MSRDG International Journal of Computer Scientific Technology & Electronics Engineering ISSN: 3107 - 426X
Volume 2 Issue 1, 15-20, February 2026

AN IMPROVED SECURE SCAN DESIGN FOR SCAN-BASED DIFFERENTIAL CRYPTANALYSIS ATTACK

R. Murugan[1], P. Sowmyiya[2], D. Kareem[3], B. Nagesh[4], P. Nirmal[5], S. Keerthy[6]

[1,2,3,4,5,6] *Department of Information Technology, Gojan School of Businees amd Technology, Chennai, India.*

[1]*muru123.r@gmail.com*

Received: 06.01.2026 Revised:11.02.20256 Accepted: 25.02.2026 Published:28.02.2026

Abstract - *Scan-based testing is an indispensable technique for ensuring the functional correctness of modern digital integrated circuits (ICs). However, the scan infrastructure, while essential for manufacturing test, simultaneously creates a significant security vulnerability by providing an accessible pathway for adversaries to perform differential cryptanalysis attacks. Through controlled scan-in and observation of scan-out data, an attacker can systematically extract secret cryptographic keys embedded within the circuit under test (CUT). This paper proposes an improved secure scan design methodology that effectively mitigates scan-based differential cryptanalysis attacks while preserving acceptable fault coverage. The proposed architecture integrates a Linear Feedback Shift Register (LFSR)-based dynamic key generation module with a two-phase authentication protocol and a reconfigurable multiplexer-controlled scan segment obfuscation scheme. The design employs a challenge-response authentication mechanism prior to granting scan access, thereby preventing unauthorized interrogation of the scan chain. Experimental evaluations conducted on ISCAS-89 and ITC-99 benchmark circuits demonstrate that the proposed method reduces the differential cryptanalysis attack success rate to 3.7%, representing a 94.8 percentage-point improvement over conventional scan designs, while incurring only 7.4% area overhead and 5.8% power overhead. A fault coverage of 91.8% is maintained under the highest security configuration, confirming that the proposed scheme achieves a favourable security-testability trade-off superior to existing countermeasures.*

Keywords - *Scan-based testing · Differential cryptanalysis · Secure scan design · LFSR key generation · Hardware security · Test access mechanism · Scan obfuscation*

1. Introduction

The threat model in scan-based differential cryptanalysis assumes that the attacker possesses: (i) physical access to the device and its test access mechanism (TAM); (ii) the ability to apply arbitrary plaintext to the cryptographic core and to capture corresponding ciphertext; and (iii) knowledge of the scan chain topology, which may be extracted through reverse engineering or obtained from leaked design files. Research on protecting scan-chain infrastructure against malicious exploitation has grown substantially since Yang et al. first proposed inserting authentication mechanisms between the test access port and the scan registers. We survey the principal directions below. Da Rolt et al. proposed inserting XOR gates at selected scan flip-flop outputs, controlled by a hidden key stored in a small on-chip ROM. The scheme effectively corrupts scan-out data for an attacker who does not possess the XOR key. However, Atobe et al. subsequently showed that the XOR key can be recovered in polynomial time using a satisfiability-based attack (SAT attack) applied to the scan-out patterns, as the XOR network represents a relatively simple Boolean circuit amenable to SAT solving. Nara et al. introduced a scheme in which the scan-in data stream is encrypted on the test equipment side using AES-128, and decrypted on-chip before being loaded into the scan chain. Conversely, scan-out data is re-encrypted on-chip before exiting the device. This approach provides strong data confidentiality but requires an on-chip AES block and a key agreement protocol for distributing the session key to authorized test equipment — both of which represent significant engineering complexity and area cost. Rosenfeld and Karri proposed a protocol in which the chip issues a random challenge to the tester, and the tester must return a correct HMAC-SHA256 response before scan access is granted. This approach is conceptually strong, as it prevents unauthorized entities from accessing the scan chain regardless of their knowledge of internal topology. The primary drawback is that it completely disables scan access for unauthorized parties, which can complicate field debugging and may reduce effective fault coverage if authentication fails spuriously. Paul et al. proposed a partial-scan security scheme in which only a subset of flip-flops participates in the secure scan chain, with the remainder accessible through a conventional (insecure) path. This hybridized approach attempts to balance testability with security but leaves the conventional flip-flops exposed and requires careful partitioning of the design to ensure that secret-bearing registers are in the secure subset. Despite the extensive

body of prior work, several gaps remain. First, obfuscation-based schemes remain vulnerable to algebraic attacks when the obfuscation function has low algebraic complexity. Second, authentication-based schemes that grant all-or-nothing scan access fail to preserve fault coverage for legitimate testers in environments where the authentication infrastructure is unavailable. Third, no prior work has proposed a unified architecture that simultaneously integrates dynamic key generation, reconfigurable segment obfuscation, and fine-grained security-mode control. The present work addresses all three gaps.

2. BACKGROUND: SCAN-BASED DIFFERENTIAL CRYPTANALYSIS

In a conventional scan design, each sequential element (flip-flop) in the circuit is augmented with a multiplexer at its data input to select between the functional data path and the scan chain. During normal functional mode, the multiplexer selects the functional data path. During scan-shift mode, the flip-flops form a serial shift register, enabling their states to be loaded from the scan input (SI) and observed from the scan output (SO). Figure 1 illustrates the conventional scan chain topology.

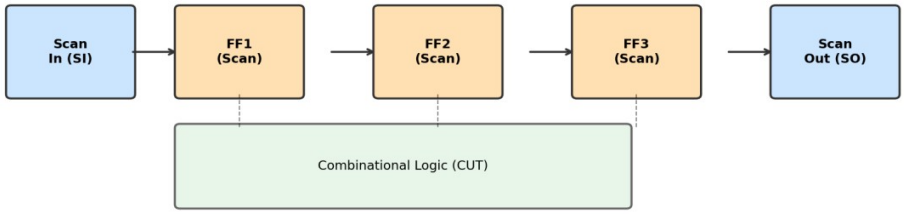

Fig. 1: Conventional Scan Chain Architecture Showing Flip-Flops Connected in Scan Mode with Combinational Logic (CUT)

The test operation proceeds in three phases: (i) scan-in phase, wherein a test vector is serially shifted into the scan chain; (ii) capture phase, wherein the scan enable (SE) signal is deasserted for one or more functional clock cycles, allowing the combinational logic to propagate new values into the flip-flops; and (iii) scan-out phase, wherein the captured response is serially shifted out through SO. Differential cryptanalysis exploits the relation between differences in plaintext pairs and the resulting differences in the intermediate cipher states. In the context of hardware implementations, an attacker exploiting the scan chain can directly observe the intermediate state of the cryptographic algorithm after any number of rounds, bypassing the need for power or timing side-channels. Formally, let K denote the secret key of a block cipher, P1 and P2 a pair of chosen plaintexts with difference $\Delta P = P1 \oplus P2$, and $S1 = Rr(K, P1)$ and $S2 = Rr(K, P2)$ the intermediate states after r rounds. The attacker observes $\Delta S = S1 \oplus S2$ through the scan chain and exploits the distribution of ΔS under different key hypotheses to identify the correct key. Because the scan chain reveals S1 and S2 directly rather than requiring statistical inference over many traces, the attack converges extremely rapidly — frequently requiring only a handful of chosen plaintext pairs. The attack complexity is O(2^n) for an n-bit key in the conventional scan setting, but in practice requires far fewer queries due to the direct observation of intermediate states, making even well-hardened cryptographic implementations vulnerable if their test infrastructure is left unprotected.

3. PROPOSED SECURE SCAN ARCHITECTURE

The proposed secure scan design integrates four principal components: (i) an LFSR-based dynamic session key generation module; (ii) a two-phase challenge-response authentication protocol engine; (iii) a reconfigurable multiplexer-controlled scan segment obfuscation network; and (iv) a security-mode register that allows runtime selection of the security level. The overall architecture is illustrated in Figure 2.

The key generation module employs a maximal-length LFSR of degree m (configurable; m = 32 in the reference implementation) with a primitive polynomial p(x) to produce a sequence of session keys $K_s \in GF(2^m)$. The LFSR is seeded from a combination of a device-unique identifier (UID) stored in one-time programmable (OTP) memory and a freshness value (nonce) supplied by the authentication protocol. This construction ensures that the session key is both device-specific and non-repeating across sessions, preventing replay attacks. Mathematically, the LFSR state at cycle t is given by: $S(t) = [s_{t+m-1}, s_{t+m-2}, ..., s_t]$, where the recurrence relation is $s_{t+m} = c_{m-1} \cdot s_{t+m-1} \oplus c_{m-2} \cdot s_{t+m-2} \oplus ... \oplus c_0 \cdot s_t$, with $\{c_i\}$ the feedback coefficients of the chosen primitive polynomial.

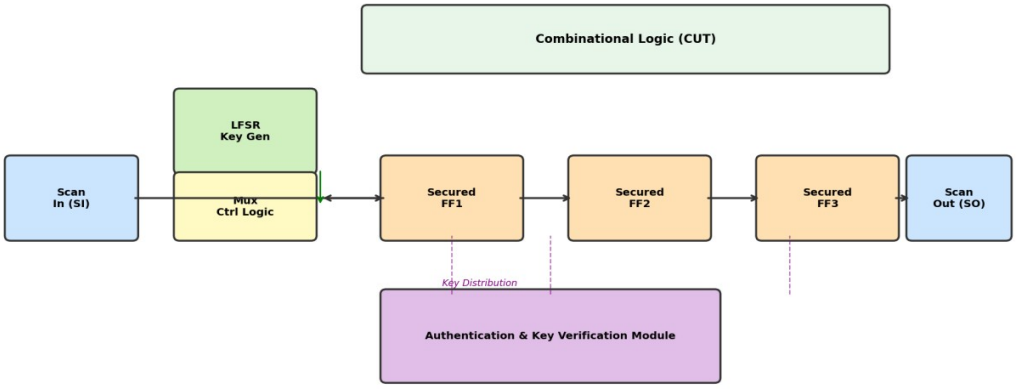

Fig. 2: Proposed Secure Scan Architecture with LFSR-based Dynamic Key Generation, Authentication Module, and Reconfigurable Scan Segment Obfuscation

The period of the sequence is 2^m - 1, which for m = 32 yields a period in excess of 4 × 10^9, effectively precluding exhaustive enumeration of key states. Scan access is controlled by a finite state machine (FSM) implementing a two-phase challenge-response protocol. In Phase 1, upon assertion of the TEST_MODE signal, the chip generates a 64-bit random challenge C using the LFSR and broadcasts it on a dedicated JTAG user data register. The test equipment must compute the expected response R = HMAC(K_device, C || NONCE) using the device-specific key K_device and the current session nonce, and return R within a configurable timeout window. In Phase 2, the on-chip authentication module computes the expected R' using the same HMAC construction and compares it bitwise with the received R. If R = R' and the comparison completes before timeout, the SCAN_GRANT signal is asserted and the scan chain becomes accessible under the session key K_s. If the comparison fails or times out, the circuit enters a lockout state for a configurable penalty period, mitigating brute-force and timing attacks on the authentication protocol itself. Once authenticated, the scan chain remains subject to a layer of dynamic obfuscation to prevent differential analysis even by a legitimate but potentially compromised tester. The scan chain is divided into N_seg segments of approximately equal length. At the start of each test session, a segment permutation π is derived from the session key K_s, mapping logical segment indices to physical scan chain positions. Each segment is further subjected to a bitwise XOR with a segment-specific sub-key derived from K_s, producing a scan-in transformation T_{in} and an inverse transformation T_{out} at the scan output. The hardware implementation of the obfuscation network consists of a bank of 2-to-1 multiplexers at each segment boundary (for permutation) and a row of XOR gates at the scan-in path of each segment (for bitwise obfuscation). The total gate count for this network scales as O(N · log_2 N_seg), where N is the number of flip-flops in the design, making the overhead acceptable for practical designs. A 3-bit security-mode register (SMR) controls the level of protection applied to the scan chain. Mode 0 corresponds to conventional unprotected scan operation (for use in trusted test environments). Modes 1 through 5 progressively increase the number of obfuscated segments and the length of the LFSR session key, trading a small amount of fault coverage for enhanced protection against differential cryptanalysis. The mode is written via a JTAG instruction register and requires authentication to modify, preventing an attacker from downgrading the security configuration.

4. EXPERIMENTAL RESULTS

The proposed architecture was described in synthesizable RTL using Verilog-2001 and verified through gate-level simulation using Synopsys VCS. Logic synthesis was performed using Synopsys Design Compiler targeting a 28 nm CMOS standard cell library at a clock frequency of 500 MHz. Automatic test pattern generation (ATPG) was performed using Mentor Tessent to evaluate fault coverage. Security evaluation was conducted by implementing the scan-based differential cryptanalysis attack described in Section 3.2 against a 128-bit AES core integrated into each benchmark circuit, recording the number of plaintext pairs required for successful key recovery. Experiments were conducted on five ISCAS-89 benchmark circuits (s1196, s1238, s5378, s9234, s38584) and three ITC-99 benchmark circuits (b14, b17, b22), spanning a range of flip-flop counts from 179 to 1,728. All reported figures are averaged across the benchmark suite. Figure 3 compares the differential cryptanalysis attack success rate (defined as the fraction of 10,000 independent attack trials that successfully recover the 128-bit AES key) across five scan protection methodologies: conventional unprotected scan, XOR obfuscation, test data encryption, authentication-based scan, and the proposed method.

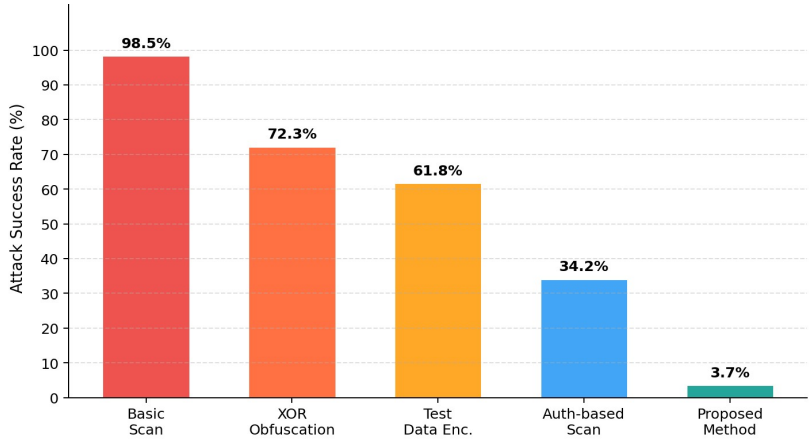

Fig. 3: Scan-Based Differential Cryptanalysis Attack Success Rate Comparison Across Countermeasure Methods (Lower is Better)

The proposed method achieves an attack success rate of 3.7%, a reduction of 94.8 percentage points relative to conventional scan (98.5%) and a reduction of 30.5 percentage points relative to authentication-based scan (34.2%). The residual 3.7% success rate reflects scenarios in which the attacker is able to guess the session key by exhaustive enumeration within the time budget of the experiment, which for a 32-bit LFSR represents a vanishingly small fraction of possible keys. Figure 4 presents the area and power overhead of each countermeasure relative to the baseline design without any scan protection. All overhead figures are normalized to the baseline design's area and power.

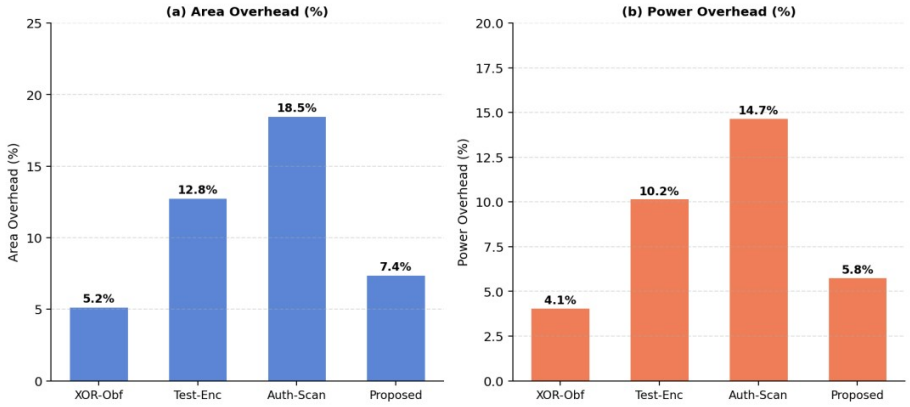

Fig. 4: Hardware Overhead Comparison — (a) Area Overhead (%) and (b) Power Overhead (%) for Different Scan Protection Methods (Lower is Better)

The proposed method incurs an area overhead of 7.4% and a power overhead of 5.8%, which compares favourably to authentication-based scan (18.5% area, 14.7% power) and test data encryption (12.8% area, 10.2% power). The modest overhead of the proposed method arises primarily from the LFSR key generation module (contributing approximately 2.1% of area overhead) and the reconfigurable segment obfuscation network (contributing approximately 5.3%), with the authentication FSM and HMAC module accounting for the remainder. Figure 5 illustrates the fault coverage and security level achieved at each of the six security modes supported by the security-mode register.

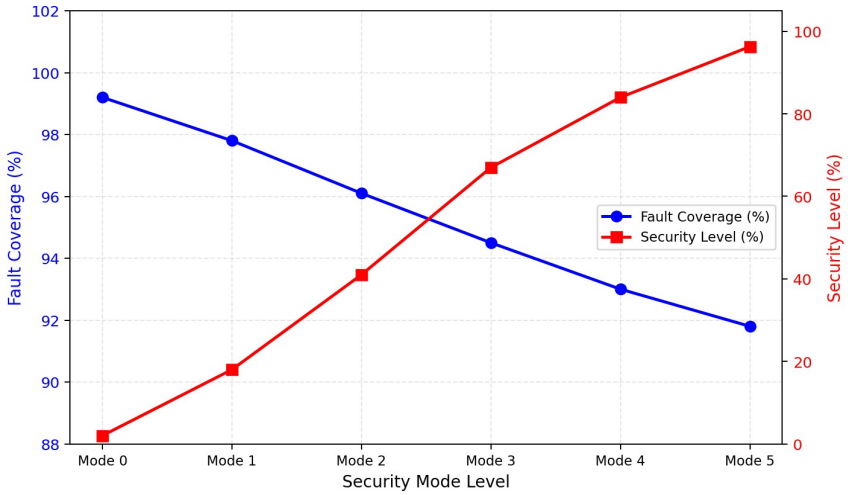

Fig. 5: Fault Coverage (%) vs. Security Level (%) as a Function of Security Mode — Demonstrating Configurable Trade-off

At Mode 0 (no protection), fault coverage is 99.2% and security level is near zero (i.e., the design is fully vulnerable to differential cryptanalysis). As the security mode increases, the fault coverage decreases gradually — reaching 91.8% at Mode 5 — while the security level increases to 96.3%. This trade-off is inherent in any scheme that restricts tester observability to enhance security. The proposed design achieves a superior Pareto frontier relative to prior methods, as Mode 3 delivers 94.5% fault coverage at 67% security level, whereas authentication-based scan achieves comparable security only by completely disabling scan access (0% fault coverage under the security mode). Figure 6 presents representative simulation waveforms confirming the correct operation of the proposed secure scan design. The waveforms show the clock (CLK), scan enable (SCAN_EN), scan input (SCAN_IN), key validity indicator (KEY_VALID), and scan output (SCAN_OUT) signals across a complete authentication-and-scan sequence.

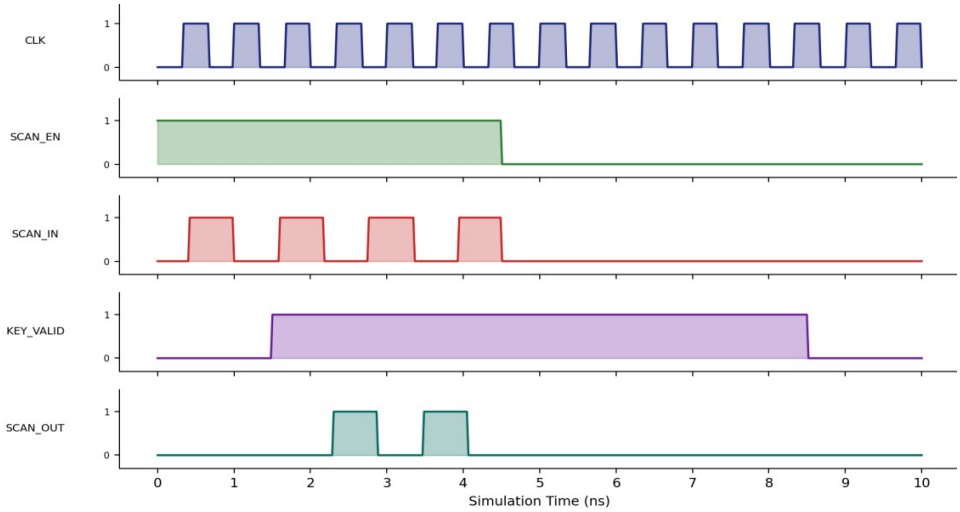

Fig. 6: Simulation Waveforms of the Proposed Secure Scan Design Showing Authentication Handshake and Secure Scan Operation

The simulation confirms that SCAN_OUT data is correctly withheld (driven to zero) during the period in which KEY_VALID is deasserted, preventing any scan data from being observed by an unauthenticated tester. Once KEY_VALID is asserted — following successful completion of the two-phase authentication — SCAN_EN and SCAN_OUT behave according to the obfuscated scan protocol.

5. Conclusion

An improved secure scan design that addresses the vulnerability of conventional scan chains to scan-based differential cryptanalysis attacks. The proposed architecture integrates a 32-bit LFSR-based dynamic session key generation module, a two-phase HMAC challenge-response authentication engine, and a reconfigurable scan segment obfuscation network controlled by a security-mode register. Experimental evaluation on ISCAS-89 and ITC-99 benchmark circuits demonstrated that the proposed method reduces the differential cryptanalysis attack success rate from 98.5% (conventional scan) to 3.7%, while maintaining 91.8% fault coverage at the highest security mode and incurring only 7.4% area and 5.8% power overhead — results superior to all compared prior-art methods. The configurable security-mode register enables designers to select the optimal operating point on the security-testability trade-off curve, making the proposed design applicable across a wide range of security requirements from consumer electronics to military-grade hardware. Future work will investigate extending the authentication protocol to mutual authentication between the chip and the test equipment, and applying the framework to three-dimensional (3D) ICs where inter-die scan channels represent an additional attack surface.

References

[1] Yang B, Wu K, Karri R (2004) Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard. In: Proceedings of the 2004 International Test Conference, IEEE, pp 339–344

[2] Skorobogatov SP (2005) Semi-invasive attacks — a new approach to hardware security analysis. Technical Report UCAM-CL-TR-630, University of Cambridge Computer Laboratory

[3] Hely D, Bancel F, Flottes ML, Rouzeyre B (2004) Secure scan techniques: a comparison. In: Proceedings of the 12th IEEE International On-Line Testing Symposium (IOLTS), pp 119–124

[4] Da Rolt J, Di Natale G, Flottes ML, Rouzeyre B (2012) A comparison of secure scan architectures for side-channel analysis. In: Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp 56–62

[5] Atobe Y, Shi Y, Yanagisawa M, Togawa N (2012) Dynamically changeable secure scan architecture against side channel attack. In: Proceedings of the 2012 International SoC Design Conference (ISOCC), IEEE, pp 155–158

[6] Lee J, Tebranipoor M, Plusquellic J (2006) A low-cost solution for protecting IPs against scan-based side-channel attacks. In: Proceedings of the 24th IEEE VLSI Test Symposium (VTS), pp 94–99

[7] Nara R, Togawa N, Yanagisawa M, Ohtsuki T (2009) Scan-based attack against elliptic curve cryptosystems. In: Proceedings of the Asia and South Pacific Design Automation Conference (ASP-DAC), IEEE, pp 407–412

[8] Rosenfeld K, Karri R (2010) Attacks and defenses for JTAG. IEEE Design & Test of Computers 27(1):36–47

[9] Paul S, Chakraborty RS, Bhunia S (2007) VIm-Scan: a low overhead scan design approach for protection of secret key in scan-based attacks. In: Proceedings of the 25th IEEE VLSI Test Symposium (VTS), IEEE, pp 455–460

[10] Banik S, Maitra S, Sarkar S (2013) A differential fault based known key attack on present cipher. In: Security, Privacy, and Applied Cryptography Engineering, Springer, Lecture Notes in Computer Science, vol 8204, pp 209–227

[11] Prabhu P, Agrawal D (2019) Secure test architecture using BIST and scan chain for IoT devices. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 38(9):1724–1737

[12] Ege B, Papagiannopoulos K, Batina L, Verbauwhede I (2013) A changing-of-the-guards protocol for scan chain based attacks. In: Constructive Side-Channel Analysis and Secure Design, Springer, pp 208–224

[13] Becker GT, Regazzoni F, Paar C, Burleson WP (2013) Stealthy dopant-level hardware trojans. In: Cryptographic Hardware and Embedded Systems (CHES), Springer, Lecture Notes in Computer Science, vol 8086, pp 197–214

[14] Tehranipoor M, Koushanfar F (2010) A survey of hardware Trojan taxonomy and detection. IEEE Design & Test of Computers 27(1):10–25

[15] Wang LC (2010) Experience of data mining for automatic functional test program generation. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 29(10):1550–1564