ISSN: 1672 - 6553

JOURNAL OF DYNAMICS AND CONTROL

VOLUME 9 ISSUE 2: 11 - 21

MATHEMATICAL MODELING AND SYNTHESIS OF REVERSIBLE CRYPTOGRAPHIC LOGIC

Premanand K. Kadbe[1], Shriram D.Markande[2]

[1]Department of Electronics and Telecommunication Engineering, G.H.Raisoni College of Engineering and Management, Wagholi, Pune, Maharashtra, India

[2]Department of Electronics and Telecommunication Engineering, Sinhgad Institute of Technology and Science (SITS,) Pune, Maharashtra, India

JOURNAL OF
DYNAMICS AND CONTROL

DOI: https://doi.org/10.71058/jodac.v9i2002

MATHEMATICAL MODELING AND SYNTHESIS OF REVERSIBLE CRYPTOGRAPHIC LOGIC

PREMANAND K. KADBE[1*], SHRIRAM D.MARKANDE[2]

[1] Department of Electronics and Telecommunication Engineering, G.H.Raisoni College of Engineering and Management, Wagholi, Pune, Maharashtra, India
[2]Department of Electronics and Telecommunication Engineering, Sinhgad Institute of Technology and Science (SITS,) Pune, Maharashtra, India

***Corresponding Author: premanand.kadbe.phdetc@ghrcem.raisoni.net**

Abstract: *Reversible logic has emerged as a pivotal area of study in the realm of computing, primarily due to its potential for energy efficient computation. Reversible cryptographic logic is an important area in applications such as signal processing, nanotechnology, bio-information, low power and lightweight applications and cyber security. The area and power constraints are as well taken into account of cryptographic protocol. In addition, intruders and hackers may snoop or modify identified data sent over the channel. Reversible cryptographic logic can be installed to prevent this situation. For this there is a need to study with optimal metrics viz. quantum cost, area, and performance. The feedback shift register is used for encryption and decryption techniques in a symmetrical way. This paper presents a comprehensive mathematical modeling framework for reversible logic circuits, focusing on the fundamental principles that govern their operation. We explore various reversible gate designs, analyze their operational efficiencies, and derive mathematical expressions that describe their behavior. By employing tools from combinatorial optimization and linear algebra, we investigate the trade-offs between circuit complexity and energy consumption. The modeling framework is validated through simulation results, which illustrate the advantages of reversible logic over traditional irreversible circuits in specific applications. Our findings highlight the significance of reversible logic in advancing quantum computing, low power digital systems and sustainable computing paradigms.*

Keywords: *Reversible logic, Cryptography, Plaintext, Ciphertext, Encryption, Decryption*

1. Introduction

There is always private data and sensitive data over computer network or internet for global communication and hence confidentiality, data availability and data integrity can be threatening. Importance of information about events in daily life and each of the growing memory demands has become an important asset. Message needs to be protected from illicit party.

Some experts claim that encryption has emerged someday voluntarily after the invention of writing diplomatic documents to wartime applications for battle plan. Therefore, in a new form cryptography appeared shortly after its widespread use and development of computer communication. With data, encryption is required if communication through unreliable media includes almost all networks, especially the Internet. Reversible computing is the computational process which is somewhat reversible. Reversible computing is commonly seen as an unconventional form of arithmetic.

Reversible logic circuit design is a trend concept to reach zero waste of energy. Designs based on reversible logic require less reversible gates to be consumed and reduces the generation of waste and also reduces the total amount of constant input. However, the computational requirements of each encryption algorithm are more complex. Built-in symmetric encryption algorithm is used to improve security ability to change the position at the same time in a bit-level sequence. But these are the approach required multiple rounds, increasing both computational time and hardware costs. Reversible logic is used to run all lossless processes and power consumption is almost zero. In a reversible logic design, the output pattern can be used to restore the input pattern to avoid information loss.

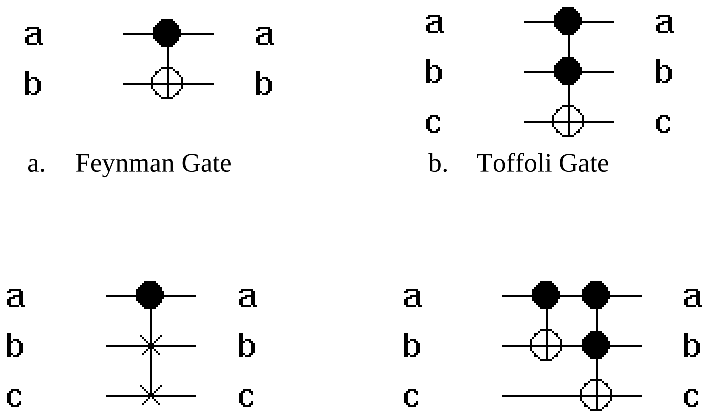
DOI: https://doi.org/10.71058/jodac.v9i2002

The remaining part of this article is organized as follow: Section 1.1 discusses basics of reversible logic, 1.2 discusses cryptography followed by their utilization in encryption and decryption methods and entropy evaluation in sections 1.3 and 1.4 respectively. The structural similarity metric measurements and chosen-plaintext assault evaluation are described in brief in section 1.6 and finally reversible logic synthesis of cryptographic circuits is mentioned in section 1.7.

1.1 Reversible Logic

According to Moore's Law, the transistor density doubles every 18 month. This allows CMOS devices to reach higher levels of Scale-down integration. Because of the physical limits of the CMOS decision has already been achieved and researchers focus on new device architectures and alternative technology to mitigate defects in CMOS technology. According to Landauer, during the calculation there is a loss of kT ln (2) joule energy information that is the basic lower limit for lost Energy dissipation. Bennett later said it was close to zero dissipation possible if calculated without information destruction. Heat dissipation currently the cause of information loss is trivial, but it contributes significantly if Moore's Law persists. Reversible computing is one of the options you can use to recover your input information from the output power consumption and fault detection circuit. On the other hand, the traditional method of error detection is not direct. The following constraints apply to reversible logic circuits. Fanout is not allowed. Feedback from the gate is not allowed. Output to input, equal number of I / O, presence of ancilla, and disposal of garbage, etc. The attributes of reversible logic circuits are the most difficult of the ones Reversible computing system.

Figure 1 shows a basic reversible logic gate with inputs on one side and the same number of outputs on the other side whereas in Figure 2 the output lines are defined with the given expression for output logic level are depicted. Figure 1.3 shows the various reversible logic gates. All gates in the Figure 1, and Figure 3 are implemented and synthesized using 2x2 and 3x3 toffoli gates.



a. Feynman Gate

b. Toffoli Gate

c. Fredkin Gate

d. Peres Gate

Figure 1. Basic Reversible Logic Gates (a) Feynman Gate; (b) Toffoli Gate; (c) Fredkin Gate; (d) Peres Gate.

DOI: https://doi.org/10.71058/jodac.v9i2002

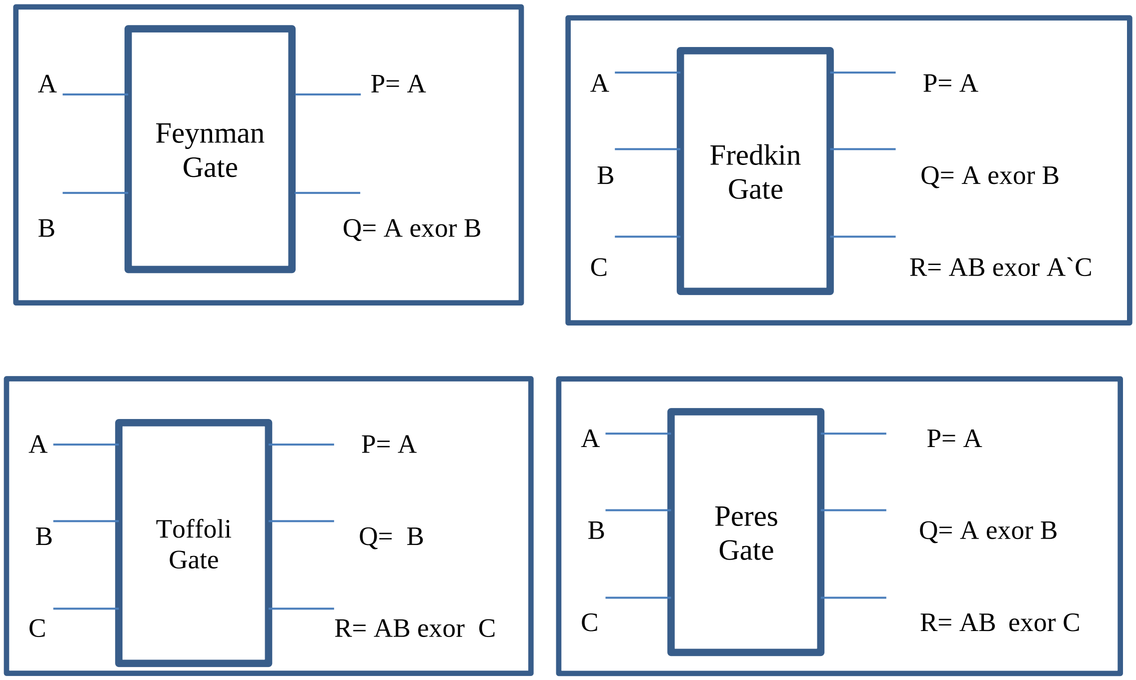
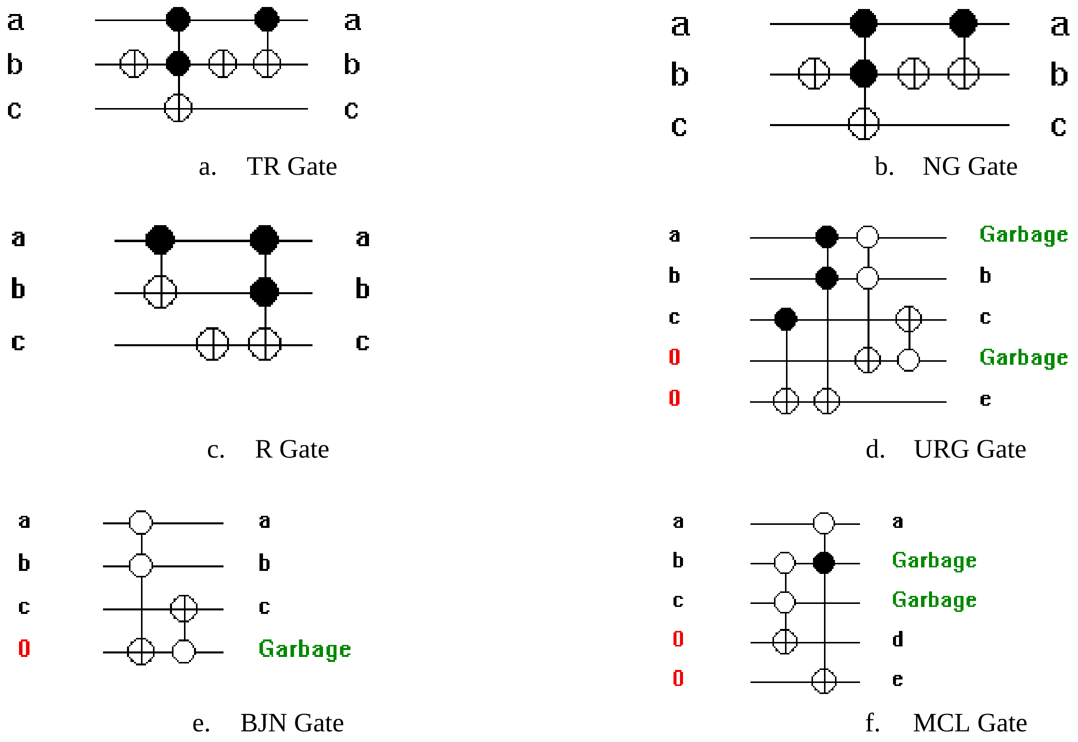


Figure 2. Basic Reversible Logic Gates block schematic



a. TR Gate

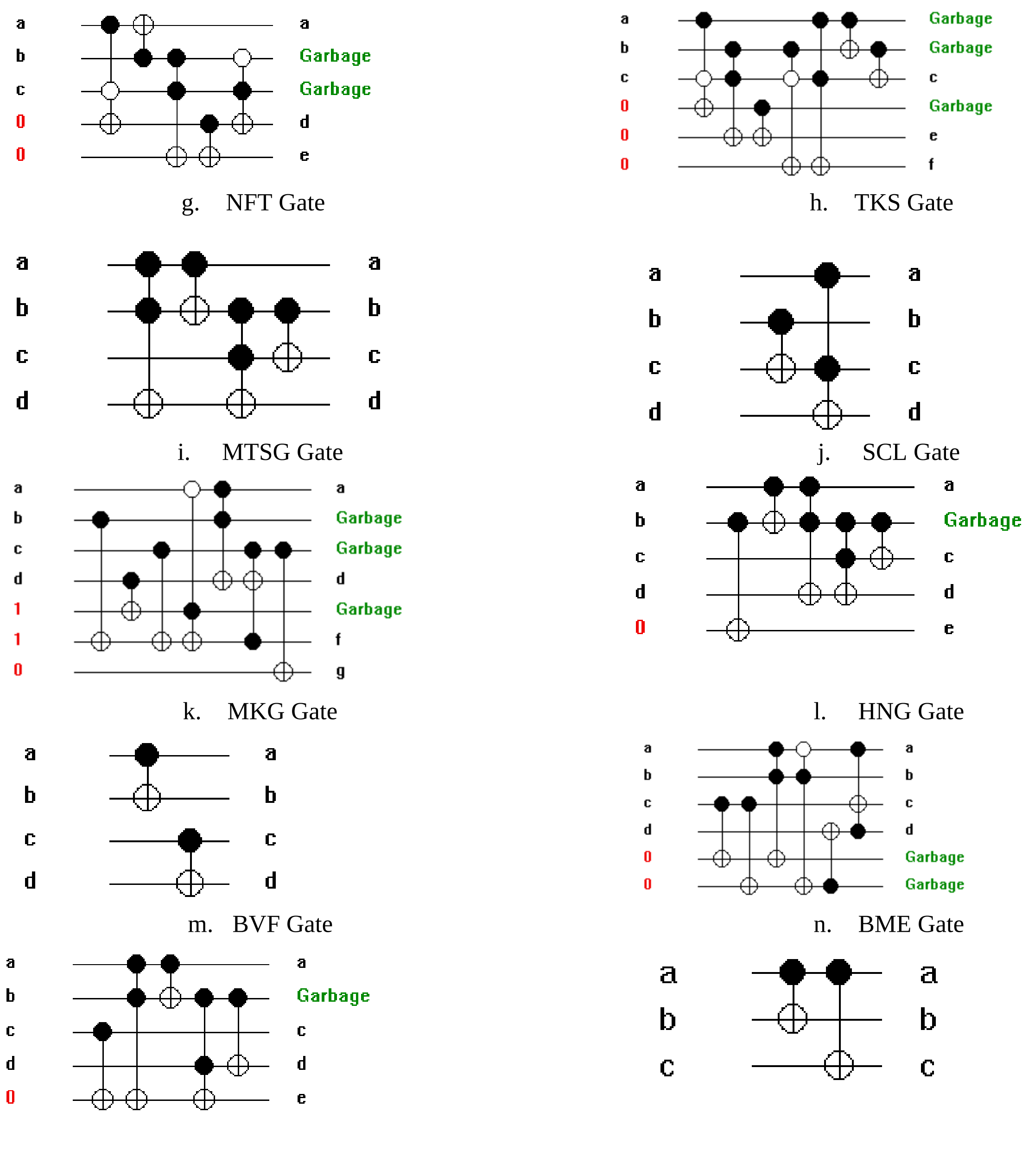
b. NG Gate

c. R Gate

d. URG Gate

e. BJN Gate

f. MCL Gate



g. NFT Gate

h. TKS Gate

i. MTSG Gate

j. SCL Gate

k. MKG Gate

l. HNG Gate

m. BVF Gate

n. BME Gate

o. DPG Gate

p. Double Feynman Gate

Figure 3. Different Reversible Logic Gates

The logic 0 constant input is used to extend a particular input line and the logic 1 constant input is used to have the complement of the selected input. Garbage lines are also used by some of the implemented logic gates. These implemented gates may not be in a quantum cost optimized format, but they do follow the equation for a single output line.

1.2 Cryptography

Encryption refers the science of crypting a message with the intention of only the intended recipient can decrypt the received message. Encryption is central to data security. It not only ensures the confidentiality of the message, but also helps to provide message integrity, authentication, and digital signatures. The first message or document sent is called plaintext, and the encrypting version is called ciphertext. Plaintext and ciphertext are binary strings of the same length. The original plaintext is encrypted whereas original plaintext restoration process is decryption. Cryptography is categorized broadly as private key and public key cryptography. The encryption or public key that should be known to the outside world and a private decryption or private key should be kept secret. Commonly used private key encryption algorithms comprise Data Encryption Standard, Advanced Encryption Standard, Blowfish, RC4, and public key encryption such as AES. Plaintext messages can be hidden in two ways. Steganography obscures the existence of the message, while encryption makes the message incomprehensible to foreigner through a range of text transformations.

2. Literature review:-

Computed Aided Design (CAD) is crucial for optimizing noisy intermediate scale quantum (NISQ) systems, using gate-based models for quantum operations. The proposed CAD Tool for Quantum Logic (CADTQL) helps designers simulate and test efficient quantum circuits for computing, communication, and sensing [1]. The study examines precision issues in floating-point storage formats that impact optimization algorithms, causing deviations from theoretical solutions and affecting algorithm performance. These insights help improve the practical application of optimization in both classical and quantum computation [2]. The article presents a quantum-inspired portfolio recommendation system that optimizes investments across global stock markets, focusing on uptrends and cross-market analysis. It emphasizes explainability and transparency, helping investors trust and understand AI-generated results, while demonstrating robust performance in assessing market relationships [3]. The AngelQ system offers quantum computing-as-a-service (QCaaS) with quantum design automation (QDA) for cloud-based quantum circuit synthesis, utilizing a quantum-inspired optimization (QiO) technique. It provides a flexible and visual platform for creating and verifying diverse quantum circuits, aiding both research and education in quantum computing [4]. The approach uses graph theory for efficient minimum-time control of Boolean control networks (BCNs), addressing all cases of fixed initial or desired states. By modeling BCN dynamics with a state transition graph (STG) and employing breath-first search algorithms, the method offers high versatility, superior time efficiency, and scalability for larger networks [5]. This paper proposes a novel method for synthesizing reversible quantum circuits by converting the reversible function into a hypercube, improving efficiency and reducing gate count. The approach uses two new indicators, adjacent Hamming distance (AHD) and total cycle distance (TCD), along with a generalized Toffoli gate set for better performance in error correction and fault tolerance [6]. The paper explores the use of reconfigurable logic for encryption and decryption, aiming to address power dissipation, delays, and heat in ICs by utilizing reversible computing and QCA technologies. The design, implemented in Verilog and verified using Xilinx Vivado, shows optimized delay and successful encryption-decryption through simulation results [7]. The paper presents two algorithms for the optimal synthesis of 4-bit reversible functions, addressing the enormous search space and storage challenges. The study demonstrates efficient synthesis techniques for various 4-bit reversible circuits and highlights their potential for optimizing quantum circuits and accommodating physical constraints in quantum information processing [8]. The paper presents a reversible logic-based encryption scheme, using a cascade of 4-input reversible gates to perform any 4-variable function. It details the design of a reconfigurable gate built from standard gates (NOT, CNOT, Toffoli, and Fredkin) and provides an 8-bit encryption/decryption scheme implemented in VHDL, with quantum cost calculation and FPGA simulation results [9]. The study proposes using reversible logic to design an Arithmetic Logic Unit (ALU) for a crypto-processor, addressing power consumption-based attacks. The approach includes a reversible Carry Save Adder (CSA) with Modified TSG gates and a Montgomery multiplier, showing improved performance in terms of gate count, garbage outputs, and quantum cost, making reversible circuits a promising solution for hardware cryptography [10]. The paper presents a reversible logic-based encryption scheme using a cascade of 4-input reversible gates that can perform any 4-variable function. It introduces a reconfigurable reversible gate built from standard gates (NOT, CNOT, Toffoli, and Fredkin), and provides a complete 8-bit encryption/decryption scheme in VHDL, with quantum cost calculation and FPGA simulation for verification [11]. Research in reversible logic synthesis and testing has surged due to the demand for low-power design and the potential of quantum computation. Reversible logic is expected to provide a sustainable solution for ultra-low power circuits, with synthesis methods ranging from exact approaches for small circuits, heuristic methods for larger ones, to functional representations like BDD and ESOP for scalability. These methods are crucial in applications like cryptographic algorithms, where transformations, such as encryption and decryption, are

DOI: https://doi.org/10.71058/jodac.v9i2002

inherently reversible [12]. The paper critically analyzes the "Reversible Logic Cryptography Design (RLCD) with Linear Feedback Shift Register (LFSR) key" scheme, highlighting its vulnerability to brute force attacks due to the short 4-bit LFSR key and the presence of traceable patterns in the encrypted images. It proposes an enhancement by adding a confusion module to eliminate perceptible patterns and improve security, but the modified scheme still fails under NIST tests, revealing flaws in the Reversible Logic Gate-based diffusion process. The study also evaluates the performance of the original and improved schemes on a 32-bit microcontroller for real-time embedded applications [13]. The research focuses on reversible logic cryptography (RLC) for applications in optical estimating, signal processing, nanotechnologies, and low-power, low-weight systems, emphasizing security, power, and area optimization. By utilizing a Linear Feedback Shift Register (LFSR) for key generation, the proposed RLC method improves performance by approximately 7% compared to traditional designs like AES and the Chaotic map technique, offering enhanced encryption and decryption in symmetric systems [14]. The research focuses on reversible logic cryptography (RLC) for applications in optical estimating, signal processing, nanotechnologies, and low-power, low-weight systems, emphasizing security, power, and area optimization. By utilizing a Linear Feedback Shift Register (LFSR) for key generation, the proposed RLC method improves performance by approximately 7% compared to traditional designs like AES and the Chaotic map technique, offering enhanced encryption and decryption in symmetric systems [15]. Reversible logic, gaining interest due to its applications in quantum, CMOS, optical, and nanotechnologies, addresses power dissipation concerns by theoretically eliminating heat generation. The study focuses on designing reversible circuits for functional modules of the DES encryption system, including a 4-bit counter and a two-way shift register, aiming to reduce power consumption and enhance security while minimizing the addition of costly garbage bits during synthesis [16].

3. Encryption and Decryption methods

Binary is a typically agreed communiqué language amongst virtual structures for changing statistics. People`s textual content languages range across the world, however the visible language of virtual snap shots conveys statistics to everyone. The use of virtual snap shots is extensively utilized in ordinary lifestyles packages which include banking, e-healthcare, and evidence of identification in e-governance. The difficulty of piracy of virtual snap shots transmitted over public networks calls for safety features which include steganography and encryption. Image steganography era protects facts via way of means of hiding an intentional photo at the back of a insignificant photo referred to as a cowl object. Along with the power of safety, throughput is the handiest overall performance metric while enforcing such a set of rules on a computer. For photo scrambling algorithms, the throughput is received via way of means of dividing the dimensions of the image by the point it takes for the set of rules to scramble the whole pixels of the photo. The imput photo length and set of rules like execution time are laid out in bits and seconds, respectively, so the unit of throughput is bits in keeping with second (bps). Lightweight metrics which includes area / code length and throughput (subject programmable gate arrays) are decisive parameters for the suitability of such safety algorithms on useful resource limited structures which includes FPGAs and microcontrollers.

Few vigilantly planned selective safety algorithms have validated light-weight parameters to be appropriate for implementation on useful resource-limited devices. In contrast, without right validation of safety parameters, cryptographic algorithms aren't essential for attaining facts safety. The encryption / decryption block of the RLCD-LFSR (Reversible Logic Cryptography Design-Linear Feedback Shift Register) set of rules includes units of 4-input SCLs, 3-input fredkin or toffoli gates, and 2-input feynman gate. Besides this the sequential operations carried out via those reversible logic gates, a 4-input XOR gate in the midst of a LFSR key of 4-bit. The Reversible Logic Gate Boolean feature is reversible handiest if every mixture of inputs maps a one-of-a-kind mixture of outputs. RLG is a virtual gate that gives a completely unique output nature for any mixture of inputs The simple set of RLGs taken into consideration consists of a 4-input SCL gate, a 3-input fredkin gate, a toffoli gate and a 2-input feynman gate and their I / O mixtures. The feasible set of input/output mixtures of RLGs key technology with LFSRs are the most effective shape of pn sequence generator used as cryptographic packages keys. An `n-bit` LFSR circuit includes `n` number

DOI: https://doi.org/10.71058/jodac.v9i2002

of D Flip-Flop (D-FFs). The RLCD-LFSR set of rules via way of means of duplicating the set of rule's encryption and decryption technique within side in equal manner turned into security evaluation [16].

The relaxation of taping record describes RLCD schemes that use LFSR circuits without MLS. In addition, the stepped forward model of the RLCD scheme proposed on this record makes use of a 14-bit LFSR. A 14-bit XNOR-primarily based LFSR polynomial totally for enforcing MLS suggests the equivalent circuit as per

$$X\ 14 + X\ 5 + X\ 3 + X + 1 \qquad (1)$$

Security investigation apart from visible quality-primarily based totally on evaluation of encrypted image. The distinctive safety evaluation offered on this consultation is on the whole encrypted image of different extension schemes focuses at the statistical parameters of the treatises mentioned here. A function of the RLCD-LFSR scheme that proves to NIST is the randomness of encrypted image. In addition to being capable of face up to decide on plaintext assaults and part detection-primarily based totally cryptanalysis, it changed into additionally evaluated. Visual analysis of cryptographic quality in the paintings of the RLCD-LFSR, 128x128 gray scale and color image had been decided on as inputs to validate the algorithm. Instead of color image different gray scale image: House, Lena, and Baboon suggest the diverse input image taken from the RLCD-LFSR scheme and their corresponding encrypted image. This suggests the authentic image taken as input through the RLCD encryption scheme and constitutes the encrypted image taken from these schemes.

3.1 Entropy evaluation

The randomness of the pixel distribution of a picture may be efficaciously measured the use of statistics for entropy evaluation as the most entropy price for an 8-bit gray scale picture with a perfect 8 bit pixel distribution. The entropy values for the unique photos vary from 6 to 7.5. In comparison, the entropy of all scrambled photos is near or more than 7.9, making sure an invariant distribution of pixel values. The entropy values of the scrambled picture are approximately the identical due to the fact there may be the identical spreading technique.

The uniform allocation of image values in any respect feasible depth tiers of a picture may be visually analyzed the use of this. The similar histogram of the unique and decrypted photos confirms the lossless and correct reconstruction of the unique picture from the corresponding encrypted picture. In comparison, the peaks within side the histogram of the scrambled picture imply that now no longer all 3 RLCD-LFSR schemes can acquire the flatter peaks required within side the histogram.

3.2 Structural Similarity Metric Measurement (SSMM)

SSMM parameter is used to degree the presence of the identical shape among photos. An SSMM price of "0" suggests a very extraordinary shape (most dissimilarity) among photos, and a price of "1" suggests a super fit of shape among photos. SSMM values suggest a development within side the encryption of the RLDC-LFSR extension scheme because of the critical function of the scrambling technique over the RLDC scheme without the scrambling module.

Decryption primarily based totally on area detection. An area is a factor in a picture in which the pixel current stage modifications or breaks sharply. Extracting edges from a picture allows perceiving the internal and outer boundaries (contours) of the picture. Another proposed decryption approach is to extract the unique picture hint from the brink detection effects of the encrypted picture. The end result of making use of an area detection technique the use of the Sobel masks algorithm to an encrypted picture received from the RLCD-LFSR scheme and the rims taken from the unique picture. Edge detection effects for encrypted photos generated with the aid of using the schemes discussed have remarkable area detection follows the bounds of the unique picture. The perceptual strains observed at the outer and internal edges diagnosed from the scrambled photos offer enough statistics to perceive the unique picture. When the use of a confusion unit within side the RLCD-LFSR enhanced scheme, scattered edges are detected within side the scrambled picture and strains of the unique picture are removed.

3.3 Chosen-plaintext assault evaluation

Image encryption algorithms that use the XOR act as an ingredient of the propagation manner may be susceptible to chosen-plaintext attacks. Cryptographic algorithms which can generate absolutely extraordinary units of pixel for a given input image are supple to choose plaintext attacks and suggest the end result of an XOR operation among the unique photo cameraman and the residence. The image of the outcomes received through XORing the encrypted cameraman and image of the residence received from the RLDC-LFSRwoMLS, RLDC-LFSRwMLS and RLDC-LFSR ended schemes, respectively can be proven easily. The main focus is on the circuit synthesis using contemporary simulation tools based on FPGA begun with modeling. The treatise explores cryptographic logic circuit applications for the development of reversible. The goal of this task is to use a reversible circuit for normal cryptographic operation. Contouring gates establish the key employed for each gate. The key to decide different ciphers is determined by different streams and different choices.

4. Reversible logic synthesis for cryptography.

Example 1. The Figure 4 shows a reconfigurable reversible gate using basic gates such as Toffoli gates and Fredkin gates, which are simple cryptographic implementations [17]. 9-bit data encryption and decryption is implemented using a single circuit. Here, a 5-bit key is utilized on both sides to encrypt and decrypt 4-bit data [18]. This circuit can be expanded for multi-bit data by simply increasing the Fredkin gates and Toffoli gates, as revealed in Figure 4. Here, a, b, and c lines are considered constant lines provided by Logic 1 on all these lines.

Example 2. A plaintext attacker collects information about a particular plaintext-ciphertext pair for the same key. In 56-bit DES, each of the two 56 possible keys is applied to a block of plaintext to determine which key produces the correct encryption.

The linear relationship between the bits of the plaintext ciphertext and the keys common to plaintext key selection is analyzed by cryptanalysis [19]. The example discussed by Bernard Menezes [19] in his book in chapter no. 5 is referred here who had thoroughly explained the process of defining the plaintext-ciphertext pair with different equations.

A linear combination of each of the following ciphertext and plaintext terms is a set of terms that can be selected in the first iteration and is represented by the output X1 to X5 of a particular plaintext P3 out of a total of 9 bits (P1 to P9). It is as follows:

X1= P3 xor I21 xor I24 xor K03 xor K11 xor K14 (2)
X2= I21 xor K27 xor I37 (3)
X3= P3 xor I24 xor I37 xor K03 xor K11 xor K14 xor K27 (4)
X4= I24 xor K25 xor I35 (5)
X5= P3 xor I35 xor I37 xor K03 xor K11 xor K14 xor K25 xor K27 (6)

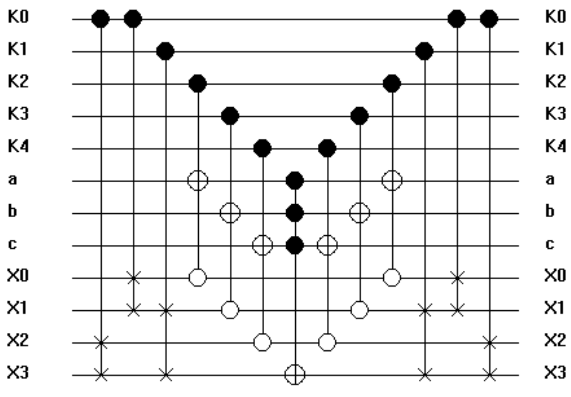


Figure 4. Reconfigurable Reversible Gate (RRG)

DOI: https://doi.org/10.71058/jodac.v9i2002

All the expressions from equation (2) to (6) can be easily converted into a synthesizable circuit as shown in Figure 5. The outputs X are the high bias random variables for the first iteration and likewise for other iterations, different random variable can be generated which forms a biased linear expression

$$X = P \text{ xor } I \text{ xor } K, \tag{7}$$

where P denotes Pm1 to Pmn bits, I denotes Im1 to Imn bits and K as the sum of selected bits for different stage round keys, excluding the last stage of equation 7.

Figure 5 shows Level 1 synthesizing a linear cryptanalysis of plaintext and ciphertext pairs using the below equation. Here, P indicates a plaintext sequence box or product cipher whose round key operation includes the function of an encryption key and the private key cipher is obtained by repeating the replacement and combination of the product cipher many times. The round key, DES Key K, is used to encrypt each plaintext bit individually using a crypto block-chain.

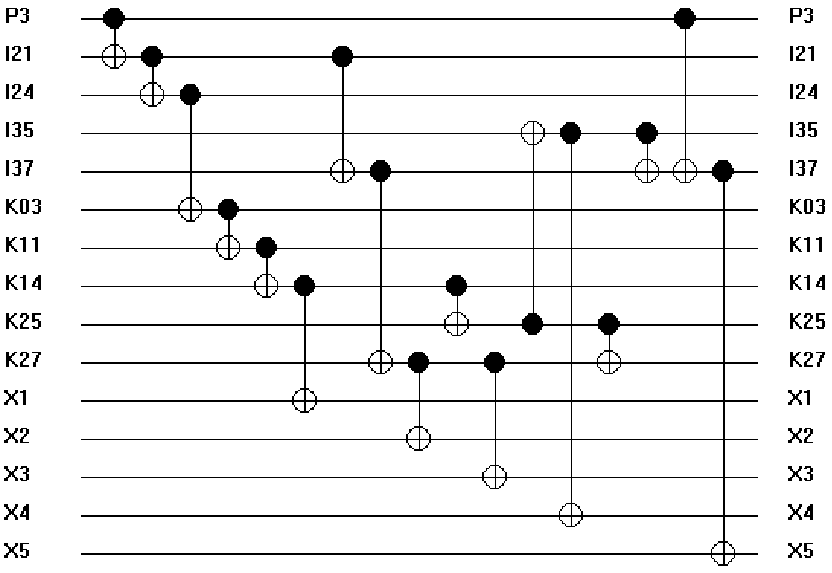


Figure 5. Level 1 synthesis of a linear cryptanalysis

5. Conclusion

This research advances the understanding of reversible logic through a robust mathematical modeling framework. The findings demonstrate that reversible circuits achieve significant reductions in energy consumption while maintaining computational efficiency thus providing a viable alternative to conventional irreversible circuits. Our analysis underscores the importance of gate-level optimizations and their impact on overall circuit performance. Future work will focus on extending these models to complex systems and integrating them with emerging technologies, such as quantum computing and nanotechnology. By continuing to refine reversible logic designs and exploring their applications we can contribute to the development of more sustainable and efficient computational systems paving the way for innovations in various fields of computer science and engineering.

Future Scope

In this article, the reversible logic used for encryption and decryption is discussed. Not only cryptography, but various different algorithms available for encryption and decryption in cyber security can be implemented using reversible logic which will save power consumption and area.

DOI: https://doi.org/10.71058/jodac.v9i2002

Funding No funding was received.

Declarations
Conflict of interest The authors declare that they have no conflict of interest.

References

[1] A. B. D. V, A. Bristow and K. -C. Chen, "A Computer Aided Design Tool for NISQ Logic Synthesis," 2023 26th International Symposium on Wireless Personal Multimedia Communications (WPMC), Tampa, FL, USA, 2023, pp. 242-247, doi: 10.1109/WPMC59531.2023.10338987.

[2] Y. -H. Chou, C. -H. Wu, Y. -C. Jiang, S. -Y. Kuo and S. -Y. Kuo, "Nanoscale Precision-Related Challenges in Classical and Quantum Optimization," in *IEEE Nanotechnology Magazine*, vol. 18, no. 3, pp. 31-43, June 2024, doi: 10.1109/MNANO.2024.3378488.

[3] Y. -H. Chou, M. -H. Chang, Y. -C. Jiang, S. -Y. Kuo, S. -Y. Kung and B. J. Sheu, "An Investigation on Quantum-Inspired Algorithms for Portfolio Optimization Across Global Markets," in *IEEE Nanotechnology Magazine*, vol. 18, no. 4, pp. 27-34, Aug. 2024, doi: 10.1109/MNANO.2024.3402755.

[4] S. -Y. Kuo, Y. -C. Jiang, Y. -H. Chou, S. -Y. Kuo and S. -Y. Kung, "Quantum Computer-Aided Design Automation," in *IEEE Nanotechnology Magazine*, vol. 17, no. 2, pp. 15-25, April 2023, doi: 10.1109/MNANO.2023.3249500.

[5] S. Gao, J. -e. Feng, Z. Li and C. Xiang, "Minimum-Time Control of Boolean Control Networks: A Fast Graphical Approach," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 71, no. 2, pp. 742-746, Feb. 2024, doi: 10.1109/TCSII.2023.3309334

[6] Y. -C. Jiang, K. -C. Tseng, C. -Y. Hua, S. -Y. Kuo, Y. -H. Chou and S. -Y. Kuo, "A Novel Hypercube-Based Heuristic for Quantum Boolean Circuit Synthesis," in *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 12, no. 3, pp. 648-661, Sept. 2022, doi: 10.1109/JETCAS.2022.3202840

[7] K. Rajesh, K. Balanagalakshmi, K. Rajyalakshmi, M. Bhanurekha, K. S. Kumar and K. Sambasivarao, "Encryption and Decryption using optimized Reconfigurable Reversible Gate," *2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP)*, VIJAYAWADA, India, 2023, pp. 1-5, doi: 10.1109/AISP57993.2023.10134930.

[8] O. Golubitsky and D. Maslov, "A Study of Optimal 4-Bit Reversible Toffoli Circuits and Their Synthesis," in *IEEE Transactions on Computers*, vol. 61, no. 9, pp. 1341-1353, Sept. 2012, doi: 10.1109/TC.2011.144

[9] Marcin Bryk, Krzysztof Gracki, Pawel Kerntopf, Marek Pawlowski, Andrzej Skorupski, Encryption using reconfigurable reversible logic gate and its simulation in FPGAs, 2016 MIXDES - 23rd International Conference Mixed Design of Integrated Circuits and Systems, 10.1109/MIXDES.2016.7529732, (203-206), (2016).

[10] Nayeem, N. M., Jamal, L. & Babu, H. M. H. (2009). Efficient Reversible Montgomery Multiplier and Its Application to Hardware Cryptography . Journal of Computer Science, 5(1), 49-56. https://doi.org/10.3844/jcssp.2009.49.56

[11] 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*, Lodz, Poland, 2016, pp. 203-206, doi: 10.1109/MIXDES.2016.7529732.

[12] K. Datta and I. Sengupta, "Embedded tutorial: Applications of reversible logic in cryptography and coding theory," 2013 26th International Conference on VLSI Design and 2013 12th International Conference on Embedded Systems, Pune, India, 2013, pp. lxvi-lxvii, doi: 10.1109/VLSID.2013.146.

[13] B. Sarala., Dr.G.A.Sathish Kumar, Efficient Design of Image Cipher Technique Using Reversible Logic, Turkish Journal of Computer and Mathematics Education, Vol.12 No.13 (2021), pp-691-700

[14] K. Datta and I. Sengupta, Embedded tutorial: Applications of reversible logic in cryptography and coding theory, 2013 26th International Conference on VLSI Design and 2013 12th International Conference on Embedded Systems, 2013, pp. lxvi-lxvii, doi: 10.1109/VLSID.2013.146.

[15] Shikha Kuchhal Rakesh Verma, Security Design of DES Using Reversible Logic, IJCSNS International

DOI: https://doi.org/10.71058/jodac.v9i2002

Journal of Computer Science and Network Security, VOL.15 No.9, September 2015 pp- 81-84

[16] Vinoth Raj, Siva Janakiraman, Sundararaman Rajagopalan, Rengarajan Amirtharajan, Security analysis of reversible logic cryptography design with LFSR key on 32-bit microcontroller, Microprocessors and Microsystems, Volume 84, 2021, 104265, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2021.104265.

[17] Patancheru Jyothi, B. Kalpana, An efficient design for Data Encryption and Decryption using Reconfigurable Reversible Logic Gates, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 10 | Oct -2017, ISSN: 2395-0072

[18] 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.

[19] Bernard Menzes, Network Security and Cryptography, Cengage Learning Publication, Third Impression 2014, ISBN-13:978-81-315-1349-1