Efficient Reversible For Quantum Computing A Novel 4-Bit LFSR Approach

J.Vanaja[1], K.Suresh Kumar[2]
[1]Dept of ECE
[2]Assistant Professor, Dept of ECE
[1, 2] TAGORE INSTITUTE OF ENGINEERING AND TECHNOLOGY(TAMILNADU)

Abstract- *Reversible logic gates are critical components in the field of quantum computing and low-power digital circuits, as they allow for the retrieval of input states from output states without any loss of information. This property ensures minimal energy dissipation, aligning with the principles of reversible computation. Their applications extend to quantum computing, cryptographic systems, and error detection and correction mechanisms. This paper presents a novel design for a Reversible D Flip-Flop (RDFF) and a 4-bit Linear Feedback Shift Register (LFSR). The Linear Feedback Shift Register (LFSR) is built utilizing four Register-Driven D Flip-Flops (RDFFs) and a feedback mechanism that incorporates a Feynman Gate. This configuration successfully showcases the capacity to generate pseudo-random sequences. The LFSR design demonstrates a 10%improvement in Total Reversible Logic Implementation Cost and27% enhancement in quantum cost, making it a more resource efficient option for reversible computing. This work makes a valuable contribution to the field of reversible computing by offering efficient designs for essential components.*

Keywords- Reversible logic, Ancilla Inputs, Garbage outputs, Low power, Linear Feedback Shift Register (LFSR).

I. INTRODUCTION

Reversible logic gates are essential in quantum computing and low-power digital circuit design due to their unique property of information conservation. Unlike conventional logic gates, reversible logic gates ensure that every output configuration can be uniquely mapped back to its corresponding input configuration. This bijective functionality means no information is lost during computation, reducing power dissipation, a crucial advantage as information loss in traditional circuits results in heat generation according to Landauer's principle. By enabling the reconstruction of original inputs from the outputs, reversible logic gates facilitate the design of energy efficient computing systems, which are essential for advancing technology in the era of quantum computing and sustainable electronics.

The design of reversible logic gates often involves implementing gates such as the Toffoli, Fredkin, and Peres gates, which can perform complex operations while maintaining reversibility. These gates can form the building blocks for more complex reversible circuits, including arithmetic and logical units, crucial for the development of quantum computers. The focus on reversible logic is not only a step toward quantum computing but also an approach to creating more sustainableand efficient classical computing systems. Reversible logic gates are also pivotal in the emerging field of nanotechnology and molecular computing, where minimizing energy dissipation is critical due to the small scale of operations. By utilizing reversible logic, these systems can perform computations with minimal energy loss, paving the way for highly efficient, next-generation computing devices. In addition, reversible logic gates adhere to certain features. For example, they do not permit fan-out, which is the process of using the output of one gate as input to other gates. Furthermore, in order to preserve their reversibility, they frequently require additional constant inputs and generate additional "garbage" outputs. Quantum computing, in which many quantum gates are intrinsically reversible, is only one of the numerous applications of reversible logic.

Other applications include encryption and low-power CMOS architecture. Multipliers play crucial roles in digital signal processing (DSP) and many mathematical processes. Multipliers that are traditionally used, on the other hand, are extremely power-hungry and add significantly to the overall energy consumption of digital systems. Because of the development of Vedic mathematics, which has effective algorithms for multiplication, there is now the possibility of designing multipliers that are not only quick but also efficient in terms of energy consumption. Whenever Vedic multipliers are combined with reversible logic, they have the potential to significantly improve computing efficiency by reducing the amount of power that is dissipated.

Additionally, the principles of reversible computing arebeing explored in fault-tolerant computing systems, where the ability to trace back steps and recover from errors can

enhance system reliability and performance. This makes reversible logic a versatile and promising area of research with wide ranging applications in both current and future technologies.

Linear Feedback Shift Registers (LFSRs) are sequential circuits that are widely utilized in several applications, including error detection and correction, cryptography and digital signal processing. An LFSR is a type of shift register where the input bit is determined by a linear function of its prior state. This function is usually implemented using exclusive OR (XOR) operations on specific bits. The feedback mechanism in LFSRs ensures that the register cycles through a sequence of states, producing pseudo-random binary sequences. These sequences are deterministic and repeat after a certain period, known as the register's length. The simplicity, speed, and ability to generate long sequences with good statistical properties make LFSRs a valuable tool in various digital applications. A Linear Feedback Shift Register (LFSR) is advantageous dueto its simplicity in design and implementation, making it efficient for hardware applications. It generates pseudo-random sequences with good statistical properties, which are useful in applications such as cryptography, error detection, and digital signal processing.Several power optimization techniques are investigated in many existing BIST architecture which is categorized into architecture level optimization and switching activity reduction. The problems encountered in existing BIST systems in terms of achievable fault coverage over highly complex digital systems demands the development of unified BIST models with new test pattern generator (TPG). In BIST application optimization over LFSR plays significant role to normalize the testing power and to achieve 100% fault coverage with improved randomness level. In this paper, bit swapping LFSR is used in conjunction with state skipping model which reduces the memory space requirement of conventional LFSR and modified Multiple Input Signature Register (MISR) for improved output response analyzes. The core objective is to reduce the switching activity during testing process using modified LFSR test pattern generator which can generate patterns with less transitions over two successive test inputs. To reduce the complexity overhead bit swapping LFSR is designed using MUX based data flow control and state skipping scheme is introduced to attain maximum fault coverage. In addition to this work, to find faults that are difficult to find the randomness is significantly increased using bit swapping and state skipping LFSR jointly.

II. LITERATURE REVIEW

2.1 Ioannis Voyiatzis, Antonis Paschalis, "A Concurrent Built-In Self-Test Architecture Based on a Self-Testing RAM"

In this paper novel input-vector monitoring concurrent BIST technique for combinational circuits based on a self-testing RAM, termed R-CBIST. Small hardware overhead, whereas there is no need to stop the ROM normal operation .In off-line BIST, the normal operation of the CUT is stalled in order to perform the test. The total circuit performance is degraded. We propose a novel technique for online testing, which we call Built-In Concurrent-Self- Test (BICST). BICST assumes the presence of underlying BIST resources for off-line testing. These resources are modified in such a way that they can be used for both off-line and online testing. We also propose a technique for sharing the BICST hardware resources between identical circuits, thereby reducing the overall extra overhead for testing.

2.2. Ioannis Voyiatzis and Constantin Halatsis "A Low-Cost Concurrent BIST Scheme for Increased Dependability"

In this paper a concurrent BIST technique for combinational circuits is presented. Significantly more efficient than the input vector monitoring techniques proposed. Concurrent Test Latency and hardware overhead trade-off, for low values of the hardware overhead. Number of theorems required Input vector-monitoring concurrent BIST techniques are suitable for the testing of ROM because they meet both above requirements. The results in low hardware overhead, and therefore it is a practical solution for the concurrent testing of ROM modules, a BIST scheme for ROM modules should meet two basic requirements no need to set the ROM off-line very high effective fault coverage.

III. METHODOLOGY

LFSR AND BILBO

A brief description about LFSR and BILBO is given in this section used to data encoded using 64 bit.

3.1 64-BIT LFSR DESIGN

In computing, a linear-feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is exclusive-or (XOR).

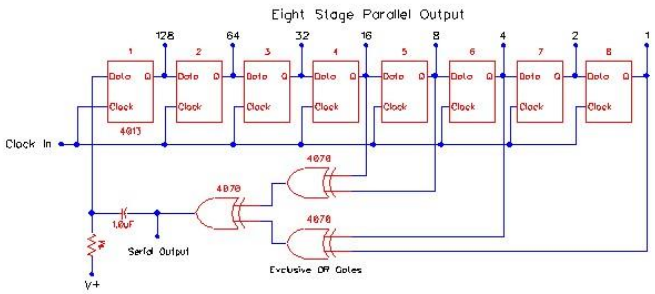

Figure 1: 64 bit LFSR structure

A simple 8-bit linear feedback shift register built from D-flip-flops. In this example, the outputs of flip-flops 8,6,5,4 are summed via XNOR gates (this is a linear operation, hence the name) and fed back into the first flipflop. Just wait for a few clock impulses and watch the output values of the register, which should appear more or less random. Depending on the logic used in the feedback path, the register follows a predefined sequence of states, with a maximum sequence length of (2^n)-1 in a n-bit register. Perhaps the most important use of LFSRs is as pseudorandom number generators, especially for automatic self-test, because the generators are very cheap and can be run at very high clock frequencies. With a register of n+1 bits, each n-bit input value can be generated. Naturally, subsequent output values are highly correlated, as only the first bit changes while all other bits are simply shifted.

Note that the feedback logic used in many textbooks has the stable state 000000, while all other states are in the single large pseudorandom sequence of the primitive polynom corresponding to the feedback path. Unfortunately, this means that a default realization with a power-on initialization to the all-zero state will not work, because the register would stay forever in the all-zero state. One obvious workaround is to use a power-on initialization to some other state, e.g. all-ones via flipflops with set inputs. The other possibility, used in this applet, is to change the feedback path so that the all-zero state is not stable. n general, a basic LFSR does not produce very good random numbers. A better sequence of numbers can be improved by picking a larger LFSR and using the lower bits for the random number. For example, if you have a 10-bit LFSR and want an 8-bit number, you can take the bottom 8 bits of the register for your number. With this method you will see each 8-bit number four times and zero, three times, before the LFSR finishes one period and repeats. This solves the problem of getting zeros, but still the numbers do not exhibit very good statistical properties. Instead you can use a subset of the LFSR for a random number to increase the permutations of the numbers and improve the random properties of the LFSR output.

3.2 64 BIT BILBO

Built In Logic Block Observer has gained importance for its ability to take up different types of responsibilities depending upon the control signals forced on it. For instance, it can function as a simple register and in other, it can function as a Pseudo Random Test Pattern Generator (PRTPG); also, to generate signatures for analysis, it can act as a Multiple Input Signature Register (MISR) too . The different modes of BILBO are tabulated in Table I for a better understanding. The clear distinction of its modes and functionality is detailed in. BILBO allows the design engineers to execute the process of testing the logic circuits in a scheduled manner so as to have a good understanding of the outputs for the state in which the BILBO functions. For example, in a clock cycle if a particular of the BILBO registers acts as a MISR; its availability for that instance is reserved. It is only in the next clock cycle, it can act as an LFSR or as a simple register depending upon the need of testing application.

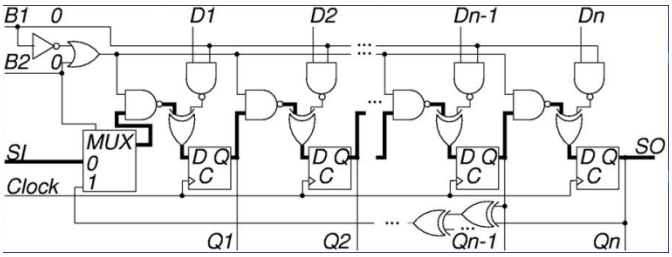

Figure 2: 64-Bit BILBO

Flip-flops from the CUT to construct the TPG and ORA functions. The basic idea is to partition the CUT into groups of flip-flops and groups of combinational logic. Each group of flip-flops is augmented with additional logic to provide multiple modes of operation. When the BILBO functions as a TPG, it provides pseudo-random test patterns by operating as an LFSR. When the BILBO functions as an ORA, it performs multiple-input signature analysis by operating as a MISR. The application of BILBO to a CUT in its simplest form is illustrated, where the flip-flops at the primary inputs and outputs are used to construct two BILBOs. The BILBO at the primary inputs generates pseudo-random test patterns as a TPG and the BILBO at the primary outputs operates as a MISR-based ORA. The task of determining whether fabricated chips are fully functional is highly complex and will be take much more time, energy and cost. It is know the debugging cost increase by abouttenfold from chip level to system level. Therefore the Design for Testability (DFT) is introduced in order to detect faults as early as possible. DFT is a name for design techniques that add certain testability features to the premise of the added features is that they make it easier to develop and apply manufacturing tests for the designed hardware. The purpose of manufacturing tests is to

validate that the product hardware contains no defects that could, otherwise, adversely affect the product's correct functioning. The figure shows how the Built in Self-Test (BIST) running in the ICs. Built-in logic block observation (BILBO) has become one of the most widely accepted techniques for self-testing of complex digital ICs. This technique is based on grouping the storage elements of the circuit in the two registers which give this technique its name. A BILBO register has four functional modes: with each of the stages acting as independent registers; as agenerator of pseudorandom sequences; as analyzer of multiple-input signatures; and resetof all stages. Now days, an engineer design the BILBO with the various type in order to make it reliability to use. As the number of transistor integrated into a single chip increase, mean that more power dissipated will be produce. BIST is requiring more circuit to be added to the digital ICs to test itself. Most of the engineers face this problem when design the ICs. In order to make the ICs run efficiently and reliability, the low power BILBO must be introduce. Then the problem power dissipated can be laminated.The power consumption is one of the most important issues especially the testing approaches are used. Power consumption due to test application, therefore, may be even higher than that required in the system mode. The increased power may reduce the life of batteries, cause some reliability problems, and may even damage the circuit under test (CUT).

1V. SIMULATION RESULTS

4.1 RTL SCHEMATIC OF 64-BIT BILBO

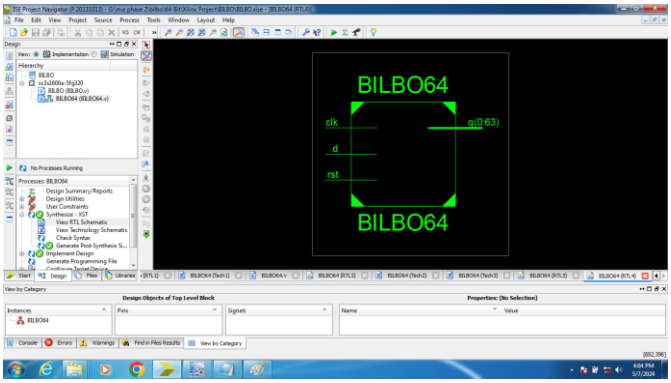

Figure 3: RTL View of 64-bit BILBO

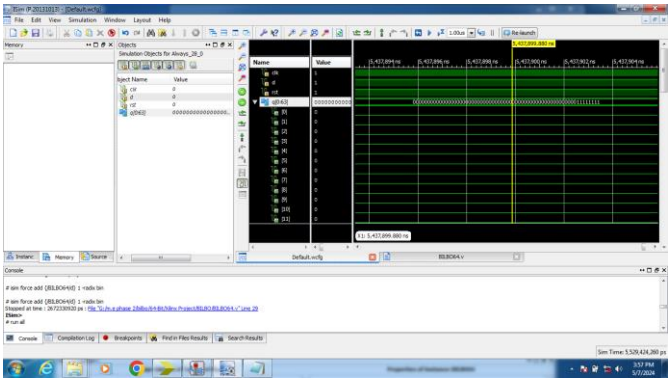

Figure 4: Xilinx Output of 64-bit BILBO

4.2 RTL SCHEMATIC 64-BIT LFSR

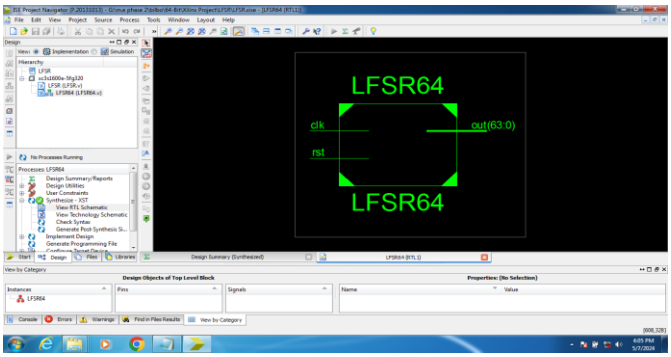

Figure: 5 RTL view of 64-bit LFSR

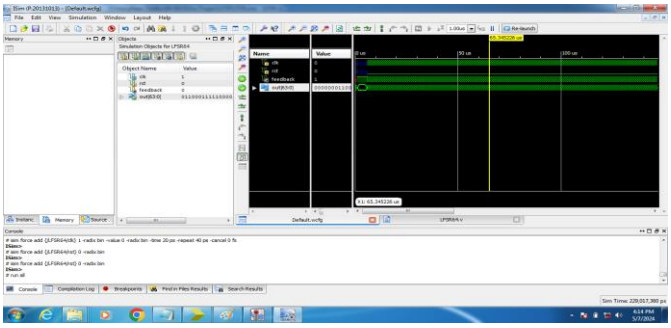

Figure: 6 Xilinx output of 64-bit LFSR

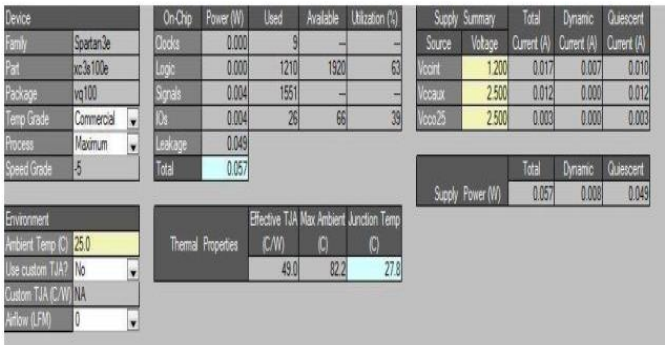

Figure 7: Power Analysis of Approximate Multiplier

V. CONCLUSION

In the proposed research work, a novel design for 4-bit Linear Feedback Shift Register (LFSR) and a Reversible D Flip-Flop (RDFF) has been proposed and implemented using Xilinx software with source code written in Verilog HDL. The RDFF achieves reversible functionality by employing a Feynman Gate and an MFG. The output of the Feynman Gate corresponds to the outcome of the D flip-flop. The Linear Feedback Shift Register (LFSR), comprised of four Register-Data-Flip-Flops (RDFFs) plus a feedback mechanism utilizing a Feynman Gate, successfully demonstrates the capability to generate pseudo-random sequences and exhibits consistent performance across a variety of initial inputs, as verified by the simulation results. The RDFF design reduces the total number of ancilla inputs by 75% compared to previous designs. Moreover, the LFSR architecture exhibits a 27% enhancement in quantum cost and a 10% improvement in Total Reversible Logic Implementation Cost (TRLIC).

REFERENCES

[1] A. Roohi, R. Zand, S. Angizi and R. F. DeMara, "A Parity-PreservingReversible QCA Gate with Self-Checking Cascadable Resiliency," in IEEE Transactions on Emerging Topics in Computing, vol. 6, no. 4, pp. 450-459, 1 Oct.-Dec. 2018.

[2] S. Raveendran et al.,"An Approximate Low-Power Lifting Scheme Using Reversible Logic," in IEEE Access, vol. 8, pp. 183367-183377, 2020.

[3] E. Fredkin and T. Toffoli, "Conservative logic," in Collision-based computing. Springer, pp. 47–81, 2002.

[4] T. Toffoli, "Reversible computing," in Automata, Languages and Programming, ser. Lecture Notes in Computer Science, J. de Bakker and J. van Leeuwen, Eds. Springer Berlin Heidelberg, 1980, vol. 85, pp. 632–644, 1980.

[5] D. P. Vasudevan, P. K. Lala, J. Di, and J. P. Parkerson, "Reversible-logic design with online testability," IEEE transactions on instrumentation and measurement, vol. 55, no. 2, pp. 406–414, 2006.

[6] Kumar, A.S., Naresh Kumar Reddy, B. "An Efficient Real-Time Embedded Application Mapping for NoC Based Multiprocessor System on Chip", Wireless Personal Communications, vol. 128, pp.2937–2952,2023.

[7] B. Naresh Kumar Reddy et al., "Evaluating the Effectiveness of Bat Optimization in an Adaptive and Energy-Efficient Network-on-Chip Routing Framework," Journal of Parallel and Distributed Computing, Vol. 188, 2024.