ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse06932020.pdf
https://doi.org/10.30534/ijatcse/2020/06932020

FPGA Implementation of Image Cryptology using Reversible Logic Gates

B. Murali Krishna[1], K. Ch. Sri Kavya[2], P.V. S. Sai Kumar[3], K. Karthik[4], Y. Siva Nagababu[5]
[1]Assoc Professor, [2]Professor, [3,4,5]UG Scholar,
[1-5]Department of ECE, Koneru Lakshmaiah Education Foundation, K L Deemed to be University, Green Fields,
Vaddeswaram, Guntur, AP, India.
[1]muralikrishna@kluniversity.in , [2]kavya@kluniversity.in, [3]satyasai9996@gmail.com,
[4]karthikkoganti73@gmail.com, [5]sivayarlagadda123s@gmail.com

ABSTRACT

Reversible calculations have lot of applications in various fields like in Nanotechnology, Low power CMOS, Optical computing, Digital Image Processing, etc. Reversible calculations are the best systematic ways to turn down heat dissipation than any other standard methods. The key requirement for reversibility is for each input and output vector to have a one-to-one relation and it is very necessary as there is no information loss in the reversible calculation which reduces the power dispersion. Ideally, zero energy is dissipated by reversible circuits. Cryptology is used to provide security and privacy to authenticated users. In this paper an Image Cryptology (IC) is proposed with secret key generated using Runtime Linear Feedback Shift Register Logic (RLFSRL) to encrypt and decrypt data using Reversible Logic Gates (RLG) on Field Programmable Gate Array *(FPGA).* ICRLG designed in verilog hardware description language (HDL) which is synthesized, simulated and implemented on Vivado and targeted on Artix-7 XC7A35T-1-CPG236 architecture.

Key words: FPGA, LFSR, Reversible Logic Gates, RLC, Encryption and Decryption.

1. INTRODUCTION

Encryption is one of the main mechanisms for data privacy, security, and safety from unauthorized access. A reversible logic gate is one of the leading designs to improve security purpose. The reversible logic operation produces zero power dissipation and provides lossless information. To avoid the Information loss in the data, output of each reversible logic gate is draws from the input. In this system most of the work is gone through scalable isogeny cryptology, AES based cryptology, etc. but the above designs require more power to execute and offer less security. To improve data security modern symmetric cryptography protocol is utilized [9]. This algorithm is used for different types of applications such and banking, medical, etc. The main drawback is that the number of iterations is more, the time of encrypting and decrypting is elevated. To overcome these problems the RLG method is introduced. Cryptosystem is designed using reversible logic gates. LFSR plays a crucial role in key generation for cryptography applications. In comparison with the conventional methods proposed method consumes better resources, with improved performance improved using RLG method [1-5].

2. CRYPTOLOGY

Cryptology is a process that uses a certain set of codes to improve privacy and provides secure communication. Modern Cryptology uses certain algorithms and security keys [10-12] to encrypt and decrypt data. Encryption is a process of translating the data into unpredictable codes. To access encrypted data, authenticated key is crucial.

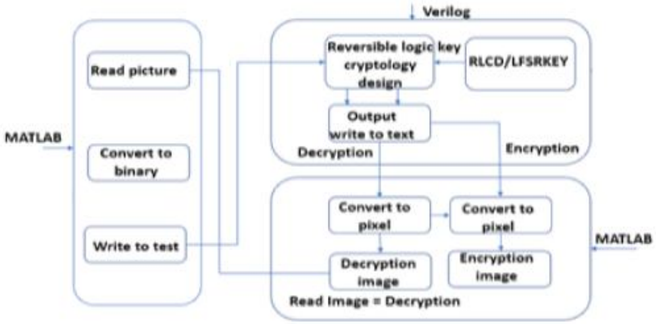


Figure 1: Image Cryptology using Reversible Logic Gates

To protect sensible electronic data such as e-mail, folders, files, and entire drives there are two types of encryption methods such as symmetric and asymmetric encryption. The process of retrieving original data from cipher with authenticated key and few operations is called decryption. To protect the information from hackers, the data will be encrypted with unique and special keys so that, the intruder cannot interpret the data. The algorithms and keys are designed in such a way that only the authenticated end users can able to encrypt and decrypt the data [6-8].

3. PROPOSED METHODOLOGY

The encryption and decryption process of Image cryptology using reversible logic gates is shown in figure 1. An Image is converted into a binary pixel format which is an acceptable in Xilinx Vivado Tool using MATLAB. HDL is used to read binary pixel values and apply reversible logic with random key generated by RLFSR for data encryption. To decrypt the original image an irreversible logic with random key is applied on received cipher a new binary pixel values are generated. MATLAB plays a crucial role in converting binary pixel values to original image vice-versa.

4. REVERSIBLE LOGIC GATES

Reversible logic gates should fall the below two conditions. No of inputs and outputs should be same. The pattern of input and output should be unique. Let input be 101 is applied to the reversible logic gate, and then it gives the output as 010. If the output is the same as input, then it represents the existence of reversible logic operation in the system. HING, PERES, CNOT reversible gates plays a crucial role to design the encryption and decryption.

4.1 CNOT Gate

The CNOT gate is shown in figure 2 is a 2*2 reversible logic gate where A, B are input and P, Q are outputs.

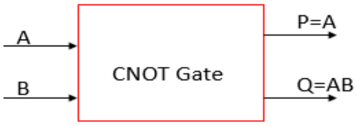


Figure 2: CNOT Gate

The logic for the CNOT gate, if the input is A then output will be P=A. If another input is B, then the output will be Q=A^B.

4.2 HING Gate

The HING gate is shown in figure 3 is a 4*4 reversible logic gate where A, B, C, D are inputs and P, Q, R, S are outputs. The logic for the HING gate, if A is given as input then the output P will be A itself Similar to B. The output of R will be A^B^C. The final output of S=(A^B) &(C^A) &(B^D).

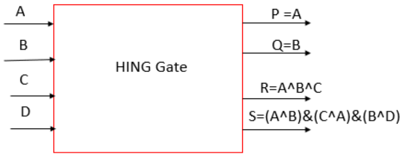


Figure 3: HING Gate

4.3 PERES Gate

The PERES gate is shown in figure 4 a 3*3 reversible logic gate where A, B, C, are inputs and P, Q, Z, are output. The logic for the PERES gate, if A is given as input then the output P will be A itself. The output of Q will be A^B. The final output of Z=(A&B) ^ C.

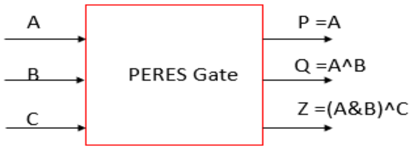


Figure 4: PERES Gate

5. RUNTIME LINEAR FEEDBACK SHIFT REGISTER LOGIC (RLFSRL)

In the area of communication, random number generators are most widely used to protect systems via pseudo-random sequences. It is applicable for key generation in cryptography applications and signature analyzers to generate test patterns for Built-In-Self Test.

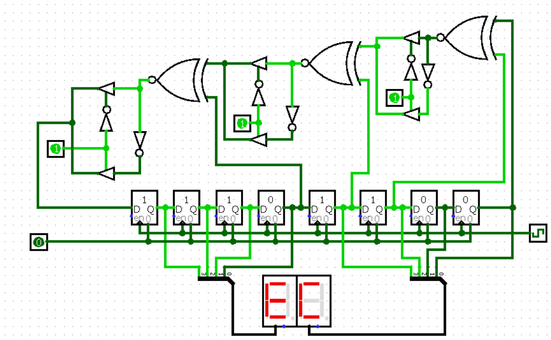


Figure 5: RLFSRL with Multiplexer

In the traditional method, using a seed value or reference value is used to generate a random number using the XOR gate. The newly proposed methods of random test patterns are generated using linear feedback shift register (LFSR) based on XOR, XNOR gates with and without seed value using a multiplexer. The multiplexer is appending to generate a random value at a user-defined state in runtime. LFSRs produce random numbers or symbols that cannot be predicted. LFSRs have a wide range of applications in gambling, statistical sampling, simulation, cryptography, completely randomized design, and mostly in the areas of mobile and space communications.

The multiplexer present for the generation of seed value uses more logic gates depending upon the bit size of the random number. To overcome this, the multiplexer can be replaced with two tri-state buffers and one inverter which utilize less hardware. The proposed RLFSRL model with less hardware without seed value shown in figure 5. When selection input is “0” circuit generates a random number using XNOR gates, when selection input is “1” random number is generated using XOR gate.

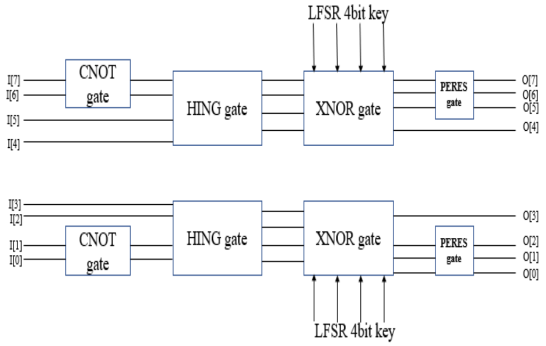


Figure 6: ICRLG Encryption process

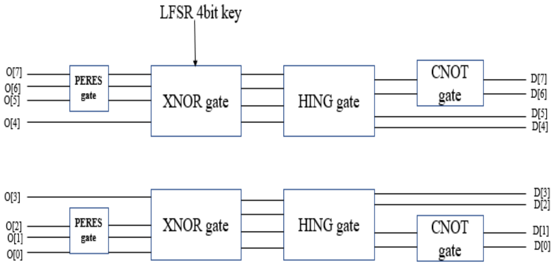


Figure 7: ICRLG Decryption process

6. ICRLG ENCRYPTION AND DECRYPTION PROCESS

In Image Cryptology Reversible Logic Gates Encryption System is shown in figure 6 initially an image is converted into binary values using MATLAB. Eight Bit encryption system is bifurcated into two nibbles MSB & LSB. The series of a binary pixel sequences obtained from the image like I0, I1, I2......I7, which are processed to MSB & LSB through a CNOT, HING, PERES reversible logic gates and RLFSRL. The 8-bit RLFSRL generates random numbers which is xnored with the binary values obtained from the specified reversible gates.

The cipher values obtained from encryption system are generated as $O_0, O_1, \dots, O_7$. In Decryption system is shown in figure 7 cipher applies as primary input followed by RLFSRL and processed by MSB & LSB through series of above specified reversible logic gates which decrypts the original binary sequences of input image and applies inputs to MATLAB for reconstruction of original image, D0, D1, D2......D7.

7. SIMULATION RESULTS

The simulation results of ICRLG encryption and decryption process are shown below.

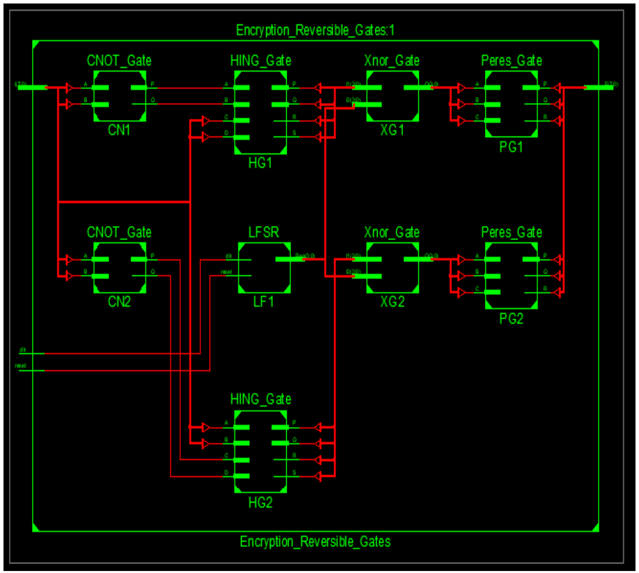


Figure 8: Encryption RTL Schematic

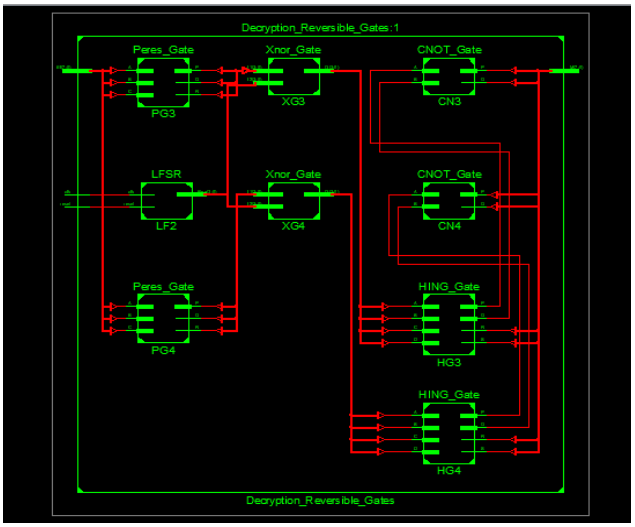


Figure 9: Decryption RTL Schematic

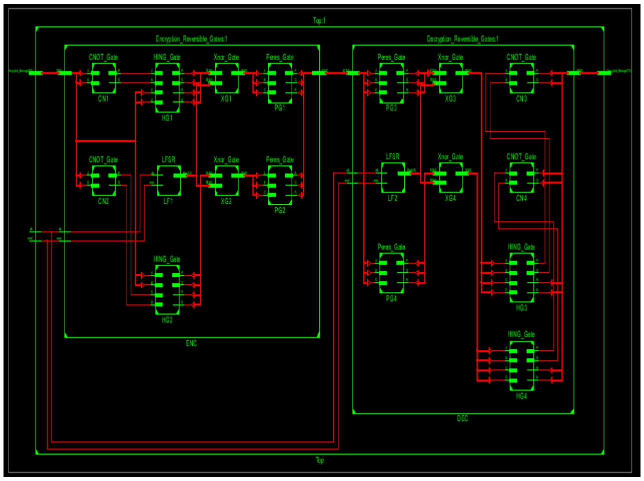
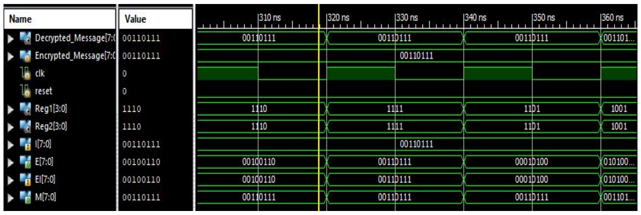


Figure 10: Encryption and Decryption RTL Schematic



```
Name                    Value     |310 ns      |320 ns      |330 ns      |340 ns      |350 ns      |360 ns
Decrypted_Message[7:0]  00110111  00110111      00110111                  00110111                  001101...
Encrypted_Message[7:0]  00110111                              00110111
clk                     0
reset                   0
Reg1[3:0]               1110      1110          1111                      1101                      1001
Reg2[3:0]               1110      1110          1111                      1101                      1001
I[7:0]                  00110111                              00110111
E[7:0]                  00100110  00100110      00110111                  00010100                  010100...
EI[7:0]                 00100110  00100110      00110111                  00010100                  010100...
M[7:0]                  00110111  00110111      00110111                  00110111                  001101...
```

Figure 11: Encrypted and Decryption Plain Text

Table 1: Device utilization summary of ICRLG

Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	4	126800	0%
Number of Slice LUTs	7	63400	0%
Number of fully used LUT-FF pairs	0	11	0%
Number of bonded IOBs	18	210	8%
Number of BUFG/BUFGCTRLs	1	32	3%

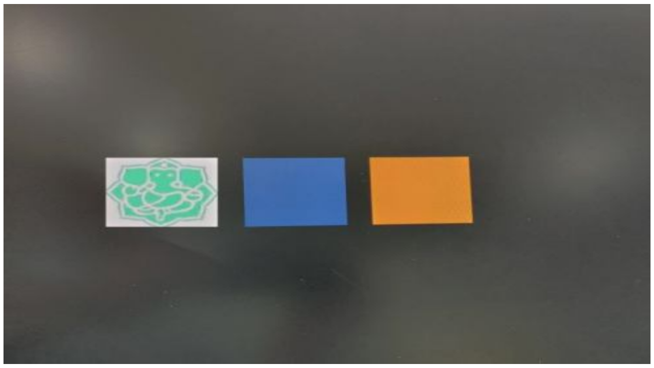


Figure 12: FPGA Implementation of Encrypted Image on Video Graphics Array (VGA) using ICRLG

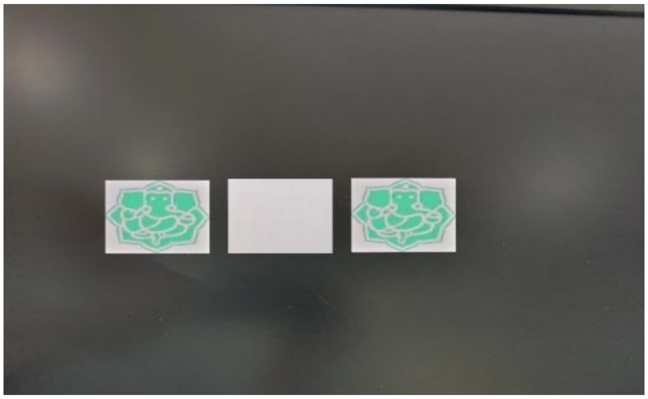


Figure 13: FPGA Implementation of Decrypted Image on VGA monitor using ICRLG

Figure 8 represents RTL schematic of ICRLG Encryption system. Whereas figure.9 signifies the RTL schematic of ICRLG Decryption system. RTL schematic output for both encryption and decryption process shown in figure.10. Simulation output of plain text encryption and decryption of ICRLG shown in figure.11. Device utilization Summary of ICRLG is shown in Table 1. FPGA Implementation of Encrypted Image using ICRLG is shown in figure.12. FPGA Implementation of Decrypted Image using ICRLG is shown in figure.13

8. CONCLUSION

ICRLG system is designed using Verilog HDL, and synthesized, simulated, and implemented on Vivado and targeted on Artix-7 XC7A35T-1-CPG236 architecture. ICRLG system consumes less resources but an added VGA peripheral consumes more resources. According to target architecture, device supports a wide variety of output peripherals like VGA, DVI, HDMI of different resolutions. Time consuming to understand the resolution of chosen target device and interface ICRLG system on VGA to display encrypted and decrypted images. Cryptology architecture is designed by PERES, CNOT, HING reversible gates. LUT, flip-flops, slices and frequency are improved in this ICRLG system. Day-to-day human beings are switching into a world with increasing digital information services and more necessity demand of cryptology. According to user needs cryptology architecture is more dynamic in nature to sustain vulnerability attacks in channel. E-Banking, shopping, database retrieval and recovery networks and government systems would need enhanced access management and data protection procedures to protect data from intruders.

REFERENCES

[1] Thapliyal H, M. B. Shri Nivas. **Novel Reversible Multiplier Architecture Using Reversible TSG Gate Computer Systems and Applications,** IJMER, Vol. 4, Iss. 1, pp. 159-167 Jan. 2014.

[2] W. D. Pan; M. Nalasani. **Reversible logic**, Volume: 24, Issue: I, IEEE Journals & Magazines pp. 38-41, Year:2005.
https://doi.org/10.1109/MP.2005.1405801

[3] Shikha Kuchhal, Rakesh Verma. **Security design of DES using reversible logic**, Volume 1, Issue 9, pp. 286-293, November 2012.

[4] Launder, R. **Irreversibility and heat generation in the computing process**, IBM J. Research and Development, pp. 183-191, 1961.
https://doi.org/10.1147/rd.53.0183

[5] Robert Wille**. Introduction to Reversible Circuit Design**, Electronics, Communication, and Photonics Conference, IEEE, 2011.

[6] Fushimi, M. and Tezuka, S. **The K-distribution of Generalized Feedback Shift Register Pseudorandom Numbers**, Communications of the ACM, volume 26, pp. 516—523, July 1983.

[7] S. Ergun and S. Ozoguz. **Truly Random Number Generators Based on a Non-autonomous Chaotic Oscillator**, AEU-International Journal Electronics & Communications, Vol. 61, No. 4, pp. 235-242, 2007.
https://doi.org/10.1016/j.aeue.2006.05.006

[8] Deepali P. Durgade, Mr. P. C. Bhaskar, Mr. B. P. Kulkarni, and P. D. Patil. **FPGA Based Authentication Unit Using Asymmetric Key Cryptography,** 14th ICSET-2017

[9] William Stallings. **Cryptography and Network Security, Principles and Practices**, 4th ed. Pearson Education, pp. 134-161, 2006.

[10] G. Jayamurugan**. Lossless and reversible data hiding in encrypted images with public-key cryptography, Digital Image Process**. 8 (6) 211–213,2016.

[11] Sailaja K L Srinivas Rao P, Ramesh Kumar P, **A new circle based symmetric key encryption technique for text data,** IJATCSE, Vol. 8, No 5, 2019.
https://doi.org/10.30534/ijatcse/2019/106852019

[12] Koduru Prasad Rao, Dr G Lavanya Devi, **Information Security Using Hilbert With Hash Value**, IJATCSE, Vol 8, No 5, 2019.
https://doi.org/10.30534/ijatcse/2019/96852019