A Review on Implementation of AES Algorithm Using FPGA

Prof. N. N. Kasat S. A. Varhade Dr. M. S. Ali

Abstract— **Everyday many users generate and interchange large amount of information in various fields through Internet, telephone conversations etc. These and other examples of applications required a security, not only in the transport of such information but also in its storage. Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an approved cryptographic algorithm that is used to protect electronic data. As we share the data through wireless network it should provide data confidentiality, integrity and authentication. 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 128 bit AES (Advanced Encryption Standard) encryption and Decryption has been made using VHDL. The proposed algorithm for encryption and decryption module will functionally verified using modelsim, will be synthesize using Quartus 2 using Altera FPGA platform and analyze the design for the power, Throughput & area.**

Index Terms— **AES, Decryption, Encryption, FPGA, Security, VHDL.**

I. INTRODUCTION

In today's world most of the communication is done using electronic media. 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. Data Security plays a vital role in such communication. So cryptography is
constantly increasing sensitive data is more vulnerable from automated spying and high efficiency and safety of Data transmission Hence, there is a need to protect data from

malicious attacks. Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. 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. 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.

The Advanced Encryption Standard (AES) was published by the National Institute of Standards and Technology (NIST) in 2001. AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. Compared to public-key ciphers such as RSA, the structure of AES and most symmetric ciphers is quite complex and cannot be explained as easily as many other cryptographic algorithms. Accordingly, the reader may wish to begin with a simplified version of AES. AES has already received widespread 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 various of AES hardware implementation architectures and optimizations have been suggested for different applications. AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. FPGA Are hardware devices whose function is not fixed which can be programmed in system. The potential advantage of encryption algorithm implemented in FPGAs includes: Algorithm agility- This term refers to the switching of cryptographic algorithm during operation. Algorithm upload- It is perceivable that fielded devices upgraded with new encryption algorithm which did not exist at design time. Algorithm modification- There are applications which require modification of a standardized algorithm. Architecture efficiency- With FPGAs it is possible to design and optimize architecture for specific parameter set. VHDL is the VHSIC Hardware Description Language. A methodology and a toolset are essential for the effective use of VHDL. Simulation and synthesis are the two main kinds of tools which operate on the VHDL language.

II. LITERATURE REVIEW

Wang Wei, Chen Jie , Xu Fei [1] introduced 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.
Yang Jun ,Ding Jun Li, Na Guo Yixiong [2],[3] presented 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. AES encryption algorithm includes key expansion process and encryption process.The overall structure of the designed reduced AES encryption and decryption system in which the upper half part is the encryption unit, the second part is the decryption unit.
Hoang Trang , Nguyen Van Loi [4] presented FPGA-based implementation of the Advanced Encryption Standard (AES) algorithm. 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.

Kbanob Thongkhome, Chalermwat Thanavijitpun [5] presented 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. AES core of portable hard disk can be design in either Basic iterative AES or One Stage Sub-pipeline AES structure according to the data rate needed. The same set of hardware is reused for all the ten iterations. This architecture is entirely based on the iterative approach of design for encryption algorithms.

III. PROPOSED WORK

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption. Encryption converts data to an unintelligible form called cipher-text. Encryption of the cipher-text converts the data back into its original form, which is called plain-text. The AES has fixed 128-bit block ciphers with cryptographic key sizes of 128 bits. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard(DES) Feistel network [10] . In 1997, the NIST initiated a five-year algorithm development process to replace the DES and Triple DES. The NIST algorithm selection process facilitated open collaboration and communication and included a close review of 15 candidates. After an intense evaluation, the Rijndael design, created by two Belgian cryptographers was the final choice.

AES ALGORITHM:

The AES algorithm operates on a fixed block size 128-bit data. The first and last rounds are somewhat different from other rounds in sense that there is an additional AddRoundKey transformation at the start of the first round and MixColumns transformation is not performed in the last round. In this paper, we use 128 bit data and also key length of 128 bits (AES-128).

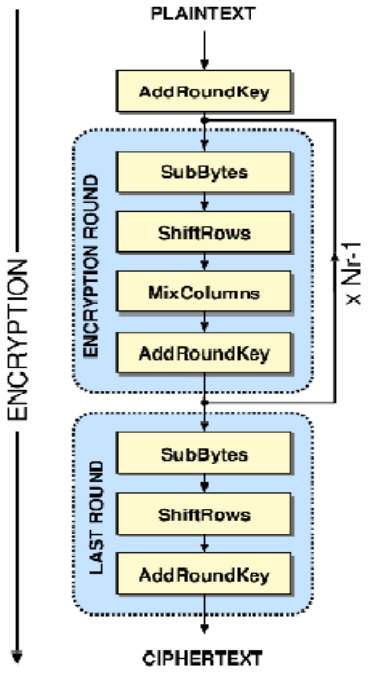

Fig.1. AES Encryption.

AES Encryption :

Encryption converts data to an unintelligible form called cipher-text. Decryption of the cipher-text converts the data back into its original form, which is called plain-text The AES algorithm operates on a 128-bit block of data and executed Nr - 1 loop times. A loop is called a round and the number of iterations of a loop, Nr, can be 10**,** 12, or 14 depending on the key length. The key length is 128, 192 or 256 bits in length respectively. The first and last rounds differ from other rounds in that there is an additional AddRoundKey transformation at the beginning of the first round and no MixCoulmns transformation is performed in the last round. In this paper, we use the key length of 128 bits (AES-128) as a model for general explanation. .AES encryption as shown in Fig. 1 consists of four operations as follows.

- *SubBytes Transformation:* SubBytes transformation is a non-linear byte substitution, operating on each of the state bytes independently. The SubBytes transformation is done using a once- precalculated substitution table called S-box. That S-box table contains 256 numbers (from 0 to 255) and their corresponding resulting values. Fig. 2 shows SubBytes Transformation.

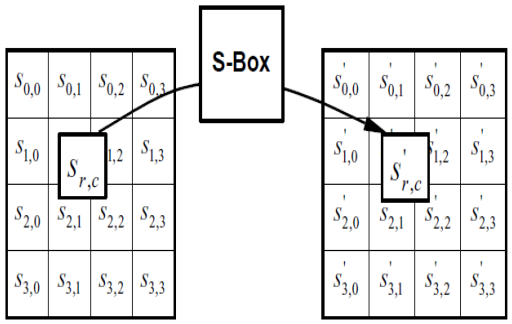

Fig.2. SubBytes Transformation

- *ShiftRows Transformation:* In ShiftRows transformation, the rows of the state are cyclically left shifted over different offsets. Row 0 is not shifted; row 1 is shifted one byte to the left; row 2 is shifted two bytes to the left and row 3 is shifted three bytes to the left. Fig. 3 shows ShiftRows Transformation

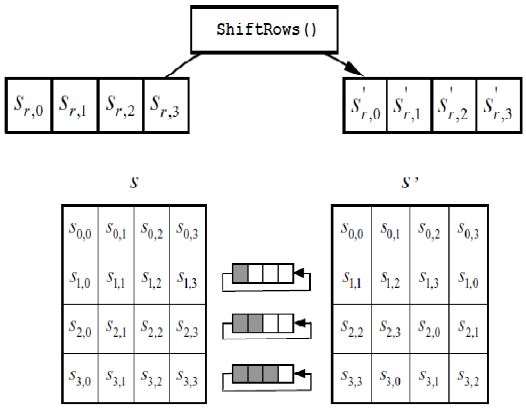

Fig. 3. ShiftRows Transformation

- *MixColumns Transformation:* In MixColumns transformation, the columns of the state are considered as polynomials over GF (2^8) and multiplied by modulo x4 + 1 with a fixed polynomial c(x), given by: c(x)={03}x3 + {01}x2 + {01}x + {02}.*Fig. 4 shows MixColumn Transformation.*

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad \text{for } 0 \le c < Nb.$$

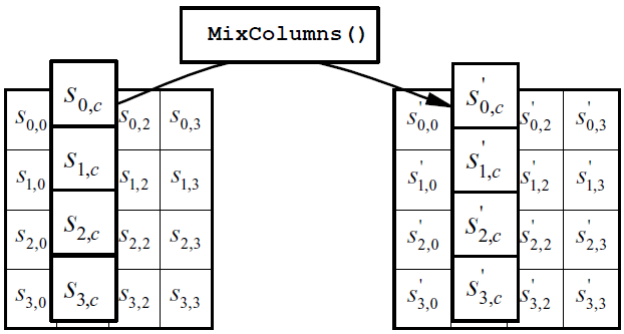

Fig. 4 MixColumn Transformation.

- *AddRoundKey Transformation:* In the AddRoundKey transformation, a Round Key is added to the State - resulted from the operation of the MixColumns transformation - by a simple bitwise XOR operation. The RoundKey of each round is derived from the main key using the KeyExpansion algorithm. The encryption/ decryption algorithm needs eleven 128-bit RoundKey, which are denoted RoundKey[0] RoundKey[10].Fig. 5 shows AddRoundKey Transformation.

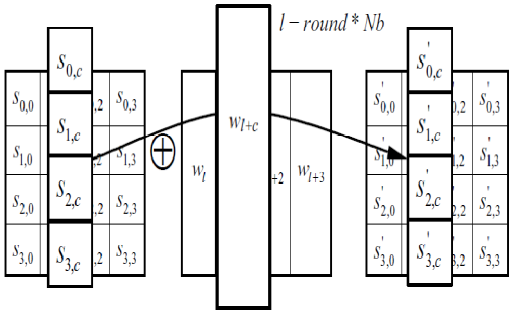

Fig. 5. AddRoundkey Transformation.

AES Decryption :

Decryption is a reverse of encryption which inverse round transformations to computes out the original plaintext of an encrypted cipher-text in reverse order. The round transformation of decryption uses the functions AddRoundKey, InvMixColumns, InvShiftRows, and InvSubBytes successively. AES Decryption shown in fig. 6.

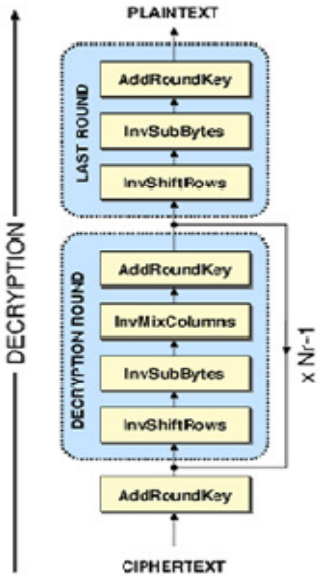

Fig. 6 AES Decryption.

- *AddRoundKey*: AddRoundKey is its own inverse function because the XOR function is its own inverse. The round keys have to be selected in reverse order. Fig. 7 shows AddRoundkey Transformation.

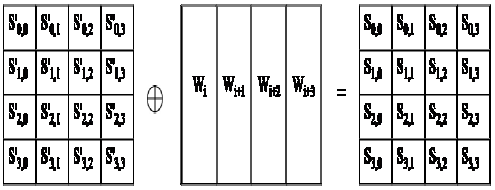

Fig. 7 AddRoundKey Transformation.

- InvMixColumn Transformation: InvMixColumns transformation is done using polynomials of degree less than 4 over GF(2^8), which coefficients are the elements in the columns of the state, are multiplied modulo ($x4 + 1$) by a fixed polynomial $d(x) = \{0b\}x3 + \{0d\}x2 + \{09\}x + \{0e\}$, where $\{0b\}$, $\{0d\}$; $\{09\}$, $\{0e\}$ denote hexadecimal values. Fig. 8 shows InvMixColumns Transformation.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad \text{for } 0 \le c < Nb$$

Fig. 8 InvMixColumn Transformation.

- *InvSubBytes Transformation*: The InvSubBytes transformation is done using a once precalculated substitution table called Inv S-box. That Inv S-box table contains 256 numbers (from 0 to 255) and their corresponding values. Fig. 9 shows InvSubBytes Transformation.

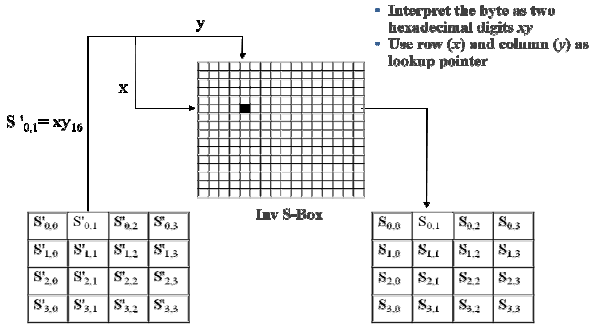

Fig. 9 InvSubBytes Transformation

- *InvShiftRows Transformation:* InvShiftRows exactly functions the same as ShiftRows, only in the opposite direction. The first row is not shifted, while the second, third and fourth rows are shifted right by one, two and three bytes respectively.Fig. 10 shows InvShiftRows Transformation.

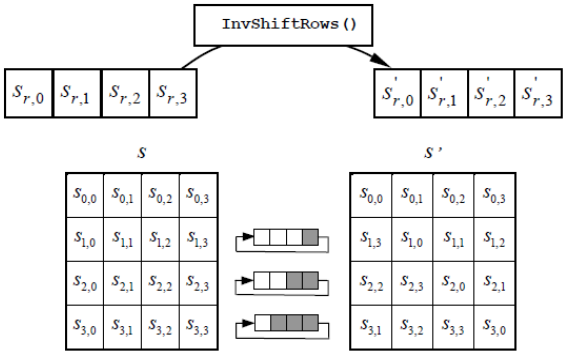

Fig. 10 InvShiftRows Transformation.

IV. CONCLUSION

AES algorithm can resist any kinds of password attacks with a strong practicability in information security and reliability. The AES algorithm can be efficiently implemented by software. Software implementations cost the smallest resources, but they offer a limited physical security and the slowest process. Besides, growing requirements for high speed, high volume secure communications combined with physical security,

hardware implementation of cryptography takes place. The Advanced Encryption Standard algorithm is a symmetric block cipher that can process data blocks of 128 bits through the use of cipher keys with lengths of 128 bits.

REFERENCES

[1] WANG Wei,CHEN Jie,XU Fei, "An Implementation of AES Algorithm Based on FPGA",Proc. 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD),pp. 1615-1617 2012

[2] Yang Jun Ding Jun Li Na Guo Yixiong "FPGA-based design and implementation of reduced AES algorithm," 2010 International Conference on Challenges in Environmental Science and Computer Engineering.

[3] Chih-Chung Lu， Shau-Yin Tseng. Integrated Design of AES(Advanced Encryption Standard) Encrypter and Decrypter[C]. Proceedings of the IEEE International Conference on Application-specific Systems，Architectures，and Processors(ASAP'02)，California，2002

[4] Hoang Trang, Nguyen Van Loi "An efficient FPGA implementation of the Advanced Encryption Standard algorithm" IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699 2012

[5] Kbanob Thongkhome, Chalermwat Thanavijitpun ,"A FPGA Design of AES Core Architecture for Portable Hard Disk" 20ll Eighth International Joint Conference on Computer Science and Software Engineering (JCSSE)

[6] 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 ComputingTechnologies, pp. 694-698 2013.

[7] PRAVIN B. GHEWARI1 MRS. JAYMALA K. PATIL1 AMIT B. CHOUGUL, " Efficient Hardware Design and Implementation of AES Cryptosystem" International Journal of Engineering Science and Technology Vol. 2(3), 2010, 213-219

[8]. Amaar, I. Ashour and M. Shiple " Design and Implementation A Compact AES Architecture for FPGA Technology", World Academy of Science, Engineering and Technology 59 2011.

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

[10] William Stallings, " Cryptography and Nework Security", Third Edition, Pearson Education, 2003