International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

FPGA Implementation And Analysis Of RC7 Algorithm Using Reversible Logic Gates

Shailaja A., Krishnamurthy G.N

Abstract*: Lightweight cryptography is one of the efficient technologies that permit the confidentiality of communication through an insecure channel. Recently, several researchers have made a study on a lightweight block cipher in the field of cryptography. In this research paper we have concentrated on the design of lightweight block cipher with its performance evaluation and security analysis. We introduce RC7-RLGC algorithm, an FPGA implementation of Rivest's Cipher 7 (RC7) algorithm using reversible logic gates to encrypt the messages. The pseudorandom numbers are generated in Reversible Logic Gates Circuits (RLGCs) are used as key; this minimizes the resource utilization in encryption process. The proposed RC7-RLGC architecture has occupied less FPGA device utilization on LP-Virtex-6 device. It has occupied 13.04 % of LUTs, 10 % of flip-flops and 36.363 % of slices less than the existing RC7 algorithm.

***Index Terms*: Light Weight Cryptography, LBCs, Encryption, Decryption, RC-7, Reversible Logic Gates, FPGA.**

I. INTRODUCTION

Lightweight cryptography is the subject of designing lightweight ciphers. The lightweight ciphers perform well in resource constrained environments. Therefore, data security has become a difficult and an imperative problem in such environments [1]. Cryptography is the technique for hiding data, so that only authenticated receivers can view it. It is a powerful way of securing information in communication [2]. Lightweight focuses the better performance of block ciphers with low-power consumption. The lightweight block ciphers provide confidentiality for Low Resource Devices (LRD) by balancing the required security with minimal resource overhead. Hence, the researchers' further study about lightweight block ciphers cryptography with trade-offs between cost, performance and security [3], [5]. Recently, the radio frequency identification methods have achieved popularity due to their small size and low cost applications [6]. The key generation is significant factor in any type of cryptographic approach. It is important parameter for improving security level of an algorithm. Hence, key generation module should be designed in a way to improve the security of the cryptographic process. However, improving the randomness of the key must significantly ensure the strength of cryptography algorithm [7].

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Shailaja A*, Department of Computer science and Engineering, Visvesvaraya Technological University, Belagavi, Karnataka.
Dr. Krishnamurthy G.N., Principal, B N M Institute of Technology, Bangalore, India.

Nowadays, the researchers are focusing on optimizing hardware implementation of the standardized block ciphers including Ultra Lightweight Block Cipher (QTL) [8] [9], Extended Tiny Encryption Algorithm (XTEA) [10], International Data Encryption Algorithm (IDEA) [11] etc. Researchers have discussed how to modify a traditional lightweight block cipher like RC7 for communication applications [12]. Several techniques have been established for improving the performances of the cryptosystem, but there is a scope for developing the existing methods to further improve the security level and reduce complexity. The essential goal of this paper is to find out a roadmap of existing work in the area of lightweight cipher implementation. Here, the RLGC based RC7 architecture is proposed for encrypting information. The random numbers are generated in RLGC for symmetric encryption key. The major objective of the proposed RC7-RLGC architecture is to provide high encryption and decryption quality with minimum FPGA device requirement and computational time.

The composition of the proposed work is: A review of recent papers on encryption and decryption algorithms in the field of light weight cryptography is presented in section-2. Section-3, gives brief explanation of the RC7-RLGC architecture. Performance analysis and results of proposed work is discussed in section 4. Section 5 presents the concluding remarks of the work.

II. LITERATURE REVIEW

Many researchers have suggested several lightweight cryptography algorithms where power, memory size and footprint are the main constraints. In this section, review on some significant contributions of existing lightweight algorithms is presented. Subramanian et al. [13] proposed reliable hardware architecture for cryptographic block cipher LED and HIGHT. This research work implemented efficient error detection architectures including variants of re-computing with encoded operands and signature based techniques to find permanent & transient faults. An authenticated encryption algorithm was applied in cryptography to provide integrity, confidentiality to the message sent in communication channel. This paper showed that the proposed methods were applied to the case study of simple, lightweight block ciphers for providing authenticated encryption with connectsed data. Error simulations were performed utilizing Xilinx ISE tool. The transient and permanent faults are not properly detected; which may affect the function of the system security.

Ismail et al. [14] presented Generalized Fractional Logistic Map Encryption (GFLME) system which was implemented on Virtex-5 FPGA, XC5VLX50T with 58.358MHz of maximum clock frequency. The proposed design of GFLME map is suitable for generating pseudorandom number keys and its application in cryptography system. In this work, the size of encryption key depends on size of bus: 20-bit, 16-bit and 11-bit. The sensitivity analysis shows that the encryption algorithm improves high sensitivity to the fractional-order key. However, decreasing the size of bus makes the system weak against brute force attacks.

Zodpe, Harshali, and Ashok Sapkal [15] implemented Advanced Encryption Standard (AES) with enhanced security features. This research proposed a new technique for producing S-box value and key needed for encryption and decryption utilizing PN sequence generator. In this work, AES algorithm with a value of the modified S - box has obtained an appreciable throughput in limited clock cycles. A Pseudorandom number generator was designed by Linear Feedback Shift Register (LFSR). The proposed algorithm may not be suitable for large encryption message process.

M. Mozaffari - Kermani et al. [16] proposed an error detection method for a Light-weight block cipher (LBCs) implemented with XTEA. The proposed fault diagnosis techniques provided high error coverage at the expense of acceptable overheads on the FPGA platforms, making the hardware architectures of the XTEA more reliable. The proposed schemes could be used to protect the extremely sensitive and resource-constrained applications and the proposed method required more cost due its more occupied area. To overcome these issues, this paper presents RC7-RLGC architecture for improving the performance of both encryption/decryption processes.

III. PROPOSED METHODOLOGY

This section describes the modified RC7 architecture with RLG circuits, which is symmetric key ultra-lightweight block cipher for lightweight cryptography. The RC6 algorithm is already implemented for improving encryption efficiency. The RC7 algorithm uses six registers instead of four registers, which makes this as a better alternative to RC6. More secure and compact block cipher provides a better performance, which is a major advantage of the proposed RC7 encryption algorithm compared to existing algorithms. The proposed RC7 architecture takes less time to encrypt the data. The brief explanation of RC7-RLGC architecture is presented in the next section.

A. RC7-RLGC Architecture

The architecture of RC7-RLGC consists of six steps. For this research work the input image Lichtenstein.jpg (Fig 4.a) of size 128×128 is considered and each pixel is converted into binary. Each pixel size is 8- bits and entire image's pixels' size is 16384 bits. Initially, input image is read in MATLAB tool and here the image is converted into a binary format. In the next step, the binary value is transformed to text output. This text format is given as input to Verilog because the Verilog cannot directly read the image. The RC7 architecture requires a symmetric key for both encryption and decryption process. Hence, pseudorandom numbers generated using RLG circuit is used as key and is input to Verilog in the fourth step. In the fifth step, the Verilog output is converted to text format for both processes. The encrypted and decrypted text outputs are converted back to pixels, and the pixel values are converted into an image in the final step.

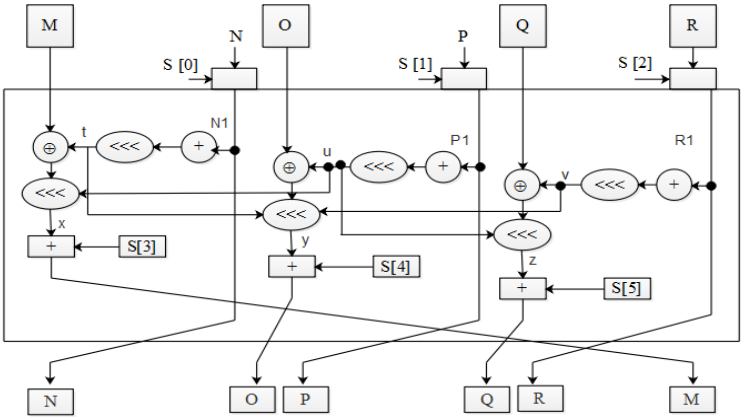

Fig. 1. Architecture of RC7-RLGC algorithm

Fig.1 shows the architecture of the proposed RC7. The algorithm consists of: input binary values stored in six w-bit input registers M, N, O, P, Q *and* R the number of rounds r, W- bit round keys represented as $S\ [0.\ldots\ldots\ldots 2r+1]$ and finally the output cipher text stored in M, N, O, P, Q *and* R. Here, 8-bit data is used as input. From this only 6-bits are considered for encryption process. This 6-bit input is stored in each registers. The final 6- bit (0-bit to 5- bit) key outputs are stored in S [0] through S [5].

Initially, value of N is added with key value S [0] and the output is represented as $N1$. The values are multiplied by $(2N1+1)$ after that, it is left shifted for three times and is represented as t.

The value stored in M is XORed with t, the output is shifted left by three. The value u is three times left shifted and the result is represented as x. In the final step, this x value is added to S [3], which is represented as M cipher text. Similarly the u *and* v are found the values, which are stored in registers P *and* R.

The values of the registers N, P *and* Q are added to S [0], S [1] and S [2], respectively. The output cipher texts are stored back in N, P *and* Q. The procedure of the proposed RC7 architecture is given as follows.

Procedure

$N = N + S[0]$

$P = P + [1]$

$R = R + S[2]$

$for\ i = 1\ to\ r\ do$

{

$t = (N \times (2N + 1)) <<< \lg w$

$u = (P \times (2P + 1)) <<< \lg w$

$v = (R \times (2R + 1)) <<< \lg w$

$M = ((M \oplus t) <<< u) + S[2i + 1]$

$O = ((O \oplus u) <<< t) + S[2i + 2]$

$Q = ((Q \oplus v) <<< t) + S[2i + 3]$

$M, N, O, P, Q, R = N, O, P, Q, R, M$

B. RLGC based Key Generation

In this section, we introduce a method for implementing encryption using reversible logic. Every logic gate utilized in a reversible logic circuit play a vital role. Reversible logic gates are the devices with same number of inputs and outputs with one-to one mapping, which helps to determine the output from the corresponding inputs and also the inputs can be recovered from their corresponding outputs [16]. For example, if 010 is input to the RLG circuit, the output produced is 101. Reverse logic occurs if it produces 010 as the output. The FPGA based simulation is very simple encryption process, which is designed by reversible gates. To design RLG any of the basic gates can be considered.

Fig. 2 shows the configuration of basic reversible logic gates used to design the key generation. The gates used are:

- SCL (Six Correction Logic) gate with *A, B, C and D* as inputs and *P, Q, R and S* as outputs.
- Toffoli gate with *A, B and C* as inputs and *P, Q and R* as outputs.
- Fredkin gate with *A, B and C* as inputs and *P, Q and R* as outputs.
- Feynman gate with *A and B* as inputs and *P and Q* as outputs.

The output of the gates is defined in the Fig. 2

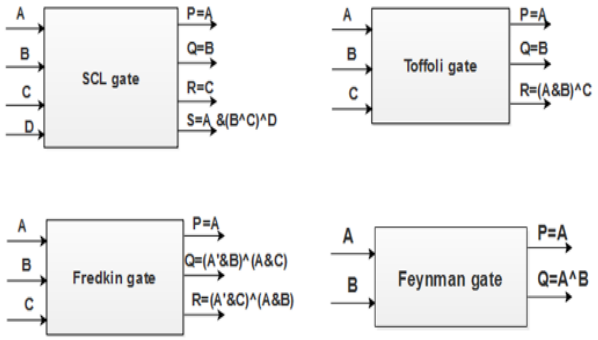

Fig. 2. Block diagram of basic reversible logic gates

The key generation process using Reversible Logic Gate Circuit (RLGC) is depicted in the figure below (Fig.3). Initially, the 8-bit data are stored in the register; these values are divided as Most Significant Bits (MSB 4-bit) and Least Significant Bits (LSB 4-bit). If counter value is zero, these separated values are given to the two different SCL gate as an input.

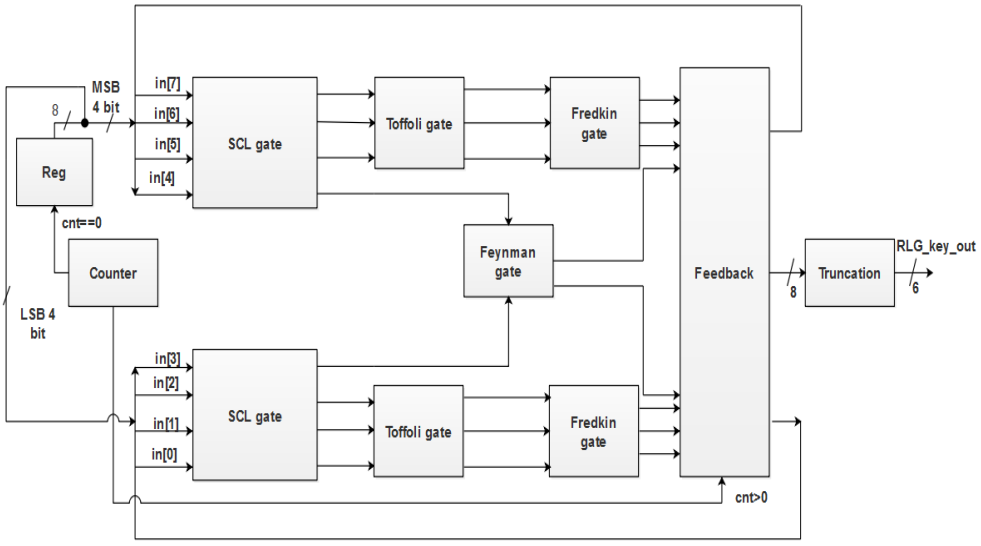

Fig. 3. Block diagram for key generation

- Inputs A, B and C of SCL gate produce outputs P, Q and R directly (Fig.2). S output is determined by XORing B and C and the result is ANDed with A. This intermediate result and D are XORed. The 3-bit SCL output is given to the Toffoli gate and 1-bit output is given to the Feynman gate.

- A and B inputs of Toffoli gate produce outputs P and Q. Output R is determined by ANDing A and B. Finally, this result and input C are XORed. These three outputs of Toffoli gate are fed as input to Fredkin gate.
- Feynman gate receives the two inputs from the two SCL gates (one from each gate). Input A determines the P (output) directly in Feynman gate. Input A and B undergo an XOR operation to produce the output Q.
- Fredkin gate receives three inputs from Toffoli gates. In Fredkin gate, input A determines P without any calculation. To determine Q, A' (complement of input A) and input B are ANDed and inputs A and C are ANDed. Perform XOR operation on the results obtained in previous step. To determine output R, complement of input A (A)' and input A are ANDed with input C and input B respectively. The results of these two outputs XORed to obtain R. The two cascade result is given to feedback. If the counter condition is greater than 0, the feedback is given as the input of the logic gates. Finally, the 8- bit output is given to truncation, to produces 6-bit RLG key output.

IV. RESULT AND DISCUSSION

The experimental results of the proposed RC7-RLGC architecture are discussed in this section. The RC7-RLGC architecture is implemented in the Xilinx tool by using Verilog code on an FPGA platform. Image based encryption process was done in this paper. Initially, an image was converted into a binary format by using MATLAB version 2018a. The binary value is given to Verilog as an input as because the VLSI tool does not directly accept the image format. The Xilinx ISE 14.1 tool is used for synthesis, simulation and generating the programmable file.

A. FPGA performance analysis

The FPGA platform is much suitable for VLSI implementations because of its flexibility, low power, and upward compatibility compared to the ASIC platform. Generally, the VLSI circuits for the bitwise algorithms require efficient performance and less latency under limited chip area and complexity because these circuits commonly require supporting High Data Rates (HDRs) of the communication networks. The performance of the RC7-RLGC architecture is evaluated in terms of LUTs, Flip Flops, Slices and frequency. The mean, variance and co-variance are analyzed for encrypted images, which represent the differences between input image and encrypted image.

Table I. Performance Comparison Of The Existing And Proposed Cryptographic Architecture

Target FPGA Devices	Cryptography Algorithms	LUT	Flip Flop	Slice	Frequency (MHz)	Required time (sec)
Virtex6 xc6vcx75t	QTL [8]	47/46560	78/93120	34/11640	228.78	2.765
	DROM-CSLA-QTL [9]	55/46560	71/93120	31/11640	248.17	2.770
	XTEA [10]	388/46560	15/93120	103/11640	70.168	9.298
	ID-XT-EA-LFSR [11]	37/46560	18/93120	16/11640	707.164	6.019
	RC7[12]	22/46560	20/93120	10/11640	545.687	4.235
	RC7-RLGC	**20/46560**	**18/93120**	**8/11640**	**440.306**	**2.135**
LP-Virtex6 xc6vlx75tl	QTL [8]	47/46560	78/46560	32/11640	188.04	3.428
	DROM-CSLA-QTL [9]	55/46560	55/46560	38/11640	204.165	3.434
	XTEA [10]	392/46560	15/93120	107/11640	73.99	9.836
	ID-XT-EA-LFSR [11]	37/46560	18/93120	15/11640	738.007	7.155
	RC7[12]	23/46560	20/93120	11/11640	458.365	6.354
	RC7-RLGC	**20/46560**	**18/93120**	**7/11640**	**353.732**	**2.199**
Virtex-7 Xc7vx330t	QTL [8]	47/204000	55/408000	36/51000	271.894	2.352
	DROM-CSLA-QTL [9]	55/204000	55/408000	36/51000	293.608	2.357
	XTEA [10]	364/204000	15/408000	105/51000	81.746	0.915
	ID-XT-EA-LFSR [11]	37/204000	18/408000	16/51000	823.588	2.145
	RC7[12]	30/204000	22/408000	15/51000	635.623	3.321
	RC7-RLGC	**27/204000**	**20/408000**	**13/51000**	**538.068**	**1.805**

Table 1 shows the performance comparison of the existing and proposed cryptographic architecture. The FPGA implementations are carried out on Xilinx family Virtex-6 and Virtex-7 with the target devices xc6vcx75t, xc6vlx75tl and Xc7vx330t. Here, the performance of the proposed RC7 architecture is compared with five efficient existing works such as QTL [8], DROM-CSLA-QTL [9], XTEA [10], ID-XT-EA-LFSR [11] and RC7[12]. In this research, both the existing and proposed architecture of RC7 is implemented in the Xilinx tool. The proposed architecture achieves the less area consumption on LP- Virtex6 xc6vlx75tl device The proposed

RC7-RLGC architecture has occupied less FPGA device utilization on LP-Virtex-6 device by 13.04 % of LUTs, 10 % of flip-flops and 36.363 % of slices than existing RC7 algorithm. From table 1, it is clear that RC7-RLGC architecture has obtained less number of LUTs, flip flops and slices than existing cryptography algorithm.

Hence, the RC7 architecture is designed for image encryption and decryption using efficient key design. The reduced values of these parameters determine reduction in area and time for image encryption in RC7-RLGC architecture.

Fig. 4. (a) Input image, (b) Encrypted image (c) Decrypted image

The proposed RC7-RLGC architecture is tested by using Lichtenstein image. Fig. 4 represents the sample input, encrypted and decrypted image for proposed work. Fig. 4 (a) and (c) reveal that decrypted image is similar to the input image and the input image is not affected in the encryption process by any type of attack. The proposed RC7-RLGC architecture provides high encryption and decryption quality with minimum FPGA requirement and system required time.

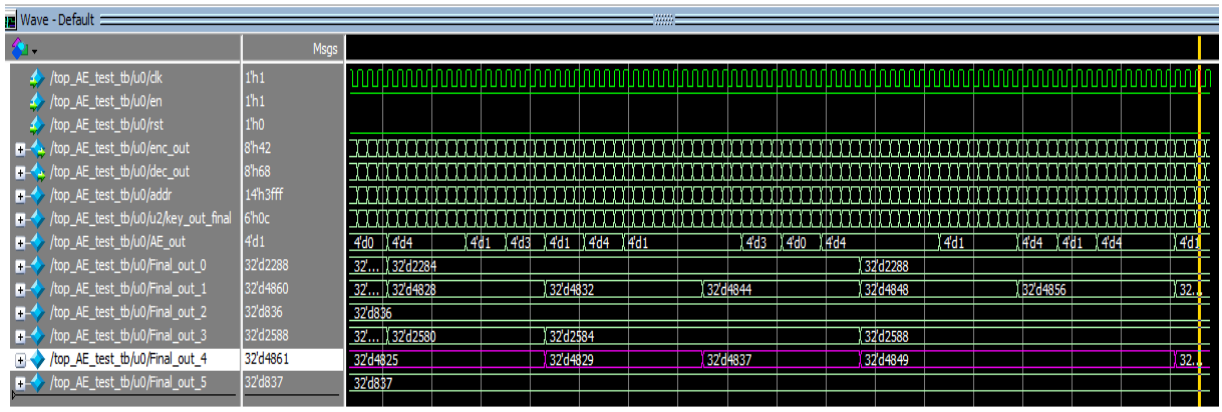

Fig. 5. Waveform of the RC7-RLGC architecture

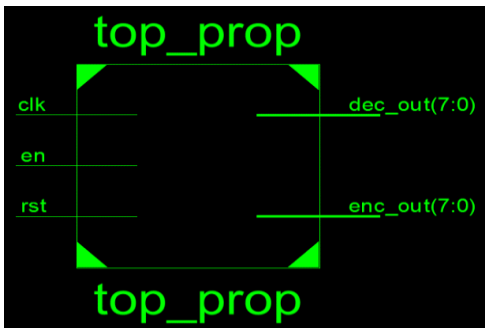

Fig. 6. Top module of the RC7-RLGC architecture

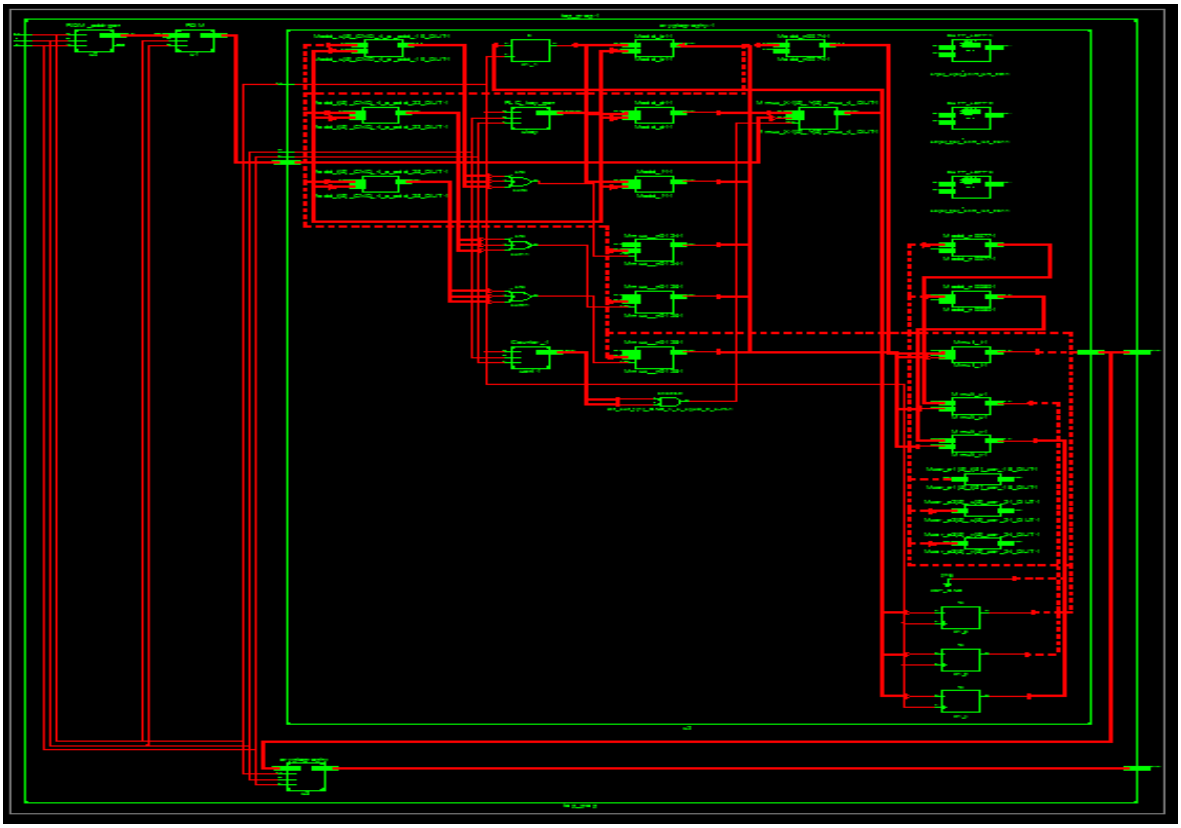

Fig. 7. Internal block of the RC7-RLGC architecture

Fig.5 shows the waveform of the proposed RC7-RLGC architecture with avalanche effect. Fig.6 shows the Register Transfer Level (RTL) view of the top module for RC7-RLGC architecture taken from the Xilinx software tool. The RC7-RLGC architecture has individual code for each block such as encryption process, the decryption process, and RLG circuit key schedule. Fig. 6 consists of the clock signal (clk), enable signal (en), reset signal (rst), dec_out (7:0), enc_out (7:0) and RLG_out (7: 0). Fig. 7 shows the internal block of the top module for the RC7-RLGC architecture in which all the internal blocks of main module are connected by using red colored wire.

B. MATLAB performance analysis

The Matlab performances of the encryption process are analyzed for different images: Lena, pepper, baboon and Lichtenstein by mean, variance and covariance. In table 2, the mean value gives the contribution of the individual pixel's intensity for the whole image. The variance is computed to detect how each and every pixel varies from the neighboring pixels and it employed in various regions.

The covariance is computed by how much two random variables change together. From the table 2, the proposed RC7 architecture has obtained 128.0326 of mean, 557450 of variance, and 56.0538 of co-variance for Lena encrypted image. 118.42 of mean, 540160 of variance, and 294.83 of co-variance for pepper encrypted image. 127.7268 of mean, 200260 of variance, and 45.6716 of co-variance for baboon encrypted image and 21 of mean, 174670 of variance, and 2.8939 of co-variance for Lichtenstein encrypted image.

Table II. Matlab Performance Evaluation Of Encryption Image For Various Images

Image	source	Mean	Variance	Covariance
Lena	Encryption image	128.032	557450	56.0538
Pepper	Encryption image	118.42	540160	294.83
Baboon	Encryption image	127.726	200260	45.6716
Lichtenstein	Encryption image	21	174670	2.8939

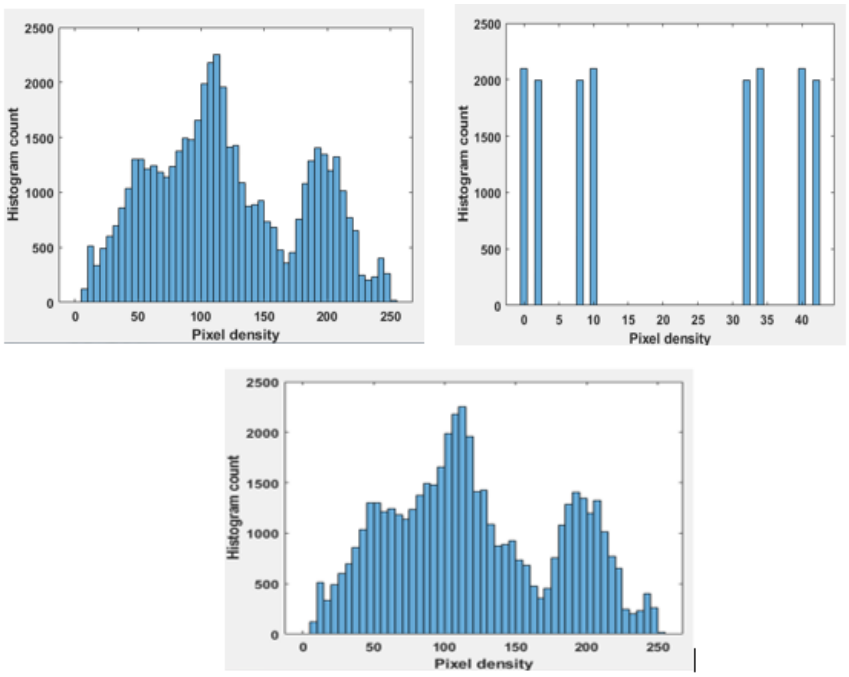

Fig. 8. (a) Input histogram (b) Encryption histogram (c) Decryption histogram

Fig.8 shows histogram of the input image and its corresponding encrypted and decrypted images. The histogram of the image generally changes even if there is a slight change in image. Here, the histogram of the input image and decrypted image are similar. The histogram of encrypted image is fairly uniform and different from the histogram of the input image which indicates that the proposed algorithm is efficient. Fig. 8 is evidence to show that the decrypted image is not affected by any attack. Hence, the image is safely transmitted to the receiver by using the RC7-RLGC architecture.

C. Security and Encryption Quality Analysis

In this section, security and encryption quality of the proposed algorithm is analyzed using avalanche effect and key sensitivity test.

a. Avalanche effect

In cryptography, avalanche effect is desirable property of block ciphers. A block cipher is said to have good avalanche effect if slight change (changing a one bit) in the input causes the output to change significantly i.e., half of the output bits must at least change. In order to analyze efficiency of block ciphers, a small change in either key or plaintext should cause significant change in cipher text. In the proposed work, the avalanche effect is computed by flipping/changing one bit in the plaintext and keeping the key constant. The image and key are converted to binary before the encryption. Here, the input image divided into blocks, each of 8 bits. One of the bits in the input block is flipped. The corresponding original and flipped blocks of data are XORed. The number of bits which have changed is computed. If the number is more or equal than the half the number of bits, then the algorithm is considered to have good avalanche, but still the algorithm is vulnerable to cryptanalysis as bits in cipher text are almost complement of each other, it may provide valuable information to the cryptanalysis. Fig. 5 shows the proposed RC7 architecture exhibits good avalanche effect with value 4.

b. Key sensitivity test

Initially, an image is encrypted using the test key K1. Then the least significant bit of the key is changed to obtain a new key K2 where K2 is (K1 – 1) or (K1 + 1) it depends on whether K1 is odd or even. Then the original image is encrypted using the new key K2. The two encrypted images encrypted using K1 and K2 are compared. If the cipher images differ significantly, then the algorithm is said to perform better. Now try to decrypt the encrypted image (encrypted using key K1) by using key K2 and decrypt the encrypted image (encrypted using key K2) by using key K1. Fig. 9 and 10 shows encrypted image with key K1 but decrypted using K2 and encrypted image with key K2 but decrypted using K1 respectively. The output has been retrieved without any degradation. The proposed algorithm does not reveal the original information. This observation reveals that the modified algorithm is as strong as the original one and the security is not violated.

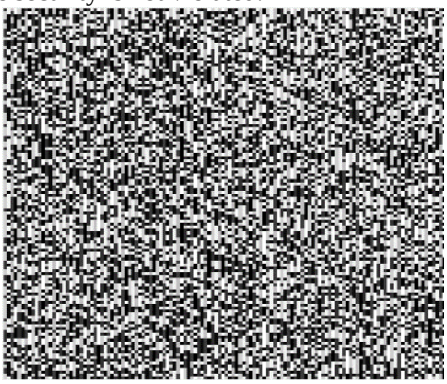

Fig. 9. Encrypted image with key K1, but decrypted using K2

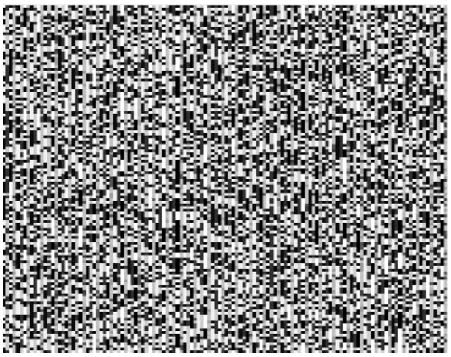

Fig.10 Encrypted image with key K2, but decrypted using K1

The RC7-RLGC architecture has improved the quality of the encryption process compared to the existing methods. From this results evaluation, the proposed architecture is much suitable for image encryption process in constrained computing environments.

V. CONCsLUSION

This paper presents a state of art investigation work in the area of popular data security approaches like Light Weight Cryptography. The proposed RC7 architecture was developed by two tools; MATLAB and Xilinx tool. The performance of the RC7-RLGC architecture was analyzed in the FPGA platform over high configurable Virtex devices such as Virtex-6, LP- Virtex-6 and Virtex-7. The RC7-RLGC architecture obtained strong security by incorporating randomized key generation RLG circuit. The proposed algorithm occupied less FPGA device utilization on LP-Virtex-6 device; 13.04 % of LUTs, 10 % of flip-flops and 36.363 % of slices than existing RC7 algorithm. It requires time of 2.199 sec for encryption process and operating frequency is 353.732 MHz. In future work, efficient lightweight cryptographic algorithms can be implemented for further minimizing the FPGA device utilization.

REFERENCES

1. H. Chen, and Y. Jui-Cheng. (2003). A new cryptography system and its VLSI realization. Journal of Systems Architecture, 49, pp. 7-9.
2. S. Dipti Kapoor, and N. Bajpai. (2010). Proposed System for data hiding using Cryptography and Steganography. International Journal of Computer Applications, 8, pp. 7-10.
3. J. Mohd, Bassam, T. Hayajneh, and A. V. Vasilakos. (2015). A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. Journal of Network and Computer Applications 58, pp. 73-93.
4. B.J. Mohd, T. Hayajneh, K.M.A. Yousef, Z.A. Khalaf, and M.Z.A. Bhuiyan. (2018). Hardware design and modeling of lightweight block ciphers for secure communications. Future Generation Computer Systems, 83, pp. 510-521.
5. B.J. Mohd, T. Hayajneh, Z.A. Khalaf, and K.M.Ahmad Yousef. (2016). Modeling and optimization of the lightweight HIGHT block cipher design with FPGA implementation. Security and Communication Networks, 9, pp. 2200-2216.
6. R. Sakthivel. (2016). VLSI Implementation of Lightweight Cryptography Algorithm. Advances in Systems Science and Applications 16, pp. 95-101.
7. C. Baskar, C. Balasubramaniyan, and D. Manivannan. (2016). Establishment of light weight cryptography for resource constraint environment using FPGA. Procedia Computer Science, 78, pp. 165-171.
8. L. Li, L. Botao, and H. Wang. (2016). QTL: A new ultra-lightweight block cipher. Microprocessors and Microsystems, 45, pp. 45-55.
9. A. Shailaja, and G.N. Krishnamurthy. (2018). Low Area FPGA Implementation of DROM-CSLA-QTL Architecture for Cryptographic Applications. International Journal of Network Security & Its Applications (IJNSA), 10.
10. A. Shailaja, and G.N. Krishnamurthy. (2019). VLSI Implementation of Hybrid Cryptography Algorithm using LFSR Key, International Journal of Intelligent Engineering and System (IJIES), 12, pp. 10-19
11. U. Pradesh, (2015). The RC7 Encryption Algorithm. International Journal of Security and Its Applications 9, pp. 55-60.
12. S. Subramanian, M. Mozaffari-Kermani, R. Azarderakhsh, and M. Nojoumian. (2017). Reliable hardware architectures for cryptographic block ciphers LED and HIGHT. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 36, pp. 1750-1758.
13. S.M. Ismail, L.A. Said, A.A. Rezk, A.G. Radwan, A.H. Madian, M.F. Abu-Elyazeed, and A.M. Soliman. (2017). Generalized fractional logistic map encryption system based on FPGA. AEU-International Journal of Electronics and Communications, 80, pp. 114-126.
14. H. Zodpe, and A. Sapkal. (2018). An efficient AES implementation using FPGA with enhanced security features. Journal of King Saud University-Engineering Sciences.
15. M. Mehran, T. Kai, R. Azarderakhsh, and S. Bayat-Sarmadi, (2014). Fault-Resilient Lightweight Cryptographic Block Ciphers for Secure Embedded Systems. IEEE Embedded Systems Letters, 4, pp.89-92.
16. K. Saranya, and V.K. Natarajan. VLSI implementation of reversible logic gates cryptography with LFSR key. Microprocessors and Microsystems, (2019)

AUTHORS PROFILE

Shailaja A obtained her B.E. degree in Computer science and Engineering from VTU in 2005, M.Tech degree in Computer science and Engineering from VTU in 2009. She is pursuing Ph.D. from VTU, Belagavi under the guidance of Dr Krishnamurthy G N. She is working as Assistant Professor in the Department of Computer science and Engineering, P D A College of Engg, Kalaburagi. She has published papers in international journals. Her area of interest includes Cryptography and Design and analysis of light weight block ciphers.

Dr.Krishnamurthy G N born on 15th March 1974, at Davangere, India. He obtained his B.E. degree in Electronics & Communication Engineering from Kuvempu University in 1996, M.Tech degree in Computer Science & Engineering from Visveswaraya technological University, India in 2000 and Ph.D. from Visveswaraya Technological University, India. He has served as Registrar (Evaluation) of Visvesvaraya Technological University, Belgaum, for a period of 2 Years on deputation from BNM Institute of Technology during the period from 22nd September 2010 to 21st September 2012 and again from 4th December 2012 to 2nd February 2013. Presently, He is serving as Principal, B N M Institute of Technology, Bangalore. He has published papers in national and international conferences, journals in the area of Cryptography. His area of interest includes Design and analysis of Block ciphers. He is a life member of Indian Society for Technical Education, India and International Association of Engineers.