International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 12, December 2014

Design and Implementation of Area Optimized AES with Modified S-Box Using Pipelining Technology

Dr.Vinodkumar Jacob[1] Akhil Madhu K[2]

[1,2]Dept of Electronics, MACE, Kothamangalam, Kerala, India

Abstract: Advanced Encryption Standard (AES) is a Federal Information Processing Standard. It is categorized as computer security standard. This paper talks about a mew FPGA-based implementation scheme of the AES-128 Encryption Algorithm. Pipelining technology is employed to maintain the speed of encryption. In order to reduce the chip size, mode of data transmission is also modified. The plaintext (128-bit) and the initial key (128-bit) as well as the output are all divided into 32-bit units controlled by the clock. The aim of the system is to reduce the hardware structure and to obtain high throughput.

Keywords: Area-Optimization, FPGA, AES, Plaintext, Cipher Text.

I. INTRODUCTION

As the computer and communication network develops rapidly, the information security needs high attention. In addition to political, military and diplomatic fields, information security is applied to the common fields of people's daily lives. Because of the defects of shot keys, the long serving DES algorithm has been broken. Therefore AES substitutes DES and became the new standard. In the financial fields in domestic, such as realizing authenticated encryption in ATM, magnetism and intelligence card, AES algorithm is widely used. In 1997, the National Institute of Standards and Technology (NIST) began a process to choose a symmetric-key encryption algorithm to protect sensitive information. In 1998, NIST has accepted fifteen candidate algorithms from all over the world. In the final round of the contest, there were five candidates. They were MARS, RC6, RIJNDAEL, SERPENT, and TWOFISH. In October 2000, NIST selected Rijndael Algorithm as the winner of the contest. Security, efficiency in software and hardware and flexibility were the primary criteria used by NIST to evaluate the candidate algorithms[1]. Rijndael algorithm was developed by Joan Daemen and Vincent Rijmen and hence the name Rijndael Algorithm. AES algorithm is a symmetric block cipher which is capable to process data blocks of 128bits. It uses cipher keys with lengths 128,192 and 256 bits.

AES algorithm finds wide range of applications in financial fields in domestic applications like authenticated encryption in ATM, magnetism card etc. In the current scenario the AES algorithm aims to have a better throughput using pipelined implementation. But, the disadvantage is that the cost of on chip resources may not be reliable in order to have high throughput. Parallel processing capabilities can be provided by using hardware security solutions based on highly optimized programmable FPGA. The design aims at high safety and cost effective reduced AES system. High

ISSN: 2278 – 909X

speed, high reliability, smaller chip area and high cost effectiveness are the main advantages of the proposed system.

As far as high performance and the security are concerned, hardware implementations are of very importance. Compared to software solutions, traditional ASIC solutions have drawback of reduced flexibility. Hence, FPGA based implementations are preferred.

II. AES ALGORITHM DESCRIPTION

The AES Algorithm can mainly be divided into two sections; key schedule and round transformation. Key schedule has two modules. They are key expansion and round key selection. In key expansion, N_k bits initial key is mapped to expanded key. From this expanded key module, the round key selection module chooses N_b bits of round key.

Important aspects for the design:

The key point for the design is to map the data in the main process to a 4×4 state matrix. In AES-128, the 128 bit initial data is divided into 16 parts each of which contains 8 bits of data. Therefore each cell in the state matrix will have one byte of data.

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

Figure 2. State Matrix[6]

In the round transformation, the byte Rotation, Mix Column, and ADD ROUND KEY are linear transformation. But round of byte substitution is a non linear transformation.

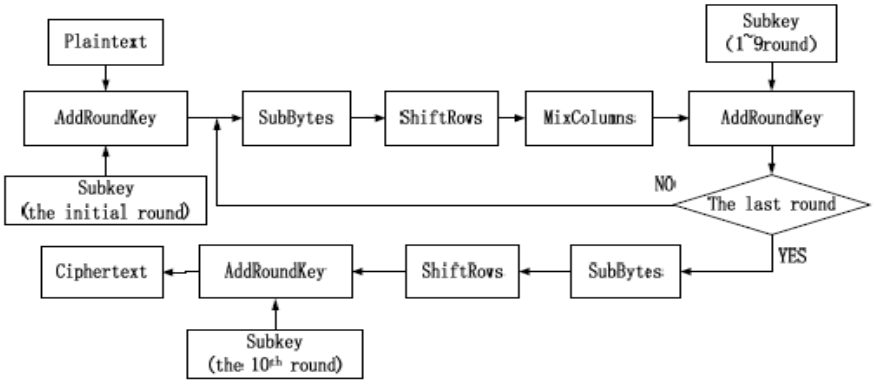

Figure 1. The Structure of Rijndael Encryption Algorithm[7]

The round key transformation consists of four modules. They are;

1. Byte Substituition
2. Byte Rotation
3. Mix Column
4. AddRoundKey

In Byte Substitution (Sub Byte), the elements of 128-bit input plaintext are replaced with the inverse elements corresponding to the Galois Field GF(2^8). The smallest unit of operation is 8 bits/group. In Byte Rotation (Shift Row), a

ISSN: 2278 – 909X

cyclic shift is applied to the 128 bit state matrix. Here the smallest operand is one row of 32 bit data. In Mix Column operation, the results of Byte rotation operation is added and multiplied with the corresponding irreducible polynomial in GF(2^8). The minimum operating unit of mix column operation is 32 bits. Add round key operation is nothing but simple XOR operation with 8 bit units.

The state matrix stores the inputs of plaintext and initial key, intermediate inputs and outputs of round transformation, as well as the output of cipher text in the AES algorithm. The state matrices are processed in one byte or one word. The various operations on the data is to be performed at least bits. For this, the 128 bits data has to be segmented. The operations are performed on each column of the state matrix.

III. PROPOSED MODEL

The proposed architectural optimization includes pipelining techniques. Multiple operations are processed simultaneously to increase speed. An optimized code has been developed and experimentally tested using Xilinx device. The main focus of the design is to attain speed. The number of blocks processed per second should be increased to achieve high throughput. At the same time silicon area optimization has to be obtained. In the improved design, the cipher text is sent to different modules of the algorithm as packets of 32 bit unit. The structure of improved AES algorithm for encryption is shown in Figure.3.

In the initial round of encryption, the 128 bits of input plain text is XORed with 128 bits of key. The operation is performed on 32 bit packet of data. The module actually XORs the initial key and the plain text.

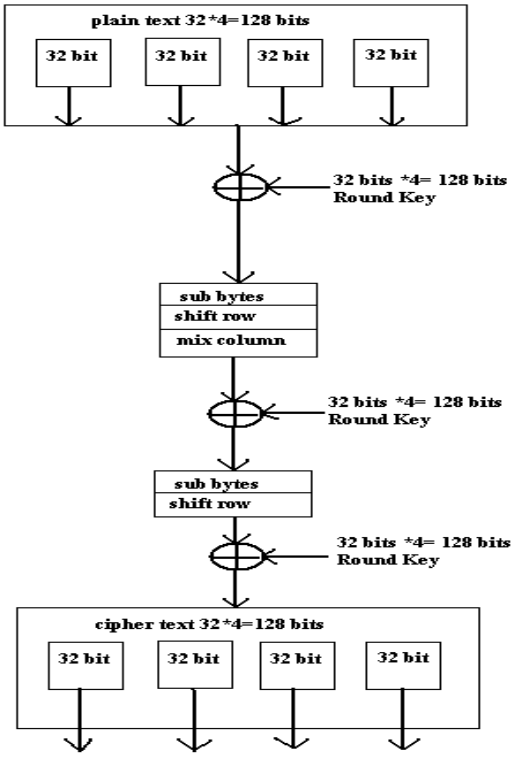

Figure 3. AES algorithm for encryption

In round transformation, SubBytes and MixColumn operations are done. In SubByte operation, each byte of data is replaced with another byte. In existing system, a 16×16 look up table is used and each byte in the data is replaced by corresponding byte in the LUT. The improved design uses a combinational logic based S-Box. This design has small area occupancy and high throughput. The modified S-Box design can use pipelining technology as compared to the typical ROM based lookup table implementation in which access time is fixed and unbreakable. The input data propagates into a composite field based S-Box. The input data first undergoes multiplicative

ISSN: 2278 – 909X

inversion. S-Box substituted values are obtained by applying Affine transformation to the multiplicative inverse.

The MixColumn operation is done based on the mathematical analysis of Galois Field GF(2^8). In this, multiplication and addition in th Galois field are performed on the data. In pipelining technology, the 128 bit data is divided into 32 bit packets and operations are performed independently on each packet of data in parallel.

The final round includes a 128 bit processing. The 128 bit resultant data from the round transformation is XORed with a 128 bit expanded key. The final output will be the 128 bit cipher text.

IV. SIMULATION AND SYNTHESIS VERIFICATION

Simulation and optimization of the VHDL code is done in ModelSim 6.5 software. Xilinx ISE Design Suite 13.2 is used for synthesizing and implementation of the code. The designed AES module is implemented on FPGA kit(SPARTAN III). To verify the working of different modules, each module is separately simulated in ModelSim.

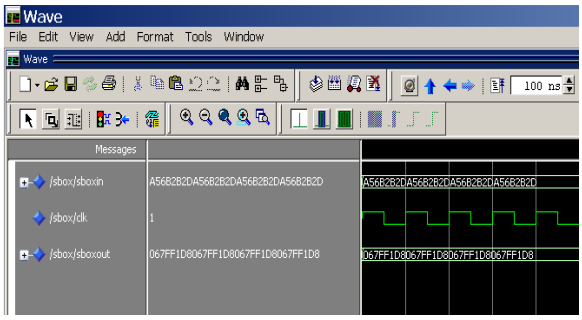

Figure.4. Simulation of 128-bit Byte Substitution

The figures numbered 4,5,6 and 7 show the simulation results of four modules in the AES encryption process. The results show that the logic function of improved algorithm is correct and satisfies the requirement of AES encryption algorithm.

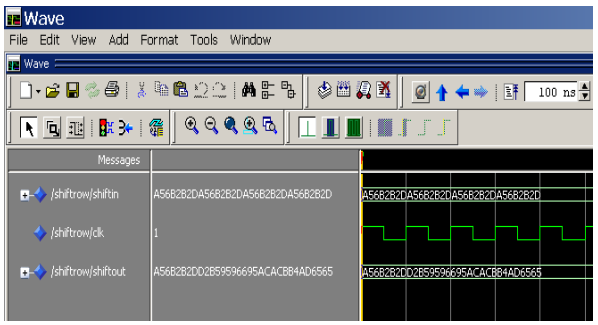

Figure.5. Simulation of 128-bit ShiftRow Transformation

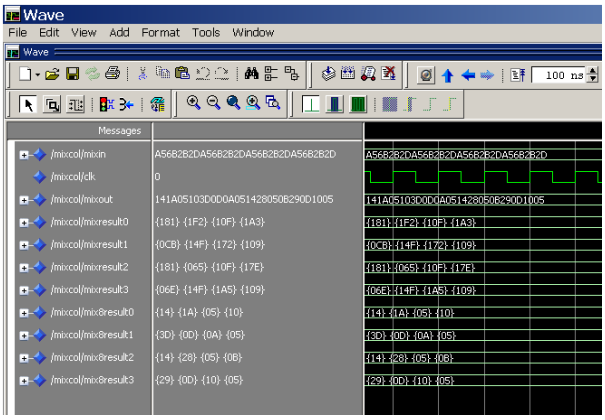

Figure.6. Simulation of 128-bit MixColumn Transformation

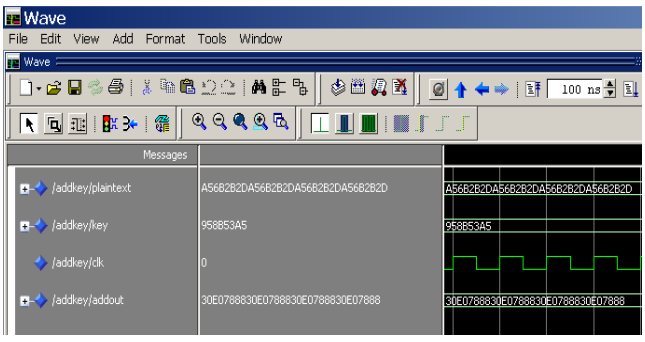

Figure.7. Simulation of 128-bit AddRoundKey Transformation

ISSN: 2278 – 909X

Xilinx project navigator is used for the analysis about physical parameters of the chip. Figure 8 shows the device utilization summary that includes the number of flip flops, LUTs, slices and logic gates used in the design.

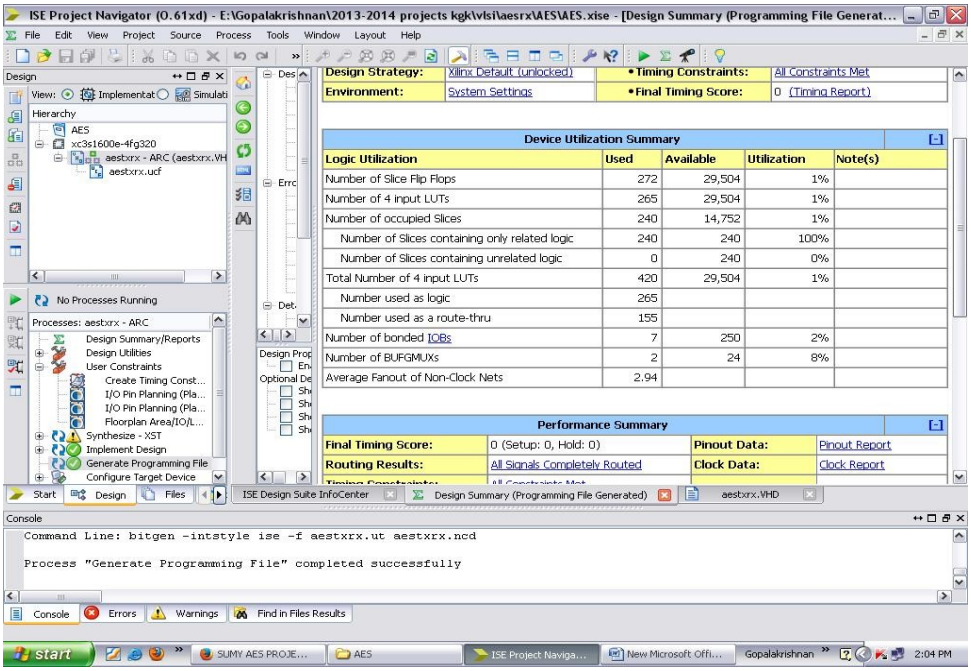

Figure 8. Device Utiization Summary

Figure 9.Power Report

Figure 10. FPGA Implementation

Figure 9 shows the power report. The cell area and dynamic power have significantly changed in the modified design. The area of the chip is significantly reduced by the pipelining technology. The power report shows that the power consumption of the circuit is relatively less compared to that of unimproved algorithm. In the improved design, the number of LUTs used is significantly reduced as it uses modified substitution box.

Table I. Comparison of parameters

	Power (mW)	Flip-Flops	LUTs	Slices
Unimproved	396	900	6513	3307
Improved	196	272	265	240

ISSN: 2278 – 909X

V. CONCLUSION

Area optimized AES algorithm is proposed in this paper. The coding was done in VHDL language and simulated using ModelSim 6.5 software. The designed module is implemented on FPGA kit. The design that employs pipelining technology could reduce the power consumption of the circuit. The device utilization summary shows that the number of flip flops, LUTs, slices and logic gates can be reduced compared to unimproved algorithm.

VI. REFERENCES

[1] Federal Information Processing Standards Publication 197, "Announcing the Advanced encryption standard (AES)"

[2] Joan Daemen, Vincent Rijmen, "AES Proposal: Rijndael"

[3] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback, "Report on the Development of the Advanced Encryption Standard (AES)" 2012 NIST

[4] Hoang Trang, Hoang Trang, "An efficient FPGA implementation of the Advanced Encryption Standard algorithm", 2012 IEEE

[5] Edwin NC Mui, "Practical Implementation of Rijndael S-Box Using Combinational Logic"

[6] Mg Suresh, Dr.Nataraj.K.R, "Area Optimized and Pipelined FPGA Implementation of AES Encryption and Decryption", 2012 IJCER

[7] Ai-Wen Luo, Qing-Ming Yi, Min Shi, "Design and Implementation of Area-optimized AES Based on FPGA" 2011 IEEE

[1]**DR.VINODKUMAR JACOB** received his M.Tech Degree from Indian Institute of Technology, Bombay and Ph.D from Cochin University of Science and Technology. He is currently working as Professor in the department of Electronics and Communication Engineering at Mar Athanasius College of Engineering, Kothamangalam, Kerala, India.

[2]**AKHIL MADHU K** received his B.Tech Degree in Electronics and Communication Enginnering from SNGCE, Ernakulam, affiliated to MG University, Kerala in the year 2012 and pursuing M.Tech degree in VLSI & Embedded Systems at Mar Athanasius College of Engineering, Kothamangalam, Kerala, India.

ISSN: 2278 – 909X