Efficient Architecture of Medium Throughput AES Encryption

Harish B E
Electronics and communications Dept
VDRIT College of engineering and Technology
Haliyal, India

Asst. Prof. Prasanna D Kulkarni
Electronics and Communications Dept
VDRIT college of engineering and Technology
Haliyal, India

***Abstract*— This paper presents an efficient architecture design of Advanced Encryption Standard (AES) algorithm for medium throughput applications. The proposed AES architecture for encryption has been implemented in Sparten-3E device on Xilinx FPGA board. With low hardware utilization, it achieves a medium throughput of 1.2Gbps and also it has low power dissipation.**

Keywords*— AES Encryption, Low Cost Architecture, FPGA Implementation

INTRODUCTION

With the increasing proliferation of images, videos and other multimedia data over the unsecured network, such as Internet, there is a serious need to encrypt those, so as to provide the security and privacy [1, 2].Advanced Encryption Standard (AES) algorithm adopted by National Institute of Standards and Technology (NIST) is a private key encryption algorithm which is widely used for the encryption and decryption [3].Although, AES can be implemented in software, its hardware implementation provides high speed with added physical security [4]. Hardware implementation can have different approaches like very high, medium and low throughput architectures trading-off area for speed, etc. There are very high throughput (range 5-30 Gbps) architectures in the literatures [5-8]. But, they cost more hardware for their implementation. Some devices such as in the field of wireless sensor network use single chip for multitasking operations [9]. So, low area implementation with medium throughput becomes an important issue here. Also, in the field of video and image encryption, simultaneous encryption and compression is done [10]. Because, the compression is of medium throughput (in Mbps) range, very high throughput will not serve any extra advantage and therefore, medium throughput implementation is unavoidable.

AES is a private key encryption algorithm consisting of following transformations-SubBytes, ShiftRows, MixColumns and AddRoundKeys [11]. AES encrypts data in blocks of 128-bits. It can accept three key sizes, 128-bit, I92-bit and 256-bit, but generates 128-bit round key for XORing with 128-bit data in the AddRoundKeys step. The number of rounds for 128-bit keys, 192-bit keys and 256-bit keys are 10, 12 and 14 respectively. Figure I shows the encryption steps and number of rounds involved for 128-bit key size. In this paper, we have proposed efficient. The proposed architecture has a medium throughput of 1.2Gbps and also, it has 10w power consumption as compared to existing medium throughput AES architecture.

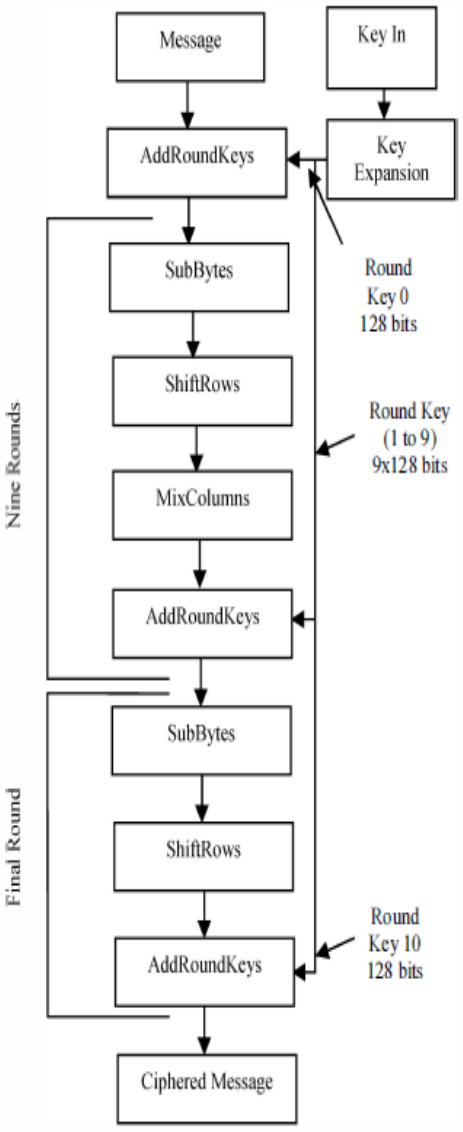
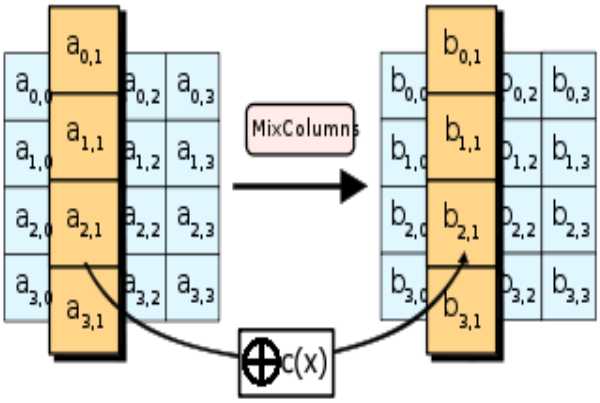


Figure l. AES Encryption steps for 128-bit key size

I. PROPOSED AES ARCHITECTURE



Figer 2 Mixcolumns operation

In the MixColumns step, the four bytes of each column of the state are combined using an XOR with fixed Matrix. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. During this operation, each column of the state is XOR by a fixed matrix:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Key expansion procedure generates 11 round keys (each of 128 bits) including the initial input key. It can be stored in registers. In the VLSI design, a single bit register takes higher area as compared to single bit ROM. So, the proposed architecture employs ROM to store the 10x128-bit Round keys. Figure 2 shows the round key storage module in ROM. There are 40 ROM sub-modules used for generation of 10 round keys. Each ROM consists of 8-bit in 4 locations.

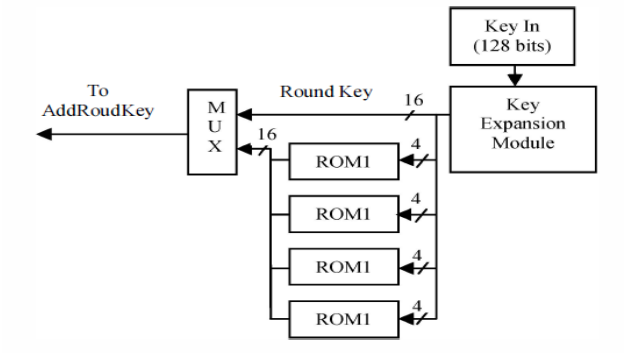


Figure 2. Round Key storage in ROM

Byte (0)	Byte (4)	Byte (8)	Byte (12)
Byte (1)	Byte (5)	Byte (9)	Byte (13)
Byte (2)	Byte (6)	Byte (10)	Byte (14)
Byte (3)	Byte (7)	Byte (11)	Byte (15)

Note: Byte values represent the state

II. FPGA IMPLEMENTATION AND COMPARISON

The AES architecture is implemented in pipelining mode. The architecture in [9] has been taken for comparison as it has medium throughput. It can be observed that the proposed architecture has high hardware efficiency in terms of throughput per slice. The power consumption results have been obtained from the XPower analyzer tool integrated in Xilinx ISE 13.1. The RTL code of the proposed architecture is written in VHDL. Simulation is done in Xilinx ISE 13.1 environment. Figure 3 shows the plaintext, key and the encrypted output and Figer 4 shows the plaintext, key and the decrypted output. The design is implemented in Spartan-3E board for prototyping and testing silicon validation.

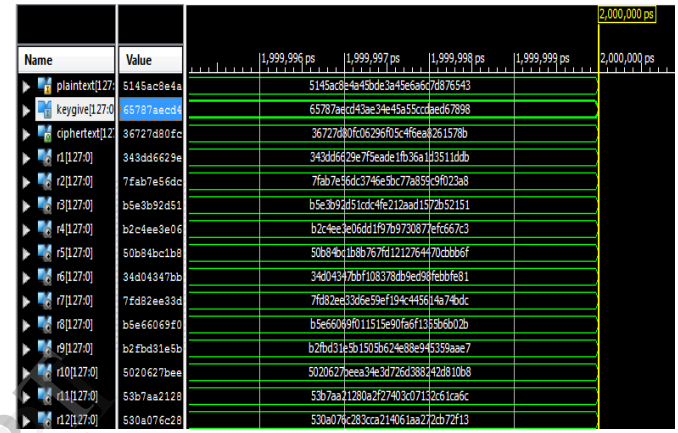


Figure 3 RTL simulation result showing 16 bytes plaintext, key and encrypted output

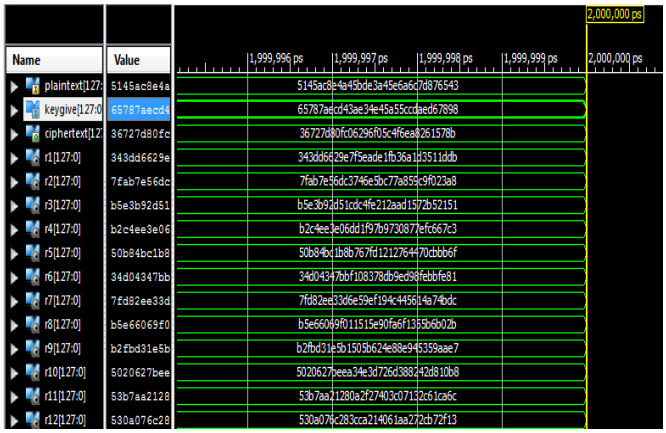


Figure 4 RTL simulation result showing 16 bytes ciphertext, key and decrypted output

In Encryption we give input as plaintext, key result shows encrypted output. Similarly, In Decryption we give input as cipertext and key result shows original output.

III. CONCLUSION

The efficient AES architecture for medium throughput has been designed and implemented in Xilinx FPGA. Mixcolumns transformation has been done by a special efficient module. The proposed architecture is efficient in terms of throughput per slice (area) and also consumes less power on comparison with existing architecture of medium throughput. The area reduction is done by storing the round keys in ROM instead of registers. Mixcolumns transformation has been done by a special efficient module.

REFERENCES

[1] Shujun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, KwokTung Lo, "On the Design of Perceptual MPEG-Video Encryption Algorithms," IEEE Transactions on Circuits and Systems for Video Technology, vo1.l7 (2), pp.214-223, Feb. 2007.

[2] Amit Pande and .Ioseph Zambreno, 'Advances in Multimedia Encryption' Springer London, 2012, pp. I 1-22.

[3] B. Bahrak and M.R. Aref, "Impossible differential attack on seven-round AES-128," lET Information Security, vo1.2 (2),pp.28-32, 2008.

[4] Ming-Haw .Iing, Zih-Heng Chen, .lian-Hong Chen and Yan-Haw Chen, "Reconfigurable system for high-speed and diversified AES using FPGA," Microprocessors and Microsystems, vol.31 (2), pp. 94-102 Mar. 2007. 978

[5] Chih-Pin Su, Tsung-Fu Lin, Chih-Tsun Huang, and Cheng-Wen Wu, "A High-Throughput Low-Cost AES Processor," IEEE Communications Magazine, vo1.41 (12), pp.86-91,Dec. 2003.

[6] Chih-Peng Fan and .Iun-Kui Hwang, "Implementations of high throughput sequential and fi.Jlly pipelined AES processors on FPGA," International Symposium on Intelligent Signal Processing and Communication Systems, 2007. ISPACS 2007, pp.353-356, Nov. 28 2007-Dec. 1 2007.

[7] Xinmiao Zhang and K.K Parhi, "High-speed VLSI architectures for the AES algorithm," IEEE Transactions on Very Large Seale Integration (VLSI) Systems, vo1.l2 (9), pp.957-967, Sept. 2004.

[8] A. Gupta, A. Ahmad, M.S.Sharif and A. Amira, "Rapid prototyping of AES encryption for wireless communication system on FPGA," 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), pp.571-575, 14-17. june 2011.

[9] .Iason Van Dyken, .lose G. and Delgado-Frias, "FPGA schemes for minimizing the power-throughput trade-ofI in executing the Advanced Encryption Standard algorithm," Journal of Systems Architecture, vol.56 (2-3), pp. 116-123, Feb.-Mar. 2010.

[10] M. Jridi and A. AlFalou, "A VLSI implementation of a new simultaneous images compression and encryption method," 2010 IEEE International Conference on Imaging Systems and Techniques (IST), pp.75-79, 1-2 July 2010.

[11] Federal Information Processing Standards Publication 197 (FIPS 197), available online, http://csrc.nist.gov/publications/fips/fips 197 /fips-197.pdf