Research Journal of Computer Systems and Engineering

ISSN: 2230-8571, 2230-8563

Volume 03 Issue 01 - 2022 (January to June)

Page 14:20

Cognitive Computing-Based Network Access Control System in Secure Physical Layer

Sandeep Dwarkanath Pande
Computer Science & Communication Engineering
MIT, Academy of Engineering, Alandi, Pune
ORCHID ID-0000-0001-6969-0423
sandeep7887pande@gmail.com

Dr Sk Hasane Ahammad
Computer Science & Communication Engineering;Signal Processing
Koneru Lakshmaiah Education Foundation and Assistant Professor
ORCHID ID-0000-0002-2587-4164
ahammadklu@gmail.com

Article History

Received: 22 January 2022
Revised: 14 April 2022
Accepted: 19 May 2022

Abstract

Blockchain technology is used in the suggested solution to create a healthcare ecosystem that is decentralised, scalable, iterative, and accessible. This will allow patients to easily and securely exchange their medical records with doctors, hospitals, research organisations, and other stakeholders while giving them total control over the privacy of their medical data.The enhanced AES algorithm is implemented quickly in this work with a transformation-based s-box for increased security. The addition of the Affine transformation for vector multiplication is what gives S-box its performance. Then, it is examined using the appropriate software design on a Xilinx Virtex-5 FPGA device with the XC5VLX50 foundation software.The suggested enhanced AES algorithm accomplishes this and has an efficiency rate of 85.6%.
Keywords: FPGA, AES, Encryption, S-box, Transformation.

1. INTRODUCTION

Securing data [1] is a vital role which has to be carried out mainly in military and diplomatic applications and also in applications like e-banking, e-mail, internet and messaging networks etc. For complex real time applications like data acquisition and processing, it is essential to establish reliable communication among multiple FPGA systems/cards [2]. AES can be employed in software as well as hardware implementation. The software implementation of AES is a slow process and thus consumeslots of processing time and also requires regular updates [3]. Due to these reasons hardware implementation is widely used for real time applications[4]. Normally there are two platforms for hardware implementations of AES namely FPGA and ASIC (Application Specific Integrated Circuit).

2. LITERATURE SURVEY

Work [5] coined an efficient resource reconfigurable hardware AES implementation using High Level Language on FPGA. Author [6] developed AES-KDS block cypher, which operated on 128 bit key length and data length, using 5 phases instead of 4 phases used in AES. Work [7]developed technique involved key expansion method integrated with S-box rotation and that property was employed thereby making S-box key-dependent where better security to the block cipher was provided. Work [8] developed dynamic S-Boxes based on cipher key. To generate S-boxes with more secure block ciphers they uses cipher text [9]. Moreover, problem raised from fixed structure S-Boxes was solved and security of block cipher was increased. Generating several S-Boxes by altering the cipher key is the major achievement of this algorithm [10].

3. PROPOSED METHODOLOGY

AES is a type of block cypher, symmetric in nature, which for commonly used applications is much more advantageous than the traditional DES method.Add Round Key is simply a bitwise XOR of current block. Proposed methodology is examined using XC5VLX50 FPGA for analysis. The maximal frequency targeted by the proposed Improved AES with S-box is 721 MHz with maximal clock frequency of 360 MHz.This simple structure is depicted in figure 1 and figure 2 shows the S box architecture.

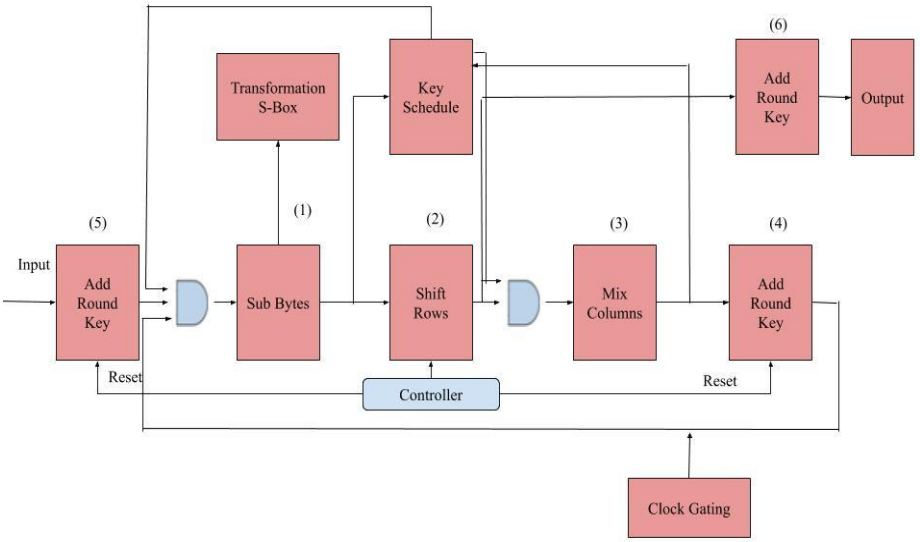

Figure 1: Architecture of proposed improved AES by Affine transformation based SBox

In AES algorithm, during the encryption process, every round except the final perform the following transformations:

i. SubBytes: Operates independently in every byte of State. Each state byte is replaced with the corresponding S-box byte.

ii. ShiftRow: Rows of the State undergo a cyclic shift over various offsets.

iii. MixColumn: A fixed polynomial is multiplied and state columns are known as polynomials over GF(28). In the last round, this operation will not be done.

iv. AddRoundKey: Performs bitwise XOR

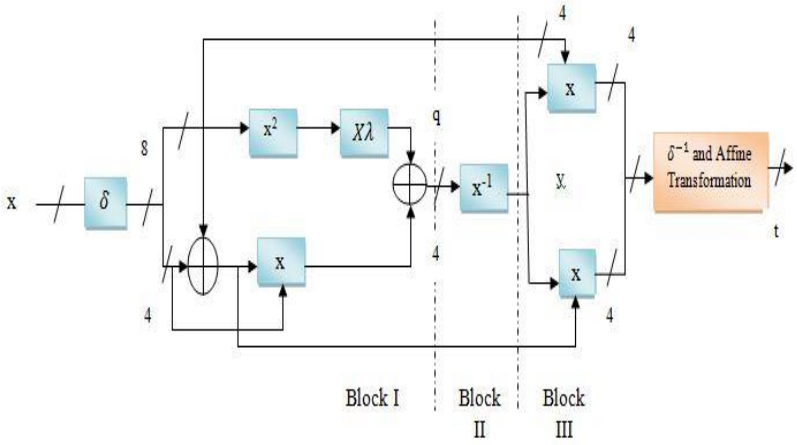

Figure 2: Architecture of S-box

3.7 Improved AES algorithm by Transformation based SBox (IAES)

Inputs: Initialization of Secret key m(k), where k is a byte vector ranging from 0 to 255.

Initial AES S-Box AES transformation based SBox(k), vector k ranges from 0 to 255.

Complex polynomials ComPoly(k) which is a vector comprising of all possible values of 30 complex polynomials.

Outputs: Key-dependent affine transformation S-Box Aff-SBox(k), byte vector k ranges from 0 to 255. Key-dependent inverse affine transformation S-Box invAff-SBox(k), byte vector k ranges from 0 to 255.

i. Secret key k is estimated depending on the entire key values by eq. (1)
   a. W(k):P←⊕k=1n AES transformation-SBox(W1(n)) (1)
ii. Select the complex polynomial n the from array ComPoly based on the key value k by eq. (2)
   a. k←P mod 30 (2)
iii. n←ComPoly (k)
iv. Now, select affine transformation constant 'a' which is dynamic reliant on key value k where a ranges from 0 to 255 by eq. (3)
   a. a←AEStrasformaitonSBox(k) (3)
v. For all n=0,1,…,255do:
   a. Now, select 'b' inverse affine transformation of every element of 'n' using active complex polynomial m:p←FndInvaffine(n,m)
   b. s←AffineTransf(p,m)
   c. Now make the decided S-box based on the key value k:
i. S-Box(n)←s⊕k
vi. Endfor
vii. Store the constants of new S-Box to DSBox: DSBox←SBox
viii. Generate key-dependent inverse dynamic S-Box InvDSBox:
ix. For all k ranging from 0 to 255 do:
   a. Inverse- trans SBoxDSBox(n))←n
x. endfor

Clock cycle utilized for both encryption and decryption process is 1 clock. Based on permutation and combination process of bits in S-box clock frequency is measured. A sequence of various amount of round functions is initiated to realize Six static designs.

- Standalone Nr: In the AES standalone implementation, N denotes the number of unrolled rounds r of the transformation based S-box.

- CGR: this is able to mimic all the unrolled standalone designs as AES algorithm is permitted to execute with the unrolled round(s) r of 1, 2, 3, 4, 5, or 10

- CGR cg: Clock gating is applied to the base CGR AES.

Turning off all the clock lines with clock gating resulted in a standby consumption that is practically independent from the circuit size. Therefore, the power consumption reduction for the technique is maximum.

4. PERFORMANCE ANALYSIS

The improved AES designed here has been captured with VHDL as well as designs instantiated with Xilinx Virtex-5 foundation software XC5VLX50. This design is synthesized with FPGA Devices. The parameters namely Throughput, Latency, Efficiency and Maximum clock frequency were employed to estimate the proposed improved AES implementation. The comparison of the proposed with exiting methods is depicted in table 1.

The **efficiency** of S-boxes is stated as that reduced overhead time and maintains good accuracy for different slides. It can be defined as eq. (4):

$$Efficiency\ (\%) = \frac{Throughput}{Number\ of\ utilized\ slices} \qquad (4)$$

Clock frequency: Conceptual tools available for overall structure to be applied and maximum clock frequency fixed by critical path.Clocks may be limited to operate only in that area to safeguard wasting power when transmitting signals to other areas of system.

Throughput: With number of stages and additional register count, number of blocks per second increases linearly through this throughput is calculated.

Latency:is about the minimum processing time for one block independently of other blocks.

Table 1: Comparison of existing and proposed AES algorithm

Parameters	**Basic AES algorithm-128 Encryption** [12]	**AES with Rijndael algorithm** [13]	**Improved AES algorithm by Transformation based S-box (IAES)** (proposed)
Throughput (Gbps)	2.86	1.97	3.45
Clock frequency (MHz)	628	739	762
Number of slice	303	1745	291
Efficiency (%)	73%	58%	85.6%
Power consumption (mw)	58mW	74Mw	30mW

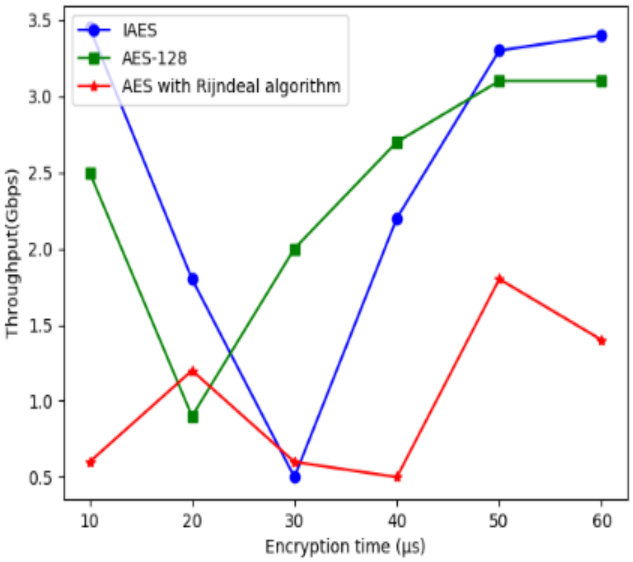

Figure 3: Analysis of throughput

Figure 3 indicates the throughput analysis of proposed method. It is shown that the proposed IAES method achieves 0.45 Gbps with average accessing time.

Figure 4 shows the performance of clock frequency between existing and proposed method. Basically, the usual frequency range of embedded microprocessors is from 100 to 600 MHz but the clock frequency of several FPGAs are from 30 to 100 MHz range. From the graph it is shown that the proposed IAES method achieves 561MHz which is having the difference rate of 10% with AES-128 and 30% with AES-RA.

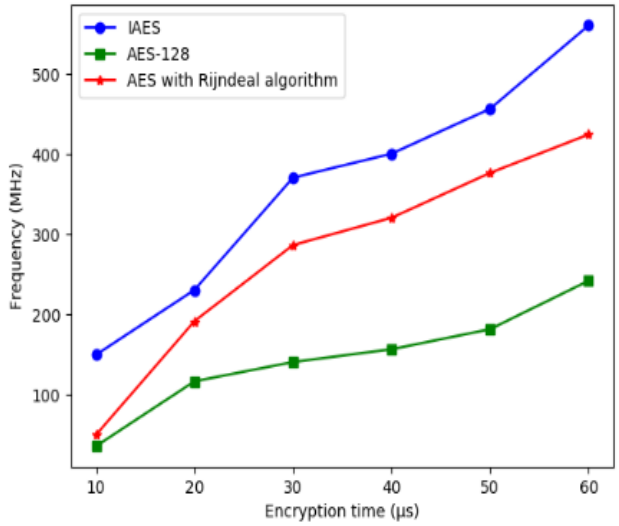

Figure4: Analysis of clock frequency

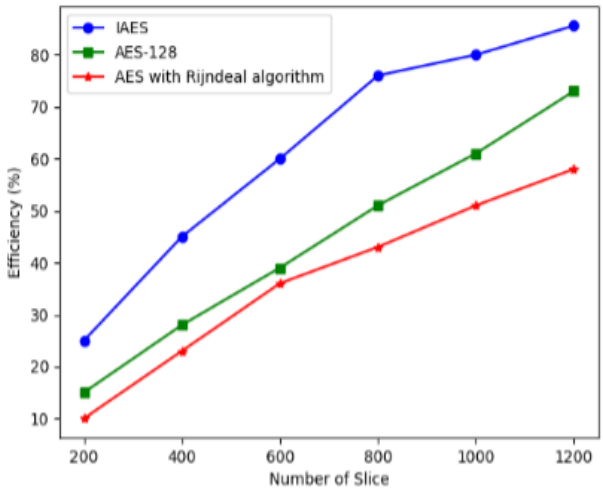

Figure 5: Overall efficiency calculation

Figure 5 shows the analysis of efficiency whereas the proposed IAES achieves 85.6% with the number of slices as 1200. Efficiency measure of AES-RA exhibits 72%, AES-128 provides efficiency level of 40% and IAES provides efficiency level of 85%. This implies that proposed IAES exhibits higher efficiency rather than AES - 128 and AES-RA technique. The efficiency of IAES is approximately 30% higher than conventional AES technique with utilizationof less number of slices results in better efficiency.

5. CONCLUSION

In this paper, an FPGA execution of improved AES utilizing high performance transformation based S-Box design applied in the step of sub-byte process during encryption and decryption is presented. The proposed method was executed on Xilinx Virtex-5 XC5VLX50 FPGA device. Modified design algorithm improves the overall security of the system with the minimized utilization of resources. The proposed IAES significant improves the performance in terms of efficiency as well as power consumption level. In terms of efficiency proposed IAES exhibits approximately 25% improved efficiency and power consumption level of IAES is 30% minimal than existing technique. Further, proposed Improved AES (IAES) algorithm by Transformation based S-box achieves the efficiency of 85.6% and throughput around 3.45GbPs when implemented in the presence of 439 LUTs. The future work is to improve the speed by including an effectual speed enhancement technique.

REFERENCES

[1] R Gayathri, E Roshith, BS Roshini, S Murugan, S Priya. (2017). Implementation of Arduino based Enhanced Fingerprint Biometric System for Secured Data Exchange.International Journal of Computational Intelligence Research, 13(8), 2113-2123.

[2] Deshpande, P. U., & Bhosale, S. A. (2015, October). AES encryption engines of many core processor arrays on FPGA by using parallel, pipeline and sequential technique. In 2015 International Conference on Energy Systems and Applications (pp. 75-80). IEEE.

[3] Nadjia, A., & Mohamed, A. (2015, March). Aesip for hybrid cryptosystem rsa-aes. In 2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices (SSD15) (pp. 1-6). IEEE.

[4] Chen, M., Li, W., Hao, Y., Qian, Y., &Humar, I. (2018). Edge cognitive computing based smart healthcare system. Future Generation Computer Systems, 86, 403-411.

[5] Cui, J., Huang, L., Zhong, H., Chang, C., & Yang, W. (2011). An improved AES S-Box and its performance analysis. International Journal of Innovative Computing, Information and Control, 7(5), 2291-2302.

[6] Chen, M., Li, W., Fortino, G., Hao, Y., Hu, L., &Humar, I. (2019). A dynamic service migration mechanism in edge cognitive computing. ACM Transactions on Internet Technology (TOIT), 19(2), 1-15.

[7] Chen, M., Herrera, F., & Hwang, K. (2018). Cognitive computing: architecture, technologies and intelligent applications. Ieee Access, 6, 19774-19783.

[8] Chen, S., Kang, J., Liu, S., & Sun, Y. (2019). Cognitive computing on unstructured data for customer co-innovation. European Journal of Marketing.

[9] Zhang, Y., Ma, X., Zhang, J., Hossain, M. S., Muhammad, G., & Amin, S. U. (2019). Edge intelligence in the cognitive Internet of Things: Improving sensitivity and interactivity. IEEE Network, 33(3), 58-64.

[10] Wu, S., Wang, M., &Zou, Y. (2018). Bidirectional cognitive computing method supported by cloud technology. Cognitive Systems Research, 52, 615-621.