ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Review on Implementation of Advanced Encryption Standard on Soft-core Processor

Amruta R.Dumane, Prof.N.G.Narole, Prof.Prashant Wanjari

M.Tech Student, Dept. of Electronics Engg. RGCER, Nagpur, Maharashtra, India.

Associate Professor, Dept. of Electronics Engg. RGCER, Nagpur, Maharashtra, India.

Associate Professor, Dept. of Electronics Engg. RGCER, Nagpur, Maharashtra, India.

ABSTRACT: With the rapid exchange of information in world, it becomes necessary to protect the data from unauthorized access. So, Security is the most important part in data communication system, where expansion in secret keys increases the security. The cryptographic algorithm uses the symmetric advanced encryption standard for both encryption and decryption purpose. Optimized code is designed for the implementation of 128- bit data encryption and decryption process. Xilinx ISE Embedded Development Kit softwareis used for synthesis purpose.

KEYWORDS:EDK, AES, Encryption and Decryption, ISE, cryptography.

I. Introduction

Cryptography is the science of writing the secret codes, enabling the confidentiality of communication through an insecure channel. It provides protection against unauthorized parties by preventing unauthorized alteration of use. It uses a cryptographic system to transform a information from paintext to cipher text, using private and public key. Basically, there are different types of cryptographic algorithm.

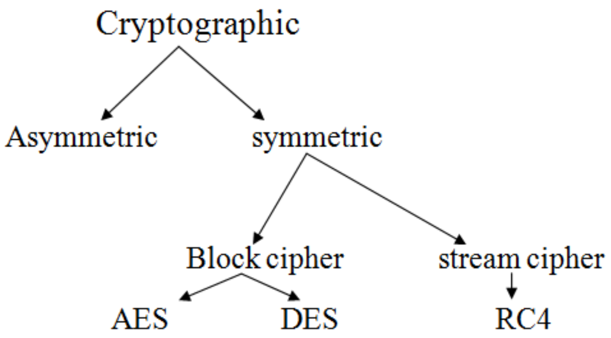

Fig1.Classification of Cryptographic algorithm

The Symmetric and asymmetric algorithm are classified according to use of the secret key. The different cryptographic algorithms are explained as follows:

RC4:

Stream cipher algorithm encrypts plaintext one byte at a time.RC4 is a stream cipher designed by Ron Rivest in 1987 for RSA security. It is a variable key-size stream cipher that provides byte-oriented operation. The algorithm is based on the use of random permutation.RC4 is used in the Transport Layer Security Standard that has been defined for communication between web browsers and servers.

DES:

Data Encryption Standard (DES) is a Feistel-type Substitution-Permutation Network (SPN) cipher. For DES, data are encrypted in 64-bit block using a 56- bit key. The same Steps and Key are used to reverse the encryption. The disadvantage of DES algorithm is that, size of Key is very short and it can easily decrytable. Disadvantage of DES algorithm removed by establishing the AES algorithm.

SMS4:

SMS4 is a 128-bit block cipher using 128-bit keys and 32 rounds to process a block. Declassified in 2006, SMS4 is used in the Chinese National Standard for Wireless Local Area Network (LAN) Authentication and Privacy Infrastructure (WAPI). SMS4 had been a proposed cipher for the Institute of Electrical and Electronics Engineers (IEEE) 802.11i standard on security mechanisms for wireless LANs, but has yet to be accepted by the IEEE or International Organization for Standardization (ISO).

AES:

Block cipher algorithm (AES) developed in 2001 by Belgium researchers. The Rijndael proposal for AES defined a cipher in which the block length and key length can be individually specified. AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256bits. The parameters of AES algorithm are explained as follows:

Table1. AES parameter

Algorithm	Key Length(words)	Block size(words)	No. of Rounds(words)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

II. LITERATURE SURVEY

A wide variety of cryptographic algorithm has been proposed in the literature:

Gurpreet Singh, Supriya [1]presented paper on "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security". Paper describes the detail study of different encryption algorithm such as RSA, DES, 3DES and AES.Author concluded that, all these technique are used for real-time encryption and decryption.AES algorithm is most efficient in terms of speed, time and Avalanche effect.

Xian Liu [2] Presented paper on "Small Logarithmic S-Boxes for Small Ciphers". In this paper, S-Box is defined by the logarithmic functions in GF (16).These S-Boxes can be used to construct a compact cipher for the devices with limited memory resources. These S-Boxes have the comparable or better properties than that designed with the inverse mapping.

WANG Wei, CHEN Jie, XU Fei [3] presented paper on "An Implementation of AES Algorithm Based on FPGA".In this paper, Pipeling and parallel methods were used for improving the computational speed. The author concluded that, the AES algorithm complete its whole process within 200MHZ clock rate. Implementation result was tested in Xilinx vertex-5FPGA.Author designed the top module of AES algorithm that consists of Round module, key expansion and control module.

M.Amr Mokhtar [4] presented paper on "High Performance Data Encryption based on Advanced Encryption Standard using FPGA".The AES algorithm was implemented on Spartan-6 FPGA. Encryption and Decryption algorithm was designed by using the stream cipher and block cipher method which increases the efficiency of the algorithm. Author concluded that image of 256*256 bit size was encrypted within 0.00053 seconds.

B.Subramanyan, VivekM.Chhabria, T.G.SankarBabu[5]presented paperon “Image Encryption Based on AES Key Expansion”. The algorithm had been experienced with standard bench mark images proposed in USC-SIPI database.Author concluded that, the key sensitivity and key space was very high which makes it resistant towards brute force attack and statistical cryptanalysis.

Yang Jun, Ding Jun, Li Na, Guo Yixiong[6] presented paper on “FPGA-based design and implementation of reduced AES algorithm”.In this paper, the designed system makes use of light external circuits that minimize the on-chip resources.The AES algorithm was designed and validated on the Altera Cyclone EP2C35F672C6 chip that reduces the hardware structure.

Chi-Wu Huang, che-Hao Chiang,Chien-lun Yen[7] presented paper on “The AES Application in image Using Different Operation Modes”. The algorithm was implemented by using different operation modes i.e.CBC, CFB, OFB and CTR etc.These operation modes have the feature to eliminate the patterns in terms of the degree of random noise in cipher image as well as the parallel operation in cipher blocks for high speed processing.

Tuan Anh Pham, Mohammad S. Hasan and Hongnian Yu [8] presented paper on “Area and Power Optimization for AES Encryption Module implementation on FPGA”.Author concluded that the implemented algorithm uses the 277 logic element and provides 5.88mw energy dissipation. Some techniques were developed to reduce the power consumption i.e.one-hot coding, clock gating.In this paper, AES algorithm implemented on Altera Cyclone II EP2C672C6.The algorithm was implemented on 8-bit architecture.

Hassan Anwar, Masoud Daneshtalab, Juha Plosila, Hannu Tenhunen [9]presented paper on “FPGA Implementation of AES-based Crypto Processor”.Media access control layer (MAC) had the ability to operate on different frequencies and provides flexibility. Algorithm was implemented with 32-bit processor. The 2 processor were used i.e. general purpose and crypto co-processor. Use of crypto processor provides the throughput of 58Gbps, latency of 240ns and minimum power consumption of 76mw at frequency of 553MHZ.

Manoj Kumar Sahoo, Akash Gaurav, Kaliprasanna Swain[10] presented paper on “Implementation of AES Algorithm on Microblaze Soft processor”.Author uses 32 bit microblaze processor for implementation.The result of implementation were tested on spartan 3 family of FPGA. Advanced encryption Standard algorithm (AES) implemented on soft microcontroller using Verilog Xilinx EDK environment.

G.H.Karimian, B.Rashidi and A.Farmani[11] presented paper on “A High Speed and Low Power Image Encryption With 128-Bit AES Algorithm”.Resource sharing, pipelining and signal gating method were used for implementation.The image of 32*32 sizes is encrypted in 1.25ms.

Angelo Barnes, Ryan Fernando, Kasuni Mettananda [12] presented paper on “Improving the Throughput of the AES Algorithm with Multicore Processors”.Author uses 2 different algorithm for implementation .The first is with fork system call in Linux and 2nd with Pthreads.Both the algorithm performed on different multiprocessor.

AES is cryptographic algorithm that protects the data from unauthorized access. Different technique will be developed for implementation of AES algorithm. Implementation of AES algorithm using VHDL code became a complex process and it became hard to analyze it on FPGA kit. So, in order to reduce the complexity, the Soft-core processor will be used.

III. CONCLUSION

Encryption algorithm is beingused by military, bank and other government sector during the last couple of decade. The main purpose of encryption is to protect the data or confidential information during the transmission over the communication channel. In this paper, AES algorithm will be implemented on soft-core processor. The use of soft-core processor reduces the complexity of the algorithm.

REFERENCES

2. Xian Liu "Small Logarithmic S-Boxes for Small Ciphers",IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" proceedings,978-1-4244-2324-8,08. 2008.
3. WANG Wei, CHEN Jie, XU Fei "An Implementation of AES Algorithm Based on FPGA",IEEE,9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012), 978-1-4673-0024-7/10,2012.
4. M. AmrMokhtar"High Performance Data Encryption based on Advanced Encryption Standard using FPGA",IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 6, 2014.
5. B.Subramanyan, Vivek.M.Chhabria"Image Encryption Based On AES Key Expansion",IEEE,2011 Second International Conference on Emerging Applications of Information Technology 978-0-7695-4329-1/11, 2011.
6. Yang Jun Ding Jun Li Na Guo Yi xiong "FPGA-based design and implementation of reduced AES algorithm", IEEE, 978-0-7695-3972-0/10, 2010.
7. Chi-Wu Huang, Che-Hao Chiang, Chien-Lun Yen, Yi-Cheng Chen, Kuo-Huang Chang and Chi-Jeng Chang "The AES Application in Image Using Different Operation Modes", IEEE,978-1-4244-5046-6/10, 2010.
8. Tuan Anh Pham, Mohammad S. Hasan and Hongnian Yu "Area and Power optimization for AES encryption module implementation on FPGA"Proceedings of the 18th International Conference on Automation & Computing, Loughborough University, Leicestershire, UK, 8 September 2012.
9. Hassan Anwar, Masoud Daneshtalab, Masoumeh Ebrahimi, Juha Plosila, Hannu Tenhunen "FPGA Implementation of AES-based Crypto Processor",IEEE , 978-1-4799-2452-3/13, 2013.
10. Kaliprasanna Swain, Manoj Kumar Sahoo, Akash Gaurav "Implementation of AES Algorithm on Microblaze soft Processor", International Journal of Engineering Sciences and Research Technology, July 2015.
11. G. H. Karimian, B. Rashidi, and A.farmani "A High Speed and Low Power Image Encryption with 128-Bit AES Algorithm ",International Journal of Computer and Electrical Engineering, Vol. 4, No. 3, June 2012.
12. Angelo Barnes, Ryan Fernando, Kasuni Mettananda and Roshan Ragel "Improving the Throughput of the AES Algorithm with Multicore Processors". JAN 2012.

BIOGRAPHY

Miss.Amruta R. Dumaneis presently pursuing final semester M.Tech in Electronics at Rajiv Gandhi College of Engineering and Research, Nagpur. She received B.Tech degree in Electronics and Tele-communication from Dr.BATU, Lonere.Her areas of interest are VLSI and VHDL.