ISSN: 2395-1680 (ONLINE)
DOI: 10.21917/ijme.2026.0378

DYNAMIC LATCH BASED LOCK ARCHITECTURE FOR ENHANCED SCAN CHAIN SECURITY

M. Pavan[1] and K.N. Madhusudhan[2]
[1]*Department of VLSI Design and Embedded Systems, B.M.S. College of Engineering, India*
[2]*Department of Electronics and Communication Engineering, B.M.S. College of Engineering, India*

Abstract

To mitigate the risks posed by scan-based side-channel attacks in integrated circuits, this work proposes a robust and adaptable architecture Dynamic Latch-Based Lock Architecture which builds on the foundational concepts of the parallel latch-based secure scan design. The proposed system is engineered to overcome limitations of earlier designs by introducing modular and parameterized key management components. Specifically, the design supports scalable key lengths of 8, 16, 32, and 64 bits, allowing customization based on the desired level of security and available hardware resources. In contrast to the fixed configurations in the base design, this architecture achieves area efficiency by minimizing the number of latches per scan path and strategically distributing logic through parameterizable modules. This reduction in latch overhead contributes to a more compact and optimized layout. In addition, clock gating mechanisms are integrated to dynamically disable portions of the scan logic during idle periods, thereby significantly reducing dynamic power consumption and improving overall energy efficiency. A notable feature of the design is a scalable Linear Feedback Shift Register (LFSR), whose length adapts to the chosen key size. This LFSR enhances security by performing runtime obfuscation of the circuit-under-test (CUT) output whenever a key mismatch is detected. This mechanism introduces unpredictability in scan outputs, effectively thwarting brute-force, SAT-based, and scan reconstruction attacks. To validate the practicality of the design, it was synthesized and tested on multiple standard ISCAS benchmark circuits including s27, s298, s1423, and s9234. Evaluation results show substantial improvements in both area and power efficiency, while preserving functional correctness and scan access for valid users. These outcomes demonstrate the scalability, effectiveness, and adaptability of the proposed architecture for modern secure hardware implementations.

Keywords:

Secure Scan Design, Latch Based Architecture, Dynamic Obfuscation, Clock Gating, Design for Testability

1. INTRODUCTION

Securing scan chains in integrated circuits (ICs) has become increasingly critical as attackers exploit design-for-test (DFT) features to launch side-channel attacks, state reconstruction, and reverse engineering. Traditional scan architectures, while essential for testability, introduce serious vulnerabilities by exposing internal states to adversaries. Several works have attempted to bridge the gap between testability and security using architectural modifications and obfuscation techniques.

The secure scan design presented in [1] introduced a parallel latch-based lock mechanism that restricts scan chain access unless a valid key is provided. While this was an important step toward scan protection, the architecture was limited by static key sizing and lacked dynamic power handling. Later advancements such as mode-based logic obfuscation [2] and dynamic-key shifting methods [3] improved runtime configurability, but still incurred overhead or required extra control mechanisms.

PUF-based authentication [4] offered chip-specific key generation but struggled with environmental robustness and error correction needs.

Efforts like skew-based locking [5] and secure DFT for crypto chips [6] emphasized structural scan protection but did not scale well in terms of area and power overheads. Similarly, lightweight scan architectures [7] and improved DFT with attack resistance [8] focused on making scan chains secure without significantly sacrificing performance. Data flow obfuscation [9] introduced logic-level circuit masking but lacked integration with scalable key control. Low-overhead scan obfuscation [10] and pseudorandom scan scrambling methods [11] added important contributions, but these techniques often operated independently of dynamic obfuscation or configurable key frameworks.

Motivated by these limitations, this paper presents a Dynamic Latch-Based Lock Architecture that integrates parameterized key generation, modular locking, clock gating for power reduction, and scalable Linear Feedback Shift Register (LFSR) based obfuscation. The design supports variable key lengths (8, 16, 32, 64 bits), enabling adaptability based on security demands and area constraints. Moreover, the architecture dynamically obfuscates scan chain behavior upon key mismatch, preventing unauthorized scan access and reducing scan-based leakage. Synthesized on multiple ISCAS benchmark circuits, including s27, s298, s1423, and s9234, the design demonstrates enhanced scan security, improved resource efficiency, and practical scalability across varying circuit complexities.

2. RELATED WORK

To address the growing vulnerabilities of scan chains in integrated circuits, numerous techniques have been proposed in the literature. The foundational work in [1] introduced a secure scan architecture using a parallel latch-based locking mechanism, offering a baseline structure for controlling scan access. Although effective, its fixed architecture limited configurability and power efficiency.

In [2], a novel obfuscation strategy was introduced using sequentially triggered mode-based design to dynamically alter circuit behaviour, significantly improving resistance to functional de-obfuscation. However, the sequential trigger adds overhead and limits key flexibility. The work in [3] presented a dynamic-key based scan architecture that allowed secure testing during manufacturing and in-field deployment. While key-shifting improved robustness, the design lacked optimization for low-power conditions.

Another approach based on physically unclonable functions (PUFs) was explored in [4], where authentication was achieved

using chip-unique identifiers. Though robust against cloning, such systems are sensitive to environmental noise and often require error correction logic. In [5], skew-based scan locking was implemented, providing runtime scan protection. However, its static locking behaviour may be susceptible to modern learning-based attacks.

Comprehensive secure DFT solutions were presented in [6] and [8], which integrate security features within test structures for cryptographic chips. These designs addressed side-channel leakage and introduced locking strategies that impair attack accuracy. SAT-based and ScanSAT attack resistances were further discussed in [7], while [9] introduced data flow obfuscation—a logic-level modification technique that complicates reverse engineering efforts.

Recent advancements in scan obfuscation include low-overhead methods like those in [10], which focused on minimizing logic cost while maintaining security. Another unique method discussed in [11] involves scan scrambling using pseudorandom values generated internally, offering test security with minimal external dependencies.

Despite their individual merits, these existing strategies often struggle to balance scalability, configurability, and low power. The proposed work overcomes these limitations by combining latch-based modular design, parameterized key length, clock gating, and scalable obfuscation to enhance security while maintaining practical resource use.

3. PROPOSED ARCHITECTURE

The proposed secure scan architecture builds upon the latch-based locking mechanism introduced in the base design, but introduces several critical modifications to enhance scalability, area efficiency, and power optimization. The system design can be described in four primary components: key generation, key comparator, obfuscation logic, and clock gating, each contributing to the secure operation of the scan chain.

3.1 KEY GENERATION

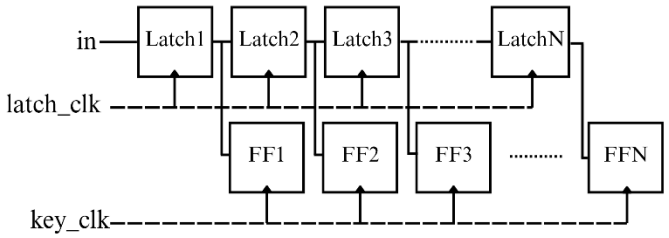

Fig.1. Latch-Based Key Generator

The key generation module has been redesigned from the original fixed-length parallel latch structure to a fully parameterized and area-optimized implementation. In the original architecture, a one-to-one mapping between latch stages and key bits resulted in redundant logic and increased silicon area, especially when handling longer keys. Our design mitigates this by reducing latch usage through internal signal reuse and optimized path staging. The module accepts a serial key input and propagates it through a configurable number of latches followed by flip-flops. This dual-stage structure ensures robust timing capture while maintaining low overhead. Parameterization supports a wide range of key lengths (e.g., 8, 16, 32, 64 bits), enabling trade-offs between hardware footprint and cryptographic strength based on application requirements. Clock input is dedicated to latches and is separately controlled from the functional scan clock, allowing isolated operation during key loading. The reduced latch count, in combination with the modular logic pipeline, contributes to considerable area savings compared to the base implementation.

3.2 KEY COMPARATOR

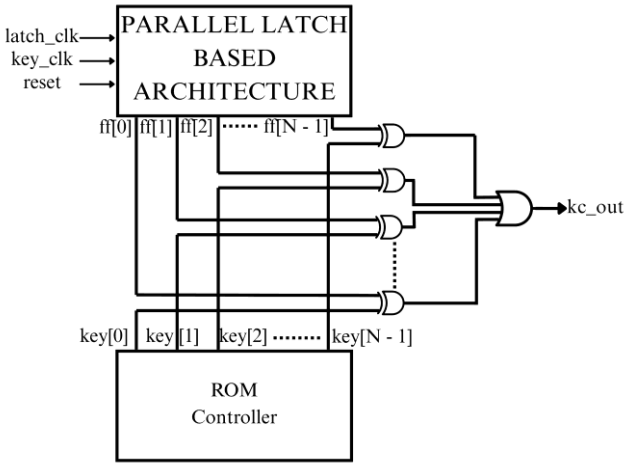

Fig.2. Key Comparator

Once the key is completely loaded into the parallel latch-flip-flop chain, the key comparator module is enabled via the key_ready signal. This comparator is implemented as a scalable logic block that performs a bitwise XOR operation between the captured key and a hardcoded golden key stored in a ROM. The width of the comparator logic matches the parameterized key size, ensuring minimal gate usage for shorter keys while still allowing scalability for enhanced protection. The XOR results are reduced using an OR tree to generate a single output bit—kc_out—which flags a mismatch when set. This approach enables a concise and efficient key validation process that is less susceptible to leakage or predictability. Because the comparator remains clock-gated until key_ready is high, it does not contribute to dynamic power consumption during the key entry phase.

3.3 OBFUSCATION LOGIC

To prevent meaningful scan data from leaking under invalid access, the system incorporates an obfuscation logic module powered by a scalable LFSR. This LFSR injects pseudo-random values into the scan output path only when the key comparator indicates a mismatch. Unlike the base paper's fixed 8-bit LFSR, the proposed design allows variable-length LFSR configuration (e.g., 2-bit, 4-bit, 8-bit, or more), defined through module parameterization.

The LFSR is seeded based on system state and toggled based on both comparator output and a cut signal derived from the circuit under test (CUT). This conditional activation ensures that obfuscation logic is engaged only when necessary, saving switching energy and reducing logic toggling when correct scan

access is granted. The randomness introduced by the LFSR makes unauthorized scan reconstruction infeasible even with repeated access attempts.

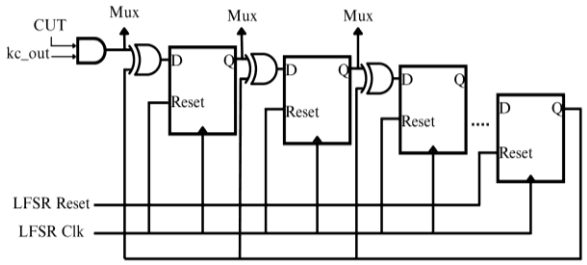

Fig.3. LFSR Obfuscation Logic

3.1. CLOCK GATING

Clock gating plays a critical role in reducing dynamic power usage in the proposed system. Initially, when the system is powered on or reset, all downstream sequential elements, including the key comparator and obfuscation logic, remain clock-gated. The gating logic is lifted only when the key_ready signal is asserted by the user, indicating that key entry is complete and scan chain authentication can proceed. This selective enablement ensures that flip-flops and LFSR logic do not experience unnecessary toggling, particularly in idle or incorrect access scenarios. Additionally, separate clock domains for the latch key loader and scan path logic allow more granular control over timing and power domains, helping to isolate power consumption to relevant blocks only. The integration of this gating scheme contributes significantly to the low-power footprint observed in the implementation results.

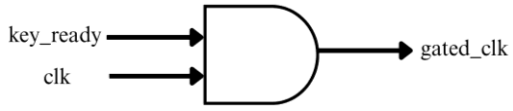

Fig.4. Clock Gating Circuit

3.4 SYSTEM INTEGRATION

The secure scan wrapper was validated using several standard ISCAS benchmark circuits, namely s27, s298, s1423, and s9234. In each case, the secure logic was integrated externally to the functional logic of the circuit under test, preserving original behaviour while enhancing security.

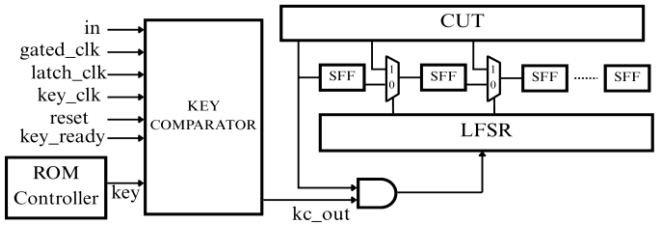

Fig.5. Complete System Integrated Circuit

The parameterized structure allows the wrapper to be reused and scaled for various system-on-chip environments, offering a practical and flexible solution for secure scan chain implementation.

3.5 WORKFLOW OF THE ARCHITECTURE

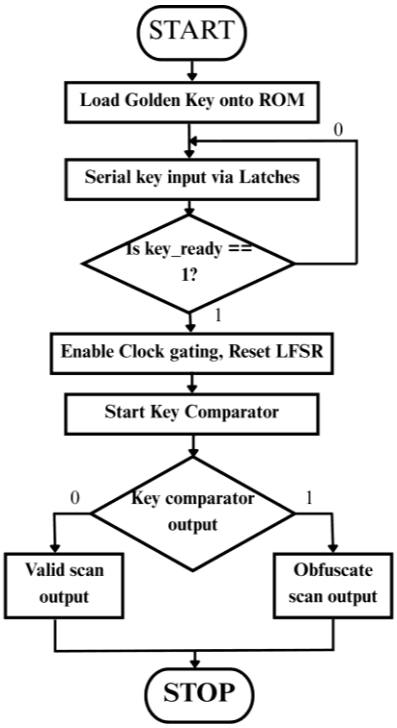

Fig.6. Workflow diagram

The flow diagram illustrates the functional workflow of the proposed secure scan locking mechanism. The process begins with system initialization, followed by key entry through a parallel latch-based key generation module. The latch chain, along with a set of flip-flops, captures the serial input stream until the entire key is loaded.

Once the input key is captured, the comparator is enabled. At this stage, the system checks whether the key comparison has been completed. If not, the flow loops back, holding further operations until the comparison is finalized. Upon successful comparison readiness, the key_ready signal is asserted, which in turn triggers clock gating. This selectively enables only the required sequential blocks, thereby reducing dynamic power dissipation during idle states. After clock gating is lifted, the output of the key comparator determines the scan behavior. If the comparator output indicates a match (logic '0'), the scan output is passed in its valid form to support standard test operations. If the comparator output indicates a mismatch (logic '1'), the scan output is obfuscated using the dynamic LFSR logic, thus preventing any meaningful data leakage from the scan chain. This conditional bifurcation of scan behavior based on key correctness forms the core security principle of the proposed architecture. The secure transition between states, controlled enablement of functional blocks, and dynamic obfuscation collectively enhance both power efficiency and resistance against scan-based side-channel attacks.

4. SECURITY ANALYSIS

The security of the proposed architecture is evaluated against a wide range of scan-based side-channel attack vectors and adversarial models discussed in the base paper. The system design

ensures that both functional correctness and confidentiality of internal values are maintained during scan operations. Key protection mechanisms include parameterized key-based access control, dynamic output obfuscation, and gated activation of critical modules.

The use of a configurable latch-based key input path, followed by a ROM-based key comparator, prevents unauthorized access through brute-force or guessing attacks. As the key width is parameterized, the entropy of the input space can be scaled based on security requirements, making brute-force attacks computationally infeasible for longer key lengths.

The proposed architecture effectively mitigates reset-and-flush-based attacks by activating scan logic only upon explicit user control (key_ready signal). This ensures that an adversary cannot induce scan output by simply toggling reset lines. Furthermore, clock gating limits internal switching activity, reducing the side-channel leakage surface.

Dynamic obfuscation is achieved through a scalable LFSR module triggered on key mismatch. This mechanism renders scan outputs unpredictable when the key does not match the golden reference, thwarting SAT-based and Scan SAT-based reverse engineering techniques. In contrast to static locking mechanisms, the dynamic behaviour introduced by the LFSR, in conjunction with the cut-based trigger, significantly increases resistance to automated solver-based attacks.

Machine learning-based SAIL attacks are also resisted due to the unpredictability and timing variance introduced by the gated LFSR, the reset-dependent latch chain, and the conditional scan output behaviour. As the output is not consistent under incorrect key conditions, learning-based models cannot generalize reliable patterns for reconstruction.

By combining these techniques in a modular and scalable structure, the proposed architecture achieves strong protection against a broad class of known scan chain attacks while remaining flexible enough to adapt to evolving adversarial strategies.

5. PERFORMANCE EVALUATION

The performance of the proposed secure scan architecture was evaluated in terms of area and power overhead using multiple ISCAS benchmark circuits—s27, s298, s1423, and s9234. The architecture was implemented in System Verilog and synthesized using Cadence Design Compiler. Parameterization allowed the key length to be scaled, with comparative results generated for 8, 16, 32, 64-bit configurations.

5.1 AREA ANALYSIS

The below table compares the area utilization of the proposed design with the base paper's design across different key lengths.

Table.1. Area Analysis

Key Size	Area (Unoptimized) (µm²)	Area (optimized) (µm²)	Reduction (%)
4 - bit	98.15	50.62	48.42
8 - bit	300.960	102.60	66.67

5.2 POWER CONSUMPTION ANALYSIS

Table.2. Power Consumption Analysis

Key Size	Power (nW) (unoptimized)	Power (nW) (optimized)	Reduction (%)
4 - bit	2558.473	2418.656	5.47
8 - bit	5410.281	4839.052	10.56

Power analysis for the same circuits was performed to evaluate the efficiency of the proposed clock-gated and obfuscation-aware design. The power consumed by the secure logic is shown below:

5.3 SCALED KEY CONFIGURATION ANALYSIS

To evaluate the scalability of the proposed secure scan architecture with respect to varying key sizes, area and power reports were generated for 16-bit, 32-bit, and 64-bit configurations. These configurations were synthesized using the same parameterized architecture, with System Verilog modules adapted to reflect different key lengths.

The results, presented in Table.4, confirm that while area and power increase with key size as expected due to wider latch and comparator paths, the proposed design maintains efficient growth. This is primarily attributed to reuse-optimized latch structures, modular comparator logic, and clock gating which reduces unnecessary power in inactive stages.

The architecture demonstrates that it scales well with security strength requirements, maintaining competitive area and power profiles across configurations.

Table.3. Area and Power Metrics for Scaled Key Configurations (16-bit, 32-bit, 64-bit)

Key Size	Area (µm²)	Power (nW)
16 - bit	212.040	4839.052
32 - bit	430.920	9679.845
64 - bit	868.680	19361.430

5.4 COMPARISON WITH PLSD – 8 [1]

A detailed side-by-side comparison of both architectures considering design methodology, hardware overhead, power usage, scalability, and resistance to common attack models is presented in the subsequent sections and tables to demonstrate the practical improvements achieved by the proposed solution.

Table.4. Comparison with base paper (PLSD-8 [1])

Feature	PLSD-8 [1]	Proposed Architecture
Key Length Support	Fixed (8-bit only)	Reconfigurable (4/8/16/32/64 bits)
Key Storage Mechanism	Hardcoded	Modular synthesizable ROM
Clock Gating	Absent or hardwired logic	Dynamic gating via comparator output
Output Obfuscation	Basic (logic XOR)	Dynamic LFSR-based

FSM Dependency	Present	Removed
Test Compatibility	Limited reuse	Fully test-compatible

5.5 AREA AND POWER REPORTS OF BENCHMARK CIRCUITS

To demonstrate the successful implementation of the proposed architecture, standard area and power reports were generated for the ISCAS benchmark circuits s27, s298, s1423, and s9234. The synthesis was performed using Cadence Design Compiler under a 28nm technology node. These reports validate that the architecture integrates cleanly with real-world designs and meets physical implementation expectations. The following table shows the synthesized area values and power for each circuit with the secure scan logic implemented:

Table.5. Area and Power Reports of Benchmark circuits

Key Size	Area (µm²)	Power (nW)
S27	43.430	425.420
S298	391.930	3117.437
S1423	1053.020	27170.259
S9234	1744.200	38724.600

3.2. SIMULATION RESULTS

To validate the proposed architecture across various real-world circuits, simulation and synthesis were conducted for four ISCAS benchmark circuits: s27, s298, s1423, and s9234. Each design was implemented in System Verilog and verified using Cadence Xcelium for functional correctness, and Cadence Design Compiler was used for synthesis.

Under, functional simulation, each circuit was simulated under two scenarios:

- With a correct key: scan outputs passed as expected.
- With an incorrect key: scan outputs scrambled due to LFSR activation.

Simulation observations:

- The key_ready signal enabled the clock and comparator.
- Incorrect key activated the LFSR, validating dynamic obfuscation.
- All circuits showed correct scan enable gating logic

Simulation waveforms confirmed the correct behavior of key matching, the comparator, and gated clock activation.

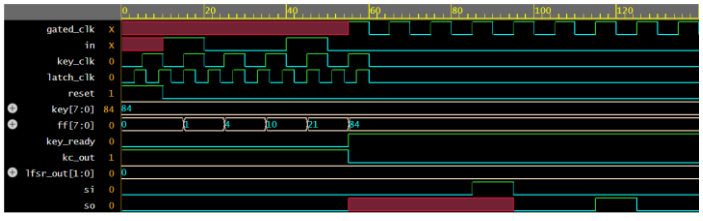

Fig.7. Valid Key, kc_out = 0, Valid scan output

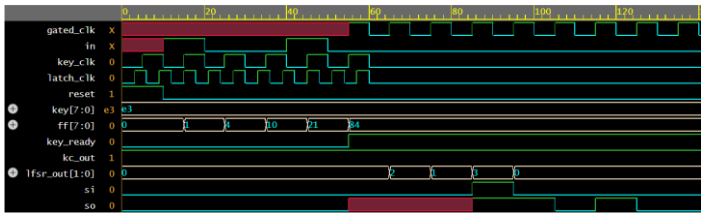

Fig.8. Invalid key, kc_out = 1, Obfuscated scan output

3.3. SYNTHESIS RESULTS

Synthesis was carried out on the Cadence Genus Compiler. The structure scales linearly for 16-, 32-, and 64-bit configurations while preserving the same control and gating hierarchy. Detailed schematics are omitted due to structural similarity.

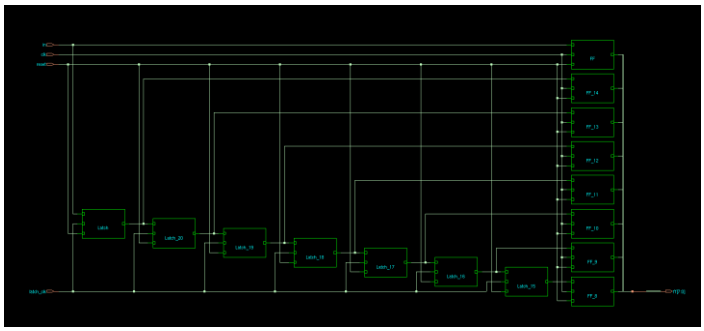

Fig.9. Key Generation Circuit

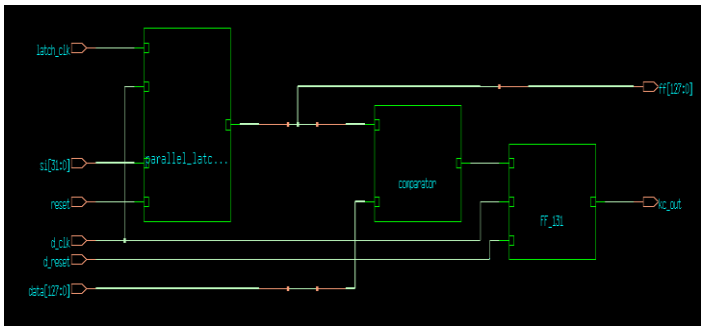

Fig.10. Key Comparator Circuit

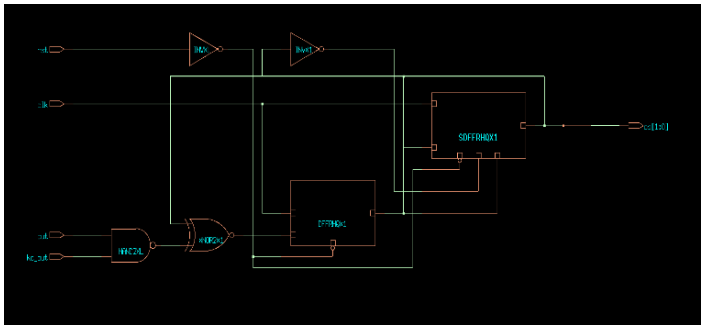

Fig.11. LFSR Circuit

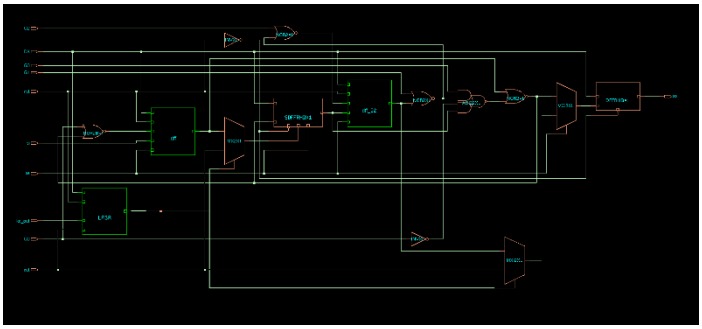

Fig.12. Dynamic Obfuscation of S27 circuit

6. CONCLUSION AND FUTURE WORK

This paper presents a dynamic latch-based secure scan architecture that improves upon existing locking mechanisms through parameterized design, reduced hardware overhead, and adaptive power management. By separating and modularizing the key generation and comparator units, the architecture supports flexible key lengths and scalable security levels, while integrating clock gating ensures reduced dynamic power usage. The implementation of a configurable LFSR further enhances scan data protection by introducing dynamic obfuscation in response to invalid key attempts. Experimental results across benchmark circuits, including s27, s298, s1423, and s9234, validate the effectiveness of the proposed system. Area reductions and measurable power savings demonstrate that the design meets both security and resource efficiency goals. Future work can explore the integration of Physically Unclonable Functions (PUFs) for chip-unique key generation, the adoption of reconfigurable scan paths to thwart structural analysis, and formal verification of obfuscation logic against side-channel leakage models. Additionally, the architecture can be extended to support dynamic key update protocols and integration with secure boot sequences for broader SoC protection.

REFERENCES

[1] Weizheng Wanga, Jian Lianga, Xiangqi Wangb, Xianmin Panc and Shuo Caia, "A Secure Scan Architecture using Parallel Latch-based Lock", *Integration*, Vol. 93, pp. 1-11, 2023.

[2] Sandhya Koteshwara, H. Chris Kim and K. Keshab Parhi, "Key-based Dynamic Functional Obfuscation of Integrated Circuits using Sequentially-Triggered Mode-based Design", *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 1, pp. 79-93, 2017.

[3] Kuen-Jong Lee, Ching-An Liu and Chia-Chi Wu, "A Dynamic-Key based Secure Scan Architecture for Manufacturing and In-Field IC Testing", *IEEE Transactions on Emerging Topics in Computing*, Vol. 10, No. 1, pp. 373-385, 2020.

[4] Qidong Wang, Aijiao Cui, Gang Qu and L. Huawei, "A New Secure Scan Design with PUF-based Key for Authentication", *Proceedings of IEEE Symposium on VLSI Test*, Vol. 3, No. 7, pp. 1-7, 2020.

[5] Hyungil Woo, Seokjun Jang and Sungho Kang, "A Secure Scan Architecture Protecting Scan Test and Scan Dump using Skew-based Lock and Key", *IEEE Access*, Vol. 9, pp. 102161-102176, 2021.

[6] Weizheng Wang, Jincheng Wang, Wei Wang, Peng Liu and Shuo Cai, "A Secure DFT Architecture Protecting Crypto Chips Against Scan-based Attacks", *IEEE Access*, Vol. 7, pp. 22206-22213, 2018.

[7] Xiangqi Wang, Xingxing Gong, Xianmin Pan and Weizheng Wang, "A Lightweight Scan Architecture against the Scan-based Side-Channel Attack", *Journal of Semiconductor Technology and Science*, Vol. 34, pp. 243-250, 2023.

[8] Weizheng Wang, Xiangqi Wang and Jin Wang, "Ensuring Cryptography Chips Security by Preventing Scan-based Side-Channel Attacks with Improved DFT Architecture", *IEEE Transactions on Systems, Man and Cybernetics: Systems*, Vol. 52, No. 3, pp. 2009-2023, 2020.

[9] Kimia Zamiri Azar, Hadi Mardani Kamali, Shervin Roshanisefat and Houman Homayoun, "Data Flow Obfuscation: A New Paradigm for Obfuscating Circuits", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 29, No. 4, pp. 643-656, 2021.

[10] Weizheng Wang, Xiangqi Wang, Xingxing Gong, Shuo Cai and Jiamin Liu, "A Low-Overhead and High-Security Scan Design based on Scan Obfuscation", *IEEE Access*, Vol. 12, pp. 182561-182570, 2024.

[11] Weizheng Wang, Yan Peng, Zuoting Ning, Peng Liu and Shuo Cai, "A Secure Scan Design based on Scan Scrambling by Pseudorandom Values and Circuit itself", *Journal of Semiconductor Technology and Science*, Vol. 21, No. 6, pp. 427-437, 2021.