RESEARCH PAPER

Low-Power Reversible LFSR Architecture for Cryptography-Oriented Applications

D. Lakshmi Narayana[1*], Bugga Chaitanya[2], Mahesh Mudavath[3], Boda Srilekha[4]
[1]Associate Professor, ECE (VLSI), Siddhartha Institute of Technology & Sciences, Ghatkesar – 500088
Email: dr.lakshman@siddhartha.org.in
[2]M.Tech, ECE (VLSI), Siddhartha Institute of Technology & Sciences, Ghatkesar – 500088
Email: 24TQ1D5702@siddhartha.co.in
[3]Associate Professor, ECE (VLSI), Siddhartha Institute of Technology & Sciences, Ghatkesar – 500088
Email: dr.mahesh@siddhartha.org.in
[4]Assistant Professor, ECE (VLSI), Siddhartha Institute of Technology & Sciences, Ghatkesar – 500088
Email: bodasrilekha.ece@siddhartha.co.in
***Corresponding Author:** D. Lakshmi Narayana, Associate Professor, ECE (VLSI), Siddhartha Institute of Technology & Sciences, Ghatkesar – 500088
Email: dr.lakshman@siddhartha.org.in

Received: 25th October 2026; **Revised:** 28th October 2026; **Accepted:** 3rd November 2026; **Available Online:** 7th November 2026

ABSTRACT
Linear Feedback Shift Registers are popular cryptographic tools to generate pseudo-random sequences as they are simple and fast. Nevertheless, traditional LFSR architecture is characterized by loss of information and high power consumption which restricts its applicability in low-power and emerging computing paradigms. The concept of reversible logic has become a focus of much attention because, in theory, it allows achieving zero information loss and lower power dissipation, thus becoming a promising solution towards energy-efficient cryptographic hardware.
This paper describes a low-power reversible LFSR architecture for cryptography-based applications. The design proposed makes use of reversible logic gates to perform the shift and feedback steps of the LFSR with reversibility being maintained. The architecture guarantees proper pseudo-random sequence generation at the expense of enhanced energy efficiency compared to traditional LFSR architectures. The proposed reversible LFSR is functionally correct and is verified by simulation, and the output shows the correct operation of the shift register and the feedback. The nature of the proposed LFSR architecture, based on its low-power nature and ability to be reversible, is particularly suitable in terms of future secure and energy-efficient cryptographic usage.

Keywords: Cryptography, Feedback Shift Register, Low-Power Design, Pseudo-Random Sequence Generation, Reversible Logic
How to cite this article: *D. Lakshmi Narayana1* Bugga Chaitanya2 Mahesh Mudavath3 Boda Srilekha4. Low-Power Reversible LFSR Architecture for Cryptography-Oriented Applications. Int J Drug Deliv Technol. 2026;16(90s):1449-1453. DOI: 10.25258/ijddt.16.90s.145.*
Source of support: ***Nil.***
Conflict of interest: *None*

I. INTRODUCTION

Cryptography is an indispensable part of a contemporary digital system and provides security in communication and data protection in deployed systems and applications, including wireless network, embedded systems, and Internet of Things (IoT) devices. One major need of cryptographic systems is the production of pseudo-random sequences that are usually achieved by the use of Linear Feedback Shift Registers (LFSRs). LFSRs are commonly used in stream ciphers, key generation, scrambling, and error detection systems due to their simplicity, speed, and their ability to be implemented easily with hardware [1]. Traditional LFSR architecture is normally instantiated by irreversible logic operation, whereas computation loss is incurred. Loss of information in digital circuits causes energy dissipation in the form of heat according to basic concepts of thermodynamics, thus these designs are not appropriate in low-power operations [2]. The increased use of cryptographic hardware in energy-saving resource limited environments, minimizing power usage has become a huge design goal [3].

Reversible logic has been found to offer a useful design paradigm to low power digital systems, where they can guarantee a one to one correlation between the input and output vectors, and thus information loss during computation can be avoided [4]. Because of this property, reversible logic has been of great interest in low-power VLSI design and quantum computing systems [5]. The design of energy efficient digital circuit with reversible logic gates allows maintaining functional correctness [6]. A number of studies have shown that reversible logic can successfully be used in sequential circuits like shift registers, pseudo-random sequence generators etc. Application of LFSRs with reversible logic gates has been found to be power efficient relative to the traditional irreversible designs [7]. Also, it has been announced that reversible logic-based cryptographic architectures can deliver less power dissipation without compromising the security of their operation [8].

Recently, reversible logic has further been investigated to provide cryptographic and security-related applications. The reversible logic-based encryption and data protection methods have proved to have increased energy efficiency and reliability [9]. There has also been an exploration of the combination of reversible logic and image encryption system as well as secure data transmission systems indicating it to be suitable with security application [10]. The design work on LFSR has been aimed at enhancing flexibility, performance

and security. LFSR architectures have been suggested to be programmable and reconfigurable in order to increase the strength of cryptography and flexibility [11]. Moreover, the implementation of shift registers and LFSRs with new technologies has shown the potential of being faster and consuming less power [12].

Reversible logic-based LFSR-based designs have been studied in security applications of high speed and low power. These designs have demonstrated better performance features and the ability to fit the current cryptographic systems [13]. Reconfigurable LFSR architectures have also found some applications in communication and coding, and again bring out the significance of efficient LFSR architectures [14]. The reversible logic-based cryptographic hardware has also been used to ensure safety of data transmission with a lot of success, which proves the suitability of the technology in the modern security-focused systems [15].

Although these progress have been made, simple and efficient reversible LFSR designs that concentrate on low power usage but at the same time make sure that pseudo-random sequences are properly generated are still required. Due to this reason, the current paper will present a low-power reversible LFSR-based architecture suitable in applications relating to cryptography.

II. LITERATURE SURVEY

LFSRs find extensive application in cryptography because they can be used to produce pseudo-random streams with a very simple hardware implementation. In their applications, they are used in stream ciphers, scrambling and generation of keys, and detection of errors. Previous research has indicated that LFSRs are fast and require little effort to apply thus they can be used on both hardware and software-based cryptographic software [1]. But this is also a problem as the simplicity of conventional LFSR designs also presents power consumption problems and security robustness. The traditional LFSRs are executed in irreversible logic circuits, in which information is lost in the process of calculation. Such loss of information leads to the dissipation of energy that turns out to be a severe constraint in low-power and energy-constrained systems like embedded systems and IoT devices [2]. With the continued development of cryptographic hardware to support portable and battery powered applications, power dissipation has become a major design consideration [3].

Reversible logic has been suggested as a good solution to the problem of power dissipation in the digital circuit. The reversible circuits guarantee a one to one match between the input and output vectors eliminating loss of information in computation [4]. Because of this property, reversible logic has become of great interest in low-power VLSI design and quantum computing applications [5]. Theoretical analysis has demonstrated that reversible circuit can greatly minimize dissipation of energy over irreversible ones [6]. A number of studies have been dedicated to reversible logic application schemes to sequential circuits. The reversible logic-based shift registers have been found to have low power consumption and still exhibit proper functional characteristics [7]. These designs make use of reversible gates to implement shift operations without the loss of information and as such they are applicable in the implementation of energy efficient sequential logic. The combination of reversible logic and cryptographic architecture has also enhanced its applicability. Logic-based cryptographic systems open to reversal have been demonstrated to consume less power whilst providing a secure data processing [8].

Reversible gate is used in encryption and decryption modules which has shown better energy efficiency without affecting cryptographic strength [9]. New investigations have been carried out in reversible logic-based LFSR architectures as applications in cryptography. These publications point out that reversible LFSRs incur smaller power consumption than traditional LFSRs and produce the right pseudo-random streams [10]. Reversible gates are also applied in feedback and shift operations and this has also been identified as a cause of power reduction. Design improvements on LFSR have also emphasized on flexibility and security. Dynamic resistance to cryptographic attacks Programmable LFSR architectures permit a customer to dynamically modify feedback polynomials [11]. It has been suggested to implement reconfigurable LFSR structure to facilitate the use of various modes of cryptography in enhancing flexibility in secure communication systems [12].

Recent studies have also explored the LFSR implementations with new architectures and technologies to further enhance the performance and efficiency. The objectives of such designs include the ability to attain increased operating speeds and low power usage without incurring compromised pseudo-random sequence generation [13]. Besides this, reconfigurable LFSRs have also been used in communication and coding applications proving their usefulness beyond cryptographic systems [14]. Cryptographic hardware that uses reversible logic has also been successfully used to provide security to data transmission systems. These applications point to the usefulness of the reversible logic in the pursuit of energy efficient and sound security solutions in a contemporary digital frameworks [15]. The presented findings support the idea that reversible logic is a prospective tool of designing low-power cryptographic devices.

III. PROPOSED WORK

The work suggested is a low-power reversible LFSR architecture, which is architected with cryptography-based applications. The core goal of the proposed architecture is to generate the pseudo-random sequences with a lower power consumption through the use of reversible logic principles. The proposed design will remain reversible (compared to the traditional LFSRs) because, unlike conventional LFSRs, where irreversible logic is applied, the proposed design will organize the input and output states in a one-to-one relationship.

A. Design Principle of Reversible LFSR

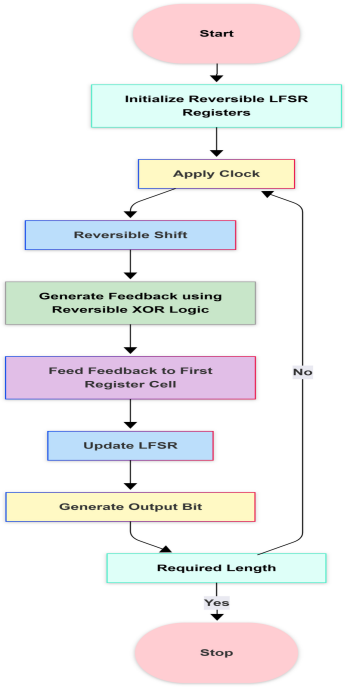

Fig. 1. Flowchart illustrating the operation of the proposed reversible LFSR architecture.

In reversible logic circuitry, every possible output state is a distinct state of the input state meaning that no information is lost when calculating the state. This property allows theoretically lower energy dissipation and reversible logic is very well adapted to low-power cryptography. The suggested reversible LFSR architecture is developed on reversible logic gates to execute the shift operation and the feedback operation and maintain reversibility. The reversible LFSR will be used in the generation of feedback by rearranging the register contents in direction defined by a characteristic polynomial. The reversible gates are used to implement the feedback logic which dictates that the state of the LFSR at a given time is uniquely defined by the state of the LFSR in the current time. The flow chart in Fig. 1 shows the operational flow of proposed reversible LFSR, its initialisation, reversible shifting, generation of feedback as well as sequence generation.

B. Architecture Description

The suggested reversible LFSR is a cascading of reversible storage elements which form a shift register. The reversible logic is carried out at each stage of the shift register, such that the shift process does not lead to information loss. XOR-based logic is generated to compute reversible feedback bit feed is based in reversible logic. The reversible logic gates combine the output of some stages of the shift register to create the feedback signal. The signal is then fed back as an input to the first stage of the register. The proposed reversible LFSR can be used to produce pseudo-random sequence to be used in cryptography by effectively designing the feedback logic and choosing the right characteristic polynomial.

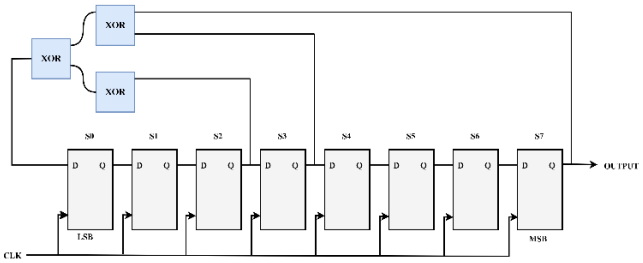

Fig. 2. Block Diagram of an 8-bit Reversible LFSR with XOR-Based Feedback.

C. Reversibility and Low-Power Characteristics

One of the main benefits of the suggested architecture is the fact that the architecture is reversible, so every internal state of the LFSR has a unique way to trace back to the previous one. This property eliminates loss of information and it is much lower than power dissipation as a result of irreversible operations. The resulting proposed reversible LFSR architecture is therefore energy efficient in nature, and suitable in low power cryptographic systems. Moreover, it has fewer switching activities and better power efficiency because there are no fan-out and feedback loops that do not satisfy reversibility constraints. These features qualify the suggested architecture to be implemented in the energy-constrained environment like a secured communication device and embedded systems.

D. Suitability for Cryptographic Applications

The suggested reversible LFSR design produces pseudo-random sequences of the correct period and randomness characteristics needed in cryptography. The architecture is especially applicable to key generation and scrambling, reversible stream cipher initialization and scrambling, as well as other applications that require low power and a reversible nature. The proposed design is also easy to scale to LFSRs of higher bit-width and can be easily adapted to larger cryptographic systems. The above characteristics render the proposed reversible LFSR an effective and convenient solution to the present cryptography-oriented hardware.

IV. Results and Discussion

The low-power reversible LFSR architecture proposed was tested to ensure that it was functionally correct, and that it was an appropriate architecture to be used in cryptography-related applications. The figures indicate the findings as waveforms of simulation and output characteristic plots, which outline proper generation of pseudo-random sequence and stability of the reversible LFSR.

A. Functional Simulation Results

The proposed reversible LFSR was checked using its functional behavior through the observation of the output sequence and successive clock cycles. The simulation waveform with the clock signal, reset signal, enable signal, and output signal is represented by Fig. 3. It is found that the sequence of output varies at each active clock edge whenever enable signal is asserted. The output generated is pseudo-random, which proves right shift and feedback operations. The fact that the proposed reversible LFSR architecture does not exhibit undefined states in the waveform is an indication of stability and proper operation of the architecture. It is also evidenced by the fact that the reversible shift and feedback operations are carried out in the proper way as the waveform lacks any defined or invalid states. These findings confirm

the functional accuracy of the proposed reversible LFSR structure.



Fig. 3. Simulation waveform of the proposed reversible LFSR showing clock-driven shift operation and reversible feedback generation.

B. LFSR State and Sequence Verification

To check whether the pseudo-random sequences were generated properly, the transitions of the LFSRs were examined. The successive clock cycles were monitored on the inner states of the LFSR and the resultant output sequence documented. The transitions between states observed prove that the LFSR transitions between valid states without repeating itself until the sequence period is achieved. The resulting sequence of output has pseudo-random properties and has the desired dynamics of an LFSR-based sequence generator. This check establishes that the feedback poly and shifting functional are properly done. The sequence acquired can be used to verify the correctness of the functionality of the proposed reversible LFSR architecture.

Conventional LFSR State Transitions: [1, 1, 1, 1], [0, 1, 1, 1], [0, 0, 1, 1], [1, 0, 0, 1], [1, 1, 0, 0]

Conventional LFSR Output Sequence: [1, 1, 1, 1, 0]

C. Output Sequence Characteristics

In order to study the behavior of the reversible LFSR further, the observed sequence of the generated output was noted throughout several clock cycles. The generated output is pseudo random in nature and this is fundamental in key generation and stream ciphers in cryptographic applications. The constant change of the output bits proves that the feedback poly as well as the shift operation are working as desired. The resultant sequence is periodic, in line with LFSR theory, which implies that the proposed architecture will provide the right sequence generation and remain reversible.

D. Graphical Analysis of Output Behavior

Besides waveform analysis, a graphical data of the LFSR output behaviour was also obtained by plotting the sequence values generated. Fig. 4 shows the output nature of the reversible LFSR in a given number of cycles. The plot demonstrates a steady change of the values of output, which proves the stable and repeatable functionality of the architecture. The fact that this graphical analysis indicates the proposed reversible LFSR as being suitable when used in cryptological applications where randomness and reliability are paramount.

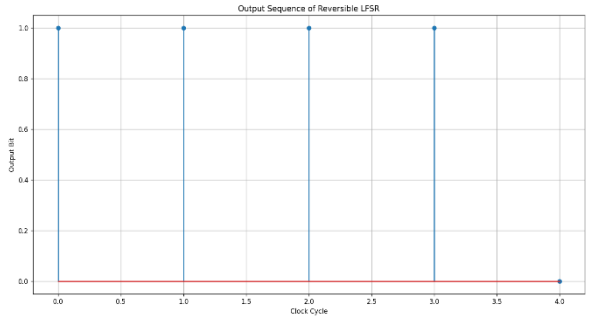

Fig. 4. Output characteristics of the proposed reversible LFSR over successive clock cycles.

The discussed findings substantiate the fact that the offered reversible LFSR architecture is able to execute proper shift and feedback functions and produce pseudo-random sequences that are necessary in cryptographic usage. The graphical and waveform results show that the system operates stably, that the state changes are correct and that no information is lost. The given architecture can be run with low-power consumption and be functionally correct through the use of reversible logic. These findings demonstrate the usefulness of reversible logic in the development of energy-efficient cryptography hardware and confirm the proposed reversible LFSR as an appropriate block of the secure and low-power systems.

E. Comparison

The functional behavior and suitability of the conventional LFSR and the proposed reversible LFSR was compared and contrasted to identify the suitability of each in cryptographic applications. The standard LFSR was originally studied by observing the internal state transitions and the resulting output sequence at a time, per successive clock cycle. The traditional design has the right state transitions and generates a pseudo-random sequence of outputs as desired. Nevertheless, the traditional LFSR implementation is done with irreversible logic, which causes loss of information with each transition of state. After the register goes to the next state, the former state cannot be uniquely reconstituted. This is an irreversible form of behavior that causes more power dissipation, thus the traditional LFSR is not so well-suited to low-power cryptographic systems. The suggested reversible LFSR architecture, in contrast, produces a parallel pseudo-random sequence of outputs but is reversible. Every state transition of the reversible LFSR has a one-to-one relation between input state and output state, and the former can be uniquely reconstructed in terms of a current state. This characteristic provides the maintenance of information and helps in the minimization of power loss. The comparison verifies that the conventional and reversible LFSRs are correct in the generation of pseudo-random sequences. The reversible LFSR, however, has a major benefit in regard to energy efficiency because it is information preserving. This renders the suggested reversible LFSR better adapted to low-power applications and cryptography friendly applications than the traditional LFSR design. Table 1 offers the comparison of the conventional LFSR and the proposed reversible LFSR architecture. The two designs produce the right pseudo-random sequences but the traditional LFSR is done on irreversible logic and it loses information as the states change. Conversely, the reversible LFSR maintains state data and enables states to be recovered uniquely in the past resulting to low power dissipation. Such a comparison demonstrates the benefits of the suggested reversible LFSR in the low-power applications in cryptography.

Table 1. Comparison of Conventional and Reversible LFSR Architectures

Parameter	Conventional LFSR	Reversible LFSR (Proposed)
Logic Type	Irreversible logic	Reversible logic
Information Loss	Present	Absent

State Recoverability	Previous state cannot be recovered	Previous state can be uniquely recovered
Power Dissipation	Higher due to information loss	Reduced due to reversibility
Suitability for Low-Power Applications	Limited	High
Cryptographic Applicability	Moderate	High

V. CONCLUSION

This paper has introduced a low-power reversible Linear Feedback Shift Register (LFSR) architecture, which is made to provide cryptography-based applications. The recommended architecture uses the principle of reversible logic to apply the shift and feedback operations with maintaining the flow of information in each state transition. The proposed reversible LFSR architecture, in contrast to the more traditional LFSR architecture, is based on reversible logic and does not lose information, thus being able to operate efficiently using energy. Simulation was used to check the functional correctness of the proposed architecture by analyzing the behavior of the waveforms, change of state and the generation of output sequences. The findings confirm that the reversible LFSR is a valid pseudo-random sequence generator and it is consistent in its behavior even when the number of clock cycles is increased. A comparative study to the standard LFSR shows that besides producing correct output sequences both architectures, the reversible LFSR has great benefits when it comes to preserving information and use in low-power cryptographic systems. The process of proper pseudo-random sequence generation, reversibility of transitions between states, and minimized power consumption make the proposed reversible architecture of LFSR ideal in the implementation of key generation, stream ciphers and secure data transmission. The simplicity and scalability of the proposed design makes it possible to expand it to higher-order LFSR-implementations and incorporate it into the larger cryptographic hardware.

REFERENCES

[1] [1] S. Karunamurthi and V. K. Natarajan, "VLSI implementation of reversible logic gates cryptography with LFSR key," *Microprocessors and Microsystems*, vol. 69, pp. 1–9, 2019.

[2] [2] V. Raj, S. Janakiraman, and S. Rajagopalan, "Security analysis of reversible logic cryptography design with LFSR key on 32-bit microcontroller," *Microprocessors and Microsystems*, vol. 83, 2021.

[3] [3] K. Rajesh and G. U. Reddy, "FPGA implementation of optimized reversible linear feedback shift registers," in *Proc. IEEE Int. Conf. on Intelligent Computing*, 2018.

[4] [4] N. Neelima, K. N. Rao, and A. S. Kumar, "Efficient reversible logic design for quantum computing: A novel 4-bit LFSR approach," in *Proc. IEEE Region 10 Conf.*, 2024.

[5] [5] S. Abdel-Hafeez, "Programmable feedback shift register," *Circuits, Systems, and Signal Processing*, vol. 42, no. 8, pp. 4213–4236, 2023.

[6] [6] H. I. Kim and J. C. Jeon, "Quantum LFSR structure for random number generation using multilayered shift register," *Sensors*, vol. 22, no. 9, 2022.

[7] [7] B. N. K. Reddy and G. S. V. Reddy, "Design and implementation of an efficient LFSR using reversible logic gates," in *Proc. IEEE Bombay Section Signature Conf.*, 2020.

[8] [8] G. Chandran and H. Mary, "VLSI implementation of image encryption and decryption using reversible logic gates," in *Proc. IEEE Int. Conf. on Computing Technologies*, 2020.

[9] [9] B. M. Krishna, K. C. S. Kavya, and P. S. Kumar, "FPGA implementation of image cryptology using reversible logic gates," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 7, 2020.

[10] [10] B. Sarala and G. A. S. Kumar, "Efficient design of image cipher technique using reversible logic," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 6, 2021.

[11] [11] M. G. Roshan and M. Gholami, "4-bit serial shift register and LFSR design in QCA technology," *Computers & Electrical Engineering*, vol. 75, pp. 1–11, 2019.

[12] [12] M. Grymel, "New programmable LFSR counters with automatic encoding and state extension," *Electronics*, vol. 13, no. 2, 2024.

[13] [13] R. Murugasami, D. Sundararajan, and K. N. K. Velukutty, "Design of high-speed 4-bit LFSR using reversible logic gates for security applications," *International Journal of Information Technology*, 2025.

[14] [14] A. Devrari and A. Kumar, "Reconfigurable linear feedback shift register for wireless communication and coding," *International Journal of Reconfigurable and Embedded Systems*, vol. 12, no. 3, 2023.

[15] [15] G. L. Madhumati and P. Bindhu, "Implementation of cryptographic architecture for secure data transmission using reversible logic gates," in *Proc. IEEE Int. Conf. on Smart Computing*, 2025.