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

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

Charrith Srinivaas¹, Manoj L², Adarsh MS³, Kiran AP⁴, Ramya K⁵

^{1, 2, 3, 4}Student, ECE, BGSIT, BG Nagara, India

⁵Asst. 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 in figure 1.
- 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.

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 an 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 AES algorithm, 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.

Start of round	After SubBytes	After ShiftRows	After MixColumns	Round key
f1 e1 7c 5d	a1 78 10 4c	a1 78 10 4c	4b 2c 33 37	6d 11 db ea
00 92 c8 b5	63 4f e8 d5	4f e8 d5 63	86 4a 9d d2	88 0b f9 00
6f 4c 8b d5	a8 29 3d 03	3d 03 a8 29	8d 89 f4 18	a3 3e 86 93
55 ef 32 0c	fc df 23 fe	fe fc df 23	6d 80 e8 d8	7a fd 41 fd
26 3d e8 fd	f7 27 9b 54	f7 27 9b 54	14 46 27 34	4e 5f 84 4e
0e 41 64 d2	ab 83 43 b5	83 43 b5 ab	15 16 46 2a	54 5f a6 a6
2e b7 72 8b	31 a9 40 3d	40 3d 31 a9	b5 15 56 d8	f7 c9 4f dc
17 7d a9 25	f0 ff d3 3f	3f f0 ff d3	bf ee d7 43	0e f3 b2 4f
5a 19 a3 7a	be d4 0a da	be d4 0a da	00 b1 54 fa	ea b5 31 7f
41 49 e0 8c	83 3b e1 64	3b e1 64 83	51 c8 76 1b	d2 8d 2b 8d
42 dc 19 04	2c 86 d4 f2	d4 f2 2c 86	2f 89 6d 99	73 ba f5 29
1f 1f 65 0c	c8 e0 4d fe	fe c8 e0 4d	d1 ff cd ea	21 d2 60 2f
ea 04 65 85	87 f2 4d 97	87 f2 4d 97	47 40 a3 4c	ac 19 28 57
83 45 5d 96	ec 6a 4c 90	6e 4c 90 ec	37 d4 70 9f	77 fa d1 5c
5c 33 9b b0	4a c3 46 e7	46 e7 4a c3	94 e4 3a 42	66 dc 29 00
f0 2d ad c5	8c d8 95 a6	a6 8c d8 95	ed a5 a6 bc	f3 21 41 6e
eb 59 8b 1b	e9 cb 3d af	e9 cb 3d af		d0 c9 e1 b6
40 2e a1 c3	09 31 32 2e	31 32 2e 09		14 ee 3f 63
f2 38 13 42	89 07 7d 2c	7d 2c 89 07		f9 25 0c 0c
1e 84 e7 d2	72 5f 94 b5	b5 72 5f 94		a8 89 c8 a6
39 02 dc 19				
25 dc 11 6a				
84 09 85 0b				
1d fb 97 32

Figure 2 - Final output after all the operations

V. CONCLUSION

- This Project explained the implementation of Advanced 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.
- 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.
- As part of Future scope low power design of Current 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. Stallings, Cryptography and Network Security Principles and Practice, 5th ed. Prentice Hall, 2011.
- [2] S. Vaudenay, A Classical Introduction to Cryptography: Application for Communication Security. Springer Science and Business Media, 2006.
- [3] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography 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 Variants", in Fast Software Encryption (FSE 2007), A. Biryukov, Ed. Springer Berlin 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

Call : 08813907089 (24*7 Support on Whatsapp)