As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology
Volume 10, Issue 02, pages 377-387.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue02.html
DOI: https://doi.org/10.46501/IJMTST1002050

Secure Visual Data Processing: Image Encryption and Decryption through Reversible Logic Gates in VLSI Design

Dr. D Naga RaviKiran, Oruganti Bhaskar Reddy, Repalle Sitha Mahalakshmi, Tiruvaipati Lakshmi Chaitanya Kumar, Sonti Priyathama Siva Krishna

Department of Electronics and Communications Engineering, Chalapathi Institute of Technology,Guntur, Andhra Pradesh, India

To Cite this Article
Dr. D Naga Ravi Kiran, Oruganti Bhaskar Reddy, Repalle Sitha Mahalakshmi, Tiruvaipati Lakshmi Chaitanya Kumar, Sonti Priyathama Siva Krishna, Secure Visual Data Processing: Image Encryption and Decryption through Reversible Logic Gates in VLSI Design, International Journal for Modern Trends in Science and Technology, 2024, 10(02), pages. 377-387.https://doi.org/10.46501/IJMTST1002050

Article Info
Received: 30 January 2024; Accepted: 21 February 2024; Published: 26 February 2024.

ABSTRACT

This work delves into the intriguing domain of reversible logic synthesis and testing, a pivotal area with implications for low-power design and quantum computing. Reversible computations find applications in quantum computing, nanotechnology, digital signal processing, bio-information, among others, necessitating robust cryptography systems to safeguard against unauthorized access and ensure data confidentiality. Addressing prevalent challenges like high area and power requirements in secure cryptography algorithms, this study introduces a novel solution: the Reversible Logic Gates Cryptography Design (RLGCD). RLGCD is adept at crafting both encryption and decryption architectures, employing a Linear Feedback Shift Register to generate encryption and decryption keys. To fortify data security, Least Significant Bit (LSB) watermarking is incorporated. The research evaluates the FPGA performance of the RLGCD architecture, revealing substantial enhancements compared to conventional systems, marking a significant stride toward efficient and secure cryptographic implementations.

Keywords: Reversible Logic, Cryptography, Quantum Computing, FPGA Performance, LSB Watermarking

1. INTRODUCTION

Reversible logic has received great attention in the recent years due to their ability to reduce the power dissipation which is the main requirement in low power VLSI design. It has wide applications in low power CMOS and Optical information processing, DNA computing, quantum computation and nanotechnology. Irreversible hardware computation results in energy dissipation due to information loss. According to Landauer's research, the amount of energy dissipated for every irreversible bit operation The heat generated due to the loss of one bit of information is very small at room temperature but when the number of bits is more as in the case of high speed computational works the heat dissipated by them will be so large that it affects theperformance and results in the reduction of lifetime of the components In 1973, Bennett showed that KTln2 energy would not dissipate from a system as long as the system allows the reproduction of the inputs from observed outputs. Reversible logic supports the process of running the system both forward and backward. This means that reversible computations can generate inputs from outputs and can stop and go back to any point inthe computation history. A circuit is said to be reversible if the input vector can be uniquely recovered from the output vector and there is a one-to-one correspondence between its input and output assignments, i.e. not only the outputs can be uniquely determined from the inputs, but also the inputs can be recovered from the outputs Energy dissipation can be reduced or even eliminated if computation becomes Information lossless.

Reversibility in computing implies that no information about the computational states can everbe lost, so we can recover any earlier stage by computing backwards or uncomputing the results. This is termed as logical reversibility. The benefits of logical reversibility can be gained only after employing physical reversibility. Physical reversibility is a process that dissipates no energy to heat. Absolutely perfect physical reversibility is practically unachievable. Computing systems give off heat when voltage levels change from positive to negative: bits from zero to one. Most of the energy needed to make that change is given off in the form of heat. Rather than changing voltages to new levels, reversible circuit elements will gradually move charge from one node to the next. This way, one can only expect to lose a minute amount of energy on each transition. Reversible computing strongly affects digital logic designs. Reversible logic elements are needed to recover the state of inputs from the outputs. It will impact instruction sets and high-level programming languages as well. Eventually, these will also have to be reversible to provide optimal efficiency.

Cryptography is the process of protecting the information by converting it in to unreadable format and thus maintains the confidentiality of the data. This process involves the conversion of plain text into cipher text by the process called encryption and the process by which the original data that is the plain text is recovered back called decryption.

One of the major challenges in VLSI design is the heat dissipation. Now reducing the size of ICs and increasing the number of transistors is happening day by day and up to now all these obeys Moore's law [1]. But with higher integration and scaling the amount of heat that is dissipated also increases. Landauer's work [2] showed that for each bit of data that is lost there will be a heat dissipation in the range of KTln(2). Where, K is the Boltzman constant and T is the temperature in Kelvin scale. The work done by Bennett presented that this heat dissipation can be eliminated if the traditional irreversible systems are converted in to reversible systems [3]. Reversible computation is the operation in which there is no loss of information and thus scatters only a small amount of heat. That is, there is no decrease in the entropy of the system. In data and telecommunications, cryptography is one of the most necessary parts since the communication even take place over untrusted mediums where the data can be easily hacked out. A cryptography system not only demands high security but also low power consumption. The cryptography system implementation using reversible logic gates offers the best solution for this.

A Reversible Logic Gate Cryptography Design (RLGCD) is presented in this paper. The biggest motivation of including reversible technologies in to cryptography includes, it gives energy efficiency much better than other conventional systems and such a cryptography system is useful for different applications such as medical field, banking, government organization etc. The key for cryptography is generated by using LFSR [4]. The FPGA performance of the RLGCD architecture is better as compared to existing methods.

Data security is importance in present time as lots of information is being communicated via network. A suitable methodology for privacy transformation is best to make a data protected over network. Different methods are implemented in order to protect the sensitive data. Now a days most of the data is secured by the technique of encryption and certificates. Most of methods are based on cryptography technique. Multi-level encryption is a new concept that is used for making the system more secure than existing cryptosystems. Multi-levelencryption is the process of encrypting the plain text with one or more time with same of different no of keys. It makes the process more complex and powerful than existing.

Cryptography and Types Cryptographyis a technique to which information is send in a secure manner so that only authorized user is able to receive this information. It refers to the scrambling of the data and make it meaningless for the third-party during transmission There are three basic components of cryptography system

Plain text: Source / information/data / original message

Key: Necessary for encryption process.

Cypher text: Unrecognized data /encrypted data / encrypted message

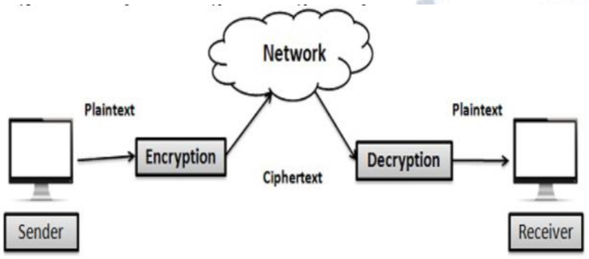


Figure 1: Encryption Decryption Process

The original message is then encoded using encryption algorithm. This process is called encryption. The reverse process to get back the encrypted data into plain text by using decryption algorithm. This process is called decryption. The process of decryption is reverse that of encryption. Cryptography is used to achievefollowing objectives:

Confidentiality: Confidentiality means to the keep information secret / private.

Data integrity: It refers to the accuracy and consistency (validity) of data over its lifetime.

Authentication: The property of being genuine and being able to be verified and trusted.

The algorithm requires the key to be kept secret or long enough so that it takes even longer to break. For example, a 40-bit key has about one trillion combinations whereas a 128-bit key has 3.4*1026 trillion combinations [1]. There are two general types of key-based algorithms: Symmetric and Asymmetric.

Symmetric Key Algorithms, also known as private-key, conventional, single-key or secret-key algorithms, require that sender and receiver agree on a key before they can communicate securely. In this type of algorithms, the encryption key and the decryption key are the same and security of information depends on the degree of key secrecy from the unauthorized user / intruders. During the transmission key must remain secret. Encryption process can be done like ENCRYPTIONKEY(MESSAGE) = CIPHER TEXT and Decryption processes as: DECRYPTIONKEY(CYPHER TEXT) = MESSAGE respectively. This method is extremely fast and efficient. It also provides integrity and confidentiality. But it fails to provide authentication. [2][3][4].

Asymmetric key algorithm, also known as public-key algorithms which operate with different encryption and decryption key. Encryption key is made public and anyone can use to encrypt a message, but only a authorized user with the appropriate decryption key can decrypt the message. There are some example which are based on this type of algorithms like RSA, Rabin and Elgamal [1][2][4]. Asymmetric algorithms are hard to implement and require significant processing power due to fundamental mathematical operations such as modulus. In this paper we will talk about the AES and RSA algorithm and their implementation in multilevel security layers which will be fast and as much more secure than existing AES and RSA. Proposed Multi-level encryption can work better compared to single encryption. Multi-level encryption involved the encryption of a message one or more times by using same algorithm with same key or same algorithms with different keys or by using different algorithms[13]. But the proposed algorithm works faster and provide extra security to data in an efficient manner. Not all algorithm with multiple computations are always better but an efficient algorithm can provide same layer of security in faster way.

2. LITERATURE REVIEW

Embedded systems having sensitive nodes such as RFID tags and nano-sensors necessitate the use of lightweight block ciphers. Error detection schemes for lightweight block ciphers are proposed in [5]. One of the fastest and most efficient block cipher in existence, XTEA (eXtended TEA) is used in this work. It uses simple addition, XOR, and shift functions, and has a very small code size, less memory requirement and less computational power. These proposed methods suitable for providing reliability but less accuracy in error rate is one of the demerit while using XTEA method.Security part design of the DES (Data Encryption Standard) using RLG [6] comprises of a reversible logic gate based two way shift register and four bit counter. Since RLG is used to implement the security part of DES, this work has good data security and low power consumption. But a specific RLG design is not provided and performance evaluations were not carried out.The S-box dimension and number of registers required can be dynamically varied with respect to the security requirements that we required [7]. In this work the safety of the cipher text was improved based on the confusion substitution of S-box and so that the internal structure of data blocks disorder by four steps of matrix transformation. Then by cyclic displacement of byte using column ambiguity function, the diffusivity of cipher text was obtained. Finally LFSR is used to generate dynamic. Thus the stochastic characteristic of secret key is improved in each round of iteration. This technique achieved high scalability. But it is difficult to achieve the S box when the dimension selected is an odd number and requires more time for encryption and decryption.In this work, two block ciphers such as HIGHT and LED which can be employed in authenticated encryption algorithms are discussed [8]. The former have a Feistel network structure and it is good for low power and low complexity embedded applications. The latter is of an efficient Advanced Encryption Standard (AES) type. This work has high error coverage and high efficiency. But it is not able to detect the permanent and transient faults.

3.SECURE VISUAL DATA PROCESSING

Reversible Logic Gates (RLGs):

RLGs are the circuits that having equal number of inputs and outputs with a unique one to one mapping relationship. Thus, it is possible to recover the input pattern from the output pattern, so that there is no information loss during computation. For example, let 110 is the pattern which is given as input to RLG. Then after completing the logic operation, it produces 001 as output. If we apply this 001 as input and obtained 110 as output then it depicts the occurrence of a reversible operation. while using traditional combinational logic circuits, for every bit of data that is lost during operation there will be an equivalent heat energy dissipation. The reason behind this is according to the second law of thermodynamics there is no way to reproduce the information once lost. So, when the computation is performed in a reversible manner then it is possible to achieve a logical zero power dissipation. i.e., there is no decrease in the entropy of the system. Constraints for designing RLGs include [9]

- RLGs do not allow fanout.
- Quantum cost should be minimum as possible.
- Optimize the design to make garbage outputs minimum.
- A reversible logic circuits should have least gate level.

The original motivation was that reversible gates dissipate less heat (or, in principle, no heat). In a normal gate, input states are lost, since less information is present in the output than was present at the input. This loss of information loses energy to the surrounding area as heat, because of thermodynamic entropy. Another way to understand this is that charges on a circuit are grounded and thus flow away, taking a small quantity of energy with them when they change state. A reversible gate only moves the states around, and since no information is lost, energy is conserved.

Universality and Toffoli gate

Any reversible gate must have the same number of input and output bits, by the pigeonhole principle. For one input bit, there are two possible reversible gates. One of them is NOT. The other is the identity gate which maps its input to the output unchanged. For two input bits, the only non-trivial gate is the controlled NOT gate which XORs the first bit to the second bit and leaves the first bit unchanged.

Truth table **Permutation matrix form**

INPUT		OUTPUT	
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Unfortunately, there are reversible functions that cannot be computed using just those gates. In other words, the set consisting of NOT and XOR gates is not universal. If we want to compute an arbitrary function using reversible gates, we need another gate. One possibility is the Toffoli gate, proposed in 1980 by Toffoli.

This gate has 3-bit inputs and outputs. If the first two bits are set, it flips the third bit. The following is a table of the input and output bits:

Truth table **Permutation matrix form**

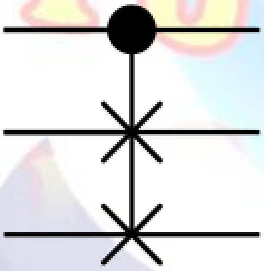
INPUT			OUTPUT		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

It can be also described as mapping bits a, b and c to a, b and c XOR (a AND b).

The Toffoli gate is universal; this means that for any Boolean functionf(x_1, x_2, ..., x_m), there is a circuit consisting of Toffoli gates which takes x_1, x_2, ..., x_m and some extra bits set to 0 or 1 and outputs x_1, x_2, ..., x_m, f(x_1, x_2, ..., x_m), and some extra bits (called garbage). Essentially, this means that one can use Toffoli gates to build systems that will perform any desired Boolean function computation in a reversible manner.

Fredkin gate



The above circuit representation of Fredkin gate. The Fredkin gate (also CSWAP gate) is a computational circuit suitable for reversible computing, invented by Ed Fredkin. It is universal, which means that any logical or arithmetic operation can be constructed entirely of Fredkin gates. The Fredkin gate is the three-bit gate that swaps the last two bits if the first bit is 1.The basic Fredkin gate is a controlledswap gate that maps three inputs (C, I_1, I_2) onto three outputs (C, O_1, O_2). The C input is mapped directly to the C output. If C = 0, no swap is performed; I_1 maps to O_1, and I_2 maps to O_2. Otherwise, the two outputs are swapped so that I_1 maps to O_2, and I_2 maps to O_1. It is easy to see that this circuit is reversible, i.e., "undoes itself" when run backwards. A generalized n×n Fredkin gate passes its first n-2 inputs unchanged to the corresponding outputs, and swaps its last two outputs if and only if the first n-2 inputs are all 1.The Fredkin gate is the reversible three-bit gate that swaps the last two bits if the first bit is 1.

Truth table **Matrix form**

INPUT			OUTPUT		
C	I_1	I_2	C	O_1	O_2
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

It has the useful property that the numbers of 0s and 1s are conserved throughout, which in the billiard ball model means the same number of balls are output as input. This corresponds nicely to the conservation of mass in physics, and helps to show that the model is not wasteful.

Logic function with XOR and AND gates

O_1 = I_1 XOR S

O_2 = I_2 XOR S

with S = (I_1 XOR I_2) AND C

It can also be implemented by the following logic:

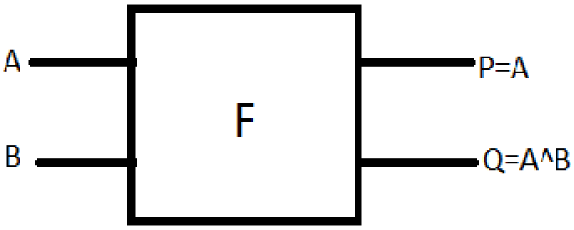
O_1 = (NOT C AND I_1) OR (C AND I_2) = CI_1+CI_2

O_2 = (C AND I_1) OR (NOT C AND I_2) = CI_1+CI_2

C_{out}= C_{in}

Feynman gate

Feynman gate is a 2*2 one through reversible gate. The input vector is I(A, B) and the output vector is O(P, Q). The outputs are defined by P=A, Q=A⊕B. Quantum cost of a Feynman gate is 1. Feynman Gate (FG) can be used as a copying gate. Since a fan out is not allowed in reversible logic, this gate is useful for duplication of the required outputs.



Truth Table of Feynman Gate

.

A	B	P	Q
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Double Feynman Gate (F2G) :

Figure 2 shows a 3*3 Double Feynman gate. The input vector is I (A, B, C) and the output vector is O (P, Q, R). The outputs are defined by P = A, Q=A B, R=AC. Quantum cost of double Feynman gate is 2.

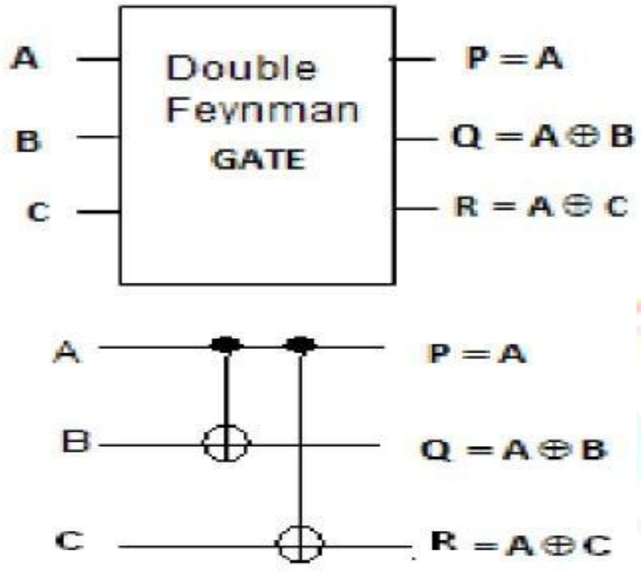


Figure 2: Double Feynman gate

Truth Table:

A	B	C	P	Q	R
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	1	1
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	0	0

Peres Gate:

Figure 3 shows a 3*3 Peres gate. The input vector is I (A, B, C) and the output vector is O (P, Q, R). The output is defined by P = A, Q = AB and R=AB C. Quantum cost of a Peres gate is 4. In the proposed design Peres gate is used because of its lowest quantum cost.

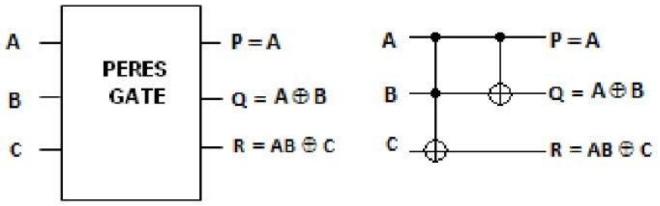


Figure 3: Peres gate

Truth Table:

A	B	C	P	Q	R
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	1	0
1	0	1	1	1	1
1	1	0	1	0	1
1	1	1	1	0	0

A full- adder using two Peres gates is as shown below. The quantum realization of this shows that its quantum cost is 8 two Peres gates are used.

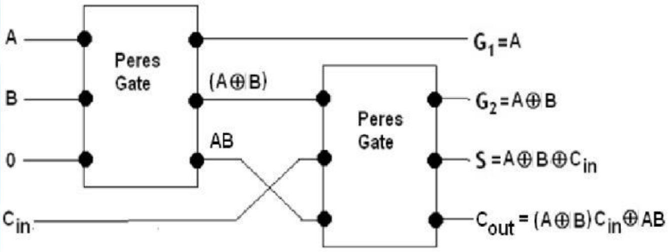
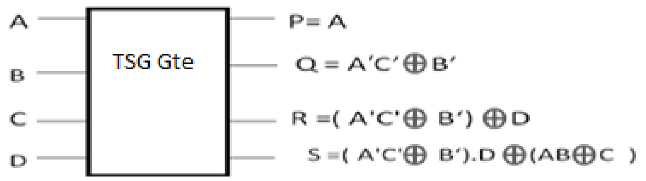


Figure 4: Full adder using two Peres gates

A single 4*4 reversible gate called PFAG gate with quantum cost of 8 is used to realize the multiplier.

TSG Gate:

Figure 5 shows a 4*4 TSG gate. The input vector is I (A, B, C, D) and the output vector is O (P, Q, R, S). The output is defined by P = A, Q = A'C'⊚ B', R = (A'C'⊚ B')⊚ D and S = (A'C'⊚ B').D⊚ (AB⊚ C) Quantum cost of a Peres gate is 4. In the proposed design Peres gate is used because of its lowest quantum cost. It can be verified that the input pattern corresponding to a particular output pattern can be uniquely determined. The proposed TSG gate is capable of implementing all Boolean functions and can also work singly as a reversible Full adder



TSG gate

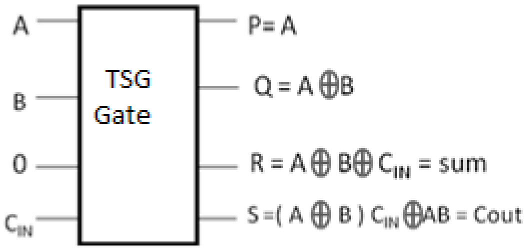


Figure 5: TSG Gate Working as Reversible Full Adder

The RLG that are used to design this new cryptography system includes Feynman gate, Fredkin gate, Toffoligate and SCL gateand are shown in Figure 6.

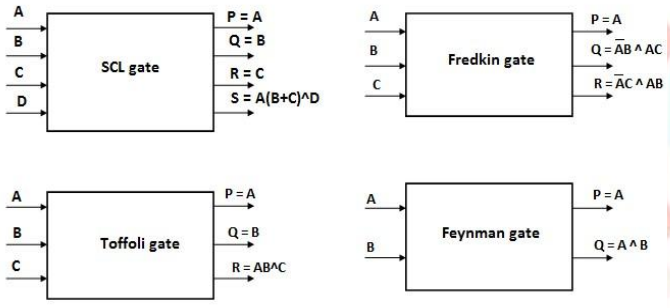


Figure 6: Block diagram of RLGs

- **Encryption process:**

The encryption process is shown in Figure 7. The pixel values are thus 8 bit binary word: i[0], i[1], i[2], i[3], i[4], i[5], i[6], i[7]. The first four LSB input bits is applied to the below SCL gate and the above SCL gate is fed by the first four MSB.

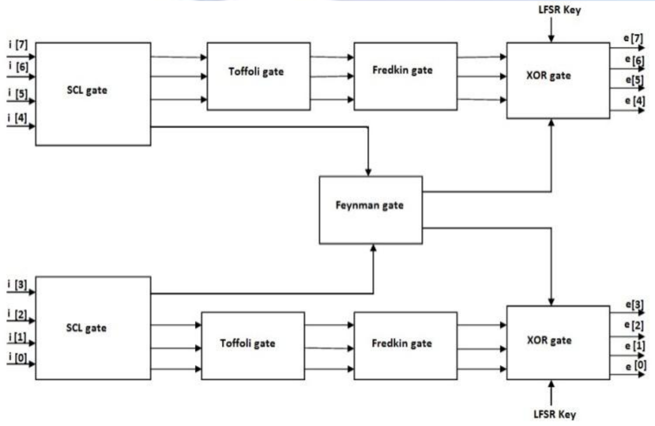


Figure 7: Encryption block

input pixel bits. Four of these inputs complete the SCL gate operation and thus produce four result bits. The first three LSB outputs from the below SCL gate perform Toffoli gate operation and provides three different output bits. Similarly, the first three MSB value outputs of SCL gate feed Toffoli gate and providesthree output bits. One of the output bits from the above and below SCL gates perform Feynman gate operation. Both Toffoli gates are followed by Fredkin gate and thus its outputs perform Fredkin gate. The Fredkin gate outputs and the Feynman gate outputs are connected to the XOR gates and thus perform XOR operation with LFSR key. Then, the XOR gate output provides the encrypted binary image pixel value e[0], e[1], e[2], e[3], e[4], e[5], e[6], e[7].

- **Decryption process:**

The process of decryption is shown in Figure 8. The decryption process is just the reverse operation of the encryption. Thus, encryption process output is fed as input to decryption process block. First, the encrypted pixel bits perform XOR operation with the key generated by the LFSR. After performing the four reversible gate operation one followed by the next the decrypted outputs are obtained at the SCL gate output. The decrypted output eight bit pixel values ared[0], d[1], d[2], d[3], d[4], d[5], d[6], d[7]. The encrypted as well as the decrypted binary output values are written into a text file. In MATLAB encrypted image and decrypted image are generated from the output text file.

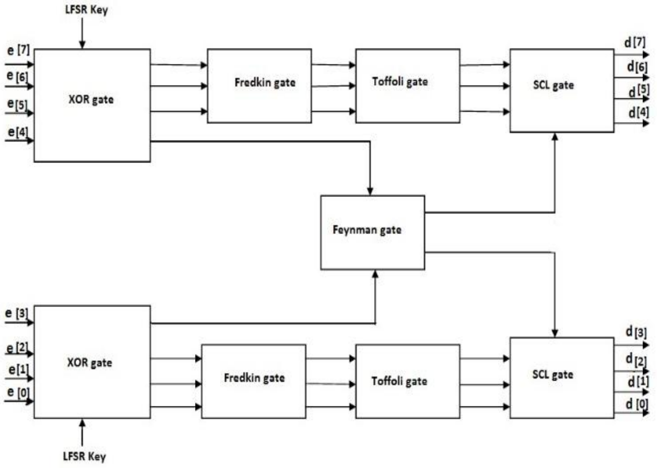


Figure 8: Decryption block

The advantages of reversable gates are as follows:

a) Low power consumption: Reversible logic gates consume less power than conventional logic gates because they do not lose information during computation. This is because reversible logic gates use feedback to generate their outputs, which allows them to reuse the same inputs multiple times.

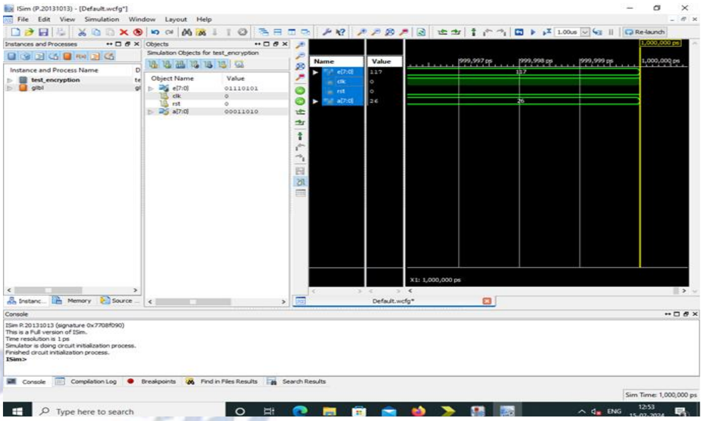
b) Reduced heat dissipation: Reversible logic gates dissipate less heat than conventional logic gates because they do not generate garbage outputs. Garbage outputs are outputs that are not needed for the computation, but are generated anyway. Conventional logic gates can generate garbage outputs, which can lead to increased heat dissipation.

c) Improved security: Reversible logic gates can be used to implement more secure encryption and decryption algorithms than conventional logic gates. This is because reversible logic gates are more resistant to power analysis attacks. Power analysis attacks are a type of attack that can be used to extract secret information from a system by analyzing its power consumption. Reversible logic gates are more resistant to power analysis attacks because they do not generate garbage outputs, which can be used by attackers to extract secret information.

d) Suitability for quantum computing: Reversible logic gates are well-suited for implementation in quantum computers. This is because reversible logic gates are unitary operations, which are the building blocks of quantum computation. Unitary operations are operations that preserve the information content of a quantum state. Reversible logic gates are unitary operations, which means that they can be used to implement quantum encryption and decryption algorithms.

4. RESULTS& DISCUSSION

Simulation results provide a comprehensive understanding of how the designed circuit behaves under different conditions. They are crucial for verifying the functionality, identifying and resolving issues, and ensuring that the circuit meets the desired specifications before physical implementation. Figure 9shows the simulation result of Encryption. In this we applied input plane test ,clock and reset based on that encrypted output is generated .



Simulation Objects for test_encryption

Object Name	Value
e[7:0]	01110101
clk	0
rst	0
a[7:0]	00011010

Name	Value
e[7:0]	117
clk	0
rst	0
a[7:0]	26

```
ISim P.20131013 (signature 0x7708f090)
This is a Full version of ISim.
Time resolution is 1 ps
Simulator is doing circuit initialization process.
Finished circuit initialization process.
ISim>
```

Figure 9: Simulation result of the encryption process

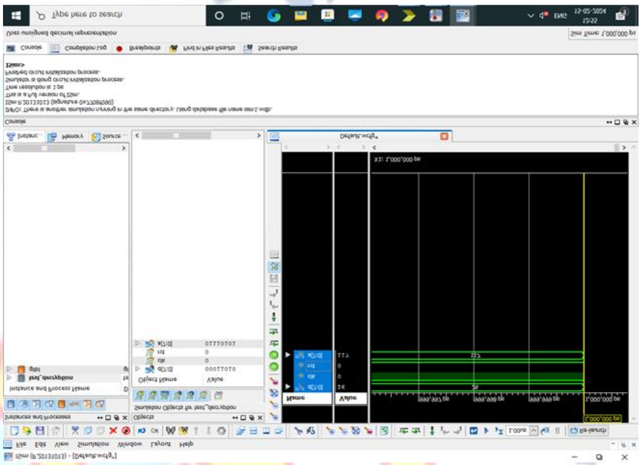


Figure 10: Simulation result of the decryption process

Figure 10 shows the simulation result of Decryption.In this we applied encrypted input,clk and rst based on that decrypted output is generated. The block diagram offers a high-level representation of the entire system, illustrating the functional blocks and their interconnections. It serves as a visual guide for system architecture, aiding designers in conceptualizing and communicating the design structure and functionality. Figure 11 shows the block diagram of the proposed encryption process.Here, we applied input data (a(7:0),clk,rst),we generated output data (encrypted e(7:0)).

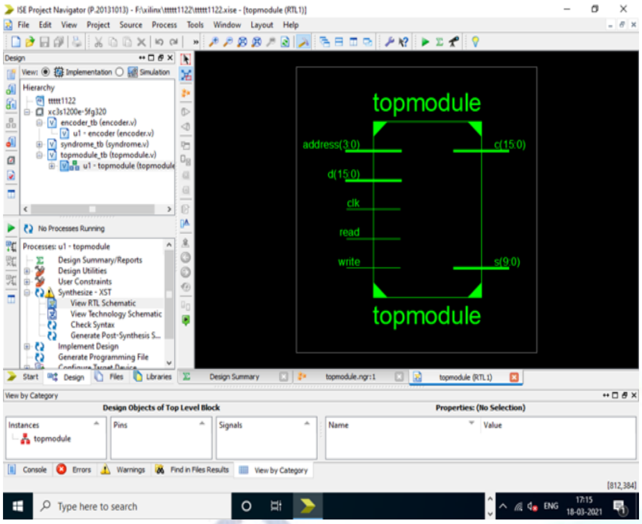


Figure 11: Block diagram of the Encryption Process

Figure 12 shows the block diagram of the proposed decryption process. Here we applied input data (e(7:0),clk,rst) and generated output data (decrypted d(7:0)).RTL schematics depict the digital logic at a higher abstraction level, showing the flow of data between registers and logic elements. This representation is vital for understanding the data flow within the circuit, facilitating optimization, synthesis, and ensuring proper mapping of the design to hardware.

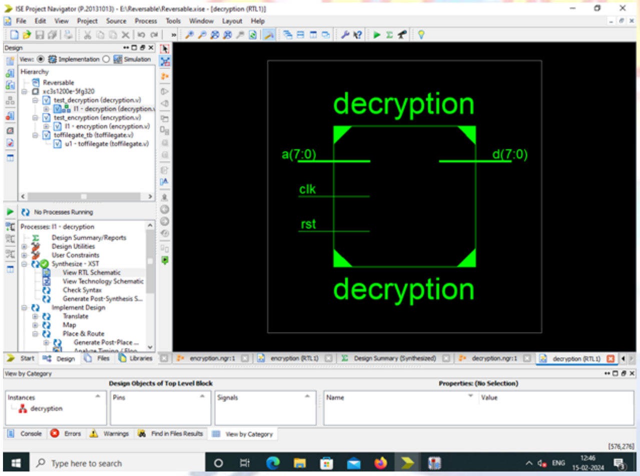


Figure 12: Block diagram of the Decryption Process

. Figures 13 & 14 shows the RTL schematic of the proposed encryption and decryption processes.

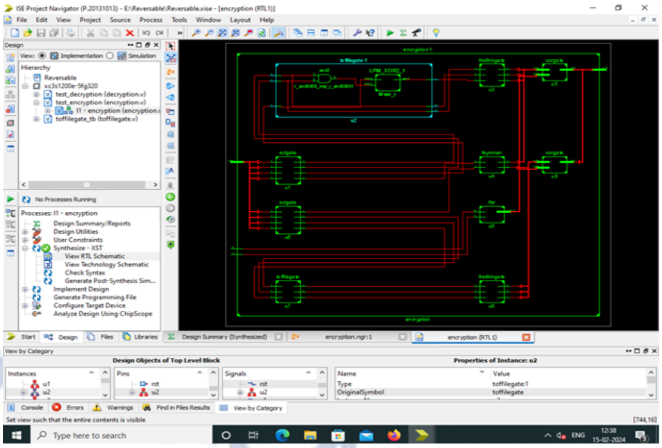


Figure 13: RTL Schematic of the Encryption process

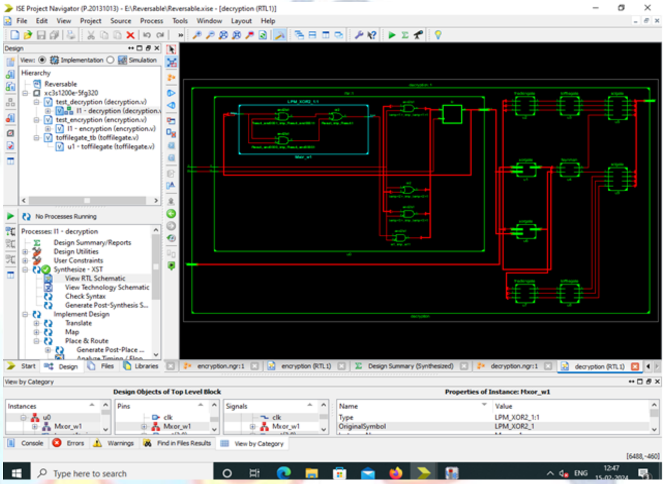
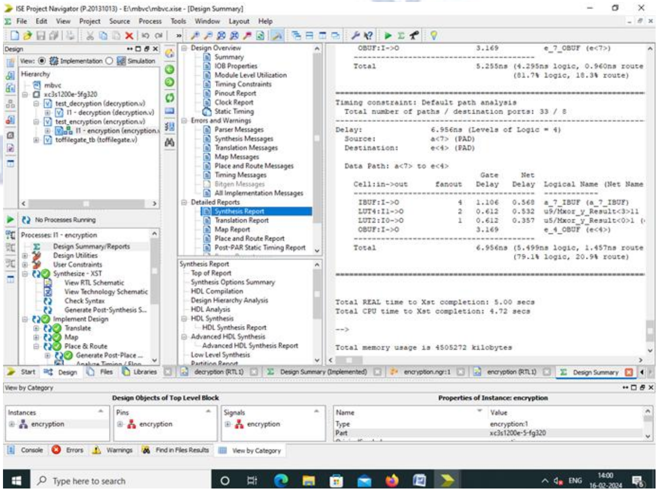


Figure 14: RTL Schematic of the Decryption process

Delay estimation is essential for ensuring that the designed circuit meets timing requirements. It helps identify and address timing issues such as setup and hold time violations, ensuring that signals propagate through the circuit within the specified time constraints. Figures15 & 16 presents the delay estimation of the encryption process and decryption process. The delay in the encryption is 6.954nsand the delay in the decryption is 7.041ns.

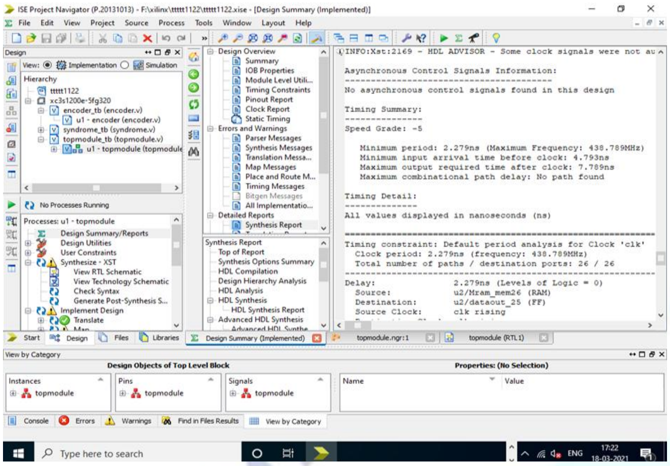


```
 OBUF:I->O                   3.169          e_7_OBUF (e<7>)
   ----------------------------------------
   Total                     5.255ns (4.295ns logic, 0.960ns route
                                     (81.7% logic, 18.3% route)

=========================================================================
Timing constraint: Default path analysis
  Total number of paths / destination ports: 33 / 8
-------------------------------------------------------------------------
Delay:               6.956ns (Levels of Logic = 4)
  Source:            a<7> (PAD)
  Destination:       e<4> (PAD)

  Data Path: a<7> to e<4>
                                Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name
    ----------------------------------------  ------------
     IBUF:I->O             4   1.106   0.568  a_7_IBUF (a_7_IBUF)
     LUT4:I1->O            2   0.612   0.532  u9/Mxor_y_Result<3>11
     LUT2:I0->O            1   0.612   0.357  u5/Mxor_y_Result<0>1 (
     OBUF:I->O                 3.169          e_4_OBUF (e<4>)
    ----------------------------------------
    Total                      6.956ns (5.499ns logic, 1.457ns route
                                       (79.1% logic, 20.9% route)

=========================================================================


Total REAL time to Xst completion: 5.00 secs
Total CPU time to Xst completion: 4.72 secs

-->

Total memory usage is 4505272 kilobytes
```

Properties of Instance: encryption

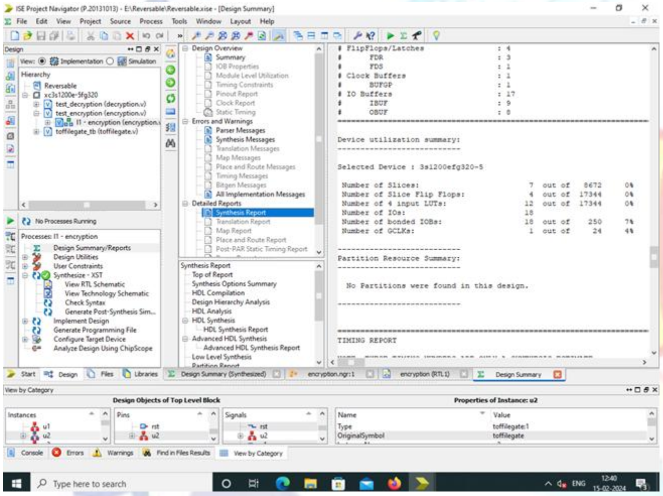
Name	Value
Type	encryption:1
Part	xc3s1200e-5-fg320

Figure 15: Delay estimation of the Encryption


ISE Project Navigator (P.20131013) - F:\xilinx\ttttt1122\ttttt1122.xise - [Design Summary (Implemented)]
File Edit View Project Source Process Tools Window Layout Help
topmodule.ngr:1
topmodule (RTL 1)
Properties: (No Selection)
Type here to search

```
INFO:Xst:2169 - HDL ADVISOR - Some clock signals were not au

Asynchronous Control Signals Information:
----------------------------------------
No asynchronous control signals found in this design

Timing Summary:
---------------
Speed Grade: -5

   Minimum period: 2.279ns (Maximum Frequency: 438.789MHz)
   Minimum input arrival time before clock: 4.793ns
   Maximum output required time after clock: 7.789ns
   Maximum combinational path delay: No path found

Timing Detail:
--------------
All values displayed in nanoseconds (ns)

=========================================================================
Timing constraint: Default period analysis for Clock 'clk'
  Clock period: 2.279ns (frequency: 438.789MHz)
  Total number of paths / destination ports: 26 / 26
-------------------------------------------------------------------------
Delay:               2.279ns (Levels of Logic = 0)
  Source:            u2/Mram_mem26 (RAM)
  Destination:       u2/dataout_25 (FF)
  Source Clock:      clk rising
```

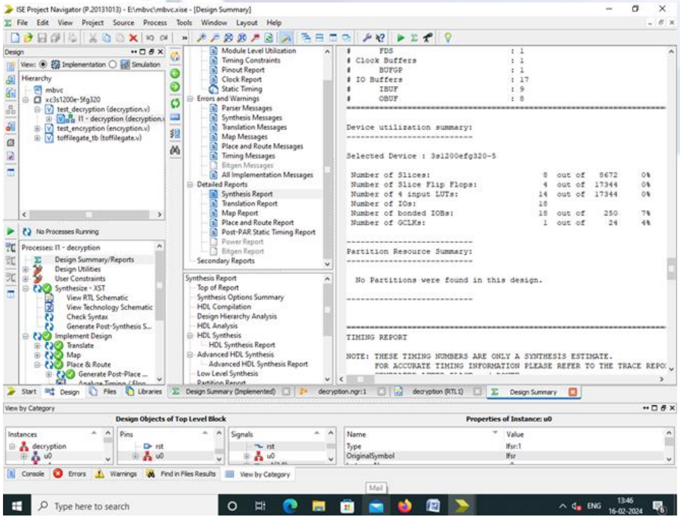
Figure 16: Delay estimation of the Decryption


ISE Project Navigator (P.20131013) - E:\Reversable\Reversable.xise - [Design Summary]
File Edit View Project Source Process Tools Window Layout Help
encryption.ngr:1
encryption (RTL1)
Design Summary
Properties of Instance: u2
Type here to search

```
# FlipFlops/Latches                : 4
#      FDR                         : 3
#      FDS                         : 1
# Clock Buffers                    : 1
#      BUFGP                       : 1
# IO Buffers                       : 17
#      IBUF                        : 9
#      OBUF                        : 8
=========================================================================

Device utilization summary:
---------------------------

Selected Device : 3s1200efg320-5

 Number of Slices:                        7  out of   8672     0%
 Number of Slice Flip Flops:              4  out of  17344     0%
 Number of 4 input LUTs:                 12  out of  17344     0%
 Number of IOs:                          18
 Number of bonded IOBs:                  18  out of    250     7%
 Number of GCLKs:                         1  out of     24     4%

---------------------------
Partition Resource Summary:
---------------------------

  No Partitions were found in this design.

---------------------------


=========================================================================
TIMING REPORT
```

Name	Value
Type	toffilegate:1
OriginalSymbol	toffilegate

Figure 17: Device utilization summary of the Encryption


ISE Project Navigator (P.20131013) - E:\mbvc\mbvc.xise - [Design Summary]
File Edit View Project Source Process Tools Window Layout Help
decryption.ngr:1
decryption (RTL1)
Design Summary
Properties of Instance: u0
Type here to search

```
#      FDS                         : 1
# Clock Buffers                    : 1
#      BUFGP                       : 1
# IO Buffers                       : 17
#      IBUF                        : 9
#      OBUF                        : 8
=========================================================================

Device utilization summary:
---------------------------

Selected Device : 3s1200efg320-5

 Number of Slices:                        8  out of   8672     0%
 Number of Slice Flip Flops:              4  out of  17344     0%
 Number of 4 input LUTs:                 14  out of  17344     0%
 Number of IOs:                          18
 Number of bonded IOBs:                  18  out of    250     7%
 Number of GCLKs:                         1  out of     24     4%

---------------------------
Partition Resource Summary:
---------------------------

  No Partitions were found in this design.

---------------------------


=========================================================================
TIMING REPORT

NOTE: THESE TIMING NUMBERS ARE ONLY A SYNTHESIS ESTIMATE.
      FOR ACCURATE TIMING INFORMATION PLEASE REFER TO THE TRACE REPO
```

Name	Value
Type	lfsr:1
OriginalSymbol	lfsr

Figure 18: Device utilization summary of the Decryption

Area estimation provides insights into the physical space occupied by the designed circuit on the semiconductor. It is crucial for optimizing the use of resources and determining the overall size of the chip. Efficient area utilization contributes to cost-effectiveness and manufacturability. Figure 17 presents the area utilization of the encryption process. It requires 12 LUTs. Figure 18 presents the area utilization of the decryption process It requires 14 LUTs. The area report shows that it contains 142 look up tables.

5. CONCLUSIONS

This work presents a Reversible Logic Gate Cryptography Design using LFSR key with watermarking. The reversible gates like Feynman, Fredkin, Toffoli and SCL gates are used in this new cryptography system design. Since a cryptography system demands not only high security but low power consumption this work is one of the best among existing systems. This input pixel values are read using Xilinx ISE. The RLGCD architecture consisting of LFSR, encryption block and decryption block is implemented in Xilinx software. This architecture is suitable for both gray scale images and color images. The watermarking using LSB technique is performed to improve the security of the data. The Xilinx performance result for Spartan3E XC3S500E device gives a far better performance as compared to other existing systems.The reversible logic gates are the fundamental requirement in the emerging field of quantum computation. Thus, each work using the reversible logic gates will help to move forward in the field of quantum logics. Since RLGCD is successfully implemented using Verilog code it can be effectively deployed on ASIC in future.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Gordon E. Moore, “Craming more components onto integrated circuits,” Electronics, pp.114-117, April 1965.

[2] Rolf Landauer, Irreversible and heat generation in the computing process, IBM Research and Development, vol.5, pp.183–191, July 1961.

[3] C.H. Bennett, “Logical reversibility of computation” IBM Research and Development, vol.17, pp.525–532, 1973.

[4] Saranya Karunamurthi, Vineyakumar Krishnasamy Natarajan, “ VLSI implementation of reversible logic gates cryptography with

LFSR key," Microprocessors and Microsystems, Elsevier, vol. 69, pp.68–78, September 2019.

[5] Mehran Mozaffari Kermani, Kaj Reza Azarderakhsh, Siavash Bavat Sarmadi, "Fault resilient lightweight cryptography block cipher for secure embedded systems," in IEEE Embedded System Letters, vol. 6, no. 4, pp.89–92, Dec. 2014.

[6] Shikha Kuchhal , Rakesh Verma, "Security design of DES using reversible logic," Int. J. Comput. Sci. Netw. Security, vol. 15, no. 9, pp. 81–84, September 2015.

[7] Z. H. A. O. Guosheng, W. A. N. G. Jain, "Security analysis and enhanced design of a dynamic block cipher," China Commun., vol. 13, pp. 15–160, January 2016.

[8] Srivatsam Subramanian, Mehran Mozaffari Kermani, Reza Azarderakhsh, Mehrdad Nojoumaian, "Reliable hardware architectures for cryptographyic block ciphers LED and HIGHT," in IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., vol. 36, no.10, pp. 1750-1758, Oct. 2017.

[9] Raghava Garipelly, P. Madhu Kiran, A. Santhosh Kumar, "A review on reversible logic gates and their implementation," in International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 3, March 2013.

[10] Abduullah Bamatraf, Rosziati Ibrahim, Mohd. Najib. B, Mohd. Salleh, "Digital watermarking algorithm using LSB," in 2010 International Conference on Computer Applications and Industrial Electronics, Kuala Lumpur, pp. 155-159, 2010.

[11] Meenal Dadhe, Prof. Anup. R. Nage, "Design of high speed VLSI architecture for LFSR with maximum length feedback polynomial," in International Journal for Scientific Research & Development, vol .3, no. 5, 2015.

[12] Y. G. Praveen Kumar, B. S. Kriyappa, M. Z. Kurian, "Implementation of power efficient 8-bit reversible linear feedback shift register for BIST," in 2017 International Conference on Inventive Systems and Control, Coimbatore, 2017.

[13] B. Koziel, R. Azarderakhsh, M. Mozaffari Kermani, D. Jao, "Postquatum cryptography on FPGA based on isogenies on elliptical curve," in IEEE Trans.Circuits Syst.I, vol. 64, no. 1, pp. 86–99, Jan. 2017.

[14] B. Koziel, R. Azarderakhsh, M. Mozaffari Kermani, "A high performance and scalable hardware architecture for isogeny based cryptography," in IEEE Trans.Comput., vol. 67, no. 11, pp. 1594–1609, Nov. 2018.

[15] H. Zodpe, A. Sapkal, "An efficient AES implementation using FPGA with enhanced security features," in J.King Saud Univ.Eng.Sci., 2018, in press.

[16] Ravikiran, D. N., & Dethe, C. G. (2018). Improvements in Routing Algorithms to Enhance Lifetime of Wireless Sensor Networks. International Journal of Computer Networks & Communications (IJCNC), 10(2), 23-32.

[17] Ravikiran, D. N., & Dethe, C. G. Fuzzy Rule Selection using LEACH Algorithm to Enhance Life Time in Wireless Sensor Networks. Advances in Wireless and Mobile Communications. ISSN, 0973-6972.

[18] Rajesh, G., Thommandru, R., & Subhani, S. M. DESIGN AND IMPLEMENTATION OF 16-BIT HIGH SPEED CARRY SELECT PARALLEL PREFIX ADDER.

[19] Polanki, K., Purimetla, N. R., Roja, D., Thommandru, R., & Javvadi, S. Predictions of Tesla Stock Price based on Machine Learning Model.

[20] Thommandru, R. A PROSPECTIVE FORECAST OF BRAIN STROKE USING MACHINE LEARNING TECHNIQUES.

[21] Rajesh, G., Raja, A., & Thommandru, R. OPTIMIZATION OF MINIATURIZED MICROSTRIP PATCH ANTENNAS WITH GA.

[22] Vellela, S. S., & Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.

[23] Vellela, S. S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimedia Tools and Applications, 83(3), 7919-7938.

[24] Praveen, S. P., Sarala, P., Kumar, T. K. M., Manuri, S. G., Srinivas, V. S., & Swapna, D. (2022, November). An Adaptive Load Balancing Technique for Multi SDN Controllers. In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1403-1409). IEEE.

[25] Priya, S. S., Vellela, S. S., Reddy, V., Javvadi, S., Sk, K. B., & Roja, D. (2023, June). Design And Implementation of An Integrated IOT Blockchain Framework for Drone Communication. In 2023 3rd International Conference on Intelligent Technologies (CONIT) (pp. 1-5). IEEE.

[26] Vellela, S. S., & Balamanigandan, R. An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Netw. Appl.(2023).

[27] Addepalli, T., Babu, K. J., Beno, A., Potti, B. M. K., Sundari, D. T., & Devana, V. K. R. (2022). Characteristic mode analysis of two port semi-circular arc-shaped multiple-input-multiple-output antenna with high isolation for 5G sub-6 GHz and wireless local area network applications. International Journal of Communication Systems, 35(14), e5257.

[28] Srija, V., & Krishna, P. B. M. (2015). Implementation of agricultural automation system using web & gsm technologies. International Journal of Research in Engineering and Technology, 04 (09), 385-389.

[29] Potti, D. B., MV, D. S., & Kodati, D. S. P. (2015). Hybrid genetic optimization to mitigate starvation in wireless mesh networks. Hybrid Genetic Optimization to Mitigate Starvation in Wireless Mesh Networks, Indian Journal of Science and Technology, 8(23).

[30] Potti, B., Subramanyam, M. V., & Prasad, K. S. (2013). A packet priority approach to mitigate starvation in wireless mesh network with multimedia traffic. International Journal of Computer Applications, 62(14).

[31] Potti, B., Subramanyam, M. V., & Satya Prasad, K. (2016). Adopting Multi-radio Channel Approach in TCP Congestion Control Mechanisms to Mitigate Starvation in Wireless Mesh Networks. In Information Science and Applications (ICISA) 2016 (pp. 85-95). Springer Singapore.