformation called as the sub bytes.AES matrix values called s_box that contains 256, 8 bit values ranges. Individual bytes of state is mapped a new bytes. Shift rows process is shift the output of sub bytes the first Row is no shifting of the bytes and second row is shifted by one position. The third rows shift in three positions. Mix columns algorithm is two steps present that are:

1.Matrix multiplication
2.Galois field multiplication

The matrix multiplication is performed each State in column multiplied against every value of the matrix of the row. The Galois field multiplication process the state bytes are treated as polynomials of Galois algebra. The add round key operation a simple XOR between current state values and round key for the current round. The encryption parameters are the input plaint text, key size and the cipher text. First step of AES is 16 bytes input plaintext in form of 4*4 bytes states and calculate no of round and key expansion. The plain text and key is XORed, and applying the round of four operation such as s-box, shift rows, mix columns and add round key operation.XOR of each bytes and key of corresponding bytes of the state is get the cipher text of Encryption algorithm.AES utilizes distinctive key lengths.AES algorithm using to encrypt the data utilized the three key function generate the cipher data is process is called as triple key AES algorithm process. In the triple key AES calculation, we need the encode process of 128 piece of information. The key gives the blend square. In the frame work,
128 piece of information is gives as the contribution of three the 128 piece of keys. This round key obtained from the cipher text an decryption occur possible of reverse function.128 piece of information gives to the input square along the three key In this square include the round activity is play out the information and key performed, It implies that change the information like substitute bytes, move change the mix columns, blend section change and involve the key activity. For 128 bit encryption we need the 10 round activity of encryption process. The decode process of the information same procedure is followed backward request of change the AES calculation. Figure 2 shows the steps involved in the Triple key AES algorithm.

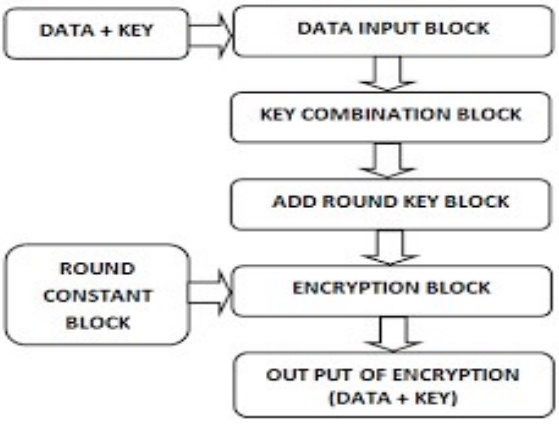


Fig.2 Triple AES algorithm

The AES encryption and decryption algorithms using triple key AES. This algorithm optimized the delay of 4.221ns in the outcome .the speed up the encryption and decryption achieve the SEA. The involve the steps shows Fig 3 basic AES encryption round operation

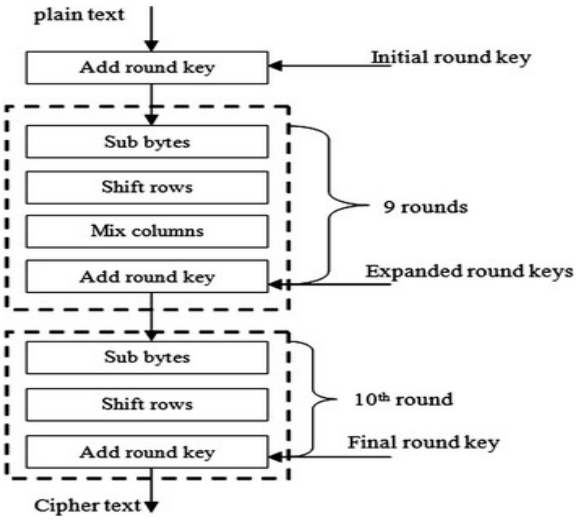


Fig.3 Basic AES algorithm

3.1 ALGORITHM OF SEA

III. PROPOSED ALGORITHM

The scalable encryption algorithm benefits from a stronger security analysis. SEA is mention the SEAn, b.SEA operate the text, key, word size. Example using 8 bit processor we derive the 48 bit block ciphers denotes the SEA48, 8. Parameters of SEA are:

1) Plain text size, key size
2) Processer size
3) Nr number of block cipher rounds
4) Nb is number of word

3.2 OPERATION OF SEA

1) Bit wise XOR
2) Mod 2^b addition
3) Substitution box
4) Word rotation
5) Bit rotation

3.3 BASIC OPERATIONS

1) Bit representation:

xb = x (n 2 − 1) x (n 2 − 2)…… X (1) X (0).

2) Word representation:

xW = xnb−1 xnb−2 . . . …x2 x1 x0.

3) Bitwise XOR ⊕:

The bitwise XOR is defined on n 2 -bit vectors: ⊕:

Z n 2 × Z n 2 →
Z n 2 : x, y →
z = x ⊕ y ⇔
z(i) =x(i)⊕y(i) $0 \le i \le n2-1$.

4) Addition mod2b ¢:

The mod 2b addition is defined¢ :

Z nb 2 b × Z nb 2 b → Z nb 2 b: x, y →
z = x ¢ y ⇔
zi = xi ¢ yi , $0 \le i \le nb - 1$

5) Substitution box S:

SEAn,b uses the following 3-bit substitution table: ST := {0, 5, 6, 7, 4, 3, 1, 2},

For efficiency purposes, it is applied bitwise to any set of three words of data using the following recursive definition:

S : Z nb 2 b → Z nb 2 b : x → x = S(x) ⇔
x3i = (x3i+2 ∧ x3i+1) ⊕ x3i
x3i+1 = (x3i+2 ∧ x3i) ⊕ x3i+1
x3i+2=(x3i∨x3i+1)⊕x3i+2 $0 \le i \le nb3-1$

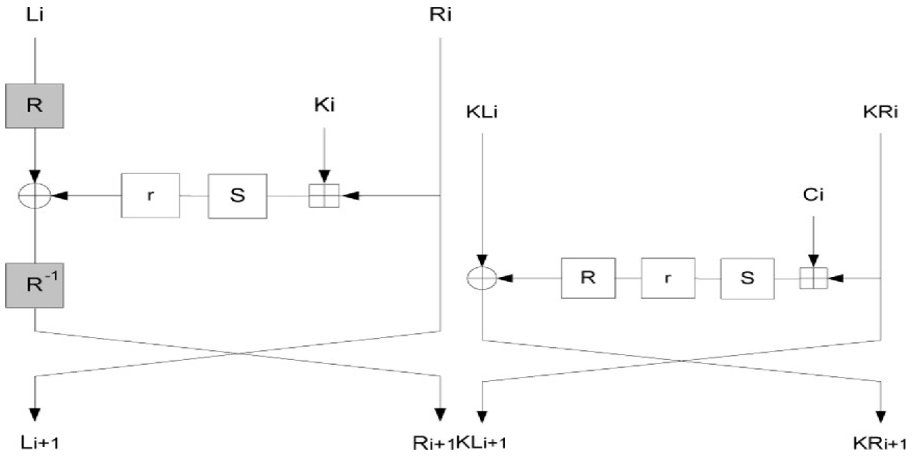


Fig.4 Encrypt/decrypt round and key round

3.4 ROUND AND KEY ROUND FUNCTION

The data encrypt and decrypt process using SEA it perform based on round and key round process. The encrypt round FE, decrypt round
FD, and key round FK.The fig.4 shows the encrypt and decrypt round and key round

$[L_{i+1}, R_{I+1}]$=F (Li, R i, Ki)

RI+1=R (Li) XOR r(S (RiI mod 2^b addition Ki))

Li+1=Ri

[Li+1, RI+1]=F_D (Li, Ri, Ki)

Ri+1=R (L XOR r(S (Ri mod 2^b adder K_i)))

Li+1=Ri [KLi+1, KRi+1]

=Fk (KLi, KRi, Ci]

KRi+1=KLi XOR R(r(S (Ri MOD 2^b ADDERR Ki))) KLi+1=KR_i

3.5 ENCRYPTION/DECRYPTION AND KEY GENERATION

The encrypt round FE, decrypt round FD and key round FK are defined as: Encryption Round FE :

Li+1 ,Ri+1 = FE Li ,
Ri , Ki ⇔ Ri+1 = R Li ⊕r S Ri ⊞ Ki , Li+1 = Ri
Decryption Round FD : Li+1 , Ri+1 = FD Li ,
Ri , Ki ⇔ Ri+1 = R −1 Li⊕r S Ri ⊞ Ki , Li+1 = Ri
Key Scheduling Round FK : KLi+1 , KRi+1 = FK KLi ,

KRi , Ci ⇔ KRi+1 = (KLi⊕R(r (S KRi ⊞ Ci))),

KLi+1 = KRi

3.5 CIPHER DESCRIPTION

This ciphering is based on the number of rounds nr and uses iterative based loop design. The pseudo code given in Figure 2.2 illustrates the necessary steps for encrypting a plain-text. where, P: Plain-text, C: Cipher-text K: Key and all these three are parameterized by bit size n. C=SEAn,b(P, K)

{

% initialization: L0&R0 = P; KL0&KR0 = K;

% key scheduling:

for i in 1 to b nr/ 2

[KLi , KRi] = FK(KLi−1, KRi−1, C(i));

switch KLb nr /2 c , KRb nr 2 c ;

for i in d nr 2 e to nr – 1

[KLi , KRi] = FK(KLi−1, KRi−1, C(r-i);

% encryption:

for i in 1 to d nr/ 2

K [Li , Ri] = FE(Li−1, Ri−1, KRi−1);

for i in d nr 2 e + 1 to nr/2

K [Li , Ri] = FE(Li−1, Ri−1, KLi−1);

% final:

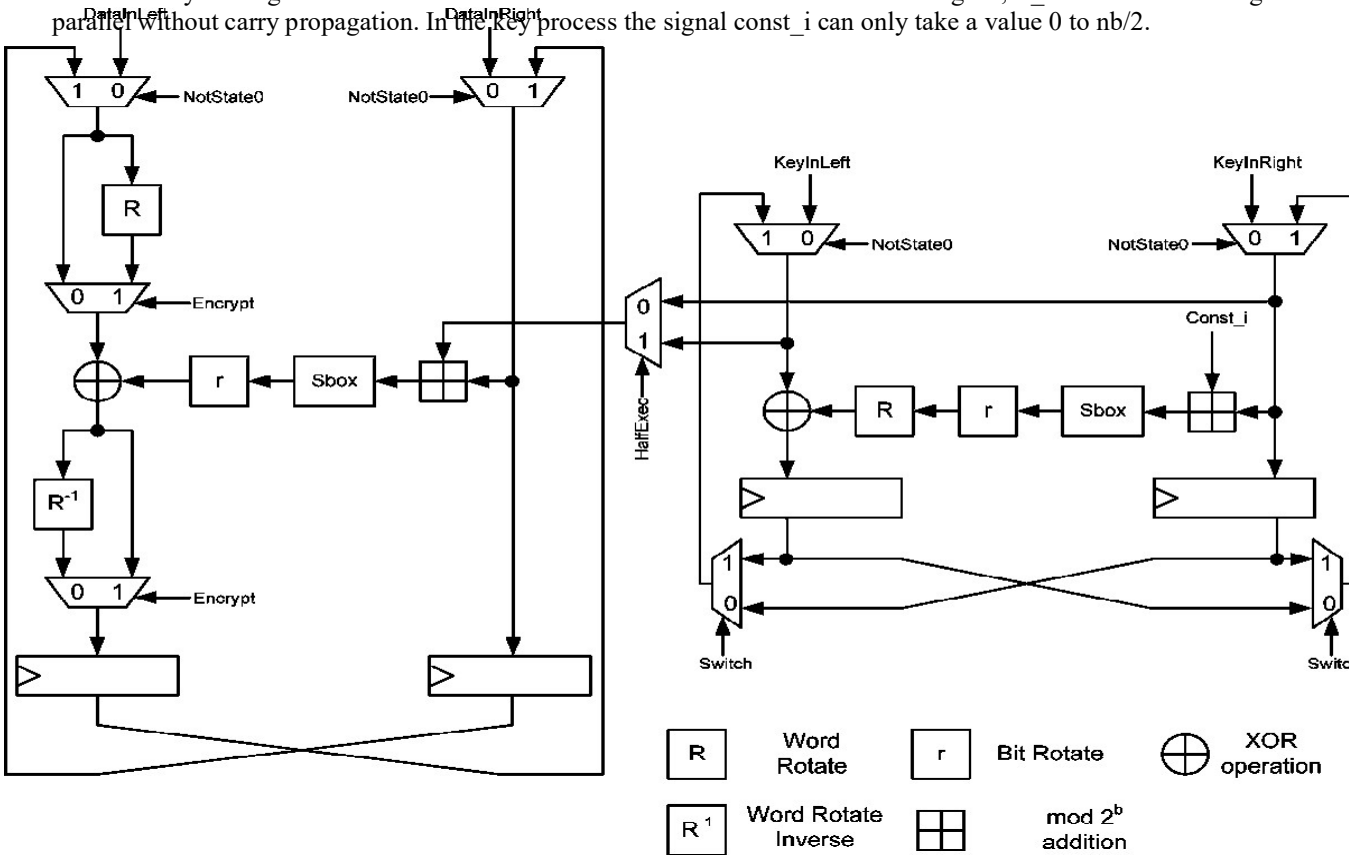
C = Rnr&Lnr ;

switch KLnr−1, KRnr−1;

},

3.5 LOOP ARCHITECTURE OF SEA

The structure of our loop for SEA is two part process. The left side is data it is round function and right side is key schedule process. Resource consuming blocks are s box and 2^b adder, word rotate and bit rotate blocks are implemented by using swapping wires. According to the specifications, the key schedule contains two multiplexors allowing the switch function. Switch left part of the round key at half of execution of the algorithm using command signal switch. The multiplexor controlled by half execution of round function with the key for the first half of the execution and transmits its left part .to support both encryption and decryption finally added two multiplexors controlled by the signal. In the round function the mod 2 adder are realized using nb, b_bits adders working the parallel without carry propagation. In the key process the signal const_i can only take a value 0 to nb/2.



4.1FPGA SYNTHESIS ANALYSIS

Fig.5 Loop architecture of SEA

IV. EXPERIMENT AND RESULT

Synthesis is the process of generating cricuit / gate level implementations from VHDL model with the inputs a VHDL model,design constraints mapping libraries etc.It is converts the design into a netlist of actual gates /blocks specified in FPGA sdevices.

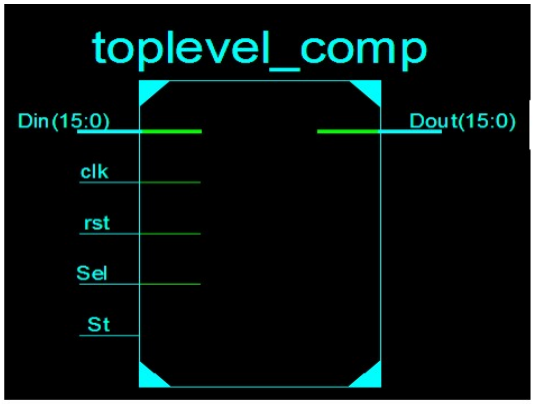
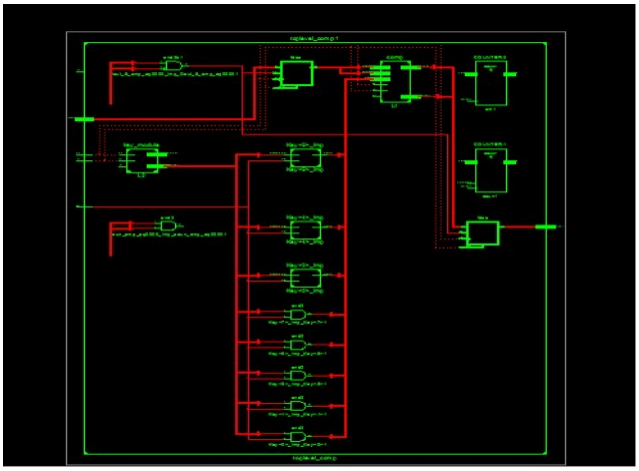


Fig.6 Schematic diagram of SEA

AES algorithm using no.of LUTs utilized is 27787 and No.of IOBs is 385 but proposed algorithm using no.of LUTs is 1920 and no.of IOBs is 66.LUTs occupied proposed work of SEA is less area compare then AES.the benefits of SEA is memory utilization occur is less.Fig.6 shows the schematic diagram encryption and decryption modules of SEA.Table gives the devices utilization report.The average connection delay for encryption and decryption is 4.05ns.Fig.7 shows the rtl diaram of SEA FPGA



F ig.7 RTL diagram of SEA FPGA

4.2 DEVICE UTILIZATON REPORT

Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Flip Flops	63	1,920	3%
Number of 4 input LUTs	31	1,920	1%
Number of occupied Slices	39	960	4%
Number of Slices containing only related logic	39	39	100%
Number of Slices containing unrelated logic	0	39	0%
Total Number of 4 input LUTs	31	1,920	1%
Number of bonded IOBs	35	66	53%
Number of BUFGMUXs	1	24	4%
Average Fanout of Non-Clock Nets	2.62		

4.3SIMULATION RESULT

Table .1 is report of device utilization

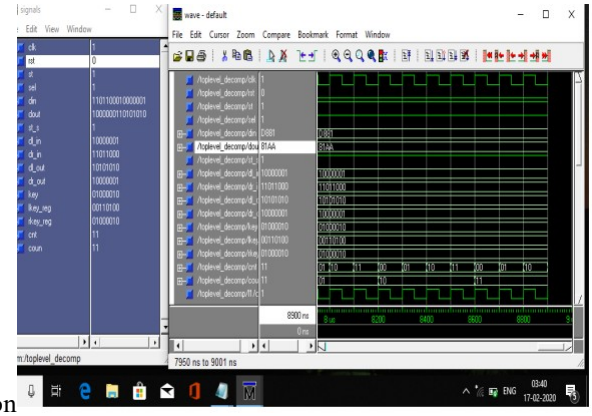


Fig.8 Simulation output of encryption

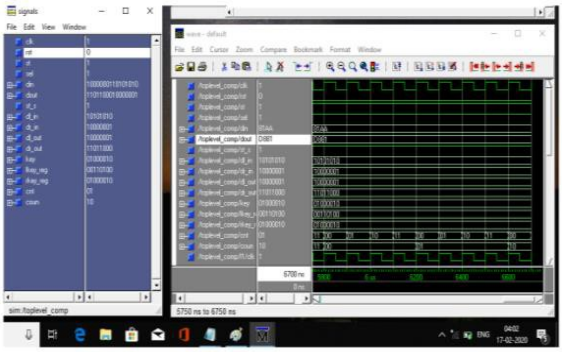


Fig.9 Simulate of decryption output

V.CONCLUSION

In this paper proposed SEA using encryption and decryption algorithm .we have optimized the delay of 4.05ns in the outcome but outcome of exisiting method of triple key AES is 4.221ns .SEA delay analysis is fast then Triple AES algorithm.SEA is 4% greater then the triple key AES algorithm process.The speed grade is -5.The outcomes that the present proposed calculation has great cryptographic quality and with additional advantage of high security analysis

REFERENCES

[1] FazalNoorbasha, Y.Divya, M.Poojitha, A.Bhavishya, K.Koteswararao, K.Hari Kishore_" FPGA design and implementation of modified AES based encryption and decryption algorithm."International journal of innovative technology and exploring engineering (IJITEE) ISSS: 2278-3075, volume-8 Issus-6s, April 2019

[2] M.Natheabanu_"FPGA based hardware implementation of encryption algorithm" International Journal of engineering and Advanced Technology (IJEAT) ISSS: 2249-8958, volume-3, Issus-4, April 2014

[3] Xinminao Zhang and KeshabK.Parthi" High-speed vlsi architectures for the AES algorithm"IEEE transactions on verylargescale integration (VLSI) systems, vol.12, no.9, September 2004

Chityalaprathyusha, P.Sharmila Rani "implementation of fast pipelined AES algorithm on Xilinx fpga"International journal of science and

research (IJSR) ISSN: 2319-7164

[4] N.Sivasankari, K.RampriyaandA.Muthukumar "Implementation of area efficient 128-bit based AES algorithm inFPGA"European journal of advances in engineering and technology, 2017, 4(7), pp541-548

[5] R.Saranya, S.KousalyaDevi, V.Lakshmiprabha, ph.d "Compression of FPGA bit stream using modified Decode aware placement algorithm.

[6] Dilja.k and DR.S .Natarajan,flowchart approach to scalable encryption algorithm Design and implementation in FPGA,IJCa proceeding on international conference on vlsi ,communicationsandinstrumentation(ICVCI)(11)