ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Implementation of Advanced Encryption Standard (AES) Algorithm on FPGA

Sankalpa N. Moharir[1], Manoj Bagde[2]

PG student [Digital Electronics], Dept. of Electronics, G.H.R.I.E.M. Jalgaon, Jalgaon Maharashtra, India[1]

Assistant Professor, Dept. of Electronics G.H.R.I.E.M. Jalgaon, Jalgaon Maharashtra, India[2]

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.

KEYWORDS: FPGA, VHDL, Encryption, Decryption, Cryptography

I.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.

Each day millions of users generate and interchange large volumes of information in various fields, such as financial and legal files, medical reports and bank services via Internet. These and other examples of applications deserve a special treatment from the security point of view, not only in the transport of such information but also in its storage. In this sense, cryptography techniques are especially applicable. This implementation will be useful in wireless security like military communication and mobile telephony where there is a greater emphasis on the speed of communication.

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).

II.LITERATURE REVIEW

The AES is a cryptographic algorithm that is used to encrypt (encipher), and decrypt, (decipher), information. Key Expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedures. 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. We describe compact data path architecture for Rijndael, where the

DOI:10.15662/IJAREEIE.2016.0506068

hardware resources are efficiently shared between encryption and decryption. The key arithmetic component S-Box has been implemented using look-up table logic or ROMs in the previous approaches, which requires a lot of hardware support This AES system can be widely used in the terminal equipments [1], [2].

The implementation of FPGA based AES algorithm is cryptography. The cryptography is the science of secret codes enabling the confidentiality of communication through insecure channel. Cryptosystems can provide confidentiality, authenticity, integrity, and non repudiation services. It protects against unauthorized parties by preventing unauthorized alteration of use. Generally speaking, it uses a cryptographic system to transform a plaintext into a cipher text, using most of the time a key. To increase the computational speed parallelism and pipelining architecture have been implemented. The simulation is done using Xilinx 13.2 version. It does not provide availability of data or systems. The salient feature of AES encryption and decryption are high throughput, parameter flexibility, implantation flexibility, no known security attack Confidentiality means that unauthorized parties cannot access information. Authenticity refers to validating the source of the message to ensure the sender is properly identified. Integrity provides assurance that the message was not modified during transmission, accidentally or intentionally. Non repudiation means that a sender cannot deny sending the message at a later date, and the receiver cannot deny receiving it. Cipher is any method of encrypting text (concealing its readability and meaning). It is also sometimes used to refer to the encrypted text message itself. A block cipher is one that breaks a message up into chunks and combines a key with each chunk (for example, 64-bits of text) [3].

To reduce the propagation delay of the S-Boxes, we developed a special logic circuit architecture named twisted-BDD, where the fan-out of signals is distributed in the S-Box. The T-Box algorithm that merges the S-Box and MixColumns function is also used. As far as the authors know, this is the first 10 Gbps AES circuit which can support all encryption modes. 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].

This describes a high effective AES core hardware architecture for implementing it to encrypt/decrypt the data in portable hard disk drive system that apply to effectively in the terms of speed, scale size and power consumption to comply with minimum speed of 5 Gbps (USB3.0). We proposed the 128 bits data path of two different AES architectures design, Basic Iterative AES, which reuses the same hardware for all the ten iterations and, One Stage Sub Pipelined AES, with one stage of outer pipelining in the data blocks that both of them are purely 128 bits data path architecture that different from the previous public paper. 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].

There is a use of FPGA chips to realize the high throughput 128 bits AES cipher processor with new high-speed and hardware sharing functional blocks. The AES functional calculations include four transformation stages, which are the Sub-Bytes, the Shift-Rows, the Mix-Columns and the Add Round Key. First, the content-addressable memory (CAM) based scheme is used to realize the proposed pipelined high-speed Sub-Bytes block. Second, the new hardware sharing architecture is applied to implement the proposed high-speed Mix-Columns block. Then the efficient low-cost Add Round Key architecture is used for real-time key generations [6].

AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for security is the key. In this project new AES algorithm with encryption and decryption was realized in Verilog Hardware Description Language. The 128-bit plaintext and 128-bit key, as well as the 128-bit output data were all divided into four 32-bit consecutive units respectively controlled by the clock. The current Area Optimized algorithm of AES are mainly based on the realization of S-box mode and the minimizing of the internal registers which could save the area of IP core significantly. 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].

DOI:10.15662/IJAREEIE.2016.0506068

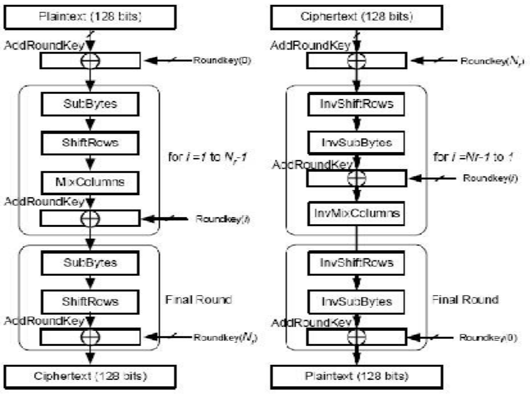
This paper presents a single chip encryptor /decryptor core implementation of Advanced Encryption Standard (AES-Rijndael) cryptosystem. The suggested architecture is capable of handling all possible combinations of standard bit lengths (128,192,256) of data and key. The architecture does reutilize pre-computed blocks, in the sense that the same hardware is shared during encryption and decryption as much as possible. AES algorithm proposed by NIST has been widely accepted as best cryptosystem for wireless communication security. Each algorithm is tested with sample vectors provided by NIST output results are perfect with minimal delay. The AES algorithm is an iterative private key symmetric block cipher that can process data block of 128- bits through the use of cipher keys with key length 128,192 and 256 bits. An efficient FPGA implementation of 128 bit block and keys 128, 192 and 256 bits of AES –Rijindael algorithm has been presented in this paper. Optimized and synthesizable VHDL code is developed for implementation of all AES-128/192/256 bit key encryption and is verified using xilinx ISE 9.2 simulation tool [11].

There are two types of encryption algorithms, We have further optimized delay and area of the conventional S-box architecture by using some efficient logic and multiplexers in the critical path. The proposed optimized S-box architecture has been implemented in 0.18 μm ASIC technology as well as Xilinx FPGA. An optimized architecture of S-box for AES encryption is proposed. *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. This novel architecture is implemented both in ASIC as well as FPGA. The ASIC implementation indicates speed improvement compared to conventional structure while maintaining area constant. FPGA implementation shows improvement in delay and area while a significant enhancement in terms of power compared to conventional architecture [12]

The mathematic principle, encryption process and logic structure of AES algorithm are introduced. So as to reach the porpose of improving the system computing speed, the pipelining and papallel 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. With the development of Computer Network and Communication Technology, a great mass of data and information need to be exchanged by public communication networks. High efficiency and high safety of Data transmission become much more important. 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].

III.PROPOSED WORK

AES encryption as shown in Fig. 1 consists of four operations



(a) Encryption (b) Decryption

Fig. 1(a):- AES Encryption Algorithm (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.

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) .

1. Shift Rows: In this transformation, the rows of the State shift cyclically to the left with different offsets[2]. In the decryption process, the shifting offsets have different values.

2. 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.

3. 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.

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 $GF(2^8)$.

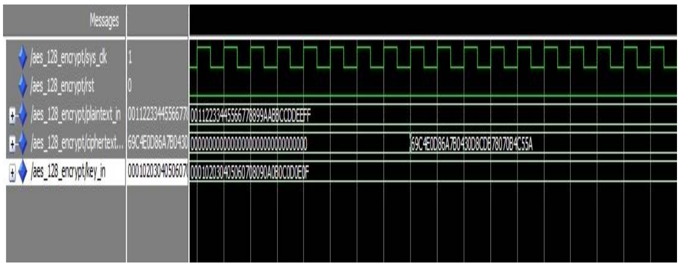
IV.RESULT AND DISCUSSION

A. Simulation Of Encryption

The Table IV shows the inputs and output of the Encryption. In AES Encryption we are using 128 bit plain text and encryption key as an input, we are getting 128 bit cipher text as an output. The simulation waveform is shown in fig. 4.1.

Table I:
AES Encryption Plain text, Key, Cipher text.

128 Bit Plain Text (Input)	00112233445566778899aabbccddeeff
128 Bit Encryption Key (Input)	000102030405060708090a0b0c0d0e0f
128 Bit Cipher Text (Output)	69c4e0d86a7b0430d8cdb78070b4c55a



```
Messages
/aes_128_encrypt/sys_clk            1
/aes_128_encrypt/rst                0
/aes_128_encrypt/plaintext_in       0011223344556677   00112233445566778899AABBCCDDEEFF
/aes_128_encrypt/ciphertext...      69C4E0D86A7B0430   00000000000000000000000000000000   69C4E0D86A7B0430D8CDB78070B4C55A
/aes_128_encrypt/key_in             0001020304050607   000102030405060708090A0B0C0D0E0F
```

Fig. 2 :Simulation Of Encryption.

The above figure shows the simulation of AES algorithm by using the FPGA platform in the model-sim software. Its show the description of transformation of plain text and cipher text using the cipher key.

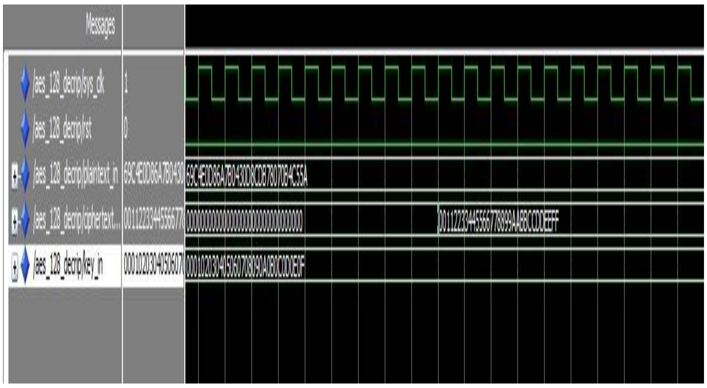
B. Simulation of Decryption:

The Table II shows the inputs and output of the Decryption. In AES Decryption we are using 128 bit plain text and decryption key as an input, we are getting 128 bit cipher text as an output. The simulation waveform is shown in fig. 3.

Table II :

AES Decryption Plain text, Key , Cipher text.

128 Bit Decryption Plaintext (Input)	69c4e0d86a7b0430d8cdb78070b4c55a
128 Bit Decryption Key (Input)	000102030405060708090a0b0c0d0e0f
128 Bit Cipher text (Output)	00112233445566778899aabbccddeeff



```
Messages
/aes_128_decrip/sys_clk        1                  
/aes_128_decrip/rst            0                  
/aes_128_decrip/plaintext_in   69C4E0D86A7B0430   69C4E0D86A7B0430D8CDB78070B4C55A
/aes_128_decrip/ciphertext...  0011223344556677   00000000000000000000000000000000   00112233445566778899AABBCCDDEEFF
/aes_128_decrip/key_in         0001020304050607   000102030405060708090A0B0C0D0E0F
```

Fig.3 : Simulation of AES Decryption.

The above figure shows the simulation of AES algorithm by using FPGA platform in the model-sim software. The figure describes about the transformation of cipher text to plain text using cipher in descryption.

V.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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

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),.pp:58-59. 2005

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), 1052-1059. 2010

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.