Gyancity Journal of Engineering and Technology,
Vol.10, No. 1, pp. 1-8, January 2024
ISSN: 2456-0065 DOI: 10.21058/gjet.2024.10003

Performance Evaluation of AES Implementations on Different FPGA Architectures

Pushpanjali Pandey [1], D M Akbar Hussain [2]
[1]*Gyancity Research Consultancy, Greater Noida, India*
pushpanjali.pandey@gyancity.com
[2]*Aalborg University, Esbjerg, Denmark*
akh@et.aau.dk

Abstract

Data transmission is always vulnerable to assaults on the digital side. Cipher strength analysis is a crucial component of a business or academic safety evaluation. For data security, a robust encryption process is needed. Therefore, Advanced Encryption Standard (AES), an encoding requirement that was better than the standard, was modified in 2001 by the United States National Institute of Standards and Technology (NIST). The AES algorithm is solely based on the substitution-permutation network design concept and efficient in both software and hardware. The described method is an algorithm that uses a single identical secret key for encryption and decryption. Public or private, commercial etc. programmes are not allowed to utilise it. To date, significant research on spot methods is presently being conducted to protect further the AES algorithm. This study aims to examine the comparison of time and performance in two FPGAs, for both the architecture of the AES.

Keywords: *FPGA, AES, DES, Encryption, Decryption, and Data transmission.*

1. Introduction

A vast volume of data is transmitted every day through internet connection on an enormous level in different areas. The data is sometimes sent by the sender to the recipient through certain unsafe methods or channels. This makes a massive mess and compromises much sensitive data. In order to counter such tactics, public and private industry are developing and using specific encryption techniques to protect sensitive information, since this is a significant problem. Cryptography is an important method to secure sensitive information from attackers. Cryptography comprises of the encryption and decryption operations of two distinct kinds [1]. The method for

encoding data is termed encryption, i.e., the conversion of plain text in complicated and unreadable data or "chip text." It avoids compromised secrecy and does not allow outsiders to access the original information readily. Finally, the authorised receiver device is to be decrypted. One method used to convert the ciphertext to the simple original text produced by the owner is usually called decryption. Cryptography is entirely reliant upon the usual permutations and substitutes for the encryption & decryption process by mathematical computations with or without a key. Modern algorithms for cryptographing offer data integrity, authentication and privacy. Furthermore, cryptography is classified into 3 techniques: symmetric (private key), asymmetric and hash function. (Public key) [2]. A single key is used in the symmetric method to encrypt and decode information, whereas two separate keys are utilised in asymmetrical cryptography. Inputs of various lengths are taken to return outputs of a fixed length using cryptographic Hash function. Overall, Symmetric key algorithms are considerably quicker to run electrically than asymmetric key algorithms and are often employed. DES (Data Encryption Standard), Blowfish, Two Fish and AES are popular symmetric key algorithms (in their years of recognition). AES is the commonly used encryption algorithm. AES (Advanced Encryption Standard). The AES algorithm was created for the development or adoption of a new symmetrical core algorithm as a project of NIST - USA. Due to improved accurate safety, higher performance, integrity, more effectiveness, flexibility and simplicity of implementation [3] Rijndael algorithm created by two of the Belgium cryptographers Vincent Riymen and Joan Daemen was completed as AES in 1997. The US government initially used it to protect secret intellects. In order to ensure the information, AES may be used both in software and hardware. It consists of three components: AES-128, AES-192 and AES-256. AES-128 uses a 128-bit key length for encrypting and encoding the message block, while 192 and 256 key lengths for encrypting and decrypting the message are used for both AES-192 and AES-256 [4].

2. Advanced Encryption Standard (AES) Algorithm

The AES algorithm has been developed in 2000 by the National Institute of Standard Technology (NIST) to overcome assaults on the Data Encryption Standard (DES) method [5]. AES is a stronger and quicker DES variant. It is a symmetrical chip block, which is equivalent to both the algorithm encryption and decryption key. The rationale for switching between DES and AES is its 56-bit key which is uncharged in the rapid calculating age of today. In addition, an AES algorithm introduces a 128-bit, 192-bit and 256-bit data key. The key size is dependent on the amount in AES, 128-bit in 10 rounds, 192-bit in 12 rounds and 256-bit in 14 rounds [6]. Each round is encrypted using a cypher key that adds the round key, manipulates sub bytes, shifts and merges rows and columns to plain text [7]. Figure 1 describes the encryption of the AES algorithm.

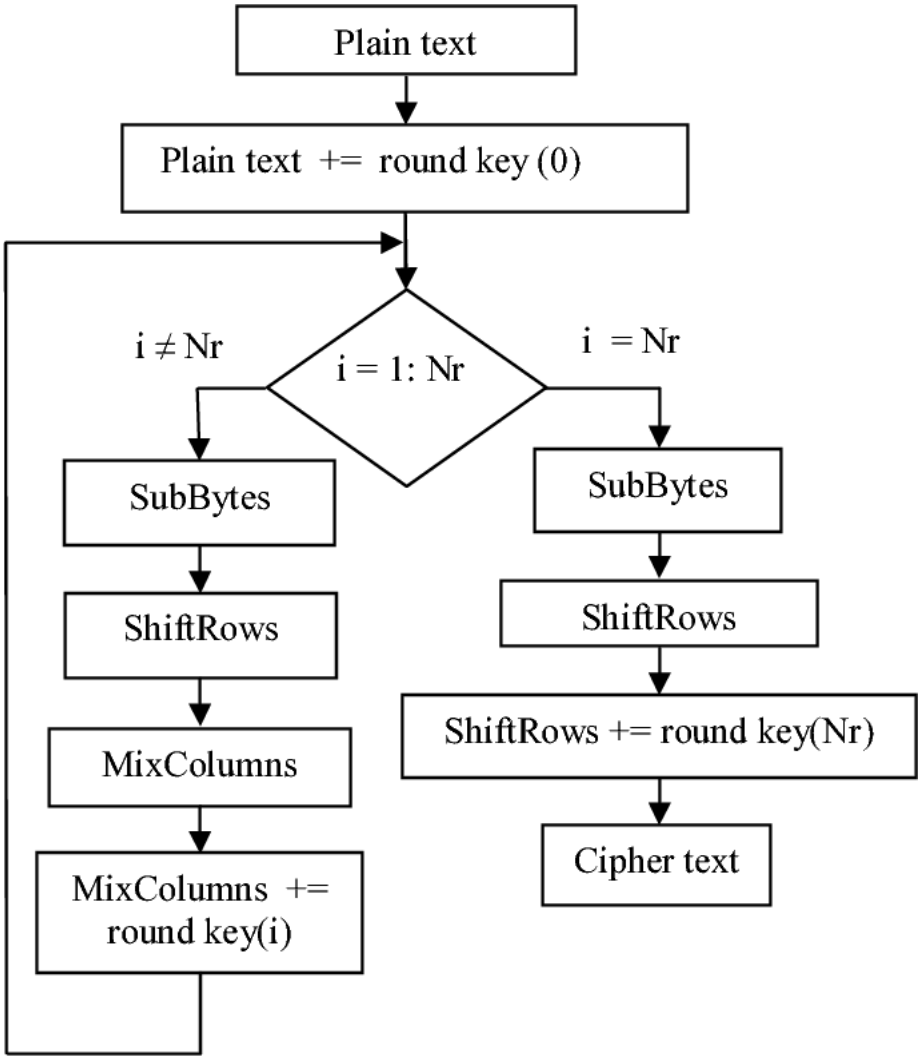

Figure 1: AES encryption method [7]

The encryption process includes the following stages mentioned below:

- Sub Bytes- We'll use an 8-bit S-Box to replace every byte with a substitution box. [5-10].
- Shift rows are moved to the left of the specified offset.
- Mix Column: Matrix multiplication is done in this step [5-10].
- Add round key: XOR process is done between key and the input [5-10].

2. Simulation on FPGA

The Virtex-6 and Spartan-6 algorithms of AES were implemented. Software was utilised to simulate Xilinx ISE. The 128-bit plain data, 128-bit size and 1-bit clock signal are available at the circuit input terminal. When the clock signal has been set, an EX-OR operation takes place in round 0 between 128-bit plain text and the 128-bit key

[8]. At round 0, the output is produced as input data for round 1 operation and the output for round 1 and so on is concurrently input for round 2. In all round stages, the key will be the same. The Figure 2 shows the internal hardware architecture for round 0 operations. The inner structure has a 128-bit flat text, which is round 0 output, a 128-bits key and an input clock signal. Two operations in round 0 which are sub bytes and rows of shifts [9]. The internal hardware from round 1 through round 9 is the same as of round 1.

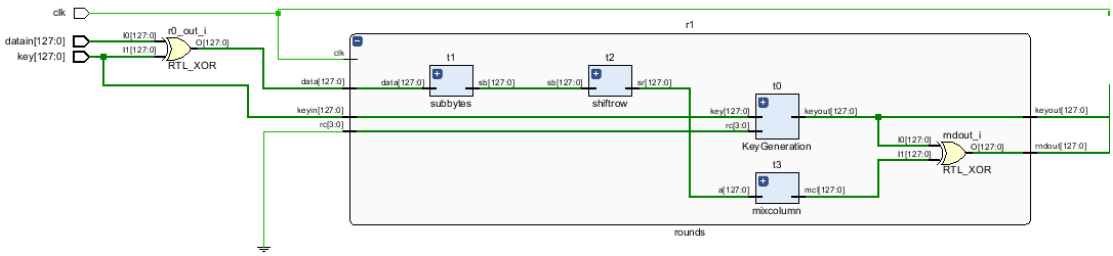

Figure 2: Internal structure of AES implantation on FPGA

3. Performance Evaluation Parameters

The calculation of the AES algorithm is done on the basis time and throughput which are specified as follows:

i. Time – It is a very significant constraint which is calculated in the performance of AES on FPGA [11-12]. The speed and performance get increased when the execution time is less. It is further sub-categorized as:
   a. Setup delay – The delay required by the external devices is known as setup delay.
   b. Hold delay – The delay required by the internal registers in known as hold delay.

ii. Throughput- It is the ratio of number of bits being processed and total time delay. For AES algorithm the processed bits will be 128 [13-15].

4. Result

Set up time delay comprises of three factors such as net delay, logic delay, and total

delay. For Virtex-6 FPGA, the logic delay is 75.30 ns, the net delay is 493.968 ns, and the total delay is 569.277 ns. For Spartan-6 FPGA, logic delay is 137.215 ns, net delay is 651.388 ns, and the total delay is 788.663 ns. The setup time delay is illustrated in table 1 and described in Fig. 3.

Table 1 Set up time delay for AES

FPGA	Total delay (ns)	Logic delay (ns)	Net delay (ns)
Virtex-6	788.663	137.215	651.388
Spartan-6	569.277	75.30	493.968

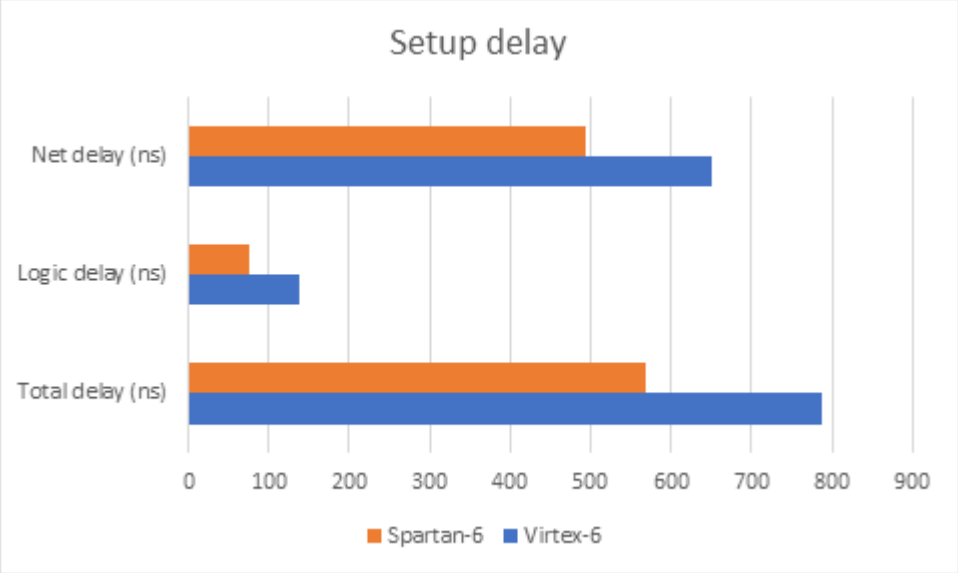

Figure 3 Setup delay time for AES

The hold delay is the combination of logic delay, net delay, and total delay. For Virtex-6 FPGA, the logic delay is 17.331 ns, net delay is 53.423 ns, and the total delay is 70.756 ns. For Spartan-6 FPGA, logic delay is 21.269 ns, net delay is 73.54 ns, and the total delay is 94.808 ns. The hold time delay defined in table 2 and represented in figure 4respectively.

Table 2 Hold time delay for AES

FPGA	Total delay (ns)	Logic delay (ns)	Net delay (ns)
Virtex-6	94.808	21.269	73.54
Spartan-6	70.756	17.331	53.423

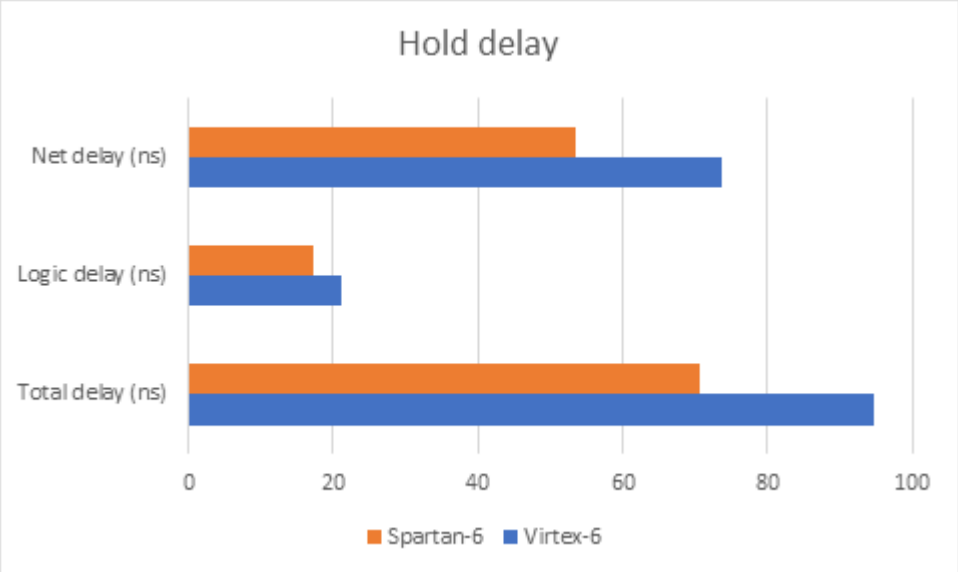

Figure 4 Hold delay time for AES

Throughput- For Virtex-6 and Spartan-6 the total delay is the sum up of set -up delay and hold delay which is 883.471 ns and 640.033 ns respectively. The number of bits processed for the AES is 128. Therefore, the throughput will be 1.44 Gbps and 1.99 Gbps for Virtex-6 and Spartan-6 respectively, as shown in figure 5.

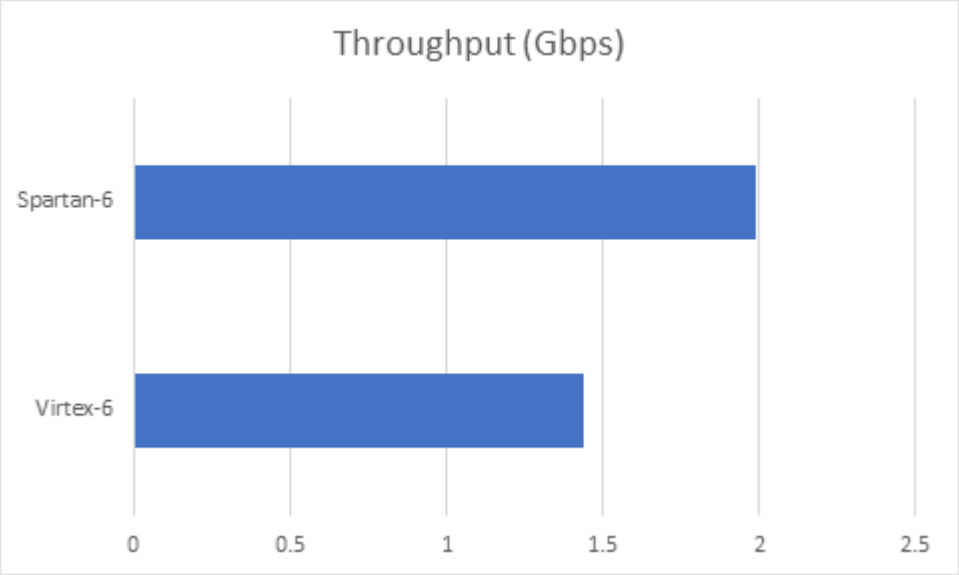

Figure 5: Throughput For AES

5. Conclusion

Data transmission is always vulnerable to assaults on the digital side. Cipher strength analysis is a crucial component of a business or academic safety evaluation. For data security, a robust encryption process is needed. Therefore, Advanced Encryption Standard (AES), an encoding requirement that was better than the standard, was modified in 2001 by the United States National Institute of Standards and Technology (NIST). The AES algorithm is solely based on the substitution-permutation network design concept and efficient in both software and hardware. This works gives an idea of encrypting AES algorithm for fast processing of IoT devices. In this the AES algorithms is implemented on two FPGA and It is observed that the Spartan-6 FPGA provides better throughput and less time delay to the FPGA devices. This high throughput and less delay in time will be very much beneficial for IoT devices.

6. Future Scope

From the above study it is observed that, every AES execution is now carried out on the Virtex and Spartan FPGA 5th series and 6th series. FPGAs in the 7th Artix, Kintex, Zynq, Ultra-Scale FPGA series are not being worked out much. The conventional and modified AES algorithm for these FPGAs may thus be implemented by researchers. Effective AES algorithms may also be designed by researchers using different power efficient methods for their AES algorithm.

References

1. The Rijndael Block Cypher - AES Proposal: Rijndael, Joan Daemen, Vincent Rijmen.
2. Joan Daemen, Vincent Rijmen The Design of Rijndael AES — The Advanced Encryption Standard, November 26, 2001
3. Lu C. C., & Tseng S. Y, "Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter in Application-Specific Systems, Architectures and Processors", Proceedings of the IEEE International Conference, 2002, pp. 277-285.
4. Nadeem H, "A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, 2006, pp. 84-89.
5. Kumar, Keshav, K. R. Ramkumar, and Amanpreet Kaur. "A lightweight AES algorithm implementation for encrypting voice messages using field programmable gate arrays." Journal of King Saud University-Computer and Information Sciences 34, no. 6 (2022): 3878-3885.
6. Berent, A, "Advanced Encryption Standard by Example", Document available at URL http://www. networkdls. com/Articles/AESbyExample. Pdf, April, 2007.
7. H. Mestiri, F. Kahri, B. Bouallegue, and M. Machhout, "A high-speed AES design resistant to fault injection attacks", Microprocessors and Microsystems, vol. 41, pp. 47–55, 2016.
8. M.Pitchaiah, Philemon Daniel, Praveen, "Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific & Engineering Research Volume 3, Issue 3, ISSN 2229-5518, March 2012.
9. Rachh, R.R.; Anami, B.S.; Ananda Mohan, P.V, "Efficient implementations of S-box and inverse S-box for AES algorithm", TENCON 2009, IEEE Region 10 Conference, pp.1–6, Nov. 2009.
10. Pandey, Bishwajeet, and Keshav Kumar. Green Communication with Field-programmable Gate Array for Sustainable Development. CRC Press, 2023.
11. 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.
12. 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 Computer and Information Sciences 29, no. 3 (2017): 295-302
13. 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 ITCC 2004, vol. 2, pp. 583–587
14. 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.
15. Kumar, Keshav, Amanpreet Kaur, K. R. Ramkumar, Anurag Shrivastava, Vishal Moyal, and Yogendra Kumar. "A design of power-efficient AES algorithm on Artix-7 FPGA for green communication." In 2021 International Conference on Technological Advancements and Innovations (ICTAI), pp. 561-564. IEEE, 2021.
16. H. Zodpe, and A. Sapkal. "An efficient AES implementation using FPGA with enhanced security features." Journal of King Saud University-Engineering Sciences 2018.