Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 2, 2020

Review Article

A NOVEL APPROCH TO MODIFIED ADVANCED ENCRYPTION STANDARD ALGORITHM

[1]N. Siddaiah, [2]Arjuna Moduli, [3]K. Bhargavram, [4]P. Murali Krishna, [5]B. Rakesh, [6]G. V. Ganesh

Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

Received: 13.11.2019 *Revised: 18.12.2019* *Accepted: 21.01.2020*

Abstract

The Internet of Things (IoT) is a self-ruling framework for web availability, furnished with sensors, applications, PCs and system collaboration to associate using an obscure remote system for data trade. As of late, IoT systems command the world by having different capacities and constant correspondence data. Other than the powerful highlights of IoT gadgets, they are staggeringly battery driven, conservative and convoluted and face numerous snags due to perilous media. Albeit numerous issues exist, the issue of vitality is currently turning into the most significant concern. Advancement of vitality utilization calculations was not straightforwardly considered. A few calculations at that point center around the equipment district to essentially alleviate and streamline it in security issues. However, because of the ongoing coming of IoT gadgets, the principle issue is to keep up humble security and lower control utilization rates. We present MAES, a lightweight form that fulfills the determination, with the Advanced Encryption Standard (AES). In planning a crisp condition, a fresh1-dimensional substitution box is proposed to develop a square framework in the MAES phase of fondness preparing. The exhibition pace of bundle transmission is around MAES 18.35%, recommending that for asset compelled conditions MAES utilizes less power than AES.

Keywords: AES, IoT, Energy Consumption, Resource Constraint Environments (RCEs), TelosB , Cryptography.

DOI: http://dx.doi.org/10.31838/jcr.07.02.115

INTRODUCTION

The Internet of Things (IoT) is the following web development that profoundly impacts our everyday life. IoT is the Internet development that connections practically the entirety of the globe. Material and real things from family unit items to business [1] are a piece of this. Accordingly, these "objects" which are associated with the Web will act or decide dependent on data assembled from the Internet with or without human communication. Along these lines, they screen the Internet utilizing various sensors with constant data. IoT manages parts of system limitation including sensor hubs, RFID labels, and so forth. Such modules have poor handling power, negligible space and vitality assets and physical catch opposition. We likewise convey through an unbound portable channel [2] and impart continuously data by means of an inconsistent remote press. Secrecy, encryption, freshness of data and culmination might be critical in specific applications. Information encryption is thusly zMd. The relating creator is Abdul Hamid. A major concern [3]. Being a major business. In any case, in view of the segments ' asset imperatives, transient security will fulfill request [4]. Asset limit implies low battery limit, diminished processor recurrence, and so forth. Crypting information utilizing uniform cryptographic calculations will devour more vitality, which lessens the segments ' lives significantly. The plan and execution of security essential frameworks fitted with profoundly limitation gadgets is joined by two key approaches[5]. Next, new lightweight cryptosystems are being made. For instance, [6-12] are a couple of lightweight cryptographic calculations proposed as of late. Moreover, to permit a lightweight update of the current standard cryptosystem. The Advanced Encryption Standard Algorithm (AES) [13], SHA-256[14] and so on.) might be refreshed as potential instances of the subsequent methodology. AES is viewed as one of the quickest and best calculations as far as security and execution unpredictability. Despite the fact that the mystery key dissemination stays a basic issue like other symmetric encryption algorithms [15]. A lot of PC preparing should be done, devouring gigantic battery control, by and by to scramble or decode a solitary square (128-piece) of information. As IoT parts have a confined asset limit, a depletion of such segments will bring about a gigantic power utilization. Investigates comparable work uncover that Substitution Layer in the round-based structure is the most vitality effective segment of AES. As for asset packed IoT vitality utilization we suggest MAES, a lightweight AES rendition, which decreases AES ' Substitution Box (S-Box) calculation. They propose a 1-Dimensional Substitution Box (S-Box) which is worked by building up another recipe to make a square network in the fondness venture of the MAES change. We use MTS400 as a sensor board together with a microcontroller, TI MSP430 and a CC2420 radio processor, to consolidate both unique AES and MAES calculations on Tiny OS 2.1.2 stage in Telos B sensor bit. Upon survey, we have discovered that MAES is great regarding bundle transmission and inactivity, individually, at generally 18.35% of AES and 23.983 milliseconds, separately. Section II gives a layout of related exercises about essentialness use levels of IoT systems. The remainder of the journal is sorted out as pursues.Section III contains the primer data on the AES square ciffer. Area IV clarifies the insights regarding strategies used to lessen vitality utilization of IoT gadgets by modification of the substitution box (SBox) of the AES with an age cycle from Rijndael S-Box. Area V clarifies the exhibition investigation.applications for data security[17].

LITERATURE SURVEY

A few research ventures have been embraced as of late, with noteworthy accomplishments of asset requirement conditions (RCEs) achieved by an assortment of regarded researchers. In any case, a large portion of them are equipment arranged and have a little territory and low power. Will give you how the square figure is applied, Bogdanov et. to the. 5] examined how a switch in (a) S-Box/Mix Cloumn structure, (b) the clock cycle speed and (c) the model unrolling would impact the vitality utilization. The count of vitality utilization by a few lightweight calculations approves the model. The recommended structure is diverged from the different degrees of moving utilizing insights. Likewise, it has demonstrated that absolute vitality utilization in one circuit has a quadratic association with the pace of unrolling during encryption, and that the most vitality serious part is a two-round, unrolled, Substitute Box (S Box). what's more, Feldhofer. Al. [16] and Moradi, etc. AS [17] and its key changes, (for example, S-Box) have been recommended for

the use of low region and low power. For the most part equipment arranged, all advancements. [16] The structure depends on the 8-piece information way that spreads 3400 Gate Equivalents (GE) and [17] a half and half information way that takes 2400 GE. [18] exhibiting that 740 pj of vitality for every validation is utilized. also, Kerckhof. al. [19] presented a relative investigation of various calculations concentrated on area, execution, power and vitality, just as condition of - the-craftsmanship control utilization cutting systems. furthermore, Batina. al. [20] broke down and thought about numerous as of late created lightweight square figures regarding zone, power and vitality utilization in light of potential upgrades for non-straight change with the AES algorithm.The vitality utilization aftereffects of different plan decisions, in any case, for example, information way length, serialization amount and spatial advancement impacts, are not considered in any of the tasks. Banik and. Al. [21] estimated the power utilization of 7 lightweight square figures conveyed in reconfigurable gadgets (FPGA) and talked about just because the subject of vitality proficiency. Our outcomes indicated that Present is the most vitality effective and fastest2-round unrolling calculation. The equipment and configuration process design decision of appropriate cryptographic calculations is a significant assignment. Kong et to coordinate the analysts and to move them. al.[22] investigated current asset controlled cryptographic arrangements. (RCEs). Creators have deliberately inspected the equipment, programming, improvement and security example of RCE's from other writing. Great and. to the [23] recommended two supplanting boards with a XOR activity and an ideal transformation, with the principal S-Box being the Rijndael S-Box, and the second, the S-Box which replaces the Mix Columns activity of the first AES. Considering reenactment examination, the improved AES calculation with a few S-Boxes shows a superior speed than the first chip. Kawle and. also, to the[24-25] likewise recommended a modificated AES to decrease the product overhead for the underlying AES calculation, utilizing condition of - the-workmanship innovations for encoding enormous size documents, for example, interactive media information.

EXISTING SYSTEM

The AES balanced key grouping, gave in December 2001 by the National Institute of Standards and Technology, is the Advanced Encryption Standard. It is a square figure not from Feistel which scrambles and unscrambles a 128-piece fixed information square. Three distinct lengths are accessible. The verification comprises of 10 preparing adjusts for 128-piece keys, 12 handling adjusts for 192-piece keys and 14 handling adjusts for 256-piece keys. Each round comprises of a few phases. AES conducts a few rounds. An information obstruct starting with one point then onto the next is changed over. The data square is known as a state when each point. Except for the last, each balance conveys four invertible changes. Three changes were rendered during the last round with the exception of the phase of the mix segments.The AES cipher structure is shown in Figure 1.

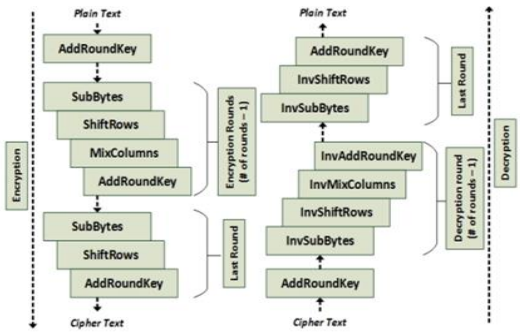


Fig. 1. General design of AES encryption and decryption

The primary transformation, subbytes, is utilized on the confirmation site: (1) Substitute bytes: It is a non-straight byte substitution, which follows up on a substitution table (S-Box) autonomously on every byte of the state. The subsequent qualities from the hunt table supplant each of the 16 bytes of the framework. The Inv Sub Bytes is utilized for decoding. Inv Sub Bits table is supplanted by framework bits.The Sub Bytes operation is shown in Figure 2.

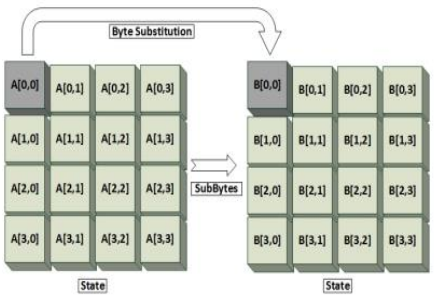


Fig. 2. SubBytes

2) Shift Rows: State bytes will be moved in each line during encryption. The procedure is called Shift Rows. The quantity of changes relies upon the state lattice push number (0, 1, 2 or 3). The line 0 bytes will not be moved and push 1, 2, 3 will be moved to 1, 2, 3 bytes will in this way be set as pursues.The Change Rows operation is shown in Figure 3.

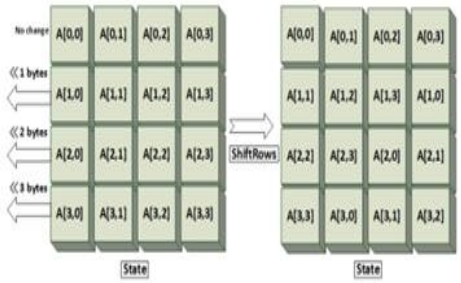


Fig. 3. ShiftRows

3) Mix Column: Conversion of Mix Columns capacities at the degree of the section. Every section of the framework is transformed into another segment. Truth be told, change is the grid duplication by a steady square network of a state segment. In the Galois field (limited field), every scientific activity are done. Rather than tally, the bytes are spoken to as polynoms.The Mix Columns process is shown in Figure 4.

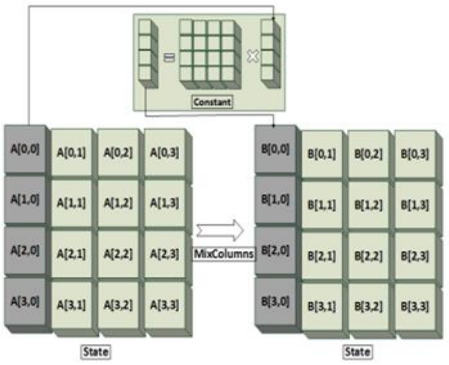


Fig. 4. MixColumns

4) Add Round Key: Add Round Key is one segment for every round. In this regard, it is near Mix Columns. Add Round Key to every section lattice, embeddings a round catchphrase. In the Add Round Key stage the option of the framework is performed. The Add Round Key activity is appeared in Figure 5. Encoding is done in all rounds aside from the last one, including sub bytes, move lines, switch segments and

addition round keys.

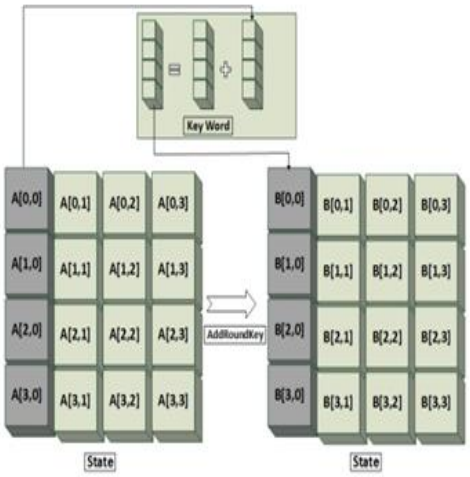


Fig. 5. AddRoundKey

In the last encryption arrangement, change Mix Columns isn't finished. Rather than the nine emphasess of Inverse Swap Rows, Inverse Sub Bytes, Inverse Add Round Key and Inverse Mix Column Conversion the unscrambling procedure essentially pursues a similar structure as the encryption. The last round is never again finished with the turn around blend tables.

MODIFIED ADVANCED ENCRYPTION STANDARD

As indicated by past research discoveries, S-Box and Mix segments have been the most vitality productive procedures of coding and decoding. We considered the Rijndael AES technique for delivering the S-Box. During the multiplicative switch and improved transformation forms in the underlying AES, the 16x 16 twofold measured query table contains. We offer another one-dimensional S-Box query table. A similar age cycle parallels that of the first.

In any case, expelling one full byte includes supplanting the S Box twice. The four bits of state byte are first supplanted, and the four different bits are supplanted by the S-Box. The Rijndael S-Box is a square lattice utilized by the Rijndael figure. A: Rijndael S-Box age process The S-Box is a determination table.

The multiplicative backwards for a given number in GF(28) is characterized and afterward changed with a relative change by the multiplicative contrarily.

1) Multiplicative Inversal Phase: The information byte is turned around by expelling a number from the multiplicative switch table in multiplicative invert stage

2) Affine Transformation: the two most significant elements of relative change are the decision of the unchangeable polynomial and the predetermined piece. In Rijndael AES the irreductible polynomial is utilized as x8 + x4+ x3++ 1, and a particular byte is chosen for the consistent segment framework 0x63. Two tasks comprise in principle of the relative change. Initially, the augmentation of a 8x8 square lattice and second, the expansion of a 8x1 consistent grid section. The 8x8 square lattice is built with the accompanying

d_i=b_i⊕b_((i+4)%8)⊕b_((i+5)%8)⊕b_((i+6)%8)⊕b_((i+7)%8)⊕C_i… … ..(1)

bi= ith bit of multiplicative opposite of information byte..(2)

Ci=ith bit of a uniquely planned byte… (3)

Figure 6 shows the generation process of the original AES replacement box (S-Box).

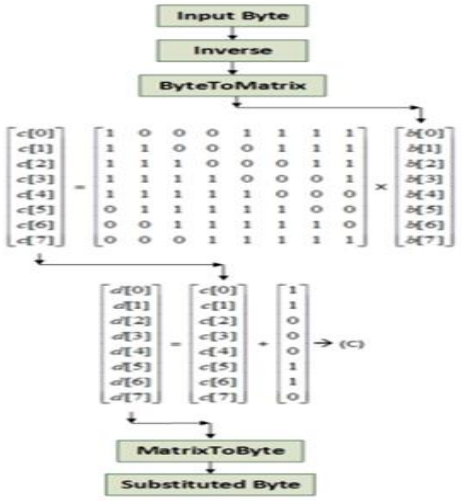


Fig. 6. Original S-Box generation process

B. Refreshed age of AES S-Box Our refreshed AES S-Box age process pursues the first AES building convention. In choosing the unchangeable polynomial and the exceptionally assigned piece, the entire procedure is diverse as it were. 1) Inverse Multiplicative Table: All number juggling tasks are performed in the Rijndael AES crosswise over Galois Field (28). The Galois Field (24) is considered in our examination. The number is x4 + x 1 + 1 x4 + x 3 + x 2 + 1 of the Grade 4 final polynomials.

The decision of the unchangeable polynomial relies upon all the produced estimations of the multiplicative reverse table and substitution set. We picked x4+x+1 as a final polynomial for our testing reason; be that as it may, we may pick any of the previously mentioned unchangeable polynomials. The 1-dimensional increased backwards table is developed utilizing the summed up Euclidean calculation. The multiplicative inverse table of the algorithm proposed is shown in Figure 7.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	9	E	D	A	7	6	F	2	C	5	A	4	3	8

Fig. 7. Multiplicative inverse table

2) Affine Transformation: There are additionally two phases to this related change process. To start with, increase of a 4x4 square framework and second, steady expansion of a 4x1 section lattice. The 4x4 square framework is rendered by condition 1 and condition 2 is di: d_i=b_i⊕b_((i+2)%4)⊕b_((i+3)%4)⊕C_i… … ..(4) bi= ith bit of multiplicative reverse of information byte ,Ci=ith bit of a uniquely structured byte which is hexadecimal of 3,8,10,13,15 as they don't create any fixed focuses… (5)

The consistent quality assortment is to some degree unsteady. Since we decide in the GF[24] the estimation of the steady section framework is somewhere in the range of 0X00 and 0x0F we can pick just five qualities, in light of the fact that after change such qualities don't create a fixed point. The fixed guide alludes toward the yield esteem age comparative with the information esteem. The generation of the proposed MAES is shown in Figure 8.

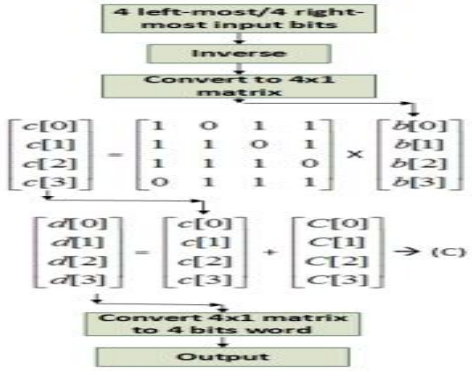


Fig. 8. Proposed MAES S-Box generation process

EXTENSION:

Various S-boxes and reverse S-boxes are shown below from Figure 9 through 13 in the case of the various values of constant value C:

Case-1: When C = 0x03

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3	4	F	B	2	1	7	0	C	D	5	9	6	E	A	8

Inverse S-box:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
7	5	4	0	1	A	C	6	F	B	E	3	8	9	D	2

Fig. 9. Case-1: When C = 0x03

Case-2: When C = 0x08

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
8	F	4	0	9	A	C	B	7	6	E	2	D	5	1	3

Inverse S-box:

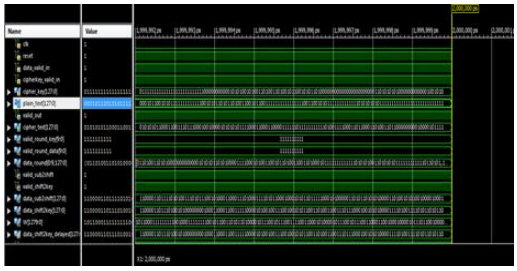
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3	E	B	F	2	D	9	8	0	4	5	7	6	C	A	1

Fig. 10. Case-2: When C = 0x08

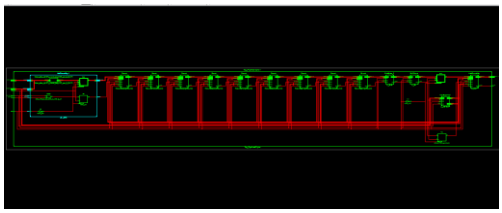
To get energy efficiency of modified encryption algorithm.

SIMULATION RESULTS

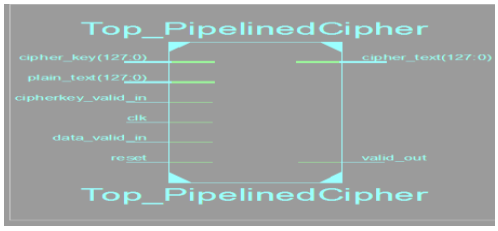
The VERILOG HDL appears in the I simulator and Xilinx ISE is a FPGA synthesis software. Veerilog HDL incorporates many parts of the proposed scheme.



RTLSCHEMATIC:



TECHNOLOGYSCHEMATIC:



DESIGNSUMMARY:

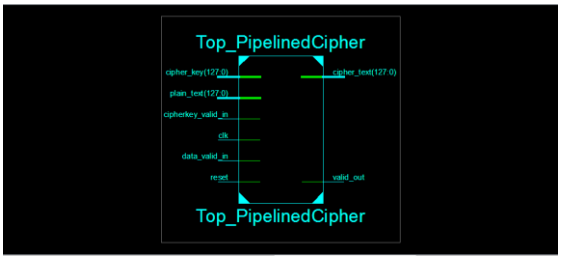
Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slice Registers	10769	385600	2%
Number of Slice LUTs	9403	192800	4%
Number of fully used LUT-FF pairs	5251	14921	35%
Number of bonded IOBs	389	600	64%
Number of BUFG/BUFGCTRLs	2	32	6%

TIMING REPORT:

```
Timing Summary:
---------------
Speed Grade: -3

   Minimum period: 1.439ns (Maximum Frequency: 695.120MHz)
   Minimum input arrival time before clock: 0.925ns
   Maximum output required time after clock: 0.515ns
   Maximum combinational path delay: No path found
```

Extension result:




```
Timing Summary:
---------------
Speed Grade: -3

   Minimum period: 1.006ns (Maximum Frequency: 994.233MHz)
   Minimum input arrival time before clock: 0.925ns
   Maximum output required time after clock: 0.515ns
   Maximum combinational path delay: No path found

Timing Details:
---------------
All values displayed in nanoseconds (ns)

--------------------------------------------------------------------------------
Timing constraint: Default period analysis for Clock 'clk'
  Clock period: 1.006ns (frequency: 994.233MHz)
  Total number of paths / destination ports: 38265 / 20943
--------------------------------------------------------------------------------
Delay:               1.006ns (Levels of Logic = 2)
  Source:            ROUND[0].U_ROUND/U_SH/data_out_119 (FF)
  Destination:       ROUND[0].U_ROUND/U_MIX/data_out_123 (FF)
  Source Clock:      clk rising
  Destination Clock: clk rising
```

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slice Registers	10769	385600	2%
Number of Slice LUTs	5803	192800	3%
Number of fully used LUT-FF pairs	5451	11121	49%
Number of bonded IOBs	389	600	64%
Number of BUFG/BUFGCTRLs	2	32	6%

CONCLUSION

An altered variant of the AES for asset compelled conditions is given in this article. Another Substitution Box is presented which works on a solitary, relative change recipe through the Galois Field (24). MAES is recognized by expanding the battery life of low-fueled gadgets by lessening vitality utilization. This methodology shows 18.35% productivity in transmission by means of the proposed MAES to the sink hub of the scrambled bundles and an expanded number of parcels transmitted. Along these lines, inertness is 29,983 milliseconds. For expansion, the wellbeing question and the unpredictability of room will be routed to make the proposed alteration progressively applicable. Along these lines, during the transmission of encoded information, we

intend to examine the multipathway directing frameworkIn request to accomplish an equivalent proficiency as far as number of bundles transmission and inertness, we will additionally execute open key cryptography, specifically elliptic-bend (ECC), with better insurance.

REFERENCES:

1. Narendra Babu T., Noorbasha F., Krishna S., Sai Charan K., Sai Kalyan R.S.V.S., FPGA implementation of cryptographic system using BODMAS sequence of operations ,2016, ARPN Journal of Engineering and Applied Sciences, Vol: 11, Issue: 19, pp: 11475 - 11479, ISSN 18196608.
2. Murali Krishna B., Rakesh Chowdary G., Chandra Vardhan G., Siva Ram K., Sai Kishore P., Madhumati G.L., Khan H., FPGA based wireless electronic security system with sensor interface through GSM ,2016, Journal of Theoretical and Applied Information Technology, Vol: 89, Issue: 2, pp: 489 - 494, ISSN 19928645
3. Charan N.S., Kishore K.H., Recognization of delay faults in cluster-based FPGA using BIST ,2016, Indian Journal of Science and Technology, Vol: 9, Issue: 28, ISSN 9746846
4. Charan N.S., Kishore K.H., Recognization of delay faults in cluster-based FPGA using BIST ,2016, Indian Journal of Science and Technology, Vol: 9, Issue: 28, ISSN 9746846
5. Paradhasaradhi D., Satya Priya K., Sabarish K., Harish P., Narasimharao G.V., Study and analysis of CMOS carry look ahead adder with leakage power reduction approaches ,2016, Indian Journal of Science and Technology, Vol: 9, Issue: 17, ISSN 9746846
6. Murali Krishna B., Siva Kumar M., Rajesh J., Inthiyaz S., Mounica J., Bhavani M., Adidela C.N., FPGA implementation by using XBee transceiver ,2016, Indian Journal of Science and Technology, Vol: 9, Issue: 17, ISSN 9746846
7. Narendra Babu T., Noorbasha F., Gunnam L.C., Implementation of high security cryptographic system with improved error correction and detection rate using FPGA ,2016, International Journal of Electrical and Computer Engineering, Vol: 6, Issue: 2, pp: 602 - 610, ISSN 20888708
8. Neelima U., Noorbasha F., Data encryption and decryption using reed-muller techniques ,2016, International Journal of Engineering and Technology, Vol: 8, Issue: 1, pp: 83 - 91, ISSN 23198613
9. Kumar P.K., Rao P.P., Kakarla H.K., Optimal design of reversible parity preserving new Full adder / Full subtractor,2017 Proceedings of 2017 11th International Conference on Intelligent Systems and Control, ISCO 2017, pp: 368-373, DOI: 10.1109/ISCO.2017.7856019, ISBN: 9.78151E+12
10. Noorbasha F., Manasa M., Gouthami R.T., Sruthi S., Priya D.H., Prashanth N., Rahman M.Z.U., FPGA implementation of cryptographic systems for symmetric encryption,2017 Journal of Theoretical and Applied Information Technology, Vol:95, issue:9, pp: 2038-2045, ISSN: 19928645
11. Murali Krishna B., Madhumati G.L., Khan H., Stochastic key generation mechanism in cryptography applications through partial reconfiguration,2017 Journal of Advanced Research in Dynamical and Control Systems, Vol:9, issue: Special Issue 12, pp: 1566-1586, ISSN: 1943023X.
12. Yadlapati A., Hari Kishore K. .," System level verification of advanced extensible interface protocol using verilog HDL ", 2018, Lecture Notes in Electrical Engineering ,Vol: 471 ,Issue: ,pp: 581 to:: 588 ,DOI: 10.1007/978-981-10-7329-8_59 ,ISSN: 18761100 9.78981E+12
13. Anil Chowdary T., Durga Prasad M. .," A short paper on testability of a SoC ", 2018, International Journal of Engineering and Technology(UAE) ,Vol: 7 ,Issue: 1.5 Special Issue 5 ,pp: 77 to:: 83 ,DOI: ,ISSN: 2227524X
14. Ramakrishna P., Hari Kishore K. .," Design of an ultra low power cmos comparator for data converters ", 2018, International Journal of Engineering and Technology(UAE) ,Vol: 7 ,Issue: 1.5 ,pp: 230 to:: 233 ,DOI: ,ISSN: 2227524X.
15. Babu C.N., Naga Siva Sai P., Priyanka C., Hari Kishore K., Bindu Bhargavi M., Karthik K. .," Comparative analysis of high speed carry skip adders ", 2018, International Journal of Engineering and Technology(UAE) ,Vol: 7 ,Issue: 1.5 ,pp: 26 to:: 30 ,DOI: ,ISSN: 2227524X
16. 154 .Priyanka C., Manoj Kumar N., Sai Priya L., Vaishnavi B., Rama Krishna M. .," Low power and high speed GDI based convolution using Vedic multiplier ", 2018, International Journal of Engineering and Technology(UAE) ,Vol: 7 ,Issue: 1.5 ,pp: 19 to:: 25 ,DOI: ,ISSN: 2227524X
17. 155 .Hari Kishore K., Durga Koteswara Rao K., Manvith G., Biswanth K., Alekhya P. .," Area, power and delay efficient 2-bit magnitude comparator using modified gdi technique in tanner 180nm technology ", 2018, International Journal of Engineering and Technology(UAE) ,Vol: 7 ,Issue: 1.5 Special Issue 5 ,pp: 90 to:: 96 ,DOI: ,ISSN: 2227524X
18. 156 .Noorbasha F., Hari Kishore K., Naveen T., Sai Anusha A., Manisha Y., Revathi K., Manasa M. .," Implementation of modified Feistel block cipher for OTP generation using Verilog HDL ", 2018, Progress In Electromagnetics Research M ,Vol: 63 ,Issue: ,pp: 163 to:: 173 ,DOI: ,ISSN: 19378726
19. Hussain S.N., Kishore K.H. .," Performance evaluation of heuristic algorithms in floor planning for ASIC design ", 2018, Journal of Advanced Research in Dynamical and Control Systems ,Vol: 10 ,Issue: 10 Special Issue ,pp: 92 to:: 97 ,DOI: ,ISSN: 1943023X
20. Murali Krishna B., Madhumati G.L., Khan H., "FPGA based pseudo random sequence generator using XOR/XNOR for communication cryptography and VLSI testing applications", International Journal of Innovative Technology and Exploring Engineering, ISSN:22783075, Vol No:8, Issue No:4, 2019, pp: 485 - 494.
21. N.Siddaiah, T.V.Aravind Swami, "Material optimization of the novel cantilever based RF MEMS switch for mobile communication" Transactions on Electrical and Electronic Materials, Springer publications, ISSN 1229-7607 Volume 20 Number 4,May,2019N.Siddaiah.et.al,"Design,simulation and analysis of U-shaped and rectangular MEMS based Trile coupled cantilevers",Journal of Scientific and Industrial research,Vol.76,April 2017,235-238
22. Nalluri Siddaiah, D.V.Rama koti Reddy, Y Bhavani Sankar, R.Anil Kumar, Hossein Pakdast, "Modeling and simulation of Triple coupled Cantilever sensor for mass sensing applications",International Journal of Electrical and computer Engineering(IJECE),vol.5,no.3,June 2015, pp.403~408,ISSN:2088-8708.
23. Nalluri Siddaiah,D.V.Rama koti Reddy,G.R.K Prasad,Hossein Pakdast, Patcha Satya Srinivas Babu, "Optical and Dielectric force gradient actuation schemes for Excitation of Triple coupled Micro cantilever sensor in mass sensing applications",ARPN Journal of Engineering and applied Sciences(JEAS), vol. 10, no. 8, May 2015,ISSN:1819-6608.
24. N. Siddaiah, et.al. "Performance analysis of cantilever-based bio-sensor for pathogen detection" International Journal of Pharmaceutical Research, 10(2), pp. 107-109,2018.
25. Siddaiah, N., Tentu, V.A.S., Rehman, M.D.Z, "Design, simulation and performance analysis of novel cantilever Rf-mems switch using serpentine meanders", International Journal of Engineering and Advanced Technology,Volume 8,issue 4,pg:1360-1366,April,2019