International Journal of Research in Science and Technology
Volume 11, Issue 1 : January - March 2024
ISSN 2394 - 9554

HIGH PERFORMANCE ENCRYPTION AND DECRYPTION ALGORITHM USING REVERSIBLE LOGIC GATES FOR CRYPTOGRAPHIC DESIGN

Sudarsana Samhita S and Trinetra J
Department of Electronics and Communication Engineering, PSG Institute of Technology and Applied Research, Coimbatore, Tamil Nadu, India

ABSTRACT
The science behind thehighest levels of encryption and decryption – cryptography, emphasizes on data security and privacy. With the elevating issues on cybercrimes and data tampering, it is highly important to use methodologies pertaining to their solutions. Correspondingly, the usage ofReversible Logic Gates (RLG) are used in order to implement this proposal. With the fast-growing technologies, several techniques are available in this regard. But the statistical role of RLG in low power CMOS, nanotechnology, cryptography, digital signal processing, optical and quantum computing is huge. It reduces circuit complexity and garbage outputs significantly. Integrating RLG with a pseudo random generator such as Cellular Automata (CA) and Linear Feedback Shift Register (LFSR), improvises the data confidentiality. Security of data watermarking could also be done using the Least Significant Bit (LSB) method. Reversible Logic Gates Cryptographic Design (RLGCD) exhibits a significant growth in performance when compared to other conventional systems.

I.INTRODUCTION
Cryptography is the process of providing secure information in the presence of adversaries. It involves conversion of the data into a different format during transmission, and decrypting to bring back the original data or the plain text. This could be done by generating unique random keys using pseudo random key generators like cellular automata. This also reduces the number of iterations. Cellular automata architecture aids in high performance ASIC and FPGA.

Encryption involves the conversion of a readable message into a non-readable format. It is one of the most secure processes in cryptography. Reversible Logic Gates exhibits lossless information transfer without power dissipation. A Modern cryptography algorithm provides security for the data in the same manner as RLG, but it becomes difficult to implement it in complex environments. Other algorithms include Quantitative Trait Loci (QTL) and Tweakable Enciphering Scheme (TES). QTL, in general, provides low resolution when compared to RLG. One of the major challenges in VLSI, being the heat dissipation, is reduced without the loss of information, by reversible computation. This results in maintaining the entropy of the system. In order to consume low power as well as provide high security, RLG is highly preferable.

The composition of the research work is as follows: Section - 2 presents a survey on the recent papers in the design of cryptography. Section – 3 covers the RLGCD architecture. In Section – 4, the comparative results and conventional methods are described. Section – 5 includes the concluding remarks of the research paper.

II. LITERATURE SURVEY

1. ***Applications of Reversible Logic in Cryptography and Coding Theory***
There are various research reversible transformations that occur in the world of cryptographic algorithms. The coding and decoding techniques that are reversible are considered which include Differentia Manchester, Bipolar AMI, etc. The different approaches cover various factors such as scalability and include certain metrics like quantum cost and gate count. The three types of synthesis approaches were taken into account by which the functionality was analyzed. However, it lacks synthesized netlist and has high cost.

2. ***Encryption Using Reconfigurable Reversible Logic Gate and Its Simulation in FPGAs***
Complete scheme for 8-bit data encryption is described. Conventional methodologies have been reaching their saturation stages,hence the designing solutions for encryption were covered. Different substitution encryption methods were used along with different cascading keys. The concept of reconfigurable reversible gates was used wherein custom hardware accelerators can be implemented. Application specific hardware could also be developed using reconfigurable RLG. The paper enabled any 32 4 – input reversible gate from the NCT library. Reconfigurable computing had timing and consistency issues. Also, the development phase for the same is still emerging.

3. ***An Efficient Reversible Cryptographic Circuit Design***
With the aim of reducing the quantum cost and number of garbage outputs,a novel design of the Montgomery Modular Multiplier was proposed. The system design was acyclic and a private key exponent was generated.

ISSN 2394 - 9554

Further improvement involved applying the quantum controlled low-cost basic logic gates. Modular Multiplier takes more time to compute while dealing with large number of bits. The area per chip was also increased.

III. CHALLENGES IN CRYPTOGRAPHY

One of the critical problems people face today is lack of data and information security. In all modern authentication related applications, secure communication is very essential for which cryptography is must. Thus, encryption of data is a critical security measure to protect data. Some of the major concerns in a cryptosystem are:

- To improve less systematic key generation
- Unstructured FPGA design
- To overcome the inability to generate efficient test patterns
- Lack of algorithms that provide high security and data protection
- Slower and inefficient performance

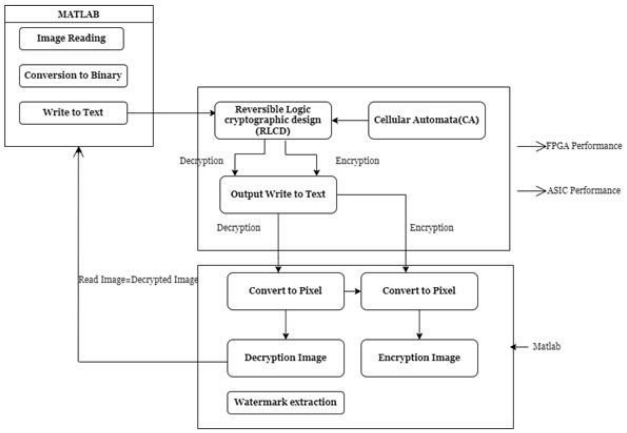

Fig.1: Overall block diagram.

PROPOSED ALGORITHM

Reversible Logic Gates (RLG):

The concept of reversibility implies that the information can never be lost. Logical reversibility can be achieved only after physical reversibility is employed. The logic behind reversible circuit portrays the ability to uniquely recover the input vector from the output vector. There is a presence of one-one correspondent mapping between the inputs and outputs. Usually, computing systems dissipate heat when voltage levels change from positive to negative; bits from zero to one. In case of reversible systems, the voltage levels are not changed, whereas the charges are subjected to mobility in terms of nodes. This results in minimal loss of energy for a very short interval of time. The conditions required for a circuit to be reversible are:

- Equal number of inputs and outputs
- Mapping between each input and corresponding output

A particular data being give to a circuit, if the same data is retrieved back, the circuit is said to be reversible. The entire reversible circuit is designed using minimum number of reversible logic gates. The parameters involved in the working of reversible logic gates are as follows:

a. Constant Inputs:

The inputs are to be maintained at a logic of either 1 or 0.

b. Garbage Outputs:

Number of unused outputs during synthesis are labelled as garbage outputs. The relation between constant inputs and garbage outputs are given as:

Output + garbage = Input + constant input

ISSN 2394 - 9554

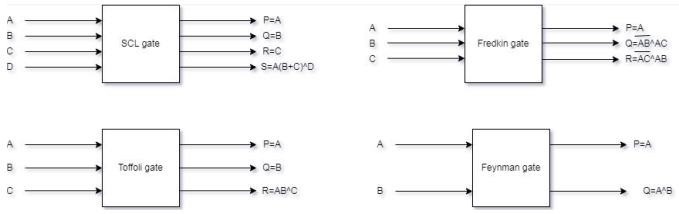

Fig.2: RLG

C. Quantum Cost:
This is calculated starting from the primitive gate, by knowing the number of primitive reversible logic gates. The Quantum costof 2 × 2 gate is represented as 1 as well as 1 × 1 gate quantum costis represented as 0.

The RLG that are used to design the cryptographic system are: Feynman gate, Fredkin gate, Toffoli gate and SCLgates. The working principle is proposed as:

- **Step 1:** The input image is converted to binary in MATLAB, where image watermarking is also done.
- **Step 2:** With the help of LSB Watermarking, the input image is converted to a binary image.
- **Step 3:** The pixel values of the binary image are noted in a text file in MATLAB.
- **Step 4:** The key generation is done by cellular automata.
- **Step 5:** The text file that is generated in MATLAB is provided as input to Verilog, where encryption and decryption is performed.
- **Step 6:** The encrypted and decrypted files are written in text files in Verilog to verify the output.
- **Step 7:**In MATLAB, the pixel values are recovered from the encrypted and decrypted binary text files. The images are then generated from the pixel values.
- **Step 8:** The decrypted image is same as the input image.
- **Step 9:** The decrypted image is used to recover the watermarks.
- **Step 10:** The FPGA performances are then evaluated using Verilog.

LSB WATERMARKING:
Least Significant Bit Watermarking is one of the simplest image watermarking methods. The process begins by inserting watermark into an image resulting in a watermarked image. The decoder is designed in such a way that it is able to detect both watermarked and unmarked input. A threshold is set up by the decoder based on the proportion of similarity. If the received image matches with the threshold, the watermark is detected and the data belongs to the user, else the data does not belong to the user. These changes cannot be detected by human eye.

Watermark is done in the third or fourth LSB of the image, since simple watermarking can survive transformations like addition of noise. Insertion of secret data in these positions is rare, hence the security is enhanced. The original input image is read in MATLAB, followed by the transfer of watermark to a binary value. The data is then embedded into the third and fourth positions of LSB. This corresponds to the watermarked input image. The reverse embedding is done in watermark extraction process. The length is extracted first, followed by the data. The binary data that is obtained is then converted back to the character, thus giving the watermark, indicating completion of the process. In case of colour image watermarking, this is done in blue component of the image, as it is less sensitive to human visuals.

ENCRYPTION:
The 8-bit binary word in pixels: i[0], i[1], i[2], i[3], i[4], i[5], i[6], i[7] are fed into the SCL gate. They produce four result bits. The first three LSB bits from the below SCL gate produces output bits which performs Toffoli gate operation. Similar operation is performed for the upper SCL gate. The remaining output bits from both SCL gates perform Feynman gate operation. Outputs of both Toffoli gates perform Fredkin gate operation. Both Fredkin and Feynman gate outputs are connected to XOR gate where key generator is fed. The desired output is thus generated as binary image pixel value: e[0], e[1], e[2], e[3], e[4], e[5], e[6], e[7].

ISSN 2394 - 9554

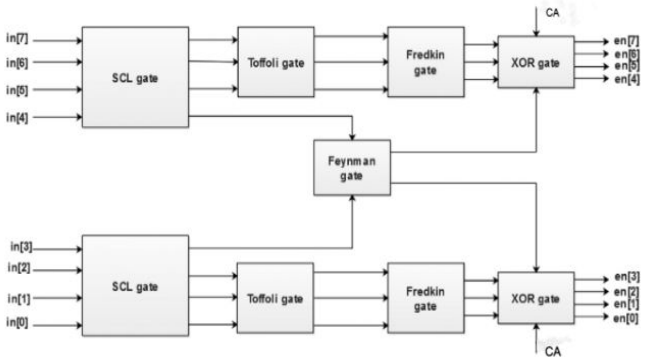

Fig.3: Encryption process

DECRYPTION

Since this is just the reverse operation of encryption, the output of encryption is fed as input here. XOR operation is performed between encrypted pixel bits and the random key generated. It is followed by the operation of four reversible logic gates, with the output being obtained at SCL gate. The block diagram of the decryption process is given below:

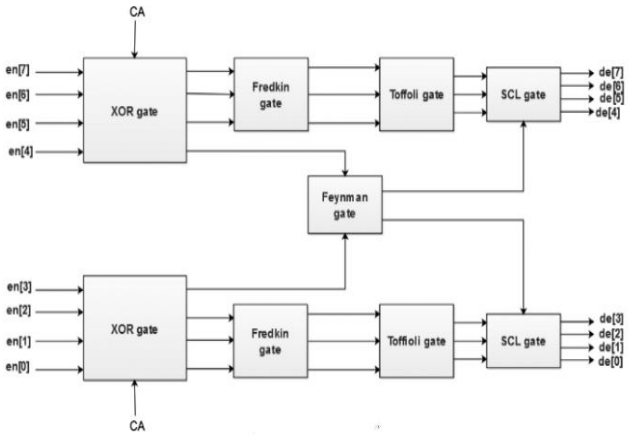

Fig.4: Decryption process

KEY GENERATORS:

LINEAR FEEDBACK SHIFT REGISTERS:

It is used to generate random key patterns. Considering 4-bit LFSR, it consists of 4 flip flops and an XNOR gate. First of all, a seed value is given to the flip flop, which is random. Then a random test pattern is created when it is clocked, by shifting the values using feedback. The feedback polynomial determines the number of random sequence generated. The maximum count value is 2^(n-1). A more secure cryptographic system is achieved using LFSR as it is suitable for both high and low speed applications including stream ciphers.

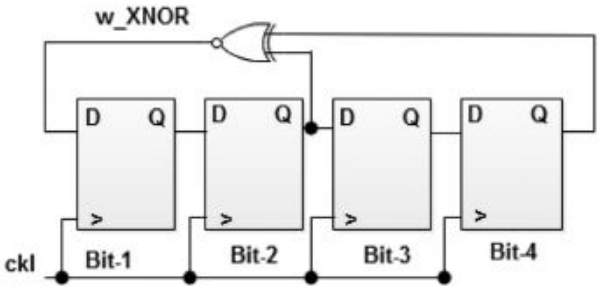

Fig.5: LFSR Block diagram

CELLULAR AUTOMATA:

Today's VLSI devices are more complex and standard testing procedures are not suitable as the chips become untestable. Therefore BIST (built in self-test) has been established where the circuit tests itself reducing test times and memory demands. LFSR and CA are two of the most common methods used for test pattern generation in BIST circuits and are simple to implement. Test pattern generation is of key importance for a BIST system. LFSRs are traditionally being used for this purpose, but there are many drawbacks. Hence, CA is

ISSN 2394 - 9554

gaining more popularity as they can be easily modified and also have high performance characteristics. Test patterns have to be more random in nature, which is not achievable to that extent using LFSR. CA generates highly random vectors which help in fault detection such as stuck-open faults, delay faults etc.

Cellular Automatas are basically a collection of nodes/cells formed by collection of flip flops.They are used to design complex systems. They are related to their neighbours logically using XOR gates. The logical relation by which a node and its neighbour are related, are called rules and the most popularrules are 90 and 150.

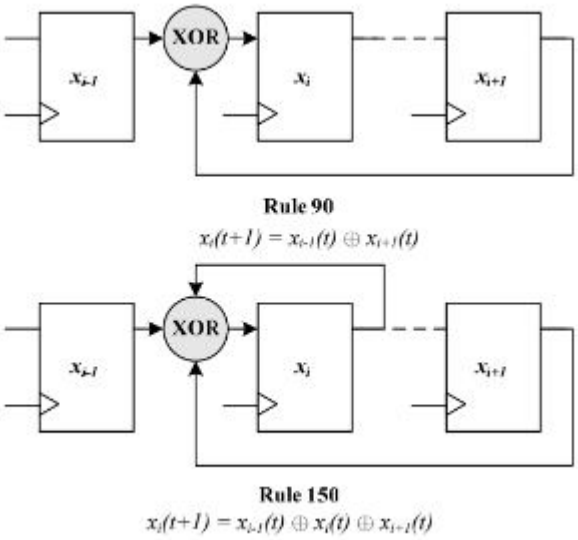

Fig.6: Rule 90 and Rule 150

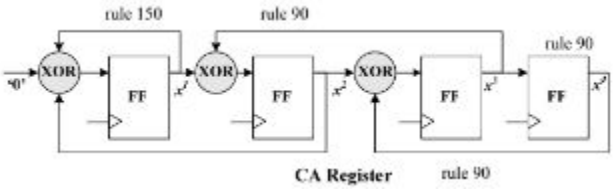

Fig.7: Cellular automata block diagram

IV. COMPARISON AND ANALYSIS

By analysing the two methods, it is found that one of the major drawbacks of LFSR is inefficient test pattern generation. They generate patterns parallelly and are strongly correlated due to shifting of data whereas, CA does not involve shifting of data. Secondly, LFSR's have feedback from their conclusion nodes. This means that if the pattern length has to be changed an update or an entire redesign is required. But in case of CAs the pattern length can be easily changed by cascading, since they do not have feedback. In terms of speed of operation, CA is higher and provides better performance. It serves to be more flexible and CAD friendly. Thus, it happens to be the best alternative for the conventional LFSR's.

V. CONCLUSION

This paper covered the cryptographic design using reversible logic gates such as SCL, Toffli, Feynman and Fredkin gates with less access time. The processes executed in MATAB include input image, binary conversion, along with output images and verification of histograms. About 20.47% delay, 8.4% of power was reduced in ASIC 180nm and 45nm technology, when compared to the conventional methods. The advancements in this area to improve the performances in ASIC and FPGA are still in progress.

REFERENCES

[1] G. Chandran, H. M. M. C and A. G, "VLSI Implementaion of Image Encryption and Decryption Using Reversible Logic Gates," 2020 International Conference on Power Electronics and Renewable Energy Applications (PEREA), 2020, pp. 1-6, doi: 10.1109/PEREA51218.2020.9339781.

[2] Karunamurthi, Saranya&KrishnasamyNatarajan, Vijeyakumar. (2019). VLSI Implementation of Reversible Logic Gates Cryptography with LFSR key.Microprocessors and Microsystems.69. 10.1016/j.micpro.2019.05.015.

[3] B. Mondal, K. Dey and S. Chakraborty, "An efficient reversible cryptographic circuit design," 2016 20th International Symposium on VLSI Design and Test (VDAT), 2016, pp. 1-6, doi: 10.1109/ISVDAT.2016.8064874.

[4] H. Thapliyal and M. Zwolinski, "Reversible Logic to Cryptographic Hardware: A New Paradigm," 2006 49th IEEE International Midwest Symposium on Circuits and Systems, 2006, pp. 342-346, doi: 10.1109/MWSCAS.2006.382067.

[5] J. C. Cerda, C. D. Martinez, J. M. Comer and D. H. K. Hoe, "An efficient FPGA random number generator using LFSRs and cellular automata," 2012 IEEE 55th International Midwest Symposium on Circuits and Systems (MWSCAS), 2012, pp. 912-915, doi: 10.1109/MWSCAS.2012.6292169.

[6] D. Datta, B. Datta and H. S. Dutta, "Design and implementation of multibit LFSR on FPGA to generate pseudorandom sequence number," 2017 Devices for Integrated Circuit (DevIC), 2017, pp. 346-349, doi: 10.1109/DEVIC.2017.8073966.

[7] A. Kaur and S. Singh, "A hybrid technique of cryptography and watermarking for data encryption and decryption," 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2016, pp. 351-356, doi: 10.1109/PDGC.2016.7913175.

[8] S. Mishra and A. Dastidar, "Hybrid Image Encryption and Decryption using Cryptography and Watermarking Technique for High Security Applications," 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), 2018, pp. 1-5, doi: 10.1109/ICCTCT.2018.8551103.

[9] M. Mohurle and V. V. Panchbhai, "Review on realization of AES encryption and decryption with power and area optimization," 2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), 2016, pp. 1-3, doi: 10.1109/ICPEICES.2016.7853276.

[10] J. Saturwar and D. N. Chaudhari, "Secure visual secret sharing scheme for color images using visual cryptography and digital watermarking," 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017, pp. 1-4, doi: 10.1109/ICECCT.2017.8117849.

[11] J. Rajski, G. Mrugalski and J. Tyszer, "Comparative study of CA-based PRPGs and LFSRs with phase shifters," Proceedings 17th IEEE VLSI Test Symposium (Cat. No.PR00146), 1999, pp. 236-245, doi: 10.1109/VTEST.1999.766671

[12] M. Bryk, K. Gracki, P. Kerntopf, M. Pawłowski and A. Skorupski, "Encryption using reconfigurable reversible logic gate and its simulation in FPGAs," 2016 MIXDES - 23rd International Conference Mixed Design of Integrated Circuits and Systems, 2016, pp. 203-206, doi: 10.1109/MIXDES.2016.7529732.

[13] P. H. Bardell, "Analysis of cellular automata used as pseudorandom pattern generators," Proceedings. International Test Conference 1990, 1990, pp. 762-768, doi: 10.1109/TEST.1990.114093.

[14] A. Bamatraf, R. Ibrahim and M. N. B. M. Salleh, "Digital watermarking algorithm using LSB," 2010 International Conference on Computer Applications and Industrial Electronics, 2010, pp. 155-159, doi: 10.1109/ICCAIE.2010.5735066.

[15] P. D. Hortensius, R. D. McLeod, W. Pries, D. M. Miller and H. C. Card, "Cellular automata-based pseudorandom number generators for built-in self-test," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 8, no. 8, pp. 842-859, Aug. 1989, doi: 10.1109/43.31545.