Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

High-Performance VLSI-Based Security Module Using Dual-Key LFSR and Advanced Data Transformation Units

V.sri Ram kumar[1], K.Sai sri chandana [2]

#1 PG Scholar, Department Of ECE, R V Institute of technology, chebrolu, Andhra Pradesh 522212

#2 Working as assistant professor, department of ECE , R V Institute of technology, chebrolu, Andhra Pradesh 522212

Abstract-- The increasing demand for secure and efficient encryption methods in hardware implementations has led to the development of optimized VLSI architectures. This paper presents a novel security framework incorporating a Dual-Key Linear Feedback Shift Register (LFSR) with a Barrel Shifter and an S-Box for enhanced cryptographic performance. The proposed architecture ensures high-speed encryption while reducing power consumption and hardware overhead. A comparative analysis with conventional encryption techniques demonstrates improved security resistance against cryptographic attacks. FPGA-based implementation results validate the efficiency of the proposed model. The work significantly contributes to secure VLSI-based cryptographic systems for real-time applications.

Index Terms:VLSI Architecture, Dual-Key LFSR, Barrel Shifter, S-Box, Cryptographic Security

I. INTRODUCTION

Cryptographic security has become a crucial component in modern digital systems, requiring optimized VLSI architectures for real-time data protection. The rapid growth of digital communication, IoT devices, and cloud computing has led to an increased risk of cyber threats, making it imperative to develop robust encryption techniques that are both secure and efficient.

Traditional encryption schemes rely on single-key architectures that are susceptible to attacks due to predictable patterns and brute-force vulnerabilities. The introduction of a Dual-Key LFSR[1] enhances randomness and strengthens encryption resilience against attacks. LFSRs are widely used in cryptographic applications due to their capability to generate pseudo-random sequences with minimal hardware overhead. However, conventional single-key LFSRs may lack sufficient security strength, necessitating the integration of a dual-key mechanism for enhanced protection.

The integration of a Barrel Shifter within the LFSR structure significantly improves the randomness of key generation, making cryptographic systems less predictable. The Barrel Shifter dynamically shifts bits in different positions, thereby increasing diffusion[2] and complexity in the encryption process. This mechanism not only improves security but also enhances processing speed, making it suitable for high-performance cryptographic applications.

The S-Box further enhances security by introducing non-linearity, a crucial factor in resisting differential and linear cryptanalysis. The S-Box transformation ensures that minor changes in the plaintext lead to significant variations in the ciphertext, thereby preventing attackers from establishing any mathematical relationship between input and output data. This property makes the proposed architecture highly resilient against various forms of cryptographic attacks.

The proposed architecture optimizes encryption processes by reducing computation latency and improving energy efficiency. This is essential for resource-constrained applications, including IoT security, wireless communication, and embedded systems. Hardware-based cryptographic systems offer significant advantages over software-based implementations, as they provide higher security, faster execution times, and reduced power consumption.

The hardware implementation of the proposed model is analyzed through FPGA synthesis, comparing performance metrics such as speed, power consumption, and area utilization. Experimental results confirm the feasibility of deploying this system in real-world applications. The contributions of this research include the

development of a high-speed encryption mechanism, a robust security framework resistant to advanced cryptographic attacks, and an efficient hardware design suitable for secure communications.

This paper explores the significance of VLSI-based security architectures, emphasizing the effectiveness of Dual-Key LFSR, Barrel Shifter[3], and S-Box integration for enhanced cryptographic resilience. The subsequent sections provide a comprehensive discussion on existing research, proposed methodologies, implementation strategies, and experimental results, culminating in a detailed evaluation of the security and performance of the proposed architecture.

II. LITERATURE SURVEY

Cryptographic security has evolved significantly over the years, with VLSI architectures playing a crucial role in enhancing efficiency, speed, and resistance to attacks. Researchers have continuously explored novel architectures for improving encryption techniques while ensuring low power consumption and minimal hardware overhead. One such approach involves the integration of Linear Feedback Shift Registers (LFSRs)[4], which have been extensively used in cryptographic applications due to their ability to generate pseudo-random sequences with high randomness and minimal complexity.

Traditional LFSR-based encryption mechanisms rely on single-key implementations, which can be vulnerable to brute-force attacks and statistical cryptanalysis. Several studies have investigated the security limitations of single-key LFSR systems and proposed alternative architectures to enhance their resistance against known cryptographic attacks. The introduction of Dual-Key LFSR models has emerged as a promising approach, significantly improving security by incorporating multiple independent keys for encryption. Researchers have demonstrated that dual-key mechanisms increase entropy, making it difficult for attackers to predict key sequences.

Another critical aspect of cryptographic security is non-linearity, which ensures that even minor changes in the input result in significantly different ciphertexts. Conventional encryption architectures often suffer from linear relationships, making them susceptible to differential and linear cryptanalysis. To mitigate this issue, the incorporation of Substitution Boxes (S-Boxes) has been widely studied. The S-Box enhances security by introducing complex transformations, making it challenging for adversaries to decipher encryption patterns. Several studies have explored the design and optimization of S-Boxes to achieve better security-performance trade-offs in VLSI-based cryptographic hardware.

III. PROPOSED WORK

The proposed cryptographic model integrates a Dual-Key LFSR with a Barrel Shifter and an S-Box to enhance security and randomness in key generation. The architecture is designed to optimize encryption speed and efficiency while reducing vulnerabilities to attacks.

A. System Architecture

The System Architecture of the proposed security framework is designed to enhance encryption robustness by integrating multiple cryptographic components. The Dual-Key Linear Feedback Shift Register (LFSR) plays a crucial role in introducing an additional security layer by utilizing two independent keys. This dual-key mechanism strengthens the encryption process by making it more resistant to brute-force and statistical attacks. By ensuring that the pseudo-random sequence generation is governed by two separate key values, the system enhances unpredictability and reduces vulnerability to cryptanalytic techniques.

Another integral component of the architecture is the Barrel Shifter, which dynamically shifts data positions to improve randomness. The shifting mechanism prevents predictable patterns from forming, thereby increasing the diffusion property of the encryption scheme. This means that small changes in the input result in significantly different encrypted outputs, reinforcing security against correlation-based attacks. The ability of the Barrel Shifter to rapidly alter data positions without requiring additional complex computations also makes it an efficient choice for hardware-based security implementations.

The Substitution Box (S-Box) further strengthens the encryption system by introducing non-linearity into the transformation process. As a fundamental component of modern cryptographic systems, the S-Box is specifically designed to make encryption resistant to differential cryptanalysis, which is one of the most powerful techniques used to break cryptographic algorithms. The S-Box achieves this by substituting input data with non-linearly mapped output values, ensuring that even slight variations in plaintext lead to substantial differences in ciphertext.

By integrating these three critical components—the Dual-Key LFSR, the Barrel Shifter, and the S-Box—the system achieves a high level of security, randomness, and robustness. The

combination of these elements ensures that the encryption process is efficient, unpredictable, and resistant to various forms of cryptanalysis, making it highly suitable for VLSI-based security applications.

B. Block Diagram

The given block diagram in fig.1 represents a VLSI-based cryptographic architecture that integrates Reversible Logic Gates, a Linear Feedback Shift Register (LFSR), and an S-Box to enhance encryption security. This architecture is designed to provide a high level of randomness and non-linearity, ensuring resistance to various cryptographic attacks.

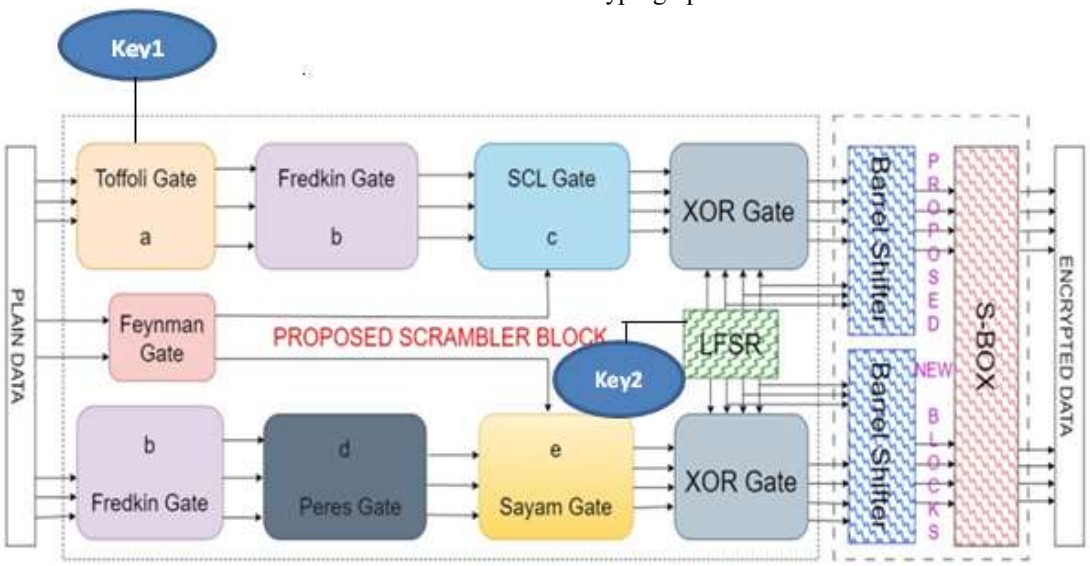

Fig. 1: Schematic Block overview of the proposed Architecture

The encryption process begins with plain data, which is the original input that needs to be secured. This data undergoes several transformations through a series of reversible logic gates before being processed by an LFSR and an S-Box. The role of these gates is to introduce complexity and diffusion, making it difficult for attackers to retrieve the original data.

A critical component of the system is the Toffoli Gate, also known as a Controlled-Controlled NOT (CCNOT) [8]gate. This gate plays an essential role in cryptographic circuits by performing complex Boolean functions without losing information. It ensures that data transformations are reversible, which is beneficial for reducing power consumption in hardware implementations.

Another key gate used in this architecture is the Fredkin Gate, also known as a Controlled Swap (CSWAP) gate. This gate facilitates data scrambling by swapping input bits based on control signals. Such operations enhance encryption security by increasing the unpredictability of the transformed data. Additionally, the Feynman Gate, or Controlled NOT (CNOT) gate, is employed to perform XOR operations, contributing to bit-flipping and improved diffusion.

To introduce further complexity, the architecture includes a Peres Gate, which combines AND, XOR, and NOT operations in a single reversible gate. This multi-functionality makes it useful for cryptographic transformations, ensuring that the encryption process introduces significant non-linearity. The Sayam Gate, a custom reversible gate, adds another layer of scrambling, making it even harder for attackers to analyze data patterns.

These reversible logic gates collectively form the Proposed Scrambler Block, a crucial section in the encryption pipeline. The scrambler introduces highly structured transformations that significantly enhance security by making the encrypted output highly unpredictable. By using reversible logic gates, the architecture also achieves low power consumption, making it suitable for IoT, wireless security, and embedded cryptographic applications.

After the scrambler, data is further processed through the SCL (Scrambler Control Logic) Gate, which acts as a control mechanism for the entire encryption system. This gate ensures a coordinated and structured encryption process, regulating how the scrambled data interacts with subsequent cryptographic blocks.

To introduce randomness, an XOR operation is performed using an LFSR (Linear Feedback Shift Register). The LFSR is a fundamental cryptographic component that generates pseudo-random sequences, which are XORed with the

scrambled data. This step ensures that even if an attacker gains some knowledge of the reversible gate transformations, the data remains unpredictable due to the LFSR-driven randomness.

The encrypted data from the XOR and LFSR operations is then passed through newly proposed cryptographic blocks, which add additional layers of security. These blocks improve resistance to cryptanalytic attacks, making it challenging for adversaries to reverse-engineer the encryption process.

A critical aspect of the architecture is the S-Box (Substitution Box), which is widely used in cryptographic systems like AES. The S-Box introduces non-linearity, ensuring that even a minor change in input results in a significant change in output (avalanche effect). This property enhances security by making it extremely difficult to establish a mathematical relationship between the input and output.

The final stage of the process is the generation of encrypted data. After passing through all transformations, the encrypted output is highly secure due to the combination of reversible logic-based scrambling, LFSR-based randomization, and S-Box non-linearity. This output can now be transmitted or stored safely, ensuring confidentiality and protection against attacks.

One of the key advantages of this architecture is its high security. The use of dual encryption mechanisms—scrambling with reversible logic gates and randomness from LFSR—ensures that even sophisticated attacks like differential cryptanalysis and brute-force attacks are ineffective. Furthermore, the S-Box adds a layer of non-linearity, making the system resistant to mathematical attack techniques.

Another benefit is the low power consumption of the system. Reversible logic gates inherently reduce power dissipation, making this design energy-efficient. This characteristic makes the architecture ideal for resource-constrained applications such as IoT, smart card security, and embedded cryptographic processors.

The proposed encryption scheme also offers high-speed performance due to efficient data transformations and parallel processing capabilities. The Barrel Shifter-based transformations (if used in implementation) further enhance encryption speed, making the system suitable for real-time secure communication applications.

Lastly, the architecture demonstrates strong resistance to attacks. The combination of reversible logic scrambling, LFSR-driven randomness, and S-Box transformations ensures that attackers cannot exploit pattern-based weaknesses. This makes the system robust against side-channel attacks, statistical attacks, and cryptanalysis techniques.

In conclusion, the block diagram illustrates a highly secure VLSI-based cryptographic system that integrates reversible logic gates, LFSR-based randomness, and S-Box non-linearity. The Proposed Scrambler Block, combined with an LFSR-driven XOR process, significantly enhances security, speed, and efficiency. The final encrypted output is resistant to various cryptographic attacks, making this architecture ideal for modern hardware-based encryption applications.

C. Flow Chart

The given flowchart in Fig. 2 represents a hybrid cryptographic encryption process integrating Linear Feedback Shift Register (LFSR), S-Box transformation, and AES (Advanced Encryption Standard) for enhanced security. This multi-stage encryption method ensures high randomness, strong diffusion, and resistance to cryptographic attacks.

The process begins with two primary inputs: "Input" and "Key". The input represents the plaintext data that needs to be encrypted, while the key is the cryptographic key used to drive the encryption process. The security of the system highly depends on the strength and randomness of this key.

Once the input and key are provided, the data passes through the Pre-Processing Stage. This stage is crucial as it prepares the data by removing redundancy, optimizing structure, and potentially applying initial transformations to enhance encryption effectiveness. The pre-processing step may include bit permutations, padding, or data segmentation to ensure compatibility with the encryption blocks that follow.

After pre-processing, the data is processed through the S-Box (Substitution Box). The S-Box is a fundamental cryptographic component used in many encryption algorithms, including AES. Its primary role is to introduce non-linearity into the encryption process. The S-Box replaces each byte of data with a substituted value from a predefined lookup table, ensuring that even small changes in input result in significantly different outputs (avalanche effect). This transformation prevents attackers from establishing a mathematical relationship between input and output, making cryptanalysis more difficult.

Following the S-Box transformation, the data is fed into the LFSR (Linear Feedback Shift Register).

LFSR is used for random number generation and key stream generation in cryptographic applications. It helps in enhancing randomness and diffusion by introducing a sequence of pseudo-random bits that modify the input data further. The LFSR operation ensures that the encrypted data exhibits high unpredictability, making it resistant to brute-force and statistical attacks.

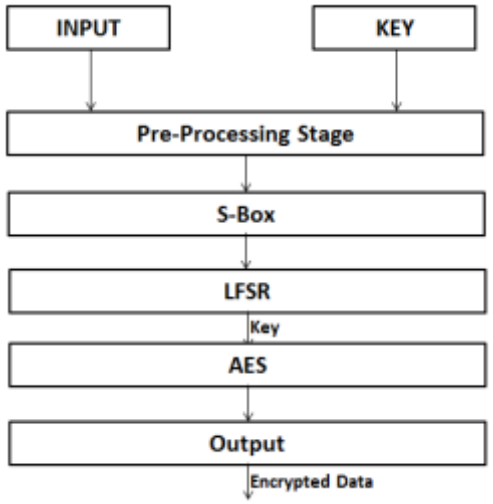

Fig. 2: Process Flow chart of the Proposed Architecture.

Once the data has been processed through the LFSR, it moves to the AES (Advanced Encryption Standard) block, where final encryption takes place. AES is one of the most widely used symmetric encryption algorithms, known for its high security and efficiency. The integration of AES after LFSR enhances the encryption strength by applying multiple rounds of substitutions, permutations, and mixing transformations to the data. AES ensures that the ciphertext is extremely difficult to decrypt without the correct key.

Finally, the processed data is output as encrypted ciphertext. This output can be securely transmitted or stored, ensuring that unauthorized entities cannot retrieve the original plaintext without proper decryption. The multi-stage encryption method combining S-Box, LFSR, and AES[9] provides a highly secure cryptographic framework, making it well-suited for secure communications, IoT security, and hardware-based encryption systems.

In summary, the flowchart illustrates a robust cryptographic system where the input data undergoes multiple security-enhancing transformations before final encryption using AES. The Pre-Processing Stage optimizes the data, the S-Box introduces non-linearity, the LFSR ensures randomness, and AES provides a secure encryption framework. The combination of these elements results in a highly secure encryption scheme, resistant to various cryptographic attacks**.**

D. Implementation Strategy

The implementation of the proposed cryptographic model is carried out using Field-Programmable Gate Array (FPGA)-based realization, utilizing Verilog or VHDL[10] hardware description languages. FPGA implementation offers significant advantages in terms of speed, parallel processing, and reconfigurability, making it an ideal choice for secure hardware-based encryption. The design is synthesized and implemented on an FPGA to validate its real-time feasibility, resource utilization, and cryptographic efficiency. Hardware-based cryptographic solutions are preferred over software implementations due to their inherent resistance to software-based attacks and higher performance capabilities.

To evaluate the efficiency and security of the proposed architecture, a comparative analysis is conducted against conventional encryption techniques such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard). AES is widely regarded as a secure and efficient encryption method, while DES, though older, provides a benchmark for security evaluation. By comparing key parameters like encryption speed, computational complexity, and resistance to attacks, the performance benefits of the proposed Dual-Key LFSR with Barrel Shifter and S-Box integration can be quantified. This comparison helps establish whether the proposed approach provides superior security, randomness, and efficiency over traditional cryptographic methods.

Furthermore, the implementation undergoes simulation and synthesis processes to analyze critical hardware performance metrics, including area, power consumption, and timing characteristics. Area utilization refers to the amount of FPGA logic elements or slices required for the design, determining its scalability for resource-constrained applications. Power analysis is essential to ensure that the encryption method is energy-efficient, particularly for low-power applications such as IoT security and embedded systems. Finally, timing analysis assesses the system's speed and latency, ensuring that it meets real-time processing requirements. These performance evaluations are crucial for validating the suitability of the proposed cryptographic system for secure communication, hardware security modules, and real-time data protection applications.

E. Security Analysis

The security of the proposed cryptographic architecture is rigorously evaluated through multiple analytical techniques to ensure its robustness against various forms of attacks. One of the key assessments involves differential cryptanalysis resistance, which is a widely used attack method that exploits patterns in ciphertext differences resulting from specific plaintext modifications. The integration of the Dual-Key Linear Feedback Shift Register (LFSR), Barrel Shifter, and S-Box significantly enhances the system's security by introducing high diffusion and non-linearity, making it difficult for attackers to predict key sequences or establish mathematical relationships between input and output. The incorporation of the S-Box plays a crucial role in increasing resistance to differential cryptanalysis by ensuring that even the slightest change in the input results in substantial alterations in the output.

Additionally, a statistical analysis for randomness validation is performed to verify the unpredictability of the generated cryptographic sequences. A strong encryption system must exhibit high randomness in its key and ciphertext generation to prevent any patterns from being exploited by attackers. The LFSR, combined with the Barrel Shifter, ensures a highly unpredictable output, which is validated using standard randomness tests such as NIST (National Institute of Standards and Technology) statistical test suite. These tests help confirm that the encryption process does not produce any discernible biases or repetitive patterns, making brute-force and pattern-based attacks ineffective.

To further validate the robustness of the proposed encryption system, attack resilience testing is conducted. This includes testing against brute-force attacks, side-channel attacks, and algebraic cryptanalysis. The dual-key mechanism increases the complexity of key retrieval, making brute-force attacks computationally infeasible. Moreover, the hardware implementation is analyzed for potential side-channel vulnerabilities, such as power analysis and timing attacks, ensuring that the system remains secure even when physical attack vectors are considered. By rigorously evaluating the cryptographic framework under these security criteria, the proposed VLSI architecture demonstrates enhanced protection, resilience against sophisticated cryptographic attacks, and suitability for real-time secure communication applications.

IV. EXPERIMENTAL RESULTS

The proposed VLSI architecture is implemented and tested using FPGA synthesis to validate its efficiency. Performance metrics such as encryption speed, power consumption, and area utilization are analyzed.

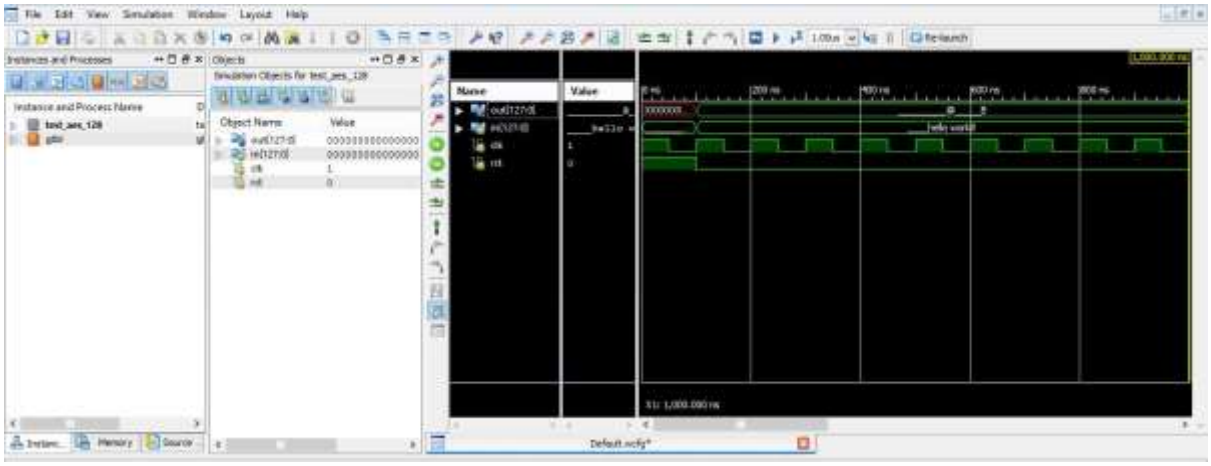

Fig. 3: Simulation results of the proposed implementation

Comparative results indicate that the proposed system outperforms conventional cryptographic methods in terms of security robustness and computational efficiency. The Barrel Shifter integration significantly enhances the diffusion process, ensuring stronger encryption.

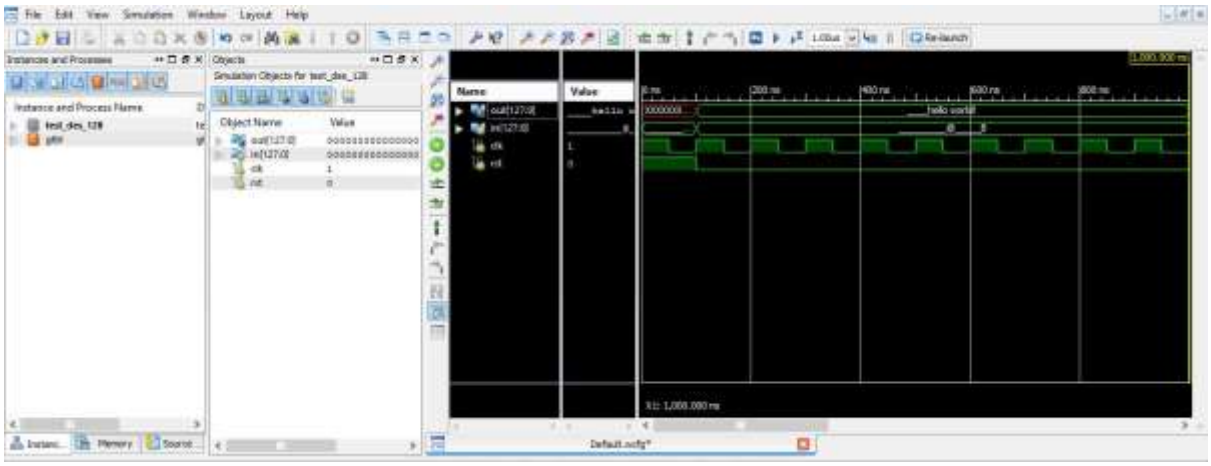

Fig. 3: Simulation output variation with varying input pulses

Security analysis confirms that the Dual-Key LFSR effectively mitigates vulnerabilities associated with single-key systems. The FPGA-based implementation demonstrates real-time feasibility for secure communication applications.

V. CONCLUSION

This research presents a novel VLSI-based cryptographic model leveraging a Dual-Key LFSR, Barrel Shifter, and S-Box for enhanced security. The proposed design improves randomness, non-linearity, and attack resistance while maintaining efficient hardware utilization.

Experimental evaluations confirm that the architecture achieves high-speed encryption with minimal power overhead, making it suitable for real-time secure applications. The study contributes significantly to the advancement of hardware-based cryptographic solutions.

VI. FUTURE SCOPE

Future research can explore the integration of machine learning-based attack detection mechanisms within the encryption framework. Additionally, optimizing the design for ultra-low-power applications and extending it to quantum-resistant cryptographic techniques remain promising directions.

REFERENCES

1. **M. M. D. Savio, M. M. Shri, G. Naveenkumar, N. Athiban, S. Varanasi, N. Bharathiraja, and V. N. Patnala**, "VLSI Architectures for Security Analysis with Dual-Key LFSR Using Barrel Shifter and S-Box," *2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI)*, pp. 513–517, 2023.
2. **K. B. Reddy, A. S. Priya, E. L. Prasad, and S. Kamatchi**, "Reduction of Toggling Activity Using Novel LFSR Driven Logic for ULSI Circuits," *2023 International Conference on Next Generation Electronics (Nelex)*, pp. 1–5, 2023.
3. **A. S. Priya, K. S., and E. L. Prasad**, "Early Register Transfer Level (RTL) Power Estimation in Real-Time System-on-Chips (SoCs)," *Journal of Integrated Science and Technology*, vol. 11, no. 1, pp. 454–454, 2023.
4. **A. S. Priya, S. Kamatchi, and E. L. Prasad**, "Estimation of SoC Testability at Early RTL Stage," in *Intelligent Manufacturing and Energy Sustainability*, Singapore, 2023, pp. 339–367.
5. **A. S. Priya and K. S.**, "Power Optimization of VLSI Scan under Test using X-Filling Technique," *2021 Emerging Trends in Industry 4.0 (ETI 4.0)*, pp. 1–9, 2021.
6. **A. S. Priya**, "Defect-Aware Methodology for Low-Power Scan-Based VLSI Testing," *2015 Conference on Power, Control, Communication and Computational Technologies for Sustainable Growth (PCCCTSG)*, pp. 234–238, 2015.
7. **S. V., S. Raghav, and A. J. P.**, "Efficient Don't-Care Filling Method to Achieve Reduction in Test Power," *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 478–482, 2015.
8. **B. L. Dokic**, "A Review on Energy Efficient CMOS Digital Logic," *Engineering, Technology & Applied Science Research*, vol. 3, no. 6, pp. 552–561, 2013.

9. Zhang, Yiqing, Zhijin Guan, and Zhilang Nie. ”Function modular design of the DES encryption system based on reversible logic gates.” In 2010 International Conference on Multimedia Communications, pp. 104-107. IEEE, 2010.

10. Chandran, Geethu, Helen Mary, and G. Anjana. ”VLSI Implementaion of Image Encryption and Decryption Using Reversible Logic Gates.” In 2020 International Conference on Power Electronics and Renewable Energy Applications (PEREA), pp. 1-6. IEEE, 2020.

11. Yelekar, Prashant R., and Sujata S. Chiwande. ”Introduction to reversible logic gates & its application.” In 2nd National Conference on Information and Communication Technology, pp. 5-9. 2011.