VOL. 10, NO. 14, AUGUST 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

FPGA IMPLEMENTATION OF HIGHLY AREA EFFICIENT ADVANCED ENCRYPTION STANDARD ALGORITHM

D. Arivazhaki, V. Vijayakumar and T. Ravi
Department of Electronics and Communication Engineering, Sathyabama University, Chennai, Tamil Nadu, India
Email: arivazhaki@gmail.com

ABSTRACT

Cryptography is art of science that encrypts plain text into cipher text (unreadable form) for security in electronic data transmission over network fields. For this method the current encryption method is Advanced encryption standard. The proposed method is hardware implementation of AES-128 and the key length is varying 128,192 and 256 bits is designed by Impulse C language with the help of Xilinx Platform Studio. Impulse C is a high level synthesis tool and supports parrel programming in particular for programming applications mainly targeting FPGA based devices.

Keywords: FPGA, cryptography, AES, impulse C.

1. INTRODUCTION

Cryptography is an ancient art developed in the year 1900; the purpose of the Cryptography is keeping the information secret in the computer field. It uses three types of keys for encryption; they are Secret key encryption, public key encryption and Hash function. AES uses Secret key algorithm for symmetric block cipher which is derived by Rijndael algorithm. This algorithm was developed by two Belgian computer scientists namely John Daemen and Vincent Rijmen. Secret key denoted as same keyword will be used for both encryption and decryption. For this encryption, there was earlier method is DES (Data Encryption Standard) which was not suitable for security because it had only 64 bit block bits and 16 rounds for permutation and substitution. Anyway speed was not enough, thereby an alternative technic 3DES was developed and more security increased. The disadvantage of 3DES is speed is too slow and its license was not free for users and this method was broken by DES cracker. At time FIPS-197(Federal Information processing and standards) announced for new encryption standard in the year 1998 [3, 4]. There was 5 standards was selected namely Mars, RC6, Rijndael, SERPANT and Two fish, there were further analysis prior to the selection of the best algorithm for better encryption is AES algorithm in the year 2000 derived by Rijndael algorithm. AES had fixed block size 128 bits and the key sixes are 128bits, 160, 192, 224 and 256 bits and can be implemented in Hardware as well as Software efficiently [5,7,8].

Impulse C is a subset of standard C developed in the year 2003; it is a high level synthesis tool and compatible function library supporting parallel programming in particularly targeting reconfigurable FPGA based devices. It allows ANCI C, standard C tools for designing and debugging applications for FPGA.

2. ADVANCED ENCRYPTION STANDARD

The proposed methods uses 128 bit data length and varying key lengths are 128, 192 and 256 bits for encryption and decryption with the help of lookup table implementation of S box and key expansion technic for developing cipher text for each round of processing [13, 14].

The block size and number of columns in the block is commonly referred as Nb and key size is Nk. Each row in the column consists of four cells of 8 bytes each. The plain text input is broken up into blocks and arranged in column wise in the state array or block. For 128 bit key length, Nb can be calculated by dividing 128 by 32 where 32 come from all bits in the single column, therefore Nb is 4. For 192 and 256 bit, Nb is 6, 8 respectively. In AES-128, the number of columns is fixed because there are 16 bytes in each row. The number of rounds can be calculated by using 6+max {Nb, Nk}.

For encryption each round of operations consist of 5 basic steps, they are

A. Sub bytes

B. Shift rows

C. Mixed columns

D. Add round key

E. Key expansion technique

The initial round and last round is differ from other rounds there is Add round key process in initial round and mixed column will not carried out in the last round [15].

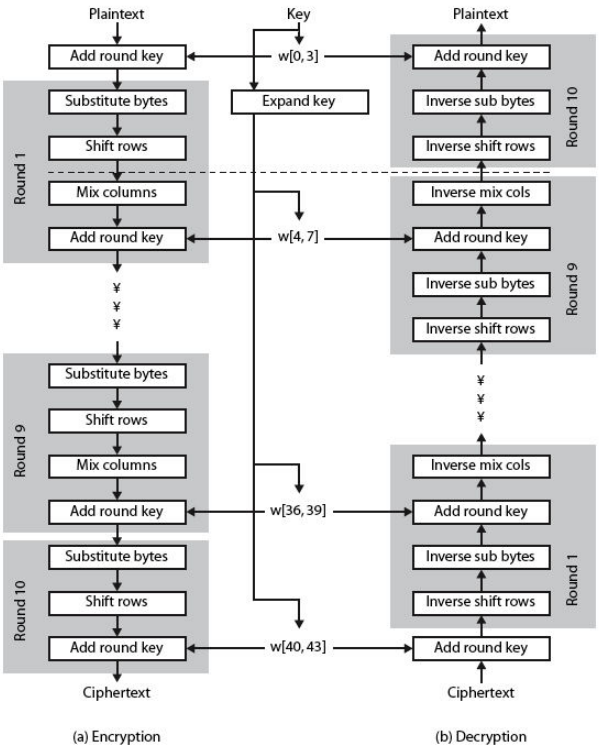

Figure-1. AES block diagram.

A. Sub bytes process

Sub bytes means substitution bytes that is byte by byte substitution using 16 X 16 lookup table S box, to find a replacement byte which is in hexadecimal form.

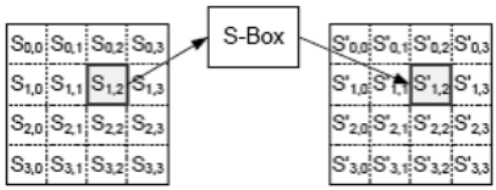

Figure-2. Sub bytes.

S box is calculated by using multiplicative inverse in Galois field GF (2^8) based on irreducible polynomial and affine transformation. This process is same for decryption, for byte substitution use i*n*verse S Box.

B. Shift rows process

The next step of round operation is shifting the rows in cyclic manner in the block. The rows are shifted X number of bytes to the left where X in the row number. If row 0, there is no shift. In row 1 will shift byte 1 byte to the left and for row 2 and 3 will shift 2 times and 3 times shifts to the left respectively.

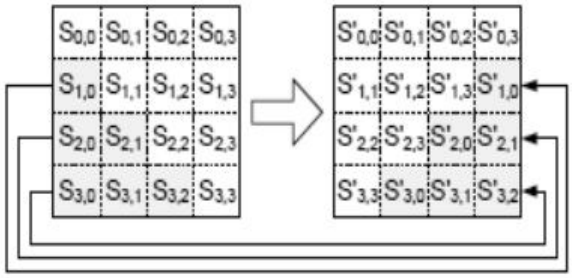

Figure-3. Shift rows.

C. Mix column process

The mix column transmission operates on the state of column by column, treating each column as 4 term polynomial over GF(2^8) and multiplied with modulo X^4+1 for fixed polynomial given by

$a(x)= (02)+(01)x+(01)x^2=(03)x^3$
$b(x) = (03)+(02)x+(01)x^2+(01)x^3$
$c(x) = (03)+(01)x+(01)x^2+(03)x^3$
$d(x)= (03)+(01)x+(01)x^2+(03)x^3$

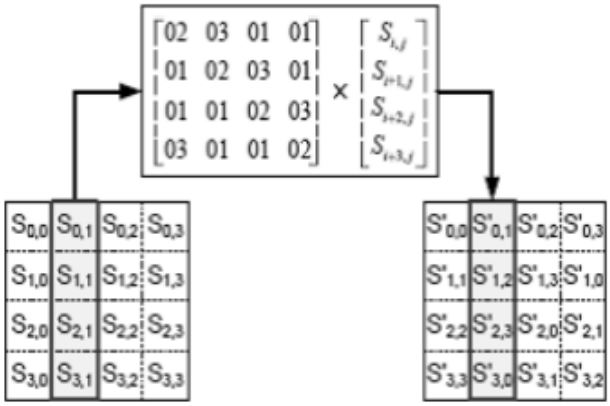

Figure-4. Mix column.

D. Add round key process

Figure-5. Add round key.

The round key values are derived from cipher key and the input state using Ex-OR operation. The key values are never reused.

E. Key expansion technique

Key expansion process is to generate round keys from the cipher for each word. The cipher key needs to be expandedfrom 16 bytes to 16(r+1) bytes. The substitution word presents in key expansion routine that takes a 4 byte input word gives 4 byte output word using S box. The rotate word function performs a cyclic permutation on input word gives cyclic right shifted 4 byte output word. Rcon is round constant is array of bytes in a word having fixed logical values. The output word is ExOred with Rcon values for initial state of each round[16].

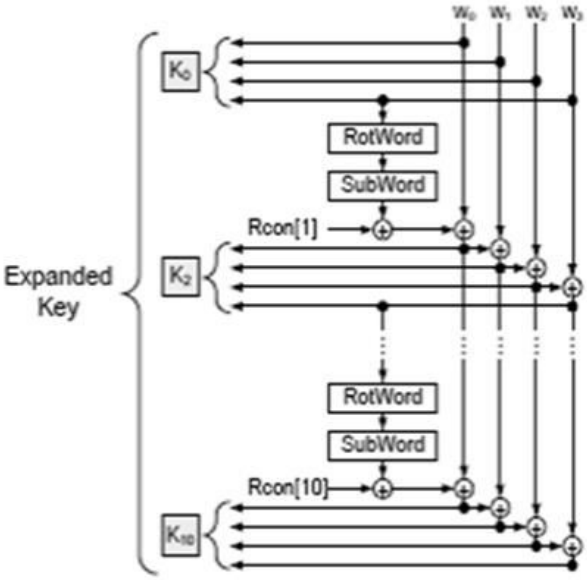

Figure-6. Key expansion process.

3. IMPLEMENTATION AND RESULTS

The implementation results uses the Spartan 3 FPGA family is XC 3S 200-5TQ by using Xilinx platform studio XPS 8.1i for easily build hardware platforms based on the micro blaze processor and GNU compiler for debugging. In this AES algorithm has been coded by using Impulse C language and the implementation is processed by XPS 8.1i tool with the help of FPGA Spartan 3 device and the results are shown in HyperTerminal window. The algorithm is testing of Encryption and decryption a fixed 128 bit block length and varying cipher key values 128, 192 and 256 bits. The implementation results are shown.

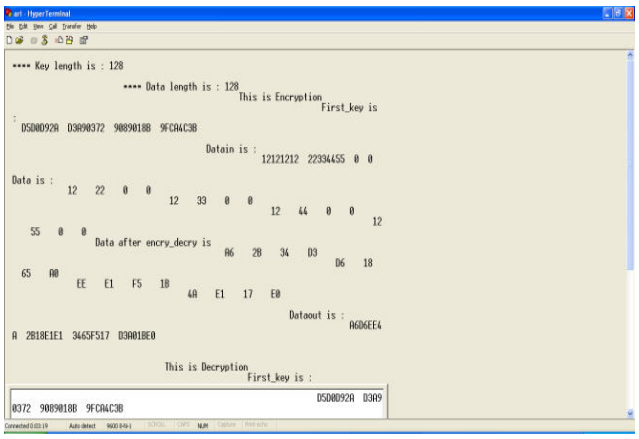

Figure-7.AES encryption, AES-128, 128 bit cipher key.

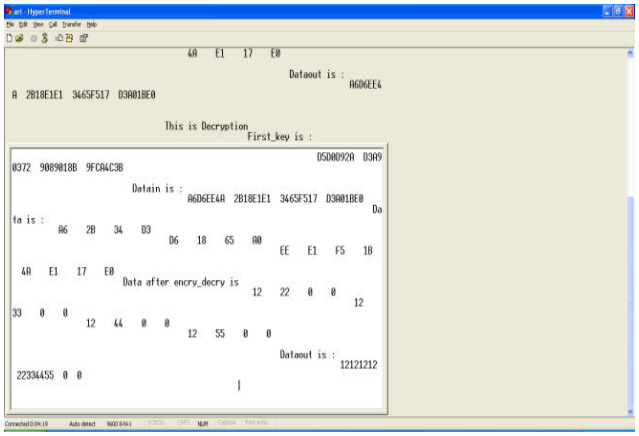

Figure-7(a). AES encryption, AES-128, 128 bit cipher key.

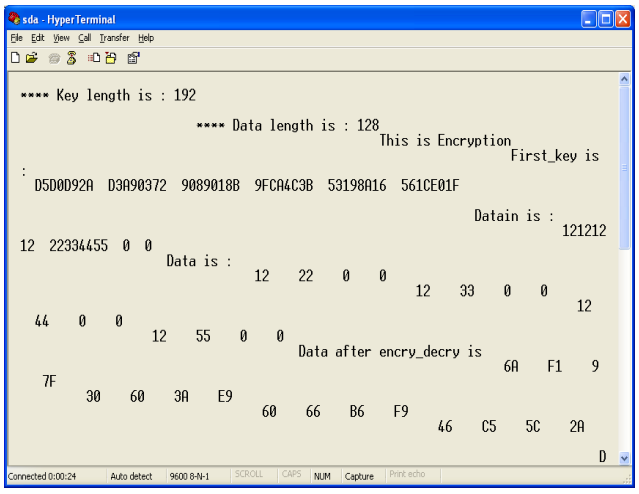

Figure-8. AES encryption, AES-128, 192 bit cipher key.

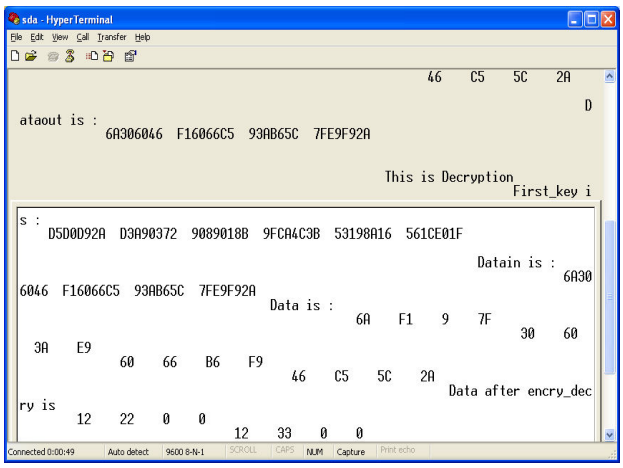

Figure-8(a). AES encryption, AES-128, 192 bit cipher key.

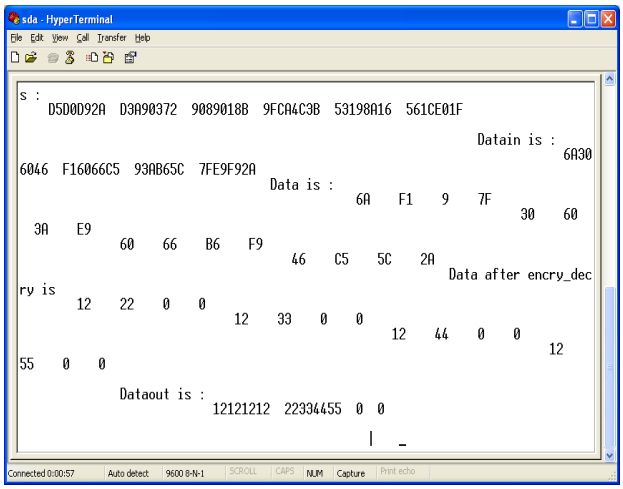

Figure-8(b). AES encryption, AES-128, 192 bit cipher key.

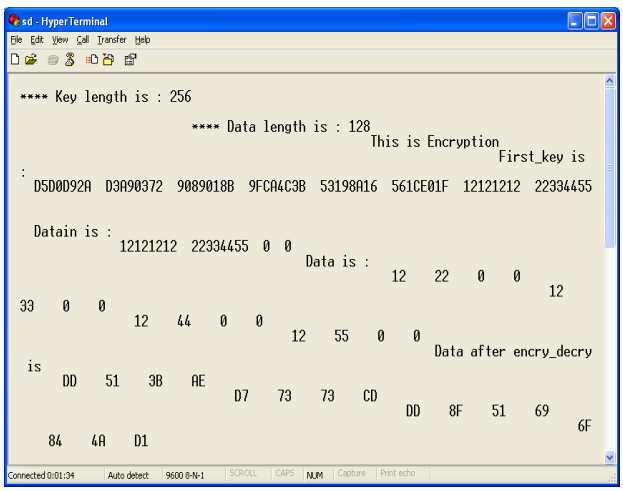

Figure-9. AES encryption, AES-128, 256 bit cipher key.

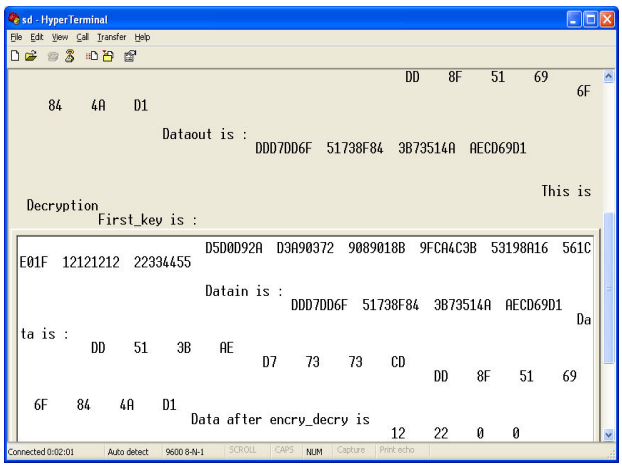

Figure-9(a). AES encryption, AES-128, 256 bit cipher key.

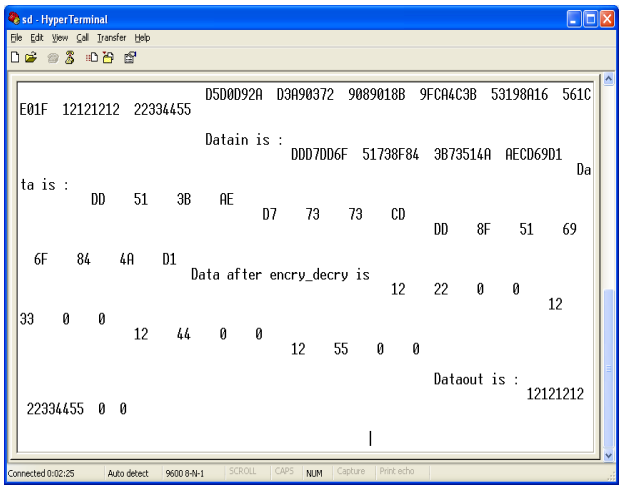

Figure-9(b). AES encryption, AES-128, 256 bit cipher key.

Device utilization summary

Resource Type	Used	Available	Percent
Slices	712	1920	37
Slice Flip Flops	898	3840	23
4 input LUTs	1377	3840	35
IOs	2296	NA	NA
bonded IOBs	0	97	0
MULT18X18s	3	12	25

4. CONCLUSIONS

The efficient Hardware implementation of Advanced Encryption Standard algorithm which includes Encryption and Decryption in this paper. AES algorithm is designed by using Impulse C language for better hardware resource utility debugged by GNU compiler in XPS 8.1i tool kit, it provides base system builder wizard enables easily creating embedded system is achieved within a minutes. AES offers the high level security with strong

key system and computational power is higher than other algorithms.

REFERENCES

[1] Daemen J.Rijmen, AES proposal, Rijndael.. The Rijndael Block Cipher, AES proposal, 1999, pp. 1-45.

[2] J. Daemen and V. Rijmen. The Rijndael Block Cipher.AES proposal document version 2, 1999.

[3] FPGA implementations of advanced encryption standard: Survey. International Journal of Advances in Engineering and Technology. 2012.

[4] Ravi Thiyagarajan and Kannan Veerappan "Ultra low power single edge triggered delay flip flop based shift registers using 10-nanometer Carbon nanotube field effect transistor "American Journal of Applied Sciences, Volume 10, Issue 12, 2013, pp.1509-1520.

[5] Ravi.T, Kannan.V "Modeling and performance analysis of ballistic carbon nanotube field effect transistor (CNTFET)" International Conference on Recent Advances in Space Technology Services and Climate Change - 2010, RSTS and CC-2010, pp. 327-331

[6] Galois Field in Cryptography Christoforus Juan Benvenuto. 2012.

[7] Hoang Trang and Nguyen van loiHochiMinh City, Vietnam. An efficient FPGA implementation of the Advanced Encryption Standard algorithm, 2012.

[8] Ravi.T, Kannan.V "Effect of N-type cntfet on double edge triggered D flip-flop based PISO shift register" International Conference On Emerging Trends in Science Engineering and Technology: Recent Advancements on Science and Engineering Innovation - INCOSET 2012, Dec-2012 pp. 344-349.

[9] AvinashKak "Finite Fields of the Form GF (2n) Lecture Notes on Computer and Network Security" Purdue University, February 3, 2015.

[10] Sumanth Kumar Reddy S, R.Sakthivel and P Praneeth "VLSI implementation of AES Crypto Processor for High Throughput. International journal of advanced engineering science and technologies" Vol, No. 6, Issue No.1, pp:022 -026.

[11] Douglas Selent "Advanced encryption standard Insight" Rivier Academic journal. 2010.

[12] Ashwini R. Tonde and Akshay P. Dhande. "Implementation of Advanced encryption standard (AES) algorithm based on FPGA".

[13] Ravi.T, Kannan.V "Design and analysis of N-type CNTFET double edge triggered D flip-flop based SISO shift register" International Conference on Nano science, Engineering and Technology, ICONSET 2011, pp. 724 – 728.

[14] Ravi.T "Design and performance analysis of ultra low power RISC processor using hybrid drowsy logic in CMOS technologies" International Journal of Applied Engineering Research, Volume 10, Number 2, 2015, pp. 4287-4296.

[15] Swati paliwal, Ravindra Gupta. "A review of some popular encryption techniques". International Journal of Advanced research in computer science and Software Engineering. 2013.

[16] VedkiranSaini, ParvinderBangar, HarjeetSingh Chauhan. Study and Literature Survey of Advanced Encryption Algorithm for Wireless Application. International Journal of Emerging Science and Engineering, 2014.