A Review on Implementation of AES Algorithm Using FPGA

[1]Asawari Ujjainkar, [2]Prof. A.B. Kharate

Department of Electronics and Tele-communication,
Amravati University, Amravati, India

Abstract: Now a day's large number of internet and wireless communication users has led to an increasing demand of security measures and devices for protecting the user data transmitted over the unsecured network so that unauthorized persons cannot access it . As we share the data through wireless network it should provide data confidentiality, integrity and authentication. The symmetric block cipher plays a major role in the bulk data encryption. Advanced Encryption Standard (AES) provides data security. 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.

Keywords: AES, Encryption, Decryption, FPGA, VHDL, Security.

I.INTRODUCTION

In today's world most of the communication is done using electronic media. Data Security plays a vital role in such communication. Increasing need of data handle in Computer Network and Communication Technology capable to great mass of data and information need to be exchanged by public communication networks. 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 applicationsdeserve a special treatment from the security point of view, notonly 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. Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against unauthorised parties by preventing unauthorised 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 militarycommunication 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 quitecomplex and cannot be explained as easily as many other cryptographic algorithms. 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 communicationsystems. The various of AES hardware implementationarchitectures and optimizations have been suggested for different applications. . The AES algorithm is a symmetric block cipher that can encrypt and decrypt information. AES is based on a design principle known as a substitution- permutation network, combination of both substitution andpermutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network.

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. AES is an iterative group code with the Key. The encryption process includes an initial key-addition called AddRoundKey, then an initial roundconversion for 1 r N −times, finally a final round conversion again. All the round conversions and initial key-addition make a state and a Round Key as the input, and each cycle carries out four different operations to the Data flow, SubBytes, ShiftRows, It is incompatible to implement the AES algorithmon hardware between the throughput and hardware resource.

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 encryption process includes an initial AddRoundKey of the initial round, and then carries out several rounds of Round transformation, and the last round also carries out Round transformation 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. The AES algorithm operates on a 128-bit block of data and executed Nr - 1 loop times. A loop iscalled a round and the number of iterations of a loop, Nr, can be 10**,** 12, or 14 depending on the key length. The key lengthis 128, 192 or 256 bits in length respectively.

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-pipelineAES 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. The key expansion block generates the key required for the corresponding iteration on the fly. This design harnesses the parallelism in the AES algorithm and increases the throughput of the design.1t is an improvement of the basic iterative architecture with respect to speed. proposed AES core architecture can be chosen upon speed or throughput requirement for supporting portable hard disk data encryption.

Pravin B. Ghewari, Jaymala K. Patil [7] Presented the cryptographic algorithms can be implemented with software orbuilt with pure hardware. However Field Programmable Gate Arrays (FPGA) implementation offers quicker solution and can be easily upgraded to incorporate any protocol changes.

This contribution investigates the AES encryption and decryption cryptosystem with regard to FPGA and Very High Speed Integrated Circuit Hardware Description language (VHDL). Optimized and Synthesizable VHDL code is developed for the implementation of both 128- bit data encryption and decryption process.

A. Amaar, I. Ashour and M. Shiple [8] presented a compact implementation of advanced encryption standard AES using different devices of FPGA technology. This implementation can be carried out through several trade-off between area and speed. The main point of the proposed architecture is to compromise the area and speed. Register- Transfer-Level (RTL) is checked frequently to avoid redundant hardware creation. Proposed architecture is implementing 128 bits data- path for both cipher key and plaintext. The developed architecture combines basic architecture with one round and chopping technique to compromise the area with speed. the proposed architecture implements one sbox (256 byte).

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. The AEShas three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard(DES) Feistel network the Rijndael design, created by two Belgian cryptographers wasthe final choice.

The AES replaced the DES with new and updated features:

- Block encryption implementation.
- 128-bit group encryption with 128, 192 and 256-bitkey lengths
- Symmetric algorithm requiring only one encryptionand decryption key
- Data security for 20-30 years
- Worldwide access
- No royalties
- Easy overall implementation.

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. Fig.(a) shows simple encryption process in which conversion of plain text to cipher text is done by using key[10] . 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.

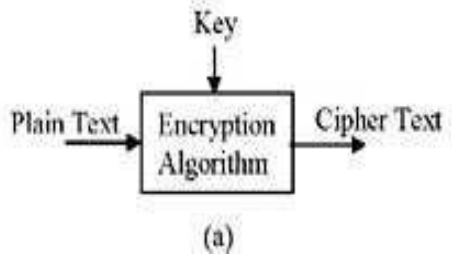
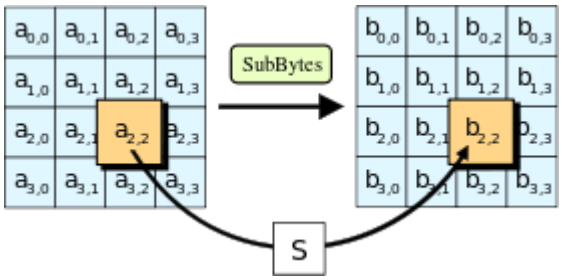
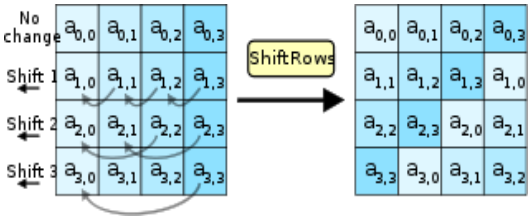


Fig. 1 AES Encryption.

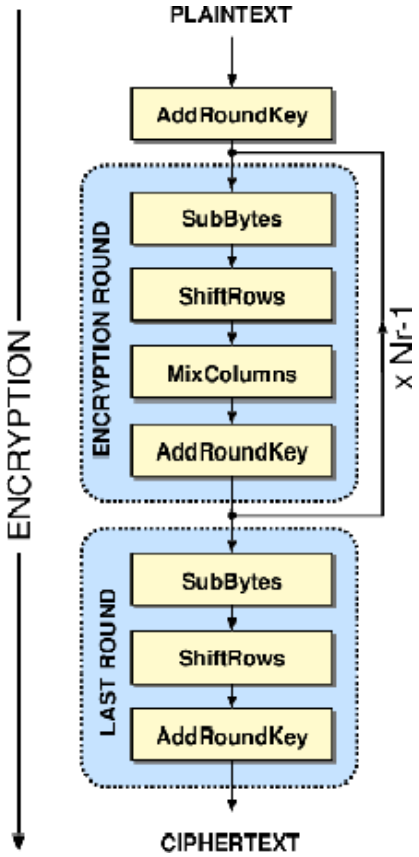
SubBytes Transformation: SubBytes transformation is a non-linear byte substitution, operating on each of the state bytes independently. The SubBytes transformation is doneusing a once- precalculated substitution table called S- box. That S-box table contains 256 numbers (from 0 to 255) and their corresponding resulting values. This approach has the significant advantage of performing the S-box computation in a single clock cycle, thus reducing the latency and avoids complexity of hardware implementation as shown in fig.



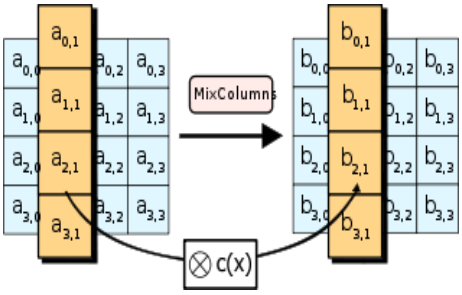
ShiftRows Transformation: *In* ShiftRows transformation, the rows of the state are cyclically left shifted over different offsets. Row 0 is not shifted; row 1is shifted one byte to the left; row 2 is shifted two bytes tothe left and row 3 is shifted three bytes to the left. Shift row transformation done as shown in fig.



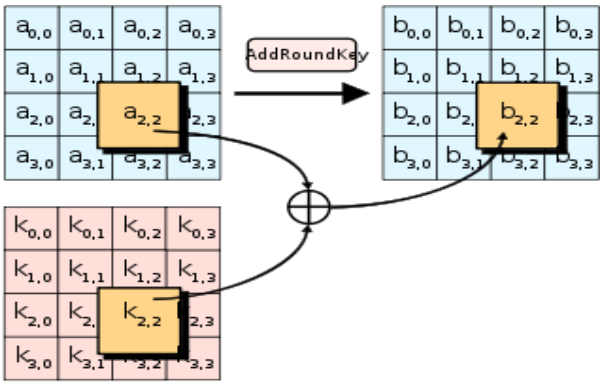
MixColumns Transformation: In MixColumns transformation, the columns of the state are considered as polynomials over GF



(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}. Mixcolumn transformation done as shown in fig.

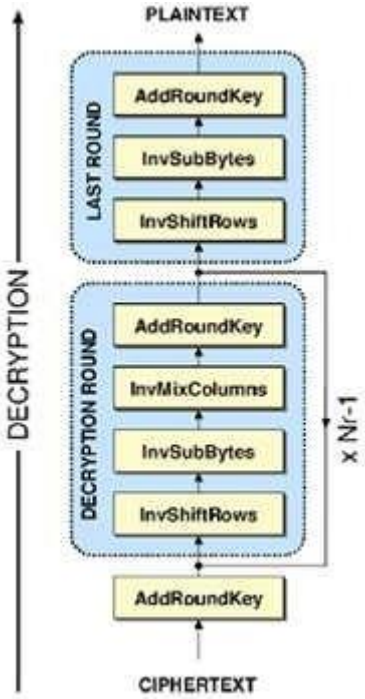


AddRoundKey Transformation: In the AddRoundKey transformation, a Round Key is added to the State - resulted from the operation of the MixColumns transformation - by a simple bitwise XOR operation. The RoundKey of each round is derived from the main key using the KeyExpansion algorithm. The encryption/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



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. Fig (b) shows decryption process in which simple conversion of cipher textto plain text is done with the help of key. The round transformation of decryption uses the functionsAddRoundKey, InvMixColumns, InvShiftRows, and InvSubBytes successively. AES decryption as shown in fig



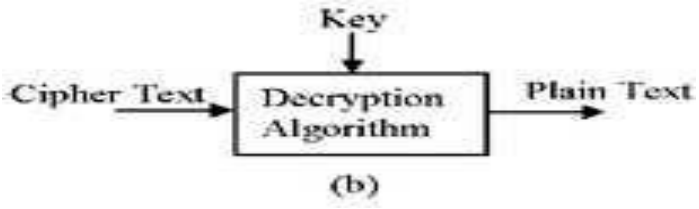
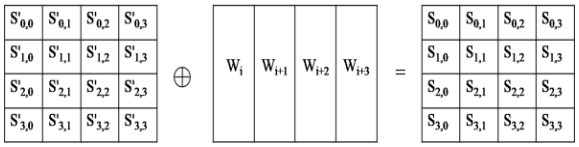
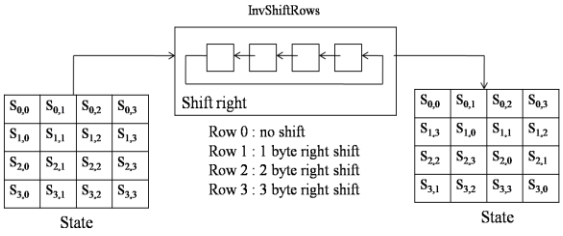


Fig. 2 AES Decryption.

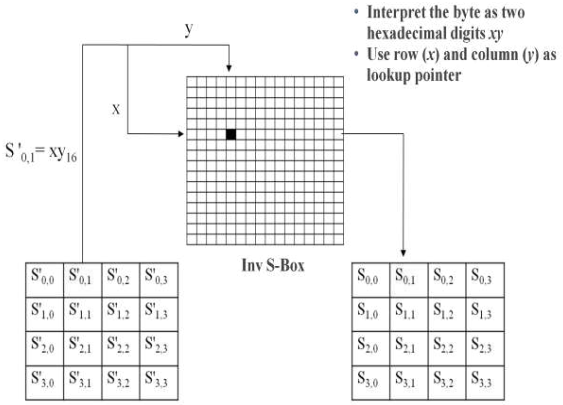
***AddRoundKey*:** AddRoundKey is its own inverse function because the XOR function is its own inverse. The round keys have to be selected in reverse order.AddRoundKey as shown in fig.



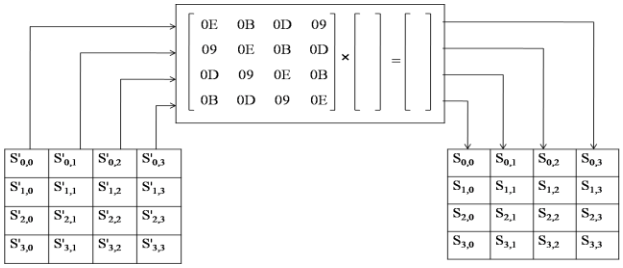
InvShiftRows Transformation: InvShiftRows exactlyfunctions the same as ShiftRows, only in the opposite direction. The first row is not shifted, while the second, third and fourth rows are shifted right by one, two and three bytes respectively.InvShiftRow transformation shown in fig.



***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.InvSub Byte transformation as shown in fig.



InvMixColumn Transformation: InvMixColumnstransformation 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.InvMix column transformation as shown in fig.



IV. CONCLUSION

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 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, 192, and 256 bits.

V. 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. A. 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