iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VIII **Month of publication:** August 2020

DOI: https://doi.org/10.22214/ijraset.2020.31056

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 8 Issue VIII Aug 2020- Available at www.ijraset.com

Datapath Optimization in AES using Pipelined Architecture

Dr. Anita Titus[1], D. Asha Preethi[2]
[1]M.E., [1]Ph.D., [2]M.E.*Department of Electronics and Communication, Jeppiaar Engineering College, Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai, India.*

Abstract:** In today's world of social distancing due to the consequences of deadly virus COVID, every way of communication is articulated through internet technology. In this pandemic situation securing the information transmitted has become a major threat since exploitation of information has become one of the major problem in world's economy. The project provides an enlightening path to establish a safer ground for communication. In the proposed technique security and confidentiality of the data transmitted is enhanced by implementing AES algorithm in the memory of the system, where the information sent are encrypted and decrypted directly in memory rather than using external registers. Thereby data stored are accessed immediately without any delay for locating the allocated address and this technique is proven to be resistive to most of the attacks. Further by using pipelining concept datapath optimization is also enhanced which in turn increases the latency and reduces the area occupied by the algorithm. The proposed architecture uses 11 S boxes for encrypting and decrypting 16-bit data using Spartan 6 TQG144 FPGA board for hardware and Xilinx 14.7 design suite for software implementation using Verilog code which offers a quicker and customizable solution. By utilizing this architecture, the overall speed and latency has been improved by reducing the usage of LUT's to 8% and the total delay to 23.081ns and number of bonded IOB's used is 79 only.
Keywords: Communication, AES algorithm, Encryption, Decryption, Pipelining, Verilog code

I. INTRODUCTION TO CRYPTOGRAPHY

The number of individuals and organizations using wide computer networks for personal and professional activities has recently increased a lot. A cryptographic algorithm is an essential part in network security. A well-known cryptographic algorithm is the Data Encryption Standard (DES), which has been widely adopted in security products. However, serious considerations arise for long-term security because of the relatively short key word length of only 56 bits and from the highly successful cryptanalysis attacks. In November 2001, the National Institute of Standards and Technology (NIST) of the United States chose the Rijndael algorithm as the suitable Advanced Encryption Standard (AES) to replace the DES algorithm. Since then, many hardware implementations have been proposed in literature. Some of them use field programmable gate arrays (FPGA) and some use application-specific integrated circuits (ASIC). The advantages of a software implementation include ease of use, ease of upgrade, portability, and flexibility. However, a software implementation offers only limited physical security, especially with respect to key storage Conversely, cryptographic algorithms (and their associated keys) implemented in hardware are, by nature, more physically secure, as they cannot easily be read or modified by an outside attacker. The downside of traditional (ASIC) hardware implementations is the lack of flexibility with respect to algorithm and parameter switching. Reconfigurable hardware devices such as FPGAs are a promising alternative for the implementation of block ciphers. FPGAs are hardware devices whose function is not fixed and can be programmed in-system.

II. EXISTING METHODOLOGY

AES-CCM in which AES block cipher core is used for the purpose of authenticated encryption. The bit order of each input block is formatted. The AES-CCM operation consists of two related processes which are generation/ encryption and decryption/verification. Firstly, in the generation/encryption process, an initial block B0, and Payload blocks (B1÷Bn) are used in CBC mode, to generate a message authentication code (MAC). Then, CTR mode whose inputs are Counter Blocks CTRi, is applied to generate the cipher-text. The size of received cipher-text is equal to sum of the length of payload and the length of MAC. In decryption/verification process, counter mode decryption is applied to cipher-text to recover 2016 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC) the MAC and the corresponding payload; then, CBC mode is applied to the payload, the associated data, and the nonce to verify the correctness of the received MAC. A successful verification indicates that the payload and its associated data come from the same source with access to the key so that a MAC provides a high level of authentication.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

Since AES encryption block is the essential part in the AESCCM core, the choice for its architecture is very important. Implemented low area AES encryption cores by using the 8-bit AES core architecture and an optimized S-box structure. For FPGA implementation, using block RAMs to implement the 8-bit AES core is also a promising solution to reduce AES core area. The penalty of this solution is that it may lead to the lower throughput due to its iterative manner. Then, using a pipeline AES structure is a promising approach to improve the throughput, such as the AES core, although this core area is 3.6 times larger than the iterative looping structure. On the other hand, it is important to note that a typical data rate in WBANs of up to 10Mbps can meet the speed requirement for most of entertainment and healthcare services. Since throughput is not the most important issue in WBANs, iteration structure is used to minimize the hardware resource and to meet the requirement of low power consumption as well.

III. PROPOSED SYSTEM

A. Pipelined Architecture of AES Algorithm

The Advanced Encryption Standard is a symmetric cryptographic algorithm which is composed of four major blocks that are repeated in N_r number of rounds. The blocks are byte substitution, shift row, mix column, and key addition. When a key size of 128 bits is used, the number of rounds the algorithm is repeated (N_r) is equal to ten and for 196 bits it is 12 and for 256 bits it is 14. Figure 1 shows the fully pipelined implementation of the AES algorithm. The shift row step is just interconnection in which the plain text of length 128 bits is put in a matrix format and there would be shift of bits in an orderly fashioned manner such that there it would be no shift in first row and one left shift in the second row and two left shift in third row and it goes on respectively and the key addition is XOR ing of the round data and the round key. The mix column step consists of a chain of XORs to permute the elements of data in each column and they would place it by mixing the column in an order. The arithmetic of these three stages can be combined in one pipeline stage for each round. On the other hand, the most exemplary step is the byte substitution phase, which is explained next.

B. Byte Substitution Phase

In AES algorithm byte substitution phase (S-box) is considered as a distinct step because the computation part is quiet complex. The byte substitution phase consists of two steps

1) The multiplicative inverse

2) The affine transformation

The multiplicative inverse for the input element GF (2^8) is calculated earlier. Later, an affine transformation for the input element GF (2^8) is applied. In order to simplify this operation composite field arithmetic is used. The S- box is typically realized as LUT in software processing. For a Shannon expression of n-variable functions the original S-box is broken down into a set of smaller size multiplexer-switched truth-table. Later the smaller tables are mapped into n-LUT of Spartan 6 FPGA. All the substitute values are calculated beforehand and later stored in the non-volatile RAM of the processor. Rijmen suggests an algorithm that calculates the byte substitution phase using the GF (2^4) operations. The input is mapped into the GF (2^4) elements and the GF (2^4) operations are used. This is the most area efficient implementation of S-boxes. Due to the long delay of this architecture, pipelining must be used the LUT usage and the critical path delay of the pipelined implementation of one S-box using this architecture synthesized for Spartan 6 FPGA (pre-place and route). The bar chart shows the delay and the pie chart shows the LUT usage. The required delay-LUT combination is the design with three pipeline stages. As the most efficient byte substitution designs are considered to have around three and six pipeline stages. In addition, to the last pipeline stage of each round of the AES algorithm which includes the shift row, mix-column and key addition phase. Therefore, for an optimum pipelined implementations of AES algorithm it may take around four or seven pipeline stages totally for each round in the cryptographic algorithm.

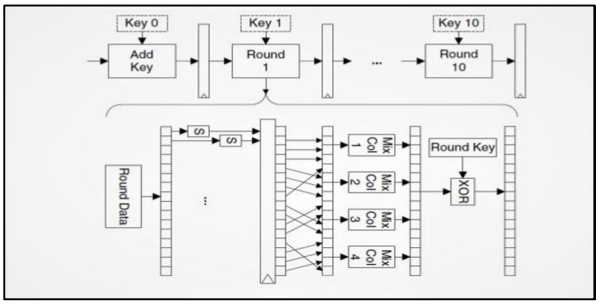


Figure 1: Fully Pipelined AES Architecture In NVMM

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The AES algorithm is implemented in non volatile main memory using pipelining architecture and it is simulated using XILINX ISE 14.7 design suite and by using Spartan 6 FPGA board the hardware implementation is carried out

Table 1

Representation of device parameters

FAMILY	SPARTAN6
PART	XC6SLX9
PACKAGE	TQG144
TEMP GRADE	C-GRADE
PROCESS	TYPICAL
SPEED GRADE	-2

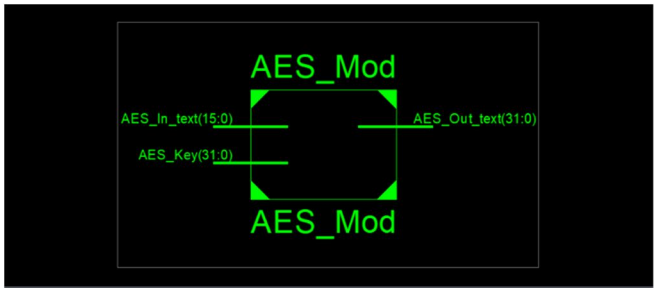


Figure 2: Representation of RTL Schematic View of AES

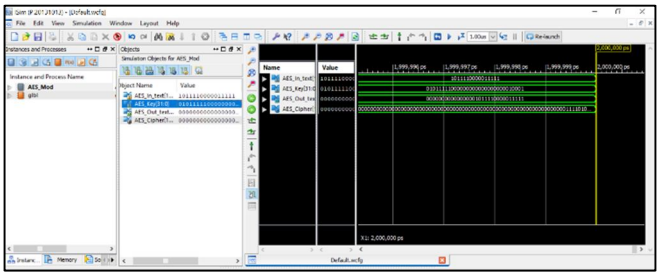


Figure 3: Simulation of AES algorithm using NVMM and Pipeline architecture

Supply Summary		Total	Dynamic	Quiescent
Source	Voltage	Current (A)	Current (A)	Current (A)
Vccint	1.200	0.004	0.000	0.004
Vccaux	2.500	0.003	0.000	0.003
Vcco25	2.500	0.001	0.000	0.001
		Total	Dynamic	Quiescent
Supply Power (W)		0.014	0.000	0.014

Figure 4 :Power Analysis of AES algorithm using Pipeline architecture

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

Table 2
Performance evaluation in terms of Latency

DEVICES	SLICE LUT'S	LATENCY(ns)
Virtex-5 (xc5vlx50-3)	2490	45.06
Virtex-7 (xc7vx690t)	10773	142.5
Spartan6 (xc6slx9)	532	32.293
Spartan6 (xc6slx9) PROPOSED SYSTEM	465	23.081

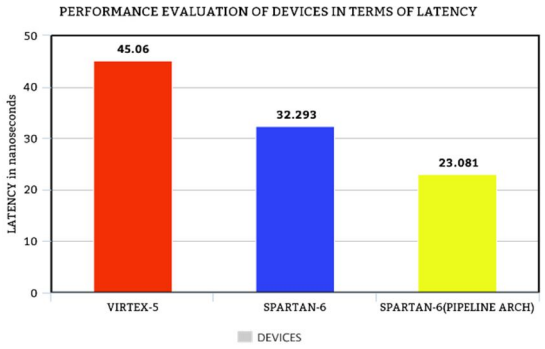


Figure 4: Bar chart representation for Latency values

Table3
Performance evaluation in terms of Usage of LUT's

DEVICES	**SLICED LUT'S**
VIRTEX-7(XC7VX90T)	551
SPARTAN-6(XC6SLX9)	532
SPARTAN-6(XC6SLX9) (PIPELINE ARCHITECTURE)	465

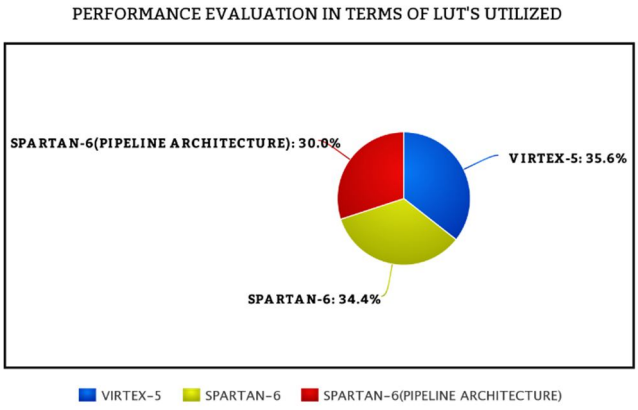


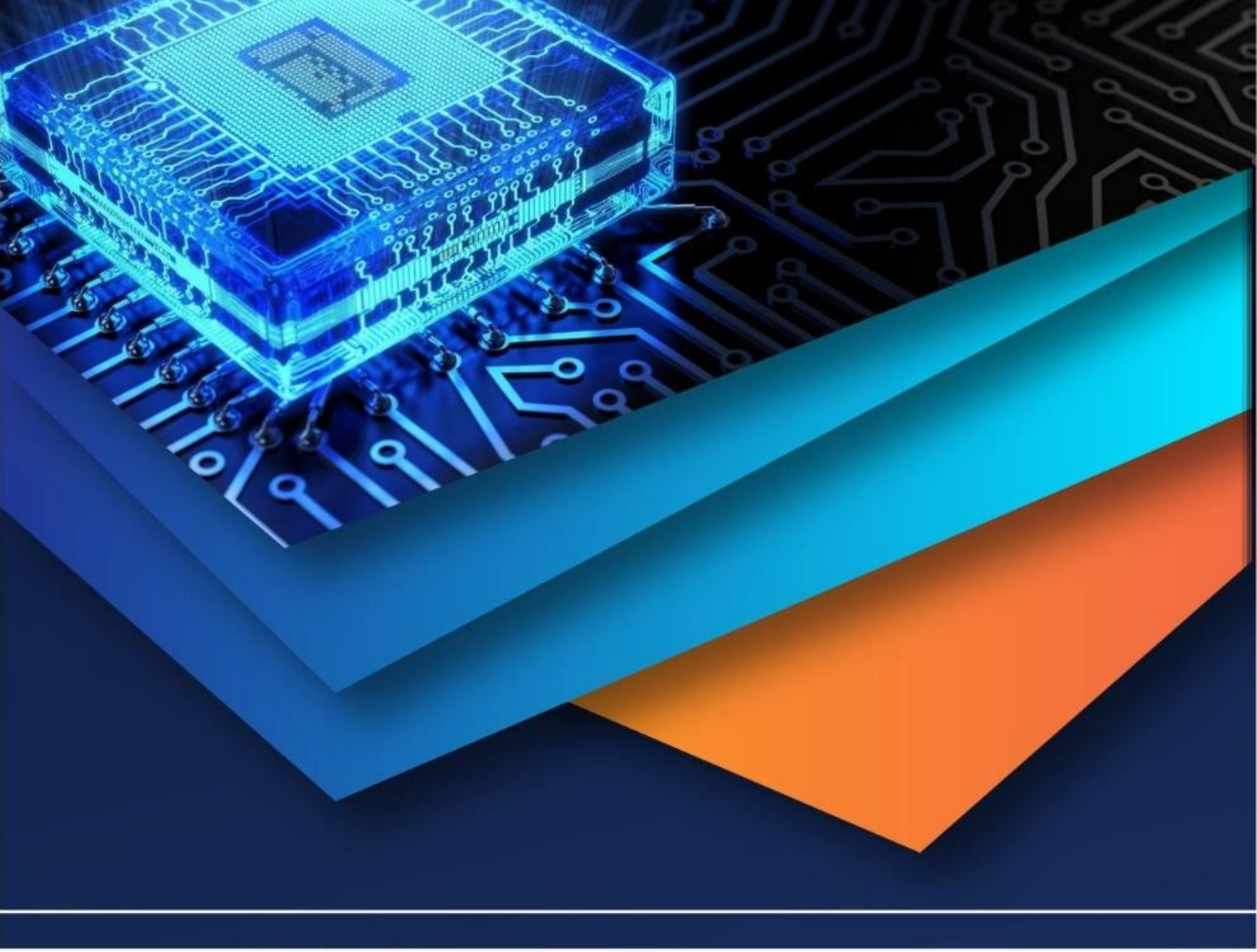
Figure 5: Pie Chart representation for usage of LUT's

V. CONCLUSION AND FUTURE WORKS

From the analysis by using AES in non volatile main memory and by utilizing pipeling architecture the latency and speed of the device is increased as the delay of masking and unmasking data took less than 23ns and the area occupied by the algorithm was also only around 8%. The Algorithm is also resistive to side attacks as it uses 10 rounds for encrypting the bits in AES Algorithm. Thereby it can be tentatively declared that AES algorithm is better solution for securing and transmitting confidential information. In future the above technique can be improvised by reducing the rounds in the algorithm. So that space for implementation of algorithm can be reduced and thereby the speed can also be increased. Or else some new encryption techniques can be adapted and evaluated to reduce side channel attacks.

REFERENCES

[1] T. Luo, W. Zhang, B. He, and D. Maskell, "A racetrack memory based in-memory booth multiplier for cryptography application," in Proc. ASP-DAC, Jan. 2016, pp. 286–291.
[2] R. Maes, A. Van Herrewege, and I. Verbauwhede, "PUFKY: A fully functional PUF-based cryptographic key generator," in Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst., 2012, pp. 302–319.
[3] S.Mathew et al., "53Gbps native GF 2 composite-field AES-encrypt/decrypt accelerator for content-protection in 45 nm high-performance microprocessors," in Proc. IEEE Symp. VLSI Circuits (VLSIC), Jun. 2010, pp. 169–170.
[4] S.Swami, J. Rakshit, and K. Mohanram, "SECRET: Smartly Encrypted Energy efficient non-volatile memories," in Proc. 53nd ACM/EDAC/IEEE Design Automat. Conf. (DAC), Jun. 2016.
[5] K.Tsuchida et al., "A 64Mb MRAM with clamped-reference and adequate-reference schemes," in Proc. ISSCC, Feb. 2010, pp. 258–259.
[6] K. Venkatesan, S. Herr, and E. Rotenberg, "Retention-aware placement in DRAM (RAPID): Software methods for quasi-non-volatile DRAM," in Proc. 12th Int. Symp. High-Perform. Comput. Archit. (HPCA), Feb. 2006, pp. 155–165.
[7] Y. Wang, L. Ni, C.-H. Chang, and H. Yu, "DW-AES: A domain walls nanowire-based AES for high throughput and energy-efficient data encryption in non-volatile memory," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2426–2440, Nov. 2016.
[8] V. Young, P. J. Nair, and M. K. Qureshi, "Deuce: Write-efficient encryption for non-volatile memories," in Proc. 20th Int. Conf. Archit. Support Program. Lang. Oper. Syst. (ASPLOS), 2015, pp. 33–44.
[9] P. Zhoum, B. Zhao, J. Yang, and Y. Zhang, "A durable and energy efficient main memory using phase change memory technology," in Proc. 36th Annu. Int. Symp. Comput. Archit. (ISCA), 2009, pp. 14–23.
[10] E. B. Barker et al., "Guideline for using cryptographic standards in the federal government: Directives, mandates and policies," Tech. Rep. Special Publication (NIST SP)-800-175A, Aug. 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY