International Journal of Engineering & Technology, 7 (2.8) (2018) 392-396

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Implementation of modified Feistel block cipher for OTP generation using Verilog HDL

Fazal Noorbasha*, K Hari Kishore, T. Naveen, A. Sai Anusha, Y. Manisha, K. Revathi, M. Manasa

Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522502
**Corresponding Author Email: fazalnoorbasha@kluniversity.in*

Abstract

In this paper we modified feistel block cipher to generate OTP (One Time Password) and implement it using Verilog HDL. To perform any online transaction using debit or credit cards, an OTP is sent to the client via SMS for his mobile number registered at the bank, then the client enters this OTP to complete the transaction. This OTP is generated at Bank server and sent to the client mobile operator. Once the OTP is generated it should be protected during the transmission from cyber attacks such as phishing, malware Trojans, etc. before it reaches the client to maintain confidentiality and integrity of information. This algorithm uniquely specifies the steps to encrypt the plain text into cryptographic cipher and to decrypt this cipher text back into original form. The proposed modified method is for improving the security.

Keywords: *Feistel Cipher, OTP, Symmetric-keys, Field Programmable Gate Array (FPGA), Verilog HDL.*

1. Introduction

Cryptography is the most important aspect of communication security which has a wide range of importance as it is a basic building block for computer security. This publication provides a complete description of algorithm for both encryption (enciphering) and decryption (deciphering) [1, 2]. Encryption converts the plaintext into an incomprehensible form called cipher text. This cipher text is converted back into original data through Decryption [3, 4].

Key is the binary value which plays a crucial role in the algorithm for both encryption and decryption. If both the sender and receiver uses same key to encrypt and decrypt data respectively then the system is referred to as symmetric, single-key encryption. If both of them use different keys to encrypt and decrypt data then it is known as asymmetric or two-key encryption [5,6,7]. In this algorithm we are implementing symmetric encryption where we use same key in both encryption and decryption of data [8, 9, 10, 11].

In this algorithm for security purpose the OTP is generated and encryption process starts only when the client enters the card number and mobile number registered at bank. If there is a mismatch in any of these credentials then OTP is not generated and displays a message as “INVALID”.

2. System Block Diagram

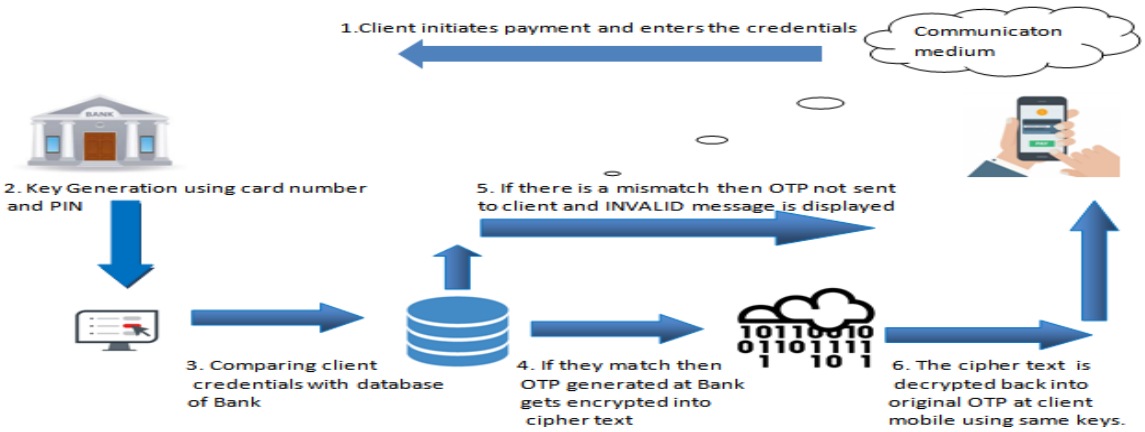

Fig. 1: System Block Diagram

Fig. 1 which is shown above is the system block diagram where initially the client begins the transaction and enters his card details and mobile number and this information is sent to the bank through the communication medium and in the next step the keys are generated using the card number and PIN of client which is explained in detail later in the algorithm and these credentials are

compared with the database of bank and if they are not matched then OTP is not sent to client and transaction fails an "INVALID" message is displayed and if they are matched then the randomly generated OTP at the bank is encrypted into cipher text. Through the communication medium this cipher text is transferred to the client mobile. Now this cipher text is decrypted back into original OTP by generating same keys at client mobile.

3. Modified Feistel Block Cipher Algorithm

The modified feistel block cipher algorithm is shown in Fig.2 and the steps in the algorithm is explained below.

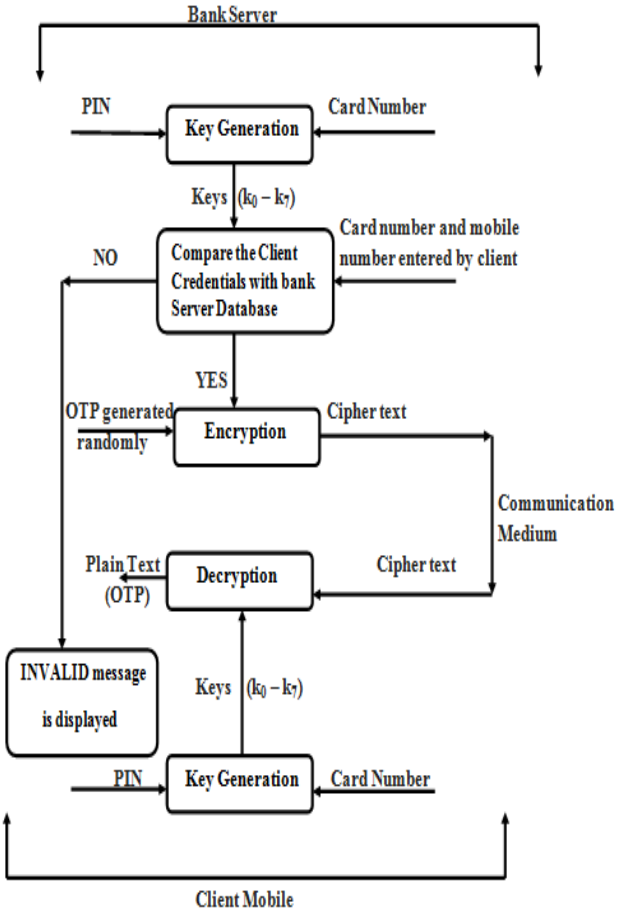

Fig. 2: Modified Feistel Block Cipher Algorithm

A. Generation of Keys

We have already specified that the key has atmost importance in this algorithm. The key is generated by using card number and PIN of the client. Some of the Ex-OR and mathematical operations are performed on this 16 digit card number and 4 digit PIN to generate keys. Let us explain the algorithm in detail mathematically with an example as follows:

Card Number: 2435 9678 2246 3234 PIN: 7682

Initially the 16 digit card number C_1 to C_{16} is taken and each digit is converted into its respective 4 bit binary form and Ex-OR operation is performed on this 4 bit binary data. As per our example C_1 which is 2 is taken and converted to binary form and Ex-OR is performed on these binary bits and store the resultant bit in Y_1.

C_1= 2 = 0 0 1 0

Y_1=0⊕ 0⊕ 1 ⊕ 0 = 1

Similarly, it is done for all the remaining digits from C_2 to C_{16} and store resultant bits in Y_2 to Y_{16}.

Again Ex-OR operation is performed on these Y_1 to Y_{16} bits as follows and result is stored in Q.

$Q_4= Y_1⊕Y_2⊕Y_3⊕Y_4$

$Q_3= Y_5⊕Y_6⊕Y_7⊕Y_8$

$Q_2= Y_9 ⊕Y_{10}⊕Y_{11}⊕Y_{12}$

$Q_1= Y_{13}⊕Y_{14}⊕Y_{15}⊕Y_{16}$

Finally we get Q = 0 0 1 0 = 2

Now, all the 4 digits in the 4 digit PIN are added and stored in P. If the value obtained after addition is a double digit then it is added further until we get a single digit.

PIN: 7682

P = 7 + 6 + 8 + 2 = 23 = 2 + 3 = 5

Incase Q value which is obtained is also a double digit then it is also added further until we get a single digit.

Now r value is calculated

r = P % Q = 5 % 2 = 1

Now, 8 keys are generated, k_0 to k_7 by using 4 digit PIN and r value. k_0 is the MSB of PIN and k_1 is decided by the number of binary 1s present in MSB of PIN where if the 1s count is even then we add r value to MSB of PIN, if the count of binary 1s is odd then we subtract r value from MSB of PIN.

k_0 = 7 = 0111

k_1= 7 – 1= 6 = 0110 because binary value of 7 is 0111 where there are odd number of 1s so we go for subtraction.

Similarly, rest of the keys are generated from the remaining digits of PIN

k_2 = 6 = 0110

k_3 = 6 + 1 = 7 = 0111 because binary value of 6 is 0110 where there are even number of 1s so we go for addition.

Similarly, k_4 = 8 = 1000

K_5 = 8 – 1 = 7 = 0111

K_6 = 2 = 0010

K_7 = 2 - 1 = 1 = 0001

B. Encryption Process

Once the keys are generated at the Bank server then the next step is encryption where the client needs to enter his mobile number that was registered at bank and the card number, then these credentials are verified with the bank database, if there is a mismatch then the process stops and a message is displayed as "INVALID". If the credentials matches with database then the process continues further where a 6 digit OTP is generated randomly. This OTP and the keys that were generated are given as inputs to the feistel block where the OTP is converted into its binary form and divided into two halves and the operation is performed where the encryption algorithm for one round is shown in Fig.3.

Likewise this data is iterated through 'n' number of rounds where we iterated it for 8 rounds in our algorithm for which we have generated 8 sub keys. The OTP that is given as input is the plaintext. Based upon sub keys the plaintext undergoes transformation for each round. The transformed output that was obtained from one round is given as input for next round which is shown in Fig.4. The final transformed output that was obtained from nth round is known as cipher text which is the final encrypted output that is sent through the communication medium to the client mobile.

Where, LB_i and RB_i – Output for Round i

F_i – Round Function i

K_i – Sub Key for Round i

For each round i = 1, 2, 3,…n, compute

$LB_{i+1} = RB_i$

$RB_{i+1} = LB_i⊕F(RB_i , K_i)$

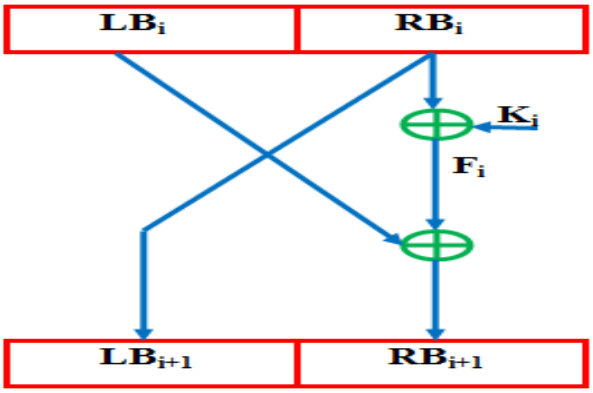

Fig. 3: Encryption Algorithm for Single Round

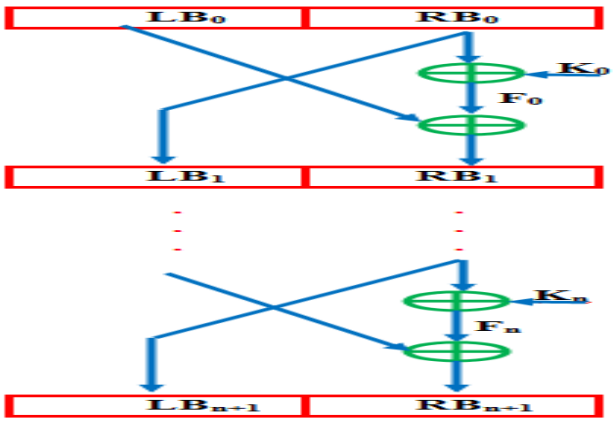

Fig. 4: Encryption Algorithm for n Rounds

As per our example let us assume OTP is 463967. The cipher text after 8th round of encryption is 000111001000011001000001.

C. Decryption Process

Once the encrypted cipher text reaches the client mobile by passing through the communication medium then sub keys are generated at the client mobile using the same card number and PIN same as done at the bank server in the encryption process. Now in the decryption process the 24 bit cipher text and sub keys are given as inputs to the Decryption Algorithm . Like the Encryption Algorithm here also the data is transformed for n rounds where the outputs obtained from one round are given as inputs for the next round i.e., the outputs obtained from round 1 are given as inputs for round 2 which is shown in Fig.5. After performing n rounds of decryption we receive the plaintext i.e., the OTP.

Where, $RB_i = LB_{i+1}$

$LB_i = RB_{i+1} \oplus F(LB_{i+1} , K_i)$

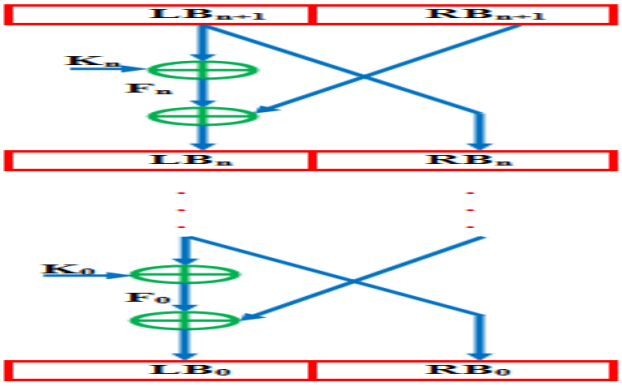

Fig. 5: Decryption Algorithm for n Rounds

In the Decryption phase after performing 8 rounds of decryption we will receive the original OTP 463967.

4. Synthesis Report

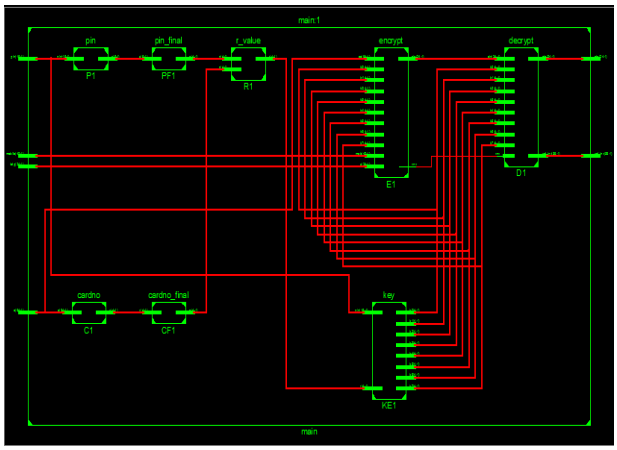

Fig. 6: RTL Schematic

The above shown Fig. 6 is the RTL schematic which is designed using xc3s400-5pq208 FPGA.

Table 1: Device Utilization Summary

Logic Utilization	Used
Number of Slice Latches	20
Number of 4 input LUTs	436
Number of Occupied Slices	230
Number of Bonded IOBs	224
Average Fan-out of Non-clock Nets	3.69

The designing requires on a total of 5 ROMs of which 4 are 19 x 4 bit and one is 37 x 4 bit ROM. It also requires 5 4-bit Latches and 11 comparators and 262 Ex-OR gates are used and 436 4 input LUTs are used which is shown in Table 1. Now the Timing details are discussed:

Speed Grade: -5

Minimum input arrival time before clock: 19.726ns

Maximum output required time after clock: 25.537ns

Maximum combinational path delay: 30.611ns

5. Results Analysis

The following figures shows the results for above explained algorithm where Fig.7 shows the timing diagram of Encryption where ‘x’ indicates the OTP generated at Bank Server, ‘ca’ indicates the card number, ‘mob’ is the mobile number entered by client, k_0 to k_7 are the keys generated using card number and PIN. The figure shows the results for 4 test cases where in the first example the mobile number entered by client matches with database and gives ‘cip’ i.e., 24 bit cipher text as output and ‘vnv’ indicates valid not valid bit as logic HIGH and ‘valid_invalid’ shows that the credentials are VALID and in second example there is a mismatch so vnv is logic LOW.

Again in third example the credentials matches with the database so the encryption process is successful and it is VALID but in the fourth example there is a mismatch with respect to card number where the LSB digit of card is entered as ‘8’ instead of ‘9’. So, this case is also INVALID.

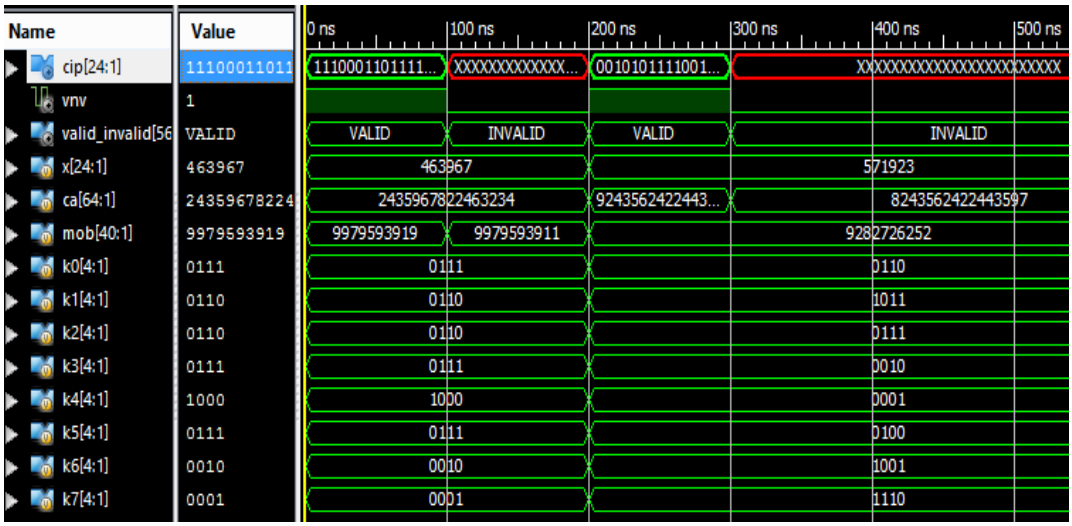

Fig. 7: Timing Diagram of Encryption

Fig.8 shows the final result after decryption where cipher text obtained from encryption is given as input and 'c' indicates card number and 'iotp' is the OTP generated at Bank Server and 'otp' is the final OTP that the client receives after Decryption. When there is a mismatch with respect to credentials entered by client then the OTP is not generated and received by the client and an "INVALID" message is displayed as shown else a "VALID" message is displayed and OTP is received. The below figure shows the results for the four examples where in the first example the credentials are matched and OTP is received and a "VALID" message is displayed and in other example there is a mismatch with respect to phone number so the OTP is not received and an "INVALID" message is displayed. Similarly, third example is VALID and fourth example is INVALID because the card number entered by client is wrong.

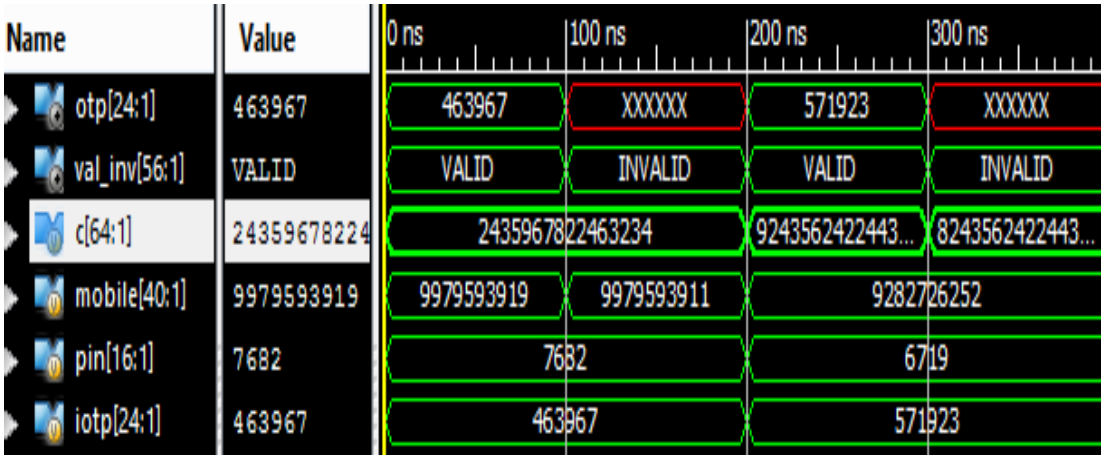

Fig. 8: Timing Diagram of Decryption

6. Conclusions

In this project we have used an adder/ subtractor for the generation of keys unlike the general feistel block cipher where only adder is used through which there is an improvement in security and in the generation of keys phase instead of generating some random numbers and using them for keys generation we used card number and PIN of client which are basically confidential and performed many Ex-OR and mathematical operations on them to generate the keys which also improves security and also an advantage of this method is that the size of input can be easily changed.

References

[1] Fazal Noorbasha, G. Jaswanth Varma, B. Ajani Kumar, Harikishore Kakarla, M. Manasa, "Data Security Based On DNA Cryptography Using S-Box Encryption", International Journal of Pure and Applied Mathematics, ISSN 1311-8080. Volume115, No.7, 2017, PP. 429-434.

[2] Fazal Noorbasha, Harikishore Kakarla, Deekshatha.A, P.G.Mounika, N.Ganga Dheeraj, M. Manasa, "Implementation of Quarter Cycle Key Cryptographic Algorithm Using Verilog HDL", International Journal of Pure and Applied Mathematics, ISSN 1311-8080. Volume115, No.7, 2017, PP. 423-427.

[3] Fazal Noorbasha, B. Anjani Kumar, G. Jaswanth Varma,Harikishore Kakarla, M. Manasa, "Data Encryption and Decryption Cryptography Using Modified AES Algorithm", International Journal of Pure and Applied Mathematics, ISSN 1311-8080. Volume115, No.7, 2017, PP.435-440.

[4] 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, ISSN: 1992-8645.

[5] M. Manasa, Fazal Noorbasha, Ch.L.Sudheshna, M.Santhosh, V.Naresh, Md. Zia Ur Rahman, "Comparative Analysis of CORDIC Algorithm and Taylor Series Expansion ", Journal of Theoretical and Applied Information Technology, 15th May 2017. Vol.95. No 9, PP. 2015-2022, ISSN: 1992-8645.

[6] 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.

[7] P. Santhamma, B. Raghavaiah, N. Suresh Babu, "Implementation

of Pipelined DES using Verilog", International Journal of Computer & Communication Technology, Volume – 3, Issue – 5, 2012.

[8] Dr. Ananathi Shesashaayee, D Sumathy, "OTP Encryption Techniques in Mobiles for Authentication and Transaction Security" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2014, PP 6193-6201.

[9] Vishal Krishnan, Hanumesh H, Prateek D Nayak, Krishanmurty M S, "OTP Authenticated and Encrption on Cloud Data", SEA International Journal of Advanced Research in Engineering, Vol. 1, Issue 1, 2016, PP 1- 6.

[10] Ramesh K., Ramesh S., "Implementing One Time Password Based Security Mechanism for securing personal health records in cloud", International conference on control, instrumentation, communication and computational technologies (ICCICCT) 10 Jul - 11 Jul 2014, PP 968 – 972.

[11] Gotimukul Venkatesh , Sunkara Venu Gopal , Mrudula Meduri ,C. Sindhu, "Application of session login and one time password in fund transfer system using RSA algorithm" International conference of Electronics, Communication and Aerospace Technology (ICECA), 2017, 20-22 April 2017, PP 732-738.

[12] 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 & Soft Computing, ISSN:978-1-4799-3486-7/14,pp.270-273,August2014.

[13] 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.

[14] 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.

[15] A Murali, K Hari Kishore, D Venkat Reddy "Integrating FPGAs with Trigger Circuitry Core System Insertions for Observability in Debugging Process" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.11, Issue No.12, page: 2643-2650, December 2016.

[16] Mahesh Mudavath, K Hari Kishore, D Venkat Reddy "Design of CMOS RF Front-End of Low Noise Amplifier for LTE System Applications Integrating FPGAs" Asian Journal of Information Technology, ISSN No: 1682-3915, Vol No.15, Issue No.20, page: 4040-4047, December 2016.

[17] 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.

[18] S Nazeer Hussain, K Hari Kishore "Computational Optimization of Placement and Routing using Genetic Algorithm" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.47, page: 1-4, December 2016.

[19] 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.

[20] 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.

[21] S.V.Manikanthan and K.srividhya "An Android based secure access control using ARM and cloud computing", Published in: Electronics and Communication Systems (ICECS), 2015 2nd International Conference on 26-27 Feb. 2015, Publisher:IEEE,DOI:10.1109/ECS.2015.7124833.

[22] T.Padmapriya and V.Saminadan, "Utility based Vertical Handoff Decision Model for LTE-A networks", International Journal of Computer Science and Information Security, ISSN 1947-5500, vol.14, no.11, November 2016.