iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VII **Month of publication:** July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36731

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

A Design Implementation and Comparative Analysis of Advanced Encryption Standard (AES) Algorithm Using Verilog HDL

Charrith Srinivaas[1], Manoj L[2], Adarsh MS[3], Kiran AP[4], Ramya K[5]
[1, 2, 3, 4]*Student, ECE, BGSIT, BG Nagara, India*
[5]*Asst. Professor, ECE, BGSIT, BG Nagara, India*

Abstract: ***As the technology is getting more and more advanced day by day in a rapid pace the problem for the security of data is also increasing at a very staggering rate. The hackers are equipped with new advanced tools and techniques to break any security system. Hence people are getting even more concerned about their data and data's security. The data security can be achieved by either software or hardware implementations or both put together working in harmony. In this work Field Programmable Gate Arrays (FPGA) device is used for hardware implementation since these devices are less complex, more flexible and provide and have far greater more efficiency. This work mainly focuses on the hardware execution of one of the security algorithms that is the Advanced Encryption Standard (AES) algorithm which is the most highly used algorithm for Encryption. The AES algorithm is executed on Vivado 2014.2 ISE Design Suite and therefore the results are observed on 28 nanometers (nm) Artix-7 FPGA. This work Mainly discusses the design implementation of the AES algorithm and the resources which are consumed in implementing the AES design on Artix-7 FPGA. The resources which are consumed are as follows- Slice Register (SR), Look-Up Tables (LUTs), Input/Output (I/O) and Global Buffer.***

I. INTRODUCTION

The process of securing data from any means of unapproved access and data corruption through its entire life is said to be data security . With the continuous improvement in the field of technology, the data is getting pretty unsecured. Every now and then hackers are trying to hack one's data. Therefore the security of data is the most concerned thing in people's minds. The security of data can be achieved by either software means or hardware means. Nowadays hardware approach is to protect the data is getting more attention. This is because by means of hardware protecting the data is more reliable, flexible and less complex. The hardware approach also gives minimal delay and provides more efficiency to data security. To protect the data from any unrecognized access there are two types of security algorithms. The first one is the Symmetric security algorithms which cover Data Encryption Standard (DES) and Advanced Encryption Standard (AES). The second one is the Asymmetric security algorithms which cover Rivest-Shamir-Adleman (RSA) & Elliptic Curve Cryptosystem (ECC) . FPGA devices are practiced for a hardware approach to secure one's data.

II. METHODOLOGY

A. *Block Diagram*

1) *Advanced Encryption Standard (AES) Algorithm:* To overcome the attacks over the Data Encryption Standard (DES) algorithm, the AES algorithm is designed by the National Institute of Standard Technology (NIST) in the year 2000. AES algorithm is a stronger and faster version of the DES algorithm. It is a symmetric key block with cipher which means both the encryption and decryption key of the algorithm are the same. The reason to switch from DES to AES is its key size of 56-bits which is cannot be defended in today's fast computing era. Hence a 128-bits, 192-bits and, 256-bits data key has been introduced in the AES algorithm. The key size depends on the number of rounds in the AES, for 10 rounds we have 128- bits, for 12 rounds 192-bits and for 14 rounds we have 256-bit size. Each round has its own encryption process which includes cipher key performing addition of round key, sub bytes manipulation, shifting and mixing of rows and columns to the plain text. The encryption process of the AES algorithm is described infigure1.

2) *Encryption Process Covers The Following Steps Which Are Described As Below*

a) *Sub bytes Step*- In this step, we have the predefined sboxes and each byte is replaced by sub-byte using an 8- bit substitution box or S-Box .

b) *Shift Row*- Rows are left shifted by a predefined offset.

c) *Mixed Columns*- Columns are mixed by some mathematical functions .

d) *Add Round Key Step*- The input of the round bit- wise XOR with the round key.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

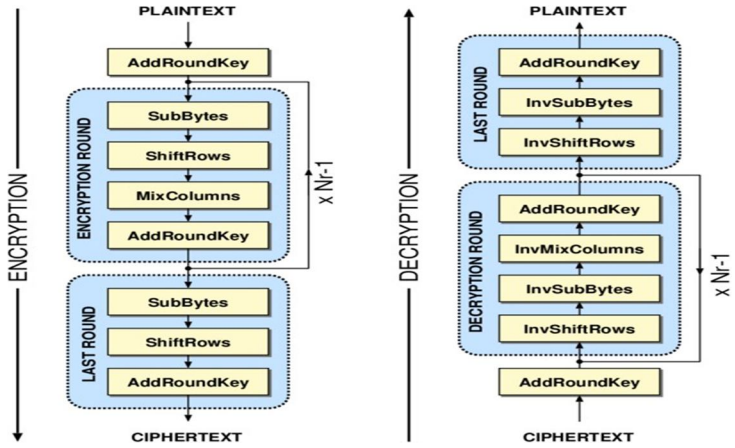


Figure 1 - Block diagram of encryption process of the AES algorithm

III. WORKING

A. S- BOX (Substitute Box)

1) Substitute box(S-BOX) serves as a look up table. Values are substituted being based on the input which acts as the address to ROM.

2) Each byte of the state is to be substituted with a 8-bit value from the S-box. The S-box will contain a permutation of all the possible 256 8-bit values.

It is a nonlinear operation and the only non-linear transformation in this encryption process.

B. Shift Rows

1) Rows are shifted as per a pattern as mentioned by the standard.

2) The Shift Rows function are operated on the rows of the state and its role is to cyclically shift the bytes in each row by a certain offset. For AES, the first row is to be left very much unchanged. Each byte of the second row is shifted one row to the left. Likewise, the third and fourth rows are shifted through offsets of two and three respectively.

C. Mix Column

1) Each column of four bytes is now transformed using a special mathematical function.

2) This function takes as a input the four bytes of one column and outputs four completely new bytes, which will replace the original column.

D. Add Round Key

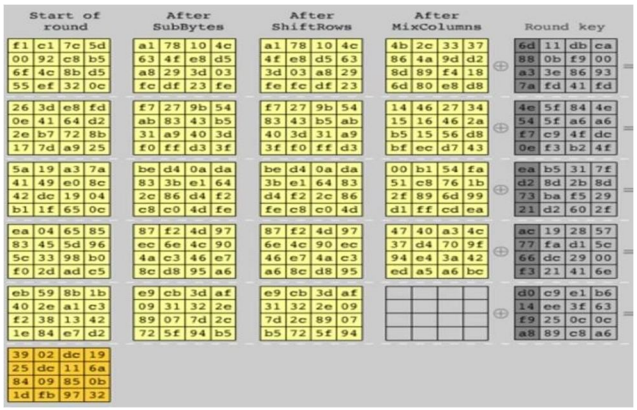
1) The transformation for the present in the cipher and inverse cipher in which it is a round key is added to the state using an XOR operation.

2) Round keys are the values derived from the cipher key using the Key Expansion routine.

IV. OUTCOME

The execution of the AES algorithm is done on Vivado 2014.2 ISE Design Suite and the results of the AES algorithm is targeted on 28 nanometers (nm) Artix-7 FPGA device . For the implementation of the AESalgorithm, the numbers of Slice Register (SR) which required are 3987, the number of Look Up Tables (LUTs) required are 4115, the number of Input/Output (I/O) ports required are 269 and the number of Global Buffer (BUFG) required is 1 . Table 1, represents the resource utilization for the AES algorithm on Artix-7 FPGA and the Register Transfer Logic (RTL) of the AES algorithm which is obtained by the synthesis process is shown in figure 3. RTL at the input side plain text of 128-bit is taken which is encrypted with a 128-bit key. Also at the input side, there is one clock signal, one start signal, one reset signal, sbox, one mix column block (mixco_done) and one key generator (keygen_done) block. After performing all the encryption process steps cipher text of 128-bit is observed at the output side . The post-synthesis simulation of the AES algorithm is represented in figure

We have enhanced the project by reducing the delay.



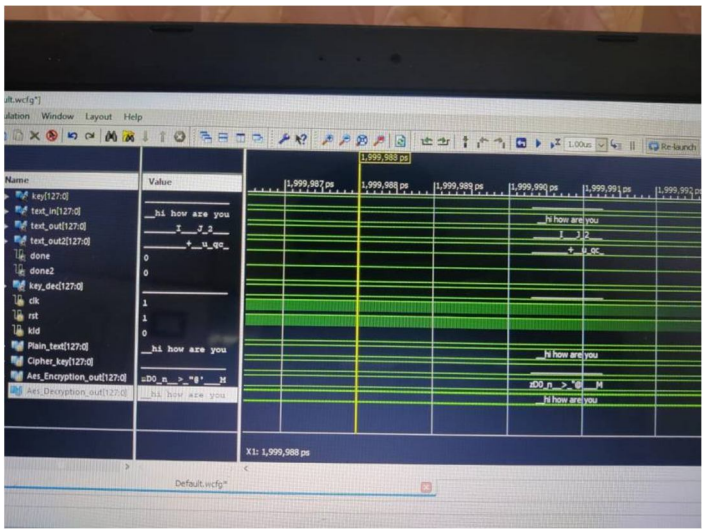


Figure 2 - Final output after all the operations

V. CONCLUSION

A. This Project explained the implementation ofAdvanced Encryption Standard in Xilinx ISE targeting a particular family of FPGA, The project describes the method of optimizing the timing critical paths of the AES to operate at much higher speeds, to be used as part of LTE Security. The implementation results of the proposed algorithm should performs better than the base algorithm with the total critical path getting further optimized therefore increasing the speed of operation. It is clearly observed from the synthesis results that in the fully pipelined AES encryption architecture the throughput is many folds greater than the conventional AES architecture and the single stage pipelining architecture.

B. The techniques which are being used at the Internal and outer Pipelining of the modules and Distributed LUT based concept, the main objective of the above techniques is to reduce the critical path delay and increase the overall speed of operation of design, the disadvantage is the increases in area and output latency. Area is not of a much problem as modern days FPGA's has huge amount of resources.

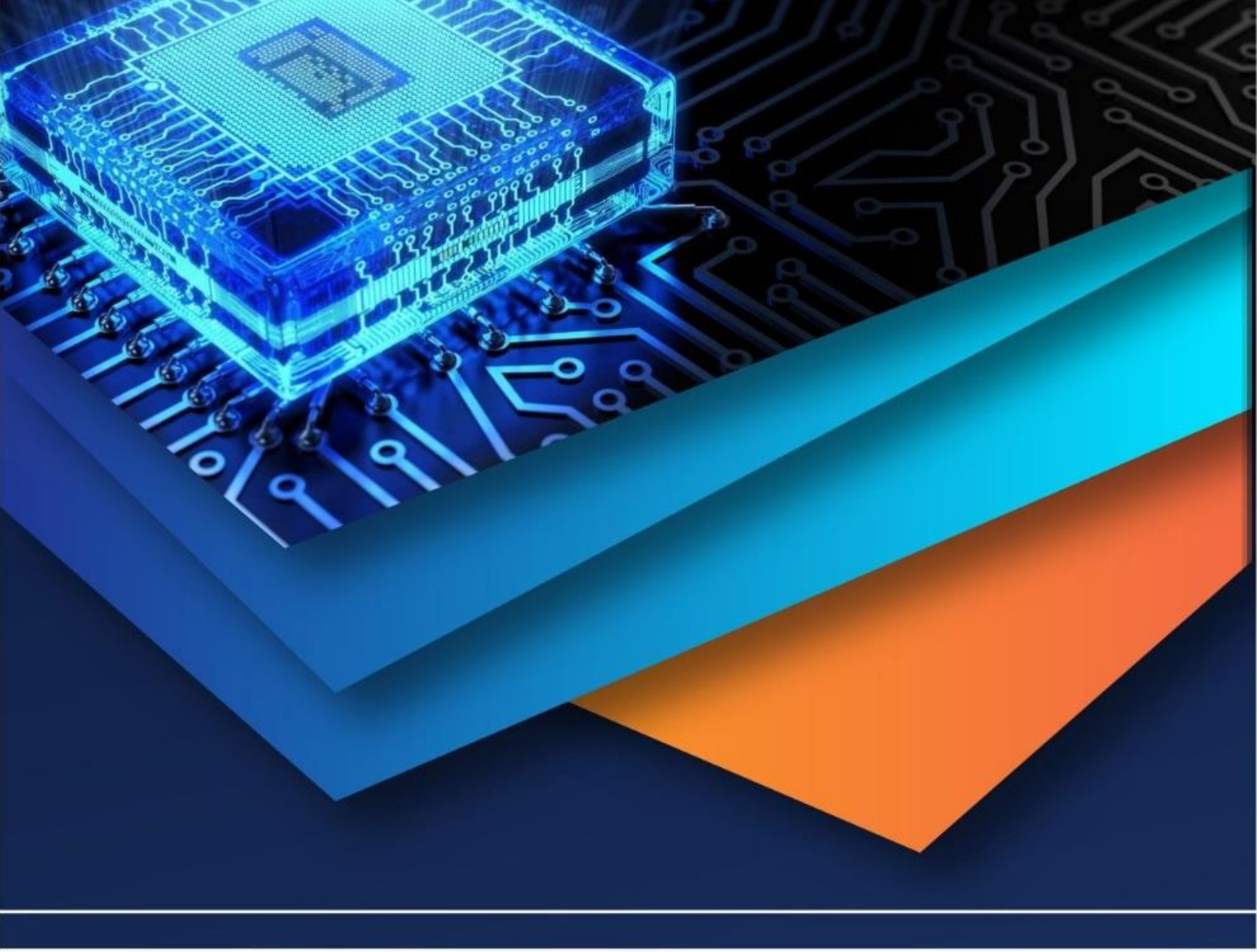
C. As part of Future scope low power design ofCurrent work can be taken forwards, as balancing speed, power and area is a challenging task. This could be integrated into an IP core using vivado and a soft core or hard core processor can be added to further test its efficiency for reconfiguring IP on run time using soft registers.

VI. FUTURE SCOPE

It is observed from the literature survey that by now every execution of the AES algorithm is done on the 5th series and 6th series of Virtex and Spartan family FPGAs. No work is done on FPGAs of the 7th series Artix, Kintex, Zynq.

REFERENCES

[1] W. Stalling, Cryptography and Network Security Principles and Practice, 5th ed. Prentice Hall,2011.
[2] S. Vaudenay, A Classsical Introduction to Cryptography: Application for Communication Security. Springer Science and Business Media,2006.
[3] T. Eisenbarth, S. Kumar, C. Paar, APoschmann, and L. Uhsadel, "A survey of lightweight-ceyptography implementation", IEEE Design and Test of Computers, vol. 24, no. 6, 2007, pp. 522-533.
[4] G. Leander, C. Paar, A. Poschmann, and K. Schramm, "New Lightweight DES Varients",in Fast Software Encryption (FSE 2007),A.Biryukov,Ed. Springer Berln Heidelberg: LNCS 4593,2007,pp.196-210.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY