

FPGA Implementation of High-Performance s-box Model and Bit-level Masking for AES Cryptosystem

B. Murali Krishna¹, Chella Santhosh², and S.K. Khasimbee³

^{1,2,3}Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India, ¹muralikrishna@kluniversity.in, ²raurisanthosh@gmail.com, ³2001080006@kluniversity.in


*Corresponding Author: B. Murali Krishna; E-mail: muralikrishna@kluniversity.in

ABSTRACT- The inadequacies inherent in the existing cryptosystem have driven the development of exploit the benefits of cipher key characteristics and associated key generation tasks in cryptosystems for high-performance security systems. In this paper, cipher key-related issues that exists in conventional symmetric AES crypto system is considered as predominant issues and also discussed other problems such as lack of throughput rate, reliability and unified key management problems are considered and solved using appropriate hierarchical transformation measures. The inner stage pipelining is introduced over composite field based s-box transformation models to reduce the path delay. In addition to that, this work also includes some bit level masking technique for AES. The improved diffusion and confusion metrics of bit masking transformation model mitigates key management related issues. An extensive analysis of data rate proved the performance metrics of proposed AES model. And finally, FPGA implementation is carried out to validate the performance metrics in real time.

Keywords: AES, Flip Flop Masking, Cryptosystem, Key Leakages, FPGA.

ARTICLE INFORMATION

Author(s): B. Murali Krishna, Chella Santhosh, S.K. Khasimbee;

Special Issue Editor: Dr. S. Gopalakrishnan ;

Received: 10/03/2022; **Accepted:** 11/05/2022; **Published:** 30/05/2022;

E-ISSN: 2347-470X ;

Paper Id: 0422SI-IJEER-2022-11;

Citation: 10.37391/IJEER.100221

Webpage-link:

<https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100221.html>



This article belongs to the Special Issue on **Intervention of Electrical, Electronics & Communication Engineering in Sustainable Development**

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

transformation is called encryption and converted irregular characters are called ciphers.

Generally, encryption algorithms fall under two categories namely asymmetric (public-key) [9] or symmetric [20]. Asymmetric cryptosystems offer improved security as compared to their counterpart symmetric model with limitations in terms of computational complexity and resource requirements and thus it is considered as complex algorithms. To narrow down the complexity overhead several lightweight cipher asymmetric models are proposed which consume fewer resources as compared to conventional asymmetric cores. In most cases, security compromises are almost matched with unified key scheduling and various models of transformation functions [21].

In last few years the influence of these vulnerable security systems is emerging steadily with the tremendous growth of smart phones and emerging IoT applications [1, 8]. Among various crypto core types used wireless and telecommunications systems AES has steadily emerged in recent years for its advantages such as improved security profile and hierarchical key and physical transform configuration [10, 12]. Moreover, the AES system exploits key localization properties which result in secured data transmission. In recent years several works investigates the modified AES system which can improve the performance rate and area efficiency and also allows to assist high-end traffic and throughput rate and to ensure compatibility over real-time environment [13, 14, 16].

2. RELATED WORK

The performance metric analyses of conventional AES cryptosystems and its potential security levels are investigated in many existing works. Most of the previous works relies on

1. INTRODUCTION

With the recent advancements in cipher cores, several methodologies are introduced to maximize the security metrics of the crypto transformation and the level of transformation required to secure the information also increased steadily. In most cases some combined approaches are used to achieve this task and also mitigate the key management's issues as well. To ensure the cryptosystems are economically viable, cipher transformation are need to be done with minimal computational complexity overhead using most simplified arithmetic computation which makes all existing crypto core models are out of choice. The inherent statistical characteristics and transformation measures of all existing public key cryptographic algorithms makes them not suitable choice for next generation security system. In cryptography, the encryption process secures the information by converting the input information into some other form which always comes with some unreadable characters. The process of data

hardware optimization on AES (Yicheng Chen et al. 2008, Mozaffari-Kermani and Arash Reyhani 2011) using various optimization methods like S-Box modification and simplified arithmetic cipher formulation for low complexity. Optimization techniques introduced for complexity reduction affects the security levels and cipher conversion rate [15, 17].

Hamalainen et al. (2006) developed area efficient and energy level optimized AES cryptosystem using 8-bit input block size using 128-bit cipher key for improved security. Experimental results carried out using 130nm CMOS library showed improved data rate of 121 Mbps with operating frequency of 153 MHz. As compared to all other state-of-the-art AES counterpart models the proposed 8-bit cryptosystem significantly maximize the throughput with least computational complexity overhead area [18].

Wong Ming et al. (2018) developed cost effective AES core for lightweight system with some intolerant security compromises. In most cases, these multipliers are readily available in modern FPGAs. Though conventional cipher avoids multiplication operations due to its high computational complexity the inclusion of this core in the proposed cipher class creates good quality cipher conversion with the least complexity overhead. Experimental results show highly resilient clone-resistant modules and the security level [7].

In Sovyn Yaroslav et al. (2019) evaluate the speed and memory requirements for various real time applications and associated resistance levels to all sorts of cipher attacks. Performance validation timing analysis and power analysis are used which ensures execution time as well and key Galois/counter mode operation is introduced for optimal implementation of GF (2128) for hardware architecture[6].

The optimization framework developed by Shanthi Rekha and Saravanan (2019) using folding based hardware sharing over AES core for low complexity and modified Substitution box for high speed of 1.053GHz operating frequency. To validate the performance metrics AES cryptosystem is integrated with an UART module and reasonable throughput and resource efficiency are noted down [5].

Sharafi Masoumeh et al. (2019) introduced a Modified Block Cipher based on a Chaotic (MBCC) algorithm using chaos theory to improve the security level against statistical and differential attacks with the least computational complexity overhead [4].

In general block cipher hardware architectures are optimized in numerous ways to cover a wide range of applications. Moreover, the flexibility of the AES always remains safe with biclique cryptanalysis irrespective of the optimization model incorporated within the core.

DhandaSumit Singh et al. (2020) developed lightweight crypto core schemes for IoT applications. And comprehensive analyzes were carried out over different types of light weight cryptosystem and associated performance tradeoff which is related to hash function variants and Elliptic Curve

Cryptography (ECC) measures. Based on the observations it is well proved that AES and ECC are the most adoptive crypto core system for lightweight cryptographic primitives [3].

In Sasdrich Pascal et al. (2020) developed optimal AES functional masking without causing any significant functional violation and latency problems. Here memory enabled masked Dual-Rail is introduced for security [2]. The strong non-interference characteristics of a nonlinear LMDPL gadget extends the probing model and evaluate complete cipher transformation within 10 cycles for AES-128 and 14 clock cycles for AES-256 operation in. finally for performance validation side-channel analysis performed using the Test Vector Leakage Assessment (TVLA) and its bivariate t-statistics are well proved the resistance level. In comparison with the conventional method [19-11] the proposed method maximize the data rate and overcome key leakage related problems using composite field and masking techniques.

3. PROPOSED ADVANCED ENCRYPTION STANDARD (AES)

The Advanced Encryption Standard (AES) is one of the prominent crypto cores that follows a symmetric key approach and offers better security. In recent times it is less vulnerable to brute force attack. The AES crypto core comprises four basic functional blocks namely Sub Bytes, Shift Rows, Mix Columns and Add Round Key to transform input plaintext into cipher text. As compared to other transformation s box plays vital role in both confusion as well as diffusion metrics. The dynamic composite field S box is included for the addition of inner stage pipelining and bit-level masking to maximize the data rate and to overcome key leakages related problems, respectively.

3.1 Dynamic Substitution Byte Transformation Model

The In LUT based sub byte transformation and its inverse models are formulated using pre-computed values. This is one of the most common S-Box for the Sub Byte operation and used ROM based lookup table to store the values. In LUT based S-Box implementation for, 256 values are pre computed and stored in dedicated memory elements and accessed directly through address bus. However, this memory element based approaches causes notable path delay overhead due to access time for read operation. Implementation of S-Box through memory elements is expensive in nature and also leads power consumption overhead.

To overcome the limitations of LUT based S-Box implementation using combinational logic offers significant complexity reduction. In addition to this, dynamic composite field based [7] approach can be pipelined for maximizing the operating frequency.

S-Box: Multiplicative Inverse of GF (28) => Affine Transformation (AT).

Inverse S-Box: Inverse Affine Transformation (AT-1) => Multiplicative Inverse of GF (28).

The vector A denotes the multiplicative inverse of the each input byte from the state array matrix (4x4) formulated for given input text. The multiplicative inversion operation is common for both types of transformation and resource can be shared and MUX based selection line is allows two separate operations as shown in *figure-1*.

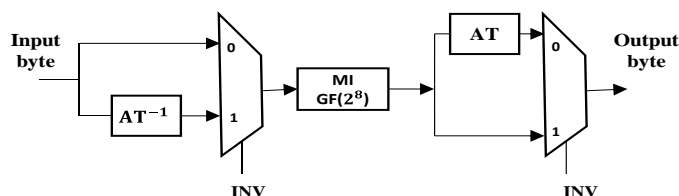


Figure 1: S-Box/Inv S-Box implementation using GF (28)

3.1.1. S-box Hierarchical Model

The basic construction of the multiplicative inverse block comprise of composite field arithmetic units as shown in *figure-2*. For S-Box transformation the multiplicative inversion of the input byte is forwarded to affine transformation which is following matrix transformation as given in *Equation (1)*:

$$\text{AT}(\mathbf{a}) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_7 \\ a_6 \\ a_5 \\ a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \quad (1)$$

As shown in *figure-2* the hardware translation of whole inverse block comprise of logic gates which consume lesser area as compared to its counterpart LUT based S-Box implementation and also shows superior path delay optimization as well.

3.1.2. Multiplicative Inversion

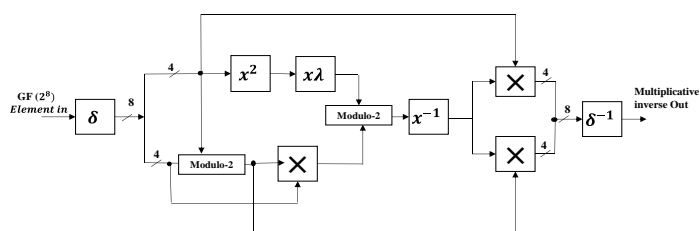


Figure 2: Multiplicative inverse block

3.2. Pipeline Architecture for Hybrid AES

The critical path delay analysis is carried out over proposed hybrid cryptosystems with associated key expansion and key stream blocks AES ciphers. The inner stage pipeline technique is used to reduce the path delay accumulation during data propagation. The key expansion and key stream generation blocks are generates two bytes for each clock cycle. The actual data processing and double swap operation are begins at Stage 1 and used pipeline registers to regulate the read-after-write operations during the swap operations. The values are read

from the pipelining registers immediately after the AES S-box computation and rotation. And modulo operations are used as post computation for key based transformation. Prior to this transformation key generation blocks are used to convert the input key into cipher using hierarchical nonlinear mapping functions which comprise of S-Box followed by successive accumulation process. Four hardware units are used to carry out for mention transformation model for improved parallel computation.

3.3. Bit Level Masking in AES

During Flip Flop masking, design allows to modify the information at every clock cycles during data propagation. To maximize the data flow controllability and reduces the observability these masking is enabled in s box transformation. Since s box is used for both encryption as well as key generation phase. The inclusion of masking, it becomes more difficult for others to explore the transformation involved in AES. As compared to conventional scan Flip Flop, masking requires only one extra modulo -2 operation and inverter to switching the logic as shown in *Table 1*. The masking is enabled in encryption side and by decryption side by knowing how to disable the mask FF externally data can be decrypted.

Table 1. Conventional FF vs. bit level mask FF

Normal Scan D FF	Bit level mask enabled D FF

FF loads data from the logic via DI while SE=0, with D being the logic's output. Because the additional inverter and XOR gate are added along the scan path, they have no effect on the design's time. While SE=1, FF's content is XORed with SI and shifted out to the next FF. As a result, hackers will have a tough time determining the relationship between the captured response and the scan-out.

4. RESULTS AND DISCUSSION

4.1 Simulation Results

In order to validate the importance of randomized mask bit generation process and to validate its influence in crypto system during cipher conversion process AES crypto system is simulated using exhaustive test bench input stimulus as shown in *figure-3* which can cover various stages of data propagation.

The potential benefits of cipher key generation and its performance efficiency in terms of transformation levels are proved for both numerical and character input as shown below.

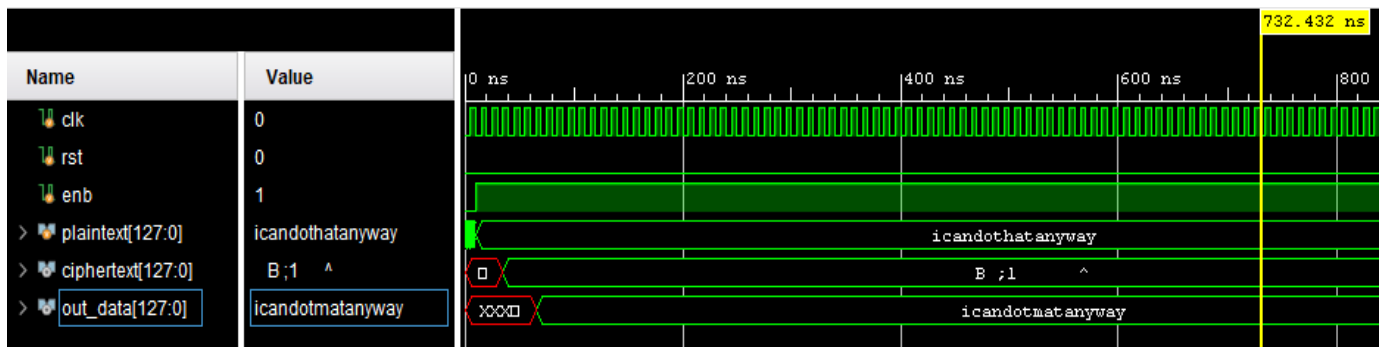


Figure 3: Encrypted and Decrypted Plain Text

3.1. Hardware Synthesis Results

In this section, the performance validation is carried based on comparison of pipelined composite field sub byte transformation over existing benchmark s box LUT-based AES core and proved the metrics of parallel sub pipelined AES both in terms of high security and path delay optimization level. The proposed AES core is designed using Verilog hardware description language (HDL) which is

synthesized and RTL Schematic is shown in *figure-4*, simulated and implemented on Vivado and targeted on Artix-7 Basys3 board for performance comparison is shown in Table 2. The primary objective goal of the high-performance crypto core is validated and associated computational complexity reduction is proved from the synthesis results. The composite S-Box model offers some significant energy efficiency due to its memory-less multiplicative inverse operations.

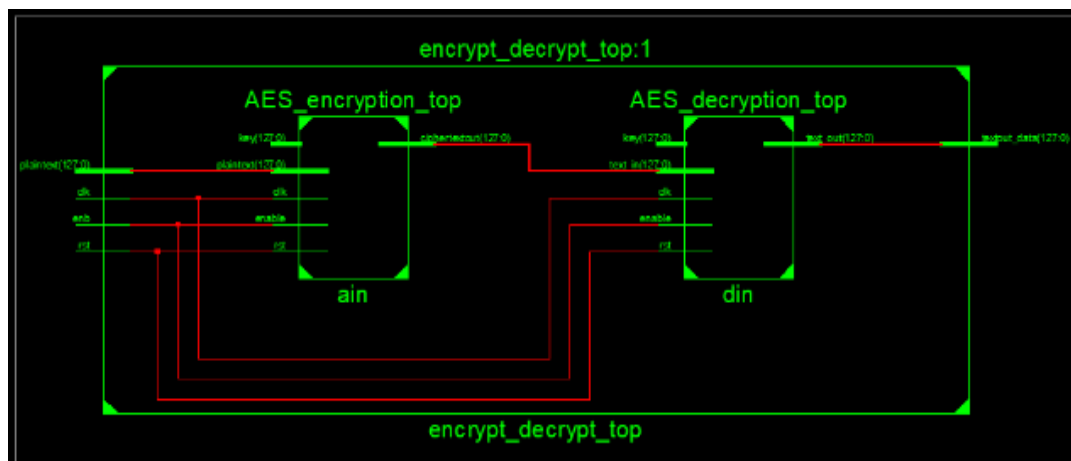


Figure 4: Encryption and Decryption RTL Schematic

Table 2. Performance comparisons of S-box

Parameter	AES LUT Based	AES Composite Based	AES Masking	AES Inner Stage Pipelining (Proposed)
Area (Slice LUTs)	40	83	58	52
Min Delay (ns)	0.489	1.974	0.534	0.370
Dynamic Power (W)	7.974	5.597	13.531	9.401
Throughput (Gbps)	43.6	10.8	39.9	57.65

4.3. Performance Calculation

The hybrid parallel sub-pipeline architecture is not only offers high speed also provides improved lifetime of the cipher key. In this cryptosystem 128 bit input text is decomposed into four blocks for parallel computation. Throughput rate is evaluated based in its operating speed in terms of maximum possible operating frequency at which the encrypt/decrypt module can operate during path delay measures as follows:

$$\begin{aligned}
 \text{Throughput} &= \text{Number of bits processed} / \text{cycle} \times F_{\text{max}} \\
 &= 128/6 \times 1/T (\text{delay}) \\
 &= 128/6 \times 1/0.370\text{ns} \\
 &= 57.65\text{Gbps}
 \end{aligned}$$

The experimental results presented in *Table 2*, it is proved that though the proposed hybrid AES core achieves maximized operating frequency due to the inclusion of parallel-processing units and the overall attainable throughput is also maximized with pipelined mechanism which is outperformed all other competitive optimization models proposed for AES core. Result also illustrates the difference in design complexity for proposed S-Box optimization and parallel processing model over architecture level optimization. The reduced arithmetic complexity, the effective implementation of the AES model also benefits with improved throughput rate without using any parallel array and pipelining mechanism.

4.4. FPGA Implementation

To validate the performance metrics associated with effective hardware synthesis the proposed AES core is implemented on Basys3 Board for verifying Design. The changes in hardware architecture for parallel inner-pipeline processing are not affecting the AES core encryption process. 128 bits of input

text is applied and encrypted cipher text and decrypted plain text is shown in *figure-5*. By using masking flip flop scheme the observability and controllability are reduced and each and every bit is masked as shown in *figure-6*. Finally, complete hardware setup is shown in *figure-7*.

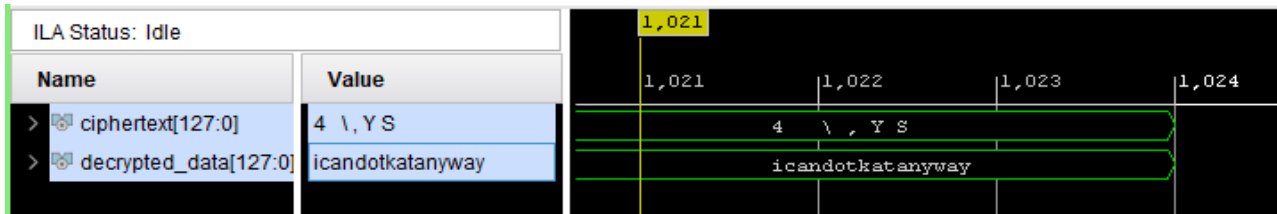


Figure 5: FPGA Implementation of Encrypted and Decrypted Plain Text

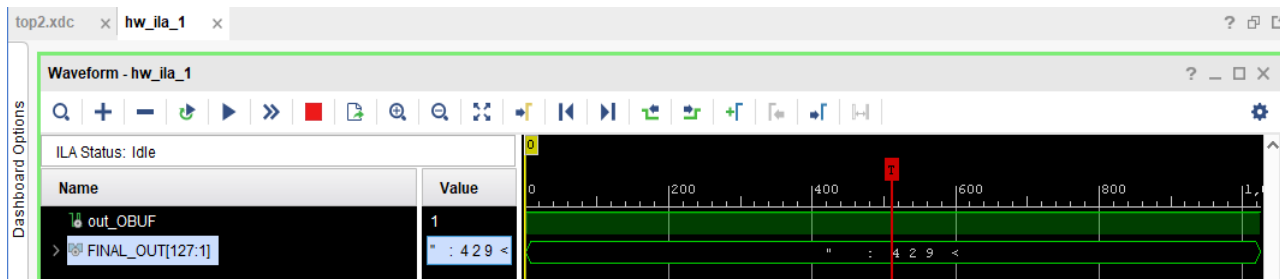


Figure 6: FPGA Implementation of masked AES

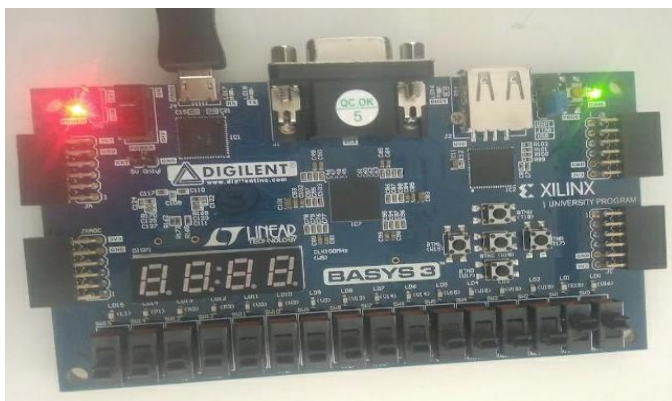


Figure 7: Basys3 Hardware connected to PC

5. CONCLUSION

A novel parallel sub pipelined AES based hardware optimized crypto system model is proposed. The composite field arithmetic are used to explore the potential benefits of inner stage pipelined optimal S-Box over conventional LUT S-Box. This model has been synthesized using FPGA hardware synthesis and the experimental results proved that the proposed model outperforms all other AES models. The bit-level masking in the AES model can able to overcome key leakages problems that exist in the conventional AES model and its FPGA implementation shows the applicability of the proposed high-performance AES cryptosystem in real-time applications.

REFERENCES

- [1] M. Qasaimeh, R.S. Al-Qassas and M. Ababneh, "Software Design and Experimental Evaluation of a Reduced AES for IoT Applications", *Future Internet*, vol. 13, no. 11, 2021.
- [2] P. Sasdrich, B. Bilgin, M. Hutter and M.E. Marson, "Low-latency hardware masking with application to AES", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 300-326, 2020.
- [3] S.S. Dhanda, B. Singh and P. Jindal, "Lightweight cryptography: a solution to secure IoT", *Wireless Personal Communications*, vol. 112, no. 3, pp. 1947-1980, 2020.
- [4] M. Sharafi, F. Fotouhi-Ghazvini, M. Shirali and M. Ghassemian, "A low power cryptography solution based on chaos theory in wireless sensor nodes", *IEEE Access*, vol. 7, pp. 8737-8753, 2019.
- [5] S. Shanthi Rekha and P. Saravanan, "Low-cost AES-128 implementation for edge devices in IoT applications", *Journal of Circuits, Systems and Computers*, vol. 28, no. 4, 2019.
- [6] Y. Sovyn, V. Khoma and M. Podpora, "Comparison of three CPU-core families for IoT applications in terms of security and performance of AES-GCM", *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 339-348, 2019.
- [7] M.M. Wong, M.D. Wong, C. Zhang and I. Hijazin, "Circuit and system design for optimal lightweight AES encryption on FPGA", *IAENG International Journal of Computer Science*, vol. 45, no. 1, pp. 52-62, 2018.
- [8] D.H. Bui, D. Puschini, S. Bacles-Min, E. Beigné and X.T. Tran, "AES datapath optimization strategies for low-power low-energy multisecurity-level internet-of-things applications", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3281-3290, 2017.
- [9] S. Adamovic, M. Milosavljevic, M. Veinovic, M. Sarac and A. Jevremovic, "Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics", *IET Biometrics*, vol. 6, no. 2, pp. 89-96, 2017.
- [10] A.A. Pammu, K.S. Chong, W.G. Ho and B.H. Gwee, "Interceptive side channel attack on AES-128 wireless communications for IoT applications", In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pp. 650-653, 2016.

- [11] D. Umesh and K. Ramesh, "Robust Scan Flip Flop Technique for Secured Advanced Encryption Standard", International Journal of Innovative Trends and Emerging Technologies, 1, no. Special Issue 2, 2015.
- [12] N.D. Parmar and P. Kadam, Pipelined implementation of dynamic Rijndael S-box. International Journal of Computer Applications vol. 111, no. 10, 2015.
- [13] Ali and F.A. Khan, "Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications", EURASIP Journal on Wireless Communications and Networking vol. 2013, no. 1, pp. 1-19, 2013.
- [14] M. Al Ameen, J. Liu and K. Kwak, Security and privacy issues in wireless sensor networks for healthcare applications. Journal of medical systems, vol. 36, no. 1, pp. 93-101, 2012.
- [15] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Efficient and high-performance parallel hardware architectures for the AES-GCM", IEEE Transactions on Computers, vol. 61, no. 8, pp. 1165-1178, 2011.
- [16] Algreto-Badillo, C. Feregrino-Urbe, R. Cumplido and M. Morales-Sandoval, "Efficient hardware architecture for the AES-CCM protocol of the IEEE 802.11 i standard. Computers & Electrical Engineering, vol. 36, no. 3, pp. 565-577, 2010.
- [17] C. Yicheng, Z. Xuecheng, L. Zhenglin, H. Yu and Z. Zhaoxia, "Energy-efficient and security-optimized AES hardware design for ubiquitous computing", Journal of Systems Engineering and Electronics, vol. 19, no. 4, pp. 652-658, 2008.
- [18] P. Hamalainen, T. Alho, M. Hannikainen and T.D. Hamalainen, "Design and implementation of low-area and low-power AES encryption hardware core". In 9th EUROMICRO conference on digital system design (DSD'06), pp. 577-583, 2006.
- [19] X. Zhang and K.K. Parhi, "High-speed VLSI architectures for the AES algorithm", IEEE transactions on very large scale integration (VLSI) systems, vol. 12, no. 9, pp. 957-967, 2004.
- [20] C.F. Grecas, S.I. Maniatis and I.S. Venieris, "Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure integration", Mobile Networks and Applications, vol. 8, no. 2, pp. 145-150.
- [21] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes". In Annual international cryptology conference, pp. 537-554, 1999.
- [22] Pradeep S (2014), Design and FPGA Implementation of Image Compression Based Fuzzy Technique. IJEER 2(2), 1-4. DOI: 10.37391/IJEER.020201. <http://ijeer.forexjournal.co.in/archive/volume-2/ijeer-020201.php>



© 2022 by the B. Murali Krishna, Chella Santhosh, S.K. Khasimbee. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).