FPGA Design and Implementation of Modified AES Based Encryption and Decryption Algorithm

Fazal Noorbasha, Y.Divya, M.Poojitha, K.Navya, A.Bhavishya, K. Koteswara Rao, K Hari Kishore

Abstract: ***Advanced Encryption Standard (AES) is an endorsed cryptographic algorithm that can be utilized to secure electronic information. AES was replacing the old Data Encryption Standard (DES) with more security. The algorithm uses a combination of logical EX-OR operations, octet substitution with S-BOX, column rotations, row rotations, and a mix column. It was successful because it was easy to implement and could run in a reasonable amount of time on a regular computer. Field Programmable Gate Arrays (FPGA) offers a faster, increasingly adjustable arrangement. In this paper, another plan of AES that is triple key AES is proposed. This beats the powerlessness of static S-Boxes and furthermore single key and double key AES encryption conspire. Thus the triple key AES calculation is more grounded when contrasted with the both past cases and give greater security to the information, pictures and etc. Finally we tested this algorithm on Spartan 3E FPGA kit.***

Keywords: AES, FPGA, Static S-Box, Look up tables

I. INTRODUCTION

In nowadays utilization of computerized information trade is expanding step by step in each field.Data security is the key parameter to be taken care to prevent the loss of information and avoid cyber-crimes [1]. Data security assumes imperative job in putting away and transmitting the information. When we transmit interactive media information, for example, sound, video, pictures and so forth over the system, cryptography gives security. The cryptography is making sure of integrity, availability, identification, confidentiality, authentication of user. It can give security and privacy of data can be provided to the user [2]. As we manage Cryptography and Networking, the fundamental point is to accomplish the security of the information. Consequently, this paper shows "An Equivalent Security in Cryptosystem by Advance Encryption Standard Using FPGA".

Revised Manuscript Received on April 14, 2019.

Fazal Noorbasha, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
Y.Divya, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
M.Poojitha, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
K.Navya, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
A.Bhavishya, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
K. Koteswara Rao, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India
K Hari Kishore, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India

Propelled Encryption Standard (AES) is an affirmed cryptographic Algorithm that can be utilized to ensure electronic information. AES is a symmetrical calculation of encoding planned to supplant DES which had just demonstrated certain issues of security in the information Protection. The Advanced Encryption Standard can be modified in programming or worked with equipment. The operation of secure cipher is based upon the operations of confusion and diffusion [3]. Anyway Field Programmable Gate Arrays (FPGAs) offer a faster, progressively adjustable arrangement; consequently we utilized the FPGA with respect to usage reason. We show how an altered structure in these Hardware gadgets results in noteworthy improvement of the plan proficiency.This paper shows an execution assessment of chose symmetric encryption calculations. The chose calculations are AES, DES, RC6, Blowfish and RC2[4].With some highlighted features like high speed encryption rate, good protection to the data the block ciphers like Rijndael and RC6 algorithms are implemented[5][6].Encryption and decryption are time performance metric speeds while space performance metric is memory utilization [7]. Stream symmetric cipher Strumok is used to send stream of information [8] [9]. A few can be closed from the reenactment results. We proceed onward to examine about the ongoing alterations that have been done on the AES conspire and their shortcomings. AES comprises of 128 square lengths of bits and backings 128 bit, 192 bit and 256 bit key length bits. The 128 bit key is sorted out into state framework which measure of 4×4[10]. The calculation begins with starting change of state grid followed by nine cycles of rounds. A round comprises of four changes- byte substitution (subbytes), row shifting (shiftrows), mixing of sections (mixcolumns) and pursued by expansion of round key called (addroundkey). From every cycle, a round key is produced by the first key through key booking process. The final round comprises of subbytes, shiftrows and addroundkey change. Subbytes transformation is actualized utilizing S-Box [11]. The S-Box is a standout amongst the most tedious procedure since it is required in each round [12]. A changed Rijndael calculation and its usage utilizing fpga are given here. In this paper, an altered Rijndael calculation that performs encryption process through three ward stages is exhibited.

AES depends on rijndael calculation which is a symmetric square figure that forms fixed information of 128-piece squares [13]. It bolsters key sizes of 128, 192 and 256 bits

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

and comprises of 10, 12 or 14 cycle rounds, individually. In this paper we will concentrate on the 128-piece form with 10 rounds. Each round blends the information with a round key, which is created from the encryption key. Figure 1 delineates the encryption round tasks of general AES. The figure keeps up an inward, 4×4 grid of bytes alluded to as state, on which the activities are performed. At first, state is loaded up with the information square andxored with the encryption key [14]. Ordinary rounds comprise of tasks called subbytes, shiftrows, mixcolumns and addroundkey. Round key age (key extension) incorporates s-box substitutions, word pivots, and xor activities performed on the encryption key [15]. Contingent upon the security level required for the application, AES utilizes distinctive key lengths.

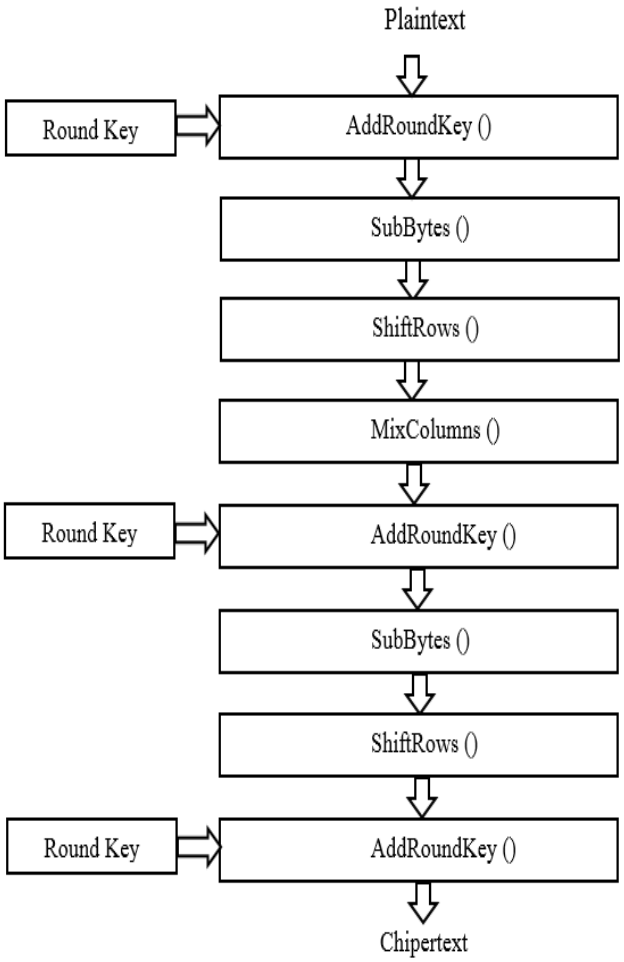

Fig. 1 AES Encryption Round Operation

II. PROPOSED AES METHOD

In the triple key AES calculation, we need to encode the 128 piece information. For these three keys are utilized separate of the 128 piece. Following figure 2 demonstrates the idea of triple key AES calculation. It comprises of a few squares which are utilized to do the encoding and disentangling of information. In this framework, 128 piece of information is given as a contribution alongside the three 128 piece keys. Each iteration cycle jumbles plain data with a round key. This round key is obtained from the cipher key and in decryption reverts the cycles of recurrence bringing about in part, a dissimilar data path. Figure 2 shows the steps involved in Triple Key AES algorithm.

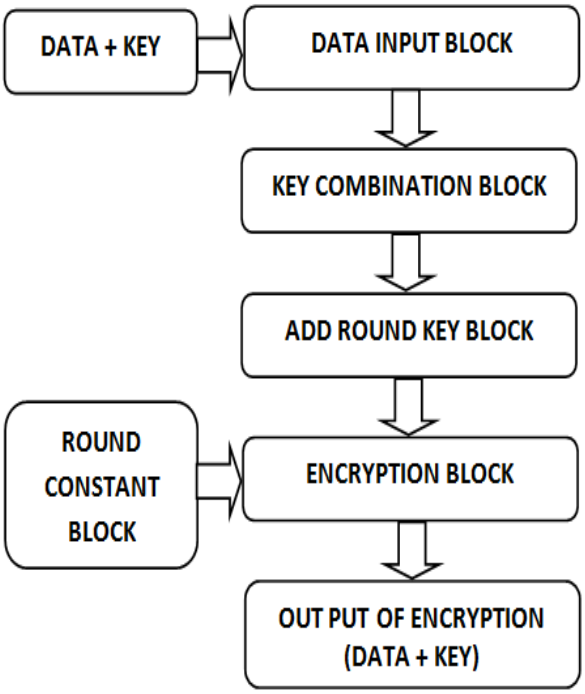

Fig. 2 Triple Key AES algorithm

Above all else 128 piece information is given to the information input square alongside the three 128 piece keys. These keys are given to the key blend square. In this square the exoring of keys are performed to get the 128 piece yield key. These yield key is next given to include round key square alongside the 128 piece input information. In these square the customary include round activity is played out that is the exoring of information and key is performed.In this way the yield of this square is sent to the real encryption square and the key extension round constants are additionally given to it. In this square all the change of customary AES calculation is performed. It implies that changes like substitute byte change, move push change, blend section change and include round key change are performed. For 128 piece information we need to perform 10 rounds of encryption. In the wake of executing these changes it will give the last encoded 128 piece information and 128 piece key. For decoding of the information same procedure is followed backward request with the assistance of converse changes of the regular AES calculation. Figure 3 shows the proposed block diagram of AES algorithms.

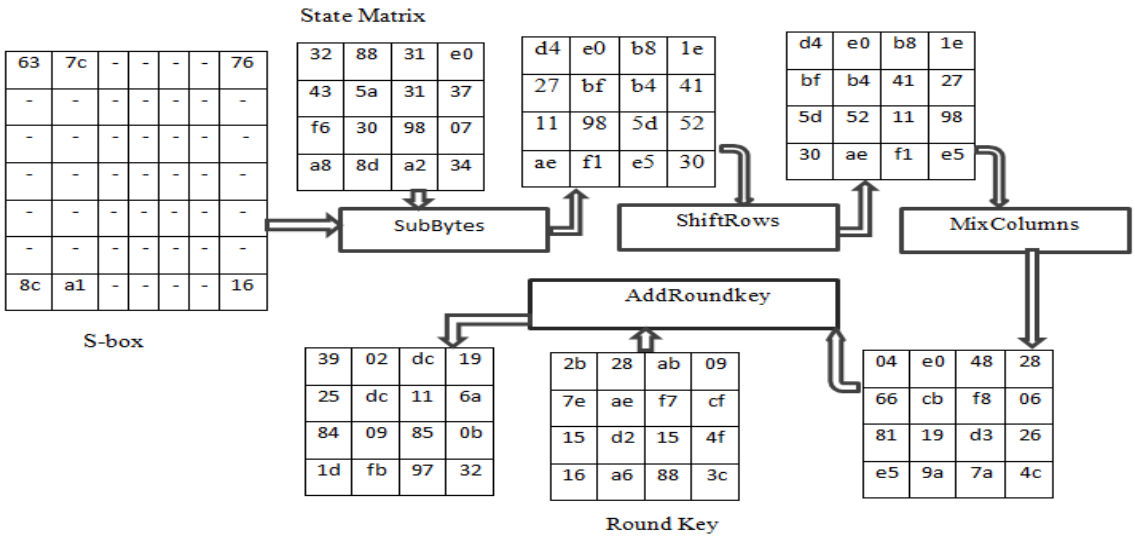

Fig. 3 Block Diagram of AES algorithms

III. FPGA SYNTHESIS ANALYSIS AND SIMULATION RESULTS

This entire get together is executed on the dynamic HDL programming with the assistance of Verilog programming. After that we had tested that calculation in Xilinx and actualized on FPGA vertex 4 for configurable equipment. Following from the accompanying outcome plainly the framework required less LUTs and rationale cuts when contrasted with the all-out LUTs and rationale cuts are accessible. Because of which the memory utilization occur is less.

Figure 4 shows the hardware implementation of the AES algorithm which shows the inputs and the flip flops that are used internally. Total CLBs utilized are 3402, No. of LUTs utilized is 27787 and No. of IOBs utilized is 385.

Field Programmable Gate Arrays (FPGAs) are becoming a critical part of every system design. Here we have used Xilinx (virtex-4) family. We have developed total hardware using Verilog HDL code. Figure 4 shows the RTL (FPGA) schematic view of Encryption and Decryption modules. The encryption and decryption FPGA device utilization is used as LUTs are 27787, input and output buffers used are 385, number of slices 1 and Global Clocks (GCLKs) are 1. The average connection delay for encryption and decryption is 4.221ns. The total power consumed for both encryption and decryption is side is 1.55W. Figure 5 shows the simulation timing results of encryption and decryption modules. Table 2 gives the device utilization report.

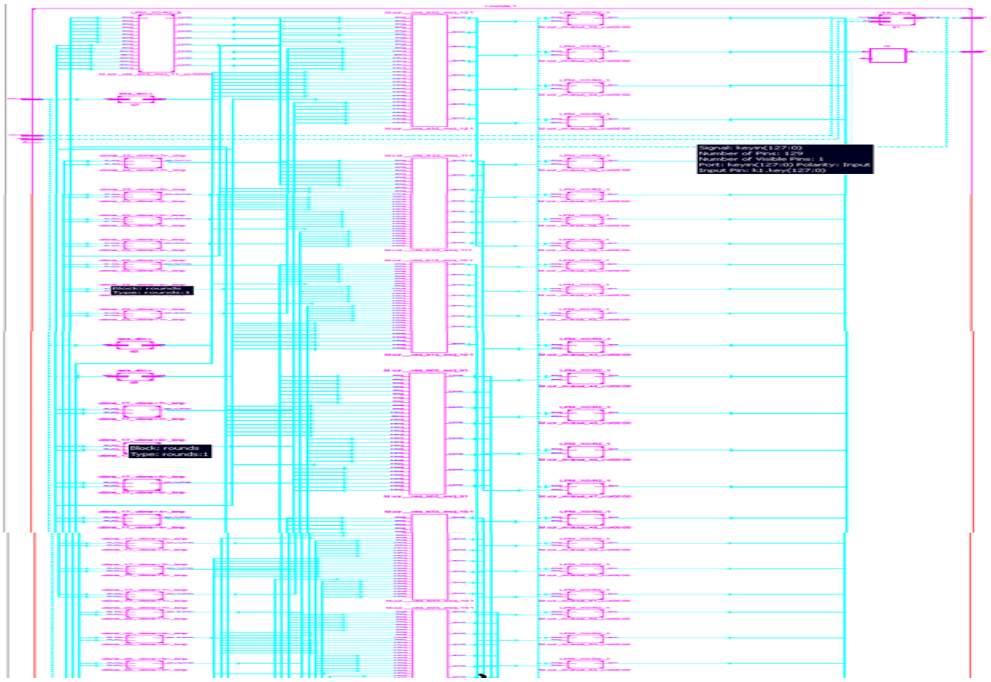

Fig. 4 RTL view of AES FPGA

Table. 1 Comparison of performance architecture

Device	Area(CLB's)	Throughput MBits/sec
XCV1000BG560-6	2902	331.5
XCV 1000	5673	353.0
XC2V600BF957-6	2943	666.7
Proposed Algorithm	3402	867.34

Table 1 compares the proposed algorithm with different FPGA devices in Xilinx. From the analysis we can derive that the proposed algorithm gives better throughput that is 15% more than that of previous output and with less delay. Figure 5 shows the AES encryption and decryption simulation timing results.

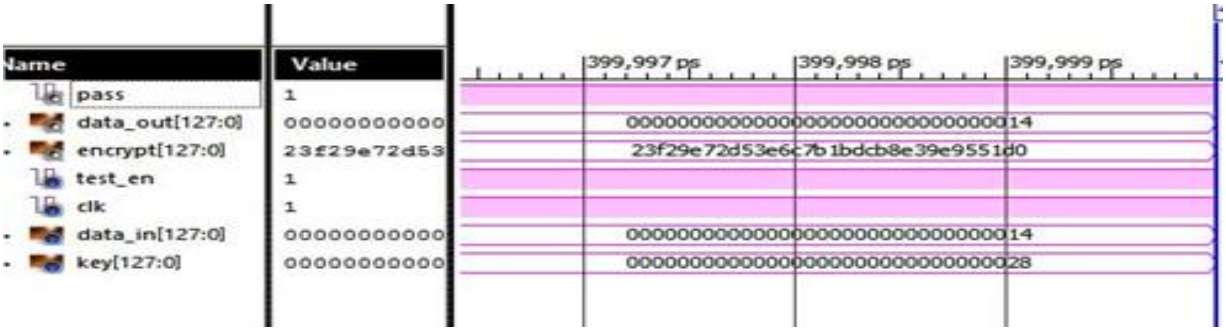

Fig. 5 AES encryption and decryption simulation timing results

IV. CONCLUSION

In this paper we have proposed AES Encryption and Decryption Algorithms using triple key AES. By using this algorithm we have optimized the delay of 4.221ns in the outcome.The total power consumed here is 1.55W. The calculation is solid as far as security and furthermore reasonable for equipment execution. The outcomes demonstrate that the present proposed calculation has great cryptographic quality, with the additional advantage of having high security.

REFERENCES

1. Muhammad Sohail Ibrahim, Irfan Ahmed , M. Imran Aslam, Muhammad Ghazaal, Muhammad Usman, Kamran Raza and Shujaat Khan, "A Low Cost FPGA based Cryptosystem Design for High Throughput Area Ratio" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 2, 2017, PP. 385-393.
2. M. Ebrahim, S. Khan, and U. B. Khalid, "Symmetric algorithm survey: A comparative analysis," International Journal of Computer Applications, Vol. 61, No. 20, 2014, PP. 12-19.
3. Nisar Ahmed, Hafiz Muhammad Shahzad Asif and Gulshan Saleem, "A Benchmark for Performance Evaluation and Security Assessment of Image Encryption Schemes", I. J. Computer Network and Information Security, Vol. 8, No. 12, 2016, PP.18-29.
4. Upputuri Neelima, Fazal Noorbasha, "Data Encryption and Decryption using Reed-Muller Techniques", International Journal of Engineering and Technology (IJET), ISSN : 0975-4024 Vol 8 No 1 Feb-Mar 2016, PP. 83-91.
5. Fazal Noorbasha, M. Manasa, R. Tulasi Gouthami, S. Sruthi, D. Hari Priya, N. Prashanth, And Md. Zia Ur Rahman, "FPGA Implementation Of Cryptographic Systems For Symmetric Encryption", Journal of Theoretical and Applied Information Technology, 15th May 2017. Vol.95. No 9, PP. 2038-2045
6. Fazal Noorbasha, C.H. Vainatheyi, R. Goutham, P. Raviteja, B. Karthik, "Implementation of Image Secured Hybrid AES - DNA Algorithm Using Verilog HDL", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018, PP. 452-458.
7. G Divya, Fazal Noorbasha, "Implementation of DNA Based Cryptography Using OTP Random Key Generation Process", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018, PP. 481-490.
8. Ali Al-Haj, Hiba Abdel-Nabi, "Digital image security based on data hiding and cryptography", 3rd International Conference on Information Management , 21-23 April 2017, PP. 437-440.
9. Dilovan Asaad Zebari, Habibollah Haron, Subhi R. M. Zeebaree, Diyar Qader Zeebaree "Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations", International Conference on Advanced Science and Engineering (ICOASE), Vol.978(1), PP.312-317,2018.
10. Wenting Yuan, Xuelin Yang, Wei Guo, Weisheng Hu, "A double-domain image encryption using hyper chaos" 19th International Conference on Transparent Optical Networks (ICTON), 2017, PP. 1-4.
11. Alexandr Kuznetsov, Vladislav Frolenko, Egor Eremin, Olga Zavgorodnia, "Research of cross-platform stream symmetric ciphers implementation", *Dependable Systems Services and Technologies (DESSERT) 2018 IEEE 9th International Conference on*, pp. 300-305, 2018.
12. J. S. Park, K. S. Bae, C. Y. Choi, D. H. Choi, and J. C. Ha, "A fault resistant implementation of AES using differential bytes between input and output," Journal of Supercomputing, vol. 67, no. 3, pp. 615-634, Mar. 2014.
13. Abdullah, A. M., and Aziz, R. H. H. (2016, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17).
14. N Sivasankari, K Rampriya and A Muthukumar ," Implementation of Area Efficient 128-bit Based AES Algorithm in FPGA", European Journal of Advances in Engineering and Technology, 2017, 4(7), PP 541-548.
15. Z Liu, L Li and X Zou, A Low-Cost Low-Power Ring Oscillator-Based Truly Random Number Generator for Encryption on Smart Cards, IEEE Transactions on Circuits and Systems II, 2016, 63 (6), PP 608-612.
16. Yadlapati, A., Kakarla, H.K. An Advanced AXI Protocol Verification using Verilog HDL (2015) Wulfenia, 22 (4), pp. 307-314.
17. Bindu Bhargavi, K., Hari Kishore, K. Low Power Bist on Memory Interface Logic (2015) International Journal of Applied Engineering Research, 10 (8), pp. 21079-21090.

18. Charan, N.S., Kishore, K.H. Recognization of delay faults in cluster based FPGA using BIST (2016) Indian Journal of Science and Technology, 9 (28).
19. Hari Kishore, K., Aswin Kumar, C.V.R.N., Vijay Srinivas, T., Govardhan, G.V., Pavan Kumar, C.N., Venkatesh, R.V. Design and analysis of high efficient UART on spartan-6 and virtex-7 devices (2015) International Journal of Applied Engineering Research, 10 (9), pp. 23043-23052.
20. Kante, S., Kakarla, H.K., Yadlapati, A. Design and verification of AMBA AHB-lite protocol using Verilog HDL (2016) International Journal of Engineering and Technology, 8 (2), pp. 734-741.
21. Bandlamoodi, S., Hari Kishore, K. An FPGA implementation of phase-locked loop (PLL) with self-healing VCO (2015) International Journal of Applied Engineering Research, 10 (14), pp. 34137-34139.
22. Murali, A., Hari Kishore, K., Rama Krishna, C.P., Kumar, S., Trinadha Rao, A. Integrating the reconfigurable devices using slow-changing key technique to achieve high performance (2017) Proceedings - 7th IEEE International Advanced Computing Conference, IACC 2017, art. no. 7976849, pp. 530-534.
23. A. Surendar, K. H. Kishore, M. Kavitha, A. Z. Ibatova, V. Samavatian "Effects of Thermo-Mechanical Fatigue and Low Cycle Fatigue Interaction on Performance of Solder Joints" IEEE Transactions on Device and Materials Reliability, P-ISSN: 1530-4388, E-ISSN: 1558-2574, Vol No: 18, Issue No: 4, Page No: 606-612, December-2018.
24. N Bala Dastagiri K Hari Kishore "A 14-bit 10kS/s Power Efficient 65nm SAR ADC for Cardiac Implantable Medical Devices" International Journal of Engineering and Technology (UAE), ISSN No: 2227-524X, Vol No: 7, Issue No: 2.8, Page No: 34-39, March 2018.
25. N Bala Dastagiri, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.
26. N Bala Dastagiri, K Hari Kishore "Analysis of Low Power Low Kickback Noise in Dynamic Comparators in Pacemakers" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.44, page: 1-4, November 2016.
27. Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.
28. Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T "Review and Analysis of Promising Technologies with Respect to fifth Generation Networks", 2014 First International Conference on Networks and Soft Computing,ISSN:978-1-4799-3486-7/14,pp.248-251,August 2014.
29. P Bala Gopal, K Hari Kishore, R.R Kalyan Venkatesh, P Harinath Mandalapu "An FPGA Implementation of On Chip UART Testing with BIST Techniques", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015.
30. Avinash Yadlapati, Hari Kishore Kakarla **"**Design and Verification of Asynchronous FIFO with Novel Architecture Using Verilog HDL**"** Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No: 14, Issue No: 1, Page No: 159-163, January 2019.