IJESMR

International Journal OF Engineering Sciences & Management Research

A REVIEW ON ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM ON FPGA

Ku Sankalpa N. Moharir[1]
[1]Student, Digital Electronics, G.H.R.I.E.M., Jalgaon, India

KEYWORDS: AES, FPGA, VHDL, Encryption, Decryption, Cryptography.

ABSTRACT

A high speed security algorithm is always necessary and important for wired/wireless communication. The symmetric block cipher plays a major role in the bulk data encryption. One of the best existing symmetric security algorithms to provide data security is advanced encryption standard (AES). AES has the advantage of being implemented in both hardware and software. Hardware implementation of the AES has lot of advantage such has increased throughput and better security level. Hardware Implementation for generalized AES (Advanced Encryption Standard) encryption and Decryption has been made using VHDL.

INTRODUCTION

Cryptography is the study of Mathematical techniques for secured communication in the presence of adversaries and also it deals with the aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. The advanced encryption standard (AES), standardized by NIST, National Institute of Standards and Technology, is a cryptographic algorithm replacement to DES (Data Encryption Standard) algorithm as the federal standard to protect sensitive information. AES has already received wide spread use because of its high security, high performance in both hardware and software. Many implementations are done in software but it seems to be too slow for fast applications such as routers and some wireless communication systems. The several of AES hardware implementation architectures and optimizations have been suggested for different applications.

AES algorithm can resist any kinds of password attacks with a strong practicability in information security and reliability. AES can be implemented in software or hardware but, hardware implementation is more suitable for high speed applications in real time.

The common goal of cryptographic algorithms is providing security. From last several years, Data Encryption Standard (DES) had been used as a cryptographic algorithm. Due to the short key length of DES it is replaced by the Rijndael algorithm which has became as a standard in the cryptography domain, known as Advanced Encryption Standard (AES).

LITERATURE REVIEW

The system aims at reduced hardware structure. Compared with the pipeline structure, it has less hardware resources and high cost-effective. And this system has high security and reliability. This AES system can be widely used in the terminal equipments [1], [2].

The design uses an iterative looping approach with block and key size of 128 bits, lookup table implementation of S-box. This gives low complexity architecture and easily achieves low latency as well as high throughput. Simulation results, performance results are presented and compared with previous reported designs [4].

The implementation result on the targeted FPGA, the basic iterative AES encryption can offer the throughput of 3.85 Gbps at 300 MHz and one stage sub pipelined AES can offer the throughput to increase the efficiency of 6.2 Gbps at 481 MHz clock speed [5].

In order to improve the safety of data in transmission. The mathematic principle, encryption process and logic structure of AES algorithm are introduced. So as to reach the purpose of improving the system computing speed, the pipelining and parallel processing methods were used. The simulation results show that the high-speed AES encryption algorithm implemented correctly. Using the method of AES encryption the data could be protected effectively [7], [8].

There are two types of encryption algorithms, *Private or symmetric key* algorithms involve only one key for encryption and decryption is more suitable for faster implementation. Whereas, *Public or asymmetric key* algorithms involve two keys, one for encryption and other for decryption has complex and has very high computation time [12].

IJESMR

International Journal OF Engineering Sciences & Management Research

AES algorithm is implementation on FPGA in order to speed data flow and reduce time for key generating. To achieve higher performance hardware implementation is better speed and reliability .The AES algorithm is used in diverse application fields like WWW servers, automated teller machines (ATMs), cellular phones and digital video recorders [13].

PROPOSED WORK

AES encryption as shown in Fig. 2 consists of four operations.

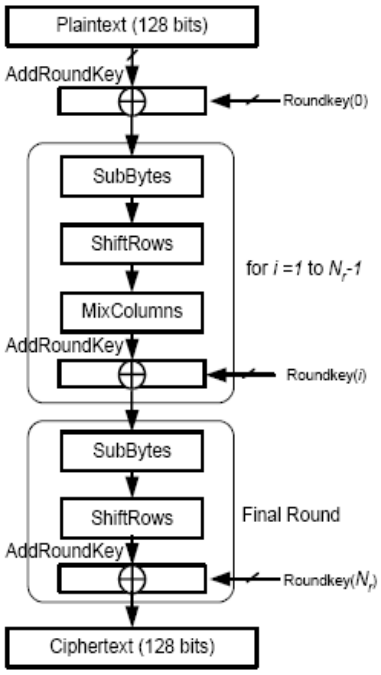

Fig. 2(a):- AES Encryption algorithm

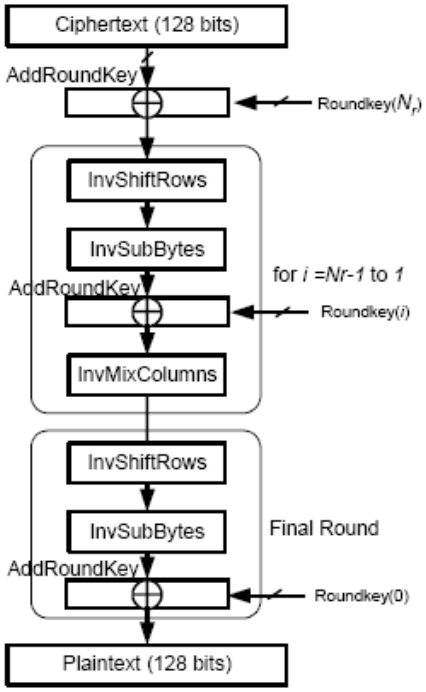

Fig. 2 (b):- AES Decryption Algorithm

As shown in Fig.2 (a), each of the first Nr −1 rounds consists of 4 transformations: Sub Bytes, Shift Rows, Mix Columns and Add Round Key. The final round excludes the Mix Columns transformation.

2.1 SUB BYTES:

This transformation is performed on each byte of the State using a substitution table(S-box). The S-box is constructed of the compositions of two transformations: multiplicative inverse in GF(28) with irreducible polynomial $m(x)+x^8+x^4+x^3+x+1$. And an affine mapping over GF(2) .

2.2 SHIFT ROWS:

In this transformation, the rows of the State shift cyclically to the left with different offsets. In the decryption process, the shifting offsets have different values.

2.3 MIX COLUMNS:

The Mix Colums transformation is performed on the State column-by-column. Each column is considered as a four-term polynomial over GF(2^8) and multiplied by a(x) modulo x^4 +1 , where $a(x)=\{03\}x^3+\{01\}x^2+\{01\}x+1$ for encryption and $a(x)=\{0B\}x^3+\{0D\}x^2+\{09\}x+\{0E\}$ for decryption.

2.4 ADD ROUND KEY:

In this transformation, a round key is added to the State using a bitwise Exclusive-OR (XOR) operation. Add Round Key is the same for the decryption process.

IJESMR

International Journal OF Engineering Sciences & Management Research

The decryption algorithm uses a different ordering of the inverse forms of the transformations used in the encryption algorithm as shown in Fig. 2(b). In the decryption process, the inverse S-box is used. The inverse S-box is constructed by first applying the inverse of the affine transformation and then computing the multiplicative inverse in GF(2^8) .

CONCLUSION

Encryption algorithm is being used by military and government over a last couple of decades for secure communication. The main purpose of encryption is to hide data from unauthorized usage. In this paper, we purposed a method to employ the crypto processor run in integration with a General Purpose Processor. In this direction, we have presented a pipeline version of AES algorithm that can encrypt data.

ACKNOWLEDGMENTS

My special thanks to all that experts who have contributed towards development of this research paper.

REFERENCES

1] *Daemen J., and Rijmen V, "The Design of Rijndael: AES-the Advanced Encryption Standard", Springer-Verlag, 2002*

2] *Ahmad, N.; Hasan, R.; Jubadi, W.M; "Design of AES S-Box usingcombinational logic optimization", IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 2010.*

3] *Mr. Atul M. Borkar, Dr. R. V. Kshirsagar and Mrs. M. V. Vyawahare, "FPGA Implementation of AES Algorithm", International Conference on Electronics Computer Technology (ICECT), pp. 401-405, 2011 3rd.*

4] *Khanob Thongkhome, Chalermwat Thanavijitpun, and Somsak Choomchuay, "An Implementation of S-Box for a Compact AES System," Proc. of 25th Int. Con [on Circuits/Systems, Computers, and Communications (ITC-CSCC2010), Pattaya, Thailand, July 2010*

5] *Chalermwat Thanavijitpun, Khanob Thongkhome, and Somsak Choomchuay, "FPGA Implementation of FOE-Portable hard disk System, "The Int. Conf on Information and CommunicationTechnology for Embedded Systems, Pattaya, Thailand, January2011*

6] *ShanxinQu, GuochuShou, YihongHu, ZhigangGuo, ZongjueQian. High Throughput Pipelined Implementation of AES on FPGA. International Symposium on Information Engineering and Electronic Commerce.2009*

7] *Jianghua Deng, Zhihua Hu, JipingNiu. The Implementation and research of AES Algorithm. Microcomputer Applications, 21(7), 2005.pp:58-59.*

8] *TianYun, Xu-Wen-Bo,Hu Bin. Xilinx ISE Design Suite 10.x Guide. Posts & Telecom Press, Bei jing, 2008*

9] *Wu Yuhua, Li Yanjun, Zhou Yukun. FPGA-based implementation and study of AES-128 algorithm. Microcomputer information, 2007.*

10] *Jongsung K, SeokhieH ,Preneel B. Related2Key RectangleAttacks on Reduced AES-192 and AES-256[C]/ / FSE 2007 ,LNCS 4593. Berlin : Springer-Verlag , 2007*

11] *L.Thulasimani and M. Madheswaran "A Single Chip Design and Implementation of AES -128/192/256 Encryption Algorithms," International Journal of Engineering Science and Technology, Vol. 2(5), 2010, 1052-1059.*

12] *Saurabh Kumar, V. K. Sharma, K. K. Mahapatra, "Low Latency VLSI Architecture of S-box for AES Encryption", Proc. International Conference on Circuits, Power and Computing Technologies, pp. 694-698 2013.*

13] *WANG Wei, CHENJie, XUFei, "An Implementation of AES Algorithm Based on FPGA", Proc. 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), pp. 1615-1617 2012*

IJESMR

International Journal OF Engineering Sciences & Management Research

AUTHOR BIBLOGRAPHY

Ku. Sankalpa N. Moharir
Received the degree in Electronics and Telecommunication from Sant Gadage Baba, Amaravti University.
Now persuing post graduation in Digital Electronics from Jalgaon.