International Journal for Modern Trends in Science and Technology
Volume 10, Issue 04, pages 33-36.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue04.html
DOI: https://doi.org/10.46501/IJMTST1004004

Implementation of Advanced Encryption Standard Algorithm using Verilog

Dr A V S Swathi [1] | R Mounika[2] | S Joshibabu [2] | Rohit M[2] | S Naga Sathvika[2]

[1] Associate Professor, Raghu Engineering college (A), Visakhapatnam, India.
[2] Raghu Engineering college (A), Visakhapatnam. India.

To Cite this Article
Dr A V S Swathi, R Mounika, S Joshibabu, Rohit M and S Naga Sathvika, Implementation of Advanced Encryption Standard Algorithm using Verilog, International Journal for Modern Trends in Science and Technology, 2024, 10(04), pages. 33-36.https://doi.org/10.46501/IJMTST1004004

Article Info
Received: 18 March 2024; Accepted: 03 April 2024; Published: 04 April 2024.

ABSTRACT

An electronic data encryption standard is known as Advanced Encryption Standard (AES). This standard is used in both software and hardware, and today it is one of the most widely used encryption techniques. However, Field Programmable Gate Arrays (FPGAs) offer a quicker and more customizable solution. This project presents the AES algorithm implementation using Verilog language and hardware evaluation using FPGA. Xilinx vivado 2022.1 software is used for simulation and optimization of the synthesizable Verilog code. Synthesizing and implementation (i.e., Translate, Map and Place and Route) of the code is carried out on Xilinx Vivado 2022.1. All the transformations of Encryption are simulated using an iterative design approach in order to minimize the hardware consumption. Xilinx ofSpartan6 or 7 series is used for hardware evaluation. This project proposes a method to integrate the AES encrypted and the AES decrypted. This method can make it a very low complexity architecture, especially in saving the hardware resource in implementing the AES Sub Bytes module and Mix columns module etc. Most designed modules can be used for both AES encryption. Besides, the architecture can still deliver a high data rate in both encryption operations. The proposed architecture is suited for hardware-critical applications, such as GPON network security, ATM Machines, smart card, PDA, and mobile phone, etc.

KEYWORDS: AES, PDA, ATM machines , GPON.

1. INTRODUCTION

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 plain text into a cipher text, using most of the time a key. In a broader sense Cryptography is best known as a way of keeping the contents of a message secret. Confidentiality of network communications, for example, is of great importance for e-commerce and other network applications. However, the applications of cryptography go far beyond simple confidentiality. In particular, cryptography allows the network business and customer to verify the authenticity and integrity of their transactions. If the trend to a global electronic

marketplace continues, better cryptographic techniques will have to be developed to protect business transactions. Sensitive information sent over an open network may be scrambled into a form that cannot be understood by a hacker or eavesdropper. This is done using a mathematical formula, known as an encryption algorithm, which transforms the bits of the message into an unintelligible form. The intended recipient has a decryption algorithm for extracting the original message.

2. LITERATURE SURVEY:

DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours. There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been Superseded by the Advanced Encryption Standard (AES).

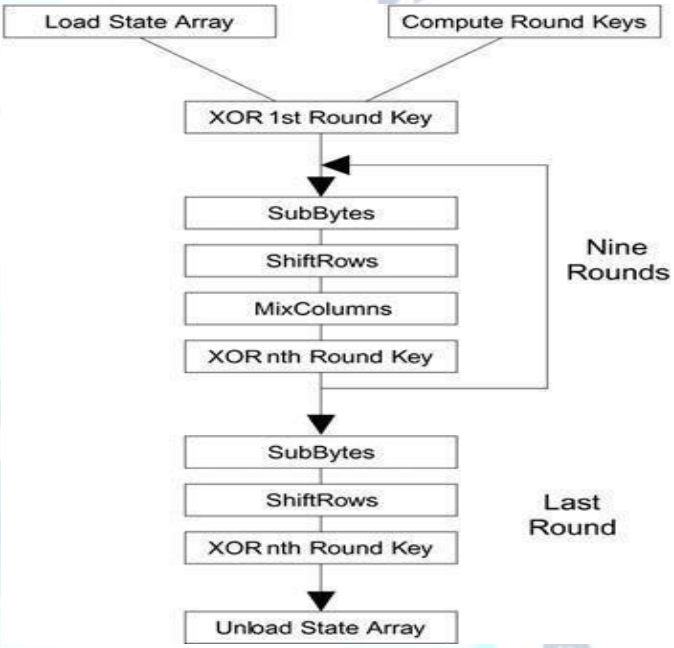
The Advanced Encryption Standard (AES) Algorithm, adopted by the U.S. government in 2001, is a block cipher transforms 128-bit data blocks under a 128-bit, 192-bit or 256-bit secret key, by means of permutation and substitution. In January 1997, the National Institute of Standards and Technology (NIST) announced the initiation of an effort to develop the AES and made a formal call for algorithms on September 12, 1997. After reviewed the results of this Preliminary research, the algorithms MARS, RC6TM, Rijndael, Serpent and Two fish were selected as finalist. And further reviewed public analysis of the finalist, NIST has decided to propose Rijndael as the new Advanced Encryption Standard (AES) on 2nd October 2000. It is expected to replace the DES and Triple DES so as to fulfil the stricter data security requirement because its enhanced security levels.

The following are the Standard AES Algorithm Specifications

For the AES algorithm, the length of the input block, the output block and the State is 128 bits. This is represented by Nb = 4, which reflects the number of 32-bit words (number of columns) in the State. For the AES algorithm, the length of the Cipher Key, K, is 128, 192, or 256 bits. The key length is represented by Nk = 4, 6, or 8, which reflects the number of 32-bit words (number of columns) in the Cipher Key. For the AES algorithm, the number of rounds to be performed during the execution of the algorithm is dependent on the key size. The number of rounds is represented by Nr, where Nr =10 when Nk = 4, Nr = 12 when Nk = 6, and Nr = 14 when Nk = 8.

Existing Method:

The Advanced Encryption Standard (AES) Algorithm, adopted by the U.S. government in 2001, is a block cipher transforms 128-bit data blocks under a 128-bit, 192- bit or 256-bit secret key, by means of permutation and substitution.



3. PROPOSED DESIGN:

The following steps such as Rot Word of Last Column, Sub Byte of Rot Word, Xor with Rcon and First Column of Key and Sub byte and Result Become First Column of Round Key One are performed using Verilog Code in Xilinx Vivado software and the resultant is show below in the Figure. The first in the AES Encryption process of Key Generation is completed.

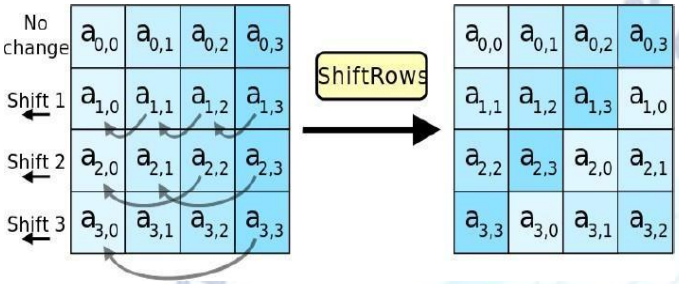
Sub Bytes operation is a non-linear byte substitution, operating on each byte of the state independently. The substitution table (S-Box) is invertible and is constructed by the composition of two transformations:

Take the multiplicative inverse in Rijndael's finite field

Apply an affine transformation as described below

i = b i +b (i+4) mod8 +b (i+5) mod8 +b (i+6) mod8 +b (i+7) mod8 +c i

In this operation, each row of the state is cyclically shifted to the left, depending on the row index. The 1st row is shifted 0 positions to the left. The 2nd row is shifted 1 position to the left. The 3rd row is shifted 2 positions to the left. The 4th row is shifted 3 positions to the left which is shown below in the Figure



The Mix Columns transformation operates on the State column-by-column, treating each column as a four-term polynomial. In these the multiplication is carried by Dot product and addition is carried by Xor Operation.

Simulation Results:

AES Encryption output for plain texts of bits 128,192,256 is converted into cipher text are shown on the below Figure 3.5. In this project we have given Input Plain text of 128 bits and keys of three different bit sizes such as 128bits, 192bits and 256bits for encryption and by using Verilog in Xilinx Vivado software we have obtained the AES Encryption output which is cipher text. The below figure represents the Encryption Output.

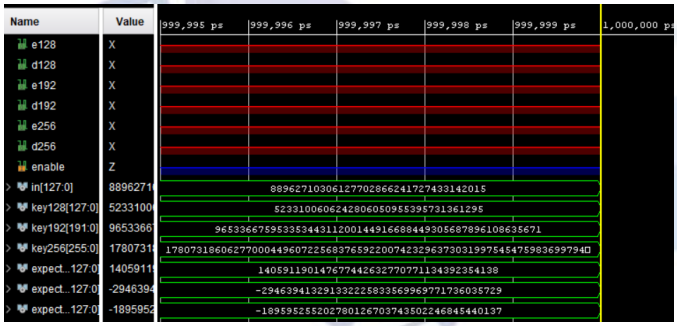


Fig: AES Encryption output

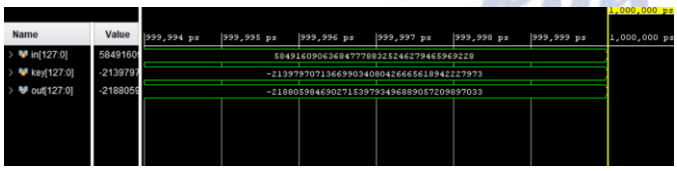


Fig: Add Round Key operation in Verilog

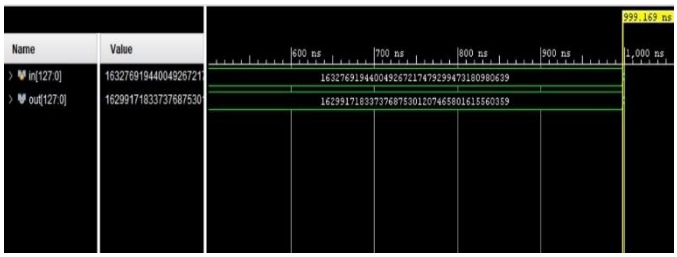


Fig: Inverse Shift rows operation in verilog

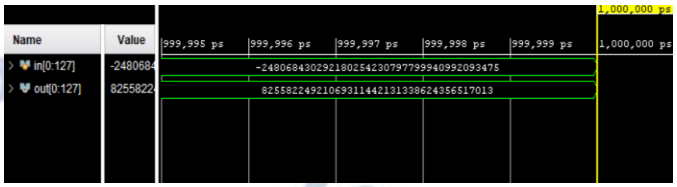


Fig: Inverse Mix column operation in Verilog

The above figures represents that the following steps in AES Decryption such as Inverse Mix Column. In the Inverse Mix column operation, we use pre-defined matrix which is not used in AES Encryption.

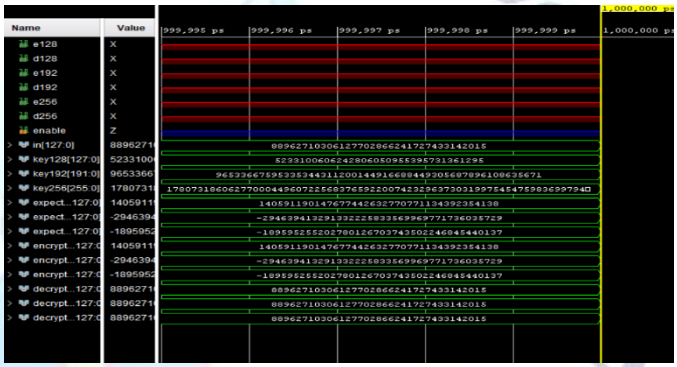


Fig: AES Decryption output

CONCLUSION:

In this project , we have successfully accomplished encryption and decryption of given input of different key bits such as 128 bits ,196 bits and 256bits by using the Advanced Encryption Standard(AES) Algorithm using the Verilog in the XILINX VIVADO Design suit. The AES is the cryptography algorithm which performed the encryption and decryption of taking the input information is known as the plain text and the final output information is the Ciphertext which is the encrypted by the AES Algorithm which is not readable form which is performed at sender or transmitter side. The cipher text is converted into plain text at receiver side if receiver uses the same key which is known as symmetric key. By using the specific operations in the algorithm like mix columns, add round keys, shifting rows, and using the s- box of different operations

performed the Advanced Encryption Standard algorithm using Verilog in XILINX VIVADO Design Suit In the Advanced Encryption Algorithm, we can implement and design the algorithm using the different rounds having the reduced steps in the algorithm, so it will reduce the power consumption and the area of the chip.There are several potential scopes for AES using Verilog. Verilog can be used to design dedicated hardware circuits for performing the encryption and decryption operations, resulting in faster and more efficient execution. Verilog can be used to design AES circuits that can be integrated with FPGA platforms for encryption and decryption of data. Verilog can be used to design hardware circuits for implementing post-quantum cryptography algorithms, including those based on AES.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] High-Speed VLSI Architectures for the AES Algorithm (IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 12, NO. 9, SEPTEMBER 2004)

[2] An Efficient Cryptography VLSI Design for Data Security (Proceedings of the International Conference on Applied Artificial Intelligence and Computing (ICAAIC 2022))

[3] Designing of AES Algorithm using Verilog (2018 4th International Conference for Convergence in Technology (I2CT))

[4] A High-Performance VLSI Architecture for Advanced Encryption Standard (AES) Algorithm (Proceedings of the 19th International Conference on VLSI Design (VLSID'06))

[5] An FPGA-Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists (IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 9)

[6] Abdullah, A. M., & Aziz, R. H. H. (2016, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17).

[7] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).

[8] Gaj, K., & Chodowiec, P. (2001, April). Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using Field Programmable Gate Arrays. In Cryptographers' Track at the RSA Conference (pp. 84-99). Springer Berlin Heidelberg.

[9] Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education India

[10] Yenuguvanilanka, J., & Elkeelany, O. (2008, April). Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm. In Southeastcon, 2008. IEEE (pp. 222225.

[11] Mohamed, A. A., & Madian, A. H. (2010, December). A Modified Rijndael Algorithm and it's Implementation using FPGA. In Electronics, Circuits, and Systems (ICECS), 2010 17th IEEE International Conference on (pp. 335-338)

[12] Deshpande, H. S., Karande, K. J., & Mulani, A. O. (2014, April). Efficient implementation of AES algorithm on FPGA. In Communications and Signal Processing (ICCSP), 2014 IEEE International Conference on (pp. 1895-1899)