2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. June 4-5, 2020

A Design Implementation and Comparative Analysis of Advanced Encryption Standard (AES) Algorithm on FPGA

Keshav Kumar
Chitkara University Institute of Engineering and Technology, Chitkara University
Punjab, India
keshav.kumar@chitkara.edu.in

K.R. Ramkumar
Chitkara University Institute of Engineering and Technology, Chitkara University
Punjab, India
k.ramkumar@chitkara.edu.in

Amanpreet Kaur
Chitkara University Institute of Engineering and Technology, Chitkara University
Punjab, India
amanpreet.kaur@chitkara.edu.in

***Abstract*—As the technology is getting advanced continuously the problem for the security of data is also increasing. The hackers are equipped with new advanced tools and techniques to break any security system. Therefore people are getting more concern about data security. The data security is achieved by either software or hardware implementations. In this work Field Programmable Gate Arrays (FPGA) device is used for hardware implementation since these devices are less complex, more flexible and provide more efficiency. This work focuses on the hardware execution of one of the security algorithms that is the Advanced Encryption Standard (AES) algorithm. The AES algorithm is executed on Vivado 2014.2 ISE Design Suite and the results are observed on 28 nanometers (nm) Artix-7 FPGA. This work discusses the design implementation of the AES algorithm and the resources 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 (BUFG).**

Keywords- Field Programmable Gate Arrays (FPGA), Advanced Encryption Standard (AES) algorithm, Artix-7 FPGA, Slice Register (SR), Look Up Tables (LUTs), Input/Output (I/O) and Global Buffer (BUFG).

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 [1]. With the continuous improvement in the field of technology, the data getting 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 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 Symmetric security algorithms which cover Data Encryption Standard (DES) and Advanced Encryption Standard (AES). The second one is Asymmetric security algorithms which cover Rivest- Shamir-Adleman (RSA) & Elliptic Curve Cryptosystem (ECC) [2]. FPGA devices are practiced for a hardware approach to secure one's data. This is because FPGA devices are more frequent give flexibility and it has good speed and throughput as compared to software approach. FPGA devices have so much variation so that it is very difficult for hackers to breach security.

II. FPGA

FPGA stands for Field Programmable Gate Arrays, these are those semiconductor-based devices that are made up of configurable logic blocks (CLBs) interconnected with programmable interconnects. FPGA devices have chosen over other devices like ASIIC because they can be reprogrammed after the manufacturing process. Therefore FPGA devices are more flexible, less complex and provide high speed, throughput, and frequency to the user [3-4]. The building blocks through which FPGA can be made up is presented in figure 1.

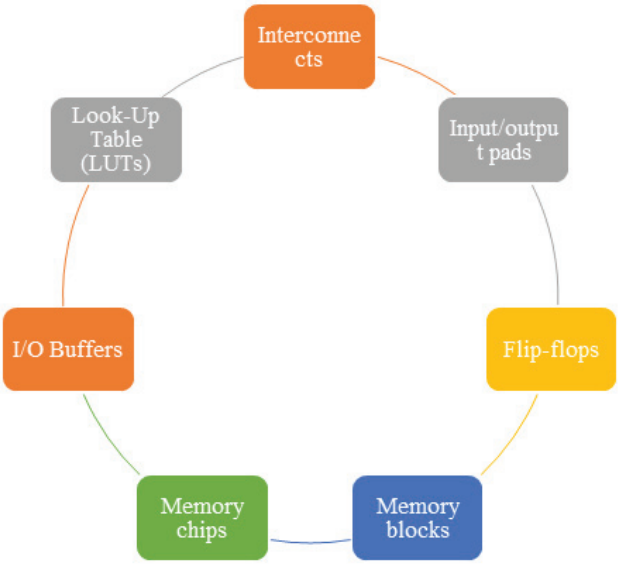

Fig. 1. Building Blocks of FPGA

Applications of FPGA includes Autonomous vehicles, Internet of Things, Data Security, Cloud Computing, Robotics, Machine vision and learning, Home Automation, video surveillance, Facial Recognition, Smart Medical diagnosis, Renewable energy, Telecom, Military, aerospace, ASIC Prototyping, Voice recognition, filtering, communication encoding, Wireless communication and many more. There is tremendous market growth of FPGA with Xilinx, Intel, Microsemi, Atmel, and Texas Instruments as key players. In order to survive in market different FPGA

978-1-7281-7016-9/20/$31.00 ©2020 IEEE

vendors promises specialized application-specific FPGA in the market. The Compound Annual Growth Rate (CAGR) is 8.64% for FPGA with the Asia Pacific is both largest and fastest-growing market in year 2018-2024. The market analysis of FPGA is shown in figure 2.

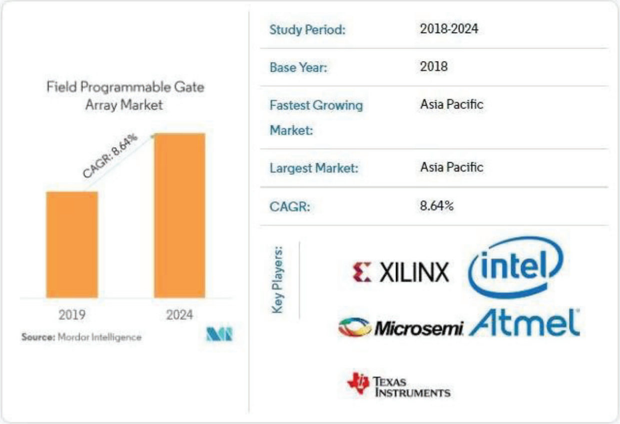

Fig. 2. Market analysis of FPGA [13].

III. 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 [5]. AES algorithm is a stronger and faster version of DES. It is a symmetric key block cipher which means both the encryption and decryption key of the algorithm are the same. The reason to move from DES to AES is its key size of 56-bits which is undefended in today's fast computing era. Hence a 128-bits, 192-bits and, 256-bits data key is introduced in the AES algorithm. The key size depends on the number of rounds of AES, for 10 rounds we have 128-bits, for 12 rounds 192-bits and for 14 rounds we have 256-bit size [6]. 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 [7]. The encryption process of the AES algorithm is described in figure 3.

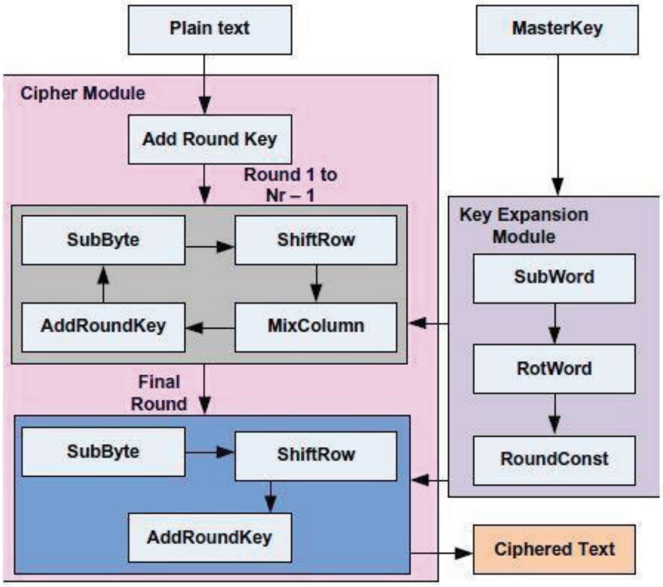

Fig. 3. AES Encryption Process [9].

Encryption Process covers the following steps which are described as below-

- Sub bytes Step- In this step, we have predefined s-boxes and each bye is replaced by sub-byte using an 8-bit substitution box or S-Box [5-10].
- Shift Row- Rows are left shifted by a predefined offset [5-10].
- Mixed Columns- Columns are mixed by some mathematical functions [5-10].
- Add Round key step- the input of the round bit- wise XOR with the round key.[5-10]

IV. IMPLEMENTATION OF AES ALGORITHM ON FPGA

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 [10-12]. For the implementation of the AES algorithm, the number of Slice Register (SR) 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 [14]. 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

TABLE I. .RESOURCE UTILIZATION FOR THE AES ALGORITHM.

Resources	Used	Available
SR	3987	126800
LUT	4115	63400
I/O	269	300
BUFG	1	32

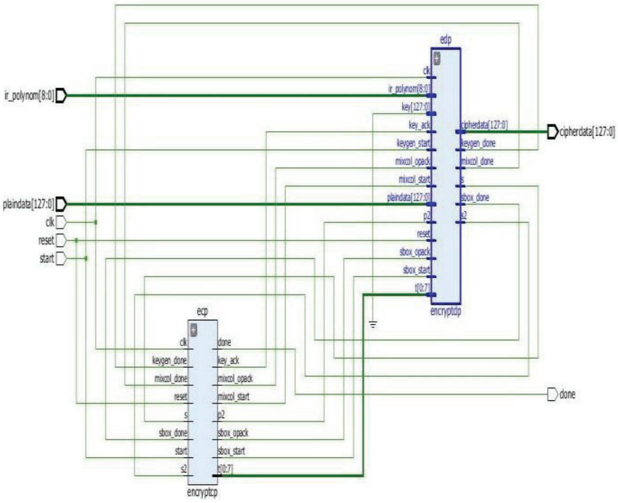

Fig. 4. RTL schematic of the AES algorithm.

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 5. In the post-synthesis process 128- bit,

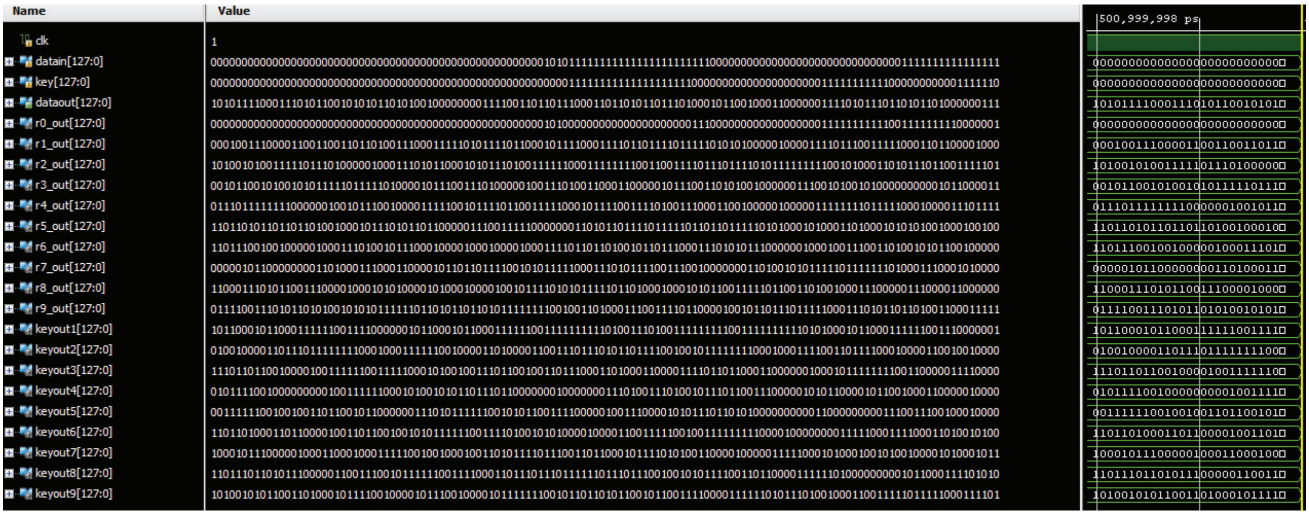

Fig. 5. Post synthesis result of the AES algorithm.

plain text is taken in hexadecimal format and key of 128-bit is taken in binary format. For this implementation, the 128-bit key is fixed for all 10 rounds of the AES encryption process. After applying 1 to clock, start and, reset signal the 128-bit cipher text is observed.

V. COMPARATIVE ANALYSIS

In this work, we have compared our design implementation of the AES algorithm from previous implemented designs of the AES algorithm on FPGA. The parameters which are taken into account for comparison are LUTs, BUFGs, SR and, I/O.

A. *Comparison of Slice Register (SR)*

Figure 6 compares the consumption of slice register with our design and with the previously implemented design. In paper [2] the number of slice register used is 954. In paper [9] researchers used two FPGA for implementing the AES design, for Virtex-5 FPGA the number of slice register used is 255 and for Spartan-6 FPGA the number of slice register used is 256. In paper [10-12] the number of slice register used is 1656, 2299 and, 2056 respectively.

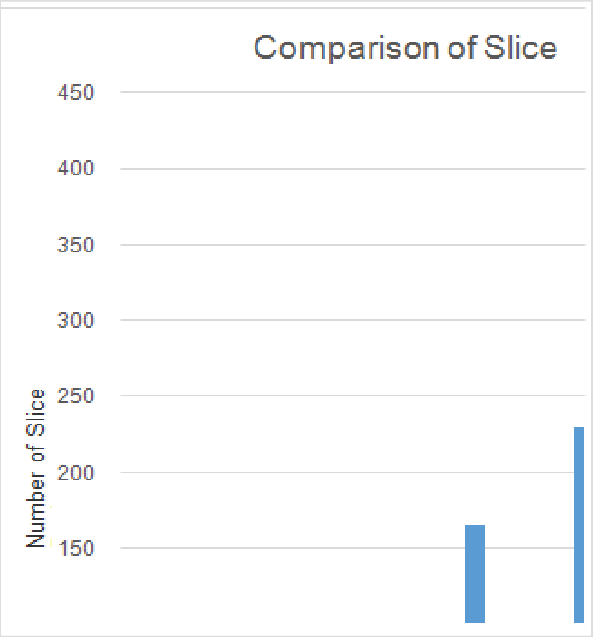

Fig. 6. Comparison of Slice Register.

In this design implementation of the AES algorithm, the requirement of the SR is most compared to the other previous work. This is because, previously implemented designs have diluted some of the mathematical computational processes of the AES algorithm, but present design implements the traditional AES algorithm which is developed by NIST.

B. *Comparison of Look-Up Tables (LUTs)*

The comparison of Look-Up Tables (LUTs) with our design and previously implemented design is shown in figure 7.

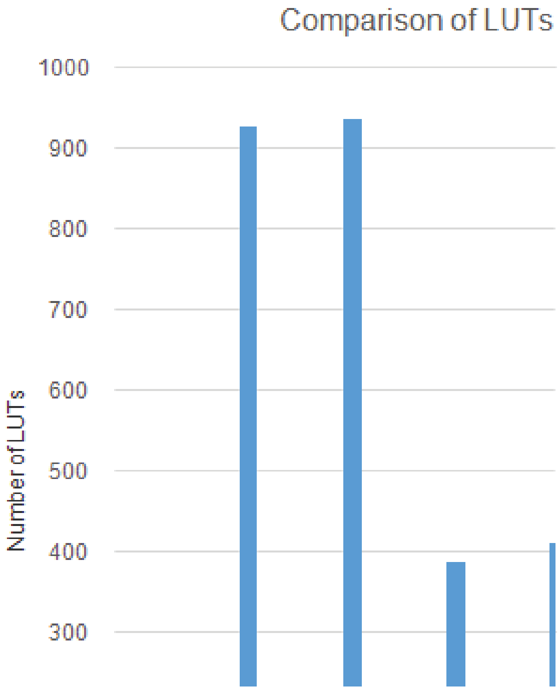

Fig. 7. Comparison of LUTs.

The present work requires 4115 LUTs for the implementation of the AES algorithm. In paper [2] the requirement of LUTs is the minimum which is 632, while in paper [9] the requirement of LUTs is the maximum which is 9276 for Virtex-5 FPGA and 9376 for Spartan-6 FPGA. In paper [12] the requirement of LUTs is 3877. In paper [9] the requirement of LUTs is maximum because in this work researchers are applying five more extra techniques for the AES algorithm implementation on FPGA.

C. *Comparison of Input/Output (I/O) and Global Buffer (BUFG)*

Figure 8 represents the comparison of the number of I/O and BUGFs used in this work and in previously implemented design.

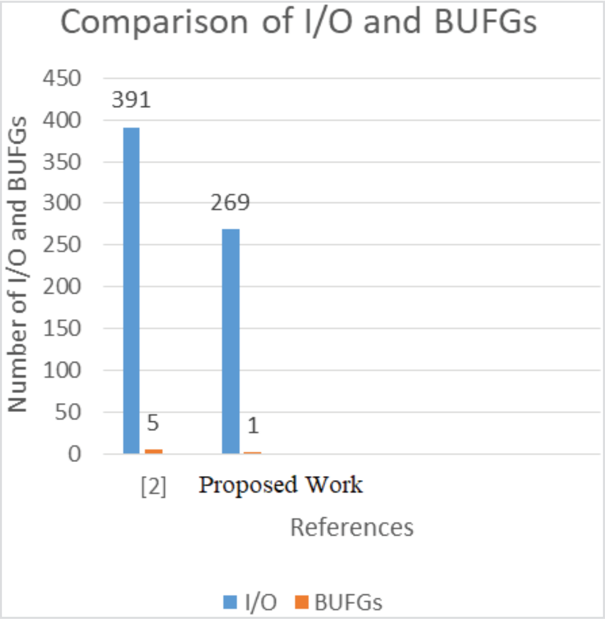

Fig. 8. Comparison of I/O and BUFGs.

In this work, the consumption of I/O ports is 269 while in paper [2] 391 I/O ports are consumed for the implementation of the AES algorithm. The consumption of BUFGs is 5 in paper [2], while in the present design the consumption of BUFGs is 1. In paper [2] the key expansion and mix column techniques are modified as compared to the original AES algorithm. Therefore the requirement of I/O and BUFGs gets increased. This work requires less number of I/O ports and BUFGs because of the implementation of the traditional AES algorithm.

VI. CONCLUSION

The design implementation of the AES algorithm is implemented on Vivado 2014.2 Design Suite and the results are observed on 28-nm Artix-7 FPGA. This work discusses the utilization of different resources namely SR, LUTs, I/O and, BUFGs consumed in implementing the AES algorithm on FPGA. The number of SR, LUTs, I/O and BUFGs required in implementation are 3987, 4115, 269 and, 1 respectively. The consumption of SR and LUTs is more in this design as compared to the previously implemented design because in previous implementations authors have modified and diluted the traditional AES algorithm. The diluted version of the AES algorithm requires a lesser number of SR and LUTs as compared to the traditional AES algorithm which is designed by NIST in the year 2000. The requirement of I/O ports and BUFGs is less in this work because no extra mathematical computational process is added in the traditional AES algorithm for key expansion and mix column process as compared to the previous design in paper [2].

VII. 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, and Ultra-Scale FPGA. Therefore researchers can implement the traditional and modified AES algorithm on these FPGAs. Also researchers can design power efficient AES algorithm by applying various power efficient techniques on the AES algorithm.

REFERENCES

[1] https://www.microfocus.com/en-us/what-is/data-security

[2] K. P. Singh, and S. Dod. "An Efficient Hardware Design and Implementation of Advanced Encryption Standard (AES) Algorithm." IACR Cryptology ePrint Archive 2016 (2016): 789.

[3] https://www.xilinx.com/products/silicon-devices/fpga/what-is-an-fpga.html

[4] https://www.techopedia.com/definition/2365/field-programmable-gate-array-fpga

[5] NIST, Advanced Encryption Standard (AES), FIPS PUBS 197, National Institute of Standards and Technology, November 2001.

[6] M. Bedoui, H. Mestiri, B. Bouallegue, and M. Machhout. "A reliable fault detection scheme for the AES hardware implementation." In 2016 International Symposium on Signal, Image, Video, and Communications (ISIVC), pp. 47-52. IEEE, 2016.

[7] H. Mestiri, F. Kahri, B. Bouallegue, and M. Machhout. "A high-speed AES design resistant to fault injection attacks." Microprocessors and Microsystems 41 (2016): 47-55.

[8] P. Katkade, and G. M. Phade. "Application of AES algorithm for data security in serial communication." In 2016 International Conference on Inventive Computation Technologies (ICICT), vol. 3, pp. 1-5. IEEE, 2016.

[9] U. Farooq r, and M. F. Aslam. "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA." Journal of King Saud University-

[10] Computer and Information Sciences 29, no. 3 (2017): 295-302

[11] G. Rouvroy, F.X. Standaert, Quisquater, J.-J., Legat, J., 2004.Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications. In: Proceedings of the International Conference on Information Technology: Coding and Computing.

[12] ITCC 2004, vol. 2, pp. 583–587

[13] M.I. Soliman, G.Y. Abozaid, 2011. {FPGA} implementation and performance evaluation of a high throughput crypto coprocessor. J. Parallel Distrib. Comput. 71, 1075–1084.

[14] J. Van Dyken, J.G. Delgado-Frias, 2010. FPGA schemes for minimizing the power-throughput trade-off in executing the advanced encryption standard algorithm. J. Syst. Archit. 56, 116–123.

[15] https://www.mordorintelligence.com/industry-reports/global-fpga-market-industry

[16] H. Zodpe, and A. Sapkal. "An efficient AES implementation using FPGA with enhanced security features." Journal of King Saud University-Engineering Sciences 2018.